الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف بالمسيلة
قسم الحقوق

مذكرة مقدمة لنيل شهادة الماستر في الحقوق: قانون جنائي

تحت عنوان :

الإرهاب الإلكتروني

من إعـــداد:
- قلميـــن خولـــة .

تحت إشراف:الدكتور
- دحية عبد اللطيـف .

الاسم واللقب	الرتبة	الجامعة	الصفة
د. مهدي رضا	أستاذ التعليم العالي	جامعة مسيلة	رئيسا
د.دحية عبد اللطيـف	أستاذ التعليم العالي	جامعة مسيلة	مشرفا ومقررا
د. والي عبد اللطيف	أستاذ التعليم العالي	جامعة مسيلة	مناقشا

السنة الجامعية:2022/2021

شكر وعرفان

أولا وقبل كل شيء نشكر الله عز وجل الذي

وفقنا وألهمنا القدرة على انجاز هذا العمل

كما نتقدم بجزيل الشكر والتقدير للأستاذ البروفيسور

" دحية عبد اللطيف " الذي ساعدنا بالقدر المستطاع

من أجل انجاز هذا العمل

ونتقدم بخالص الشكر والتقدير:

كل من علمنا حرفا منذ بداية مشوارنا الدراسي

من الأساتذة الذي بذلوا كل الجهود في سبيل

تكويننا وساعدونا على اكتساب العلم والمعرفة

وأشكر لجنة المناقشة على قبولها مناقشة

هذه المذكرة، وعلى التوجيهات والملاحظات

التي سوف تقدمها لنا .

وفي الأخير نتقدم بالشكر الجزيل لكل من

ساعدنا ودعمنا من قريب أو بعيد من أجل

انجاز هذه المذكرة

إهداء

اللهم لك الحمد والشكر كما ينبغي لجلال وجهك وعظيم سلطانك

وعلو مكانك.

الحمد الله والصلاة والسلام على رسول الله "صلى الله عليه و سلم"

أهدي ثمرة جهدي إلى من ربياني إلى اللذان أوقدا شمعة

حياتهما ليضيئا دربي إلى أمي الغالية أطال الله في

عمرها و إلى أبي العزيز أدامهما الله تاجا فوق رأسي

إلى من نشأت و ترعرت بينهم إخوتي و أخواتي

كل بإسمه

إلى كل من ساعدني

للوصول إلى هنا.

قلمين خولة

مقدمة:

مما لاشك فيه أن الشعوب والمجتمعات البشرية لطالما عانت من العنف والتقتيل منذ عصور خلت نتيجة لانتشار الإجرام وتنازع القوى،ولعل أبشع صور هذه الجرائم وأخطرها تتمثل في الإرهاب الذي ما إن ذكر حمل في طياته جراحا غائرة وفيضات من الآلام التي تقشعر لها الأبدان وما خلفه إزهاق لالاف الأرواح من الأبرياء،هذا الإرهاب الغاشم الذي تخالف مظاهره مبادئ الفطرة السوية للبشر،فأصبح بذلك هاجسا يأرق الدول ومولدا للرعب ومنبها عن عودة السيناريوهات الدامية في المجتمعات التي طالما تخبطت فيها الشعوب لعقود طالت.

كما أن التطور التكنولوجي الذي أضحى العالم يعيش فيه قد أدى إلى تغير شكل الحياة على وجه الأرض وتباين موازين القوى،فأصبح الاعتماد على وسائل تقنية المعلومات يزداد يوما بعد يوم ليغزو المؤسسات المالية والمرافق العامة والتعليمية وحتى مؤسسات الأمن داخل الدول،ماسأهم في نقل المجتمعات التقليدية إلى مجتمعات ذكية وحديثة لدرجة أن القرن 21 أصبح يطلق عليه تسميته عصر المعلوماتية والسرعة. وان كانت للوسائل التكنولوجية المتطورة مالا يعد ولا يحصى من المزايا فان هذا لا يخفي ولا يغطي الوجه الأخر والمظلم للمعلوماتية والذي يعبر عن الاستغلالات السلبية والضارة وما تبعه من تطور في أساليب ارتكاب وتنفيذ الجرائم. ما أسهم في ظهور أشكال وأنماط جديدة لها كالسطو على برامج الحاسوب وسرقة المعطيات وتصاعد التهديدات الأمنية الأمر الذي استقطب اهتمام المجتمع الدولي بشكل لم يسبق له مثيل نظرا لما تثيره من مخأوف مفرطة على امن الدول واستقرار الشعوب وما تملكه من انتهاكات لحرمة الحرية والحياة لاسيما مع التطور الذي يشهده مجال التسلح وتعزيز التحالفات الإرهابية مع الفواعل الأخرى خاصة شبكة الانترنت والفضاء الرقمي،ما انجر ونجم عنه ظهور اخطر التصرفات العدائية الإجرامية،والمتمثلة في"الإرهاب الالكتروني"،الذي ارتبط اسمه مؤخرا بأغلب الأحداث والوقائع المتسارعة على الساحة الدولية والوطنية وخاصة العربية أوما أطلق عليه تسمية" ثورات الربيع العربي"،جراء استغلال

تكنولوجيا الإعلام والاتصال في تحقيق أغراض إرهابية غير مشروعة وترويج العنف والتطرف وبث الرعب والخوف.

وفي غمرة التصدي لجريمة الإرهاب الالكتروني السبيراني،لا ينبغي إطلاقا إغفال جانب مهم جدا،وهو أن الإرهاب الحديث محصلة جهد وعمل طويل وتنظيم محكم يتغذى على روافد فكرية ونفسية وعقائدية عميقة ومادية،وعقول في قمة الذكاء والعبقرية،ويملك من الوسائل وترسانات الأسلحة ما تنوء به العصبة من الدول العظمة،ما جعل العالم بأسره يقف شبه عاجز عن مواجهته،وعليه فان جريمة الإرهاب الرقمي تكتسي أهمية بالغة بسبب ما قد ينجم عنه من مخاطر تعصف بالأفراد والحكومات وتهدد امن واستقرار المجتمعات وتماسكها.

أهمية الموضوع:

1- الأهمية النظرية:

تكمن الأهمية النظرية لدراسة ظاهرة الإرهاب الإلكتروني في كونه أحدث الجرائم و أشدها خطورة،وأحد أهم القضايا الحديثة في العالم،و التي أخذت قدرا كبيرا من الاهتمامات القانونية والسياسية لما يمتاز به من تطور و استعمال لتكنولوجيا الإعلام و الاتصال ،كما أن العالم بات يعيش في ثورة تكنولوجية متطورة لاسيما بعد أحداث 11 سبتمبر 2001 ما جعل من الإرهاب الإلكتروني عبارة عن قضية محورية تشكل خطرا محدقا بالجميع سواء الأفراد أو الحكومات،و بالتالي تظهر الأهمية العلمية لهذه الجريمة في محأولة توضيح مفهوم جريمة الإرهاب الإلكتروني و إطاره القانوني.

2- الأهمية العلمية:

إن الإرهاب الإلكتروني باعتباره خطر المستقبل يقتضي التعاون والتنسيق بين الدول لضبط هذه الجريمة لاسيما من الناحية القانونية و التعامل مع هذا الخطر بكل جدية

وصرامة بغية مواجهة هذا الإرهاب ، الذي يهدد الإنسانية جمعاء،كما ان الأهمية العملية لدراسة جريمة الإرهاب الرقمي تكمن في تبيان مدى تأثير استخدام التكنولوجيا المتطورة ومدى استفادة الإرهاب منها في تنفيذ مخططاته الغاشمة التي لن تستثني أي طرف في تشكيل الخطر عليه،وبالتالي ينبغي دراسة هذه الظاهرة على جميع المستويات سواء العالمية أو الإقليمية أو المحلية.

أهداف الدراسة:

نهدف من خلال دراستها لهذا الموضوع إلى تسليط الضوء على تحديد مفهوم شامل للإرهاب الإلكتروني وبيان أهم خصائصه و الأسباب المؤدية إليه،وتميزه عن غيره من الجرائم المشابهة له والمتداخلة معه،ومن ثم توضيح كيفيات استخدام الإرهاب للقوة التكنولوجية و أهم الأسلحة التي يعتمد عليها في تنفيذ مخططاته الإجرامية و أخطر الجرائم التي تم تنفيذها إلى حد الآن ،بالإضافة إلى تحديد الأركان العامة لهذه الجريمة من الناحية القانونية و الغاية التي يسعى الإرهاب السبيراني إلى تحقيقها و كذا التطرق إلى آليات مكافحة هذه الجريمة على كافة الأصعدة الوطنية و الإقليمية و حتى العالمية.

أسباب اختيار الموضوع :

1- الأسباب الشخصية :

الميول الذاتي منذ صغر السن إلى الاهتمام بالقضايا المعاصرة لاسيما تلك التي تعصف بالأرواح،وتهدد امن واستقرار الشعوب،وكذا الاهتمام بجريمة الإرهاب كأحد اخطر الجرائم التي عرفتها البشرية وأكثرها بشاعة وعنفا،ناهيك عن الاستمتاع بدراسة القدرات الخارقة والذكاء الحاد الذي يمتاز به المخترق الإرهابي،أو المجرم الذكي من خلال دراسة آليات وضعه للخطط وكيفيات شن هجماته وتنفيذها باحترافية مطلقة.

2- الأسباب الموضوعية :

إن جريمة الإرهاب السيبراني من الجرائم الحديثة التي يجب بذل الجهد في دراستها لما له من أبعاد ومخاطر عميقة ومساس بكافة القطاعات خاصة الحيوية منها فضلا عن كونه محل اهتمام الرأي العام العالمي والمحلي لاسيما بسبب عدم وجود إطار قانوني لضبطه،وانطوائه على خطورة مستقبلية كبيرة تقتضي العلاج والوقاية الفعالة قبل وقوع الكارثة وتدمير البشرية.

إشكالية الدراسة:

نظرا للأهمية البالغة لهذا الموضوع وتفرع المصطلحات التي تنطوي عليها جريمة الإرهاب الإلكتروني جاء موضوع دراستنا الموسومة بعنوان "الإرهاب الالكتروني" الذي أردنا من خلاله الوقوف على أهم جوانبه و إبراز خطورته و محأولة فهم البيان القانوني له و سبل مكافحته و عليه جاءت صياغة إشكالية الموضوع على النحو الثاني:

ما المقصود بالإرهاب الالكتروني؟ وما هي آليات مكافحته؟

- منهج الدراسة :

- المنهج الوصفي التحليلي: لقد ساعدنا هذا المنهج في فهم الآراء ودراسة المعطيات والخروج بالنتائج من خلال تدقيق الأفكار وتحليلها.

- المنهج الإحصائي: برغم من أن الاعتماد عليه من خلال بحثنا هذا كان شبه نادر،إلا انه سأهم في إعطاء بعض الإحصائيات التي مكنتنا من تعميق الفهم.

- منهج دراسة الحالة: أين أعطى هذا المنهج إمكانية في جمع بعض البيانات القانونية للدول والمنظمات العالمية وكذا الإقليمية.

- تقسيمات الموضوع:

مقدمة:

الفصل الأول: الإطار المفاهيمي لجريمة الإرهاب الالكتروني.

المبحث الأول: مفهوم الإرهاب الالكتروني.

المطلب الأول: تعريف الإرهاب الالكتروني.

الفرع الأول: تعريف الإرهاب .

الفرع الثاني: تعريف الإرهاب الالكتروني .

الفرع الثالث: تمييز جريمة الإرهاب الالكتروني عن غيرها من الجرائم .

المطلب الثاني: خصائص وأسباب الإرهاب الالكتروني والآثار الناجمة عنه.

الفرع الأول: أسباب الإرهاب الالكتروني.

الفرع الثاني: خصائص الإرهاب الالكتروني

المبحث الثاني: آليات استخدام القوة الالكترونية في الجرائم الإرهاب.

المطلب الأول: أركان جريمة الإرهاب الالكتروني والأسلحة المستخدمة فيه.

الفرع الأول: أركان جريمة لإرهاب الالكتروني.

الفرع الثاني: أسلحة الإرهاب الالكتروني.

المطلب الثاني: كيفيات توظيف الإرهاب للقوة التكنولوجية والجرائم الناجمة عنها.

الفرع الأول:التكنولوجيا المتطورة واستخداماتها في العمل الإرهابي.

الفرع الثاني: أشهر جرائم الإرهاب الالكتروني .

الفصل الثاني: آليات مكافحة جريمة الإرهاب الالكتروني.

الفصل الأول: الإطار المفاهيمي لجريمة الإرهاب الإلكتروني.

إن التطور الهائل الذي بات يشهده العالم لاسيما في مجال تكنولوجيا الإعلام والاتصال قد أدى بدوره إلى تطور وسائل الإجرام وتسارع وتيرة التهديدات وتنوع أنماط النشاط الهجومي الموجه ضد شبكة الانترنت والأنظمة المتصلة بها، ومع مطلع موجة الانتشار الرهيب التكنولوجي في شتى بقاع العالم قد أخذ إلى الاستغلال السلبي لمعطيات التكنولوجيا، مما أسهم في ظهور أنواع جديدة وطفرات مستحدثة للجرائم كالجريمة الإلكترونية والحروب الرقمية ولعل أبرز هذه الجرائم هي جريمة الإرهاب الإلكتروني التي تعتبر أخطر الجرائم التي باتت تهدد الأمن الداخلي والسلم الدولي. وسنتطرق من خلال هذا الفصل إلى الإحاطة بالإطار المفاهيمي لجريمة الإرهاب الإلكتروني وأركانها وأهم خصائصها وكذا أسبابها وكيفيات استخدام التكنولوجيا في الأعمال الإرهابية وكذا الآثار الناجمة عنها. عبر المبحثين التاليين:

المبحث الأول: مفهوم الإرهاب الإلكتروني:

يحضى الإرهاب الإلكتروني بمفهوم واسع وعميق جراء صعوبة ضبط المصطلحات التي تنصب في سياقه، وتداخل مفاهيمه مع الكثير من الجرائم المشابهة له، فالتطرق لمفهومه يقتضي منا دراسة كل من تعريف الإرهاب التقليدي عموما ومن ثم، التطرق إلى تعريف الإرهاب الإلكتروني وبيان أهم الجرائم التي ينبغي تمييزه عنها، وذلك عبر المطالب التالية:

المطلب الأول: تعريف الإرهاب الإلكتروني:

نستعرض فيما يلي كل من التعريف اللغوي والاصطلاحي لجريمة الإرهاب:

الفرع الأول: تعريف الإرهاب:

❖ **أولا: الإرهاب لغة:** كلمة إرهاب مشتقة من الفعل المزيد أرهب ويقال أرهب فلان بمعنى أخافه وأفزعه[1]، وعرفت المعاجم العربية القديمة الفعل رهب، ويرهب، ورهبة، رهبانا، فيقال: فلان راهب منه الله بمعنى خائف من عقابه[2]، هذا وقد استعمل صيغ الإرهاب في القرآن الكريم في عدة مواضيع وبعدة معاني مختلفة منها قوله تعإلى:« **فَلَمَّا أَلْقَوْا سَحَرُوا أَعْيُنَ النَّاسِ وَاسْتَرْهَبُوهُمْ وَجَاءُوا بِسِحْرٍ عَظِيمٍ** » جاءت بمعنى الخوف والهلع. سورة الأعراب الآية 116، كما وردت في قوله تعإلى « **وَٱضْمُمْ إِلَيْكَ جَنَاحَكَ مِنَ ٱلرَّهْبِ** » سورة القص، الآية 32، والتي وردت بمعنى الخشية.

كما جاء في سورة الحديد الآية 27 **وَجَعَلْنَا فِي قُلُوبِ الَّذِينَ اتَّبَعُوهُ رَأْفَةً وَرَحْمَةً وَرَهْبَانِيَّةً ابْتَدَعُوهَا** ».

وقوله تعإلى« **وَأَعِدُّواْ لَهُم مَّا ٱسْتَطَعْتُم مِّن قُوَّةٍۖ وَمِن رِّبَاطِ ٱلْخَيْلِ تُرْهِبُونَ بِهِۦ عَدُوَّ ٱللَّهِ وَعَدُوَّكُمْ**. سورة الأنفال الآية 60 بمعنى القوة والبأس الشديد والتخويف وإفزاع العدو.

وقوله « **لَأَنتُمْ أَشَدُّ رَهْبَةً فِي صُدُورِهِم** ». سورة الحشر الآية 13. وردت بمعنى التخويف للكافرين .

وقوله تعإلى:« **وَلَا تَشْتَرُوا بِآيَاتِي ثَمَنًا قَلِيلًا وَإِيَّايَ فَاتَّقُونِ** ». سورة البقرة الآية 40. وردت بمعنى الخشية من الله تعإلى، والإرهاب في معجم الوسيط تعني وهن يطلق على الذين يسلكون بسيل العنف والإرهاب لتحقيق أهدافهم السياسية، والإرهابي في المنجد تعني من يلجأ إلى الإرهاب لإقامة سلطة. الإرهاب في الرائد تعني"رعب تحدثه أعمال عنف كالقتل وإلقاء القنابل والمتفجرات والتخريب"، وبالإضافة إلى المعاجم اللغوية معاجم متخصصة التي تحدثت عن الإرهاب، أما الحكم الإرهابي فهو"نوع من الحكم الاستبدادي يقوم على سياسة

[1] – خليل عبد الله حسين"الإرهاب الإلكتروني– المفهوم والمخاطر"، ورقة مقدمة لمؤتمر الإرهاب الإلكتروني، معهد التنمية الإدارية، مصر، 2016 .

[2] – نجلاء عبد الفتاح طه "دور الإعلام في حل القضايا المعاصرة –الإرهاب، جرائم الانترنت، قضايا العولمة"، دار التعليم الجامعي، مصر، 2015، ص، ص، 7و8 .

التعامل مع الشعب بالشدة والعنف بغية القضاء على النزاعات والحركات التحريرية والاستقلالية[1] .

❖ **ثانيا: التعريف الاصطلاحي للإرهاب:**

إن مسألة تحديد تعريف جامع وعام للإرهاب أثارت جدلا سياسيا وفقهيا وقانونيا واسعا على مر العصور، لاسيما بخصوص ما يتعارض مع مصالح بعض الدول وتهديد استقرارها فاختلفت التعريفات وتباينت، فعرفت الموسوعة السياسية الإرهاب على أنه" استخدام العنف غير القانوني أو التهديد بأشكال مختلفة كالاغتيال والتشريد والتعذيب والتخريب والنسق بغية تحقيق هدف سياسي معين مثل كسر روح المقأومة والالتزام عند الأفراد وهدم المعنويات والمؤسسات كوسيلة من وسائل الحصول على المعلومات والأموال، وبشكل عام هو استخدام العنف لاسيما لإخضاع طرف منأوئ لمشيئة الجهة الإرهابية[2] .

هذا وقد تطرقت اتفاقية جونيف 1937 لجريمة" الإرهابية باعتبارها نوعا واحدا وهو الإرهاب الفردي الموجه ضد أمن الدولة وحددت جرائم معينة تعتبرها ضمن الجرائم الإرهابية، وعرفت الإرهاب بأنه" الأعمال الإجرامية الموجهة ضد الدولة والتي يكون من شأنها إثارة الفزع والرعب بين الأفراد"[3] .

كما تطرقت الاتفاقية العربية لمكافحة الإرهاب إلى تعريفه ضمن الفقرة الثانية من المادة الأولى بقولها" هو كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي .

ويهدف إلى إلقاء الرعب بين الناس وتعريض حريتهم و امنهم للخطر أو إلحاق الضرر بالبيئة أو بإحدى المرافق أو الأملاك العامة أو الخاصة واحتلالها، أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر[4] .

أما عن الاتفاقيات الدولية فعرفه مجلس الأمن الدولي بأنه "كل عمل جرمي ضد المدنيين بقصد التسبب في الوفاة أو الجروح البليغة أو أخذ الرهائن من أجل إثارة الرعب بين

---

[1] – عبد العزيز صقر الغامدي" الإرهاب والعولمة"، أكاديمية ثابت للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، 2002، ص ص 15،16 .

[2]– عبد الوهاب الكيالي" الموسوعة السياسية"، المؤسسة العربية للدراسات والنشر، الجزء 7، بيروت، 1954، ص 153 .

[3] – وفاء لطفي حسين عبد الواحد" الإرهاب الإلكتروني والأمن القومي في ظل جائحة كوفيد 19، ص 444 .

[4] – المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب، عام 1998 .

الناس أو موجهة إلى حكومة أو منظمة دولية لحملها على القيام بعمل ما أو الامتناع عنه، وكل الأعمال الأخرى التي تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالإرهاب والتي لا يمكن تبريرها بأي اعتبار سياسي أو فلسفي أو إيديولوجي أوعرقي أو ديني[1] .

هذا وقد تناول المشرع الجزائري مسألة الإرهاب ضمن المرسوم التشريعي 92-03 المؤرخ في 1992. بقوله "هو أية مخالفة تستهدف أمن الدولة ووحدة الإقليم، واستقرار المؤسسات وسيرها العادي بواسطة عمل هدفه زرع الخوف في وسط السكان وخلق حالة انعدام الأمن والمساس بالأشخاص والممتلكات، وقد أورد المشرع كلمتي الفعل والعمل كتعبير عن السلوك الإجرامي، هذا وقد نصت المادة 87 مكرر من قانون العقوبات والأمر 95-11 المؤرخ في 1995 أنه يعد فعلا إرهابيا أو تخريبيا في مفهوم هذا الأمر، كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يلي:

- بث الرعب في الأوساط وخلق حالة انعدام الأمن من خلال الاعتداء المعنوي والجسدي على الأشخاص أو تعريض حياتهم وأمنهم للخطر أو المساس بممتلكاتهم .
- عرقلة حركة المرور أو حركة النقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية .
- الاعتداء على رموز الأمن والجمهورية ونبشن أو تدنيس القبور.
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة[2] .

الفرع الثاني: تعريف الإرهاب الإلكتروني:

إن الإرهاب الالكتروني أو السيبراني أو الإفتراضي لا يزال إلى حد الساعة يخلو من تعريف موحد ودقيق ويرى البعض أن ذلك يرجع إلى تحولات بنيوية مست المجال العالمي تنحصر في عاملين الأول يتمثل في انهيار النظام الاشتراكي الأمر الذي أدى إلى ظهور أنواع جديدة من المخاطر ترتبط بتهديدات الأمن السيبراني كالحرب الرقمية والإرهاب المعلوماتي .

[1] – قرار مجلس الأمن الدولي، العدد 1566، عام 2004 .

[2] – رافعي ربيع" الإرهاب وعلاقة بالجريمة المنظمة– والإرهاب الالكتروني نموذجا"، مجلة القانون والعلوم السياسية، العدد 01، الجلد 07، 2021.

أما العامل الثاني فيتصل بالانترنت في حد ذاتها التي تجعل من إرهابي الغد قد يلحق أكبر ضرر من خلال لوحة مفاتيح فقط، وقد كان أول ظهور لمصطلح الإرهاب الالكتروني على يد باري كولين الذي عرفه بأنه "هو هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية، وإن الهجمة يجب أن تكون ذات أثر تخريبي مكافئ للأفعال المادية للإرهاب"[1].

كما عرفه جيمس لويس بأنه "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنية التحتية الوطنية المهمة كالطاقة والنقل والعمليات الحكومية أو بهدف ترهيب حكومة ما أو مدنيين"[2].

وعرفت دورشي دينينغ الإرهاب الالكتروني على انه "الهجوم القائم على مهاجمة الحاسوب، وانه التهديد به و يهدف إلى الترويع وإجبار الحكومات أو المجتمعات على تحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمرا وتخريبيا، لتوليد الخوف بحيث يكون مشابها للأفعال المادية للإرهاب"[3] .

وتجدر الإشارة أن وزارة الدفاع الأمريكية هي الأخرى عمدت إلى وضع تعريف للإرهاب الالكتروني فعرفته على أنه "استخدام أجهزة الكمبيوتر والانترنت لإجراء حرب ضمن الفضاء الالكتروني"[4]، هذا وعرفته الاتفاقية الأولى لمكافحة الإجرام عبر الانترنت في بوتسدام 2021 على أنه "هجمات غير مشروعة أو تهديدات لهجمات ضد الحواسيب أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الانتقام والابتزاز والإجبار أو التأثير على الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة، وبالتالي ينعت الشخص بأنه إرهابي على الانترنت وليس فقط مخترقا، فلا

[1] – وفاء لطفي "الجهود الدولية" في مكافحة الإرهاب السيراني– التجربة الماليزية"، مجلة كلية الاقتصاد والعلوم السياسية، العدد 01، المجلد 23، جانفي 2022، ص 159.

[2] – جمال بوزايدية 'الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية'التحديات والآفاق المستقبلية '.مجلة العلوم القانونية والسياسية' العدد1,المجلد 10'ص 1270'

[3] – . الكر محمد,بن مرزوق عنتره .البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب مجلة العلوم الإنسانية والاجتماعية'العدد 38'2018'ص32,

[4] – غريب حكيم، شرقي صبرينة "تداعيات الحرب الالكترونية على العلاقات الدولية – الدراسة في الهجود الإلكتروني على إيران (فيروس ستكسنس)، ص 95 .

بد أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات أو على الأقل تحدث أذى كافيا من اجل نشر الخوف والرعب"[1] .

وعلى ضوء ذلك ورد تعريف الإرهاب الالكتروني ضمن الموسوعة الالكترونية بأنه" استخدام التقنيات الرقمية لإخافة وإخضاع الآخر أو القيام بمهاجمة نضم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية"[2] أما على المستوى الأمني فقد تطرقت وكالة الاستخبارات الأمريكية إلى تعريف الإرهاب الالكتروني بأنه" هجوم تحضيري ذو دوافع سياسية موجه ضد نضم معلومات الكومبيوتر وبرامجه والبيانات والمعلومات والتي تنتج من عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين". كما عرفه مركز الحماية البنية التحتية القومية الأمريكية بأنه"عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر وبرامجه، والاتصالات السلكية واللاسلكية ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف تأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو ايديولوجية[3] .

هذا و يعتبر تعريف الصليب الأحمر للإرهاب الالكتروني أكثر دقة ووضوح فعرفه على أنه"عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف لتحقيق أغراض منها اختراق النظام المعلوماتي أو جمع ونقل وتشفير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق، واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي كالصناعات والبنية التحتية" .

وتجدر الإشارة إلى أن التعريف الذي جاء به مجمع الفقه الإسلامي الذي صنف من أفضل التعاريف وأشهرها وأكثرها إلماما وشمولية وتحديدا للسلوك الإرهابي الرقمي فعرفه بأنه "العدوان الذي يمارسه أفراد أو جماعات دول بغيا على الإنسان دينه، عقله، ماله، عرضه، ويشمل أصناف التخويف والأذى والتهديد وقطع الطريق وكل فعل من أفعال العنف أو التهديد يقع تنفيذا لمشروع إجرامي فردي أو جماعي يهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم أو أحوالهم للخطر، ومن صنفه

[1] – سعيد عبيدي "الإرهاب الإلكتروني"، مجلة العلوم الإنسانية، العدد 02، تندوف، 2017، ص 35 .

[2] – رافعي ربيع "الإرهاب الدولي وعلاقته بالجريمة المنظمة"، المرجع السابق، ص 73 .

[3] – سامر مؤيد، عبد اللطيف نوري– رشيد الشافعي "دور المنظمات الدولية في مكافحة الإرهاب الرقمي، بحث مقدم بجامعة كربلاء، 2016، ص 3 و4 .

إلحاق الضرر بالبيئة والمرافق العامة والأملاك الخاصة أو الموارد الطبيعية فكل هذا من صور الفساد في الأرض التي نهى الله عنها" .

يتضح من التعاريف المتنوعة سالفة الذكر أنه بالرغم من اختلاف المعايير والمفاهيم إلا أنها تتصب جميعا ضمن مفهوم واحد مفاده أن الإرهاب الإلكتروني ما هو إلا جريمة إرهابية مقترنة بوسائل غاية في الحداثة والتطور تستعمل خصيصا لإخافة وإخضاع الآخرين وإلحاق الضرر والأذى والتهديد المادي والمعنوي وزعزعة الأمن المحلي والسلم العالمي، عبر الانتقال من المسار الإرهابي التقليدي إلى الإرهاب الحديث[1].

الفرع الثالث: تمييز جريمة الإرهاب الإلكتروني عن غيرها من الجرائم .

هناك الكثير من الجرائم التي تتداخل مع جريمة الإرهاب الإلكتروني والتي يصعب على الشخص العادي التفريق بينها وسنتناول ضمن هذا الفرع أهم الجرائم التي تتشابه مع جريمة الإرهاب الإلكتروني .

أولا: تمييز جريمة الإرهاب التقليدي عن جريمة الإرهاب الالكتروني:

1- أوجه التشابه: يتداخل الإرهاب الالكتروني ويجتمع مع الإرهاب التقليدي في مجموعة من العناصر من بينها أن كلأهما يعتبر من الأعمال غير المشروعة التي جرمتها الاتفاقيات الدولية بالإضافة إلى أن كل من هذين الجريمتين يتم ارتكابهما بغرض المساس بالنظام[2] العام وتعريض سلامة المجتمع للخطر ويقومان وراء دوافع دينية وسياسية[3] .

كما تتفقان من حيث الغاية التي يسعيان إلى تحقيقها والمتمثلة أساسا في نشر الهلع والذعر والخوف في نفوس الآخرين[4] وابتزاز الدول ومحأولة السيطرة على نظامها الداخلي والانتقام من المعارضين لأفكارهم، وتمويل أنشطتهم الإرهابية من خلال الاستيلاء على ممتلكات الناس ومحأولتهم تجنيد أعضاء جدد والانخراط إلى صفوف الجماعات

[1] – بن يحي الطاهر ناعوس "مكافحة الإرهاب الإلكتروني ضرورة بشرية وفريضة شرعية"، ص 04 .

[2] – سامر مؤيد عبد اللطيف، مرجع نفسه، ص 07 .

[3] – مايا حسين ملا خاطر "الإطار القانوني لجريمة الإرهاب"، مجلة جامعة النصر، العراق، 2016، ص 137 .

[4] – بن صويلح أمال "الهيئة الوطنية للوقاية من الجرائم المنفصلة بتكنولوجيا الإعلام، الملتقى الدولي حول الإجرام السبيراني– المفاهيم والتحديات–خطوة عامة نحو مكافحة الإرهاب الالكتروني، جامعة 8 ماي، 2017، ص 03 .

الإرهابية[1] **أما أوجه الاختلاف:** فتكمن أساسا في الوسائل التي تتخذ لارتكاب الأفعال الإرهابية، فالإرهاب التقليدي يعتمد على الوسائل المادية القديمة التقليدية في تنفيذ الهجمات الإرهابية من خلال استعمال الأسلحة التي تترك أثارا على أرض الواقع كاستعمال الأسلحة الفتاكة اليدوية والمتفجرات والقنابل واختطاف الطائرات المدنية وتغيير مسارها إلى أماكن تواجدهم لتحقيق أغراضهم الإرهابية[2]. أما الإرهاب الرقمي فيعتمد على وسائل ناعمة لا تحدث أضرار مادية واضحة كونه مرتبط بالانترنت الذي يقع ضمن بيئة افتراضية من اختراق المواقع الالكترونية وتدميرها عن طريق نشر الفيروسات وبرامج التجسس على الدول وتخريب البيانات ومحوها، وهو الاختلاف الجوهري والأساسي بين هذين النوعين من الجرائم[3].

كما أن الإرهاب التقليدي يسهل كشف آثاره من طرف أجهزة الأمن على خلاف الإرهاب الذي يحتاج إلى خبرة عالية وفنية[4]، وتجدر الإشارة أيضا أن الإرهاب الالكتروني لا يحتاج إلى الانتقال إلى مسرح الهجوم لتنفيذ مخططه على عكس الإرهابي العادي الذي يفدي بحياته في أغلب الأحيان في سبيل تحقيق أهدافه[5].

كما أن الإرهابي التقليدي يلجأ إلى العنف واستعمال القوة بينما يكتفي الإرهابي الالكتروني بوسائل ثابتة تبدو في الظاهر أنها مسالمة على الرغم من أن خطورتها قد تكون اشد من خطورة الإرهاب التقليدي[6] .

---

[1] – سامر مؤيد عبد اللطيف نوري رشيد الشافعي" دور المنظمات الدولية في مكافحة الإرهاب الرقمي"، مرجع سابق، ص 07 .

[2] – منير محمد الجنيبي، ممدوح محمد الجنبي "جرائم الانترنت والحاسوب الآلي ووسائل مكافحتها"، دار الفكر الجامعي، الإسكندرية، 2005، ص 110 .

[3] – جعفر حسن جاسم الطائي" جرائم تكنولوجيا المعلومات جديد للجريمة الحديثة"، الطبعة 01، دار البداية، عمان، 2007، ص 494 ..

[4] – علي جاسم محمد التميمي "الإرهاب الالكتروني وأثره على المجتمع"، المجلة السياسية، جامعة المشتهرية، العراق، ص 491 .

[5] – جعفر حسن جاسم الطائي" جرائم تكنولوجيا المعلومات جديد للجريمة الحديثة"، المرجع نفسه.

[6] – إسراء طارق جواد كاظم "جريمة الإرهاب الالكتروني – دراسة مقارنة"، رسالة من متطلبات نيل شهادة الماجستير في القانون العام"، كلية الحقوق، جامعة النهرين، العراق، 2012، ص 63 .

ثانيا: تمييز جريمة الإرهاب الإلكتروني عن جريمة المافيا المعلوماتية:

نلاحظ في الأونة الأخيرة زيادة كبيرة في عدد الجرائم التي ترتكبها الجماعات الإجرامية المنظمة، حيث اتسع النطاق الإقليمي لهذه الجرائم، فلم تعد تقتصر على تنفيذ جرائمها داخل حدود الدولة الواحدة، وإنما تعدى ذلك ليشمل دولا عديدة .

كما أن أنشطة وممارسة هذه الجماعات هي الأخرى توسعت بحيث لم تعد مقتصرة على الترهيب والاتجار بالمخدرات بل أصبحت عملياتها أكثر خطورة، ولعل هذه الجماعات قد تمكنت من امتلاك الأسلحة النووية أو الذرية أو البيولوجيا أو الكيميائية والمتاجرة بها فالمافيا المعلوماتية هي "مجموعة الأشخاص التي تستخدم تقنية المعلومات والشبكات بطرق غير مشروعة للحصول على المكاسب المادية، ويتسم عملها بطابع التنظيم والتخطيط والسرية والاستمرارية، وفي سياق مقارنة جريمة الإرهاب وجريمة المافيا المعلوماتية فلا بد من ذكر الفوارق بين الجريمتين وأوجه التداخل ومما لا شك فيه أن الجرائم جميعا بما فيها الإرهاب الالكتروني والمافيا المعلوماتية تشكل اعتداء على مصالح يحميها القانون، لاسيما أن تلك الجرائم وجد بها سمات مشتركة **أوجه الاختلاف** كلأهما يستخدم أسلوب التهديد والترهيب وبث الرعب والفزع في صفوف الناس، كما تشابهت من حيث كيفية التخطيط والتنظيم فضلا عن التنسيق والتعاون الدولي الذي قد يحدث بين منظمات الإرهاب المعلوماتي ومنظمات المافيا المعلوماتية في حال التقائهم لتبادل المعلومات وتحقيق أهداف مشتركة .

- بالإضافة أن كلأهما يتعدى حدود الدولة الواحدة فتصبح عبارة عن جرائم ذات أبعاد دولية.

2- أوجه الاختلاف:

بالرغم أن كلا الجريمتين تشتركان في الكثير من العوامل إلا أنه هناك مجموعة من الفوارق التي تمكننا من الفصل بينهما فجريمة الإرهاب الالكتروني يمكن لشخص واحد ارتكابها بينما يستحيل ذلك بالنسبة لجريمة المافيا المعلوماتية لأنها تتطلب وجود عدد كبير من الأشخاص يتزعمهم واحد منهم يأتمرون بأمره وينتهون بنهيه، كما أن الهدف الذي يسعى إليه الإرهاب الالكتروني عادة ما يكون سياسيا على خلاف جرائم المافيا المعلوماتية التي يكون غرضها الربح غير المشروع .

كما أن المافيا المعلوماتية تسعى لترهيب الأفراد وهي بصدد الحصول على أموالهم ومنهم من يبلغ السلطات الحكومية إلا أن الإرهاب الالكتروني موجه إلى كل من الأفراد والدولة لإظهار هذه الأخيرة بمظهر الكيان الهزيل لأضعاف ثقة المواطن بدولته[1] .

ثالثا: تمييز جريمة الإرهاب الالكتروني عن الجريمة الالكترونية:

تستأثر الجريمة الالكترونية بالقدرة الفائقة، والقدرات الخارقة لمرتكبيها والقادرة علة إلحاق خسائر فادحة كونها تتمحور حول عدة أشكال منها التجسس الالكتروني والقرصنة والجرائم المنظمة والمواقع التحريضية، وذلك بسبب ما تواجهه جهات التحقيق المختصة من صعوبة في ضبط الجاني أو إلقاء القبض عليه، لأن معظم هذه الجرائم تتم بصورة مستترة خفية مع غياب أي دليل مرئي، فظاهرة الجريمة الالكترونية تحولت من مجرد تحريف للمعطيات إلى غش معلوماتي ومن ثم إلى جريمة الكترونية منظمة وصولا إلى الإرهاب الالكتروني السبيراني في وقتنا الراهن، حيث يصعب على الكثير التمييز بين الاستغلال السلبي للفضاءات الرقمية وبين الاستخدامات ذات الطابع الإجرامي وبين استخدامها كسلاح إرهابي فتاك، وعليه فإن العديد من الأنماط يمكن تصنيفها ضمن خانة الإرهاب الرقمي إذا ما وجهت نحو هدف معين وأغراض سياسية أو عسكرية، وعليه يمكن القول أن الجريمة الالكترونية مع مرور الزمن تمخضت على ظهور أبشع وأخطر الجرائم التي جاءت في صورة الإرهاب سبيراني الذي يعكس مدى بشاعة التفكير المتطرف ما يعكس الترابط الشديد بينهما، الأمر الذي يميز الإرهاب الرقمي عن الكثير من الجرائم الذي تستخدم التقنيات المتطورة المعلوماتية، لما ينطوي عليه من إرعاب ورهبة للحكومات والأشخاص، فهو جريمة تتسم بالسرعة والتطوير في أساليبها ما يعكس طابعها الاستمراري على خلاف الجريمة الالكترونية وبالتالي تعتبر أقل عنفا إذا ما قارناها بالإرهاب الالكتروني، غير أن العامل المشترك بين هذين الجريمتين ينجلي بصورة أوضح في صعوبة إيجاد الدليل المادي الملموس الذي يثبت أنها حدثت بالفعل، فضلا عن سهولة إتلاف وتدمير هذه البيانات[2] .

---

[1] – عبد الرحمان عوض رجا ملاحة، فتيحة عمارة "جريمة الإرهاب المعلوماتي أسبابه وأساليبه"، مجلة جامعة الأمير عبد القادر، العدد 01، مجلد 34، 2020، ص 1330– 1331 .

[2] – جدي وفاء " الإرهاب الالكتروني أسبابه بين النص والتطبيق"، مجلة مقاربات، العدد 05، المجلد 03، أكتوبر 2015، ص، ص 36 ، 37.

المطلب الثاني: خصائص وأسباب الإرهاب الالكتروني:

إن الإرهاب الالكتروني بوصفة جريمة جديدة ومستحدثة يعكس تميزه بجملة من الخصائص وظهور عدة دوافع أدت بدورها إلى تفاقم انتشاره لاسيما في الأونة الأخيرة مما نجم عنه أضرار عظيمة يصعب وضع حد لها أو جبرها أو تلافيها، وسنتطرق في الفروع التالية إلى أهم الأسباب التي سأهمت في تطور انتشار الإرهاب الرقمي وابرز خصائصه

الفرع الأول: أسباب الإرهاب الالكتروني:

لقد سأهم التطور الراهن في مجال الانترنت ومعطيات العلم والتكنولوجيا في تهيئة البيئة الخصبة لامتداد جذور الإرهاب وتغلغلها في شتى بقاع الأرض وتنقسم هذه الدوافع إلى نوعين أسباب عامة وأسباب خاصة .

أولا: الأسباب العامة:

1- الدوافع الشخصية:

تتمثل الدوافع الشخصية المؤدية إلى الإرهاب في العديد من المظاهر كالرغبة في التطور وحب الشهرة أين يندفع الشخص إلى البحث عن عوامل باطلة كالتخريب والتدمير لصناعة شخصية عظيمة وصلبة في نظره، أو من منحى معاكس قد يدفعه إلى الانخراط في الجماعات الإرهابية الإحساس بالإحباط والفشل في تحقيق الرغبات والأهداف أو الوصول إلى الغايات المنشودة أو الشعور بالظلم وعدم الإنصاف والبطالة والاحتقار إلى أدنى أسس العيش الكريم الأمر الذي قد يسوق الشخص إلى الخوض متاهات الإرهاب والإجرام، فضلا عن نقمة هذا الأخير على المجتمع الذي يعيش فيه بسبب إصدار العدالة وضياع الحقوق وظهور الطبقية مما يسأهم في تربية الحقد الداخلي والأزمات النفسية فيسعى إلى القيام بأي عمل يضر المجتمع بدافع الانتقام، وخرب النظام العام، وسلب راحة المجتمع .

2- أسباب فكرية:

- الفراغ الفكري والجهل بتعاليم الحديث الإسلامي الحنيف وآدابه ومبادئه .
- الفهم الفاطن للدين وأحكامه وسوء تفسيره واعتماد الشباب على بعضهم البعض في الرجوع إلى العلماء حيث يقول ابن مسعود "لا يزال الناس بخير إذا أخذ والعلم عنه أكابرهم وعن علمائهم وأمنائهم، فإذا أخذوه عن صفارهم وشرارهم هلكوا" .

– الجعل بمقاصد الشريعة الإسلامية المتمثلة أساسا في حفظ الدين والعقل والمال والنفس، وتحريف وتأويل المعاني بالشك .

– التشدد والغلو والتطرف، الذي حذر الإسلام منه حتى لو كان بلباس الدين ويقول النبي صلى الله عليه وسلم: «هلك المتنطعون» .

– الانقسامات الفكرية المتباينة بين التيارات والأحزاب واختلاف المذاهب[1] .

3– الأسباب السياسية:

هي مجموعة التصرفات التي تتخذها دولة معينة مع شعبها أبرزها التهميش دور المواطنين في اتخاذ القرارات المصيرية وعدم فتح المجال للحوار بين الشعب والسلطة وظهور الدكتاتورية وانعدام العدالة ولاسيما في الدول العربية، وانتهاك حرية التعبير وقهر النظام وانعدام معنى الديمقراطية واضطهاد شعوبها، مما يولد التيارات المعادية للنظام من أجل العمل على الانتقام من خلال العمل الإرهابي إلى جانب احتكار الأملاك العمومية وجعلها في يد البرجوازية .

4– الأسباب الاقتصادية:

انتشار الفقر والبطالة وغلاء المعيشة وقلة الإنتاج والتصدير للدول الأجنبية ما أدى إلى ظهور عجز في الميزان التجاري، والجهل بكيفية استغلال المواد الاقتصادية الوطنية .

5– الأسباب الاجتماعية:

تتمثل عموما في التفكك العائلي وكثرة الطلاق وموت الأهل ما ينتج عنه انحراف الأبناء وغياب الرقابة وتصحيح المسار ووقوعهم في مصيدة الإرهاب، بالإضافة إلى غياب دور الإعلام في توعية المجتمع وتحسيس الأفراد بمخاطر الإرهاب[2] .

ثانيا: الأسباب الخاصة:

إن من بين الأسباب التي سأهمت بشكل مباشر في مساعدة المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أغراضهم غير المشروعة تتمثل فيما يلي:

---

[1] – محمودي قادة "مخاطر ومظاهر الإرهاب الالكتروني"، مجلة الدراسات الحقوقية، العدد التاسع، جامعة ابن خلدون، تيارت، ص، ص، 199 – 170 .

[2] – غلاف كريمة، جرلال زهرة "جريمة الإرهاب الالكترونية"، مذكرة لنيل شهادة ماستر اكاديمي في الحقوق ' جامعة الرحمان ميرة، بجاية، 2019، ص 19 .

1- ضعف بيئة الشبكات المعلوماتية وقابليتها للاحتراف:

إن الهشاشة التي تعتبر معظم البنية الأساسية للشبكة العالمية للمعلومات، تشكل ممرا تعمل المنظمات الإرهابية بشكل مستمر عليه من خلال استخدام وسائل المعلومات الالكترونية المتطورة، ومما شجعها على ذلك أن الشبكات الالكترونية مصممة في الأصل بشكل مفتوح، وتحتوي الأنظمة المعلوماتية على ثغرات معلوماتية التي يمكن للمنظمات الإرهابية استغلالها في التسلل إلى البنية المعلوماتية التحتية وممارسة العمليات التخريبية والإرهابية، حيث يستطيع محترف الحاسوب الدخول ووضع ما يريد على الشبكة وتقديم نفسه بالهوية التي يريدها[1].

2- عدم وضوح الهوية الرقمية للمستخدم:

إن هذا يعد من أهم أسباب الفنية التي أدت بشكل خاص إلى ظهور الإرهاب الالكتروني فالإرهابي الرقمي أو محترف الحاسوب بإمكانه صناعة شخصية وهمية والتخفي ورائها وشن هجمات الكترونية بعيدا عن مراقبة السلطات العامة والحيلولة دون التعرف عليه.

3- سهولة استخدام شبكة المعلومات وقلة التكلفة:

إن هذا السبب هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون الحاجة إلى مصادر تمويل كما هو الحال في الإرهاب التقليدي، فشن الهجوم الإرهابي الالكتروني لا يتطلب أكثر من جهاز حاسوب آلي متصل بشبكة انترنت ومزود بالبرامج اللازمة، فصعوبة الإثبات وقلة التكلفة تعتبر من أقوى الدوافع لارتكاب جرائم الإرهاب الالكتروني لما توفره للمجرم من إمكانيات وحرية في التنقل بين المواقع التي يستهدفها .

4- الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة:

إن غياب القوانين الخاصة بتنظيم مثل هكذا جرائم يجعل من الدولة ضعيفة في مجابهة الجرائم المتطورة نظرا لغياب الخبرة التقنية والإجراءات اللازمة والخاصة بالمحاكمة والعقاب، الأمر الذي أدى إلى إفلات المجرمين، وصعوبة إثبات هزيمة الإرهاب الالكتروني،[2] وحتى

[1] – جدي وفاء "الإرهاب الالكتروني وأسبابه بين النص والتطبيق"، المرجع السابق، ص 40 .

[2] – بن مرزوق عنتره "جريمة الالكتروني–الأسباب وآليات العلاج"، مجلة الحقوق والعلوم الإنسانية، العدد الثاني، المجلد 11، جامعة مسيلة، 2018، ص 513 .

الوقاية من دولة أو عدة دول بوضع تشريع خاص بهذه الجريمة فإن الإرهابي بإمكانه التنقل إلى بلد آخر والقيام بتنفيذ هجماته دون إمكانية كشفه أو معاقبته .

5- صعوبة اكتشاف واثبات جريمة الإرهاب الالكتروني:

مما يثير الانتباه في أغلب الجرائم المعلوماتية لا يعلم بوقوع الجريمة أصلا وخاصة في مجال جرائم الاختراق، وهذا ما يساعد الإرهابي السيبراني على الحركة بكل حرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، كما أن صعوبة الإثبات تعد من أقوى الدوافع التي تساعد على اختراق جريمة الإرهاب الالكتروني لأنها عادة ما تعطي المجرم أملا في الإفلات من المتابعة والعقاب[1] .

الفرع الثاني: خصائص الإرهاب الالكتروني.

يتحلى الإرهاب الالكتروني بجملة من الخصائص تجعل منه جريمة قائمة بذاتها ومختلفة عن غيرها من الجرائم تتجلى فيما يلي:

أولا: استعمال الأسلحة الناعمة:

حيث يستخدم الإرهابيون في جريمة الإرهاب الالكتروني السلاح التقني المتمثل في أجهزة الكومبيوتر المتصلة بشبكة الانترنت أو أي جهاز آخر متطور من أجل القيام بالعمليات الإرهابية، وتجدر الإشارة أن الجناة فيها مختفين وراء الشاشات ومنتشرين عبر كافة بقاع العالم، ويمارسون الحروب المعلوماتية النفسية، وهم بذلك لا يحتاجون إلى استعمال وسائل تقليدية كالأسلحة العنيفة. لأن البيئة الافتراضية قد عملة على نقل الصراع من ساحات الحروب الأرضية إلى عالم افتراضي، وهو ما جعل الأفراد الناجمة عنها أخطر بكثير من تلك الناجمة عن الإرهاب التقليدي[2] .

ثانيا: صعوبة إثبات واكتشاف الجريمة:

إن الجريمة الإرهابية التي تقوم على استعمال تكنولوجيا الإعلام والاتصال هي من أصعب الجرائم اكتشافا من طرف الأجهزة الأمنية نظرا لانعدام الخبرة وقلة التجربة لاسيما من حيث التحقيق، مما يخفي عليها نوع من الاستحالة في الإثبات وإقالة الدليل على

[1] – إسراء طارق جواد كاظم الجابري "جريمة الإرهاب الإلكتروني"، المرجع السابق .

[2] – محمد عبيد الكعبي "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت"، الطبعة الثانية، دار النهضة العربية، القاهرة، 2009، ص 96 .

مرتكبيها وفاعليها. فضلا عن إمكانية لجوء الجناة فيها إلى إتلاف القرائن والأدلة العلمية. ما ينجم عنه إفلات الإرهابي الرقمي من العقاب في أغلب الأحيان[1] .

ثالثا: جريمة عابرة للدول:

في أغلب الأحيان وبخلاف الإرهاب التقليدي نجد أنه في جريمة الإرهاب الإلكتروني يكون المجرم في بلد والواقعة الإجرامية في بلد آخر كونها متجأوزة للحدود وعابرة للقارات وغير خاضعة لنطاق إقليمي محدد، فبإمكان الإرهابي تنفيذ هجومه ضد الدولة وانتهاك خصوصيها والاستيلاء على مخططاتها وأموالها وبرتوكولات الأمن القومي الخاصة بها، دون أن تتمكن الدولة الضحية من معرفته أو تحديد مكان تواجده أو كشف المجرم واسترجاع بياناتها، أو إنزال العقاب عليه، فضلا عن أنه يمكن للدولة في حد ذاتها ممارسة الإرهاب الالكتروني[2] على شعبها بغية الضغط عليه وقمع حقوقه وحرياته لاسيما حرية التعبير .

المبحث الثاني: آليات استخدام القوة التكنولوجية في جرائم الإرهاب.

إن الإرهاب اليوم لم يعد يقتصر على الوسائل التقليدية في تنفيذ مخططاته الإجرامية بل عمل على استحداث أساليب جديدة في قمة التطور والحداثة تضمن تنفيذ وشن الهجمات باحترافية ودقة عالية،وسنتناول أهم هذه الأسلحة وكذا آليات استخدامها في تنفيذ مخططاتها الإرهابية،وذلك عبر المطالب التالية:

المطلب الأول: أركان جريمة الإرهاب الالكتروني والأسلحة المستعملة فيه:

إن الجريمة الإرهابية وعلى غرار باقي الجرائم تقوم على جملة من الأركان التي تخرج الفعل من دائرة الإباحة إلى نطاق التجريم وترسم له كيانه المادي والمعنوي الذي يفصله عن غيره من الجرائم.

---

[1] – لورنس سعيد حوامدة "الجرائم المعلوماتية، أركانها وآليات مكافحتها"، مجلة الميزان للدراسات الإسلامية والقانونية، العدد 03، جامعة العلوم الإسلامية العالمية– السعودية، 2017، ص 15 .

[2] – عبد القادر الشيخلي "طبيعة الإرهاب الالكتروني"، المؤتمر الإسلامي العالمي لمكافحة الإرهاب، رابطة العالم الإسلامي– السعودية، 2015، ص 07 .

الفرع الأول: أركان جريمة الإرهاب الالكتروني:

جريمة الإرهاب الالكتروني بوصفها فعل إجرامي لا بد أن تتوفر فيها بعض الشروط الأزمة لقيامها والتي يطلق عليها قانونا تسمية أركان الجريمة هذه الأركان تتكون من ثلاثة عناصر هي الركن المعنوي والركن الشرعي وكذا الركن المادي[1].

أولا: الركن الشرعي:

يتمثل الركن الشرعي في جريمة الإرهاب الالكتروني بوجود نص قانوني يجرم الفعل، فلا جريمة ولا عقوبة إلا بنص قانوني صادر عن الفعل الإرهابي يخرجه من دائرة الإباحة إلى أصفاد التجريم، وإعطائها وصف الجرائم الإرهابية السيبرانية في حالة تم ارتكابها بواسطة تكنولوجيا الإعلام والاتصال[2]. وقد جرم المشرع الأفعال الإرهابية بموجب المادة 87 مكرر إلى 87 مكرر.

وفي هذا الصدد أصدر المشرع الجزائري القانون 16-02 المتمم لأمر 66-156 المتضمن قانون العقوبات والذي جرم من خلاله أفعال الإرهاب في المادة 87 مكرر 11 والمادة 87 مكرر 12 في القسم الرابع مكرر من الفصل الأول في الكتاب الثالث تحت عنوان الجرائم الموصوفة بأفعال إرهابية تخريبية، وتجفيف منابع تمويل الإرهاب من خلال صدور قانون 05-01 المتعلق بالوقاية من جرائم تبييض الأموال وتمويل الإرهاب المعدل والمتمم من قانون 15-06 .

وفي نفس السياق وفي إطار مكافحة الجريمة ومنع انتشارها لاسيما تلك المتعلقة باستعمال وسائل الإعلام والاتصال،استحدث المشرع الجزائري القانون 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بالتكنولوجيات الحديثة وكرس غيره جملة من التدابير الوقائية لمنع الجريمة ومكافحة هذه الظاهرة، ومتابعتها بالإجراءات العامة الواردة في قانون الإجراءات الجزائية المستحدثة في مجال جمع الأدلة والكشف عن منابع الجريمة ومتابعتها، فضلا عن استحداث القانون 15-04 المتضمن تعديل قانون العقوبات والمتعلق أساسا، بالمساس بالأنظمة المعالجة الآلية للمعطيات في المادة 394 المكرر إلى غاية

[1] – ياسمين أحمد صالح "الإرهاب الالكتروني في ضل أزمة كورونا – الأنماط والتداعيات"، مجلة كلية السياسية والاقتصاد، العدد 09، 2021، ص 67 .

[2] – عبد الرحمان عوض رجاملاحة، فتيحة عمارة "جريمة الإرهاب المعلوماتي"،المرجع السابق ص1325 .

المادة 394 مكرر 7، ويلاحظ أن المشرع وإن كان لم ينص صراحة على جريمة الإرهاب الالكتروني إلا أنه من خلال القوانين سالفة الذكر يستشف أن المشرع قد لمح وقصد هذه الظاهرة ضمنيا [1].

ثانيا: الركن المادي:

إن الركن المادي في أي جريمة يقصد به مجموعة العناصر والأفعال التي تشكل في مجملها اعتداء على حقوق التي يصونها القانون، الأمر الذي يسمح بإهدار الأمن والاستقرار وضياع الحقوق ويتكون الركن المادي في الغالب من ثلاث عناصر تتمثل في سلوك الإجرامي نتيجته والعلاقة السببية بين الفعل والنتيجة، وبأخذ الركن المادي في جريمة الإرهاب الالكتروني لاسيما من حيث السلوك الإجرامي العديد من الصور وهي تتحقق بإمكانية إيقاع الفعل باستخدام تقنية أنظمة المعلومات وفي كل حالة يرتبط فيها النشاط موضوع الفعل بنطاق الالكتروني يعتمد عليه شريطة أن يتحقق فيما يلي:

- استخدام القدر الكافي من العنف والتهديد، ومفهوم العنف هنا مستحدث وذو طابع معنوي أكثر من ما هو مادي، بمعنى أن يظهر في مدى قدرة الجاني على استخدام تقنية أنظمة المعلومات بالقدر الكافي لإيقاع الضرر.
- أن يكون من شأن استخدام هذا العنف أو التهديد به إيقاع الرعب بين الناس أو تعريض حياتهم للخطر .
- أن يتبع هذا السلوك تنفيذ العمل الفردي أو الجماعي ومن أشكال السلوك الإجرامي المادي القادر على إظهار الإرهاب الالكتروني إلى حيز الوجود كالجرائم المستوجبة للعقاب واستخدام العنف أو التهديد بهدف تعريض المجتمع وأمنه للخطر والإخلال بالنظام العام وإلحاق الضرر بالبيئة أو المرافق العامة أو المساس بالموارد الوطنية وتعطيل أحكام الدستور والقوانين وفي هذه الحالات يكفي فقط احتمال الضرر .
- القيام بالعمليات المصرفية الالكترونية الداخلية أو الخارجية التي تتعلق بإيداع الأموال لدى البنوك من إحدى المؤسسات المالية والتي تكون محل شبهة في الصلة بالعمل الإرهابي .

[1] – المادة 87 مكرر، 87 مكرر 12 .من الأمر 66_156 المؤرخ في 8 يونيو 1966المتضمن قانون العقوبات المعدل والمتمم' الجريدة الرسمية' العدد49

– استخدام العنف أو التهديد لاستخدامه بهدف تعطيل الاتصالات أو أنظمة الحاسوب أو بهدف اختراق الشبكات التقنية وأنظمة المعلومة أو التشويش عليها[1] .

كما قد نص المشرع الجزائري على المستوى المحلي بموجب المادة 87 مكرر 11 من قانون العقوبات الفقرة الأولى على مجموعة من السلوكيات التي تدخل في إطار الإرهاب الالكتروني كتنظيم السفر باستخدام تكنولوجيا الإعلام والاتصال بقصد ارتكاب أعمال إرهابية وكذلك تمويل الإرهاب في صورة مباشرة أو غير مباشرة، وتجنيد الأشخاص لصالح الإرهاب أو تنظيم إرهابي باستخدام هذه الوسائل[2]،وكذا عرقلة سير المؤسسات والسلطات وبث الرعب في أوساط أفراد المجتمع [3].

أما النتيجة في جرائم الإرهاب الالكتروني فتتمثل في كل من المدلول المادي والقانوني ويقصد بالمدلول المادي للنتيجة ذلك الأثر الذي تحدثه في العالم الخارجي باعتبارها حقيقة مادية لها كيان، وتكون إما عبارة عن خسائر مادية أو بشرية أو عبارة عن خسائر معنوية كخلق أزمات نفسية وحالة الذعر والرعب والهلع في أوساط الأفراد أو الجماعات ومن ثم نقول أن السلوك الإجرامي الإرهابي هو الذي أدى إلى ظهور هذه النتيجة كأثر حتمي مباشر أما المدلول القانوني فيقصد به ما يسببه الجاني من مخاطر وأضرار تهدد أو تصيب مصلحة يحميها القانون، كالاعتداء على الأرواح والانتهاك حرمة الحياة الخاصة وتعريض المصالح والأمن للخطر ونشر حالة اللا استقرار، وعلى سبيل المثال تعتبر جريمة الإشادة بأفعال الإرهاب جريمة تكمن نتيجتها في حمل الناس على مساعدة وتشجيع الإرهاب والاعتراف به، وقد قسم الفقه الجرائم إلى جرائم خطر وجرائم ضرر،و مما لا شك فيه أن جريمة الإرهاب الالكتروني هي من جرائم الخطر[4].

[1] – شعبني صابرة " الإرهاب الالكتروني– الأشكال والدوافع"، مجلة العلوم الإنسانية والاجتماعية' العدد10ص ص444، 441 .

[2] – المادة 87 مكرر 11 ، المرجع السابق .

[3] – ياسمين أحمد صالح "الإرهاب في ظل أزمة كورونا– الأنظمة والتحديات"، ص 67، مرجع سابق .

[4] – ضيف مفيدة "سياسة المشرع في مواجهة ظاهرة الإرهاب"، مذكرة لنيل شهادة الماجستير في قانون العقوبات والعلوم الجنائية، جامعة الإخوة منتوري، قسنطينة، 2010، ص 50، 51 .

ويجب أن تحوز على القدر الكافي من الضرر الوخيم ونشر الرعب[1]، والنتيجة في الجريمة لا بد من تحققها فلا يمكن تصور الشروع في جرائم الإرهاب الالكتروني ما عاد في بعض الحالات الخاصة والنادرة، وتجدر الإشارة أن الشروع في الجنايات معاقب عليه بنفس عقوبة الجريمة التامة إذا اقترنت السلوكيات الإجرامية بنتيجة وكانت متوفرة على القصد الجنائي، بالإضافة إلى وجوب تحقق صلة وعلاقة ترابطية بين الفعل الإرهابي الالكتروني وبين النتيجة الجرمية المتحققة وبفعلها تقوم المسؤولية الجنائية للفاعل إذا ما اقترنت بإرادته الحرة بتنفيذها وإرادة تحقيق النتيجة منها أو على الأقل القبول بها، فالعلاقة السببية هي التي تسند النتيجة للفعل، وتبعا لذلك فإن انتفاء العلاقة السببية يؤدي إلى انتفاء مسؤولية الجاني ما لم ترتبط أفعاله بالقصد الجنائي فالرابط بين السلوك والنتيجة هو العلاقة بين السبب والمسبب أي بين العلة والمعلول فهي صلة تشرط بين ظاهرتين على نحو ضروري لازم بتعاقب زمني يفيد أن أحدهما كان سبب للآخر[2].

ثالثا: الركن المعنوي:

إن الجريمة الإرهابية الالكترونية لا تكفي بكونها جريمة مادية فقط وإنما هي عبارة عن كيان معنوي يشمل الأصول الإرادية لماديات الجريمة والسيطرة عليها، أي هو العامل الباطني الخفي، فلا محل للمساءلة الشخصية عن جريمة معينة ما لم تتجه إرادته الحرة الكاملة إلى ارتكابها وتحقيق النتيجة من خلال سلوكياته، فإذا ثبت أن الجاني لم يقصد تلك الأفعال أو فعلها بدون إرادة فإنه لا مجال لنسبة النتيجة إليه [3].

والجرائم الإرهابية عموما هي جرائم عمدية لا تقع قانونا إلا إذا توافر القصد الجنائي لدى مرتكبها والقصد الجنائي الواجب توفره هنا هو كل من القصد الجنائي العالم المتكون من عنصري العلم والإرادة وكذا القصد الجنائي الخاص بجريمة الإرهاب دون سواها، ويقصد بالعلم أن يعلم الجاني أن الفعل يقوم به يشكل جريمة معاقب عليها وفقا للقانون وأن فعله من شأنه تحقيق نتيجة تنطوي على آثار وخيمة وأضرار جسيمة ومع ذلك تتجه إرادته إلى الإقبال على السلوك الإجرامي وكذا تحقيق النتيجة منه أو على الأقل القبول بها وتتقيد تبعا

[1] – إسراء طارق جواد كاظم "جريمة الإرهاب الالكتروني – دراسة مقارنة"، مرجع سابق، ص 72 .

[2] – مصطفى سعد حمدي مخلف "جريمة الإرهاب عبر الوسائل الالكترونية، المرجع السابق، ص 50، 51 .

[3] – مصطفى سعد محمد مخلف ,المرجع نفسه, ص 71 .

لذلك والمسؤولية الجنائية إذا كانت الأفعال نابعة علن الجهل أو الغلط، علما أن إرادة الجاني في جريمة الإرهاب الالكتروني يجب أن تتجه إلى إحداث الخوف والرعب والفزع وكذلك الاعتداء على سلامة وأمن الأفراد أو الحكومات، تجدر الإشارة أن القانون لا يعاقب من تم حمله على تنفيذ جريمة إرهابية عن طريق الإكراه والتهديد، وكذلك الحال بالنسبة لمن قام بفعل إجرامي تأمر به السلطات، وهو ما يعرف بأسباب الإباحة أما القصد الجاني الخاص فيتعلق بجريمة الإرهاب الالكتروني على وجه الخصوص ولا يمكن إطباقها على غيرها من الجرائم وفي هذا الصدد نصت المادة 87 مكرر 03 من قانون العقوبات صراحة على انه لم يشر إلى العلم في الجرائم الماسة بأمن الدولة بوجه عام وكذلك بجرائم إرهابية والتي مفادها أن من يتولى تأسيس أو تنظيم جماعة يكون غرضها القيام بعمل يجرمه القانون لا يمكنه الاعتداد بعدم العلم والإرادة[1] لأنه يعلم مسبقا بطبيعة نشاطها أو الافتراض بوجودها. والعلم في جريمة التأسيس هو علم مفترض. والقصد الجنائي الخاص عموما يتعلق بالجريمة الإرهابية الالكترونية وهو كل فعل يتجه فيها القصد الجنائي إلى التشجيع على الإرهاب وبث الرعب في الأوساط والحث على الانخراط في صفوف الإرهاب .

الفرع الثاني: أسلحة الإرهاب الالكتروني:

مما لا شك فيه أن تغيير مسار الإرهاب من التقليدي إلى الحديث قد نجم عنه التطور في استعمال الأسلحة الحديثة، فلم تعد الحرب قائمة على الأسلحة التدميرية التقليدية وإنما تكفي كبسة زر إلى إلحاق الأضرار التي عجزت القنابل النووية على إلحاقها ومن بين الوسائل الحديثة التي بات الإرهاب يعتمد عليها في تنفيذ هجوماته هي أجزاء وتفاصيل صغيرة على مستوى الحاسوب الآلي وشبكة الانترنت وسنستعرض فيما يلي أهم هذه الأسلحة وأكثرها شيوعا .

أولا: الفيروسات:

إن فيروس الحاسوب الآلي هو عبارة عن برنامج صغير ودقيق يضعه المخربين بهدف إلحاق أكبر ضرر للحاسوب الآلي ومخزوناته ويستخدم في سبيل ذلك العديد من التقنيات لأداء وظيفته وهي ليست مدمرة بطبيعتها[2]، وقد عمد مركز الحسابات الشخصية بالولايات

[1] – ضيف مفيدة "سياسة المشرع في مواجهة الإرهاب الالكتروني"، المرجع السابق، ص 53، 54، 55 .

[2] – أحمد محمد عبد الرؤوف المنيفي "فيروسات الحاسب الآلي"،الطبعة الاولى' ص 4 .

المتحدة الأمريكية إلى تعريف الفيروس بأنه"عبارة عن برنامج ضار يصيب أنظمة الحاسوب بأسلوب يشابه إلى حد كبير الفيروسات الحيوية التي تصيب الإنسان، وهي عادة برامج صغيرة جدا مكتوبة بلغة متدنية المستوى مثل لغة التجميع مما يزيد من صعوبة اكتشافه والعثور عليه، وعندها يقوم بالتحول داخل الحاسوب الآلي بحثا عن برامج سليمة وعندما يعثر عليه يعمل فورا على استنساخ نفسه كتدخل منه وتستغرق كل هذه العملية أقل من جزء من الثانية ويقوم البرنامج فيما بعد بتنفيذ أوامر الفيروسات[1]، وتنقسم الفيروسات عموما إلى فيروسات الملفات التي تهاجم نظام التشغيل والتطبيقات وفيروسات الماكرو والتي تصيب برنامج التطبيقات المكتسبة كالورد وأكسل، والفيروسات الخفية أو ما يطلق عليها بفيروسات الأشباح وهي عبارة عن برامج مخادعة تختبئ في الذاكرة ثم تتصدى لتشخيص وفحص قطاع التشغيل وتعمل على إرسال تقارير مزيفة إلى السجل بأن القطاع غير مصاب وسليم، فمن خصائص هذه الفيروسات القدرة على الاستنساخ والانتشار السريع فضلا عن قدرتها لتدمير للبرامج السليمة والمعلومات .

ومن أشهر هذه الفيروسات، فيروس ساسر وماديوم وفيروس جوبوت وهي فيروسات شغلتها المنظمات الإرهابية لما لها من خاصية في استغلال الثغرات الأمنية الموجودة في نظام الويندأوز، ويعمل على إيقاف برامج المقأومة مثل برنامج جدار النار .

ومن بين الأضرار التي يسببها الفيروس هناك أضرار تقع على مكونات منطقية حيث يعمل فيها الفيروس على احتلال ذاكرة الحاسوب وإتلافها ومسح المعلومات وجعلها غير قابلة للاسترجاع وكذا تعطيل الحاسوب عن التشغيل حيث يجعله يشتغل وينطفئ تلقائيا كلما أراد المستخدم فتحه فضلا عن تغيير وظيفة لوحة المفاتيح وجعلها تعمل وتكتب بصورة غير صحيحة، أما الأضرار المادية فتتمثل في تقليل سعة التخريب والذاكرة الرئيسية للحاسوب وتدمير الأقراص الصلبة وإيقاف شبكات المعلومات المتدفقة في حال تعرض أحد الحواسيب المرتبطة بها لهجوم فيروسي[2] .

[1] – ربيع محمود الصغير "القصد الجنائي في الجرائم المنظمة بالانترنت والمعلومات"، دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، الطبعة الأولى، مصر، 2017، ص 397 .

[2] – عبد الرحمان عوض رجا ملاحة "جريمة الإرهاب المعلوماتي أسبابه وأساليبه"، المرجع السابق، ص 1243 .

ثانيا: أحصنة طروادة وبرامج الدودة:

يختلف حصان طروادة عن الفيروس من حيث أنه لا يمتلك خاصية التكاثر والإلصاق والتموضع على الملفات، فهو برنامج فيروسي يملك القدرة على الاختفاء داخل البرامج الأخرى الأصلية للنظام الالكتروني، وهي برامج مستقلة تعمل على التنشيط والنشر ليبدأ الأعمال التخريبية ويفعل أسلوبه الخاص وبرامج استيقاظه ويعمل على تدمير النظام بأكمله[1]، أما برامج الدودة فهي تتكاثر تلقائيا أثناء تنقلها و تعمل على تقليل كفاءة الشبكة أو التخريب الفعلي للملفات والبرامج وأنظمة التشغيل من خلال استغلال الثغرات والفجوات الموجودة على مستوى الأنظمة الالكترونية الأخرى[2] .

ثالثا: القنابل المعلوماتية:

تعتبر القنابل المعلوماتية من الأسلحة الأكثر شيوعا في الأعمال الإرهابية وهي تنقسم إلى قنابل منطقية تعتبر جزء من برنامج ينفذ في لحظة محددة أو ضمن فترة زمنية منتظمة يتم وضعه في شبكة "معلوماتية بغية تحديد ظروف النظام وتسهيل تنفيذ الأعمال غير المشروعة وهي عبارة عن جزء سري من البرمجة تنفجر في لحظة محددة بدقة لإبطال عمل البرامج الأخرى، بالإضافة إلى القنابل الزمنية ويتم وضعها بناءا على تحديد زمني دقيق للانفجار وتتسبب في خسائر وخيمة تتمثل في الإتلاف والتدمير الكلي للحاسوب ومن الصعب جدا التنبؤ بوقت انفجارها ويرجع ذلك لعدم إمكانية تحديد سبب التفجير الذي لا يعلم به سوى مرتكب الجريمة[3] .

المطلب الثاني: كيفية توظيف الإرهاب للقوة التكنولوجية والجرائم الناجمة عنها:

أصبحت التكنولوجيا أحد أهم العوامل الإستراتيجية التي تستخدمها المنظمات الإرهابية وأنصارها في تحقيق الأغراض الإرهابية التي تشمل الاستقطاب والتمويل والدعاية وكذا شن العديد من الجرائم عبر مجموعة متنوعة من المواقع ذات الأضرار الوخيمة التي تعجز الدول

[1] – هدى حامد فشقوش "جرائم الحاسب الالكتروني في التشريع المقارن"، الطبعة الأولى، دار النهضة العربية، مصر، 2000، ص 103 .

[2] – علي جعفر "جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة – دراسة مقارنة"، الطبعة الأولى، مكتبة زيت الحقوقية والأدبية، لبنان، 2003، ص ص 252 ، 254 .

[3] – عبد الرحمان عوض رجا ملاحة، المرجع السابق، ص 1343 .

والكيانات المتضررة عن جبرها، وسنتناول ضمن هذا المطلب الكيفيات التي تستخدم فيها التكنولوجيا من طرف الجماعات الإرهابية وكذا أهم الجرائم والأكثر شيوعا في هذا المجال .

الفرع الأول: التكنولوجيا المتطورة واستخداماتها في العمل الإرهابي:

أولا: تبادل وتدأول المعلومات الإرهابية:

تستخدم الجماعات الإرهابية الانترنت من أجل الدعاية من خلال وسائط متعددة تحمل تعاليم إيديولوجية أو إرشادات كلية من أجل التشجيع على القيام بها عبر الرسائل الافتراضية والعروض الإيضاحية والمجلات والأطروحات والملفات الصوتية والمرئية وألعاب الفيديو التي تصممها المنظمات الإرهابية خصيصا لهذا الغرض[1]، كذلك من خلال الربط الشبكي الذي يقصد به القدرة على الاتصال والتخفي حيث تستخدم الجماعات الإرهابية أنماط البناء الهيكلي الخاص بها من أجل تقليل مخاطر اللقاء المادي ووضع الرسائل المشفرة غير الملفتة لانتباه ومن دون الإفصاح عن الهوية أو ترك دليل واضح، هذا وتمتاز الشبكة بوفرة المعلومات وتعدد الثقافات فضلا عن أنها تزخر بالبيانات الهامة والحساسة التي يسعى الإرهابيون للحصول عليها كالمنشآت النووية ومصادر توليد الطاقة وأماكن القيادة والبروتوكولات الخاصة بسبل مكافحة الإرهاب وجمع أكبر قدر من المعلومات، وكذا التأثير على الرأي العام العالمي من خلال الحروب الإعلامية الدعائية المفرطة والترويج لأفكار التطرق والتعرف على اهتمامات المستخدم، ونشر البيانات الإرهابية والتحريض على الحروب والتأثير على مختلف الشرائح والهيئات وأبرز مثال عن ذلك ما ينشر من مواد حول لقاءات القادة وزعماء التنظيمات الإرهابية المتطرفة بالإضافة إلى المواد والمحتويات المتعلقة بنشر الرعب والخوف كنشر فيديوهات القتل والتعذيب والتفجيرات وتقوم من جهة أخرى بكسب المتعاطفين معها وتعبئة الأفراد وحشد أكبر قدر من الشباب واستقطابهم من أجل إقحامهم في التجنيد وتوجيههم للدعم والمساندة عن طريق بث الأفكار والفلسفة والمرجعيات الإرهابية والمذاهب المغلوطة من أجل التأثير على الفئات الهشة في المجتمع، ما يعكس الإقبال الشديد والمرعب للشباب على الجماعات الإرهابية والانخراط في صفوفها لاسيما المراهقين والقصر وحتى الأطفال ضمن المجموعات الإرهابية كتصميم ألعاب الفيديوالتي

[1]– utilisation de l'internet a des fins terroristes, En collaboration avec l équipe spéciae de le terrorisme contre terrorisme de l'orgamisation unies. P4.5.6

تشيد بالقتل وتنفيذ الهجمات الانتحارية ضد دولة معينة أو إحدى الشخصيات مع مكافأة اللاعب على نجاحه و تصميم هذه الأخيرة بلغات متعددة ما جعلها تلقى رواجا واسعا في صفوف المتلقين[1].

كما استخدم الإرهابي الرقمي بعض ألعاب الفيديو للتواصل بين أعضائه عبر الذبذبات الصوتية، وقد تمت في هذا الصدد عملية مهمة حول تجنيد الأطفال في الولايات المتحدة الأمريكية بواسطة لعبة تحمل اسم Rolocs30 (رولوكس)، وذلك لتنفيذ العمليات الإرهابية داخل أراضيهم من خلال جذبهم للجهاد، وكذلك لعبة Call of Daty. كال أوف داتي والتي أصدر منها تنظيم داعش نسخة خاصة به[2] .

ثانيا: التخطيط والتدريب والحصول على التمويل:

إن العمليات الإرهابية غاية في التعقيد والصعوبة فهي تحتاج إلى تخطيط محكم وتنسيق شامل، وتعتبر الشبكة الإعلامية للتكنولوجيا وسيلة الاتصال ألاكثر أهمية للجماعات الإرهابية لما تتيحه لهم من حرية في التخطيط والتدقيق والتنسيق الشامل بما يسهل على الإرهابيين ترتيب حركاتهم وتوقيت هجومهم. من خلال الاستعانة ببيانات إحصائية سكانية يتم انتقائها من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية ويتعرف الإرهابيون على الأشخاص ذوي التعاطف والقلوب الرحيمة واستدراجهم لدفع تبرعات مالية لأشخاص اعتبارية يكونون ستار وواجهة للإرهاب ويتم ذلك بواسطة رسائل البريد الالكتروني أو ساحات الحوار الرقمية بطرق ذكية وأساليب احتيالية ومخادعة بما لا يدع مجال للشك من طرف المتبرع[3]. ويتم ذلك إما عن طريق الطلب المباشر. أو من خلال عمليات الدفع عبر الانترنت وسرقة بطاقات الإتمان والأوراق المالية وانتحال الشخصية أو خدمات الدفع البديلة مثل (باي بال) أو "سكايب"، كما أنه في السنوات الأخيرة أصبحت التنظيمات الإرهابية تستخدم الانترنت بوصفه ساحة بديلة لتدريب الإرهابيين من خلال مجموعة متزايدة من الوسائط التي توفر منصات لنشر أدلة عملية في صورة كتيبات أو

[1] – توفيق شريخي "الإرهاب الالكتروني وتأثيره على أمن الدولة"، مذكرة لنيل شهادة ماستر اكادمي في العلوم السياسية، تخصص إستراتيجية وعلاقات دولية، جامعة محمد بوضياف، المسيلة، ص 46 .

[2] – شرقي صبرينة– غريب حكيم "الإرهاب الالكتروني والتحول في مفهوم القوة"، مجلة الباحث للدراسات الأكاديمية، العدد 02، مجلد 07، المدرسة الوطنية العليا للعلوم السياسية، 2020، ص 566 .

[3] – محمودي قادة، المرجع السابق ص 181 .

مقاطع صوت وفيديو، وكذا جملة واسعة من المعلومات والنصائح كما تتيح تعليمات مفصلة غالبا ما تتخذ شكل وسائط متعددة يسهل الاطلاع عليها حول الموضوعات المتعلقة بكيفية الانضمام للجماعات الإرهابية وآليات وضع المتفجرات والتدريب على استخدام الأسلحة النارية وكيفية التخطيط للهجمات الإرهابية عبر أي نقطة من بقاع الأرض وهكذا تكون المنصات الرقمية بمثابة معسكرات للتدريب الافتراضي وتبادل الأساليب والتقنيات وتطوير المهارات الإرهابية[1]، أو ما يعرف بالتلقين الالكتروني الذي يتعلق على وجه الخصوص بصناعة الأسلحة القتالية وأساليب التفخيخ والصناعة الكيمأوية والقنابل اليدوية[2].

كما تضم المنتديات الجهادية مجموعة من الإصدارات حول الدورات التدريبية، كما تسعى المنظمات الإرهابية بخطوة جديدة إلى إعادة استقطاب وتجنيد عناصر إرهابية سبق لها أن اشتركت في القتال في مناطق الصراع عبر ربوع العالم مما يعتبر أسلوبا جديدا ومختصرا للوقت مما قد سأهم بدور كبير في حشد أعداد كبيرة من المقاتلين في سبيل تنفيذ مخططات الإرهاب[3] .

الفرع الثاني: أشهر جرائم الإرهاب الإلكتروني:

أولا: إنشاء المواقع واختراقها وتدميرها:

إن الانتشار السريع للتكنولوجيا قد فتح المجال أمام الإرهاب لإنشاء مواقع خاصة بهم لبث أفكارهم ومبادئهم والدعوى إلى الجهاد ونشر التطرف، وشرح الطرق التفصيلية لعمليات الاختراق وكيفيات التدمير والدخول إلى المواقع المحجوبة وكذا أساليب نشر الفيروسات بهدف خدمة أغراضهم والتي تعتبر بمثابة المقر الافتراضي لهم، وتجدر الإشارة أن وجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومرأوغ بصورة عميقة، فإذا ظهر موقع إرهابي اليوم فإنه سرعان ما يتغير نمطه الالكتروني في اليوم الموالي ثم يختفي ويظهر مرة أخرى

---

[1]– utilisation de l’internet a des fins terroristes, En collaboration avec l équipe spéciale de le terrorisme contre terrorisme de l’organisation unies. P8

[2]– مهني محمد "تأثير الإرهاب الالكتروني على تغيير مفهوم القوة في العلاقات الدولية– توظيف المنظمات الإرهابية لمواقع التواصل الاجتماعي"، المرجع السابق، ص 35 .

[3] – نورة بلعبيدي "توظيف تنظيم الدولة الإسلامية"، الأنظمة الاتصالية الرقمية في استراتيجياته الإرهابية، المدرسة الوطنية العليا للعلوم السياسية، ص ص، 191، 193 .

بشكل جديد وتصميم مغاير وعنوان الكتروني مختلف[1]، كما يستخدم الإرهابيون مواقع ويب لا يمكن إظهارها للمتصفح العادي وإنما يتطلب الولوج إليها تقنيات تشفير معقدة للتواصل فيما بينهم وهي ما يطلق عليه اسم الويب المظلم Dark Wep [2].

هذا وقد نجد أن للمنظمة الإرهابية الواحدة آلاف المواقع لضمان انتشار أوسع بحيث حتى ولو منعت من الدخول إلى بعضها فإن المواقع الأخرى تبقى متاحة للاستغلال[3]، فضلا عن استخدام البريد الالكتروني الذي يتيح هو الآخر إمكانية التواصل بين أفراد المنظمات الإرهابية عبر العالم[4]،لما يمتاز به من سرعة وهو يعتبر من أشهر الوسائل، كما يعمل الإرهابي الرقمي في جهة معاكسة على تخريب باقي المواقع كليا أو جزئيا من خلال زرع الفيروسات في أنظمة الأجهزة مما يسبب خللا في برنامج التشغيل، ومن بين البرمجيات الخبيثة المستعملة في ذلك، برنامج الباب المسحور التي تسمح بتجنب إجراءات الأمان القياسية لدى المحترف،وبالتالي تسهيل إجراء تعديلات للبرمجيات والتي تسمح الواحدة منها بتعطيل حوالي 6000 جهاز في أقل من جزء من الثانية وذلك بعد سرقة كل ما تحتويه من بيانات[5] .

ثانيا: التجسس الالكتروني :

إن التجسس الالكتروني يعبر بصفة عامة عن انتهاك خصوصية الغير من خلال القدرة على الدخول غير المشروع والاطلاع على شبكات وأنظمة الخصم، بهدف الحصول على المعلومات التي قد تشمل خطط أو بروتوكولات الأمن القومي أو خطط عسكرية دفاعية أو نماذج جديدة لتقنيات الهجوم،أو حول مخططات سرية للحرب وكذا أهم الدراسات والأبحاث التي توصل إليها الخصم المعتدى عليه،و كل الاستطلاعات الاستخباراتية والسياسية وذلك دون أن يصاحب هذا الاختراق تدمير أو تخريب لتلك البيانات والمعلومات، كما قد تلجأ

---

[1] – حسنين شفيق "الإعلام الجديد والجرائم الالكترونية– التسريبات والتجسس الالكتروني، الإرهاب"، الطبعة الأولى، دار فكر وفن للطباعة والنشر والتوزيع، 2016ص ص163,162

[2] – رافعي ربيع، المرجع السابق، ص 175 .

[3] – وفاء لطفي حسين عبد الواحد "الإرهاب الالكتروني في ظل جائحة كوفيد 19"، المرجع السابق، ص 447 .

[4] – غلاف كريمة، جرلال زهرة "جريمة الإرهاب الالكتروني، المرجع السابق، ص 22 .

[5] – وهيبة يشرف "مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الالكتروني في ظل المجتمع المعلوماتي، جامعة باتنة، ص ص 66، 67 .

الجماعات الإرهابية إلى تصميم وإعداد خرائط لشبكات الحاسوب الآلي والاعتماد عليها مستقبلا في تنفيذ العمليات الإرهابية عبر الفضاء الرقمي، كما يمكن شحن الشبكة بأنواع صعبة من الفيروسات من خلال ترك ثغرات، تكون بمثابة أبواب خلفية للقيام بمهام معينة ونقل البيانات إلى أجهزة المخترق[1]، ويشمل التجسس الالكتروني الإرهابي جميع أنواع المعلومات السياسية المتعلقة بالمشاريع المتخذة بين الدول والحكومات وكذا المعاهدات والاتفاقيات السرية، كما تشمل عمليات التجسس تلك المعلومات الاقتصادية التي تعتبر أهم ركائز الأمن ومعرفة أحداث الصناعات المالية التي تتمحور حولها ثروات منطقة معينة ومحأولة الوصول إليها،وكذا المعلومات العسكرية التي تشمل تطورات الجيوش داخل الدول والأجهزة العسكرية والذخائر والعتاد الحربي وكل ما يتعلق بجانب الأمن الاستراتيجي للدول وآخر ما توصلوا إليه في المجالات العلمية والاختراعات الحديثة من أجل سرقتها والاستفادة منها أو أخذ الاحتياطات اللازمة منها والحذر وذلك من خلال الصناعات المضادة لها[2].
وكذالك زرع عملاء سريين من أجل التجسس على المعلومات وتسريبها إلى المستخدم' وتجدر الإشارة إلى أن التجسس على الحكومات والأفراد بات شائعا إلى حد كبير ولم يعد مقتصرا على وكالة الأمن القومي الأمريكي التي لطالما تورطت في فضائح كبرى حول العالم بخصوص عمليات الجوسسة وكذا ما يقوم به الجيش الالكتروني السوري من عمليات الاختراق[3] .

[1] – Dennis. Murplry, information opération primer, 1st eduction carlish U.5.Armu War Colleu .USA.2010.p169.

[2] – محمد أحمد عبد الفتاح "الإرهاب السيبراني https://ar.wexipedia.arg/w/index.ph p? ».

[3] – حسنين شقيق "الإعلام الجديد والجرائم الالكترونية– التسريبات والتجسس الالكتروني والإرهاب"، المرجع السابق، ص ص 162، 169 .

الفصل الثاني: آليات مكافحة جريمة الإرهاب الالكتروني.

تمهيد:

إن تصاعد وتيرة استخدام الوسائل التكنولوجية الحديثة يوما بعد يوم قد سأهم في خلق الفرصة والبيئة لزرع جذور الإرهاب، ما أنجز عنه ارتفاع كبير وتعاظم في الخسائر الناشئة عنه، وانتهاكا لحرمة الأشخاص والدول والأمم جمعاء، ودق ناقوس الخطر لدى الدول خاصة ولدى المجتمع الدولي عامة، والذي أتم عنه ضرورة المسارعة في اتخاذ التدابير والإجراءات اللازمة لحصر انتشار الإرهاب وتبر جذوره التي انتشرت كالنار في الهشيم، وبحثا منهم عن تعزيز سبل الوقاية والبحث من اجل صيانة الحقوق وحفظ السلم والأمن العالميين 'وسنتطرق فيما يلي إلى أهم الجهود التي قامت بها الدول سواء على المستوى الوطني أو الاقليمي وكذا العالمي وذلك عبر المبحثين التاليين

المبحث الأول: آليات مكافحة الإرهاب الالكتروني على الصعيد العالمي.

إن التصدي لجريمة في قمة الحداثة وأوج القوة كالإرهاب الالكتروني أمر شبه مستحيل من طرف واحد، لذلك لا بد من التعاون بين جميع الدول في إطار التصدي لهذه الجريمة بما يتوافق مع التشريعات الدولية القائمة بحفظ السلم العالمي والأمن الداخلي، وفي هذا الصدد سنتطرق إلى أهم المنظمات العالمية التي نادت بمكافحة الإرهاب بشتى أنواعه وذلك من خلال المطلبين التاليين.

المطلب الأول: آليات مكافحة الإرهاب الإلكتروني على مستوى هيئة الأمم المتحدة:

سعت هيئة الأمم المتحدة منذ البداية إلى تحقيق السلم والأمن الدوليين وتحقيقا لذلك عملت على قمع العدوان واتخاذ التدابير المشتركة والفعالة لمنع الأسباب التي تهدد السلم وإزالتها وفقا لمبادئ العدل والقانون الدولي، وكذا حل المنازعات الدولية وتنمية العلاقات بين الأمم والشعوب وتحقيق التعاون الدولي وتعزيز احترام حقوق الإنسان ونبذ مظاهر العنف والتطرف ما جعل هيئة الأمم تسعى لتنسيق الأعمال من خلال أجهزتها وإرساء السلم والأمن العالميين لاسيما في ظل التطور التكنولوجي الهائل الذي يشهده العالم .

الفرع الأول: جهود منظمة الأمم المتحدة في التصدي للإرهاب الالكتروني:

لقد أصدرت الأمم المتحدة قرارا بشأن التطورات الراهنة في مجال الاتصالات السلكية واللاسلكية والمعلومات، في سياق الأمن الدولي عبر جمعيتها العامة، كما اتخذت قرارا آخر يهدف إلى إرساء ثقافة عالمية لأمن الفضاء الالكتروني، والذي تم اعتباره من أهم القرارات لما يحمله في طياته من حث للدول والمنظمات الإقليمية على مضاعفة الجهود والتعاون وحماية البنية التحتية للمعلومات[1]، هذا وتعتبر الولايات المتحدة الأمريكية من الدول السباقة في مواجهة الإرهاب بشتى أنواعه انطلاقا من خبرتها الكبيرة في معالجة المسائل الهامة على مر العصور وتشجيع الدول على ذلك، وتجدر الإشارة أن ميثاق الأمم المتحدة لم ينص

[1] – شفيق نوران "أثر التهديدات الالكترونية على العلاقات الدولية"، الطبعة الأولى، المكتب العربي للمعارف، مصر، 2015، ص 108.

صراحة على تجريم الإرهاب الالكتروني، إلا أنه يفهم من فحوى مختلف قراراته انه يعتبر استعمال تكنولوجيا الإعلام والاتصال بطريقة غير سلمية وإجرامية إنما هو انتهاكا لقواعد السلم والأمن الدوليين ما يتعارض مع مبادئها المعبر عنها من خلال ميثاق الأمم المتحدة والذي نص على تجريم استخدام القوة، ضد سلامة الإقليم والاستقلال السياسي للدول، ومما لا شك فيه أن الإرهاب الالكتروني وما ينطوي عليه من عنف وتعدي على خصوصيات الدول وانتهاك حرمتها يدخل ضمن هذا العدوان[1].

كما نص على أن لجوء الدول إلى حل نزاعاتها عبر الفضاء الرقمي يجعل السلم والأمن معرضين للخطر وهو ما جاء في المادة الثانية من ميثاق الأمم المتحدة والتي تنص في الفقرة 3 منها على أنه" يفض جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر"[2]. هذا وقد اشرف الأمين العام للأمم المتحدة عام 2004 كوفي عنان على تشكيل فريق جنوبي لدراسة قضية الانترنت وإدارة المخاطر الناجمة عنها مع إنشاء لجنة من الخبراء الحكوميين بهدف مناقشة الإجراءات اللازمة لمواجهة الأخطار في مجال الأمن السيبراني للدول، وكذا تقوية أمن نظم الاتصالات العالمية التكنولوجية[3]، وفي هذا الصدد ثم اتخاذ جملة من الإجراءات والتدابير الفعالة لمكافحة الأعمال الإرهابية الالكترونية وحتى الإرهابية التقليدية والتي تمثلت أساسا في الامتناع عن تقديم أي شكل من أشكال الدعم السريع أو الخفي للجماعات الإرهابية وعدم توفير الملاذ لمن يمول الجماعات الإرهابية أو يعمل على إدارتها أو ارتكاب الأعمال التي تدخل في دائرتها وتشجيع الدول على تبادل المعلومات مع الدول الأعضاء وكذا دعوة المنظمات الإقليمية والدولية لتعزيز التعاون مع الأمم المتحدة، كما اتخذت عام 2002 في الدورة 258/56 قرارا يدعو غلى استخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية، حيث أصبح فعلا يشكل تهديدا للأمن والسلم العالميين كل استخدام للوسائل التقنية التكنولوجية من اجل التأثير على الأمن المعلوماتي المرتبط والمتعلق بأثر هذا الاستخدام .

---

[1] – سارة بوحادة "مداخلة حول أثر الإرهاب E على أمن واستقرار الدول"، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، ص 15.

[2] – سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، المرجع نفسه، ص 11.

[3] – محمد أمين الشوابكة "جرائم الحاسوب والانترنت، الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص 73.

وعموما فإن الأمم المتحدة ركزت في سبيل حفظ الأمن المعلوماتي على 3 نقاط رئيسية تتعلق الأولى بضرورة حرية التنقل والتعبير وجمع المعلومات والدعوى إلى مراقبة الانترنت، أما النقطة الثانية فتتعلق بالتحذير من مخاطر الإرهاب الالكتروني وتنمية الوعي الدولي وإدانة كل من يساهم في أفعال مخالفة للسلم، هذا ويتمحور العنصر الثالث حول المواجهة العالمية لمظاهر الإرهاب الرقمي وضرورة وضع جملة من الإستراتجيات الشاملة لمكافحة هذه الجريمة على أرض الواقع[1]، وفي عام 2006 اعتمدت الجمعية العامة للأمم المتحدة قرارا بعنوان إستراتجية الأمم المتحدة في مكافحة الإرهاب في المادة 12، حيث جاء في الفقرة الأولى منها أنه"تنسيق الجهود على الصعيدين الدولي والإقليمي لمكافحة شتى أشكال الإرهاب ومظاهره على الانترنت. وكذا استعمال تكنولوجيا الإعلام كأداة لمكافحة الإرهاب"، وعليه فإن مكافحة الإرهاب الالكتروني لن يتحقق إلا بتعزيز الإطار القانوني والتشريعي على المستوى العالمي من أجل منع التهديدات وقمع العدوان كما نصت على ضرورة اتخاذ خطوات عملية فردية وجماعية في سبيل ذلك وفي عام 2009 تم إنشاء فرقة عمل معنية بالتنفيذ في مجال مكافحة الإرهاب واكتسبت طابعا مؤسساتيا في إدارة الشؤون السياسية التابعة للأمم المتحدة عبر القرار 64-235، وفي عام 2011 عمدت الأمم المتحدة إلى إنشاء مركز الأمم المتحدة الدولي لمكافحة الإرهاب من أجل توفير وتعزيز التعاون الدولي في تنفيذ الاستراتجيات العالمية لمواجهة الإرهاب بشتى أنواعه[2]، كما أقر الأمين العام للأمم المتحدة بخطورة الإرهاب السيبراني الذي يعتبر بمثابة الأرض الخصبة للأعمال الإرهابية بكيفية عابرة للقارات والحدود وفي هذا السياق حث الدول على العمل بطريقة موحدة. حيث كان أول تصريح له في عام 2006 حول خطورة الهجمات الإرهابية في الفضاء الرقمي. ضمن التقرير الصادر عن الأمم المتحدة بعنوان (استخدام الانترنت في أغراض إرهابية) وكان ذلك أول عمل منهجي تنتهجه الأمم المتحدة بخصوص الإرهاب السيبراني، ويعتبر هذا التقرير مرشدا فنيا وتقنيا عالي المستوى يحتوي على أهم الإيضاحات وكذا التوصيات التي تكفل تحقيق سبل التعاون الأمني والقضائي .

[1] – سامر مؤيد عبد اللطيف، المرجع السابق، ص 20.

[2] – ثامر علجة "الجهود الدولية في مكافحة الإرهاب الالكتروني"، مجلة الباحث للدراسات الأكاديمية، العدد 01، المجلد 08، 2021، ص 37 .

وفي عام 2015 وعملا بالبند 97 من قرار مجلس الأمن 2253 أصدرت الجمعية العامة للأمم المتحدة قرارين حول الإمارة الإسلامية بخصوص تجنيد الإرهاب عبر مواقع التواصل الاجتماعي، وأصدرت بهذا الشأن جملة من التوصيات حول استحداث إجراءات محلية عاجلة للحد من هذه الظاهرة، ودعت الشركات العالمية مثل شركة (فيسبوك) إلى التعاون الدولي من أجل تدمير حسابات الجماعات الإرهابية وإزالة محتواها على نطاق واسع، ومن الملاحظ أن هذه الإجراءات هي وقائية تعمل على محاربة العنف والأفكار المتشددة المتطرفة[1] .

الفرع الثاني: جهود مجلس الأمن في التصدي للإرهاب السيبراني.

إن مجلس الأمن بصفته يتمتع باختصاص هام في نطاق حفظ الأمن والسلم الدوليين والذي يعتبر أهم الاختصاصات على الإطلاق، وعليه فإن كل الأفعال التي من شأنها زعزعة أمان العالم وتهديد بقاءه تدخل ضمن اختصاصات مجلس الأمن باعتباره الجهة المناط بها حفظ السلم والأمن مما يمنحه صلاحية إصدار القرارات واتخاذ ما يراه مناسبا، ومن المعروف ودون أدنى شك أن تجريم العمليات الإرهابية والإرهاب مهما كان نوعه يتفق مع روح ومبادئ ومقاصد مجلس الأمن لما تنطوي عليه هذه الأعمال من انتهاكات صارخة ضد السلام العالمي[2]، وفي هذا الخصوص أصدر مجلس الأمن جملة من القرارات. لاسيما القرار 1269 عام 1999 الذي دعا فيه جميع الدول إلى ضرورة التنفيذ الكامل للاتفاقيات الدولية الخاصة بمكافحة الإرهاب وانضمام أكبر عدد من الدول إليها، كما يقترح اعتماد المزيد من الاتفاقيات فيما يتعلق بقضايا الإرهاب الالكتروني .

وفي هذا الصدد أصدر مجلس الأمن أشهر قرار ثم اتخاذه وهو القرار رقم 1373 الذي تضمن جملة من التدابير الملزمة للدول وأهما التزام جميع الدول بتجريم تقديم المساعدة للأنشطة والجماعات الإرهابية.

---

[1] – العشعاش إسحاق "الإرهاب السيبراني وتحديات الدول"، دراسة مقارنة مع الاتفاقيات الدولية، مجلة بحوث، الجزء الأول، العدد 12، 2018، السابق، ص 193.

[2] – محمود أديب فتاح آغا الكاكة "اختصاصات مجلس الأمن في التصدي للإرهاب الالكتروني"، مجلة دراسات علوم الشريعة والقانون، العدد 01، كالمجلد 07، ص 653 .

كما أنشئت لجنة "تتكون من جميع أعضاء مجلس الأمن من أجل مراقبة مدى تنفيذ هذا القرار[1]، كما دعا في القرار 635 إلى اتخاذ كافة التدابير اللازمة لمنع أعمال الإرهاب التي ترتكب ضد الطيران المدني، وأصدر بذات الخصوص القرار رقم 731 عام 1992 على إثر حوادث تفجير الطائرات الذي أدان بشدة الهجوم الجبان الذي استهدف الركاب، فضلا عن القرار 1377 الذي أدان هو الآخر الهجمات الإرهابية بغض النظر عن أهدافها، واعتبر أن الإرهاب يشكل تهديدا للسلم والأمن الدوليين ودعا فيها كافة الدول إلى ضرورة الاستعجال في وضع اتفاقيات وبروتوكولات دولية متعلقة بمكافحة شتى أنواع الإرهاب[2]، هذا وقد عمد مجلس الأمن إلى فرض مجموعة من التدابير على الدول بخصوص التضييق على الإرهاب الالكتروني وذلك عام 2014 بموجب القرار رقم 2161 عقب إنشاء لجان مختصة للعمل عملا بالقرار رقم 1267 الصادر عام 2011 بشأن بتنظيم القاعدة، وكذا القرار رقم 2253 الصادر عام 2015 المتعلق بتنظيم الدولة الإسلامية في العراق والشام، وتعمل هذه اللجان على تقليص أثر انعكاسات التطرف والفكر الجهادي المغرض على المجتمعات[3] .

تجدر الإشارة أن مجلس الأمن لم يتطرق بشكل موسع وشامل لجريمة الإرهاب الالكتروني، غير أنه لا يمكن بأي حال من الأحوال إنكار الطبيعة المتشابهة للإرهاب الالكتروني والإرهاب التقليدي لاسيما من حيث أغراض هذه المنظمات ومدى عصفها بالسلم والأمن العالميين الذي يعتبر الحفاظ عليه من أهم الاختصاصات المناطة به[4].

المطلب الثاني:آليات مكافحة الإرهاب السيبراني في إطار المنظمات الدولية الأخرى.

إن الخطوة الأولى لمعالجة جريمة الإرهاب السيبراني تتجلى في الإقرار بوجوده والقبول به أولا وتنامي الوعي بخطورة الجرائم الإرهابية لاسيما تلك التي تستعمل تكنولوجيا الإعلام

[1] – قرار مجلس الأمن رقم 1437 الصادر في 28 سبتمبر 2001 .

[2] – محمد أديب فتاح آغا الكاكة "اختصاصات مجلس الأمن في التصدي للإرهاب الدولي الالكتروني"، المرجع السابق، ص 653.

[3] – العشعاش إسحاق، المرجع السابق، ص 194.

[4] – محمد أديب فتاح آغا الكاكة، المرجع نفسه، ص 653 .

والاتصال، وعليه سعت العديد من المنظمات الدولية إلى تبني جملة من الاستراتجيات من أجل مكافحة هذه الجريمة .

الفرع الأول: جهود الاتحاد الدولي للاتصالات والمنظمة العالمية للملكية الفكرية في مكافحة الإرهاب الالكتروني.

تم إنشاء الاتحاد الدولي للاتصالات بموجب اتفاقية باريس لعام 1865 تحت تسمية التلغراف الدولي، وقد تم تعديله لتصبح تسميته بالاتحاد الدولي للاتصالات السلكية واللاسلكية، وهذا قبل انضمامه للأمم المتحدة سنة 1947، وقد سأهم في وضع المعايير الأساسية المتعلقة بالأمن السيبراني لمكافحة الإجرام والإرهاب الإلكتروني، وذلك من خلال عمله الوثيق مع باقي المنظمات الأخرى والاشتراك مع الوكالة الأوروبية لأمن الشبكات، ويقوم بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، وكذلك تنسيق آلية لاسترجاع الثقة في المجال الرقمي من خلال إطلاق برنامج الأمن السيبراني[1]، كما تم تعيين فريق مشكل من خبراء وقدم في هذا الصدد جملة من الاقتراحات، كما قام بنشر دليل أمني لمساعدة الدول في تعزيز أمنها السيبراني، كما يضع إطارا لتقوية الأمن تحت تسمية (برنامج الأمن السيبراني العالمي)، بحيث تم تعيين خبراء في هذا المجال بغية إسداء المشورة لباقي الدول، كما نضمت القمة العالمية لمجتمع أمن المعلومات التي يرعاها الإتحاد الدولي للاتصالات[2]، وكذا تقديم جملة من التوصيات. أهمها ضرورة بناء القدرات من خلال نشر الوعي الاستراتيجي ونقل الخبرة وتعزيز الحماية الرقمية وكذلك التركيز على التدابير الرئيسية الرامية لمعالجة مواطن الضعف في البرمجيات الالكترونية والتعاون الدولي لوضع إستراتجية الحوار وإسداء المشورة بشأن كيفية التعاون مع الأنشطة الإجرامية المعلوماتية من خلال وضع تشريعات متوافقة عالميا للحماية من الأخطار الالكترونية ووضع هياكل تنظيمية لمنع الهجمات السبيرانية وتعقبها والرد عليها وإدارة الأزمات المتعلقة بها، وحماية أنظمة البنية التحتية للمعلومات[3].

[1] – سامر مؤيد عبد اللطيف، نوري رشيد الشافعي، المرجع السابق، ص 20 .

[2] – العشعاش إسحاق، المرجع السابق، ص 194.

[3] – توفيق شريخي "الإرهاب الالكتروني وتأثيره على أمن الدولة"، المرجع السابق، ص 62.

أما المنظمة الدولية لحماية الملكية الفكرية فقد تم إنشائها عام 1967 بموجب اتفاقية ستوك هولم وانضمت للأمم المتحدة عام 1974، وتعمل هذه المنظمة على توقيع معاهدات دولية جديدة والتنسيق بين التشريعات القومية وتقديم الدعم الفني والقانوني للدول السائرة في طريق النمو، وتعكس المنظمة حاجتها إلى حماية البرامج وبدورها شكلت لتحقيق هذا الغرض مجموعة عمل منظم يحوي عددا من الخبراء بهدف حماية الحواسيب والبرمجيات من الهجمات السيبرانية والتهديدات الرقمية[1].

كما نصت الاتفاقية الدولية الأولى المتعلقة بجرائم الانترنت والتي جاء إبرامها في23 نوفمبر 2001، بهدف التعاون الدولي في سبيل مكافحة الجرائم السبيرانية والتي تم إبرامها في بوتسدام عاصمة المجر وتجدر الإشارة أن هذه المنظمة لم تتطرق بصفة مباشرة إلى جرائم الإرهابي الالكتروني غير أنه بنصها على الجرائم الالكترونية عموما يفهم أن الإرهاب الرقمي يدخل ضمن صلاحياتها وعضوية هذه الاتفاقية مفتوحة لأي دولة من دول العالم بالرغم من أنه تم إنشائها في أوروبا وتم التوقيع عليها من طرف الولايات المتحدة الأمريكية بالإضافة إلى 26 دولة أخرى من دول العالم، وأعلنت بدورها أن الجرائم السيبرانية التي جاء النص عليها بموجب اتفاقية بوتسدام قد تكون في حكم الجرائم الإرهابية حسب ما نص عليه القانون المعمول به وذلك بموجب المذكرة التوجيهية المتعلقة بجرائم الإرهاب الرقمي التي أصدرتها لجنة الاتفاقية والتي تطرقت إلى الإرهاب الالكتروني بطريقة غير مباشرة بما يسمح بتطبيق بنود الاتفاقية على الأفعال الإرهابية التي تستخدم التقنيات التكنولوجية في تحقيق أغراضها. وشن الهجمات باستخدام الذكاء الاصطناعي الرقمي[2]، وعلى العموم قد تم التشديد على ضرورة التكاتف والتعاون الدولي في سبيل التصدي لجميع الجرائم الماسة والمهددة بزعزعة السلم والأمن الدولي بما فيه الإرهاب السيبراني والسعي إلى خلق إطار قانوني تشريعي موحد على المستوى العالمي.

[1] – طارق عزت رخاء "المنظمات الدولية المعاصرة"، الطبعة الأولى، دار النهضة العربية، مصر، 2006، ص 214.

[2] – وفاء لطفي "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني، التجربة الماليزية نموذجا"، المرجع السابق، ص 163.

الفرع الثالث: جهود المنظمة الدولية للشرطة الجنائية (الأنتربول) في التصدي للإرهاب السيبراني.

منذ أن ظهرت التعاونات الدولية في مجال الشرطة الجنائية، سعت منذ البداية إلى تأكيد وتشجيع التكاثف بين مختلف أجهزة الشرطة التابعة للدول الأطراف في منظمة الانتربول، على نحو ناجع وفعال يضمن محاربة مختلف الجرائم، وذلك عبر تكريس التعاون الفعلي بين الدول وتقديم المساعدات بغية جمع المعلومات الإجرامية والوصول إلى المجرمين عبر إنشاء مجموعة من المكاتب المركزية الوطنية التابعة للشرطة الدولية المتواجدة على مستوى إقليم كل دولة من الدول الأطراف لاسيما في مجال الجرائم المتعلقة بالانترنت، وتمارس هذه المنظمة مهامها بطريقتين الأولى تتم من خلال اللجنة التنفيذية والجمعية العامة بواسطة السكرتارية العامة وهو يتعلق بالدول المركزية، أما الثاني فيتم مباشرة بواسطة أجهزة الشرطة بين الدول الأطراف وهي تتعلق بالدول اللامركزية، هذا وقد تم إنشاء الشرطة الأوروبية عام 1991 من طرف المجلس الأوروبي بغية متابعة وملاحقة المجرمين لاسيما بخصوص تلك الجرائم المتعلقة بالانترنت والتكنولوجيات المتطورة.

كما تم إنشاء المكتب العربي للشرطة الجنائية على مستوى مجلس الوزراء الداخلية وذلك بغية تعزيز التعاون في مجال مكافحة الإجرام وملاحقة الجناة من خلال تبادل المعلومات بين مختلف أجهزة الشرطة وذلك في حدود ما تسمح به القوانين المعمول بها داخليا في الدول الأطراف التابعة للشرطة الجنائية الدولية[1]، كما قد أعلن الانتربول عام 1981 على أول مبادرة من أجل مواجهة الجريمة الالكترونية والإرهاب ومن ثم إنشاء معهد قانون القضاء الالكتروني في جامعة جورج تاون عام 1995، كما يسعى الانتربول إلى مكافحة الإرهاب السبيراني من خلال التدخل وإجراء المتابعة والتحقيق لاسيما من خلال قرار عملية الشرطة الجنائية لعام 2005 المعتمد من طرف الجمعية العامة في برلين [2].

[1] – إسراء طارق جواد كاظم، المرجع السابق، ص 114.

[2] – إسحاق العشعاش، المرجع السابق، ص ص 194، 195 .

المبحث الثاني: جهود المنظمات الإقليمية والمحلية في التصدي لجريمة الإرهاب الإلكتروني:

لطالما كان الإرهاب أهم القضايا الشائكة التي اجتاحت الدول وعصفت بأمن شعوبها واستقرارها لاسيما بعد التطور الذي شهده العالم في مجال تكنولوجيا الإعلام والاتصال، غير أن المنظمة الإقليمية والجهود الوطنية سعت بكل طاقتها إلى محاولة التخفيف من حدة هذا الشبح الغامض ووضع الحلول والاستراتيجيات لمجابهته، مما جعلها تكون أكثر عرضة للفتك بسلامة أمنها وسنتطرق من خلال المطلبين التاليين إلى أهم الجهود الأوربية والعربية للتصدي للإرهاب الالكتروني.

المطلب الأول: آليات مكافحة الإرهاب الإلكتروني على المستوى الأوروبي والعربي:

الفرع الأول: جهود الإتحاد الأوروبي في التصدي للإرهاب الالكتروني:

مما لاشك فيه أن الاتحاد الأوروبي كان سباقا وفعالا في مجال حماية الأمن والتصدي للجرائم على تنوعها لاسيما الإرهاب والإرهاب الالكتروني، أين عمل الاتحاد الأوروبي إلى إطلاق جملة من التوصيات في مجال استخدام التكنولوجيا وحماية الشبكة العنكبوتية، حيث وقع المجلس الأوروبي في هذا الصدد على اتفاقية حول حماية الأشخاص في إطار مواجهة الجرائم المتعلقة بسرقة الأسرار والغش الرقمي كما اصدر في ذات السياق جملة من القواعد التوجيهية على غرا باقي الجهود التي تمثلت في معاهدة أوروبا والخاصة بحماية الأشخاص من مخاطر التكنولوجيا عام 1980 واصدر في ذات الخصوص مجموعة من التوصيات حول استغلال التكنولوجيا بموجب التوصية رقم 1/1 المتعلقة بتنظيم البيانات وكذا الإرشاد الأوروبي المتعلق بالحماية القانونية للبيانات الالكترونية والصادر عن جهود السوق الأوروبية المشتركة.

هذا وقد عمل الاتحاد إلى إصدار اتفاقية شاملة في ستراتبورغ المتعلقة بجرائم الحاسوب والتي دعت بدورها إلى ضرورة حماية المجتمع من الهجمات السيبرانية ووضع

الاستراتيجيات اللازمة لمجابهتها وكذا التشريعات الضرورية في سبيل تحقيق ذلك[1] كما استعرض حلف الناتو قدراته التكنولوجية من خلال الهجوم السيبراني الذي تعرضت له استونيا عام 2007 أين تبنى سياسة عالية المستوى من حيث الدفاع وقام بإنشاء مركز للبحث المتقدم، كما قام بعقد المؤتمر الدولي للنزاعات المسلحة الدولية الرقمية والذي استعرض من خلاله عديد الموضوعات الأمنية التي كان أهمها ضرورة التصدي للإرهاب الالكتروني[2]

وسعيا إلى ضمان حماية امثل لاستخدامات التكنولوجيا وتوفير الأمن قد تم إنشاء الشبكة الأوروبية للأمن وامن المعلومات تحت تسمية ENISA عام 2004 طبقا لما نصت عليه لائحة الاتحاد الأوروبي رقم 460، ويشمل هيكلها مجموعة من ضباط الاتصال التابعيين للدول الأعضاء، وكذا مجموعة من الممثلين الدائمين لهذه الدول والتي أقرت بدورها عددا من الوثائق الأساسية لمكافحة الإرهاب السيبراني وكذا وضع مشروع الإستراتيجية الوطنية للأمن الرقمي داخل الاتحاد الأوروبي بالإضافة إلى تصميم مجموعة عالمية تحتوي على أهم التدريبات في سبيل تحقيق الأمن السيبراني.

هذا وقد تشارك كل من مركز الأقمار الصناعية التابع للاتحاد الأوروبي ووكالة الدفاع الأوروبية ومعهد الاتحاد الأوروبي للدراسات وظيفة حفظ الأمن داخل أوروبا من خلال بث روح التعاون القضائي في المسائل الجنائية من اجل مكافحة الجرائم الكبرى لاسيما تلك المتعلقة بقضايا الإرهاب والإرهاب الالكتروني وكذا تبادل الخبرات المكتسبة في سبيل تحقيق هذه الأهداف[3]

الفرع الثاني: جهود جامعة الدول العربية في التصدي للإرهاب الالكتروني:

إن جامعة الدول العربية لم تنص صراحة على جرائم الإرهاب وهذا ما هو ملاحظ من تفحص دستورها المتمثل أساسا في ميثاق الجامعة العربية، غير انه وبالرجوع للمادتين الثانية (2) والثالثة (3) منه نلمس رغبة المنظمة في تحقيق التكاتف بين الدول العربية بغية تحقيق

[1]– عبد الصبور عبد القوي "الجريمة الإلكترونية", دار العلوم للنشر والتوزيع ,مصر– 2008, ص 168.

[2]– إسحاق العشعاش, المرجع السابق, ص 196.

[3]– ناصر العلجة "الجهود الدولية في مكافحة الإرهاب الإلكتروني", المرجع السابق, ص 39

حماية الحقوق وضمان استمرارية السيادة، وهو ما ينطوي على نبذ التعرض لسلامة الدول والتحريض ضد الأنظمة باستعمال الوسائط التكنولوجية والسعي إلى إقرار وسائل التعاون مع الهيئات الدولية الأخرى من اجل كفالة السلم والأمن العربيين.

وقد توصلت هذه الجهود المبذولة إلى جملة من الحلول الأمنية والتي اقرها مجلس الوزراء الداخلية العرب، الذي أكد على ضرورة المحافظة على سلامة الوطن العربي والتصدي للمحاولات العدائية الإرهابية، وأهم ما توصل إليه العرب من خلال هذا المنبر هو إقرار قانون جزائي عربي موحد، كقانون نموذجي تضمن فصلا خاصا بالاعتداءات على حقوق الأشخاص باستعمال الوسائل التكنولوجية الحديثة وذلك بموجب القرار 229 الصادر عام 1996، مع النص بموجب المواد 461، 462، 463 منه على توفير الحماية للأسرار من خطر الهجمات الرقمية، وكيفية جمع المعلومات و الاطلاع عليها ومعاقبة الفاعلين فيها على عرقلة وإفساد الأنظمة المعلوماتية وقرصنة البيانات[1]

كما جاء في ظل الإستراتيجية العربية لمكافحة الإرهاب عام 1997 والتي أعربت عن اهتمام جامعة الدول العربية بمسائل الإرهاب والتي أقرت بدورها جملة من الاستراتيجيات الوطنية من اجل إحداث تعديلات جهة على التشريعات وتوظيف التكنولوجيا والوسائل الحديثة في تطوير الحماية الأمنية وضرورة المشاركة في المؤتمرات الدولية، وقد نظمت الخطة السادسة المقترحة لتنفيذ هذه الإستراتيجية ضرورة تفعيل الرقابة على الوسائل الإعلامية وكذا الشبكة المتطورة من طرف المكتب العربي للإعلام، وبذل الجهود المكثفة لمنع الاستغلال السلبي لمواقع التواصل الاجتماعي من طرف المنظمات الإرهابية.

وكذا ضرورة تصميم تشريع خاص بمكافحة الجرائم السيبرانية وتفعيل دور المساهمة العربية، في مجال مجابهة الإرهاب في هذا الصدد جاء إقرار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في عام 2010 والتي تضمن أهم صور الإرهاب الالكتروني، لاسيما في المادة 15 منها التي نصت على تجريم نشر أفكار التطرف وطرق صنع المتفجرات ونشر الفتنة والاعتداء على الديانات وحرية المعتقد، وألزمت هذه الأخيرة الدول

[1]– سامر عبد اللطيف مؤيد, نوري رشيد المالكي "دور المنظمات الدولية في مكافحة الإرهاب الرقمي", البحث المقدم بجامعة كربلاء, 2016, ص ص 24,25 – المادة الأولى والثانية من ميثاق جامعة الدول العربية.

الأطراف فيها على ضرورة تجريم كل ما من شانه تغذية جذور الإرهاب وتجفيف منابع نشر التطرف والفكر الجهادي التكفيري وكذا سلوكيات التشكيك في الديانات والفتأوى المغرضة سواء السمعية منها والبصرية أو تحقير الشعوب والديانات لأي تمييز كان، وكذا كل الأفعال والسلوكيات التي تعصف بحرية التدين والاعتقاد تحت المسميات الدينية أو السياسية.[1]

أما الصورة الثانية التي نصت عليها الاتفاقية فقد شملت تجريم تمويل الإرهاب والمنظمات الإرهابية وكذا التدريب عل ارتكاب الجرائم الإرهابية بواسطة التقنيات المعلوماتية ومنع تمويل الإرهاب سواء كان مصدر ذلك مشروعا كالجمعيات الخيرية وعمليات التبرع وسواء كن مصدرها غير مشروع كسرقة البنوك وتبيض الأموال وقرصنة بطاقات الائتمان وغيرها، وهو الفعل الذي عرفته الاتفاقية العربية لمكافحة جريمة غسيل الأموال وتمويل الإرهاب في2010 بأنه"جمع أو تقديم أو نقل الأموال بأي وسيلة مباشرة أو غير مباشرة لاستخدامها في أغراض إرهابية".

لان تقنية الأموال أصبحت أهم الوسائل المستعملة في التمويل الإرهابي،وكذا نصت على تجريم كل الأفعال التي تسهل الاتصال بين المنظمات الإرهابية،أما فيما يتعلق باليات المكافحة التي نصت عليها فقد تضمنت ضرورة الحفظ العاجل للبيانات المعلوماتية المخزنة والأمر بتسليمها،ويقتضي ذلك إن تكون هذه الأخيرة محمية بشكل امن من جميع المخاطر التي قد تؤدي إلى المساس بسلامتها وذلك بموجب المادة 23 من الاتفاقية والتي ألزمت بدورها الدول الأطراف باتخاذ الإجراءات التشريعية اللازمة من اجل التحقيق في الجرائم الإرهابية السيبرانية .

وكذا تفتيش المعلومات المخزنة وضبط المعلومات والبيانات،الأمر الذي يتيح إمكانية التوصل إلى أدلة ملموسة ومادية حول الجريمة والجمع الفوري للمعلومات وتتبع المستخدمين

[1]– توفيق مجاهد "جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010", مجلة العلوم القانونية والسياسية العدد 03, المجلد 09, ديسمبر 2018, ص ص 86,57.

واعتراض بيانات المحتوى وكذا ضرورة التعاون الدولي بخصوص تسليم المجرمين وتقديم المساعدة فيما بين الدول الأطراف.[1]

المطلب الثاني: آليات التصدي للإرهابي الالكتروني في الجزائر:

إن الجزائر .وبعد كل ما عانته من ويلات الإرهاب في العشرية السوداء،ونجاحها الباهض في تجفيف منابع الإرهاب،إلا أنها ليست بمنأى عن التطورات الجديدة الراهنة والمستحدثة في مجال الإجرام لاسيما الإرهاب الرقمي جعلها أكثر عرضة من سابقها للهجمات المحتملة من طرف الجماعات الإرهابية التي تهدف إلى إحباط معنويات المجتمع والجيش وإلحاق اكبر الخسائر المادية وإحداث الشلل التام في مختلف القطاعات الحيوية.

الفرع الأول: ميكانيزمات الجزائر في مواجهة الإرهاب الالكتروني :

لطالما عانت الدولة الجزائرية من نكسات الإرهاب ما جعلها تبادر إلى اجتماع دعت إليه خبراء منطقة الحوض المتوسط لمكافحة هذه الجريمةعام1998 بغية تحقيق فضاء متوسطي مستقر وامن وتقديم وثيقة تحتوي على مجموعة من المبادئ لمكافحة الإرهاب ودعم أواصر الشراكة السياسية والأمنية،وأهم هذه المبادئ التي حملتها هذه الوثيقة هي منع استعمال الوسائل التكنولوجيا والإعلام بغرض الدعاية للإرهاب[2]،كما اتخذت الجزائر جملة من الإجراءات ضد الجرائم الرقمية من اجل القيام بالتحقيقات الأزمة وحماية النظام العام ومقتضيات التحري وذلك وفقا لقانون الإجراءات الجزائية الجزائرية،مع وضع الآليات اللازمة للحجز والتفتيش والقيام بمراقبة الاتصالات الالكترونية[3]، وقد عمد المشرع الجزائري إلى استحداث مواد قانونية جديدة تمثلت أساسا في المواد من87مكرر إلى87مكرر 6 من قانون

[1]– توفيق مجاهد "جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010", المرجع السابق, ص ص 90,88

[2]– العربي العربي "التهديدات الأمنية اللاتماثلية في المجال المقاربي وأساليب المواجهة", بحث مقدم للمجلة الإفريقية للعلوم السياسية, قسم قضايا الأمن العسكري والسياسي. ص 2.

[3]– أمال بن صويلح "الهيئة الوطنية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خطوة هامة نحو مكافحة الإرهاب الإلكتروني", المرجع السابق, ص 4

العقوبات والتي أشارت بدورها إلى تجريم التحريض على القيام بأعمال إرهابية أو الانخراط في صفوفها[1].

كما عمدت إلى ممارسة عملية المراقبة من قبل الجهات المختصة فيما يتعلق بالوقاية من الأعمال الإرهابية وأفعال التخريب وكذا الجرائم الماسة بأمن المعلومات وامن الدولة.وذلك من خلال اتخاذ التدابير التقنية اللازمة والأغراض الموجهة لها بغية تجميع وتسجيل المعطيات ذات الصلة بالوقاية من الأفعال الإرهابية والاعتداء على سلامة وامن الدولة على نحو يهدد النظام العام أو مؤسسات الدفاع الوطني وكذا المؤسسات السياسية والاقتصادية[2].

كما عمدت الجزائر بناء على الاتفاقيات الدولية الثنائية وكذا المعاهدات ذات الصلة في إطار تنفيذ المساعدات الدولية القضائية المتبادلة فيما يتعلق بإجراءات التحري والتحقيق وإلقاء القبض وجمع الأدلة الخاصة بالجرائم الالكترونية ذات الطبيعة الإرهابية،كما بادرت الجزائر إلى المشاركة في فعاليات المؤتمرات والاجتماعات القائمة على تجريم ومنع استعمال الفضاء الرقمي في مجال الأعمال الإرهابية أو الدعائية لها من خلال المنصات الرقمية على غرار اتفاق الجزائر وباريس في عام 2008 الذي يهدف إلى دعم التعاون الأمني في سبيل تتبع الجرائم المعلوماتية بما في ذلك جرائم الإرهاب السبيراني الذي تديره الشبكات الإرهابية الجهادية،حيث استفادت هذه الجماعات الإرهابية من التقنيات المتطورة وسعت إلى استغلالها وتحقيق إغراضها التدميرية[3].

وهو ما دفع الجزائر إلى فرض قيود وضوابط على شبكة الانترنت من خلال تعديل القوانين السابقة وسن تشريعات جديدة وإنشاء جملة من الهيئات والمؤسسات التي تعمل في إطار التصدي إلى الإرهاب الالكتروني وذلك من خلال رفع كفاءات قوات الأمن في التصدي للإرهاب والجريمة وكذا الإرهاب الرقمي المستجد من خلال اجتماع 5+5 أو ما يعرف باجتماع دول غرب حوض المتوسط[4].

---

[1]– العشعاش إسحاق, المرجع السابق, ص 185.

[2]– أمال بن صويلح, المرجع السابق, ص 4.

[3]– توفيق شرقي, المرجع السابق, ص 55.

[4]– الأخضر عمر الدهيمي "دور مؤسسات المجتمع المدني في التصدي للإرهاب, التجربة الجزائرية في مكافحة الإرهاب", الطبعة الأولى, جامعة نايف للعلوم الأمنية, مركز الدراسات والبحوث, الرياض, ص ص 233,232

وتجدر الإشارة أن خصوصية الجرائم السبيرانية لاسيما تلك المتعلقة بجرائم الإرهاب تقتضي التأهيل وتدريب العاملين في جهاز التحري والتحقيق في هكذا نوع من الجرائم، وذلك كونها تعتمد على مهارات عالمية وتقنيات فنية في مجال تكنولوجيا الإعلام والاتصال وما تتميز به من سرعة فائقة وتقنيات متطورة في وسائل وأساليب ارتكاب الجرائم،وهو ما أدى إلى ظهور فجوة وفراغ تنظيمي بخصوص تلك الجرائم المستحدثة وتفاقم مدى خطورتها، والتي لا يمكن بأي حل من الأحوال إخضاعها للقواعد التقليدية الخاصة بقانون العقوبات وقانون الإجراءات الجزائرية[1]، وبناء على ما نصت عليه اتفاقية بودا بست للإجرام السيبراني في المادة 14 منها والتي أكدت على ضرورة إنشاء هياكل خاصة بالتصدي للجرائم السيبرانية نتيجة عجز أجهزة الضبط القضائي عن التحقيق فيها والكشف عن مرتكبيها،عمدت مختلف الأنظمة المقارنة ومن بينها الجزائر إلى إضفاء تعديلات جديدة على مستوى قوانينها الداخلية وكذا استحداث قوانين جديدة في إطار مكافحة الجريمة السيبرانية سعيا منها إلى استدراك الفراغ القانوني الذي أحدثته هذه الجرائم ولو نسبيا وعليه اصدر المشرع الجزائري القانون15-04 المتضمن تعديل قانون العقوبات وخصص القسم السابع مكرر منه للجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات،وقد تضمن 8مواد[2]،حيث نصت المواد من394 مكرر إلى 394 مكرر7 من قانون العقوبات والذي نظم القسم السابع مكرر والذي نظم العقوبات الطائلة للأفعال المجرمة الماسة بأنظمة المعالجة الآلية للمعطيات والتي صنفها المشرع الجزائري بطريقة تقنية ودون التعرض للأغراض التي تستهدفها،

غير أن المشرع ضاعف من هذه العقوبات في حال استهدافها للدفاع الوطني أو المؤسسات العمومية،وبالتالي يكفي ربط الغاية من ارتكاب هذه الجريمة بالوسيلة المعدة لذلك متى تم تكييف العمل الإرهابي في إطاره الافتراضي،كما أضاف المشرع تعديل آخر لقانون العقوبات بموجب القانون 16-02 الذي أضاف المادة 87 مكرر11 التي تعاقب كل جزائري أو أجنبي يرتكب أفعال إرهابية أو يشارك فيها أو يعمل على إدارة تنفيذها أو الإشراف على

[1]- حورية بن سيدهم "أمن الفضاء السيبراني, التحديات والحلول", المجلة الجزائرية للأمن الإنساني, العدد 02, المجلد 05, جامعة باتنة 1, 2020, ص ص 140,137.

[2]- بارة سمير "الأمن السبيراني في الجزائر, السياسات والمؤسسات", المجلة الجزائرية للأمن الإنساني, العدد 04, قاصدي مرباح, ورقلة, 2017 ص264.

التدريب عليها أو تلقيه لذلك باستخدام تكنولوجيا الإعلام والاتصال وذلك في الفقرة الثانية والثالثة من هذه المادة،كما أضاف تعديل المادة 87 مكرر 12 الذي نص على معاقبة كل من يستخدم تكنولوجيا الإعلام والاتصال في دعم الأعمال الإرهابية أو تنظيمها أو نشر أفكارها بطريقة مباشرة أو غير مباشرة أو كذا أو تجنيد الأشخاص لصالح جمعية أو تنظيم ذو أغراض إرهابية.

كما أدرج المشرع الجزائري بموجب المادة 65،51،41،40،37،16 ،15 من قانون الإجراءات الجزائرية للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب القانون 04-14،كما اصدر المرسوم التنفيذي06-384الذي وسع من الاختصاص الإقليمي للجهات القضائية بخصوص الجرائم المرتكبة في المواد السابقة،كما أضاف المشرع القانون 09-04 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والذي أضافت المادة15 منه إمكانية نظر المحاكم الجزائرية في الجرائم الواقعة الخارجة التراب الوطني والمستهدفة لمؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الوطنية[1]،كما استحدث المشرع الجزائري مجموعة من الأجهزة العملياتية التقنية المختصة من اجل تحقيق اكبر قدر من الأمن المعلوماتي.

لعل أبرزها إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وذلك بموجب المادة13 من القانون 09-04 التي نصت على انه "تنشا هيئة وطنية، وتنظيمها وسيرها عن طريق التنظيم" ،كما نصت المادة 14 من ذات القانون على مهام هذه الهيئة المتمثلة أساسا في الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال' وكذا مكافحتها من خلال التنسيق مع الهيئات المماثلة لها في الخارج، وتم بالفعل إنشاءها بموجب المرسوم الرئاسي 15-261 المؤرخ في2015، وتعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل، ثم تكليفها باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وكذا تقديم المساعدة للسلطات القضائية وكذا مصالح الشرطة القضائية من خلال جمع المعلومات والخبرة القضائية وضمان المراقبة الوقائية للاتصالات الرقمية قصد الكشف عن الجرائم

[1]-العشعاش إسحاق "الإرهاب السيبراني وتحديات الدولة, دراسة مقارنة" المرجع السابق, ص ص187,186

المتعلقة بالأعمال الإرهابية والتخريبية والمساس بامن الدولة[1]، كما تم في ذات السياق إنشاء مركز الوقاية من جرائم الإعلام الآلي التابع للدرك الوطني والذي يعتبر المركز الوحيد في الجزائر المختص في التصدي لجرائم تكنولوجيا المعلومات، تم إنشاءه في 2008، يقضي بتامين المنظومة المعلوماتية لخدمة الأمن العمومي، وهو يعمل على تحليل المعطيات والبيانات بخصوص الجرائم المعلوماتية.

وقد تم اعتباره بمثابة مركز للتوثيق وتحديد هوية مرتكبي الجرائم السيبرانية سواء كانوا أفراد أو عصابات، وهو يهدف إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من اجل مكافحة هذا النوع من الجرائم كما يعمل على وضع قوانين لتنظيم مجال استغلال المعلومة بالتنسيق مع وزارة العدل وكذا العمل على تطوير أساليب التعامل مع الجرائم من خلال المعهد الخاص بعلم الإجرام، وقد استطاعت قيادة الدرك الوطني بفضل التكوين المستمر والناجح لأفرادها وكذا تبادل الخبرات من توفير القوى المؤهلة من مهندسي الإعلام الآلي ورجال القانون في سبيل التصدي للجرائم الالكترونية لاسيما تلك المتعلقة بالإرهاب.

ولمزيد من الفعالية في مكافحة الإجرام بشتى أنواعه تم إنشاء المعهد الدولي للأدلة الجنائية بموجب المرسوم الرئاسي 133-04 والذي دخل حيز النفاذ في سنة 2009، وهو عبارة عن مؤسسة عمومية ذات طابع إداري تعمل تحت وصاية وزير الدفاع، ويضطلع المعهد بمهمة تكوين المورد البشري في إطار التحريات الأولية وإجراءات التحقيق القضائي وكذا اقتناء المعدات الضرورية لذلك، ويقوم بالعديد من المهام التي من شانها تلبية الطلبات الواردة من طرف السلطات القضائية وضباط الشرطة القضائية ويحتوي إلى جانب مصلحة البصمات على مصلحة مختصة بالإعلام الآلي، تعمل على رصد وتتبع عمليات الاختراق والقرصنة وتفكيك البرامج المعلوماتية ويتكون من 11 دائرة متخصصة[2]، وكذا التشكيل الأمني المختص للردع والوقاية من الجرائم السيبرانية أو ما يسمى بالشرطة الالكترونية وذلك من خلال إنشاء المصلحة المركزية للجريمة الالكترونية التابعة لمديرية الشرطة القضائية والتي كانت عبارة عن فصل امني متواجد على مستوى المديرية العامة للأمن الوطني، ثم تم

[1]- إدريس عطية :مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري" مجلة المصداقية, كلية الحقوق والعلوم السياسية, جامعة العربي التبسي, الجزائر, ص114.

[2]-رقية عواشرية "أمن القضاء السبيراني, التحديات والحلول", المجلة الجزائرية للأمن للإحسان, العدد 02, جامعة سطيف 2020 ص140.

دمج هذه التشكيلات سنة 2015 وإعادة تقسيمها إلى فصائل فرعية متوزعة على باقي الولايات[1].

إن تميز هذه الجرائم من ارتكابها واعتمادها على الوسائل الالكترونية وتميزها بالطابع التقني وكذا ارتكابها في بيئة غير مادية قد دفع المشرع سنة 2021 إلى إنشاء قطب جزائي متخصص وطنيا في مكافحة هذه الجرائم السيبرانية، وذلك من خلال الأمر 21-11 المعدل والمتمم لقانون الإجراءات الجزائية، وهذا القطب جاء في إطار تفعيل الجهاز القضائي ودعم قطاع العدالة للتمكن من متابعة هذه الجرائم مع وضع جملة من الأفكار المتعلقة باختصاصات هذا القطب، وقد جاء المشرع بتوسيع في مفهوم الجرائم التي تدخل ضمن اختصاص هذا القطب أين عرف الجريمة المعلوماتية في المادة 2 من قانون 04 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية."

أما القطب الجزائي فهو جهة قضائية مختصة بالنظر في بعض الجرائم التي حددها القانون ولا يمكن اعتبارها جهات قضائية خاصة تنشط بإجراءات قانونية مستقلة تخرج عن النظام القضائي ساري المفعول، وعليه يظهر القطب الجزائي كوسيلة لضمان فعالية الممارسة القطبية بخصوص الجرائم التكنولوجية، أما عن الاختصاص المحلي للقطب فبالرجوع إلى القانون 14-04 نجد أن المشرع قد عمد إلى تمديد الاختصاص المحلي لبعض المحاكم المذكورة على سبيل الحصر إلى دائرة اختصاص محاكم أخرى من خلال المرسوم التنفيذي 348-06 والتي تتعلق بالجرائم الخطيرة والمعقدة، وقد خص المشرع القطب الجزائي باختصاص محلي حسب المادة 329 من قانون الإجراءات الجزائية "تختص محليا بالنظر في الجنحة محكمة محل الجريمة أو محكمة محل إقامة احد المتهمين أو شركائهم أو محل إلقاء القبض عليهم، حتى لو كان هذا القبض لسبب آخر" كما وضح المشرع استثناء على هذا الاختصاص أين يجوز تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى إذا كانت الجرائم تتعلق بالجريمة المنظمة أو المخدرات أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم الإرهاب وتبييض الأموال، كما من

[1]- العشعاش إسحاق, المرجع السابق, ص188.

المشرع اختصاصا حصريا للقطب الجزائي فبما يتعلق بالجرائم المعقدة والخطيرة لاسيما تلك العابرة للحدود الجزائرية وذلك بموجب المادة 211 مكرر24 و211 مكرر25 لمكافحة أنحاء التراب الوطني[1].

تجدر الإشارة أن المشرع الجزائري لم ينص بصريح العبارة عن جريمة الإرهاب الإلكتروني، لكن بالنظر إلى القوانين المستحدثة في ظل الجرائم المعلوماتية وبما أن الإرهاب السيبراني يتم باستخدام تكنولوجيا المعلومات كما انه يعتبر من اخطر الجرائم فضلا عن خصوصيته العابرة للحدود الجزائرية وخطورته على النظام العام الوطني الداخلي فانه يفهم من فحوى المواد سالفة الذكر أنها جميعا تنطبق على جريمة الإرهاب الالكتروني كونها تنفذ بواسطة تكنولوجيا الإعلام والاتصال.

[1]– بن عميور أمينة, بوحلايس إلهام "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال", مجلة البحوث في العقود وقانون الأعمال ,العدد 01, المجلد 07, جامعة الإخوة منتوري, قسنطينة, الجزائر, 2022, ص ص75,74.

خاتمة:

إن العالم اليوم عرضة لهجمات إرهابية تستغل تكنولوجيا الإعلام والاتصال في بث الرعب ونشر الخوف والفزع،وإلحاق الضرر بشتى معالم الحياة،فالإرهاب السيبراني أصبح هاجسا يؤرق جميع الدول والشعوب،لاسيما وأن أغلب التنظيمات الإرهابية تسعى مؤخرا إلى إبراز صورتها في أذهان الجميع من خلال تطوير أساليب التنسيق في أعمالها واستقطاب الشباب للتجنيد في صفوفها وترويج العنف والتطرف واستهداف أهم المرافق الحيوية للدول،ومن هنا يأتي دور المنظمات الإقليمية والدول في التصدي لهذه الجرائم من خلال تطوير أنظمتها الوقائية والردعية وتكريس دور التعاون على كافة الأصعدة فيما بين الدول،لاسيما وأننا نعلم جيدا أنه ما من دولة تستطيع بمفردها النجاح في مواجهة هذه الأنماط والطفرات الإجرامية المستحدثة وخاصة الإرهاب الرقمي وعليه يجب السعي إلى سد الفراغات التنظيمية واستحداث الأساليب الجديدة للمواجهة خاصة وأن الإرهاب لا يتوقف عند هذا الحد فحسب بل يسعى إلى حياكة سيناريوهات جديدة قد تقضي مستقبلا على معالم الحياة على وجه الأرض .

النتائج:

من خلال الدراسة السابقة للموضوع نستخلص النتائج التالية:

- عدم وجود تعريف شامل وموحد لجريمة الإرهاب الالكتروني من الناحية الاصطلاحية بسبب تعدد واختلاط الآراء والاتجاهات بين المتخصصين والفقهاء وبين الدول نظرا لتضارب المصالح فما ينظر إليه البعض على أنه جريمة إرهابية، قد يراه البعض الآخر أفعالا مشروعة ومباحة.
- تعدد الأسباب المؤدية لجريمة الإرهاب السيبراني وتنوع مظاهر استخدام للقوة الالكترونية من أجل ترويج أفكار العنف والتطرف وبث الرعب والخوف وتطور الجرائم المترتبة عنه،وكذا عمق وفضاعة الآثار الناجمة عنه والتي لا يمكن بأي حال من الأحوال جبرها أو الحد من انتشارها .

- الفرق الجوهري بين الإرهاب التقليدي والإرهاب السيبراني يكمن من حيث الوسيلة المستعملة في تنفيذ المخططات وشن الهجمات والمعبر عنها بتكنولوجيا الإعلام والاتصال .
- بالرغم من وجود عدة محاولات دولية وإقليمية ووطنية لوضع اتفاقيات تجرم وتكافح الإرهاب الرقمي إلا أنها بقيت قاصرة عن مواجهته بالقدر الكافي نظرا للفراغ التنظيمي،وعجز اغلب دول العالم عن مواكبة تطور أساليب الإجرام الإرهابي .
- غياب جهة الرقابة والسيطرة على القطاعات الالكترونية ما أدى إلى استفحال الجرائم الرقمية وتعدد أنواعها والتي تعمل على توظيف الشبكة المعلوماتية لخدمة أغراضها الخفية،فضلا عن خصوصيته العابرة للحدود والقارات .
- عدم نجاعة وفعالية أغلب القوانين والإجراءات المستحدثة في مجال مكافحة الإرهاب السيبراني نظرا لما تمتاز به هذه الجريمة من مرونة في تغيير أساليبها وسرعة انتشارها .
- بالرغم من الاختصاص المنوط بالأجهزة العالمية الكبرى لاسيما مجلس الأمن في مجال حفظ السلم والأمن العالميين إلا أنه ينسحب فيما يتعلق بجريمة الإرهاب الالكتروني خاصة أنها من أخطر وأفضع الجرائم المهددة لمبادئه التي يعمل على حمايتها .
- جريمة الإرهاب الالكتروني من أكبر مهددات الأمن القومي الداخلي في جميع دول العالم والتي تعمل على إضعاف الاستراتجيات الدفاعية الوطنية .
- استحالة وضع خرائط عملية توضح مواطن تمركز الجماعات الإرهابية بدقة بسبب إمكانية التلاعب ببرامج تغيير المواقع والإحداثيات من طرف التنظيمات الإرهابية .

التوصيات :

- تحديد تعريف شامل وموحد من الناحية الاصطلاحية لجريمة الإرهاب السيبراني .
- التوعية والتحذير من مخاطر الإرهاب الالكتروني .
- ضرورة سعي الدول إلى تطوير القدرات الدفاعية العسكرية والقانونية من الناحية التكنولوجية،وتأسيس وحدات للأمن الرقمي وتزويدها بالموارد البشرية والتقنية اللازمة .
- تعزيز الجهود الدولية والعمل على تحقيق التعاون والتنسيق وإبرام الاتفاقيات الثنائية، والمعاهدات الدولية الشاملة لجميع أشكال وصور الإرهاب السيبراني وتبادل الخبرات القضائية وتدريب رجال العدالة .

- مساهمة الدول الرائدة والمتطورة في تنظيم دورات تدريبية في المجال الفني والتقني من أجل مساعدة باقي الدول على التصدي للجرائم الرقمية لاسيما تلك المتعلقة بالإرهاب .
- ضرورة لجوء المشرع الجزائري إلى اعتماد الإطار القانوني المناسب وفصل تجريم الإرهاب الالكتروني عن تجريم الإرهاب التقليدي والجريمة الالكترونية، ووضع الإجراءات الجنائية الخاصة به لاسيما بعد فشل الإجراءات التقليدية، واستحداث نصوص قانونية شاملة وواضحة ومرنة قابلة للتطور والتغيير بما يتناسب مع النمط السريع للجرائم الالكترونية خاصة الإرهاب السيبراني .
- العمل على إخضاع المعاملات الالكترونية للأحكام القانونية من أجل تجفيف منابع الإجرام والإرهاب .
- رصد وتتبع النشاطات الإرهابية على مستوى الشبكة الرقمية العالمية وتدميرها ودراسة الإرهاب السيبراني بعمق وجدية في المراكز البحثية وتنظيم المؤتمرات العلمية وإيجاد الحلول الناجعة،وتشكيل فرق مختصة للتواصل مع الجهات الأمنية والتنسيق معها .
- العمل على حل النزاعات الدولية والإقليمية التي تعتبر عنصر مغذي للجماعات والمنظمات الإرهابية التي تستعمل ستار حركات التحرر من أجل تحقيق أغراضها الإرهابية لاسيما بسبب ما تكتسيه هذه الظاهرة من طابع متجاوز للحدود وعابر للقارات .

قائمة المصادر والمراجع

أولا: القوانين.

1. القانون 09 – 04 المؤرخ في 5 أوت 2003 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها،الجريدة الرسمية،العدد 47.

2. الأمر 66 – 156 الصادر في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الجزائري،الجريدة الرسمية،العدد 48.

3. المرسوم الرئاسي 15 – 261 المؤرخ في 8 أكتوبر 2015،الجريدة الرسمية،العدد 53 المحدد لتشكيله وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

4. الأمر 66 – 156 الصادر في 8 يونيو المتضمن قانون العقوبات،الجريدة الرسمية،العدد 49.

ثانيا: الكتب.

1. أحمد محمد عبد الرؤوف المنيفي "فيروسات الحاسب الآلي ".

2. الأخضر عمر الدهيمي "دور مؤسسات المجتمع المدني في التصدي للإرهاب،التجربة الجزائرية في مكافحة الإرهاب"،الطبعة الأولى،جامعة نايف للعلوم الأمنية،مركز الدراسات والبحوث،الرياض.

3. بن سالم إيمان "جريمة التجنيد الالكتروني للإرهاب وفق قانون العقوبات الجزائري"،الطبعة الأولى،المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية،برلين،2018.

4. بن يحي الطاهر ناعوس "مكافحة الإرهاب الالكتروني ضرورة بشرية وفريضة شرعية".

5. جعفر حسن جاسم الطائي "جرائم تكنولوجيا المعلومات الجديدة للجريمة الحديثة"،دار البداية،عمان،2017.

6. حسنين شفيق "الإعلام الجديد والجرائم الالكترونية– التسريبات والتجسس الالكتروني والإرهاب"،الطبعة الأولى،دار فكر وفن للطباعة والنشر والتوزيع،2015.

7. هدى حامد قشقوش "جرائم الحاسب الالكتروني في التشريع المقارن"،الطبعة الأولى،دار النهضة العربية،مصر،2000.

8. محمد أمين الشوابكة "جرائم الحاسوب والانترنت- الجريمة المعلوماتية"،الطبعة الأولى،دار الثقافة للنشر والتوزيع،الأردن،2009.

9. منير محمد الجنيبي "جرائم الانترنت والحاسوب الآلي ووسائل مكافحتها"،دار الفكر الجامعي،الإسكندرية،2015.

10. محمد عبيد الكعيبي "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت"،الطبعة الثانية،دار النهضة العربية،القاهرة،2009.

11. علي جعفر "جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة- دراسة مقارنة"،الطبعة الأولى،مكتبة زين الحقوقية والأدبية،لبنان،2003.

12. عبد العزيز صقر الغامدي "الإرهاب والعولمة"،أكاديمية نايف للعلوم الأمنية،مركز الدراسات والبحوث،الرياض،2002.

13. عبد الوهاب الكيالي "الموسوعة السياسية"،المؤسسة العربية للدراسات والنشر ،بيروت،1954.

14. عبد الصبور عبد القوي "الجريمة الالكترونية"،دار العلوم للنشر والتوزيع،مصر ،2008.

15. ربيع محمود الصغير "القصد الجنائي في الجرائم المتعلقة بالانترنت والمعلوماتية"،دراسة مقارنة،الطبعة الأولى،مركز الدراسات العربية للنشر والتوزيع،مصر ،2017.

16. شفيق نوران "أثر التهديدات الالكترونية على العلاقات الدولية"،الطبعة الأولى،المكتب العربي للمعارف،مصر ،2015.

17. طارق عزت رخاء "المنظمات الدولية المعاصرة"،الطبعة الأولى،دار النهضة العربية،مصر ،2006.

المجلات والملتقيات والمداخلات:

1. الكر محمد بن مرزوق عنترة "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"،مجلة العلوم الإنسانية والاجتماعية،العدد 38،2018.

2. إدريس عطية "مكانة الأمن السبيراني – التحديات والحلول"،المجلة الجزائرية للأمن الإنساني،جامعة سطيف،العدد 02،مجلد 05،2020.

3. بن مرزوق عنترة "جريمة الإرهاب الالكتروني- الأسباب وآليات العلاج"،مجلة الحقوق والعلوم الإنسانية،جامعة مسيلة،العدد 02،المجلد 11،2018.

4. بن صويلح أمال "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام"،الملتقى الدولي حول الجرائم السبيرانية،خطوة عامة نحو مكافحة الإرهاب الالكتروني،جامعة 08 ماي،2017.

5. بارة سمير "الأمن السبيراني"،جامعة قاصدي مرباح،ورقلة،العدد 04،2017.

6. بن عميور أمينة "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،مجلة البحوث في العقود وقانون الأعمال،جامعة الإخوة منتوري قسنطينة،العدد الأول،2022.

7. توفيق مجاهد "جريمة الإرهاب الالكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010"،مجلة العلوم القانونية والسياسية،العدد 03،2018.

8. جمال بوزايدة،"الإستراتيجية الجزائرية في مواجهة الجرائم السبيرانية"،مجلة العلوم القانونية والسياسية،العدد الأول،2022..

9. خليل عبد الله حسين "الإرهاب الالكتروني- المفهوم والمخاطر"،ورقة مقدمة لمؤتمر الإرهاب الالكتروني،معهد التنمية الإدارية،مصر ،2016.

10. وفاء لطفي حسين عبد الواحد "الإرهاب الالكتروني والأمن القومي في ظل جائحة كوفيد19 ".

11. رافعي ربيع "الإرهاب وعلاقته بالجريمة المنظمة – الإرهاب الالكتروني نموذجا"،مجلة القانون والعلوم السياسية،العدد الأول،2021.

12. غريب حكيم،شرقي صبرينة "تداعيات الحرب الالكترونية على العلاقات الدولية- دراسة في الهجوم الالكتروني على إيران (فيروس ستكنست).

13. سعيد عبيدي "الإرهاب الالكتروني"،مجلة العلوم الإنسانية،العدد 02،2017.

14. مايا حسين ملا خاطر "الإطار القانوني لجريمة الإرهاب"،مجلة جامعة النصر ،2016.

15. محمود أديب فتاح آغا الكاكة "اختصاصات مجلس الأمن في التصدي للإرهاب الدولي الالكتروني"،مجلة دراسات علوم الشريعة والقانون،العدد الأول.

16. حورية بن سيدهم "أمن الفضاء السبيراني- التحديات والحلول"،المجلة الجزائرية للأمن الإنساني"،العدد 02،2020.

17. رقية عواشرية "أمن الفضاء السبيراني – التحديات والحلول"،المجلة الجزائرية للأمن الإنساني،العدد 02.

18. علي جاسم محمد التميمي "الإرهاب الالكتروني وأثره على المجتمع"،المجلة السياسية،جامعة النهرين،العراق.

19. عبد الرحمان عوض رجا ملاحة،فتيحة عمارة "جريمة الإرهاب المعلوماتي- أساباه وأساليبه"،مجلة جامعة الأمير عبد القادر،العدد الأول،2020.

20. جدي وفاء "الإرهاب الالكتروني- أسبابه بين النص والتطبيق"،مجلة مقاربات،العدد 05،2015.

21. لورنس سعيد حوامدة "الجرائم المعلوماتية- أركانها وآليات مكافحتها"،مجلة الميزان للدراسات الإسلامية والقانونية،العدد 03،2017.

22. عبد القادر الشيخلي "طبيعة الإرهاب الالكتروني"،المؤتمر الإسلامي العالمي لمكافحة الإرهاب،السعودية،2015.

23. ياسمين أحمد صالح "الإرهاب في ظل أزمة كورونا"،مجلة كلية السياسة والاقتصاد،العدد 09،2021.

24. شعبي صابرة "الإرهاب الالكتروني- الأشكال والدوافع"،مجلة العلوم الإنسانية والاجتماعية،العدد 10.

25. شرقي صبرينة،غريب حكيم "الإرهاب الالكتروني والتحول في مفهوم القوة"،مجلة الباحث للدراسات الأكاديمية،العدد 02،2020.

26. نورة بلعبيدي "توظيف تنظيم الدولة الإسلامية للأنظمة الاتصالاتية الرقمية في استراتجياته الإرهابية"،المدرسة الوطنية العليا للعلوم السياسية .

27. وهيبة يشرف "مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الالكتروني في ظل المجتمع المعلوماتي"،جامعة باتنة .

28. سارة بوحادة "مداخلة حول أثر الإرهاب الالكتروني على أمن واستقرار الدول"،المدرسة الوطنية العليا للعلوم السياسية،الجزائر .

29. ناصر العلي "الجهود الدولية في مكافحة الإرهاب الالكتروني"،مجلة الباحث للدراسات الأكاديمية،العدد الأول،2018.

30. بوزيد مختاري "الملتقى الوطني لآليات مكافحة الجرائم الالكترونية في التشريع الجزائري"،2017.

ربعا: المذكرات والرسائل العلمية والبحوث.

1. إسراء طارق جواد كاظم "جريمة الإرهاب الالكتروني– دراسة مقارنة"،رسالة من متطلبات نيل شهادة الماجستير في القانون العام،كلية الحقوق،جامعة النهرين،العراق

2. ضيف مفيدة "سياسة المشرع في مواجهة ظاهرة الإرهاب "،مذكرة لنيل شهادة الماجستير في قانون العقوبات والعلوم الجنائية،جامعة الإخوة منتوري، قسنطينة .

3. مصطفى سعد محمد مخلف "جريمة الإرهاب عبر الوسائل الالكترونية "،مذكرة لنيل شهادة الماجستير ،تخصص قانون عام،جامعة الشرق الأوسط،2017.

4. توفيق شريخي "الإرهاب الالكتروني وتأثيره على أمن الدولة "،مذكرة لنيل شهادة ماستر أكاديمي في العلوم السياسية،تخصص إستراتجية وعلاقات دولية،جامعة مسيلة .

5. جرلال زهرة،غلاف كريمة "جريمة الإرهاب الالكتروني "،مذكرة لنيل شهادة ماستر أكاديمي في الحقوق،تخصص قانون جنائي،جامعة عبد الرحمان ميرة،2019.

6. مهني محمد "تأثير الإرهاب الالكتروني على تغيير مفهوم القوة في العلاقات الدولية "،مذكرة لنيل شهادة ماستر أكاديمي في العلوم السياسية والعلاقات الدولية،جامعة مسيلة،2018.

7. العربي العربي "التهديدات الأمنية اللاتماثلية في المجال المقاربي وأساليب المواجهة"،بحث مقدم للمجلة الإفريقية للعلوم السياسية،قسم قضايا الأمن العسكري والسياسي .

8. سامر مؤيد عبد اللطيف،نوري رشيد المالكي "دور المنظمات الدولية في مكافحة الإرهاب الرقمي"،بحث مقدم بجامعة كربلاء،2016.

المراجع باللغة الأجنبية:

1. Utilization de l'internet ades fins terrorists' united national office on Drngs and crème .
2. Dennis. Murpry, information opération primer, 1st education carlish U.5.Armu War Colleu .USA.2010..

الفهرس:

الملخص

إن التكنولوجيا المتطورة أصبحت جزء لا يتجزأ من الحياة اليومية واجتاحت اغلب مجالات الحياة لما تتميز به من فوائد وتسهيلات, غير أن الاستخدامات السلبية للشبكة المعلوماتية والأجهزة الحديثة لاسيما من طرف العصابات الإجرامية والمنظمات الإرهابية سأهم في ظهور أنواع جديدة من الجرائم الرقمية, لعل أخطرها وأبرزها جريمة الإرهاب الالكتروني التي تعتبر أسرع الجرائم انتشارا وأكثرها فتكا بالأشخاص والحكومات, الأمر الذي دفع بالعديد من المظلمات العالمية والإقليمية إلى إبرام معاهدات واتفاقيات تهدف إلى مكافحة هذه الجريمة, كما عمد المشرع الجزائري في ذات السياق إلى استحداث مجموعة من الهيئات والقوانين المتعلقة بجرائم تكنولوجيا الإعلام والاتصال أبرزها القانون 09_04 وكذا القطب الجزائي السيبراني المتخصص, وكل ذلك جاء من اجل التصدي لجريمة الإرهاب السيبراني والعمل على الحد من مخاطره وتفادي السيناريوهات القادمة المنبئة عن أخطار عظيمة.

Abstract:

Advanced technology has become an integral part of everyday life and has conquered reas of life due to the advantages and facilities it offers. However, the negative uses of the information network and modern devices, in particular by criminal gangs and terrorist organizations, have contributed to the emergence of many cyber-crimes, such as cyber-terrorism, one of the most dangerous and important crime which is considered to be one of the fastest growing and deadliest crimes for people and governments. Thus, many global and regional organizations have been pushed to sign agreements and conventions aimed at combating this crime. In addition, the Algerian legislator proceeded, in the same context, to the creation of a set of bodies and laws relating to crimes of information and communication technologies including law 09/04 as well as the specialized cybercrime pole with the aim of combating cyberterrorism and attempting to limit its dangers in order to avoid future scenarios that predict great dangers.

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي: جامعة محمد بوضياف - المسيلة -

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): قلمين حوله ..... الصفة: طالب، أستاذ، باحث ..... طالب .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: 206693448 والصادرة بتاريخ 04 - 05 - 2021

المسجل(ة) بكلية / معهد كلية الحقوق قسم القانون الجنائي

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: الإرهاب الإلكتروني .....

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 2022/06/09

توقيع المعني (ة)

شوهد على التوقيع
بالجزائر في: 09 جوان 2022
رئيس المجلس الشعبي البلدي
وتفويض منه المتصرف الاقليمي
عمري فيصل

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
inistry of Higher Education and Scientific Research
جامعة محمد بوضياف – المسيلة
Mohammed Boudiaf University - M'sila
Faculty of Law and Political Science
كلية الحقوق والعلوم السياسية

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

القسم: الحقوق

الصورة

استمارة معلومات

- **المعلومات الشخصية:**

اللقب والاسم: قلمين حولة

Nom et prénom :

تاريخ الازدياد: 21 نوفمبر 1998 مكان الازدياد: حمام الضلعة المسيلة

اسم الأب: الطاهر اسم ولقب الأم: لحلي نوارة

الحالة العائلية: عزباء العنوان الشخصي: الحي القديم - حمام الضلعة المسيلة

الهاتف: 06.75.54.34.86 البريد الإلكتروني: marlinoyou06@gmail.com

رقم التسجيل: 171735087724

سنة أول تسجيل: 2021/2020

سنة نهاية الدراسة: 2022/2021

- **شهادة الباكالوريا:**

المعدل: 10.17 الشعبة / التخصص: علوم تجريبية سنة: 2017

- **شهادة الليسانس:**

التخصص: قانون عام سنة التخرج: 2020

- **شهادة الماستر:**

التخصص: قانون جنائي سنة التخرج: 2022

- **الوضعية المهنية:**

موظف/ عامل ☐ وظيف عمومي ☐ قطاع خاص ☐ عاطل عن العمل ☒

الهيئة المستخدمة: / اسم المؤسسة: /

الرتبة في العمل: /

صيغة العمل : دائم ☐ في إطار العقود ☐ نوع العقد

إمضاء الطالب (ة)