جامعة المنصورة

كلية الحقوق

الدراسات العليا

قسم القانون الجنائى

المواجهة الجنائية للإرهاب الإلكترونى

دراسة مقارنة

إشراف

أ.د/ أحمد شوقى عمر أبو خطوة

أستاذ القانون الجنائى

بكلية الحقوق- جامعة المنصورة

وعميد الكلية الأسبق

إعداد الباحث

راكان خالد سعود

٢٠٢٤

المقدمة

١- موضوع الدراسة:

يشهد العالم الحديث ثورة تقنية معلوماتية تكنولوجية هائلة، وتطوراً ملحوظاً في كافة مناحي الحياة، وكان لهذا التطور دوراً حيوياً في تسهيل وتسريع المعاملات وغيرها من حول العالم، وعلى الرغم من مزايا التكنولوجيا الرقمية، إلا أن هناك من يستغلها بما يخدم أهوائه الشخصية بطرق غير قانونية

ولأنه عالم واسع وشامل وكبير ويجمع الكثير من الأشخاص من حول العالم أطلق عليه مصطلح العالم الافتراضي، لأنه يجمع عدد هائل من الناس من حول العالم في مكان واحد بشكل افتراضي.

ويعد الإرهاب الإلكترونى من أخطر التهديدات المحدقة بالأمن القومى، الأمر الذي دفع المجتمع الدولي لحشد جهوده عن طريق منظماته من أجل الحد من الإرهاب عموماً والإرهاب الإلكترونى خصوصاً،وأصبحت القضايا المتعلقة بالإرهاب مصدر قلق خطير لانها تشكل خطراً على الأمن القومي

ويمكن القول أن السبب الرئيسي في انتشار الارهاب الإلكترونى هو أن الإرهابي لا يحتاج إلى أداة متفجرة أو عالية التقنية للقيام بمهاجمة الضحية ولكنه يحتاج فقط إلى نقل الفيروسات أو البرامجيات الخبيثة كل هذا يساعد الارهابي أن يكون غير معلوم الهوية مما يقلل من خطر وقوعه في أيدي السلطات.

٢- أهداف الدراسة:

١. بيان مفهوم الإرهاب الإلكترونى .

٢. التعرف على مخاطر الإرهاب الإلكترونى.

٣. بيان خصائص الإرهاب الإلكترونى.

٤. بيان صور جرائم الإرهاب الإلكترونى والمسؤلية الجنائية عنها.

٣- مشكلة الدراسة:

مع التطورات المتلاحقة للتكنولوجيا أضحى الأختلاف بين الجريمة السيبرانية والجريمة العادية يزداد انطماساً بشكل عام. فمع التزايد المستمر للعولمة وانتشار الأجهزة الإلكترونية أدى إلى التطور السريع في وسائل ارتكاب الجرائم، ومنها جرائم الإرهاب الإلكترونى.

وقد تغيرت خطط الإرهاب وأدواته المستخدَمة بمرور الوقت، ولاح في الأفق شبح الإرهاب الإلكتروني (السيبراني)، الذي يستهدف فيه الإرهابيون البُنى التحتية للدول، وأنظمة معلوماتها، وقواعدها العسكرية.

وتكمن مشكلة الدراسة فى الإجابة على الأسئلة التالية:

- ما مفهوم الإرهاب الإلكترونى ؟
- ما هى مخاطر الإرهاب الإلكترونى؟
- ماهى خصائص الإرهاب الإلكترونى؟
- ما هى صور جرائم الإرهاب الإلكترونى والمسؤلية الجنائية عنها؟

٤- منهج الدراسة :

تعتمد الدراسة على المنهج التحليلي والمنهج المقارن بين التشريعات فى مصر والكويت وفرنسا.

٥ - خطة الدراسة:

المبحث الأول : مفهوم الإرهاب الإلكترونى.

المبحث الثانى: مخاطر الإرهاب الإلكترونى وخصائصه ودور الأمن السيبرانى فى مواجهته

المبحث الثالث: صور جرائم الإرهاب الإلكترونى والمسؤلية الجنائية عنها.

الخاتمة.

المبحث الأول

مفهوم الإرهاب الإلكترونى

يعد الإرهاب اليوم ظاهرة إجرامية تهدد الوجود الإنساني، خاصةً مع مـــا تشهده الإنسانية من تطور تتطلبه الحياة المعاصرة، فالتقدم في مجال المعلومـــات دفع بظهور طفرة جديدة في صناعة الإرهاب الأمر الذي أدى إلى ظهور خطـــر جديد تمثل في الإرهاب الإلكترونى. والإرهابي هو من يلجأ إلى الإرهاب لإقامـــة سلطته.

وتشتق كلمة الإرهاب لغةً من الفعل أرهب[١] ، إذ نقول أره هب ، فلاناً ، أي خوفه وفزعه ، ورهب الشيء أي أخافه ، أما الإرهابيون (Terrorists) فهو وصف يطلق على أولئك الأفراد الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم (٢) والإرهاب الإلكترونى أصبح محوراً لإهتمام المنظمات الدولية والدول والأفراد [٣]

---

(١) ورد في لسان العرب: رهب: رَهِبَ بالكسر، يَرْهَبُ رَهبَةً ، بالضم رُهْباً، ورَهَباً، بالتحريك ، أي خافَ ورَهِبَ الشيءَ رَهْباً ورَهَباً ورَهْبةً: خافَه. وتَرَهَّبَ غيره إذا تَوعّدَه، وأَرْهَبَه ورَهَّبَه واسترْهَبَه: أخافَه وفَزعَّه. والرّاهِبة: هي الحالة التي تُرْهِبُ أي تُفزع وتُخوّفُ يقال أَسْمَعُكَ راهباً أي خائفاً. انظر: بن منظور، لسان العرب، ج٥، ط٣، دار إحياء التراث العربي، بيروت، ١٩٩٩، ص٣٣٧.

(٢) د. هالة أحمد الرشيدي ، الإرهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، ط١، دار النهضة العربية ، ٢٠٢٠ ، ص ٢٠.

(٣) عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، ط ١ ، المركز العربي للنشر والتوزيع ، القاهرة ، ٢٠٢١، ص٢٢

وجاء مفهوم الإرهاب فى قانون تنظيم قوائم الكيانات الإرهابية والإرهابيين رقم ٨ لسنة ٢٠١٥، حيث نصت المادة ١ على تعريف الإرهابى بـــأنه كل شخص طبيعي يرتكب أو يشرع في ارتكاب أو يحرض أو يهدد أو يخطط في الداخل أو الخارج لجريمة إرهابية بأية وسيلة كانت، ولو بشكل منفرد، أو يساهم في هذه الجريمة في إطار مشروع إجرامي مشترك، أو تولي قيادة أو زعامة أو إدارة أو إنشاء أو تأسيس أو اشترك في عضوية أي من الكيانات الإرهابية المنصوص عليها في المادة رقم (١) من هذا القانون أو قام بتمويلها، أو ساهم في نشاطها مع علمه بذلك.

ويعرفه مكتب التحقيقات الفيدرالي الارهاب السيبراني على أنه الهجوم المتعمد ذو الدوافع السياسية [٤].

وعرف البعض الإرهاب الإلكترونى بأنه: استخدام الإنترنت للقيام بأعمال عنف تؤدي إلى خسائر في الأرواح أو ضرر جسدي كبير من أجل تحقيق مكاسب سياسية من خلال الترهيب [٥]

وقيل أن السلوك يعد عملاً إرهابياً إذا كان يتسم بطابع العنف، ويكون نتيجته إحداث الخوف بين الناس، أو تهديد سلامتهم. وقد انتقد الفقه هذا المعيار من جهة أنه يكشف عن بعض صور الإرهاب ووسائله إلا أنه يبقى قاصراً عن الإحاطة بجميع صورة، فهناك بعض الصور من الأعمال الإرهابية التي ترتكب بدون استخدام وسائل العنف ومع ذلك لا يمكن إنكار طبيعتها الإرهابية، مثل تسميم مصادر المياه ونشر الأوبئة [٦].

ويُشير الإرهاب السيبراني الهجينHybrid Cyber Terrorism، وفيه يستخدم الإرهابيون البيئة السيبرانية في مختلف الانشطة فى الدعاية، والتخطيط لهجمات أرهابية فعلية، وتجنيد أعضاء جدد، وجمع الأموال، والتبرعات... الخ [٧]

ويعرف الباحث الإرهاب الإلكترونى بأنه نقطة التقاء الفضاء الإلكتروني والإرهاب، من خلال الهجوم على الكمبيوتر والشبكات والمعلومات المخزنة فيها لتحقيق أهداف سياسية أو اجتماعية، وهو التهديد أو الهجوم غير القانوني بشن هجماتٍ على أنظمة المعلومات، والبرامج، والبيانات، والمواقع الإلكترونية.

---

(4) FBI, 2002.code of Federal. Regulations.28 CFR. Section 0.85 on Judicial Administration. July 2001

(5)However, uradnik, Kathleen: cyber terrorism. 2011. California, Greenwood Retrieved, 4 December, 2016, pp. 140-149.

(٦) شذى عبد الجليل حسن، المواجهة الجنائية لجريمة تمويل الإرهاب، دراسة مقارنة مع التشريعات العربية والأجنبية والمعايير الدولية، رسالة دكتوراه، جامعة القاهرة، ٢٠١٨م، ص ٢١.

(٧)محمود أحمد القرعان، الجرائم الإلكترونية ، دار وائل للنشر والتوزيع، الطبعة الاولى، عمان ٢٠١٧، ص١١.

المبحث الثانى

مخاطر الإرهاب الإلكترونى وخصائصه

ودور الأمن السيبرانى فى مواجهته

للإرهاب الإلكترونى العديد من الخصائص التي تميِّزه عن الإرهاب في صورته التقليدية، والتي تسعى في نهاية الأمر لتحقيق أهداف غير مشروعة، وهي[٨]:

١. أن الإرهاب الإلكترونى إرهاب عابر للقارات والحدود

٢. صعوبة اكتشاف أثر الجاني في مرتكب واقعة الإرهاب الإلكترونى ، حيث يوجد صعوبات تقف حائلًا دون الوصول لدليل مادي يربط الجاني بالواقعة.

٣. الارهاب الإلكترونى يعد أحد أخطر أنواع الإرهاب، إذ إنه يؤثر بالسلب على الأمن القومي للدولة المستهدفة.

٤. لا يحتاج الارهاب الإلكترونى إلى العنف والقوة بل يتطلب كمبيوتر متصل بالانترنت ومزود ببعض البرامج اللازمة وبعض الخبرة[٩].

ففي عام ٢٠١٩ صدر تقرير دولى جاء فيه أن الإرهاب له خطورة كبيرة وهجَماتُه تتسبّب في أضرار اقتصادية كبيرة، أو اضطرابات جيوسياسية، أو مشاهدَ ومواقف تتصدع فيها الثقة بشبكة الإنترنت على نطاق شاسع.

---

(٨) علي عدنان الفيل، الإجرام الإلكتروني: دراسة مقارنة، ط١، منشورات زين القانونية، بيروت ٢٠١١، ص٧٤.

(٩) د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً، مجلة كلية الاقتصاد والعلوم السياسية جامعة القاهرة, مج٢٣, ع١، ٢٠٢٢، ص١٥١

وتتمثل الهجَمات الإرهابية واسعة النطاق بأفراد أو جماعات تهدف إلى إلحاق أضرار بشرية أو مادية واسعة النطاق.

وهذا الارهاب له صلة وثيقة بانهيار البِنية التحتية للمعلومات الهامة، وخطر إطلاق أسلحة الدمار الشامل.

وقد تتعدد طرائق العمل من استعمال البرامج التخريبية الخبيثة و(فيروسات) البرامج، إلى حجب الخِدْمات، والأعمال الاستخباراتية التجسُّسية على الشبكة وغيرها.ويمكن القول أن الجماعات الإرهابيّة استفادت من التطبيقات التكنولوجية[١٠].

وقد اتجهت الدول على العمل على تنظيم عملية وضع السياسات المثلى للتعامل مع الارهاب السيبراني من قبل الحكومات.

ففي ظل التحولات الرقمية التي يعيشها العالم ، تعتبر البيئة الرقمية عاملاً هاماً في انتشار مخاطر وتهديدات، وقد أصبحت هذه التهديدات تمس ليس فقط أمن المؤسسات وإنما أمن الأفراد وبذلك تكون شكلت تحدياً للدولة في سعييها لتحقيق أمنها القومي.

كما أنه من أبرز معالم الصراعات السياسية والتجارية بين الدول، ومن الناحية النظرية، فهي تعني الأنشطة الخبيثة من خلال الإنترنت ، والتي تستهدف البنى التحتية أو المنشآت والمؤسسات ، وهي قادرة على تعطيل البنية التحتية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية.

---

(١٠) د. هبه جمال الدين العزب، العلوم السياسية ما بين تأثير تقنيات الذكاء الاصطناعي ومراجعة أركان ووظائف مفهوم الدولة وبنية النظام العالمي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٣، العدد ١، يناير ٢٠٢٢ ص١١١.

وتتسم الجرائم السيبرانية بطابع سرية الهوية ولا تترك سوى القليل من الآثر، بالاضافة إلى ذلك لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية [١١].

واتساقا مع ما سبق فأمن المعلومات قد تجاوز مفهومه التقني ليشمل الأبعاد الأمنية والدفاعية والاستراتيجية، فضلا عن أنها أصبحت جزءاً لا يتجزأ من خطط الأمن القومي والمواثيق الدفاعية للتحالفات العسكرية.

كما أنها باتت محل اهتمام دائم في ظل التطور التكنولوجي المذهل الذي بقدر ما يحمله للعالم من فرص فإن في طياته مخاطر جمة، ومن ثم حاجة دول العالم الماسة إلى تشريعات دولية واضحة ومحددة بشأن مواجهة الإرهاب الإلكترونى.

وأصبحت الجرائم السيبرانية أكثر تعقداً، نظراً للتطور التكنولوجي وهذه التكنولوجيا تعتبر سلاح ذو حدين: فهي تجلب مزايا للدول والحكومات ولكن تجلب مزايا ا أيضاً لمرتكبي هذه الجرائم.

وقد يستعمل الإرهابي التكنولوجيا في اعتدائه أو التسهيل له، كأن يستخدم أنظمة معينة من خـــلال هجوم سيبراني [١٢] فالعديد من المنظمات الإرهابية تستخدم شبكات الإنترنت لتنفيذ عمليتها الارهابية [١٣]

وإدراكًا لخطورة التهديدات السيبرانية عمومًا وخطورة الإرهاب السيبراني خصوصًا، فقد أولت الكويت ومصر اهتماماً بالغًا بسبل مجابهة ذلك

---

(١١) تقرير الأمم المتحدة، مكافحة استخدام تكنولوجيا المعلومات والانصالات للاغراض الإجرامية، ص ٤٨.

(12) Daived p.Fidler, Russel Buchan, Emily Crawford,"Study Group on Cyber Security, Terrorism, and International Law"International Law Association, Report,2016,p29.

(١٣) د. أحمد يوسف جمعة، الإرهاب السيبراني والعملات الافتراضية والتجسس الالكتروني ، دراسة تحليلية تتناول استخدامات الارهاب للفضاء السيبراني ، ط١ ، دار الأهرام للنشر والتوزيع والإصدارات القانونية ، ، ٢٠٢٢ ، ص ٤٣.

التهديد، وسارعتا باتخاذ العديد من التدابير والإجراءات بما يدعم جهود والتحول الرقمي ورقمنة الخدمات الحكومية وتبني المعاملات الرقمية.

وتتسم التهديدات السيبرانية بأنها ديناميكية ومتغيرة، وبالإضافة إلى ذلك فإن التهديدات التي تواجه الكويت لا تختلف عن تلك التي تواجه بقية العالم مثل برامج التجسس وبرامج الفدية والتصيد الإلكتروني وأيضاً ما يعرف بهجمات الحرمان من الخدمات، مما يتطلب ضرورة العمل والحرص على حماية أمن تلك المعلومات والبيانات المتوفرة على مختلف الأنظمة[١٤].

واتخاذ جميع الإجراءات الضرورية من أخطار الهجمات السيبرانية من خلال إصدار تشريعات فعالة تحمى الأمن السيبرانى، فهذه الجرائم تمثل تحدياً كبيراً للأجهزة الأمنية والتشريعية، في كل الدول، ذلك أن عملية التشريع تستغرق وقتًا طويلاً لمواجهة تلك المخاطر [١٥] .

ويحظى الأمن السيبراني باهتمام العديد من الدول، خاصةً مع ظهور تهديدات قد تصل لحرب إلكترونية وإرهاب إلكترونى، وقد دخلت الكويت عالم الأمن السيبراني إذ أعلنت الحكومة الكويتية عن استراتيجية الكويت للأمن السيبراني ٢٠١٧/ــ ٢٠٢٠ وهي استراتيجية فنية قائمة على ثلاثة أمور الرؤية والمهمة والأهداف، وأهداف هذه الاستراتيجية هي تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الآمن والصحيح للفضاء الالكتروني [١٦]

---

[١٤] د.عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، مجلة كلية الشريعة والقانون بأسيوط، العدد ٣٤، ج٣، ٢٠٢٢ ، ص٢٩.

[١٥] د. أميرة عبد العظيم، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، مجلة البحوث الفقهية والقانونية بدمنهور ، العدد الخامس والثلاثون، ٢٠٢٠م، ص٣٨٨.

[١٦] أصدرت الكويت إستراتيجية للأمن السيبراني ٢٠١٧/ ٢٠٢٠، حددت أهدافها في تعزيز ثقافة الأمن السيبراني، التي تدعم الاستخدام الآمن والصحيح للفضاء الإلكتروني، وحماية ومراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية، والتعاون بين مختلف الجهات المعنية، بينما أشارت الإستراتيجية إلى إنشاء المركز الوطني للأمن السيبراني، يهدف المركز إلى تحقيق الأهداف المنبثقة من استراتيجية الأمن السيبراني.

ويعد إنشاء المركز وطني للأمن السيبراني أمر مهم في أداء الدولة بالمؤشرات العالمية المعنية مثل مؤشر الأمن السيبراني العالمي الذي بدوره يقيس في أحد محاوره التدابير القائمة على وجود مؤسسات تنسيق وسياسات واستراتيجيات لتطوير الأمن السيبراني على المستوى الوطني.

وفي آخر بيانات صادرة عن الاتحاد الدولي للاتصالات، احتلت الكويت الترتيب الـــ٦٥ في مؤشر الأمن السيبراني العالمي لعام ٢٠٢٠، مرتفعة عن العام السابق عليه، حينما كانت في المركز الـــ٦٧، في حين كانت في الترتيب الـــ١٣٩ عام ٢٠١٧، ثم قفزت إلى المركز الـــ٧٢ في عام ٢٠١٨، ما يعني أن هناك تطوراً تدريجياً ملحوظاً في هذا المجال[١٧]

ويستند المؤشر إلى ٥ معايير: قانونية، تقنية، تنظيمية، تنمية قدرات الأمن الالكتروني واجراءات التعاون بين الشركات والدول.

وتهدف منصة المركز الوطني للأمن السيبراني إلى تبادل البيانات وتعزيز الأمن السيبراني ما بين الجهات الحكومية لاتخاذ الاجراءات الاحترازية وذلك قبل وقوع اي هجوم سيبراني ، كما تعمل المنصة على مساندة قطاعات دولة الكويت الحيوية لتعزيز سبل الحماية لأنظمتها ودعم الاستجابة للحوادث المتعلقة بالأمن السيبراني ، حيث يتم التعامل مع الهجمات السيبرانية بسرعة وجدية ما بين الهيئة العامة للاتصالات وتقنية المعلومات والمختصين من مزودي خدمات الانترنت

ويسعى المركز الوطنى من خلاله استراتيجيته التى تتماشى مع رؤية الكويت ٢٠٣٥ إلى توفير فضاء سيبرانى آمن يدعم ويحمى المصالح الوطنية من الهجمات الإلكترونية وعمليات القرصنة إلى جانب مساندة قطاعات الدولة وتعزيز سبل الحماية لأنظمتها [١٨]

---

[17] https://www.aljarida.com/articles/1655140772392935800

(١٨) انظر: موقع الهيئة العامة للاتصالات وتقنية المعلومات عبر الرابط التالى:

وقد أولى القانون الكويتي أهمية للأمن السيبرانى، فنجد أن القانون رقم ٦٣ لسنة ٢٠١٥ يكافح ويتصدى لجرائم تقنية المعلومات، حيث تتسع استخدامات الشبكات الدولية في وقتنا الحاضر

وقد صدر فى الكويت مرسوم أميري بإنشاء المركز الوطني للأمن السيبراني، لبناء منظومة فعالة لحماية الفضاء الإلكتروني للدولة [١٩].

وحدّد المرسوم اختصاصات المركز في سبيل تحقيق أهدافه، وهي:

١ – إعداد إستراتيجيات وسياسات ومعايير وآليات تنفيذ الأمن السيبراني واقتراح تعديلها، بناء على اقتراح المجلس.

٢ – إعداد الخطة الوطنية لمواجهة المخاطر والتهديدات المتعلقة بالأمن السيبراني وتعديلها، ومتابعة تنفيذها بعد اعتمادها من اللجنة الوطنية العليا، بناء على اقتراح المجلس.

٣ – متابعة تنفيذ الجهات المعنية للإستراتيجية وخطط ومعايير وسياسات الأمن السيبراني الصادرة عن المركز.

٤ – وضع الإطار التنظيمي وآليات الحوكمة لتطبيق الإستراتيجية.

٥ – إعداد وتصنيف وتحديد البنية الأساسية للأمن السيبراني والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الصلة بالأمن السيبراني.

٦ – إجراء تدريبات ومسابقات الأمن السيبراني.

٧ – تنظيم عمل الشركات والخبراء والاستشاريين وغيرهم، ممن يقدمون خدمات الأمن السيراني، ومنح الترخيص، وإعداد سجل يقيد فيه المستوفون للمعايير الأمنية.

٨ – وضع الشروط والمواصفات الفنية لأي أجهزة أو أنظمة مرتبطة بمجال الأمن السيبراني.

---

https://citra.gov.kw/sites/ar/Pages/cybersecurity.aspx

([١٩]) مرسوم أميري رقم ٣٧ لسنة ٢٠٢٢ بإنشاء المركز الوطني للأمن السيبراني.

٩ – وضع الشروط والمعايير الوظيفية لشغل وظائف الأمن السيبراني بالجهات المعنية.

١٠ – القيام بالفحص الأمني التقني، والتدقيق على أنظمة وشبكات الجهات المعنية، للتأكد من التزامها بالمعايير والسياسات التي يصدرها المركز.

١١ – التدخل التقني، إذا ما تطلب الأمر، للتصدي لحوادث الأمن السيبراني، التي تتعرض لها الشبكات والجهات المعنية.

١٢ – مراقبة ورصد التهديدات الإلكترونية لشبكات الجهات المعنية، بما يكفل التصدي لأي تهديدات قد تلحق ضرراً بمنظومة الأمن الوطني، أو اقتصاد الدولة، أو علاقاتها الدولية والإقليمية.

١٣ – تقديم المساندة والاستشارة التقنية للجهات المعنية، من خلال الاستدلال، ومساندة التحقيق في الجرائم المتعلقة بالأمن السيبراني.

١٤ – إبداء الرأي التقني في الموضوعات المتعلقة بالأمن السيبراني.

١٥ – التنسيق والتعاون مع الجهات المعنية للعمل وفق بنود إطار الحوكمة الوطنية للأمن السيبراني.

١٦ – إعداد ودعم الدراسات والبرامج والبحوث العلمية اللازمة، الأكاديمية والمهنية المحلية والدولية، لتطوير منظومة الأمن السيبراني، بالتنسيق مع المؤسسات.

١٧ – إعداد التقارير الدورية، والسنوية في شأن تنفيذ الإستراتيجية، ورفعها إلى مجلس الوزراء.

١٨ – إعداد تقارير دورية حول الأمن السيبراني الوطني، ورفعها إلى مجلس الوزراء.

١٩ – تبادل المعلومات مع المراكز النظيرة المحلية والدولية.

٢٠ – تمثيل الدولة بالاشتراك في المنظمات والمؤتمرات واللجان والاجتماعات الإقليمية والدولية ذات الصلة.

وقد أصدر رئيس مجلس الوزراء المصرى قراراً بشأن الأمن السيبراني[٢٠]، وتنص المادة الأولى للقرار على التزام كافة الجهات الحكومية بكافة مستوياتها وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني

وقد نصت المادة الثانية للقرار على أن يتولى وزير الاتصالات وتكنولوجيا المعلومات وضع وتحديد قواعد وإجراءات تأمين البنية المعلوماتية الحرجة لقطاعات الدولة، ومتابعة تنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني وتطبيق أحكام هذا القرار.

يتضح من قرار تشكيل المجلس الأعلى للأمن السيبراني أنه يهدف إلى حماية المعلومات لدى الجهات مع الاهتمام بإدارات المعلومات والاتصالات في الوزارات والجهات المختلفة، والتأكد من توافر التمويل اللازم لضمان تنفيذ منظومة الأمن السيبرانى، مع ضرورة وضوح الإطار التشريعى الخاص به.

وفي ظل مواكبة التطور التكنولوجي والتحول الرقمي لابد من مواجهة العقبات والمعوقات الالكترونية بما يتناسب مع أهمية المعلومات لكل فرد أو مؤسسة وحماية هذه المعلومات من أي تلف أو هجوم إلكتروني قد يؤثر سلباَ في تقدم هذا التطور الراهن إضافة إلى ذلك تجهيز الموظفين وإعدادهم وتأهيلهم وتثقيفهم في أهمية الأمن السيبراني وكيفية التعامل في حالة حدوث أي مخاطر إلكترونية محتملة.

ويهدف الأمن السيبرانى إلى تعزيز قدرات الدول الأعضاء على منع الهجمات الإلكترونية التي تقوم بها الجهات الفاعلة الإرهابية ضد البنية التحتية الحيوية. كما يسعى البرنامج أيضاً إلى تخفيف تأثير هذه الهجمات الإلكترونية واستعادة وإصلاح الأنظمة المستهدفة في حالة حدوث تلك الهجمات.

حيث تعد الحرب السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول، من الناحية النظرية يقصد بالحرب السيبرانية الأنشطة

---

(٢٠) قرار رئيس مجلس الوزراء بشأن الأمن السيبراني، الجريدة الرسيمة في عددها رقم ١٧ مكرر (ب) بتاريخ ٢ مايو٢٠١٧.

الخبيثة من خلال شبكة الإنترنت المدعومة من دولة ما، والتي تستهدف البنى التحتية أو المنشآت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي قادرة على تعطيل تشغيل البنية التحتية الحيوية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية.

وأصبحت الجرائم السيبرانية أكثر تعقداً، نظراً للتطور التكنولوجي مثل إنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي وخدمات من قبيل برنامج حماية الخصوصية أونيون روتر والشبكة الخفية، كل هذه التكنولوجيا تعتبر سلاح ذو حدين: فهي تجلب مزايا للدول والحكومات ولكن تجلبها أيضا لمرتكبي الجرائم الإلكترونية.

وزاد الاهتمام بالأمن السيبرانى مع زيادة اعتماد العالم على الكمبيوتر وشبكة الإنترنت وتعود إرهاصاته إلى منتصف الخمسينيات من القرن الماضي مع بداية استخدام الحاسب الألي لمعالجة وحفظ المعلومات.

ومع مطلع التسعينيات وظهور الإنترنت وإقبال الكثير من الدول على استخدامها في المجال الأمني والعسكري لتحقيق قفزات نوعية في المجالات الأمنية والسياسية. وبدأ الحديث عن قدرة شبكة المعلومات الدولية على إعادة بلورة الأشكال التقليدية وقواعد القوة الدولية والمقدرات الدولية للوحدات الفاعلة في النسق الدولي

ويأتي الاهتمام بالأمن السيبراني مع زيادة الخسائر الناتجه عن الهجمات الألكترونية، وما يعنيه ذلك من تهديدات على الأمن القومي للدول، وبالتبعية على السلم والأمن الدوليين. فمن المتوقع أن تصل الأضرار الناجمة عن جرائم الإنترنت إلى ما يقدر بنحو ١٠,٥ تريليون دولار بحلول عام ٢٠٢٥ [٢١]

([21])Amy Borrett and Georges Corbineau, Cybersecurity rankings reveal leading global cyber powers, TECHMOINITOR, Nov. 27, 2020.

وتشير العديد من التقارير الدولية إلى ارتفاع عدد الجرائم والهجمات الإلكترونية من مختلف الأنماط والدرجات، لتصل إلى ٥٥٦ مليون جريمة في عام ٢٠١٧ ، أي بمعدل ١,٥ مليون جريمة في اليوم، و١٨ جريمة أو هجمة في الثانية، ما يكبد المؤسسات والأفراد وحتى الحكومات، خسائر مالية تتجاوز ١٠٠ مليار دولار، بينما سيصل عدد الكيانات التي ستتعرض للهجمات إلى ٢٣٢,٤ مليون كيان، ما بين أفراد ومؤسسات وقطاعات حكومية وخاصة[٢٢].

لذلك اتجهت معظم الدول، إلى إقرار سياسات وقائية ودفاعية، ضد الهجمات الإلكترونية، وخصصت الدول الكبرى، مثل الولايات المتحدة الأميركية واستراليا، والمملكة المتحدة، مبالغ طائلة، لمعالجة مسائل الأمن السيبرانى، واستقرار الفضاء الإلكترونى من مخاطر الإرهاب الإلكترونى.

ويعتبر الإرهاب الإلكترونى تهديداً رئيسياً يواجه جميع الدول، مما يدفعها لسن تشريعات تجرم الهجمات الإلكترونية، وتبادل الخبرات دون تأثير على استقلالية القرار وأولوية المصلحة الوطنية [٢٣].

لقد تعاملت الأمم المتحدة، مع تقنيات المعلومات والاتصالات، خاصةً فيما يتعلق بالإنترنت، من منطلق كونها أداة للتنمية الاجتماعية والاقتصادية، فقد عهدت إلى المجلس الاقتصادي الاجتماعي، لمتابعة قضايا التنمية المتعلقة بالإنترنت.

وفي المقابل، تهتم اللجنة الخاصة بالعدالة الجنائية ومنع الجريمة، الموكلة بمتابعة الجهود الدولية في مكافحة ومنع الجرائم الوطنية والعابرة للحدود، بالقضايا المتعلقة بجرائم الإنترنت[٢٤].

---

(٢٢)

/https://cybersecurityventures.com

(٢٣) د. هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي مجلة كلية الاقتصاد والعلوم السياسية , جامعة القاهرة ، مج٢٤, ع١، ص ٢٠٢٣، ص ١٩٣

وقامت الأمم المتحدة بعدد من الجهود للتصدي للهجمات والجرائم السيبرانية [٢٥] تنوعت بين وضع قواعد موضوعية وإجرائية ومؤتمرات وقمم دولية وجهود لبعض الهيئات والأجهزة التابعة لها

كما أقر المجلس الأوروبي اتفاقية مكافحة الجريمة الإلكترونية [٢٦] وتعتبر أحكام هذه المعاهدة، منسجمة مع متطلبات مكافحة الجريمة الإلكترونية، لاسيما وأنها تطلب من الدول الأعضاء، إنشاء مراكز اتصال، تعمل بحسب مبدأ استمرارية الخدمة، أي تأمين متابعة على امتداد ساعات اليوم، بحيث تكون دائمة الاستعداد، للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية، وللتعاون مع القوات المعنية بمكافحة الجريمة، بسرعة وفعالية.

([24]) Economic and Social Council Resolution 1992/22: Implementation of General Assembly Resolution 46/152 concerning operational activities and coordination in the field of crime prevention and criminal justice, E/1992/92, 30 July 1992.

([٢٥]) حيث قامت لجنة الأمم المتحدة لمنع الجريمة والعدالة الجنائية في أبريل ٢٠١٠ في دورتها الثانية عشرة بصياغة مجموعة من الإعلانات تضمنت إنشأ فريق خبراء حكومي دولي لبحث مشكلة الجريمة السيبرانية والاستجابات الدولية لها. كما افتتح المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة دورته لعام ٢٠١٠ بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلاً عن التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع. أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن "توحد أداءها" بشأن هذه القضية. وحذّروا من أن النطاق الدولي لحرب سيبرانية فعلية وعواقبها الوخيمة سوف تقضي استجابة منسقة؛ ولا تكفي الآن استراتيجيات اعتماد حلول على أساس مخصص وتقوية الدفاع. وأهتمت الأمم المتحدة بالبناء المؤسسي فقانت بإنشاء بعض الكيانات مثل الشراكة التعددية ضد التهديدات السيبرانية Impact عام ٢٠٠٩ كأول منظمة تدعمها الأمم المتحدة للتحالف لدعم الأمن السيبراني

([٢٦]) مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، العدد ٢، ٢٠١٩.

وتعالج اتفاقية المجلس الأوروبي بشأن الجرائم السيبرانية بعض الجرائم الإلكترونية من خلال توفير أحكام قانونية نموذجية يمكن أن تعتمدها البلدان وتكيفها مع احتياجاتها الخاصة.

وعلى الرغم من أن الاتفاقية تقدم بعض الحلول القانونية للجرائم من قبيل النفاذ غير القانوني (القرصنة) واعتراض الاتصالات، فإنها لا تعالج بعض أنواع عمليات الهجوم السيبراني الأكثر تهديداً مثل التجسس للحصول على البيانات وأعمال التخريب.

ويرى الباحث ضرورة رفع كفاءة الأشخاص المختصين بمكافحة الإرهاب الإلكترونى، وضرورة تأمين البنى التحتية الحيوية والحث على استمرار التقييم الدوري الشامل لمستوى الأمن السيبراني في دولة الكويت في القطاعات كافة وتحديد الفجوات للوصول إلى المستوى المنشود .

المبحث الثالث

صور جرائم الإرهاب الإلكترونى والمسؤلية الجنائية عنها

تمهيد وتقسيم:

بات الإرهاب الإلكترونى جاذبًا لمختلف التنظيمات الإرهابية لأنه يتطلب عدداً أقل من الأشخاص والموارد، ويمكنها من استهداف أهداف واسعة النطاق، مع الحفاظ على مجهولية هوية الإرهابيين لا سيما مع إمكانية تواجدهم في أماكن بعيدة عن المواقع الفعلية المستهدفة.

فمن خلال الإرهاب الإلكترونى ، يمكن للإرهابيين إلحاق أضرار مادية ومعنوية بالدول المستهدفة على نحو يفوق تلك التي قد تنجم عن الإرهاب التقليدي كاتلاف المستندات والسجلات الإلكترونية[١].

وهناك صور عديدة للارهاب الإلكترونى ومنها استخدام الذكاء الاصطناعى فى الإرهاب واختراق البيانات والمواقع الإلكترونية للدولة ونشر الشائعات الإلكترونية ونعرض لها على النحو التالى:

أولاً- استخدام الذكاء الاصطناعى فى الإرهاب:

تتمثل أهم مخاطر الذكاء الاصطناعي[٢] في سهولة ارتكاب عمليات الاختراق والإرهاب السيبراني وهو ارهاب المستقبل[١]، بجانب تسريب البيانات

---

[١] راشد محمد المري: الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر دراسة مقارنة، القاهرة، دار النهضة العربية، ٢٠١٨، ص١٢.

[٢]عرف البعض الذكاء الاصطناعى بأنه هو العلم القادر على بناء الآلات التي تؤدي مهاماً تتطلب قدرا قدرا من الذكاء البشري عندما يقوم بها الإنسان. د. محمود عبدالغنى فريد جاد المولى، الإتجاهات

والمعلومات، وإساءة استخدام الذكاء الاصطناعي، وتقديم نصوص تحاول فيها روبوتات الدردشة إقناع المستخدِم بما هو غير صحيح أو غير مشروع قانونًا.

ومن الممكن أن تخترق الجماعات الإرهابية الأنظمة الأمنية والدفاعية للدول، حيث إن جميع المنظومات الإلكترونية التي تعمل على نطاق شبكي أو تتفاعل مع بيئات إلكترونية مناظرة، من الممكن أن تكون عرضة دائمًا للاختراق من خلال مخارج البيانات المتبادلة ومداخلها

إضافة إلى وجود قابلية دائمًا لزرع برمجيات خبيثة، سواءً للتجسس أو للتخريب. لذا، تستطيع الجماعات الإرهابية أن تُعدّل البرمجيات الأصلية؛ سواءً بنسخ البيانات أو التحكم في المخرجات بما يتوافق مع أغراض تلك الجماعات.

وانتشر الذكاء الاصطناعي [٢] بشكل متزايد حتى خرج عن النطاقات المشروعة سواءً للدفاع أو الأمن أو الملاحقة والاستهداف، إضافة إلى الاستخدامات المدنية، وانتقلت إلى نطاق آخر غير مشروع.

كما يستفيد الإرهابيون[٣] من التعليم الآلي والعميق [٤] والأشكال الأخرى لتطبيقات للذكاء الاصطناعي في الاستعدادات لهجامتهم وجمع المعلومات عند تنفيذ الهجمات ،ويمكن للمهام الآلية أن تجعل حجم هذه الهجمات وتأثيرها أكبر. وقد

الحديثة فى المسئولية الجنائية للكيانات التى تعمل بتقنيات الذكاء الإصطناعى، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنوفية، المجلد ٥٣، العدد ٣، مايو ٢٠٢١، ص ٤٩٨

(١) محمود محمد عبد الحليم محمود مرشد، الأحكام الموضوعية والإجرائية لجرائم الإرهاب، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٤٤٣هـ/٢٠٢٢م

(2) S.Samoili, M.López Cobo, E. Gómez, G.De Prato, F. Martinez-Plumed and B.Delipetrev,Al watch. European Union: Joint Research Centre, 2020, p7.

(٣) د. هبه جمال الدين العزب، العلوم السياسية ما بين تأثير تقنيات الذكاء الاصطناعي ومراجعة أركان ووظائف مفهوم الدولة وبنية النظام العالمي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٣، العدد ١، يناير ٢٠٢٢ ص١١١.

(4) ONGSULEE, Pariwat. Artificial intelligence, machine learning and deep learning. In: 2017 15th international conference on ICT and knowledge engineering (ICT&KE). IEEE, 2017. p. 1-6.

تصدى المُشَرِّع للترويج للجريمة الإرهابية في قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥ [١].

ثانياً- الاختراق الإلكتروني والشائعات الإلكترونية

نظراً لمخاطر الإرهاب الإلكتروني والاختراق الإلكتروني جرم المشرع الكويتي الأنشطة الإرهابية فقد نصت المادة ٢ من القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات، على جريمة الولوج الغير مشروع إلى الحاسب الآلي، بتشديد العقوبة في فقراتها الثانية والثالثة في حالة إذا ما نتج عن هذا الدخول تلف أو إلغاء للبيانات أو في حالة سرقة المعلومات الشخصية، كما ونصت الفقرة الرابعة على تشديد العقوبة إذا كانت الجريمة لغرض او أثناء تأدية وظيفة.

وتضمنت المادة ٣ تشديد العقوبة إذا كانت البيانات حكومية أو مرتبطة بحسابات العاملين في المنشآت المصرفية، بما في ذلك أيضاً استخدام أي وسيلة من الوسائل التقنية المعلومات في عمليات تهديد الأشخاص وابتزازهم، وتشديد العقوبة في حال التهديد بارتكاب جناية تمس بشرف الأشخاص أو كرامتهم.

---

(١) تنص المادة ٢٩ من هذا القانون: يُعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعًا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج. ويُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعًا إلكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها.

مما سبق يتضح أهميّة الأمن السيبراني في الأمور المرتبطة بحماية البيانات من المهاجمين ، إذ يمكن أن تكون هذه البيانات حساسة، أو معلومات حكومية مهمة.

كما يُشكّل وجود برامج الأمن السيبراني وآليات الدفاع الإلكترونية وسيلة متطورة ذات أهمية كبيرة في الحفاظ على البُنية التحتية الحيوية وبرامج الخدمات المالية .

وتمثل الشائعات خطورة كبيرة وبالتالي فإن ترويجها في قضية معينة لا يتم بشكل عشوائي، فقد يتم استخدام حملات التأثير في الرأي العام عبر الفضاء الإلكتروني وتمثل الشائعات خطراً كبيراً يُهدد استقرار الدول [١] وتضييع الحقوق[٢].

وقد جرم المشرع الكويتى فى المادة (١٤) من قانون الجزاء الكويتى نشر الشائعات [٣]

---

(1) SAHAFIZADEH, Ebrahim; LADANI, Behrouz Tork. The impact of group propagation on rumor spreading in mobile social networks. Physica A: Statistical Mechanics and its Applications, 2018.p. 133

(2) HINDAW El-Sayed Fettouh Mohamed.MODERN ADMINISTRATIVE METHODS TO COMBAT ELECTRONIC RUMORS. Journal of Legal, Ethical and Regulatory Issues, 2021, p.1-11.

(٣) القانون رقـــم ٣١ لسنة ١٩٧٠ بشأن جرائم أمن الدولة الخارجي والداخلي.

فنص على أنه يعاقب بالحبس المؤقت الذي لا تقل مدته عن ثلاث سنوات كل من أذاع عمداً في زمن الحرب أخباراً أو بيانات أو إشاعات كاذبة أو مغرضة أو عمد إلى دعاية مثيرة وكان من شأن ذلك كله إلحاق الضرر بالاستعدادات الحربية للدفاع عن البلاد أو بالعمليات الحربية للقوات المسلحة أو إثارة الفزع بين الناس أو إضعاف الجلد في الأمة. وتكون العقوبة الحبس المؤقت الذي لا تقل مدته عن خمس سنوات إذا ارتكبت الجريمة نتيجة التخابر مع دولة أجنبية. وتكون العقوبة الحبس المؤبد إذا ارتكبت الجريمة نتيجة التخابر مع دولة معادية. وتنص المادة (١٥) على العقاب بالحبس المؤقت الذي لا تقل مدته عن ثلاث سنوات كل كويتي أو مستوطن في الكويت أذاع عمداً في الخارج أخباراً أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للبلاد وكان من شأن ذلك إضعاف الثقة المالية بالدولة أو هيبتها واعتبارها أو باشر بأية طريقة كانت نشاطاً من شأنه الإضرار بالمصالح القومية للبلاد.

ويرى الباحث أن الأمن السيبرانى يساعد فى مواجهة الشائعات الإلكترونية، وتقليل مخاطر الهجمات الإلكترونية على الصعيد الفردي، إذ يمكن أن تتسبب هذه الهجمات إلى تعرض الأفراد لسرقة هوياتهم وابتزازهم، والاعتداء على حياتهم الخاصة، وبالتالي إحداث أضرار وخيمة في حياة الأفراد.

الخاتمة

فى نهاية هذه الدراسة توصل الباحث إلى النتائج والتوصيات التالية:

أولاً- النتائج:

١. إدراكًا لخطورة التهديدات السيبرانية عموماً وخطورة الإرهاب الإلكترونى خصوصاً، فقد أولت الكويت ومصر اهتماماً بالغًا بسبل مجابهة ذلك التهديد، وسارعتا باتخاذ العديد من التدابير والإجراءات لتنظيم الفضاء السيبراني وحماية البيانات على مختلف المستويات، بما يدعم جهود والتحول الرقمي ورقمنة الخدمات الحكومية وتبني المعاملات الرقمية.

٢. تصدى المشرع الكويتي لحماية المجتمع من مخاطر الإرهاب الإلكترونى وذلك بتجريم الأنشطة الارهابية

٣. أضحى الفضاء السيبراني ساحة جاذبة للتنظيمات الإرهابية، لأنه يُمكّنها من القيام بأنشطتها على نطاق واسع. فمن خلال الإرهاب السيبراني، يمكن للإرهابيين إلحاق أضرار مادية ومعنوية بالدول المستهدفة على نحو يفوق تلك التي قد تنجم عن الإرهاب التقليدي.

٤. قدرة الإرهاب السيبراني على التأثير في مجموعات واسعة من السكان تُمكّن التنظيمات الإرهابية من تحقيق مختلف أهدافها الاستراتيجية بسهولة متزايدة.

٥. بات الإرهاب الإلكترونى أشد خطورةً، بعدما استطاع الإنترنت اختراق جميع الحواجز، وأصبح بمثابة إرهاب المستقبل الذي يعتمد بدوره على الذكاء الاصطناعي .

٦. نظراً لمخاطر الإرهاب الإلكترونى والاختراق الإلكترونى جرم المشرع الكويتى الأنشطة الإرهابية فقد نصت المادة ٢ من القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات، على جريمة الولوج الغير مشروع إلى الحاسب الآلي، بتشديد العقوبة في فقراتها الثانية والثالثة في حالة إذا ما نتج عن هذا الدخول تلف أو إلغاء للبيانات أو في حالة سرقة المعلومات الشخصية، كما ونصت الفقرة الرابعة على تشديد العقوبة إذا كانت الجريمة لغرض او أثناء تأدية وظيفة.

ثانياً- التوصيات:

١. نوصى المشرع الكويتى بتعديل نص المادة ٢ من القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات، بالنص صراحة على تجريم استخدام تطبيقات الذكاء الاصطناعى فى الإرهاب الإلكترونى وتشديد العقوبات فى هذه الحالة.

٢. نوصى المشرع الكويتى بتعديل نص المادة ١٥ من القانون رقم ٣١ لسنة ١٩٧٠ بشأن جرائم أمن الدولة الخارجي والداخلي، لتكون العقوبة السجن مدة لا تقل عن ٥ سنوات كل كويتي أو مستوطن في الكويت أذاع عمداً في الخارج أخباراً أو بيانات أو إشاعات كاذبة أو مغرضة حول الأوضاع الداخلية للبلاد وكان من شأن ذلك إضعاف الثقة المالية بالدولة أو هيبتها واعتبارها أو باشر بأية طريقة كانت نشاطاً من شأنه الإضرار بالمصالح القومية للبلاد.

٣. ضرورة العمل على تنظيم القوانين الخاصة بمقدمي الخدمات فى منظومة البيانات، وتشديد العقوبات لجرائم اختراقها, والتأكيد على ضرورة النص على تجريم الدخول غير المشروع، للجهات العامة والخاصة، غير المخولة قانوناً بتلك البيانات والمنظومات التقنية، منعاً، لإساءة استعمال السلطة، وأن يتم ذلك بإذن قضائي.

٤. التأكد من مواءمة التشريعات الوطنية مع التشريعات الدولية، والتوسع في توقيع الاتفاقيات الثنائية ومتعددة الأطراف لدفع التعاون في مجال مكافحة الإرهاب بشكل عام ومكافحة الإرهاب السيبراني بشكل خاص.

٥. ضرورة رفع كفاءة الأشخاص المختصين بمكافحة الإرهاب الإلكترونى، والحث على استمرار التقييم الدوري الشامل لمستوى الأمن السيبراني في دولة الكويت في القطاعات كافة وتحديد الفجوات للوصول إلى المستوى المنشود.

قائمة المراجع

١- الكتب:

١. د. أحمد يوسف جمعة، الإرهاب السيبراني والعملات الافتراضية والتجسس الالكتروني ، دراسة تحليلية تتناول استخدامات الارهاب للفضاء السيبراني ، ط١ ، دار الأهرام للنشر والتوزيع والإصدارات القانونية ، ٢٠٢٢ .

٢. شادى عبد السلام، حروب الجيل الخامس، أساليب التفجير من الداخل على الساحة الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، ابوظبي، الامارات، ٢٠٢٠.

٣. د.عمر عباس خضير العبيدي، الإرهاب الالكتروني في نطاق القانون الدولي، ط ١ ، المركز العربي للنشر والتوزيع ، القاهرة ، ٢٠٢١.

٤. د.عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، ٢٠٠٩.

٥. علي عدنان الفيل، الإجرام الإلكتروني: دراسة مقارنة، ط١، منشورات زين القانونية، بيروت ٢٠١١، ص٧٤.

٦. د.راشد محمد المري: الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر دراسة مقارنة، القاهرة، دار النهضة العربية، ٢٠١٨.

٧. د. مي ممدوح قايد، السياسة الجنائية لمواجهة الارهاب المعاصر، دار النهضة العربية، ٢٠٢٢.

٨. محمود أحمد القرعان، الجرائم الإلكترونية ، دار وائل للنشر والتوزيع، الطبعة الاولى، عمان ٢٠١٧.

٩. د. محمود صالح العادلي، موسوعة القانون الجنائي للإرهاب، الجزء الثاني، السياسة الجنائية لمواجهة العنف الإرهابي، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.

١٠. نسرين عبد الحميد ، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكنرية، ٢٠٠٥.

١١. هالة أحمد الرشيدي، الإرهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، دار النهضة العربية، ٢٠٢٠,

٢- الرسائل العلمية:

١٢. أحمد يوسف محمد جمعة، الإرهاب الإلكترونى فى ضوء أحكام القانون الدولى، رسالة دكتوراه، كلية الحقوق جامعة المنصورة، ٢٠٢١.

١٣. شذى عبد الجليل حسن، المواجهة الجنائية لجريمة تمويل الإرهاب، دراسة مقارنة مع التشريعات العربية والأجنبية والمعايير الدولية، رسالة دكتوراه، جامعة القاهرة، ٢٠١٨.

١٤. علي محمد عامر العجمي، الإرهاب في القانون الجنائي دراسة مقارنة، رسالة دكتوراه ، كلية الحقوق، جامعة طنطا، ٢٠٠٩.

١٥. محمود محمد عبد الحليم محمود مرشد، الأحكام الموضوعية والإجرائية لجرائم الإرهاب، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٢٢.

٣- الأبحاث والمجلات العلمية:

١٦. د. سليم محمد سليم حسين، السياسة الجنائية في مواجهة الإرهاب الإلكتروني دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، المجلد ٦١، العدد ٢، يوليو ٢٠١٩.

١٧. د. سكينة العابد، أمن المعلومات عبر شبكات التواصل الاجتماعي موقع فيسبوك نموذجا، المجلة العربية للمعلوماتية وأمن المعلومات، المجلد ١، العدد ١، أكتوبر ٢٠٢٠ .

١٨. د. عمار ياسر زهير البابلي، الذكاء الاصطناعى ومكافحة الشائعات، مجلد مسابقة أبحاث مركز بحوث الشرطة "دورية محكمة"، أكاديمية الشرطة ، القاهرة ، ٢٠٢٢.

١٩. د.راشد عبيد حسن البغام النقبي، دور التواصل الاجتماعي في خلق الفكر الإرهابي، المجلة القانونية، المجلد ١٢، العدد ٦، ٢٠٢٢ .

٢٠. د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً، مجلة كلية الاقتصاد والعلوم السياسية جامعة القاهرة, مج٢٣, ع١، ٢٠٢٢.

٢١. د. هبه جمال الدين العزب، العلوم السياسية ما بين تأثير تقنيات الذكاء الاصطناعي ومراجعة أركان ووظائف مفهوم الدولة وبنية النظام العالمي، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٣، العدد ١، يناير٢٠٢٢ .

٢٢. د. هبة جمال الدين، الأمن السيبراني والتحول في النظام الدولي مجلة كلية الاقتصاد والعلوم السياسية , جامعة القاهرة ، مج٢٤, ع١، ٢٠٢٣.

٢٣. د. محمود عبدالغنى فريد جاد المولى، الإتجاهات الحديثة فى المسئولية الجنائية للكيانات التى تعمل بتقنيات الذكاء الإصطناعى، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنوفية، المجلد ٥٣، العدد ٣، مايو ٢٠٢١.

٢٤. مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، العدد ٢، ٢٠١٩.

٢٥. د.عابد فايد عبد الفتاح، القانون في مواجهة الشائعات ، مجلة الفكر الشرطي ، المجلد ٢٤ ، س ٩٢، عدد يناير ٢٠١٥م .

٢٦. د.عادل موسى عوض جاب الله، وسائل حماية الأمن السيبراني دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، مجلة كلية الشريعة والقانون بأسيوط العدد ٣٤، الإصدار الأول، ج٣، ٢٠٢٢ ، ص٢٩.

٢٧. د.أميرة عبد العظيم، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، مجلة البحوث الفقهية والقانونية بدمنهور ، العدد الخامس والثلاثون، ٢٠٢٠م.

٤- المراجع الأجنبية

1. Amy Borrett and Georges Corbineau, Cybersecurity rankings reveal leading global cyber powers, TECHMOINITOR, Nov. 27, 2020.

2. Eric Morris and Alan hoe, Terrorism: threat and response , London , the Macmillan press L T D,1997.

3. NDUBUEZE, Philip N. History, Evolution and Challenges of Cyber Criminological Scholarship. International Journal of Cyber Criminology, 2021.

4. FBI, 2002.code of Federal. Regulations.28 CFR. Section 0.85 on Judicial Administration. July 2001.

5. However, uradnik, Kathleen: cyber terrorism. 2011.

6. California, Greenwood Retrieved, 4 December, 2016.

7. Daived p.Fidler, Russel Buchan, Emily Crawford,"Study Group on Cyber Security, Terrorism, and International Law"International Law Association, Report,2016.

8. S.Samoili, M.López Cobo, E. Gómez, G.De Prato, F. Martinez-Plumed and B.Delipetrev,Al watch. European Union: Joint Research Centre, 2020.

9. ONGSULEE, Pariwat. Artificial intelligence, machine learning and deep learning. In: 2017 15th international conference on ICT and knowledge engineering (ICT&KE). IEEE, 2017.

10. SAHAFIZADEH, Ebrahim; LADANI, Behrouz Tork. The impact of group propagation on rumor spreading in mobile social networks. Physica A: Statistical Mechanics and its Applications, 2018.

11. HINDAW El-Sayed Fettouh Mohamed.MODERN ADMINISTRATIVE METHODS TO COMBAT ELECTRONIC RUMORS. Journal of Legal, Ethical and Regulatory Issues, 2021.