www.refaad.com

المجلة الدولية للدراسات القانونية والفقهية المقارنة

International Journal of Legal and Comparative Jurisprudence Studies (LCJS)

Journal Homepage: https://www.refaad.com/views/LCJS/Home.aspx

ISSN: 2708-6607(Online) 2708-6593(Print)

مواجهة الإرهاب السيبراني في القانون الجزائي الأردني والمعاهدات الدولية

عقل يوسف مقابلة

أستاذ القانون الجنائي- قسم القانون العام-كلية القانون- جامعة اليرموك- الأردن

makableh@yu.edu.jo

استلام البحث: ٢٠٢٠/٩/٨ مراجعة البحث: ٢٠٢٠/٩/٢٧ قبول البحث: ٢٠٢٠/١٠/٢٥ **DOI:** https://doi.org/10.31559/LCJS2020.1.3.1

الملخص:

ظهرت جريمة الإرهاب السيبراني في أعقاب التطور المتسارع الذي طرأ في عالم التكنولوجيا الرقمية والشبكة المعلوماتية التي أتاحت لبعض الأفراد والجماعات القيام بالأعمال الإرهابية، وسهلت عمل هذه الجماعات والترويج لها،وتمويلها، وارتكاب أشكال متعددة من الجرائم، كجرائم المخدرات، ونشر الأفلام الإباحية، والدخول إلى المواقع الإلكترونية بدون إذن أصحابها، والإطلاع على المعلومات الموجودة عليها أو إتلافها.

ولقد أصبحت جريمة الإرهاب السيبراني ظاهرة خطيرة عابرة للحدود والقارات تهدد شريحة كبيرة من سكان العالم لأن الجناة يلجأون إلى وسائل مختلفة عند القيام بها، الأمر الذي أوجب على مختلف الدول القيام بالعديد من الجهود من أجل مكافحتها والحد من مخاطرها. ولكن الجهود التي بذلت على المستوى الوطني أو الدولي لم تكن كافية للحد من هذه الظاهرة، بسبب العديد من العقبات التي حدت من فاعلية هذه الجهود، كعدم اتفاق الدول على الأفعال التي تشكل جريمة الإرهاب السيبراني، هذا بالإضافة إلى نقص الخبرة لدى أجهزة مراقبة وملاحقة الجناة في بعض الدول.

وقد انتهت هذه الدراسة إلى مجموعة من التوصيات أهمها تفعيل التعاون الدولي في مجال المكافحة، وضرورة توفير كوادر قادرة على المراقبة والملاحقة، وتوفير المعدات اللازمة لهم.

الكلمات المفتاحية: التكنولوجيا الرقمية والشبكة المعلوماتية؛ الجريمة العابرة للحدود؛ القانون والانترنت؛ المواقع الإلكترونية؛ مخاطر الشبكة المعلوماتية؛ مكافحة الإرهاب.

المقدمة:

تُعد جريمة الإرهاب السيبراني ظاهرة خطيرة تهدد حقوق الأفراد ومصالحهم في مختلف أنحاء العالم. وقد اتخذت هذه الجريمة العديد من الأشكال حتى بات من الصعب ضبطها والسيطرة عليها.

وقد ظهرت هذه الجريمة مع التطور السريع الذي طرأ في علم التكنولوجيا الرقمية والشبكة المعلوماتية التي أتاحت القيام بالأعمال الإرهابية على كافة الصعد، فسهلت عمل الجماعات الإرهابية والترويج لها وتمويلها، وكذلك سهلت ارتكاب جرائم القرصنة ونشر الأفلام الإباحية وتجارة المخدرات...الخ.

وقد أصبحت هذه الجريمة ظاهرة عابرة للحدود والقارات، وتهدد شريحة كبيرة من سكان العالم، لأن الجناة يلجأون إلى وسائل متعددة ومتنوعة عند القيام بها.

ومن أجل الحد من هذه الظاهرة الآفة بذلت جهود حثيثة سواءً على المستوى الدولي أو الوطني من أجل الحد منها، كإصدار الأمم المتحدة العديد من القرارات، وكذلك إبرام بعض الاتفاقات الأقليمية من أجل مكافحتها. ولكن هذه الجهود اصطدمت بعدد من الصعوبات التي حدت من ذلك بسبب سهولة استخدام الإنترنت، ونقص الخبرة الفنية لدى الأجهزة الأمنية المختصة بالمراقبة والملاحقة والمعاقبة، وعدم وجود اتفاق دولي على الأفعال التي

تشكل جريمة الإرهاب السيبراني، لأن ما يعد جريمة في بعض الدول يعد مباحاً في دول اخرى، وصعوبة إثبات هذه الجريمة نظراً لصعوبة الوصول إلى الدليل بسبب سهولة محوه من قبل الجاني، ونقص التعاون الدولي بين أجهزة المراقبة والملاحقة وعدم قيام الكثير من الأفراد والمؤسسات (كالبنوك) بالإبلاغ عن هذه الجريمة خوفاً من تراجع ثقة العملاء بها.

مشكلة البحث:

تكمن مشكلة البحث في عدم وجود تعريف دولي للإرهاب السيبراني، وعدم وجود معاهدة دولية خاصة بالإرهاب السيبراني، وعدم كفاية الجهود التي بذلت لمواجهته وخاصة على المستوى الدولي، حيث أصبح الإرهاب السيبراني يشكل ظاهرة خطيرة عابرة للحدود وتهدد شريحة كبيرة من سكان العالم.

أهمية البحث:

تسليط الضوء على المخاطر الناجمة عن التقدم التكنولوجي وما نتج عنه من جرائم متعددة قد يكون أخطرها الإرهاب السيبراني(الإلكتروني).

أهداف البحث:

حض مختلف دول العالم على بذل كل الجهود الممكنة من أجل مكافحة هذه الجريمة،وذلك من خلال سن وتعديل القوانين باستمرار من أجل مواكبة التطور المتسارع في وسائل الاتصال وتكنولوجيا المعلومات، وتفعيل التعاون من أجل هذه الغاية المهمة سواء على المستوى الوطني أو الدولي وتبصير الأفراد والجماعات والحكومات بمخاطر هذه الجريمة.

منهجية البحث:

المنهج العلمي المتبع في البحث هو المنهج الوصفي،بحيث يتم عرض النصوص القانونية الوطنية ونصوص المعاهدات الدولية، وكذلك التعرض لبعض الأحكام القضائية والآراء الفقهية المتعلقة بالأمن السيبراني.

خطة البحث:

المبحث الأول: ماهية الإرهاب السيبراني.

المطلب الأول: تعريف الإرهاب السيبراني وسماته.

الفرع الأول: تعريف الإرهاب السيبراني.

الفرع الثاني: سمات الإرهاب السيبراني.

المطلب الثاني: أسباب الإرهاب السيبراني ومخاطره.

الفرع الأول: أسباب الإرهاب السيبراني.

الفرع الثاني: مخاطر الإرهاب السيبراني.

المبحث الثاني: وسائل الإرهاب السيبراني والجهود التي بذلت لمكافحته.

المطلب الأول: وسائل الإرهاب السيبراني.

المطلب الثاني: جهود مكافحة الإرهاب السيبراني والعقبات التي تحد من ذلك.

الفرع الأول: جهود مكافحة الإرهاب السيبراني.

الفرع الثاني: العقبات التي تحد من جهود المكافحة.

المبحث الأول: ماهية الإرهاب السيبراني

لاشك بأن الإرهاب السيبراني قد أصبح ظاهرة اجتماعية تعاني منها الكثير من الدول والأفراد، وذلك بسبب الآثار السلبية التي تنجم عنها. لذلك لابد من تعريف القارئ بهذه الجريمة، وسماتها، وأسبابها، ومخاطرها.

وبناءً عليه قسّم هذا المبحث إلى مطلبين خصص المطلب الأول لتعريف الإرهاب السيبراني وسماته،وخصص المطلب الثاني لأسباب الإرهاب السيبراني ومخاطره.

المطلب الأول: تعريف الإرهاب السيبراني وسماته

قسم هذا المطلب إلى فرعين، خصص الأول منهما لتعريف الإرهاب السيبراني وخصص الثاني لسمات الإرهاب السيبراني.

الفرع الأول: تعريف الإرهاب السيبراني

أولاً: تعريف الإرهاب السيبراني على المستوى الوطني:

بما أن الإرهاب السيبراني نوع من الإرهاب، فلا بد من الوقوف على تعريف المشرع للإرهاب بشكل عام ثم نأتي لتعريف الإرهاب السيبراني.

لقد عرف المشرع الأردني الإرهاب في المادة (١/١٤٧) من قانون العقوبات الأردني رقم (١٦) لسنة ١٩٦٠ وبغض النظر عن نوعه أو وسيلته بأنه كل عمل مقصود أو التهديد به أو الامتناع عنه أيا كانت بواعثه أو أغراضه أو وسائله يقع تنفيذا لمشروع إجرامي فردي أو جماعي من شأنه تعريض سلامة المجتمع وأمنه للخطر أو أحداث فتنة إذا كان من شأن ذلك الإخلال بالنظام العام أو إلقاء الرعب بين الناس أو ترويعهم أو تعريض حياتهم للخطر أو إلحاق الضرر بالبيئة أو المرافق والأملاك العامة أو الأملاك الخاصة أو المرافق الدولية أو البعثات الدبلوماسية أو احتلال أي منها أو الاستيلاء عليها أو تعريض الموارد الوطنية أو الاقتصادية للخطر أو إرغام سلطة شرعية أو منظمة دولية أو أقليمية على القيام بأي عمل أو الامتناع عنه أو تعطيل لتطبيق الدستور أو القوانين أو الأنظمة.

وكذلك فقد اعتبر المشرع الأردني في المادة (٢/١٤٧) من قانون العقوبات سالف الذكر الأعمال المصرفية المشبوهة من جرائم الإرهاب سواءً كانت متعلقة بأيداع الأموال أو بتحويلها إلى أي جهة لها علاقة بنشاط إرهابي.

ومما يلاحظ على هذا التعريف بأنه تعريف عام ومطول قد ينطبق على مختلف انواع الإرهاب مع اختلاف الوسيلة احيانا كما هو الشأن في الإرهاب السيبراني، والدليل على ذلك أن المشرع الأردني قد وضع تعريفا جديدا خاصا بالإرهاب السيبراني في قانون منع الإرهاب الأردني رقم (٥٥) لسنة ٢٠٠٦ حيث جاء بالمادة(٣/هـ)منه مع مراعاة أحكام قانون العقوبات أو أي قانون آخر، تعتبر الأعمال التالية في حكم الأعمال الإرهابية المحظورة،وهي استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني لتسهيل القيام بالأعمال الإرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم.

وكذلك جاء بالمادة (١٥) من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥ بأن كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

ثانياً: التعريف الدولي للإرهاب السيبراني:

لقد صرح نيل والش رئيس قسم الجرائم الإلكترونية في إدارة مكافحة غسل الأموال وتمويل الإرهاب بالأمم المتحدة في مقابلة في برنامج بلا حدود الذي نشرته قناة الجزيرة بتاريخ ٢٠١٩/٦/٥ بأنه لا يوجد تعريف موحد لدى الأمم المتحدة لتعريف الجرائم السيبرانية -رغم خطورتها- نظراً لأسباب مختلفة بعضها سياسي، وبالتالي فإن الأمر في تعريفها يعتمد على ما تحدده القوانين في كل دولة كما تختلف وفقاً للتقسيم السياسي والمالي.

ورغم ذلك فان اتفاقية مجلس أوروبا التي أبرمت في مدينة بودابست عام ٢٠٠١ المتعلقة بالجريمة السيبرانية عرفت الإرهاب السيبراني بأنه (هجمات غير مشروعة،أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً توجه من أجل الانتقام أو الابتزاز أو إجبار الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية).

ثالثاً: تعريف الفقه للإرهاب السيبراني:

وبما أن الإرهاب السيبراني جريمة حديثة ولها وسائلها الخاصة بها وهي نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني فقد تم تعريفه بأنه(التخويف أو التهديد المادي أو المعنوي باستخدام الوسائل الإلكترونية،وقد تقوم به الدول أو الجماعات أو الأفراد على الإنسان بدينه أو نفسه أو عقله أو عرضه أو ماله،بغير حق،وبشتى صور الافساد في الأرض) [١].

وعرف الإرهاب السيبراني أيضا بأنه فعل إجرامي يرتكب باستخدام تكنولوجيا المعلومات والاتصالات،ينتج عنه تدمير أو تعطيل للخدمات من أجل خلق حالة من الخوف وسط الجمهور بغرض إكراه الحكومات أو الجمهور للقبول بأجندة سياسية أو اجتماعية أو فكرية معينة[٢].

[١] عبد الرحمن بن عبد الله السند،٢٠٠٤، وسائل الإرهاب الإلكتروني وحكمها في الاسلام وطرق مكافحتها،المؤتمر العالمي- موقف الاسلام من الإرهاب، جامعة الأمام محمد بن سعود الاسلامية،السعودية،ص٨.

[٢] بندر عقاب درويش،٢٠١٧،الاثبات في جرائم الإرهاب الإلكتروني، رسالة ماجستير قدمت لجامعة العلوم الاسلامية-عمان-الاردن،ص١٦.

وقد عرفه البعض بأنه التهديد أو الهجوم غير القانوني بشن هجمات على أجهزة الكمبيوتر وأنظمة المعلومات والبرامج والبيانات بهدف ترهيب وإكراه الحكومات من أجل تحقيق أهداف مختلفة[٣].

وبناءً على ما تقدم يستطيع الباحث تعريف الإرهاب السيبراني بأنه عبارة عن هجمات مباشرة على البنية التحتية السيبرانية للضحية من خلال الشبكات المعلوماتية أو نظم المعلومات من أجل إفساد وظائف أنظمة المعلومات باستخدام فيروسات الكمبيوتر والديدان وغيرها أو من أجل القرصنة لهدم المواقع الإلكترونية وتعطيل الحياة اليومية باستهداف البنية التحتية التي تدار بأجهزة الكمبيوتر كتلك المتعلقة بالمرافق الطبية أو البورصات أو النقل أو الأنظمة المالية أو امدادات المياه وخدمات الاتصال .

الفرع الثاني: سمات الإرهاب السيبراني

هنالك مجموعة من السمات التي تميز الإرهاب السيبراني عن الإرهاب التقليدي ومن أهمها ما يلي:

أولاً: حداثة الإرهاب السيبراني:

يعتمد الإرهاب السيبراني على الموارد المعلوماتية والوسائل الإلكترونية التي هي نتاج التطور التقني في عصر المعلومات، وهذا يعني أنه يختلف عن الإرهاب التقليدي.

وبناءً على ذلك فأنه يعد من أبرز الجرائم المستحدثة التي ظهرت بعد التطور الهائل والسريع في مجال الإتصالات وتكنولوجيا المعلومات الذي تجاوز امكانات الدول وأضعف قدراتها في تطبيق قوانينها،لدرجة أن أمنها وأمن رعاياها أصبح مهدداً [٤] .

ثانياً: عابر للحدود والقارات:

يُعد الإرهاب السيبراني من الجرائم العابرة للحدود والقارات، بسبب استخدام الجناة الفضاء السيبراني من أجل نشر أهدافهم والتأثير على الرأي العام، وتجنيد أعضاء جدد من مختلف أنحاء العالم، والحصول على التمويل اللازم[٥].

وكذلك فإن الهجمات السيبرانية لا تتقيد بالموقع الجغرافي، مما يتيح للتنظيمات الإرهابية تنفيذ هجماتها على مختلف المواقع دون التواجد المادي بها، ودون التعرض لمخاطر الاعتقال أو الرد المضاد، على عكس الإرهاب التقليدي الذي يتطلب تواجد الإرهابيين جسديًا في المواقع المستهدفة لزرع الألغام، وإلقاء القنابل، وإطلاق النيران، وخطف الضحايا، وغير ذلك.[٦]

ثالثاً :صعوبة إثباته:

يتميز الإرهاب السيبراني بأنه من الصعب إثباته،بسبب عدم وجود أدلة مادية واضحة كما هو الحال في الإرهاب التقليدي[٧]، هذا بالإضافة إلى أن الجناة الذين يقومون بارتكابه أصحاب خبرة وعلى درجة عالية من الكفاءة، والقدرة على الخداع والتضليل [٨]، حيث أنه من الصعب الكشف عن هوية الإرهابيين في الفضاء السيبراني نظرًا لجملةٍ من الأسباب، يأتي في مقدمتها تعدد الطرق التقنية لإخفاء الهوية على الإنترنت؛ فقد يقوم مرتكبو الهجمات السيبرانية بتغيير عنوان بروتوكول الإنترنت- IP الذي يمكن استخدامه لتتبع مجرمي الإنترنت- عبر أجهزة الكمبيوتر المخترقة إلى مستخدمين أبرياء.

كما يتجه عددٌ كبير من متصفحي الإنترنت لاستخدام أسماء مستعارة، وتسجيل الدخول إلى مواقع الويب المختلفة بهوية مجهولة بقصد إخفاء هويتهم الحقيقية، فيصعب على الأجهزة الأمنية تعقبهم، هذا بالاضافة إلى أنه في الفضاء السيبراني لا توجد الحواجز المادية التي تقوض التنظيمات الإرهابية كالحدود القومية، ونقاط التفتيش، والجمارك، وغيرها، وكذلك اختلاف الزمان والمكان والقوانين المطبقة في الدول التي ترتكب فيها هذه الجريمة[٩].

---

[٣] رغده البهي،٢٠١٩،الإرهاب السيبراني:المفهوم والسمات والانماط، المركز المصري للفكر والدراسات الاستراتيجية،ص١.

[٤] خالد ممدوح ابراهيم،٢٠٠٩،الجرائم المعلوماتية،ط١،دار الفكر العربي الجامعي،الاسكندرية ،ص٨٦؛و د.عبدالرحمن البحر،١٩٩٩،معوقات التحقيق في جرائم الإنترنت-رسالة ماجستير،جامعة نايف العربية للعلوم الأمنية،ص٦.

[٥] جمال علي دهشان،٢٠١٨،الإرهاب في العصر الرقمي،المجلة الدولية للبحوث في العلوم التربوية،المجلد ١،العدد (٣)،ص٩٧؛ود.ليلى الجنابي،٢٠١٧،فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية،ص٤.الموقع: http://www.ahewar.org/debat/show.art.asp?aid=571423&r=0

[٦] رغدة البهي،المرجع السابق،ص٨.

[٧] عبد الرحمن عبد العزيز الشنيفي،١٩٩١،حرب المعلومات،مكتبة غريب-الرياض-المملكة العربية السعودية،ص١١٣.

[٨] محمد محي الدين عوضين،١٩٩٣،مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات،دار النهضة العربية-القاهرة،ص٤٧٦.

[٩] خالد يونس عرب،١٩٩٤،جرائم الحاسوب،رسالة ماجستير-الجامعة الأردنية،ص٨١؛دعاوى الجرائم الإلكترونية وادلة إثباتها في التشريعات العربية بين الواقع والمأمول أحد محاور المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية الذي عقد في السودان عام ٢٠١١م،١٤٣٣هـ.

رابعاً: سهولة ارتكابه وقلة تكاليفه:

بسبب سهولة هذه النوع من الإرهاب، فأنه يستهوي الكثير من الأفراد، فالركن المادي فيه يتم في الغالب بضغطة زر من أزرار الحاسوب وإمكانية القيام بذلك عن بعد، وكذلك قلة تكلفة ارتكابه،فهو لا يحتاج إلا لجهاز حاسوب والدخول على شبكة الإنترنت[١٠].

وبمعنى آخر فان تكلفة شن الهجمات السيبرانية أقل من تكلفة الإرهاب التقليدي، إذ يتطلب الأخير شراء الأسلحة والمتفجرات والمعدات، بجانب السفر والتخطيط والتدريب، وغير ذلك، بينما تقتصر متطلبات الإرهاب السيبراني على أجهزة الكمبيوتر الشخصية المتصلة بالإنترنت والمهارات التقنية اللازمة. ولا تتطلب الهجمات السيبرانية سوى الحد الأدنى من الموارد المالية بسبب انخفاض تكلفة أدوات الكمبيوتر وانتشارها، وسهولة الوصول إليها. ولا يتطلب الإرهاب السيبراني تدريبًا بدنيًّا مكثفًا أو معالجاتٍ نفسية كما هو الحال في الأشكال التقليدية للإرهاب، مما يقلل الخسائر البشرية في صفوف التنظيمات الإرهابية [١١].

خامساً: تعدد الخيارات المستهدفة:

يمكن أن يستهدف الإرهاب السيبراني أجهزة وشبكات الكمبيوتر الخاصة بالحكومات، والأفراد، والمرافق العامة، وشركات الطيران، وما إلى ذلك. مما يعني تنوع الأهداف المحتملة، وتعدد نقاط الضعف التي يمكن استهدافها. وتتزايد خطورة استهداف البنى التحتية الحيوية، مثل: شبكات الطاقة الكهربائية، وخدمات الطوارئ لتزايد تعقيد أنظمة الكمبيوتر التي تديرها، مما يعني بالتبعية صعوبة القضاء على كافة نقاط ضعفه[١٢].

سادساً: سرعة شن الهجمات:

يمكن إطلاق برامج ضارة مثل فيروسات الكمبيوتر والديدان ونشرها بسهولة خلال فترة زمنية قصيرة للغاية دون أدنى تدخلٍ بشري. وجدير بالذكر أن السرعة التي تنتشر بها تلك البرامج الضارة لا تتصل بالمهاجم، بل بسرعة اتصال الضحايا بالإنترنت[١٣].

وفي الختام يمكن القول بأن الإرهاب السيبراني يتميز بمجموعة من السمات التي تميزه عن الإرهاب التقليدي سواءً أثناء الهجوم أو أثناء الدفاع.

المطلب الثاني: أسباب الإرهاب السيبراني ومخاطره

قسم هذا المطلب إلى فرعين،خصص الأول منهما لأسباب الإرهاب السيبراني،وخصص الثاني لمخاطر الإرهاب السيبراني.

الفرع الأول: أسباب الإرهاب السيبراني

هناك العديد من الأسباب التي تسهم في ارتكاب جريمة الإرهاب السيبراني، ومن أهمها ما يلي:

أولاً: التطور العلمي والتكنولوجي الذي هيأ المجال الخصب لأحداث تغييرات متنوعة على كافة المجالات ومنها تطور مظاهر الإرهاب السيبراني،ففي مجال الجريمة استفاد المجرمون من معطيات العلم والتكنولوجيا، ونظم المعلومات، والاتصالات المتطورة، الأمر الذي ساهم في ظهور القلاقل السياسية والاجتماعية في كثير من دول العالم، ومثال ذلك ظهور الكثير من الجرائم التي لم تكن معروفة، كجرائم الحاسوب والإنترنت وجرائم المعلوماتية[١٤].

ثانياً: تهميش الشباب، وعدم اشتراكهم في العمل السياسي، وعدم إيجاد فرص عمل لهم لتصريف طاقاتهم في عمل نافع وما ينجم عن ذلك من فقر وعوز يجعلهم عاجزين عن تأمين احتياجاتهم قد يدفع البعض منهم إلى الانحراف والالتحاق بالجماعات الإرهابية من أجل الحصول على المال[١٥].

ثالثاً: صعوبة الرقابة على الإنترنت، وصعوبة المحاسبة على ما ينشر فيه مما جعله مرتعاً خصباً للإرهابيين لأنه بيئة مناسبة لممارسة الأعمال الإرهابية ونشر الأفكار المتطرفة التي تفسد وجدان البعض من الأفراد وتدفع بهم إلى التمرد من أجل تحقيق أهداف خاصة تتعارض مع مصالح المجتمع[١٦].

رابعاً: تمتع الإرهابيين بقدرة وخبرة عاليتين ومتميزتين في استيعاب نظم وبرامج الإنترنت وتوظيفها في تحقيق أهدافهم[١٧].

خامساً: ضعف الرقابة على الشبكات المعلوماتية: إن ضعف الرقابة على الشبكات المعلوماتية يجعلها عرضة للاختراق من قبل الجماعات الإرهابية، وذلك بسبب انفتاحها وغياب القيود والحواجز الأمنية غالباً، وهذا يسهل الدخول إلى الحواسيب بدون إذن أو تصريح [١٨] للحصول على المعلومات

---

[١٠] محمود احمد عبابنة؛ومحمد عمر الرازق ،٢٠٠٩،جرائم الحاسوب وأبعادها الدولية،ط١،دار الثقافة-عمان،ص٣٠؛

[١١] رغدة البهي،المرجع السابق،ص٧.

[١٢] رغدة البهي،المرجع السابق،ص٨.

[١٣] رغدة البهي،المرجع السابق،ص٨؛و د.ليلى الجنابي،المرجع السابق،ص٤.

[١٤] حنين بوادي ،٢٠٠٤،تجربة مواجهة الإرهاب،ط١،دار الفكر الجامعي-الاسكندرية،ص١٦.

[١٥] بدر هويمل الزبن،٢٠١٢،الإرهاب في الفضاء الإلكتروني، رسالة ماجستير-جامعة عمان العربية،الاردن،ص٧٦؛عبد الفتاح بيومي حجازي،٢٠٠١،مكافحة جرائم الكمبيوتر والإنترنت،دار الفكر العربي-الاسكندرية،ص١٠٦.

[١٦] بدر هويمل الزبن،المرجع السابق،ص٧٧.

[١٧] بدر هويمل الزبن،المرجع السابق،ص٧٧.

[18] Rizger M.kadir:the offense of unauthorized access in computer crimes legislation a comparative study,journal of shria and law,issue no.40-october 2009,p48.

وخاصة التي تتعلق بالأمن القومي أو علاقة الدولة بغيرها من الدول،علما بأنه يمكن الولوج لتلك المعلومات باستخدام عدة برمجيات إلكترونية [١٩] ،من أهمها فيروسات الحاسوب، كالديدان، حصان طروادة، والرقائق، والقنابل.

١. الديدان: وهي عبارة عن برامج يتم إرسالها عن طريق شبكة المعلومات من أجل التخريب وسرقة البيانات الشخصية أو قطع الاتصال بشبكة الإنترنت.
٢. حصان طروادة: وهو عبارة عن شيفرة توضع في أحد البرامج التي تستخدم بكثرة وهي تسمح بسرقة البيانات ومن الصعب اكتشافها لأنها سريعة الانتقال بين برمجيات الجهاز.
٣. الرقائق: وهي العقل المدبر في الأجهزة الإلكترونية، تكون مربوطة بصورة مباشرة مع مصدرها، ويمكن إيقاف الجهاز الذي تعمل عليه بوقت معين من خلال الاتصال بها عن بعد.
٤. القنابل: وهي نبضات كهرومغناطيسية يتم القائها في موقع إلكتروني حساس وحين تنفجر تقوم بمسح كافة البيانات والمعلومات عن الأجهزة الإلكترونية[٢٠].

الفرع الثاني: مخاطر الإرهاب السيبراني

تزداد مخاطر الإرهاب السيبراني في الدول المتقدمة وذلك بسبب اعتمادها بشكل أساسي على الأنظمة المعلوماتية مما جعلها هدفاً سهلاً للهجمات الإرهابية. فبدلاً من استخدام الأسلحة تستطيع الجماعات الإرهابية من خلال جهاز كمبيوتر متصل بالإنترنت من تدمير بنية معلوماتية يفوق أثرها أثر التفجيرات، وقد تخترق أنظمة الملاحة الجوية أو البحرية وتقوم بتغيير مسارات الطائرات والسفن أو شل حركتها، وقد تكون هذه الهجمات موجهة على المصارف وشبكات المال العالمية أو المحلية [٢١] .

وبمعنى آخر فقد أدى التطور التكنولوجي إلى سهولة قيام الجماعات الإرهابية بشن الهجمات الإرهابية السيبرانية السرية والعلنية من أجل استهداف البيانات العسكرية أو المالية أو محطات الطاقة.

ويمكن تلخيص أهم الأهداف التي تشن عليها الهجمات الإرهابية السيبرانية[٢٢] بما يلي:

١. استهداف البنية التحتية للمنظومات الاقتصادية.
٢. سرقة المعلومات العسكرية أو تبديلها أو تدميرها إلكترونياً.
٣. السيطرة على الأنظمة العسكرية، وذلك من خلال التحكم بمحطات إطلاق الصواريخ.
٤. الهجوم على أهداف ومواقع إلكترونية.
٥. الحرب النفسية،وذلك من خلال إرسال رسائل بريدية أو عن طريق الهاتف تحتوي على تهديد أو مطالب معينة.
٦. تشويه صورة الرموز الوطنية من خلال الادعاءات الكاذبة التي يتم نشرها عبر مواقع التواصل الاجتماعي ومثال ذلك التدخل في الانتخابات الذي يتم عبر بث معلومات وأخبار زائفة، أو استخدام برامج حاسوبية مكررة أصبحت تباع وتشترى لتشويه صورة بعض الأفراد أو لتلميع صورة افراد آخرين.

وفي الختام نستطيع القول بأنه توجد عدة مظاهر للإرهاب السيبراني [٢٣] ومن أهمها:

١. المظهر الأمني: حيث تعمل الجماعات الإرهابية من خلال السلاح الإلكتروني على قطع شبكات الاتصال بين الوحدات العسكرية والأجهزة الأمنية والقيادات المركزية وتعطيل أنظمة الملاحة الجوية والبحرية وإخراج الصواريخ عن مسارها.
٢. المظهر السياسي: تقوم الجماعات الإرهابية بتهديد القيادات السياسية البارزة بالقتل، أو اختراق البريد الإلكتروني الخاص بهم وإفشاء اسرارهم، أو تهديدهم بتفجير بعض المنشآت الوطنية ان لم يستجيبوا لمطالب الإرهابيين.

[١٩] احمد خليفة الملط،٢٠٠٥،الجرائم المعلوماتية،دار الفكر الجامعي، ط١، الاسكندرية،ص١٤٦.
[٢٠] أيهاب خليفة،٢٠١٧،القوة الإلكترونية،المركز العربي للنشر والتوزيع-ابو ظبي ،ص٨٣.
[٢١] مصطفى يوسف الكافي،٢٠١١،الإدارة الإلكترونية إدارة بلا أوراق،مؤسسة رسلان للطباعة والنشر والتوزيع-دمشق-سوريا،ص٤٣٧.
[٢٢] أيهاب خليفة،المرجع السابق،ص١٢٩.
[٢٣] علي عبد الفتاح،٢٠١٦،الإعلام الدبلوماسي والسياسي،البازوري للنشر-عمان-الاردن،ص٢٠٧.

٣. المظهر الاقتصادي: ويتم ذلك من خلال اختراق أنظمة المصارف والأسواق المالية مما يلحق الضرر باقتصاد الدولة واستثماراتها الدولية والوطنية[٢٤]، نتيجة قيام جماعات إرهابية متخصصة باستغلال وسائل التواصل الاجتماعي الإلكترونية لنقل الاموال المحظورة وتوظيف العملات الرقمية كالبيتكوين .

٤. المظهر الاجتماعي: تقوم الجماعات الإرهابية باختراق المواقع الإلكترونية الإباحية من أجل إفساد بعض أفراد المجتمع وخاصة المراهقين منهم،مما يؤدي إلى زيادة ارتكاب الجرائم الماسة بالعرض[٢٥] .

المبحث الثاني: وسائل الإرهاب السيبراني والجهود التي بذلت لمكافحته

قسم هذا المبحث إلى مطلبين،خصص الأول منهما لوسائل الإرهاب السيبراني(علما بأن هذه الوسائل تمثل أركان جريمة الأمن السيبراني شريطة توافر القصد الجرمي لدى الجاني)،وخصص الثاني لجهود مكافحة الإرهاب السيبراني والعقبات التي تحد من ذلك.

المطلب الأول: وسائل الإرهاب السيبراني

تنص المادة(٣) من قانون منع الإرهاب الأردني رقم (٥٥) لسنة ٢٠٠٦ على أنه(مع مراعاة أحكام قانون العقوبات أو أي قانون آخر تعتبر الأعمال التالية في حكم الأعمال الإرهابية المحظورة).

وما يهمنا في هذا المقام هو الأعمال المحظورة التي نصت عليها الفقرة(ه) من المادة الثالثة المذكورة أعلاه وهي (استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر اعمال عدائية أو انتقامية تقع عليهم).

وكذلك تنص المادة (١٥) من قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ على أنه(كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها يعاقب بالعقوبة المنصوص عليها في ذلك التشريع).

ونلاحظ من النصين السابقين بأن المشرع الأردني قد جرم استخدام النظام المعلوماتي أو شبكة الإنترنت أو المواقع الإلكترونية أو أي وسيلة نشر أو اعلان تسهل القيام بأعمال إرهابية أو تدعم جماعة أو جمعية تقوم بأعمال إرهابية أو تروج افكارها أو التي تفسد القيم والأخلاق وتشجع على العنف[٢٦]، أو تمولها ،واعتبرها من الأعمال المحظورة المعاقب عليها بالأشغال المؤقتة أو المؤبدة بموجب المادة(١٤٨) من قانون العقوبات الأردني رقم (١٦) لسنة ١٩٦٠.

وبناءً عليه نرى ان وسائل ارتكاب جريمة الإرهاب السيبراني متعددة،ومن أهمها ما يلي:

أولاً:البريد الإلكتروني:

يُعد البريد الإلكتروني من أبرز الخدمات التي تقدمها شبكة الإنترنت، وذلك بسبب سرعة إيصال الرسائل وسهولة الاطلاع عليها في أي مكان في العالم[٢٧].

ورغم أن البريد الإلكتروني قد أصبح أكثر الوسائل استخداما في مختلف الانشطة،إلا أنه يعد من أكثر الوسائل المستخدمة في الإرهاب السيبراني،حيث يمكن من خلاله تحقيق التواصل بين الشبكات والخلايا الإرهابية المتواجدة في اماكن مختلفة ويتم تبادل المعلومات فيما بينها،علما بأن الكثير من العمليات الإرهابية التي حدثت مؤخرا كان للبريد الإلكتروني الدور الاكبر في التواصل وتبادل المعلومات بين المخططين للعمليات الإرهابية وبين القائمين بها[٢٨] .

ولا يفوتنا ان نذكر في هذا المقام ان البريد الإلكتروني قد يكون هدفا من أهداف الإرهاب عندما يتم اختراق بريد الآخرين بهدف التجسس عليهم والاطلاع على أسرارهم وتوظيفها في العمليات الإرهابية[٢٩].

---

[٢٤] عبد الله عبد العزيز فهد العجلان،٢٠٠٨،الإرهاب الإلكتروني في عصر المعلومات،بحث قدم في المؤتمر الدولي لحمأية أمن المعلومات والخصوصية في قانون الإنترنت الذي عقد في القاهرة بتاريخ ٢-٢٠٠٨/٦/٤،ص١٩:نأيل عبد الرحمن صالح،٢٠٠٤،واقع جرائم الحاسب الآلي في التشريع الأردني،مؤتمر القانون والكمبيوتر والإنترنت-جامعة الامارات العربية المتحدة،كلية الشريعة والقانون،المجلد الأول،ط٣،وقد عقد المؤتمر من ١-٣/مأيو/٢٠٠٠،ص١٨٩.

[25] Dolf Zillman and Jennings Bryant,"pornography, sexual callousness, and the trivialization of rape", journal of communications 32,1982, p32.

[26] Raed S A Faqir, Saleh Sharari, Salameh A. Salameh, cyber-crimes and technical issues under the Jordanian information system crimes law, Journal of politics and law No2,2014, p4.

[٢٧] عبد الرحمن بن عبد الله السند،مرجع سابق،ص٣٥:احمد علي احمد الزبون،٢٠١٥،الجرائم الواقعة على أمن الدولة الداخلي في الشريعة الاسلامية والقانون الأردني،ص١٥٤.

[٢٨] عبد الرحمن بن عبد الله السند،مرجع سابق،ص٣٦.

[٢٩] محمد سعيد عبد المجيد،٢٠٠٦،المعلوماتية والجريمة،مكتبة الاسراء للطبع والنشر والتوزيع-طنطا-مصر،ص٨٥.

ثانياً: تدمير و إنشاء المو اقع الإلكترونية:

يقصد بتدمير المواقع الإلكترونية الدخول غير المشروع إلى نقطة ارتباط رئيسية أو فرعية متصلة بالإنترنت بهدف تدمير نقطة الاتصال أو النظام، أو تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت، علماً بأن عملية الاختراق وتسريب البيانات والرموز الخاصة ببرامج شبكة الإنترنت تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي اخترق فيها الموقع، فالبعد الجغرافي لا أهمية له في الحد من عمليات الاختراق الإلكترونية[٣٠].

وقد يتم تدمير المواقع الإلكترونية عن طريق ضخ عشرات الآلاف من الرسائل الإلكترونية من الحاسوب الخاص بالشخص المدمر إلى الموقع المستهدف من أجل التأثير على السعة التخزينية للموقع،فتشكل هذه الرسائل الإلكترونية ضغطا يؤدي إلى تخريب الموقع العامل على الشبكة،وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي(الخارق) أو تمكنه من حرية الاطلاع وتصفح الموقع المستهدف بسهولة،والحصول على كل ما يريده من معلومات وأرقام وبيانات خاصة بالموقع المعتدى عليه[٣١].

وقد يقوم الأفراد والجماعات الإرهابية بإنشاء مواقع إلكترونية لهم عبر الإنترنت من أجل نشر أفكارهم ودعواتهم إلى الإضرار بالمجتمعات، ونشر الرذيلة بين الأفراد من خلال إنشاء المواقع الإلكترونية الإباحية[٣٢] ومن أجل تجنيد أشخاص جدد وضمهم إلى جماعاتهم، كما يقومون بنشر الوسائل التي يتبعونها عند القيام بجرائمهم،علما بأنهم يعتمدون في مخططاتهم على طرق بسيطة تتيح للجميع الدخول إلى مواقعهم وتصفحها بكل يسر وسهولة[٣٣].

ثالثاً: اختراق الحماية الأمنية للمعلومات السرية باستخدام الفيروسات:

تقوم الجماعات الإرهابية بمهاجمة أجهزة الحاسوب والشبكات المعلوماتية من أجل تحقيق الأهداف التي تسعى اليها.وتكون هذه الطريقة أكثر خطورة كلما كان الجناة أكثر خبرة ودراية في تكنولوجيا المعلومات،ومن أهم الأهداف التي يسعون إلى تحقيقها هي تدمير المواقع التي تمتلكها الدول أو الحكومات أو الأفراد أو الشركات أو اتلافها[٣٤].

والمقصود بالفيروسات هو البرامج التي لها قدرة على العمل في الخفاء، وللفيروس مجموعة من الشيفرات الهدف منها تعديل المعلومات أو تكرارها في أجهزة الحاسوب الخاصة بالضحية.

ومن أهم الأضرار التي تنتج عن الفيروسات:

١. الإضرار بالمعلومات والأسرار الموجودة بأجهزة الحاسوب المستهدفة والتي قد تكون مملوكة للدول أو الحكومات أو الأفراد أو الشركات أو المنظمات. ومثال ذلك ما قام به بعض الإرهابيين باختراق أجهزة الحاسوب الخاصة بوزارة الدفاع الأمريكية وسرقة ونشر مجموعة كبيرة من الوثائق والمستندات العسكرية[٣٥].
٢. إلحاق الضرر المادي بأجهزة الحاسوب المستهدفة نفسها وذلك بتعطيلها وشل حركتها، ومثال ذلك فيروس (Friday) الذي انتشر في المملكة المتحدة وتسبب في خسائر كبيرة في قطاع المصارف والشركات المملوكة للدولة والتي قدرت ب (١٥)مليار دولار[٣٦].

ومن الأمثلة على الفيروسات القنابل المعلوماتية وهي النبضة الكهرومغناطيسية (EMP) وهو مصطلح يطلق على نوع من الانفجار الكهرومغناطيسي الإشعاعي الذي ينشأ بسبب انفجار و/أو من تقلبات مفاجئة في المجال المغناطيسي. ويمكن الاستفادة من التغيرات السريعة في الحقول الكهربائية في بعض الأنظمة الكهربائية لتدمير عناصرها الإلكترونية بتأثير إنهيار الجهد.

ومن الأمثلة على القنابل المعلوماتية ما قام به أحد العاملين في مؤسسة حكومية فرنسية بزرع قنبلة زمنية في شبكة معلومات الشركة التي يعمل بها لكي تنفجر هذه القنبلة بعد ستة أشهر من تاريخ تركه للعمل، وهذا ما تم فعلا حيث انفجرت القنبلة وتسببت بخسائر كبيرة للشركة[٣٧].

---

[٣٠] موزة المزروعي، ٢٠٠٠، الاختراعات الإلكترونية خطر كيف نواجهه، مجلة افاق الاقتصادية، الامارات العربية المتحدة، العدد(٩)، ص٥٤.

[٣١] ولاء البحيري، ٢٠١٢، مستقبل الإرهاب الإلكتروني وأساليب مواجهته، مجلة النهضة-كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، مجلد(١٣)، العدد الرابع.

[32] Edward Donnerstein,"pornography: its effects on violence against women" in Malamuth and Donnerstein, eds,pornography and sexual aggression, academic press,1984

[٣٣] محمد عبد اللطيف عبدالعال، ١٩٩٤، جريمة الإرهاب، دار النهضة العربية-القاهرة، ص٥٤؛احمد علي احمد الزبون، مرجع سابق، ص١٥٦؛أيسر محمد عطية القيسي، ٢٠١٤، دور الاليات الحديثة في الحد من الجرائم المستحدثة، بحث قدم لمؤتمر الجرائم المستخدمة في ظل التغيرات الأقليمية والدولية الذي عقد في عمان بتاريخ ٢-٢٠١٤/٩/٤، ص٢.

[٣٤] زين العابدين عواد كاظم الكردي، ٢٠١٨، جرائم الإرهاب، منشورات الحلبي الحقوقية-بيروت، ص١١١.

[35] Raed S A Faqir, Saleh Sharari, Salameh A, previous reference, p8.

[٣٦] زين العابدين عواد كاظم الكردي، المرجع السابق، ص١١٢.

[٣٧] زين العابدين عواد كاظم الكردي، المرجع السابق، ص١١٢.

رابعاً: الاتصال والتخطيط والترويج الإعلامي:

تقوم الجماعات الإرهابية باستخدام البريد الإلكتروني وشبكات التواصل الاجتماعي الحديثة من أجل تبادل المعلومات والمقترحات بين أعضائها والتخطيط لعملياتها، وذلك لدرء المخاطر التي قد تنجم عن اللقاءات المباشرة بين اعضاء الجماعة الإرهابية، ومن أجل الابتعاد قدر الامكان عن استخدام وسائل الاتصال التقليدية التي قد يؤدي استخدامها إلى انكشاف أمر الإرهابيين[٣٨].

وتقوم الجماعات الإرهابية بنشر البيانات والتصريحات والنشرات من أجل بث الافكار المتطرفة التي تتبناها من خلال المواقع الإلكترونية الخاصة بها.

وكذلك تقوم بنشر الأخبار الكاذبة المضللة للأجهزة الأمنية والرأي العام، ونشر الآراء التي تبث الفرقة بين أبناءً المجتمع، والإساءة إلى الاديان والأخلاق[٣٩] أو الأعراف أو الأصول، وتشويه سمعة الاشخاص والتحريض عليهم، ونشر الأفلام الإباحية[٤٠] ونشر ثقافة العنف والتشجيع على الاستخدام المفرط له من خلال نشر الصور والتسجيلات ومقاطع الفيديو التي تمس بالأخلاق[٤١] والتي تحتوي على مشاهد مرعبة من أجل نشر الرعب والخوف بين الأفراد. ومن الأمثلة على ذلك نشر الجماعة الإرهابية(داعش) الفيديو الذي يحتوي على حادثة ذبح الرهائن الأقباط المصريين[٤٢]

ويضاف إلى ذلك قيام الجماعات الإرهابية باستخدام المواقع الإلكترونية التابعة لها من أجل الترويج للفكر الذي تتبناه، وزيادة اعداد الانصار، وكسب المزيد من الأتباع المتعاطفين مع أفكارها.

وكذلك تقوم الجماعات الإرهابية بالتجسس[٤٣]واستغلال المواقع الإلكترونية وغيرها من وسائل الاتصال الحديثة من أجل الحصول على الدعم المالي واللوجستي من أجل تامين المال اللازم لأنشطتها الإجرامية، وقد يتم ذلك من خلال التحويلات المالية غير المشروعة أو من خلال الوصول إلى حسابات عملاء البنوك وتحويل الاموال الموجودة في حساباتهم إلى الجماعات الإرهابية، أو من خلال الاتجار بالمخدرات وغسل الأموال والاتجار بالبشر أو الأسلحة أو الآثار[٤٤].

المطلب الثاني: جهود مكافحة الإرهاب السيبراني والعقبات التي تحد من ذلك

يُعد الإرهاب السيبراني من أحدث الجرائم العابرة للقارات التي تحتاج إلى تضافر الجهود الوطنية والدولية من أجل مكافحتها والحد من مخاطرها، وإزالة العقبات التي تحد من فاعلية هذه الجهود. علماً بأن من أهم العوامل التي يجب أخذها في الاعتبار هو قيام الدول بسن التشريعات الموضوعية والإجرائية الجنائية أولاً.

وبناءً عليه قسم هذا المطلب إلى فرعين خصص الأول لجهود المكافحة، وخصص الثاني للعقبات التي تحد من جهود المكافحة.

الفرع الأول: جهود مكافحة الإرهاب السيبراني

إن الجهود التي تبذل على المستوى الوطني لا تكفي لمكافحة جريمة الإرهاب السيبراني، لذلك لابد من تضافر الجهود التي تبذل على المستوى الوطني مع الجهود التي تبذل على المستوى الدولي من أجل مكافحة هذه الجريمة .

وبناءً عليه سنعرض لهذه الجهود في بندين نخصص البند الأول منهما لجهود المكافحة على المستوى الوطني، ونخصص الثاني منهما لجهود المكافحة على المستوى الدولي.

أولاً:جهود المكافحة على المستوى الوطني:

لقد جرم المشرع الأردني بشكل صريح وواضح استخدام النظام المعلوماتي والشبكة المعلوماتية أو المواقع الإلكترونية أو أي وسيلة نشر تسهل القيام بأعمال إرهابية وذلك من خلال سن عدد من القوانين التي تجرم وتعاقب على هذه الجريمة الخطيرة، ومثال ذلك قانون منع الإرهاب الأردني رقم (٥٥) لسنة ٢٠٠٦، وقانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥[٤٥]، بالإضافة إلى قانون العقوبات الأردني رقم (١٦) لسنة ١٩٦٠ الذي احتوى على بعض المواد التي تجرم وتعاقب على استخدام العنف أو التهديد باستخدامه بأي وسيلة كانت سواءً وسيلة تقليدية،أو وسيلة إلكترونية.

---

[٣٨] وليد محمد ابو ربة،٢٠١٢،التعرف على الإرهاب الإلكتروني،ندوة استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين التي عقدت في الرياض بتاريخ ٩-٢٠١١/٥/١١،منشورات جامعة نايف للعلوم الأمنية-الرياض،ص٥٣.

[39] Ulla Cralsson,"violence and pornography on media", Nordicom, Goteborg, 2006.

[40] Audrey: protection children on the internet mission impossible, pace law, faculty publication,2009, p326.

[41] Shihab A. Hameed, effects of internet drawbacks on moral and social values of users in education, Australian journal of basic and applied sciences,2011, p2.

[٤٢] فايز عبد الله الشهري،٢٠١٢،ثقافة التطرف والإرهاب على شبكة الإنترنت، منشورات جامعة الامير نايف للعلوم الأمنية-الرياض،ص١٦.

[43] David Freet and Rajeev Agrawal, Cyber Espionage, springer international publishing ,2017, p2.

[٤٤] فايز عبدالله الشهري،المرجع السابق،ص١٧.

[45] Raed S A Faqir. Saleh Sharari, Salameh A, previous reference, p7.

وعند الرجوع إلى قانون منع الإرهاب الأردني سالف الذكر نجد بأنه جاء بالمادة (٣/هـ) منه (مع مراعاة احكام قانون العقوبات أو أي قانون اخر، تعتبر الأعمال التالية في حكم الأعمال الإرهابية المحظورة ،ومنها استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو اعلام أو انشاء موقع إلكتروني لتسهيل القيام بأعمال إرهابية أو لدعم جماعة إرهابية أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر اعمال عدائية أو انتقامية)، وقد فرض المشرع الأردني عقوبة الأشغال المؤقتة لمدة خمس سنوات على الأقل على مرتكب الفعل، أما إذا نتج عن الفعل إلحاق الضرر ولو جزئيا في بناية عامة أو خاصة أو مؤسسة صناعية أو سفينة أو طائرة أو أي وسيلة نقل أو أي منشآت اخرى، أو تعطيل الاتصالات أو أنظمة الحاسوب أو اختراق شبكاتها أو التشويش عليها أو تعطيل وسائل النقل أو إلحاق الضرر بها كلياً أو جزئياً، فيعاقب بالأشغال المؤبدة بموجب المادة (٢/٧) من قانون منع الإرهاب سالف الذكر والمادة (٢/١٤٨+٣) من قانون العقوبات الأردني رقم (١٦) لسنة ١٩٦٠.

وكذلك جاء بالمادة (١٥) من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥ بأن كل من ارتكب أي جريمة يعاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات يعاقب بالعقوبة المنصوص عليها في ذلك التشريع.

وأخيراً فقد سن المشرع الأردني قانون الأمن السيبراني رقم (١٦) لسنة ٢٠١٩ الذي نصت المادة (٥/أ) منه على إنشاء مركز وطني للأمن السيبراني، من أجل بناءً منظومة فعالة للأمن السيبراني على المستوى الوطني لحماية المملكة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني، وسلامة الاشخاص والممتلكات والمعلومات.

وأما القضاء الأردني فقد أسهم في مكافحة الإرهاب السيبراني من خلال اصداره للعديد من الأحكام في هذا المجال. فعلى سبيل المثال أصدرت محكمة التمييز بصفتها الجزائية الحكم رقم (٣٥٢٨) لسنة ٢٠١٨، المتضمن تأييدها لقرار الحكم الصادر عن محكمة أمن الدولة في القضية رقم (٢٠١٨/٦٦٠٩) تاريخ ٢٠١٨/١٠/٣ القاضي بالحكم على الجاني بالأشغال المؤقتة لمدة لا تقل عن عشر سنوات استناداً لأحكام المادة(٣/هـ) من قانون منع الإرهاب سالف الذكر بسبب قيامه باستخدام التكنولوجيا الحديثة وإنشاء مواقع إلكترونية بهدف الترويج لأفكاره وإنشاء جماعات تهدف إلى القيام بأعمال من شأنها تعريض أمن وسلامة المواطنين للخطر عن طريق استخدام الشبكات الإلكترونية والمعلوماتية لتنفيذ جرائمهم[٤٦].

وكذلك أيدت محكمة التمييز بصفتها الجزائية بموجب الحكم الصادر عنها رقم (١٢٣)لسنة ٢٠١٦ القرار الصادر عن محكمة أمن الدولة في القضية الجزائية رقم (٤٥٤٩) لسنة ٢٠١٥ تاريخ ٢٠١٥/١٢/١٤ والقاضي بمعاقبة المتهم الأول في القضية بالأشغال المؤقتة لمدة ثلاث سنوات والرسوم، وخمس سنوات والرسوم للمتهمين الثاني والثالث استنادا لأحكام المادتين(٣/هـ) و (٧/ج) من قانون منع الإرهاب رقم (٥٥) لسنة ٢٠٠٦ بسبب تأييدهم لتنظيم الدولة الاسلامية(داعش) ومتابعة أخباره والترويج لأفكاره بين بعض الاشخاص في مدينة السلط[٤٧].

وكذلك أيدت محكمة التمييز بصفتها الجزائية بموجب الحكم الصادر عنها رقم(٢٠١٥/٥٣٣)الحكم الصادر عن محكمة أمن الدولة في القضية رقم (٢٠١٤/٨٠٧٨) تاريخ ٢٠١٥/٢/٢ المتضمن معاقبة الجاني بالأشغال المؤقتة لمدة سنتين بعد التخفيف بسبب قيامه باستخدام وسائل التفاعل الاجتماعي من أجل الترويج لأفكار تنظيم ارهابي ونشر صور ومقاطع فيديو متعلقة بهذا التنظيم خلافا لأحكام المادة (٣/هـ) من قانون منع الإرهاب رقم (٥٥)لسنة ٢٠٠٦[٤٨].

وكذلك فإن المملكة الأردنية الهاشمية شاركت في وضع العديد من الاتفاقيات والمعاهدات التي تكافح الإرهاب السيبراني، ومثال ذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أبرمت عام ٢٠١٨، ومن قبلها الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب بكافة أنواعه لسنة ٢٠١٠، وذلك من أجل حماية المواطن الأردني والعربي من جرائم الإرهاب السيبراني.

وفي هذا المقام لابد من الإشارة إلى أن الحكومة الأردنية قد قامت بتطوير قدرات أجهزة الأمن في مجال جرائم الإرهاب السيبراني، ووفرت لهم المعدات والأجهزة اللازمة لمكافحة هذه الجرائم،وأنشأت قسماً خاصاً في جهاز الأمن العام الأردني عام ٢٠٠٨ تحت مسمى قسم الاسناد الفني، وفي عام ٢٠١٣ وبعد تطور العمل داخل هذا القسم تم تغيير تسميته لتصبح قسم الجرائم الإلكترونية، وفي عام ٢٠١٥ وتزامناً مع صدور قانون الجرائم الإلكترونية تم تغيير التسمية لتصبح وحدة مكافحة الجرائم الإلكترونية وتتبع إدارة البحث الجنائي وتضم هذه الوحدة ثلاثة فروع هي:

١-فرع التحقيق ٢-فرع المعلومات ٣-فرع المختبر الرقمي

واجبات وحدة مكافحة الجرائم الإلكترونية:

تقوم هذه الوحدة بالعديد من الواجبات،ولن يتسع المقام لذكرها كلها،لذا سنكتفي بذكر بعضها:

١. وضع الخطط الاستراتيجية والبرامج اللازمة لمكافحة الجرائم الإلكترونية.
٢. عقد الدورات التدريبية والتأهيلية لتطوير قدرات العاملين في مكافحة الجرائم الإلكترونية.

[٤٦] منشورات قسطاس www.gistas.com

[٤٧] منشورات قسطاس www.gistas.com

[٤٨] منشورات قسطاس www.gistas.com

٣. نشر الوعي والثقافة الإلكترونية في المجتمع.
٤. فتح وتعزيز قنوات اتصال وتعاون على المستوى المحلي والأقليمي والدولي.
٥. تنفيذ الاتفاقيات الدولية والأقليمية والثنائية فيما يتعلق بالجرائم الإلكترونية.
٦. تنفيذ القوانين السارية والتي تشكل إطار عام في مجال مكافحة الجريمة.
٧. استرجاع الأدلة الرقمية وتوثيقها وتحليلها وتقديمها للجهات ذات الاختصاص وتزويد الجهات القضائية بتقارير الخبرة الفنية.
٨. التحقيق في الجرائم الإلكترونية والجرائم المرتبطة بالحاسوب وجرائم تطبيقات الاتصالات.
٩. وتقوم الوحدة أيضاً من خلال الدوريات الإلكترونية بملاحقة كافة الجرائم الإلكترونية كالدخول غير المشروع على المواقع الإلكترونية والتلاعب بالمحتوى الإلكتروني وانتحال صفة موقع إلكتروني أو شخصية مالكة، واستخدام البرمجيات الخبيثة، والاعتراض والتنصت على شبكة الإنترنت أو نظام المعلومات والحصول على بيانات أو معلومات بطاقات الائتمان والمعلومات المصرفية عبر الإنترنت، والترويج للدعارة،وتسهيل القيام بأعمال إرهابية أو دعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية، أو بث النعرات الطائفية والدينية المختلفة.

انجازات وحدة مكافحة الجرائم الإلكترونية:

لقد تعاملت هذه الوحدة مع الآلاف من قضايا الجرائم الإلكترونية في الاعوام ٢٠١٨،٢٠١٧،٢٠١٦،٢٠١٥، وقد أودعت إلى القضاء عدداً كبيراً منها، وقد تنوعت هذه القضايا بين انتحال الشخصية، والابتزاز الإلكتروني، وسرقة بريد إلكتروني، واختراق مواقع إلكترونية، والتهديد، والتشهير، وتعطيل أنظمة المعلومات، وذلك حسب الجدول التالي:

القضايا التي تعاملت معها الوحدة

السنة	عدد القضايا
٢٠١٥م	٤٧٠٠
٢٠١٦م	٥٧٠٠
٢٠١٧م	٦٢٤٠
٢٠١٨م	٧٦٥٢

وقد عزا بعض المحللون سبب زيادة هذه الجرائم إلى زيادة استخدام الهواتف الذكية في الاردن،حيث بلغ عدد هذه الهواتف أكثر من عشرة ملايين هاتف[٤٩].

وفي الختام أود الإشارة إلى أن الجهود التشريعية والقضائية لا تكفي لوحدها لمكافحة جرائم الإرهاب السيبراني،لذا فلابد من أن يضاف اليها جهود تقوم بها الأجهزة الأمنية والإعلامية والأفراد من أجل رصد ومتابعة أنشطة الإرهابيين وتزويد الجهات المختصة بالمعلومات اللازمة عن هذه الانشطة.

ومن أجل الحد من آثار جريمة الإرهاب السيبراني فلابد من أخذ الأمور التالية في الاعتبار:

١. إبراز وسائل الإعلام والنشر للآثار السلبية التي تلحق بالأفراد من جرائم الإرهاب السيبراني[٥٠].
٢. بث الوعي بين الأفراد من أجل التصدي لجرائم الإرهاب السيبراني[٥١].
٣. القيام بالإجراءات اللازمة من أجل منع وقوع الجرائم الإرهابية[٥٢].
٤. التسريع في اجراءات ضبط الجناة،ومعاقبتهم بالعقوبات الرادعة،من أجل اعادة الثقة إلى نفوس المواطنين[٥٣].
٥. ضرورة حجب المواقع الإلكترونية التي تشكل خطراً على فكر الأفراد،وخاصة فئة الشباب[٥٤].

وفي هذا المقام، أود الإشارة إلى أنه تم انشاء مختبر للتحقيقات الرقمية في جامعة الاميرة سمية من أجل نشر الوعي بالجرائم الإلكترونية عام ٢٠١٩، وكذلك فقد تم فتح برنامج ماجستير في الجرائم الإلكترونية والأمن السيبراني. وهذا ما فعلته أيضا من قبل كلية الملك عبد الله الثاني لتكنولوجيا المعلومات في الجامعة الأردنية التي انشأت مختبر لتكنولوجيا المعلومات مجهز بأحدث الأجهزة والبرمجيات المتعلقة بالتحقيقات الجنائية الرقمية.

جهود دولة الكويت:

بعد ثورة الاتصالات وظهور الجريمة الإلكترونية قامت دولة الكويت بإصدار العديد من القوانين من أجل مكافحتها، ومثال ذلك:

---

[٤٩] موقع وحدة الجرائم الإلكترونية psd.gov.jo

[٥٠] غادة نصار،٢٠١٧،الإرهاب والجريمة الإلكترونية،العربي للنشر والتوزيع-القاهرة،ط١،ص١٣٢.

[٥١] عبد الرزاق سندالي،٢٠١٩،التشريع المغربي في مجال الجرائم الإلكترونية،بحث قدم في الندوة الأقليمية حول الجرائم المتصلة بالكمبيوتر،الرباط-المغرب،ص٧١.

[٥٢] حنين بوادي،المرجع السابق،ص٥٤.

[٥٣] بدر هويمل الزبن،المرجع السابق،ص١٨٦؛علي بن عبد الله العسيري ٢٠٠٦،الإرهاب والقرصنة البحرية،جامعة الامير نايف للعلوم الأمنية-الرياض،ط١،ص٢٣٦.

[٥٤] غادة نصار،المرجع السابق،ص١٣٣.

١. قانون اساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت،رقم (٩) لسنة ٢٠٠١،والذي عدل بموجب القانون المعدل رقم (٤٠) لسنة ٢٠٠٧، الذي جرم التصوير بتلك الأجهزة دون علم الشخص أو رضاه، أو اختراق تلك الأجهزة والحصول على ما تحتويه من مقاطع مصورة.
٢. قانون المعاملات الإلكترونية رقم (٢٠) لسنة ٢٠١٤ الذي جرم العديد من الأفعال الإلكترونية غير المشروعة، كالدخول غير المشروع إلى النظام الإلكتروني أو تعطيله أو إتلافه أو الحصول على البيانات بدون إذن.
٣. قانون إنشاء هيئة تنظيم الاتصالات وتقنية المعلومات رقم (٣٧) لسنة ٢٠١٤ الذي جرم بعض الأفعال التي تستخدم فيها وسائل الاتصال الحديثة كالحض على الفجور والتحريض والتشهير بالغير والابتزاز...الخ.
٤. قانون الجرائم الإلكترونية رقم (٦٣) لسنة ٢٠١٥ والذي جرم كافة الأعمال غير المشروعة التي ترتكب بواسطة وسائل تقنية المعلومات والتي تمس بحقوق الأفراد والتي تشكل اعتداء على النظام المعلوماتي ذاته، كالدخول إليه بدون إذن،أو تزوير أو اتلاف البيانات، وقد فرض المشرع الكويتي على بعض هذه الجرائم عقوبة الحبس لمدة لا تزيد عن عشر سنوات، والغرامة التي لا تقل عن عشرين ألف دينار ولا تزيد عن خمسين ألف دينار أو بأحدى هاتين العقوبتين، كل من قام باستخدام الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات بغسل الأموال أو بتحويل أموال غير مشروعة أو بنقلها أو بإخفاء مصدرها غير المشروع...الخ المادة (٩) من القانون المذكور اعلاه.

وكذلك فعل المشرع الكويتي في المادة (١٠) من نفس القانون حيث فرض نفس العقوبة التي نصت عليها المادة (٩) على كل من انشأ موقعا لمنظمة إرهابية أو لشخص ارهابي أو نشر عن أيهما معلومات على الشبكة المعلوماتية أو بأحد وسائل تقنية المعلومات ولو تحت مسميات كاذبة، لتسهيل الاتصالات بأحدى قياداتها أو أعضائها أو ترويج أفكارها أو تمويلها...الخ.

ويضاف إلى ما ذكر مساهمة دولة الكويت بإبرام العديد من الاتفاقيات الثنائية والأقليمية، كالتوقيع على مذكرة التفاهم بشأن التعاون الأقليمي في مجال الحكومة الإلكترونية مع جمهورية سنغافورة عام ٢٠١٧، والتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صدر بشأنها القانون رقم (٦٠) لسنة ٢٠١٣.

ولم تتوقف جهود الدولة الكويتية عند هذا الحد، بل استضافت مؤتمر الأمن السيبراني الخليجي الثاني الذي خصص لجهود مواجهة الجرائم الإلكترونية والذي استمر لمدة يومين ١٣-٢٠١٩/١١/١٤ والذي شاركت فيه كلا من دولة الكويت ودولة قطر ودولة عمان، حيث دعا خبراء أمن المعلومات في هذه الدول إلى ضرورة توحيد الجهود الخليجية لمواجهة تحديات الأمن السيبراني وتوفير الحماية اللازمة للبيانات والمعلومات الحساسة الخاصة بدول مجلس التعاون الخليجي، من خلال وضع استراتيجيات وطنية لمواجهة تلك التحديات نظراً للمعطيات التقنية سريعة التطور وتزايد الهجمات الإلكترونية نظراً لكثافة الربط الشبكي الإلكتروني،وما يصاحبها من تعدي على حقوق الأفراد وأموالهم، وأن الجرائم الإلكترونية لم تعد تقتصر على الأفراد والمؤسسات بل وصلت لتهديد أمن الدول وسلامة مرافقها واقتصادها، الأمر الذي يتطلب تسخير كافة القدرات التكنولوجية، وتأهيل الموارد البشرية وتحسين القدرة على التعامل مع قضايا الأمن السيبراني للحد من المخاطر الإلكترونية المهددة لاقتصاد الدول وأمنها الوطني.

ومما يذكر في هذا المقام أن رئيسة الجمعية الكويتية لأمن المعلومات السيدة صفاء زمان قد اكدت انتشار عمليات الاختراق بصورة كبيرة خليجيا، مما نتج عنه زيادة معدلات الجرائم الإلكترونية، كما ذكرت أيضاً في تصريح للجزيرة نت ان عدد الجرائم الإلكترونية في تزايد مستمر حيث بلغ عدد هذا الجرائم في عام ٢٠١٣(٩٩٧) جريمة تقريباً حسب احصائيات إدارة الجرائم الإلكترونية، ووصلت عام ٢٠١٨ إلى (٤٥٠٢) جريمة، ويتراوح عددها عام ٢٠١٩ بين خمسة وستة آلاف جريمة تم الإبلاغ عنها ناهيك عن اختراق الحسابات التي لم يقم اصحابها بالإبلاغ عنها.

من جهتها قالت مديرة إدارة نظم المعلومات للموارد البشرية في وزارة الخدمة المدنية في سلطنة عمان فاطمة البلوشي، أن المركز الوطني لسلامة المعلومات في السلطنة تعامل مع (١٨٣٩) حادثاً أمنياً خلال عام ٢٠١٧ وارتفع العدد إلى (٢٣٣٤) خلال ٢٠١٨.

ويضاف إلى الجهود الكويتية أيضاً قيام وزارة العدل الكويتية بإجراء دراسة ميدانية حول الجرائم الإلكترونية في المجتمع الكويتي عامي ٢٠١٧-٢٠١٨، وقد خلصت الدراسة إلى مجموعة من التوصيات المستمدة من نتائجها، ومن أهمها ما يلي:

١. دراسة إمكانية الانضمام لاتفاقية مجلس أوروبا لمكافحة الجرائم الإلكترونية التي أبرمت عام ٢٠٠١ في بودابست، باعتبارها فرصة خارجية متاحة أمام دولة الكويت لتطوير الإطار التشريعي لمكافحة الجرائم الإلكترونية وتبادل الخبرات مع الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية.
٢. تفعيل الشراكة والتنسيق بين المؤسسات الوطنية المعنية بالوقاية والحماية من الجرائم الإلكترونية عن طريق انشاء مجلس، على أن يكون ذلك بسن تشريع ينص صراحة على أهميته وأطرافه ومجالات عمله.
٣. إعداد خطة وطنية للمؤسسات المعنية بمكافحة الجرائم الإلكترونية والتركيز على بناءً قدرات تلك المؤسسات وموظفيها وتطوير عملها وتحسين خدماتها.
٤. توعية الأحداث باستخدام الأجهزة الإلكترونية وبطرق التعامل المثلى مع وسائل التواصل الاجتماعي والألعاب الإلكترونية، وتوعية الأحداث أيضاً بالتبعات القانونية التي تترتب على ارتكابهم للجرائم الإلكترونية، وكذلك توعية الأسر بدورها الاجتماعي في عصر تكنولوجيا المعلومات.
٥. مراجعة التشريعات الناظمة للجريمة الإلكترونية وتطويرها شريطة موائمتها مع غيرها من التشريعات العالمية المتقدمة.

٦. مراجعة المناهج المدرسية وتطويرها من خلال تضمينها معلومات تتعلق بأهمية الوعي بالجرائم الإلكترونية، وبث رسائل توعية عن موقف الشريعة الاسلامية من الجرائم الإلكترونية عبر وسائل الاتصال المتاحة، هذا بالإضافة إلى تفعيل دور وزارة الأوقاف والعاملين فيها من أجل التصدي للجريمة الإلكترونية.

ثانياً: جهود المكافحة على المستوى الدولي:

ظهر الإنترنت كشبكة اعلام اجتماعي منذ العام ١٩٦٠ في الولايات المتحدة على يد شركات تجارية خاصة بتكليف من الحكومة، وقد بدأ تسويقه عام ١٩٩٠، ومنذ العام ٢٠٠٩ أصبح أكثر من ربع سكان العالم موصولاً على الشبكة العنكبوتية، وقد نشأ عن استخدام الإنترنت الكثير من الجرائم، لذا باتت الحاجة ملحة لنشوء تعاون دولي من أجل مكافحة الإرهاب السيبراني.

ومن أبرز هذه الجهود:

١. قرارات الجمعية العامة للأمم المتحدة

أصدرت الجمعية العامة للأمم المتحدة منذ عام ١٩٩٠ العديد من القرارات من أجل مكافحة الإرهاب السيبراني، ونشرت أيضاً دليلاً لمنع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في عام ١٩٩٤[٥٥].

ومن أهم القرارات التي أصدرتها الجمعية العامة في هذا الشأن القرار رقم (٥٦/١٢١) بتاريخ ٢٠٠١/١٢/١٩ الخاص بمكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات والذي يدعو الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات إلى أن تأخذ في الاعتبار عمل لجنة منع الجريمة والعدالة الاجتماعية، والقرار رقم (٥٨/١٩٩) بتاريخ ٢٠٠٤/١/٣٠ المتعلق بإنشاء ثقافة عالمية للأمن السيبراني ويدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني[٥٦]، وغيرها من القرارات التي توالت والتي لن يتسع المجال إلى ذكرها.

٢. الاتحاد الدولي للاتصالات

يعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات. وقد وضع الاتحاد الدولي للاتصالات مخططًا لتعزيز الأمن السيبراني العالمي يتضمن تحقيق سبعة أهداف هي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.
- وضع استراتيجيات لتهيئة الأرضية الوطنية والأقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلّقة بجرائم الإنترنت.
- وضع استراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.
- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.
- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.
- تطوير استراتيجية عالمية لتسهيل بناءً القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.
- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها[٥٧].

٣. اتفاقية المجلس الأوروبي بشأن جرائم الإنترنت

اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام ١٩٧٦. وفي العام ١٩٩٦، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية. عملت اللجنة بين العامين ١٩٩٧ و٢٠٠٠ على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر نيسان/أبريل ٢٠٠١. وتم التصديق على الاتفاقية من قبل ٣٠ دولة بحلول العام ٢٠١٠.

إن اتفاقية جرائم الإنترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى[٥٨].

وقد حضت الاتفاقية على تحقيق الأهداف التالية:

---

[٥٥] أحمد أمين أحمد الشوابكة،٢٠٠٤،جرائم الحاسوب والإنترنت-الجريمة المعلوماتية ،دار الثقافة،عمان-الاردن،ص٧٤.

[٥٦] جورج لبكي،٢٠١٣،المعاهدات الدولية للانترنت-حقائق وتحديات،مجلة الدفاع الوطني اللبناني،العدد ٨٣،كانون الثاني/٢٠١٣-لبنان،ص٤.

[٥٧] جورج لبكي،المرجع السابق،ص٤.

[٥٨] جورج لبكي،المرجع السابق،ص٤.

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونياً بواسطة الكمبيوتر.
- تعيين نظام سريع وفعال للتعاون الدولي.
- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.
- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

وتتضمن الاتفاقية أيضاً المبادئ العامة المتعلقة بالتعاون الدولي في المواضيع التالية:

- تسليم المجرمين.
- المساعدة الدولية المتبادلة.
- إعطاء المعلومات بصورة آلية.
- إنشاء الولاية القضائية على أي جريمة.
- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.
- الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقات الدولية.

ولن يتسع المقام لعرض كل الجهود الدولية التي بذلت في هذا المجال،لذا سنكتفي بهذا القدر.

وبالرغم من كل الجهود التي بذلت سواءً على المستوى الوطني أو الدولي إلا أن الإرهاب السيبراني مازال يتنامى بازدياد، وذلك بسبب العقبات التي تحد من جهود المكافحة، وهذا ما سنتعرض إليه في الفرع التالي.

الفرع الثاني: العقبات التي تحد من جهود المكافحة

إن العقبات التي تحد من مكافحة جريمة الإرهاب السيبراني متعددة، ومتنوعة، ولن يتسع المقام للتعرف عليها بشكل كامل، لذا سنكتفي بالوقوف على أهمها:

١. زيادة معدل النمو السكاني وسرعة انتشار الإنترنت:

إن زيادة معدل النمو السكاني وخاصة في الدول النامية، وسرعة انتشار الإنترنت، وزيادة عدد المستخدمين، وزيادة عدد الأجهزة التي توفر خدمة الوصول إلى الإنترنت أدت إلى زيادة عدد ضحايا الإرهاب السيبراني، وزيادة معدل نمو الجريمة، وخاصة الجرائم الاقتصادية[٥٩].

٢. عدم استجابة التشريعات الدولية للمتطلبات الجديدة للتعاون الدولي اللازم لمكافحة الإرهاب السيبراني:

رغم وجود بعض الاتفاقيات الأقليمية في مجال مكافحة الجريمة السيبرانية كاتفاقية مجلس أوروبا التي أبرمت عام٢٠٠١ في بودابست، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي أبرمت عام ٢٠١٨ وغيرها من الاتفاقيات الأقليمية، إلا أنها تشريعات مجزأة بسبب الاختلافات في نطاق الدول الأعضاء المنضمين إليها وفي محتوى تلك الاتفاقيات[٦٠]، لذلك فإن المجتمع الدولي بحاجة ماسة إلى وضع إطار قانوني عالمي لمكافحة الجريمة السيبرانية التي تتزايد خطورتها مع مرور الوقت، ولاسيما لمواجهة التحديات الجديدة الناشئة عن التكنولوجيا الجديدة كالحوسبة السحابية، والذكاء الاصطناعي، وانترنت الأشياء، والعملات الرقمية المشفرة، وأن يقرر هذا الاطار (الاتفاقية العالمية) تحت رعاية الامم المتحدة[٦١].

٣. التمسك بحق الخصوصية والسيادة الوطنية:

قد يكون التمسك باحترام خصوصية الانسان وسيادة الدولة أحيانا عقبة أمام الحصول على المعلومات والبيانات اللازمة من أجل مكافحة الإرهاب السيبراني، لذلك يجب على الدول أن تسعى جاهدة إلى تحقيق التوازن بين احترام السيادة الوطنية وحماية حقوق الأفراد والشركات وبين تيسير التحقيقات وتحسين كفاءة الحصول على الأدلة من خلال تحسين إجراءات المساعدة القضائية والتعاون في مجال إنفاذ القانون[٦٢].

---

[٥٩] تقرير الامين العام للامم المتحدة لعام ٢٠١٩ الذي قدم للجمعية العامة في دورتها رقم ٧٤،البند ٣٤٠.

[٦٠] عبدالفتاح بيومي حجازي،المرجع السابق،ص١٥٤.

[٦١] تقرير الامين العام للامم المتحدة لعام ٢٠١٩،المرجع السابق،البند ٦٩.

[٦٢] هانيا فقيه،٢٠١٨،حمأية الحق في الخصوصية المعلوماتية،منشور في القاعدة البيبليوغرافيا، مركز المعلوماتية القانونية،الجامعة اللبنانية،بيروت،ص٣ ؛نادر عبد العزيز شافي،٢٠٠٧،بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني،مجلة الجيش اللبناني،عدد ٢٦٣،بيروت؛شيماء عطاالله،٢٠١٥،تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية،المؤتمر العلمي الثاني لكلية القانون الكويتية العالمية،مجلة كلية القانون الكويتية العالمية،العدد ١٠،السنة الثالثة،ص٥٠١.

إن تنفيذ طلبات التعاون الدولي التي ترسل في اطار معاهدات المساعدة القانونية المتبادلة بطيئة للغاية، وتكون أحياناً غير قابلة للتطبيق بسبب سرعة التخلص من البيانات الرقمية نظراً للكم الهائل من المعلومات المتداولة على مستوى العالم، والتكاليف المرتبطة بتخزينها، مما يدفع الشركات إلى عدم الاحتفاظ بالبيانات إلا لمدة لا تزيد عما هو ضروري لأعمالها[٦٣].

٤. إن السلوك الاجرامي المرتبط بتكنولوجيا المعلومات والاتصالات مستمر التغيير والتكيف، وعابر للحدود، ويقسم إلى افعال صغيرة، يقوم بها في كثير من الاحيان مجرمون مختلفون يؤدي كل منهم دورا وأحدا في إطار المنظمة الإجرامية، مما يؤدي إلى زيادة تعقيد الجريمة وتطورها، ويوفر حماية أوسع للمجرمين، لأن بعض مكونات الجريمة قد لا تشكل جرائم جنائية في بعض الولايات القضائية خاصة إذا كانت الجريمة موزعة على ولايات قضائية متعددة.

٥. ولا يقتصر اثر الاستفادة من الشبكات الموزعة التي تستخدم التكنولوجيا السيبرانية على اسغلال مواطن الضعف في نظم العدالة الوطنية،بل هو يحول أيضاً الولاية الأقليمية للدول وسيادتها إلى اداة تستخدم ضدها[٦٤].

٦. صعوبة الحصول على المعلومات المطلوبة من الدول الاخرى، لأن هذا الأمر يتطلب معرفة مكان وجودها، وهل هي متاحة للاطلاع عليها أم لا، وهل هي في شكل مفهوم أم لا، فهذا كله يعتمد إلى حد كبير على نوع المعلومات أو البيانات الحاسوبية التي قد يخزن بعضها على مدى طويل، بينما يحذف البعض الاخر كبيانات حركة المرور بوتيرة أسرع، هذا بالإضافة إلى أن عمل شركات الاتصال يمتد إلى أكثر من دولة ويخضع لقوانين وطنية أو اقيليمية، الأمر الذي يجعل الية الوصول إلى البيانات أو حفظها تختلف من دولة إلى أخرى[٦٥].

٧. عدم وجود قوانين موضوعية وطنية في العديد من الدول، لتجريم الأفعال الجرمية ذات الصلة باستخدام تكنولوجيا المعلومات والاتصالات، والتي تشكل أساسا للتعاون الدولي من خلال الاعتراف المتبادل بهذه الجرائم[٦٦] .

٨. عدم كفاية الامكانات أو القدرات التقنية اللازمة لإجراء التحقيقات الرقمية، وعدم توافر الكوادر ذات المهارات المهنية اللازمة في تكنولوجيا المعلومات والاتصالات وعدم القدرة على تدريب هذه الكوادر في العديد من دول العالم الفقيرة، نظراً لضعف الامكانات المادية لديها، وتقاعس الدول المتقدمة الغنية عن مساعدتها من أجل تطوير قدراتها التقنية والبشرية وخاصة العاملين في مجال انفاذ القوانين الوطنية[٦٧] .

٩. ضعف سيادة القانون في بعض الدول وخاصة الدول التي تقوم بإيواء مرتكبي الجرائم السيبرانية مما يشكل عقبة عابرة للحدود أمام الجهود التي تبذل لمكافحة هذه الجريمة[٦٨].

١٠. عدم قيام الكثير من الأفراد والمؤسسات المجني عليها بالتبليغ عن جرائم المعلوماتية ومثال ذلك البنوك بحجة أن الابلاغ عن هذه الجرائم يؤدي إلى تراجع ثقة العملاء فيها[٦٩].

١١. عدم توافر الإرادة السياسية لدى بعض الدول لمكافحة هذه الجريمة من أجل تحقيق بعض المصالح وخاصة الاقتصادية.

١٢. نقص التعاون بين أجهزة المراقبة والملاحقة في كثير من الدول[٧٠] وصعوبة تحديد الجهة المختصة بالملاحقة والتحقيق والمحاكمة نظرا لارتكاب الجريمة السيبرانية من خارج حدود الدولة،خاصة وأن بعض الدول تعتقد أن إجراءات الملاحقة والتحقيق والمحاكمة قد تمس بسيادتها الوطنية أو حقوق أفرادها[٧١].

١٣. وأما في الاردن على وجه التحديد فإن العقبات الرئيسية التي تحد من مكافحة استخدام تكنولوجيا المعلومات للأغراض غير المشروعة وحسب الورقة التي قدمتها الجهة الأردنية المختصة إلى الجمعية العامة للأمم المتحدة في دورتها رقم (٧٤)عام٢٠١٩ التي تضمنها تقرير الامين العام للأمم المتحدة في البند رقم(١٧٦)فهي:

- وجود برمجيات وبرامج مجانية تخفي هويات المستخدمين وتجعل من الصعب تعقبهم وكشفهم.

---

[٦٣] موزة المزروعي،المرجع السابق،ص٧٨؛اسامة احمد مناعسة وآخرون ،٢٠٠١،جرائم الحاسب الآلي والإنترنت،ط١،دار وائل،عمان-الأردن،ص٢٨٩.

[٦٤] تقرير الامين العام للامم المتحدة،المرجع السابق،البند ٦٣.

[٦٥] تقرير الامين العام للامم المتحدة،المرجع السابق،البند ٦٥.

[66] Raed S A Faqir, Saleh Sharari, Salameh A, previous reference, p7.

[٦٧] Schwartz. D: deficiencies in regulations for anti-money laundering in a cyberlaundering age including COMET: central online AMA merchant enforcement tool, M. alowa state university, 2009, p47-65؛وجمال علي دهشان، ٢٠١٨،الإرهاب في العصر الرقمي،المجلة الدولية للبحوث في العلوم التربوية،المجلد الأول،العدد الثالث؛و د.محمد علي قطب،٢٠١٠،الجرائم المعلوماتية وطرق مواجهتها،الاكاديمية الملكية للشرطة-وزارة الداخلية-البحرين ،ص٢-٩.

[٦٨] تقرير الامين العام للامم المتحدة،المرجع السابق،البند ٣٩٤/و.

[٦٩] هلالي عبد الاه احمد،١٩٩٩،حجية المخرجات الكمبيوترية في المواد الجنائية،دراسة مقارنة،جامعة أسيوط-مصر،ص٤٧.

[70] Elena Chernrnko, Oleg demidov, Fyodor lukyanov,"Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms", from International Institutions and Global Governance Program,2018

[71] Raed S A Faqir, Saleh Sharari, Salameh A, previous reference, p3.

- توافر المعلومات وسهولة الحصول عليها وإمكانية اكتساب المعرفة باستخدام الأدوات الإجرامية والخبرة في استخدامها من مواقع مجانية عديدة على مواقع الشبكة العالمية.
- الشبكة الخفية التي تشكل مرتعاً خصباً للأعمال غير المشروعة الأمر الذي يجعل عملية رصد هذه المواقع ومراقبتها صعبة، بسبب استخدام التشفير لمنع كشف هوية المستخدمين.
- بطئ الاجراءات وتبادل المعلومات في قضايا الجرائم السيبرانية التي تقع في عدة دول، علماً بأن الجريمة السيبرانية تتطلب سرعة الإجراءات والمعالجة قبل محو الادلة.
- عدم تجاوب بعض منصات التواصل الاجتماعية، وعدم تعاونها بخصوص تبادل المعلومات مع أجهزة انفاذ القانون.
- الحاجة الماسة إلى بناءً القدرات من خلال برامج تدريبية دولية وتبادل الخبرات مع الدول المتقدمة في مسائل الجريمة السيبرانية.

الخاتمة:

تناولت هذه الدراسة الإرهاب السيبراني من حيث تعريفه، وسماته، وأسبابه، ومخاطره في المبحث الأول، وتناولت أيضاً وسائل الإرهاب السيبراني والجهود التي بذلت لمكافحته والعقبات التي تحد من ذلك في المبحث الثاني.

النتائج:

خلصت الدراسة إلى مجموعة من النتائج أهمها ما يلي:

١. تعد جريمة الإرهاب السيبراني من الجرائم المستحدثة والتي نشأت بعد التطور المتسارع الذي طرأ على وسائل الاتصال وتكنولوجيا المعلومات.
٢. من أهم العوامل التي تدفع الجناة للقيام بجريمة الإرهاب السيبراني هو سهولة ارتكابها وصعوبة رقابة وملاحقة الجناة.
٣. جريمة الإرهاب السيبراني جريمة عابرة للحدود والقارات، مما يصعب معه تحديد الدولة المختصة بالملاحقة والتحقيق والمحاكمة.
٤. صعوبة اثبات هذه الجريمة نظراً لسهولة محو الادلة.
٥. قلة الأفراد والمؤسسات التي تقوم بالإبلاغ عن هذه الجريمة خوفاً من اهتزاز ثقة العملاء بها.
٦. ضعف التعاون الدولي في مجال مكافحة هذه الجريمة.
٧. نقص المعدات والخبرة لدى الأجهزة الأمنية المختصة بالمراقبة والملاحقة في دول كثيرة.

التوصيات:

وبناءً على النتائج التي خلصت اليها الدراسة فإننا نوصي بما يلي:

١. لقد باتت الحاجة ماسة إلى وضع اتفاقية دولية وقوانين موضوعية وإجرائية وطنية لمكافحة هذه الآفة ويمكن الاستفادة من الاتفاقيات الأقليمية التي وضعت في هذا المجال كاتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لعام ٢٠٠١، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٣، بشرط أن لا تتضمن هذه القوانين حظر الدخول إلى شبكة الإنترنت إلا بالقدر الذي يحمي خصوصية الأفراد والأمن القومي ومكافحة الإرهاب.
٢. على الدول أن تحرص على تحقيق التوازن بين احترام السيادة الوطنية وحماية حقوق الأفراد وبين تيسير التحقيقات وتحسين كفاءة الحصول على الأدلة من خلال تحسين إجراءات المساعدة القضائية والتعاون في مجال انفاذ القانون.
٣. على الدول أن تسرع اجراءات المساعدة القضائية وتبادل المعلومات في قضايا الإرهاب السيبراني التي تقع في عدة دول، لأن الجريمة السيبرانية تتطلب سرعة الاجراءات قبل محو الأدلة.
٤. على الدول القيام بالتحديث الفوري للقوانين الموجودة إن لم تضع قوانين جديدة تتعلق بمكافحة جرائم تقنية المعلومات والاتصالات لكي تتلائم مع التكنولوجيا الجديدة .
٥. على الدول اعتماد معيار موحد لمكافحة الإرهاب السيبراني لمنع المجرمين من استغلال الدول التي لديها قوانين أقل صرامة.
٦. توظيف محققين يمتلكون معرفة تقنية عالية وقادرين على مواكبة أحدث التقنيات في هذا المجال.
٧. نشر الثقافة الرقمية للتعريف بالإرهاب السيبراني وسبل الوقاية منه ومكافحته عن طريق أجهزة الدولة المعنية وتبني استراتيجيات توعوية على المستوى المحلي والأقليمي تهدف إلى حماية الأفراد والمجتمعات من مخاطر الإرهاب السيبراني ولا سيما فئة الشباب .
٨. مساعدة الدول المتقدمة الغنية للدول النامية الفقيرة بالموارد المالية والتقنيات اللازمة لمكافحة الإرهاب السيبراني هذا بالإضافة إلى تبادل الخبرات الدولية في مجال مكافحة الإرهاب السيبراني.

المراجع:

أولاً: المراجع العربية:

١. الاشعل، عبد الله. (٢٠٠٢). "الديمقراطية وحقوق الانسان في العلاقات الدولية". مجلة شؤون خليجية: (٢٩).

٢. ابراهيم، خالد ممدوح. (٢٠٠٩). الجرائم المعلوماتية. ط١. دار الفكر العربي الجامعي. الاسكندرية.

٣. ابورية، وليد محمد. (٢٠١٢). "التعرف على الإرهاب الإلكتروني،ندوة استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين التي عقدت في الرياض بتاريخ ٩-٢٠١١/٥/١١". منشورات جامعة نايف للعلوم الأمنية-الرياض.

٤. أحمد، هلالي عبد الاله. (١٩٩٩). "حجية المخرجات الكمبيوترية في المواد الجنائية،دراسة مقارنة". جامعة أسيوط- مصر.

٥. البحر، عبدالرحمن. (١٩٩٩). "معوقات التحقيق في جرائم الإنترنت". رسالة ماجستير. جامعة نايف العربية للعلوم الأمنية.

٦. البحيري، ولاء. (٢٠١٢). "مستقبل الإرهاب الإلكتروني وأساليب مواجهته". مجلة النهضة- كلية الاقتصاد والعلوم السياسية: جامعة القاهرة. ١٣(٤)

٧. البهي، رغده. (٢٠١٩). الإرهاب السيبراني:المفهوم والسمات والانماط. المركز المصري للفكر والدراسات الاستراتيجية.

٨. بوادي، حنين. (٢٠٠٤). تجربة مواجهة الإرهاب. ط١. دار الفكر الجامعي- الاسكندرية.

٩. الجنابي، ليلى. (٢٠١٧). فعالية القوانين الوطنية والدزلية في مكافحة الجرائم السيبرانية http://www.ahewar.org/debat/show.art.asp?aid=571423&r=0

١٠. حجازي، عبد الفتاح بيومي. (٢٠٠١). مكافحة جرائم الكمبيوتر والإنترنت. دار الفكر العربي- الاسكندرية.

١١. خليفة أيهاب. (٢٠١٧). القوة الإلكترونية. المركز العربي للنشر والتوزيع- ابو ظبي.

١٢. درويش، بندر عقاب. (٢٠١٧). "الاثبات في جرائم الإرهاب الإلكتروني". رسالة ماجستير قدمت لجامعة العلوم الاسلامية- عمان- الاردن.

١٣. دهشان، جمال علي. (٢٠١٨). "الإرهاب في العصر الرقمي". المجلة الدولية للبحوث في العلوم التربوية: ١ (٣).

١٤. الزبن، بدر هويمل. (٢٠١٢). "الإرهاب في الفضاء الإلكتروني". رسالة ماجستير- جامعة عمان العربية. الاردن.

١٥. الزبون، احمد علي احمد. (٢٠١٥). "الجرائم الواقعة على أمن الدولة الداخلي في الشريعة الاسلامية والقانون الأردني".

١٦. الزبيدي، وليد. (٢٠٠٣). القرصنة على الإنترنت والحاسوب. التشريعات القانونية. ط١. دار اسامة. عمان- الأردن.

١٧. سندالي، عبد الرزاق. (٢٠١٩). "التشريع المغربي في مجال الجرائم الإلكترونية". بحث قدم في الندوة الأقليمية حول الجرائم المتصلة بالكمبيوتر. الرباط- المغرب.

١٨. السند، عبد الرحمن بن عبد الله. (٢٠٠٤). "وسائل الإرهاب الإلكتروني وحكمها في الاسلام وطرق مكافحتها". المؤتمر العالمي- موقف الاسلام من الإرهاب. جامعة الأمام محمد بن سعود الاسلامية. السعودية.

١٩. سرور، احمد فتحي. (٢٠٠٩). المواجهة القانونية للإرهاب. دار النهضة العربية- القاهرة.

٢٠. شافي، نادر عبد العزيز. (٢٠٠٧). "بين احترام الحريات الشخصية ومراعاة مصلحة الدولة والأمن الوطني". مجلة الجيش اللبناني: (٢٦٣). بيروت.

٢١. الشنيفي، عبد الرحمن عبد العزيز. (١٩٩١). حرب المعلومات. مكتبة غريب- الرياض- المملكة العربية السعودية.

٢٢. الشوابكة، أحمد أمين أحمد. (٢٠٠٤). جرائم الحاسوب والإنترنت-الجريمة المعلوماتية. دار الثقافة. عمان-الاردن.

٢٣. الشهري، فايز عبد الله. (٢٠١٢). "ثقافة التطرف والإرهاب على شبكة الإنترنت". منشورات جامعة الامير نايف للعلوم الأمنية- الرياض.

٢٤. صالح، نايل عبد الرحمن. (٢٠٠٤). "واقع جرائم الحاسب الآلي في التشريع الأردني". مؤتمر القانون والكمبيوتر والإنترنت- جامعة الامارات العربية المتحدة. كلية الشريعة والقانون. المجلد الأول. ط٣. وقد عقد المؤتمر من ١-٣/مايو/٢٠٠٠.

٢٥. عبابنة، محمود احمد؛ و الرازقي، محمد معمر. (٢٠٠٩). جرائم الحاسوب وأبعادها الدولية. ط١. دار الثقافة- عمان.

٢٦. عبدالعال، محمد عبد اللطيف. (١٩٩٤). جريمة الإرهاب. دار النهضة العربية- القاهرة.

٢٧. عبدالفتاح، علي. (٢٠١٦). الإعلام الدبلوماسي والسياسي. البازوري للنشر-عمان- الاردن.

٢٨. عبدالمجيد، محمد سعيد. (٢٠٠٦). المعلوماتية والجريمة. مكتبة الاسراء للطبع والنشر والتوزيع- طنطا- مصر.

٢٩. العجلان، عبد الله عبد العزيز فهد. (٢٠٠٨). "الإرهاب الإلكتروني في عصر المعلومات". بحث قدم في المؤتمر الدولي لحمأية أمن المعلومات والخصوصية في قانون الإنترنت الذي عقد في القاهرة بتاريخ ٢-٢٠٠٨/٦/٤.

٣٠. عرب، خالد يونس. (١٩٩٤). "جرائم الحاسوب". رسالة ماجستير. الجامعة الأردنية.

٣١. العسيري، علي بن عبد الله. (٢٠٠٦). الإرهاب والقرصنة البحرية. جامعة الامير نايف للعلوم الأمنية- الرياض. ط١.

٣٢. عطا الله شيماء. (٢٠١٥). "تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية،المؤتمر العلمي الثاني لكلية القانون الكويتية العالمية". مجلة كلية القانون الكويتية العالمية: (١٠). السنة الثالثة.

٣٣. عوضين، محمد محيي الدين. (١٩٩٣). "مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات". دار النهضة العربية- القاهرة.

٣٤. فقيه، هانيا. (٢٠١٨). "حماية الحق في الخصوصية المعلوماتية،منشور في القاعدة البيبليوغرافيا". مركز المعلوماتية القانونية. الجامعة اللبنانية. بيروت.

٣٥. قطب، محمد علي. (٢٠١٠). "الجرائم المعلوماتية وطرق مواجهتها". الالكاديمية الملكية للشرطة- وزارة الداخلية- البحرين.

٣٦. القيسي، أيسر محمد عطية. (٢٠١٤). "دور الاليات الحديثة في الحد من الجرائم المستحدثة". بحث قدم لمؤتمر الجرائم المستخدمة في ظل التغيرات الأقليمية والدولية الذي عقد في عمان بتاريخ ٢-٢٠١٤/٩/٤.

٣٧. الكافي، مصطفى يوسف. (٢٠١١). الإدارة الإلكترونية إدارة بلا أوراق. مؤسسة رسلان للطباعة والنشر والتوزيع- دمشق- سوريا.

٣٨. الكردي زين العابدين عواد كاظم. (٢٠١٨). "جرائم الإرهاب". منشورات الحلبي الحقوقية- بيروت.

٣٩. الكيلاني، هيثم. (١٩٩٧). "الإرهاب يؤسس دولة". دار الشروق- بيروت. ط١.

٤٠. لبكي، جورج. (٢٠١٣). "المعاهدات الدولية للانترنت-حقائق وتحديات". مجلة الدفاع الوطني اللبناني: (٨٣)، كانون الثاني/٢٠١٣-لبنان.

٤١. المزروعي، موزة. (٢٠٠٠). "الاختراعات الإلكترونية خطر كيف نواجهه". مجلة افاق الاقتصادية: الامارات العربية المتحدة. (٩).

٤٢. الملط، احمد خليفة. (٢٠٠٥). الجرائم المعلوماتية. دار الفكر الجامعي. ط١. الاسكندرية.

٤٣. مناعسة، اسامة احمد وآخرون. (٢٠٠١). جرائم الحاسب الآلي والإنترنت. ط١. دار وائل. عمان-الأردن.

٤٤. نصار، غادة. (٢٠١٧). الإرهاب والجريمة الإلكترونية. العربي للنشر والتوزيع-القاهرة. ط١.

ثانياً: المراجع الأجنبية:

[1] Audrey (2009). protection children on the internet mission impossible, pace law, fculty publication.

[2] Chernrnko, Elena, Demidov, Oleg & Lukyanov, Fyodor. (2018)."Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms",from International Institutions and Global Governance Program. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

[3] Cralsson, Ulla. (2006). "violence and pornography on media", Nordicom, Goteborg, https://pdfs.semanticscholar.org/988a/5c28cbc3e6cd27c83792305fd48c4334a36a.pdf.

[4] Donnerstein, Edward. (1984)."pornography: its effects on violence against women" in Malamuth and Donnerstein, eds, pornography and sexual aggression, academic press.

[5] Faqir, Raed S A, Sharari, Saleh & Salameh A. (2014). "cyber crimes and technical issues under the Jordanian information system crimes law", Journal of politics and law, 7(2), https://doi.org/10.5539/jpl.v7n2p94.

[6] Freet, David & Agrawal, Rajeev (2017). Cyber Espionage, springer internationl publishing.

[7] Hameed, Shihab A. (2011). "Effects of internet drawbacks on moral and social values of users in education", Australian journal of basic and applied sciences.

[8] Kadir, Rizger M. (2009). "The offense of unauthorized access in computer crimes legislation a comparative study", journal of shria and law, (4).

[9] Schwartz. D. (2009). Deficiencies in regulations for anti-money laundering in a cyberlaundering age including COMET: central online AMA merchant enforcement tool, M.a lowa state university.

[10] Zillman, Dolf & Bryant, Jennings. (1982). "pornography, sexual callousness, and the trivialization of rape", journal of communications, 32(4): 10-21, https://doi.org/10.1111/j.1460-2466.1982.tb02514.x

ثالثاً: القوانين:

١. قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥.

٢. قانون منع الإرهاب الأردني رقم (٥٥) لسنة ٢٠٠٦.

٣. قانون العقوبات الأردني رقم (١٦) لسنة ١٩٦٠.

٤. قانون الأمن السيبراني الأردني رقم (١٦) لسنة ٢٠١٩.

٥. قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لسنة ٢٠١٥.

رابعاً: الاتفاقيات:

١. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٣.

٢. الاتفاقية العربية لمكافحة الإرهاب لعام ١٩٩٤.

٣. اتفاقية جنيف لقمع الإرهاب لعام ١٩٧٣.

٤. اتفاقية المجلس الأوروبي التي وضعت عام ٢٠٠١ وتم التصديق عليها عام ٢٠١٠ الخاصة بجرائم الإنترنت.

٥. تقرير الامين العام للامم المتحدة لعام ٢٠١٩ الذي قدم للجمعية العامة في دورتها رقم ٧٤.
٦. دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها الصادر عن الجمعية العامة للأمم المتحدة عام ١٩٩٤.
٧. مبادئ محكمة التمييز الأردنية بصفتها الجزائية (موقع قسطاس www.gistas.com).
٨. المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية،٢٠١١،دعاوى الجرائم الإلكترونية وادلة إثباتها في التشريعات العربية بين الواقع والمأمول،السودان.https://carjj.org/%D8%A5%D8%AC%D8%AA%D9%85%D8%A7%D8%B9/1457
٩. مجمع الفقه الاسلامي،١٤٣٣هـ،مجلة البحوث الاسلامية،العدد(٩٧)،الرياض.

www.refaad.com

المجلة الدولية للدراسات القانونية والفقهية المقارنة

International Journal of Legal and Comparative Jurisprudence Studies (LCJS)

Journal Homepage: https://www.refaad.com/views/LCJS/Home.aspx

ISSN: 2708-6607(Online) 2708-6593(Print)

Confronting cyber terrorism in the Jordanian criminal law and international treaties

Aqel Yousef Makableh

Professor of Criminal Law, Department of Public Law, College of Law, Yarmouk University, Jordan

makableh@yu.edu.jo

Received: 8/9/2020 Revised: 27/9/2020 Accepted: 25/10/2020 DOI: https://doi.org/10.31559/LCJS2020.1.3.1

Abstract: The crime of cyber terrorism has appeared following the rapid developments in digital technology and the Internet, which have enabled many individuals and groups to carry out terrorist acts and facilitated the operations, promotion, and financing of these groups to commit various forms of crimes, such as drug trafficking, spreading pornographic movies, and accessing Web Sites, without authorization from their owners, to access data or to destroy it.

The electronic terrorism crime has become a dangerous phenomenon that transcends frontiers and continents and threatens a large portion of world population because the perpetrators resort to different means and methods in committing that crime. This necessitates that all countries make more efforts to combat this crime and reduce its hazards. However, the efforts exerted at the national and international levels have not so far been sufficient due to a number of obstacles that limit the efficiency of these efforts, such as the lack of agreement among states on the acts that constitute a crime of international terrorism and the lack of expertise on the side of enforcement agencies that control and trace the perpetrators in some countries.

This study concludes with a number of recommendations, most importantly to enhance the international cooperation in the field of combating crime and the need for capacity building of human resources, with appropriate equipment, to be able to control and trace criminals.

Keywords: *Counter-Terrorism; Digital technology and information network; Internet and the law; Risks of information network; Transnational crime; websites.*

References:

[1] 'babnh, Mhmwd Ahmd: W Alrazqy, Mhmd M'emr. (2009). Jra'm Alhaswb Wab'adha Aldwlyh. T1. Dar Althqafh- 'man.

[2] 'bdal'al, Mhmd 'bd Alltyf. (1994). Jrymt Alerhab. Dar Alnhdh Al'rbyh- Alqahrh.

[3] 'bdalftah, 'ly. (2016). Ale'lam Aldblwmasy Walsyasy. Albazwry Llnshr-'man- Alardn.

[4] 'bdalmjyd, Mhmd S'yd. (2006). Alm'lwmatyh Waljrymh. Mktbt Alasra' Lltb' Walnshr Waltwzy'- Tnta- Msr.

[5] Al'jlan, 'bd Allh 'bd Al'zyz Fhd. (2008). "Alerhab Alelktrwny Fy 'sr Alm'lwmat". Bhth Qdm Fy Alm'tmr Aldwly Lhmayh Amn Alm'lwmat Walkhswsyh Fy Qanwn Alentrnt Aldy 'qd Fy Alqahrh Btarykh 2-4/6/2008.

[6] 'rb, Khald Ywns. (1994). "Jra'm Alhaswb". Rsalt Majstyr. Aljam'h Alardnyh.

[7] Al'syry, 'ly Bn 'bd Allh. (2006). Alerhab Walqrsnh Albhryh. Jam't Alamyr Nayf Ll'lwm Alamnyh- Alryad. T1.

[8] 'ta Allh Shyma'. (2015). "Traj' Alhq Fy Alkhswsyh Fy Mwajhh Alatsalat Alelktrwnyh,Alm'tmr Al'lmy Althany Lklyt Alqanwn Alkwytyh Al'almyh". Mjlt Klyt Alqanwn Alkwytyh Al'almyh: (10). Alsnh Althalthh.

[9] 'wdyn, Mhmd Mhyy Aldyn. (1993). "Mshklat Alsyash Aljna'yh Alm'asrh Fy Jra'm Nzm Alm'lwmat". Dar Alnhdh Al'rbyh- Alqahrh.

[10] Alash'l, 'bd Allh. (2002). "Aldymqratyh Whqwq Alansan Fy Al'laqat Aldwlyh". Mjlt Sh'wn Khlyjyh: (29).

[11] Abrahym, Khald Mmdwh. (2009). Aljra'm Alm'lwmatyh. T1. Dar Alfkr Al'rby Aljam'y. Alaskndryh.

[12] Abwryh, Wlyd Mhmd. (2012). "Alt'rf 'la Alerhab Alelktrwny,Ndwh Ast'mal Alentrnt Fy Tmwyl Alerhab Wtjnyd Alerhabyyn Alty 'qdt Fy Alryad Btarykh 9-11/5/2011". Mnshwrat Jam't Nayf Ll'lwm Alamnyh-Alryad.

[13] Ahmd, Hlaly 'bd Alalh. (1999). "Hjyt Almkhrjat Alkmbywtryh Fy Almwad Aljna'yh,Drash Mqarnh". Jam't Asywt- Msr.

[14] Albhr, 'bdalrhmn. (1999). "M'wqat Althqyq Fy Jra'm Alentrnt". Rsalt Majstyr. Jam't Nayf Al'rbyh Ll'lwm Alamnyh.

[15] Albhy, Rghdh. (2019). Alerhab Alsybrany:Almfhwm Walsmat Walanmat. Almrkz Almsry Llfkr Waldrasat Alastratyjyh.

[16] Albhyry, Wla'. (2012). "Mstqbl Alerhab Alelktrwny Wasalyb Mwajhth". Mjlt Alnhdh- Klyt Alaqtsad Wal'lwm Alsyasyh: Jam't Alqahrh. 13(4)

[17] Bwady, Hnyn. (2004). Tjrbt Mwajht Alerhab. T1. Dar Alfkr Aljam'y- Alaskndryh.

[18] Dhshan, Jmal 'ly. (2018). "Alerhab Fy Al'sr Alrqmy". Almjlh Aldwlyh Llbhwth Fy Al'lwm Altrbwyh: 1 (3).

[19] Drwysh, Bndr 'qab. (2017). "Alathbat Fy Jra'm Alerhab Alelktrwny". Rsalt Majstyr Qdmt Ljam't Al'lwm Alaslamyh- 'man-Alardn.

[20] Fqyh, Hanya. (2018). "Hmayt Alhq Fy Alkhswsyh Alm'lwmatyh,Mnshwr Fy Alqa'dh Albyblywghrafya". Mrkz Alm'lwmatyh Alqanwnyh. Aljam'h Allbnanyh. Byrwt.

[21] Hjazy, 'bd Alftah Bywmy. (2001). Mkafht Jra'm Alkmbywtr Walentrnt. Dar Alfkr Al'rby- Alaskndryh.

[22] Aljnaby, Lyla. (2017). F'alyt Alqwanyn Alwtnyh Waldzlyh Fy Mkafhh Aljra'em Alsybranyh http://www.ahewar.org/debat/show.art.asp?aid=571423&r=0

[23] Khlyfh Ayhab. (2017). Alqwh Alelktrwnyh. Almrkz Al'rby Llnshr Waltwzy'- Abw Zby.

[24] Alkafy, Mstfa Ywsf. (2011). Aledarh Alelktrwnyh Edart Bla Awraq. M'sst Rslan Lltba'h Walnshr Waltwzy'- Dmshq- Swrya.

[25] Alkrdy Zyn Al'abdyn 'wad Kazm. (2018). "Jra'm Alerhab". Mnshwrat Alhlby Alhqwqyh- Byrwt.

[26] Alkylany, Hythm. (1997). "Alerhab Y'ss Dwlh". Dar Alshrwq- Byrwt. T1.

[27] Lbky, Jwrj. (2013). "Alm'ahdat Aldwlyh Llantrnt-Hqa'eq Wthdyat". Mjlt Aldfa' Alwtny Allbnany: (83), Kanwn Althany/2013-Lbnan.

[28] Almzrw'y, Mwzh. (2000). "Alakhtra'at Alelktrwnyh Khtr Kyf Nwajhh". Mjlt Afaq Alaqtsadyh: Alamarat Al'rbyh Almthdh. (9).

[29] Almlt, Ahmd Khlyfh. (2005). Aljra'm Alm'lwmatyh. Dar Alfkr Aljam'y. T1. Alaskndryh.

[30] Mna'st, Asamh Ahmd Wakhrwn. (2001). Jra'm Alhasb Alaly Walentrnt. T1. Dar Wa'l. 'man-Alardn.

[31] Nsar, Ghadh. (2017). Alerhab Waljrymh Alelktrwnyh. Al'rby Llnshr Waltwzy'-Alqahrh. T1.

[32] Qtb, Mhmd 'ly. (2010). "Aljra'm Alm'lwmatyh Wtrq Mwajhtha". Alalkadymyh Almlkyh Llshrth- Wzart Aldakhlyh- Albhryn.

[33] Alqysy, Aysr Mhmd 'tyh. (2014). "Dwr Alalyat Alhdythh Fy Alhd Mn Aljra'm Almsthdthh". Bhth Qdm Lm'tmr Aljra'm Almstkhdmh Fy Zl Altghyrat Alaqlymyh Waldwlyh Aldy 'qd Fy 'man Btarykh 2-4/9/2014.

[34] Salh, Nayl 'bd Alrhmn. (2004). "Waq' Jra'm Alhasb Alaly Fy Altshry' Alardny". M'tmr Alqanwn Walkmbywtr Walentrnt-Jam't Alamarat Al'rbyh Almthdh. Klyt Alshry'h Walqanwn. Almjld Alawl. T3. Wqd 'qd Alm'tmr Mn 1-3/Mayw/2000.

[35] Shafy, Nadr 'bd Al'zyz. (2007). "Byn Ahtram Alhryat Alshkhsyh Wmra'ah Mslhh Aldwlh Walamn Alwtny". Mjlt Aljysh Allbnany: (263). Byrwt.

[36] Alshnyfy, 'bd Alrhmn 'bd Al'zyz. (1991). Hrb Alm'lwmat. Mktbh Ghryb- Alryad- Almmlkh Al'rbyh Als'wdyh.

[37] Alshwabkh, Ahmd Amyn Ahmd. (2004). Jra'm Alhaswb Walentrnt-Aljrymh Alm'elwmatyh. Dar Althqafh. 'man-Alardn.

[38] Alshhry, Fayz 'bd Allh. (2012). "Thqafh Alttrf Walerhab 'la Shbkh Alentrnt". Mnshwrat Jam't Alamyr Nayf Ll'lwm Alamnyh- Alryad.

[39] Sndaly, 'bd Alrzaq. (2019). "Altshry' Almghrby Fy Mjal Aljra'm Alelktrwnyh". Bhth Qdm Fy Alndwh Alaqlymyh Hwl Aljra'm Almtslh Balkmbywtr. Alrbat- Almghrb.

[40] Alsnd, 'bd Alrhmn Bn 'bd Allh. (2004). "Wsa'l Alerhab Alelktrwny Whkmha Fy Alaslam Wtrq Mkafhtha". Alm'tmr Al'almy-Mwqf Alaslam Mn Alerhab. Jam't Alamam Mhmd Bn S'wd Alaslamyh. Als'wdyh.

[41] Srwr, Ahmd Fthy. (2009). Almwajhh Alqanwnyh Llerhab. Dar Alnhdh Al'rbyh- Alqahrh.

[42] Alzbn, Bdr Hwyml. (2012). "Alerhab Fy Alfda' Alelktrwny". Rsalt Majstyr- Jam't 'man Al'rbyh. Alardn.

[43] Alzbwn, Ahmd 'ly Ahmd. (2015). "Aljra'm Alwaq'h 'la Amn Aldwlh Aldakhly Fy Alshry'h Alaslamyh Walqanwn Alardny".

[44] Alzbydy, Wlyd. (2003). Alqrsnh 'la Alentrnt Walhaswb. Altshry'at Alqanwnyh. T1. Dar Asamh. 'man- Alardn.