وزرة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي برج بوعريريج
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لإستكمال متطلبات لنيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون إعلام آلي

الموسومة بـ:

الإرهاب الالكتروني

(التحديات والمواجهة)

من إعداد الطلبة:

- **قاسمي رحمة**
- **بوخروبة كريمة**

تحت إشراف الأستاذ

ميهوب يزيد

- **لجنة المناقشة:**

الإسم واللقب	الرتبة	الصفة
عياش حمزة	أستاذ محاضر "أ"	رئيسا
ميهوب يزيد	أستاذ محاضر "أ"	مشرفا ومقررا
خلفة سمير	أستاذ محاضر "أ"	ممتحنا

السنة الجامعية: 2022/2021

﴿... يَرْفَعِ اللهُ الذِينَ آَمَنُوا مِنْكُمْ

وَالذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ...﴾

[المجادلة: 11]

شكر وعرفان

بسم الله الرحمن الرحيم , و الصلاة و السلام على أشرف الخلق سيدنا محمد وعلى اله و صحبه أجمعين.

نحمد الله عز وجل الذي وفقنا لإتمام هذا العمل

" اللهم لك الحمد حتى ترضى و لك الحمد اذا رضيت ولك الحمد بعد الرضا "

نشكر الأستاذ الفضيل "ميهوب يزيد" الذي تكرم بكل تواضع قبول الاشراف على مذكرة تخرجنا فكان له فضل كبير علينا بعد كل النصائح و الارشادات و التوجيهات التي أضاء لنا بها الطريق

أسأل الله أن يوفيك أجر الجهد المبذول في سبيل نشر العلم

نشكر كل من ساهم في مساعدتنا في انجاز هذا العمل من قريب او من بعيد.

إهداء

قال الله تعالى " وقضى ربك ألا تعبدوا الا إياه و بالوالدين احسانا " صدق الله العظيم

إلى التي الجنة تحت أقدامها الى التي حملتني وهنا على وهن و ساندتني منذ صغري و دعمتني في كامل مشوار حياتي حتى وصلت الى ما أنا عليه اليوم أمي اللهم احفظها لنا .

الى أبي جنتي و عزتي و سندي بعد الله الى من كان سببا في ثمرة عملي هذا أطال الله في عمره .

الى أخي الوحيد و ضلعي الثابت وفقه الله

الى أمي الثانية عمتي التي لا طالما دعمتني حفظها الله

الى كامل أقربائي و صديقاتي أدامكم الله

الى أساتذتي الذين رافقوني و علموني منذ الصغر جزاكم الله خيرا

اللهم أدم علينا نعمة الأمن والسلام

كريمة

إهداء

قال الله تعالى " واخفض لهما جناح الذل من الرحمة

وقل ربي ارحمهما كما ربياني صغيرا "

صدق الله العظيم

أهدي ثمرة جهدي:

مثلي الأعلى , وسندي بعد الله التي لا طالما رافقتني منذ الصغر في كل خطوة كنت أخطوها نحو مستقبلي تلك التي أعجز عن إيجاد وصف يليق بها..... أمي الحبيبة حفظها الله لنا.

الى ضلعي الثابت الذي لا يميل، و ملجئي و مأمني أبي رزقه الله العافية

إلى اخوتي قوتي و عوني من بعد الله

الى كل أقاربي و صديقاتي و زملائي في الدراسة، أدامكم الله

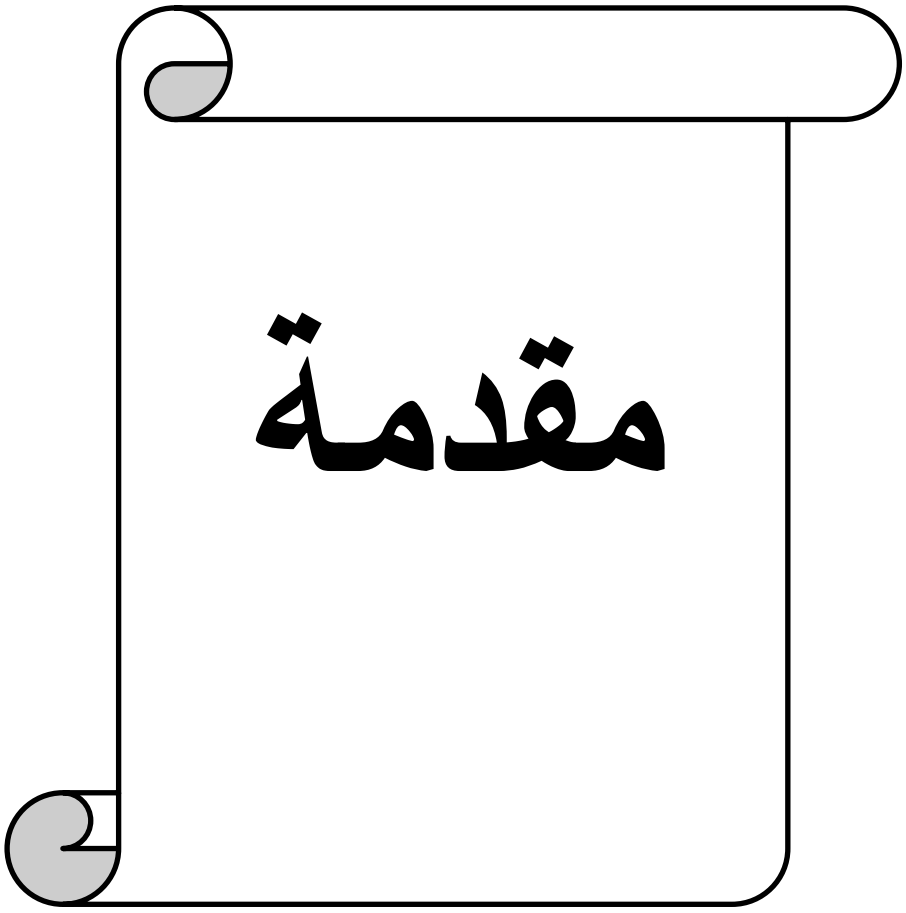
الى كل الأساتذة الأفاضل الذين ساهموا في تدريسي

ووصولي لهذه المرحلة جزاكم الله خيرا

اللهم احفظ بلدي " الجزائر "

واحفظ اخواني وأخواتي في فلسطين نصركم الله

رحمة


مقدمة

مقدمة

لقد شهدت السنوات الأخيرة تطورا رهيبا في شتى المجالات وهذا نتيجة لثورة تكنولوجيا المعلومات فهذه الثورة الجديدة التي تقوم على المعرفة والمعلومات قد مست أيضا المجال الإجرامي الذي تطور بشكل ملحوظ حيث أصبحت الإنترنت والحواسيب الآلية وسيلة لنشر النشاط الإجرامي وتنفيذه.

ومن بين هذه الجرائم الإرهاب الالكتروني الذي يعتبر من أخطر وأبشع الجرائم التي ترتكب عن طريق الانترنت فهو يشكل تهديدا للعالم من خلال إنشاء حسابات خاصة بالإرهابيين بهدف التواصل بينهم ونشر الخوف والهلع بين الناس ولتحقيق العديد من الأغراض الإرهابية الأخرى.

ونظرا للانتشار السريع لهذه الجريمة كان لابد على الدول والمنظمات أن تلتفت لها وتعيرها قدرا كبيرا من الاهتمام وذلك بسن تشريعات وقوانين للتصدي لها والحد منها.

إن الإرهاب الالكتروني قد فاق خطورة الإرهاب التقليدي لأنه عابر للحدود الإقليمية وأسبابه في الغالب ما تكون سياسية أو دينية كما أن الخطر الذي يلحقه بالأفراد والمجتمعات كبير جدا ويتحقق بسرعة كبيرة، لأنه وبكل بساطة ينجز بواسطة وسائل الكترونية وأسلحة رقمية متطورة.

وتكمن أهمية دراسة هذا الموضوع في كونه موضوع جديد فهو يعبر عن الإرهاب لكن بالطريقة المعاصرة، حيث أنه يرتبط ارتباطا وثيقا بتقنية المعلومات ومن المهم التطرق والتعرف عليه من أجل تحذير الفئات التي يستهدفها وإعلامهم بالمخاطر التي تنجم عنه خاصة أنه يتميز بسرعة الانتشار وعبوره للحدود الإقليمية.

وتهدف هذه الدراسة إلى التعريف بموضوع الإرهاب الالكتروني وتميزه عن الإرهاب العادي وباقي الجرائم الأخرى المشابهة له، وتهدف أيضا إلى التنبيه من مخاطر الإرهاب الالكتروني وذلك بتوعية الأفراد والمجتمعات منه عن طريق ذكر مختلف التهديدات التي يشكلها ومختلف الجهود التي تبنتها الدول والمنظمات للتصدي له.

وقد دفعنا إلى اختيار هذا الموضوع أسباب شخصية نظرا لارتباطه بمجال دراستنا كطلبة في تخصص قانون الإعلام الآلي والإنترنت إذ كان لابد من التطرق إلى موضوع الإرهاب باستعمال الشبكة المعلوماتية، ومن بين الأسباب الذاتية أيضا هو كونه موضوع جديد على الساحة الإجرامية ومن المهم تسليط الضوء عليه أما فيما يخص الأسباب الموضوعية هو الإلمام بجميع الجوانب التي تعرفنا بهذا الموضوع والإحاطة بالدوافع التي تؤدي إلى إرتكابه، وما مدى مساهمة مختلف الآليات والجهود المبذولة في مكافحة الإرهاب الالكتروني.

ومما سبق لنا ذكره توصلنا إلى طرح الإشكالية التالية:

ما هي التحديات التي يطرحها الإرهاب الالكتروني على الساحة الدولية ؟

وتتفرع هذه الإشكالية العامة لأسئلة جزئية:

- ما مفهوم الإرهاب الالكتروني ؟
- ما هي أركان التي يقوم عليها الإرهاب الالكتروني ؟
- كيف تم التصدي لمواجهة الإرهاب الالكتروني على المستوى الدولي و الوطني ؟

وللإجابة على هذه الإشكالية اتبعنا المنهج الوصفي الذي قمنا من خلاله بوصف جريمة الإرهاب الالكتروني عن طريق التوصل إلى بعض التعريفات الخاصة به وذكر ما يميزه عن المصطلحات المشابهة له، كما دعمناه بالمنهج التحليلي وذلك بذكر المواد التي خصصت لهذه الجريمة.

أما فيما يخص الصعوبات التي واجهناها تشعب الموضوع وصعوبة الإلمام بمختلف جوانبه فضلا على اختلاط الأبعاد السياسية مع المقاربات القانونية للموضوع الذي التزامنا بالتركيز على الجوانب القانونية وقد انعكس ذلك حتى على مستوى المادة العلمية للبحث، بحيث وجدنا صعوبة كبيرة في إيجاد المراجع التي تتركز على الجوانب القانونية المحصنة وقد قمنا بتقسيم الخطة إلى فصلين.

الفصل الأول: تناولنا فيه ماهية الإرهاب الالكتروني وقمنا بتجزئته إلى (المبحث الأول) الإطار المفاهيمي للإرهاب الالكتروني و(المبحث الثاني) أركان الإرهاب الالكتروني.

الفصل الثاني: تناولنا فيه من خلال (المبحث الأول) مكافحة الإرهاب الالكتروني على المستوى الدولي (المبحث الثاني) الجهود الوطنية لمكافحة الإرهاب الالكتروني.

الفصل الأول:

ماهية الإرهاب الالكتروني

إن التطور الذي يشهده العالم في السنوات الأخيرة، يعود فضله للقفزة النوعية الحاصلة في مجال وسائل الاتصال والانترنت التي تطورت بشكل ملحوظ وهذا التطور مس حتى الجرائم التي ازدادت انتشار وخطورة ومن بين هذه الأخيرة (الجرائم) الإرهاب الالكتروني الذي يعتمد بدوره على شبكة الانترنت، وقد ظهرت العديد من التعريفات لهذه الجريمة وكان لابد من تمييزها عن المفاهيم المشابهة لها، والتعرف على أسبابها ومخاطرها التي تعددت دون أن ننسى مختلف الأركان التي يقوم عليها الإرهاب باستخدام الوسائل الالكترونية.

وبما أن الإرهاب الالكتروني هو من الجرائم الحديثة التي اتخذ مجرميها الشبكة المعلوماتية والانترنت وسيلة لتطبيقه، ومن أجل بث الرعب ونشر الخوف بين الناس والكثير من الأفعال الأخرى لذا كان من الضروري تخصيص هذا الفصل من أجل تحديد مفهوم الإرهاب الالكتروني وقد قمنا بتقسيمه لمبحثين المبحث الأول خصصناه للإطار المفاهيمي للإرهاب الالكتروني والمبحث الثاني الذي تطرقنا فيه إلى أركانه.

المبحث الأول: الإطار المفاهيمي للإرهاب الالكتروني

الإرهاب الالكتروني مصطلح جديد ظهر نتيجة التطور الحاصل في مجال وسائل الاتصال ويصنف ضمن الجرائم العصرية لأنه يتصل بشبكة الانترنت ويتم بوسائل متطورة وهو عابر للحدود الوطنية لذا وجب علينا التطرق لتعريفه وتبيان كل من أسبابه ومختلف مخاطره وأركانه.

المطلب الأول: مفهوم الإرهاب الالكتروني

من أجل تقديم تعريف للإرهاب الالكتروني لا بد أولا من اللجوء إلى تحديد معنى الإرهاب لأنه من المفاهيم الغامضة التي لا يمكن تحديدها بسهولة والتعرف عليه يسهل علينا الوصول إلى تحديد معنى الإرهاب الالكتروني إضافة للتعرف على أهم خصائصه وأهدافه وفصله عن المفاهيم المشابهة له.

الفرع الأول: تعريف الإرهاب الالكتروني

سوف نتطرق في هذا الفرع إلى تعريف الإرهاب العادي والالكتروني

أولا: تعريف الإرهاب العادي:

سوف نتناول فيه المدلول اللغوي إضافة إلى بعض التعاريف الاصطلاحية وتعريفه حسب المشرع الجزائري.

الإرهاب مأخوذ من رهب بالكسر يرهب رهبة رهبا وهو بمعنى خاف مع تحرر واضطراب وترهبه بمعنى توعده والإرهاب بكسر الهمزة بمعنى الإزعاج والإخافة واسترعبه بمعنى أخافه وفزعه والرهبة تعني طول الخوف واستمراره لأنه يديم الخوف،[1] وفي قوله تعالى "واسترهبوهم وجاءوا بسحر عظيم 115" أي استدعوا رهبتهم وارهبوهم والرهبة

[1]– هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، دار الكتب العلمية للنشر، لبنان 2005، ص22.

الخوف،[1] وفي قوله تعالى "واعدوا لهم ما استطعتم من قوة و من رباط الخيل ترهبون به عدو الله وعدوكم 60 "،[2] هذه التعريفات هي معنى الإرهاب في اللغة.

أما في الاصطلاح فلقد تعددت تعاريف الإرهاب الالكتروني فمجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي بأنه العدوان الذي يمارسه أفراد أو جماعات أو دول بغيا على الإنسان في دينه أو دمه أو عقله و حاله و عرضه و يشمل صفوف التخويف الأذى و التهديد و القتل بغير حق وما يتصل بصورة الحرابة وإخافة السبيل و قطع الطريق و كل فعل من أفعال العنف أو التهديد يقع تنفيذا لمشروع إجرامي فردي أو جماعي، يهدف إلى إتباع الرعب بين الناس أو ترويجهم بإيذائهم أو تعريض حياتهم أو حوريتهم أو أمنهم أو أموالهم إلى الخطر"[3]، كما عرف في الاتفاقية العربية لمكافحة الإرهاب على أنه " كل فعل من أفعال العنف أو التهديد أيا كانت بوادره أو أغراضه، يقع تنفيذا لمشروع إجرامي جماعيا أو فرديا، يهدف إلى إلقاء الرعب بين الناس، أو ترويهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم إلى الخطر أو إلحاق الضرر بالبيئة أو أحد المرافق أو الأملاك العامة أو الخاصة.[4]

أما المشروع الجزائري فقد تناول ظاهرة الإرهاب بموجب المرسوم التشريعي رقم 92/03 المتعلق بمكافحة التخريب والإرهاب والذي يعتبر أول تشريع يحدد مفهوم الجريمة الإرهابية ويجرمها، لقد أورد في المادة الأولى من التشريع الصادر في سبتمبر 1992 تعريف الإرهاب حيث نصت هذه المادة على أنه " يعتبر عملا تخريبيا أو إرهابيا في

[1]– سورة الأعراف، الآية 116.

[2]– سورة الأنفال، الآية60.

[3]– علي بوعمرة، جريمة الإرهاب الإلكتروني، مذكرة مقدمة ضمن متطلبات لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة، 2021/2020، ص8.

[4]– عبد القادر زهير النقوزي، المفهوم القانوني لجرائم الإرهاب الداخلي و الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية لبنان 2008، ص29.

مفهوم هذا المرسوم التشريعي كل مخالفة تستهدف أمن الدولة والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يلي:

- عرقلة سير المؤسسات العمومية و الاعتداء على حياة أعوانها أو ممتلكاتها أو عرقلة تطبيق القوانين والتنظيمات.
- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء على الأشخاص أو تعريض حياتهم أو أمنهم للخطر أو المس بممتلكاتهم.
- الاعتداء على المحيط وعلى وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواذ عليها أو احتلالها دون مسوغ قانوني، وتدنيس القبور أو الاعتداء على رموز الجمهورية، أو عرقلة عمل السلطات العمومية أو حرية ممارسة القيادة والحريات العامة وسير المؤسسات المساعدة المرفق العام. [1]

إذا من خلال ما سبق نلخص القول بان الإرهاب هو مشروع إجرامي هدفه إلقاء الرعب بين الناس.

ثانيا: تعريف الإرهاب الالكتروني

الإرهاب الالكتروني هو النشاط أو الهجوم المعتمد الذي يملك دوافع سياسية وسعي للتأثير في قرارات الحكومية والرأي العام العالمي وسيتقدم القضاء الالكتروني بوصفه عاملا مساعدا وسيأتي عملية التنفيذ للعمل الإرهابي أو الحربي، كما يسعى لإحداث تأثير محتوي ونفسي عبر التحريض على بث الكرامة الدينية وحروب الأفكار،وأن يتم في صورة رقمية من خلال استقدام بيانات الأسلحة الالكترونية الجديدة في معارك تدور رحالها في

[1]– سارة جلاب، سياسة مكافحة الإرهاب (دراسة مقارنة بين الجزائر والولايات المتحدة الأمريكية، مذكرة تكميلية لنيل شهادة الماستر، تخصص سياسات عامة مقارنة، كلية الحقوق والعلوم السياسية جامعة العربي بن المهيدي،2015/2014 ص12.

الفضاء الالكتروني والذي قد يقتصر تأثيرها على بعدها الرقمي أو قد تتعدى لإصابة أهداف مادية تتعلق بالبنية التحتية الحيوية.[1]

وهنالك من عرفه بأنه: هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا، توجه من أجل الانتقام أو ابتزاز أو إجبار أو تأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة. وبالتالي فلكي ينعت شخصا ما بأنه إرهابيا على الانترنت، وليس فقط مخترقا، فلابد وأن تؤدي الهجمات التي يثبتها إلى العنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافيا من أجل نشر الخوف والرعب، فالإرهاب الالكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويج الآخرين وإلحاق الضرر بهم أو تهديدهم. [2]

كما عرفت وكالة المخابرات المركزية الأمريكية الإرهاب الالكتروني على أنه " أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر، وبرامجه والبيانات والمعلومات التي تنتج من عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين.[3]

إذن الإرهاب الالكتروني هو العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو، الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو

[1]– بن صفية وداد، تأثير المتغير التكنولوجي على الفواعل الدولية الجديدة الإرهاب الالكتروني نموذجا، مذكرة لنيل شهادة الماستر الأكاديمي تخصص إستراتيجية وعلاقات دولية , كلية الحقوق والعلوم السياسية جامعة محمد بوضياف، المسيلة، 2018/2017، ص51.

[2]– علي عدنان الفيل، الاجرام الالكتروني، دراسة مقارنة ط1، مكتبة زين الحقوقية والأدبية لبنان، 2011، ص6.

[3]– عادل عبد الصادق، القوة في العلاقات الدولية نمط جديد تحديات مختلفة، ط2 المركز العربي لأبحاث الفضاء – الالكتروني، القاهرة، 2009، ص113.

ماله أو عقله بغير حق، باستخدام الموارد المعلوماتية والوسائل الالكترونية، كشوف العدوان و صور الفساد.[1]

مما سبق نقول أن الإرهاب الالكتروني هو مشروع إجرامي يتم بواسطة وسائل إلكترونية.

الفرع الثاني: خصائص الإرهاب الالكتروني

بعد ما تعرفنا على الإرهاب الالكتروني والمقصود بهذا المصطلح، لا حظنا أن هذا الأخير لديه مجموعة من الخصائص التي تميزه وسوف نلخصها فيما يلي:

- صعوبة اكتشاف هذه الجريمة وذلك يعود لنقص الخبرة لدي بعض الجهات الأمنية والقضائية.
- صعوبة إثبات جريمة الإرهاب الالكتروني وهذا نظرا لغياب الدليل الرقمي، إضافة لسهولة إتلافه وتدميره
- الابتعاد عن العنف والقوة وذلك لاعتماده على الحاسب الآلي، الذي يتصل بالشبكة المعلوماتية مزودا ببعض البرامج اللازمة.
- عابر الدول والقارات فهو لا يخضع لدولة واحدة.
- مُرتكب هذه الجريمة يكون عادة من المتخصصين في مجال تقنية المعلومات، أو لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الشبكات المعلوماتية.[2]

الفرع الثالث: أهداف الإرهاب الالكتروني

يهدف الإرهاب الالكتروني إلى تحقيق مجموعة من الأهداف الغير مشروعة وتتمثل في:

- نشر الخوف والرعب بين الأشخاص والدول والشعوب.

---

[1]– علي عدنان الفيل، مرجع سابق، ص 59.

[2]– مصطفى يوسف كافي، الإدارة الإلكترونية، دار مؤسسة رسلان للطباعة والنشر، سوريا، دمشق، 2011، ص 441.

- الإخلال بالنظام العام والأمن المعلوماتي، وزعزعة الطمأنينة.
- تعريض سلامة المجتمع وأمنه إلى الخطر.
- الانتقام من الخصوم.
- الدعاية والإعلان بموجب الانتباه، إضافة إلى إثارة الرأي العام.
- جمع الأموال والاستيلاء عليها.
- التسبب في إحداث الضرر بوسائل الاتصالات وتقنية المعلومات، وبالأموال، والسلطات العامة والخاصة.[1]

الفرع الرابع: تمييز الإرهاب الالكتروني عن المفاهيم المشابهة

سنقوم بتمييزه عما يلي:

أولا: تمييز الإرهاب الالكتروني عن الإرهاب العادي

سوف نتطرق فيه إلى أبرز أوجه الاختلاف والتشابه بينهما.

الوسيلة المستعملة في ارتكاب الأفعال الإرهابية: يعتمد الإرهاب العادي على وسائل تقليدية مادية لتنفيذ هجماته وذلك باستعمال أسلحة تترك اثأر على أرض الواقع، كاستعمال القنابل والمتفجرات، وخطف الطائرات المدنية وتغير مسارها إلى أماكن معينة لتحقيق الغرض الإرهابي، في حين أن الإرهاب الالكتروني لا يعتمد على الوسائل مادية فهو مرتبط لتحقيق بالانترنت، وذلك باختراق المواقع الالكترونية وتدميرها بنشر الفيروسات، وتخريب البيانات ومحوها وهذا هو الاختلاف الجوهري بين كل من الإرهاب العادي والالكتروني.[2]

---

[1]– حسنين شفيق، الاعلام الجديد والجرائم الالكترونية، التسريبات، التجسس، الإرهاب الالكتروني، دار الفكر والفن للطباعة والنشر والتوزيع، مصر 2014 ص، 191–190.

[2]– غلاف كريمة جرلال زوهرة، جريمة الإرهاب الالكتروني، مذكرة لنيل شهادة الماستر، تخص القانون الجنائي والعلوم الجناية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية 2019/2018، ص 25.

- **خصوصية المجرم:** فالمجرم في الإرهاب التقليدي يكون غالبا غير متعلم، على عكس المجرم الإرهابي المعلوماتي الذي يكون على درجة عالية من المعرفة في المجال الرقمي.[1]
- **طريقة تنفيذ الجريمة:** مجرم الإرهاب التقليدي يفدي بحياته من أجل تحقيق قضيته الإرهابية، في حين أن المجرم الإرهابي المعلوماتي لا يحتاج إلى التنقل إلى ساحة الهجوم يكفي فقط إتقانه في استعمال الوسائل التقنية.[2]

هذه البعض من الاختلافات التي توصلنا إليها من خلال دراسة كل من الإرهاب التقليدي و الإرهاب الرقمي، وسوف نتطرق الآن إلى ابرز أوجه التشابه بينهما والتي تتمثل في:

- الاستناد على قاعدة واحدة وهي التهديد وما يحدثه من فزع وخوف وترويع يؤدي إلى انعدام الاستقرار النفسي لدى المجني عليه.[3]
- كل من الإرهاب التقليدي والإرهاب الالكتروني يقومان على خلفية دوافع سياسية أو عرقية أو دينية.[4]
- كلاهما الغرض منهما الإخلال بالنظام العام، وتعريض سلامة أفراد المجتمع وأمنه إلى الخطر.[5]

---

[1]– غلاف كريمة جرلال زوهرة، المرجع السابق، ص 25.

[2]– أنظر المرجع نفسه، ص 25.

[3]– بن صويلح أمال، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام، الملتقى الدولي حول الإجرام السيبيراني المفاهيم والتحديات خطوة عامة نحو مكافحة الإرهاب الإلكتروني للجزائر، جامعة 8 ماي 1945، قالمة، يومي 11 و 12 أفريل، 2017، ص3.

[4]– هروال هيبة نبيلة، جرائم الانترنت أطروحة دكتوراه كلية ح – ع – س جامعة أبي بكر، بالقايد، تلمسان، 2014/2013، ص 337.

[5]–هروال هيبة نبيلة، نفس المرجع، ص 337.

ثانيا: تمييز الإرهاب الإلكتروني عن الجريمة الالكترونية

الجريمة الالكترونية عرفها المشروع الجزائري في المادة 2 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأنه المساس بأنظمة المعالجة للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسجل ارتكابها عن طريق المنظومة المعلوماتية أو نظام الاتصالات الالكترونية. [1]

وتختلف الجريمة المعلوماتية عن الإرهاب الالكتروني في كون المجرم المعلوماتي أقل خطورة من المجرم الإرهابي المعلوماتي، والجريمة المعلوماتية يكون هدفها دائما تحقيق الربح في حين أن الإرهاب الالكتروني يسعى دائما إلى تحقيق أغراض سياسية، ثقافية، دينية.[2]

أما من ناحية النقاط المشتركة بين هاتين الجريمتين هو أن كلاهما من الجرائم الجديدة، وعبورها للحدود الوطنية،وهما جريمتين لا تتطلبان العنف ولا القوة في ارتكابها والمجرم الذي ينفذها يمتاز بالذكاء.

ثالثا: تمييز الإرهاب الالكتروني عن حرب المعلومات.

حرب المعلومات: هي استخدام المعلومات لاستغلال وتخريب وتدمير وتعطيل معلومات الخصم وعملياته المبنية على المعلومات، ونظم معلوماته وشبكاتي الحاسب الآلي الخاصة بها وكذلك الحماية من خطر الهجوم من قبل الخصم.[3]

ومن أبرز أوجه التشابه بينه و بين الإرهاب الالكتروني:

- ذكاء و الخبرة مرتكبيها.
- قلة التكلفة.

---

[1]– القانون رقم 04/09، المؤرخ في 5 غشت، سنة 2009، يحتوي على القواعد الخاصة من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الجريدة الرسمية، العدد 47.

[2]– غلاف كريمة، جرلال زوهرة، مرجع سابق، ص 27– 28.

[3]– عادل عبد الصادق، مرجع سابق، 133.

- صعوبة الاكتشاف، وغياب الأدلة.
- إضافة أن كلاهما تتم عبر شبكة الانترنت وباستخدام الحاسب الآلي.

ولكن هذا التشابه لا ينفي وجود مجموعة من الاختلافات بينهما.

فالإرهاب الالكتروني يتخذ من حرب المعلومات أداة التنفيذ أهدافهم، إضافة أنه يمكن لحرب المعلومات أن تتحول إلى إرهاب الكتروني إذا تم استخدامها من طرف جماعة إرهابية.[1]

رابعا: تمييز الإرهاب الالكتروني عن الجريمة المنظمة:

عَرفت الجمعية العامة لمنظمة الأمم المتحدة يوم 15 نوفمبر 2000 حسب مضمون المادة الثانية– أ – الجريمة المنظمة على أنها " الجريمة التي ترتكب من طرف جماعة إجرامية محددة البنية، مؤلفة من 3 أشخاص أو أكثر، موجودة لفترة زمنية.[2] وتتشابه هذه الجريمة مع الإرهاب الالكتروني فيما يلي:

- كلاهما من الجرائم العابرة للحدود.
- كلاهما يهدفان إلى بث الرعب و الخوف بين الناس.
- يعتمدان على وسائل الاتصال الحديثة.
- يسعيان دائما لإعاقة التنمية الاقتصادية للدول.[3]

ومن أبرز الاختلافات التي تخيم على هاتين الجريمتين هي كالأتي:

المجرم الإرهابي يكشف عن أعماله الإرهابية بواسطة وسائل الإعلام الالكتروني في حين أن مجرم المنظمة ينجز أعماله بسرية تامة بعيدا عن الأنظار.

---

[1]– شاشوة ياسمينة , الإرهاب الالكتروني بين مخاطره واليات مكافحته، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية ح–ع–س، جامعة أكلي محند أولحاج، البويرة، 2020/2019، ص 20.

[2]– المرسوم الرئاسي رقم 02–55 مؤرخ في 5 فبراير 2002 تتضمن التصديق بتحفظ على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، الجريدة الرسمية العدد 9، الصادر في 2002/02/10.

[3]– غلاف كريمة، جرلال زهرة، المرجع السابق، ص30–31.

الجريمة المنظمة لا تعرف بها الدولة ككيان ولا تتفاوض مع مجرميها، في حين أن التنظيمات الإرهابية تعترف بأنها كيان قائم وتحاول التفاوض مع مجرميها لتسليم أنفسهم.

الجريمة المنظمة يشترط فيها عنصر الجماعة على عكس جريمة الإرهاب التي تتم في إطار فردي أو جماعي.

من حيث الهدف: الإرهاب الالكتروني أهداف يمكن أن تكون دينية أو سياسية أو مادية..... الخ في حين أن الجريمة المنظمة هدفها هو الحصول على أرباح مادية.[1]

المطلب الثاني: أسباب الإرهاب الالكتروني و مخاطره.

يعتبر الإرهاب الالكتروني أخطر أنواع الإرهاب فتكا، لذلك فان مخاطره متعددة وهذا راجع لعدة أسباب ودوافع عامة و خاصة، ومن هنا سنقوم بتقسيم هذا المطلب إلى فرعين، الفرع الأول (الأسباب العامة والخاصة للإرهاب الالكتروني)، أما الفرع الثاني فنتناول فيه (مخاطر الإرهاب الالكتروني)

الفرع الأول: أسباب الإرهاب الالكتروني

ونتناول فيه ما يلي:

أولا: الأسباب العامة للإرهاب الإلكتروني

أ- الأسباب الاقتصادية

- تفاقم الأزمات الاقتصادية في المجتمعات الدولية بالإضافة إلى المتغيرات الاقتصادية العالمية والاستغلال غير المشروعة للموارد الاقتصادية للمعين عدم إقامة تعاون دولي جدي من قبل الأمم المتحدة وعدم إيجاد تنظيم عاجل ودائم لعدد من المشاكل العالمية مثل اغتصاب الأراضي والاضطهاد.[2]

[1]- هروال هيبة نبيلة، المرجع السابق، ص329.

[2]- مصطفى يوسف كافي، جرائم (الفساد – غسيل الأموال – الساحة – الإرهاب الالكتروني المعلوماتية)، الطبعة الأولى، مكتبة المجمع العربي للنشر والتوزيع، عمان – الأردن، 2014، ص 145 – 146.

- معاناة الأفراد من المشاكل الاقتصادية المتعلقة بالإسكان والفقر وغلاء المعيشة والتضخم في أسعار المواد الغذائية والخدمات الأساسية وعدم تحسن دخل الفرد مما يؤدي إلى تفشي روح التذمر وبدفع الشباب إلى التطرف والإرهاب.[1]
- بالإضافة إلى هذا في المجتمعات المختلفة وعدم توفر فرص العمل مهما ساهم في ظهور جرائم السرقات والإرهاب.
- التقدم التقني لأنظمة المصرفية العالمية ومما أدى إليه من سهولة انتقال الأموال وتحويلها بين جميع أرجاء العالم عن طريق شبكة الانترنت ساعد المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أهدافهم غير المشروعة.[2]

ب- الأسباب الشخصية والنفسية

يرتبط العامل الشخصي والنفسي ارتباطا وثيقا بالعوامل السياسية والأيديولوجية والاقتصادية، فالشباب المُهمش الذي يفقد معنى الحياة في دول العالم النامي لأسباب تتعلق بالظلم وعدم الإنصاف والبطالة والفقر والافتقار للحياة الكريمة يكونون عرضة لانجراف في عالمي الجريمة والإرهاب.[3]

- وعلى المستوى الفردي تلعب العوامل النفسية دورا في غاية الأهمية في تحديد سلوكيات الإنسان المعادي للمجتمع، خاصة عندما تتعرض تلك الجوانب لبعض الاضطرابات والتقلبات النفسية والمرضية التي يمكن إرجاعها لأسباب وراثية أو مفاجئة، فمثل هذه الجوانب النفسية قد تكون الدافع الحقيقي لاقتحام الفرد في عالم الإرهاب وتلعب وسائل الإعلام دورا كبيرا في تحقيق العوامل النفسية للفرد وتأجيج روح الانتقام لديه وعلى الصعيد الثقافي فان شعوب دول العالم النائي من الانعكاسات

[1]- مصطفى يوسف كافي ، المرجع السابق، ص145-146.

[2]- مصطفى يوسف كافي، جرائم (الفساد – غسيل الأموال – الساحة – الإرهاب الالكتروني المعلوماتية)،المرجع السابق، ص 145-146.

[3]- خلود عبد الرحيم العالول، الإرهاب الإلكتروني، بحث علمي قانوني لنيل لقب أستاذة في المحاماة، نقابة المحامين، فرع دمشق، الجمهورية السورية، ص 38-39.

السلبية التي خلفتها العولمة المتمثلة بالتبعية الثقافية وأزمة الهوية، الأمر الذي يتبع إلى خلق صراعات ثقافية داخل المجتمع الواحد بعضه يؤدي الإرهاب والأخر يعارضه.[1]

ج- الأسباب السياسية

إن من أبرز الأسباب و الدوافع السياسية لظاهر الإرهاب ما يلي:

- السياسات غير العادلة التي تنتهجها بعض الدول ضد مواطنيها والكبت السياسي الذي تمارسه عليهم وتهميش دول للمواطن وتغيبه عن المشاركة السياسية وانتهاك حقوقه وعدم تلبية متطلبات التوازن الاجتماعي وانعدام تفعيل دور مؤسسات المجتمع المدني.[2]

- الإحباط السياسي وذلك لأن كثير من البلدان العربية والإسلامية لم تكتفي بالتهميش الجماعات الإسلامية بل وقفت في وجهها وتصدرت لأربابها وحصرت نشاطها وجمدت عطاءها حتى في بعض البلدان التي تدعى الديمقراطية وحرية وهذا من شأنه أن يولد المنظمات السرية وردود الأفعال الغاضبة التي لا تجد ما تصب فيه غضبها سوى الإرهاب.[3]

- معاناة بعض المجتمعات و الشعوب الدولية من ظلم و اضطهاد و احتلال و سيطرة الاستعمارية و سلب الأموال والمقدرات دفع تلك الشعوب إلى التشدد و التطرف بإضافة إلى غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروة الوطنية.

---

[1]- خلود عبد الرحيم العالول، المرجع السابق، ص 38-39.

[2]- إسراء طارق جواد كاضم الجابري، الإرهاب الالكتروني - دراسة مقارنة - رسالة مقدمة لنيل درجة الماجستير : تخصص قانون عام كلية الحقوق، جامعة النهرين، العراق 2013، ص 32- 33.

[3]- المرجع نفسه، ص32-33.

– التفاوت في توزيع الخدمات و المرافق الأساسية، الاستيلاء على الأموال العامة وافتقار النظام الدولي إلى الحزم في الرد على المخالفات والانتهاكات التي تتعرض لها مواثيق بعقوبات دولية شاملة ورادعة.[1]

د– الأسباب الاجتماعية

تتمثل الأسباب الاجتماعية المؤدية إلى ظهور الإرهاب الالكتروني فيما يلي:

- التفكك الأسري و الاجتماعي و الذي يؤدي إلى انتشار الأمراض النفسية والانحراف والإجرام والإرهاب، ذلك لأن الأسرة المترابطة تحيط الأشخاص بشعور التمسك والتعاون فالمجتمعات ذات الترابط الأسرة لا تظهر بينهم الأعمال الإرهابية بالقدر نفسه الذي تظهر فيه عند المجتمعات المفككة اجتماعيا.[2]
- غياب التربية الحسنة التي توجه الأشخاص لمكارم الأخلاق و محاسنها وانعدام التربية الإيمانية القائمة على مرتكزات و دعائم قوية من نصوص الوحي واستبصار المصلحة العامة ودرء المفاسد الطارئة.[3]
- الفراغ العاطفي و الذي يعتبر سبب من أسباب ظهور الإرهاب ذلك لأنه مفسدة للمرء و داء مهلك متلف لدين و النفس فإذا لم تشتغل النفس بما ينفع شغلتك هيا بما لا ينفع، والفراغ النفسي والروحي والعقلي والذهني أرض خصبة لقبول كل فكر هدام وغلو وتطرف.
- فقد الهوية المجتمعية و العقيدة الصحيحة للمجتمع، وفقدان العدل وانتشار الظلم بين المجتمع وعدم الحكم بما أنزل الله، غياب دور العلماء وانشغالهم و تقصير بعض أهل

[1]– إسراء طارق جواد كاضم الجابري، المرجع السابق ، ص32–33.

[2]– المرجع نفسه، ص 34–35.

[3]– المرجع نفسه، ص 34–35.

العلم والفقه والمعرفة في القيام بواجب النصح والإرشاد والتوجيه للمجتمع كل هذه الأسباب الاجتماعية تؤدي إلي تفشي ظاهرة الإرهاب.[1]

ثانيا: الأسباب الخاصة للإرهاب الالكتروني

تتضمن الأسباب الخاصة للإرهاب الإلكتروني ما يلي:

أ- غياب الحدود الجغرافية و تدني مستوى المخاطرة

يعد غياب الحدود المكانية المحددة في الطبيعة الجغرافية على شبكة الانترنت بالإضافة إلى عدم وضوح الهوية الافتراضية أو الرقمية للمستخدم المتوطن في البيئة المفتوحة فرصة سائحة للإرهابيين، بحيث باستطاعة محترف الحاسوب تقديم نفسه بالهوية والصفة التي يرغب بها أو يتخفى وراء شخصية افتراضية وهمية الأمر الذي يسهل عليه شن هجومه الإرهاب الكترونيا دون الحاجة إلى المغامرة و المخاطرة المباشرة وبعيدا عن أعين الرقابة الأمن.[2]

ب- الفراغ التنظيمي و القانوني و غياب السيطرة و الرقابة على الشبكة المعلوماتية

إن الفراغ الرهيب والملحوظ الذي تعاني منة التنظيمات والقوانين لدى بعض المجتمعات العالمية حول الإرهاب الالكتروني والجرائم المعلوماتية يعتبر أحد أهم الأسباب الرئيسية لانتشاره، ونظرا لغياب قوانين ولوائح تجريمية عالمية ومتكاملة جعلت من المجرمين يعتمدون الانطلاق من بلدان نفتقد لهذه القوانين واللوائح ويركزون في هجماتهم على بلدان توجد بها هذه القوانين الصارمة في التعامل مع مثل هذه الحالات والأمر الذي أدى إلى ظهور مشكلة تنازع القوانين.[3]

---

[1]- إسراء طارق جواد كاضم الجابري، الإرهاب الالكتروني، المرجع السابق، ، ص34-35.

[2]- توفيق شريخي، الإرهاب الإلكتروني وتأثيره على أمن الدولة،مذكرة لنيل شهادة ماستر أكاديمي، تخصص استراتيجية وعلاقات دولية، جامعة محمد بوضياف- المسيلة-، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2018/2015، ص 17.

[3]- توفيق شريخي، المرجع نفسه، ص17.

ج- ضعف بنية الشبكات المعلوماتية و قابليتها للاختراق

إن شبكة المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها رغبة في التوسع وتسهيل دخول المستخدمين ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل لبنى المعلومات المخزنة، وممارسة العمليات التخريبية والإرهابية.[1]

د- سهولة الاستخدام و قلة التكلفة

إن الشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستخدام، قليلة التكلفة لا ستغرق وقتا وجهدا كبيرا مما هيأ الإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير مشروعة ومن دون الحاجة إلى مصادر تمويل ضخمة فالقيام بشن هجوم إرهابي الكتروني لا يتطلب إلى أثر من جهاز حاسب إلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة.[2]

الفرع الثاني: مخاطر الإرهاب الالكتروني

إن الإرهاب الالكتروني شأنه شأن الجرائم المعلوماتية الأخرى ينتج عنه عدة مخاطر سنقوم بتناولها في هذا الفرع:

أولا: مخاطر الإرهاب الالكتروني على المؤسسات.

يعد الإرهاب الالكتروني من أكبر المخاطر التي تهدد المؤسسات من خلال احتراق شبكات اتصالها والنفاذ إلى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها المختلفة وفي ظل المنافسة التي تشهد معظم الأسواق الحالية أصبح التحسب على مختلف أنشطة الشركات مصدر قلق حقيقي.[3]

---

[1]- علي عدنان الفيل، المرجع السابق،ص72.

[2]- المرجع نفسه، ،ص72.

[3]- علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، دار المنشأة المعارف، الإسكندرية، مصر، 2006، ص 15.

ومن بين مخاطر الإرهاب الأخرى على المؤسسات إسقاط موقع المؤسسة على الانترنت وذلك بأن يصوب عليه العديد من الرسائل المولدة تلقائيا التي تظل تنهمر إلى أن تصل إلى حد يعجز الموقع تماما عن ملاحقتها ليسقط وبالتالي تسقط معه جميع المعاملات التجارية والمالية الالكترونية التي يوفرها موقع المؤسسة لعملائه وشريكاته ومن الرسائل الأخرى التي تتعرض لها المؤسسات فك شفرة الحماية السرية للبيانات التي تتبادلها مع الآخرين خارج المؤسسة من عملاء ووكلاء وما شبه ذلك، وقد عرف العالم من قبل تهديد وذلك من خلال قيام شباب من النرويج بنشر عدة برامج في عدة أسطر يمكن به فك الشفرة الرقمية التي تبث بها أفلام عبر الشبكة وهو دليل الإرهاب في السطو على المؤسسات والتهديد نفسه الذي تواجهه حماية الملكية الفكرية.[1]

ثانيا: مخاطر الإرهاب الالكتروني على الدول

الإرهاب الالكتروني نشاط أو هجوم متعمد يمتلك دوافع سياسية شعر لتأثير على الدولة والرأي العام العالمي ويستخدم الفضاء الالكتروني بوصفه عاملا مساعدا ووسيطا في تنفيذ العمل الإرهابي وقد ظهر الارتباط من الانترنت والإرهاب بشكل واضح في الآونة الأخيرة وانتقلت المواجهة ضد الإرهاب والإرهابيين من مواجهة مادية إلى مواجهة الكترونية وتحولت الحروب الوقعة إلى حروب رقمية وأصبحت الانترنت من أشد الأسلحة فتكا و هدما إذا ما استخدم لأغراض سيئة وتحقيق نوايا إرهابية.[2]

وتتمثل خطورة جرائم الإرهاب الالكتروني على الدول فيما يمكن أن يترتب عليها من أضرار جسمية وخسائر مالية ضخمة مثل تعطيل عمليات التحويل المالي أو الدخول إلى شبكات التحكم في المرافق العامة مما يتسبب في شلل المبني التحتية الأساسية، هذا

[1]– شاشوة ياسمينة، المرجع السابق، ص47–48–49.

[2]– المرجع نفسه، ص47–48–49.

وقد أصبح الإرهاب يشكل هاجسا حقيقيا وتهديد الكل الدول إذا انه يهدد أمنها وسياستها و اقتصادها.[1]

لقد شهد العالم أسره كيف تم تحويل الطائرات المدنية في تفجير برحي التجارة العالميين في أمريكا فيما عرف بهجمات 11 سبتمبر 2001 حيث تمكن الإرهابيين من استغلال تكنولوجيا المعلومات المتطورة في التخطيط والتنفيذ لهذه العملية التي تشكل أكبر اختراق معلوماتي أسفر عن سقوط ألاف الضحايا في تاريخ الولايات المتحدة، الأمر الذي أدى بثلاثين دولة إلى توقيع اتفاقية مكافحة الإجرام المعلوماتي في العاصمة المجرية بودابست من نفس العام.[2]

ثالثا: مخاطر الإرهاب الالكتروني على الأفراد

لا تقتصر مخاطر الإرهاب الالكتروني على الدول والمؤسسات فقط بل تمتد لشكل خطرا وتهديدا لسلامة وأمن و راحة الفرد إذا أنه وبظهور الحاسبات الآلية تغير شكل الحياة في العالم وأصبح من أساسياتها في الأفنية الجديدة، ولكن هذا الاختراع العبقري تحول إلى لغم داخل كل بيت خاصة بعد استخدامه في الدخول إلى شبكة المعلومات الدولية " الانترنت" ومن هنا فان الحفاظ على الخصوصية في حياة كل شخص أضحى من المستحيلات لوجود الإرهاب الإلكتروني الذي يهدد هذه الخصوصية من خلال التجسس على البريد الالكتروني واختراق الصفحات الخاصة في المواقع التواصل الاجتماعي وبالتالي ابتزاز الأفراد ومن بين أهم مخاطر الإرهاب الإلكتروني على الأفراد نجد الابتزاز والتهديد المعلوماتي حيث شهدت شبكة الانترنت حالات للابتزاز المعلوماتي وذلك من خلال التجسس على حلقات الدردشة عبر مواقع التواصل الاجتماعي.[3]

[1]– شاشوة ياسمينة ،المرجع السابق، ص47–48–49.

[2]– المرجع نفسه، ص47–48–49.

[3]– خلود عبد الرحيم العالول، المرجع السابق، ص58.

وفي الغالب يستهدف هذا النوع من الإرهاب الشخصيات المعروفة سواء الحكومية أو العسكرية والفنية حيث ينتج الانترنت والتكنولوجيا وسائل مبتكرة للابتزاز من بينها انتحال شخصية الأفراد وذلك من أجل الاستفادة من سمعتهم و أموالهم أو بهدف استدراجهم للبوح بأسرارهم من خلال إنشاء حسابات مزورة من أجل التعارف ثم فضحهم واستغلال وتشويه سمعتهم ونشر المعلومات السرية والصور الشخصية عنهم بهدف المساس بكرامتهم وتهديدهم ومن بين حالات التهديد وابتزاز الأشخاص نذكر على

سبيل المثال التهديد بالوثائق المزورة التي يتم تزويرها الكترونيا أو لوج إلى الأسرار المهنية (سير الأشخاص) إضافة إلى النصب و الاحتيال بشتى الأشكال....[1]

رابعا: المخاطر الأخرى للإرهاب الالكتروني

لم تكتفي مخاطر الإرهاب الالكتروني على الأفراد والمؤسسات والدول بل امتدت لتشمل مخاطر أخرى مرعبة تهدد البشرية حسب (باري كوليين) ومن بين هذه المخاطر نذكر ما يلي:

الوصول عن بعد إلى أنظمة التحكم بمصانع الحبوب وتغير مشتريات مكملات الحديد للإضرار بصحة المستهلكين إجراء تعديلات عن بعد في معالج حليب الأطفال الرضع للإضرار بهم، تعطيل المعارف والمعاملات المالية الدولية والبورصات لافتقاد الثقة في النظام، تغير مكونات صناعة الأدوية عن بعد لدى شركات الأدوية وتغير الضغط في خطوط الغاز وإحمال شبكة الكهرباء مما يوقع إنفجارات وحرائق مروعة بالإضافة إلى هذا مهاجمة أنظمة التحكم في الحركة الجوية وجعل الطائرتين مدنيتين تتصادمان عن طريق الولوج إلى أجهزة استشعار في قمرة القيادة الطائرة وهذا ممكن في خطوط السكك الحديدية أيضا.....[2]

[1]– خلود عبد الرحيم العالول، المرجع سابق، ص 59.

[2]– شاشوة ياسمينة، المرجع السابق، ص48–49.

المبحث الثاني: أركان جريمة الإرهاب الالكتروني

إن التطرق إلى تعريف الإرهاب الإلكتروني، وذكر مختلف الدوافع والأسباب المؤدية له وتميزه من كل ما يشابهه من مصطلحات والكثير من الأمور الأخرى التي تطرقنا إليها في المبحث الأول هو أمر غير كافي للتعرف على هاته الجريمة التي أصبحت بدورها تشكل خطرا على حياة الأفراد وعلى أمن الدولة لذا من المهم أن نخصص هذا المبحث لأركان الإرهاب الالكتروني الذي قمنا بتقسيمه إلى 3 مطالب.

المطلب الأول: الركن الشرعي لجريمة الإرهاب الالكتروني

سنخصص هذا المطلب للتطرق إلى مختلف التشريعات التي جرمت الإرهاب الالكتروني

الفرع الأول: تجريم الإرهاب الالكتروني في التشريع الجزائري

حيث تم تناوله فيما يلي:

أولا: الركن الشرعي للجريمة الواردة في المادة 87 مكرر.

يقصد بالنص الشرعي الذي يجرم الإرهاب الالكتروني حيث أن المشرع الجزائري لم يخص هذه الجريمة بنص خاص، حيث أشار إلى جريمة الإرهاب وصور السلوك الإجرامي لها، والأفعال المشكلة لجريمة الإرهاب وذلك في القسم الرابع تحت عنوان الجرائم الموصوفة بأفعال تخريبيه وإرهابية حيث جاءت المادة 87 مكرر من الإطار العام للسلوكيات الإجرامية بصفة عامة، وبالتالي فهي تشمل كل صور وأشكال الإرهاب بما فيها الإرهاب الالكتروني.[1]

[1]– هاجر عون، الإرهاب الالكتروني، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن المهيدي، أم البواقي، 2016/2015، ص 25.

ثانيا: الركن الشرعي لجريمة الإرهاب الواردة في المادة 394 مكررة

جُرمت الأفعال الماسة بالمعالجة الآلية لأنظمة المعطيات في القانون 04-15 المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر394 مكرر7 إذ جرمت الأفعال الماسة بالمعالجة الآلية لأنظمة المعطيات، سواء كانت وسيلة أو غاية للجريمة.[1]

الفرع الثاني: تجريم الإرهاب الالكتروني في بعض تشريعات الدول العربية

سنتطرق فيه إلى تشريعات كل من دولة الإمارات العربية المتحدة، وقطر والمملكة العربية السعودية والأردن.

أولا: الإمارات العربية المتحدة: حيث نصت في المادة 21 من قانون مكافحة جرائم تقنية المعلومات (04 -06) على تحريم الإرهاب الإلكتروني بقولها "كل من أنشأ موقعا أو تنشر معلومات على الشبكة المعلوماتية أو إحدى الوسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهه لتسهيل الاتصالات بقيادتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو تشر كيفية تصنيع الأجهزة الحازمة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالحبس مدة لا تزيد عن 5 سنوات". [2]

ثانيا: المملكة العربية السعودية: حيث نصت في نظام مكافحة الجرائم المعلوماتية في المادة السابعة منه على ما يلي" السجن مدة لا تزيد عن عشر سنوات؛ وبغرامة لا تزيد عن خمس ملايين ريال لكل شخص ينشئ موقعا لمنظمات إرهابية على الشبكة المعلوماتية، أو إحدى أجهزة الحاسب الآلي أو نشره لتسهيل الاتصالات بقيادات تلك المنظمات،أو أي من أعضائها، أو ترويج أفكارها أو تمويلها، أو تشر كيفية تصنيع الحارقة أو المتفجرات،أو أية أداة تستخدم في الأعمال الإرهابية، أو من يقوم بالدخول غير

[1]- هاجر عون، الإرهاب الالكتروني، المرجع السابق، ص 25.

[2]- المرجع نفسه، ص 25-26.

المشروع إلى مواقع الكترونية أو نظم معلوماتية مباشرة أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني".[1]

ثالثا: جريمة الإرهاب الالكتروني في التشريع الأردني: لقد جرم المشرع الأردني جريمة الإرهاب الإلكتروني من خلال المواد الواردة في قانون العقوبات الأردني رقم 16 لسنة 1960 في المادة (147/1) وقانون منع الإرهاب الإلكتروني رقم (2014/ 88) في المادة رقم (3 / هـ) والفصول به تاريخ 2014/6/1.[2]

المطلب الثاني: الركن المادي لجريمة الإرهاب الالكتروني

إن الإرهاب الإلكتروني كغيره من الجرائم الأخرى يحتاج في تطبيقه إلى وسائل مادية من أجل إتمام هذه الجريمة وتحقيق غايتهم وقد قسمنا هذا المطلب المعنون بالركن المادي لجريمة الإرهاب الإلكتروني إلى 3 فروع وهي:

الفرع الأول: إنشاء مواقع إرهابية إلكترونية

يقوم الإرهابيون بإنشاء و تصميم مواقع لهم على شبكة الانترنت للدعوة لأفكارهم المتطرفة، ولإعطاء التعليمات والتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد عبر القيام بشن هجمات إرهابية، وقد أنشأت مواقع، إرهابية ليبان كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية الفتاكة، ولشرح اختراق البريد الالكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة،ولتعليم طرق نشر الفيروسات.[3]

---

[1]– هاجر عون، الإرهاب الالكتروني، المرجع السابق، ص 25.

[2]– المرجع نفسه، ص 26.

[3]– يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، الجزائر، 2019، ص214–215.

يعتبر الوجود الإرهابي النشاط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم مسرعان ما يغير نمطه الالكتروني غدا، ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان الكتروني مختلف، ومن الأمثلة على بعض المواقع الإلكترونية الغربية التي قام بإنشائها وتصميمها بعض الشخصيات الإرهابية نذكر منها ما يلي:

- **ذروة السنام:** وهي صحيفة الكترونية دورية للقسم الإعلامي لتنظيم القاعدة
- **صوت الجهاد:** و هي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب وتصدر بصيغتي **(WORD)** (**PDF)** وتتضمن مجموعة من البيانات مع قادة التنظيم ومنظريه.[1]
- **موقع نداء:** بعد الموقع الرسمي لتنظيم القاعدة الإرهابي أسس بعد أحداث 11 سبتمبر ومنه تصدر البيانات الإعلامية للقاعدة.
- **موقع البتار:** و هي مجلة عسكرية الكترونية متخصصة تصدر عن التنظيم الإرهابي و تختص بالمعلومات العسكرية و الميدانية و القتالية.[2]

الفرع الثاني: تدمير المواقع الالكترونية

يقصد بها الدخول غير المشروع على نقطة الارتباط أساسية أو فرعية متصلة بالانترنت من خلال نظام ألي **(Server– pc)** أو مجموعة نظام مترابطة شبكيا

[1]– العجلان، عبد الله بن عبد العزيز بن فهد، الإرهاب المعلوماتي، مداخلة في المؤتمر الدولي، الأول لمكافحة الجرائم المعلوماتية،– ICACC –، كلية علوم الحاسب والمعلومات، جامعة، الإمام محمد بن سعود الإسلامية، نوفمبر2015، المملكة العربية السعودية، الرياض، متوفر على الموقع :http://search.mandumah.com/Record/690587 ، تاريخ التصفح 14 ماي 2022، الساعة: 13:30.

[2]– سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد 08ج 01 ، 2017، ص 17.

(Internet) بهدف تخريب نقطة الاتصال أو نظام، وليس هناك وسيلة تقنية يمكن تطبيقها وتحول تماما دون تحميل المواقع بشكل دائم إذن أن المتغيرات التقنية وإلمام المحترق بالثغرات في التطبيقات التي بينت في معظمها على أساس التصميم المفتوح لمنظم الإجراء**open soutcp** سواء كان في ذلك في مكونات نقطة الاتصال أو نظام أو الشبكة أو البرمجة جعلت الحيلولة دون الاختراقات صعبة جدا.[1]

كما أن هناك منظمات إرهابية تدخل ضمن عملها ومسؤوليتها في الاختراق وتصدير مواقع، ومن المعلوم أن لدى المؤسسات من الإمكانيات والقدرات ما ليس لدى الأفراد أو تم عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة برامج شبكة الانترنت وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المحترف في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الالكترونية، ولا تزال نسبة كبيرة من الاختراقات لم تكشف بعد سبب التعقيد به نظام تشغيل الحاسب الآلي.[2]

الفرع الثالث: التهديد والتجسس الالكتروني

نتطرق في هذا الفرع إلى ما يلي:

أولا: التهديد الإلكتروني

تقوم المنظمات والجماعات الإرهابية بالتهديد والترويع الالكتروني عبر وسائل الاتصالات وتقنية المعلومات المختلفة، وتعتبر الشبكة العالمية **(Internet)**من أهم وسائل التهديد وترويع الالكتروني، وتتعدد أساليب التهديد والترويع وتتنوع طرقه، وذلك من أجل نشر الخوف و الرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل

[1]– عبد الرحمان بن عبد الله السند، وسائل الإرهاب الالكتروني حكمها في الإسلام وطرق مكافحتها، ط 1، جامعة الإمام محمد بن سعود الإسلامية، 2004، ص 19.

[2]– سليماني مباركة، المرجع السابق، ص 347.

المالي والإبراز قوة التنظيم الإرهابي من ناحية أخرى، والمقصود بالتهديد الوعيد بنشر وزرع الخوف في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أن ضررا ما سيلحقه أو سيلحق أشخاصا أو أشياء له بها صلة، ولقد تعددت الأساليب الإرهابية في التهديد، فتارة يكون التهديد بقتل شخصيات سياسة بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير المنشآت الوطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية، في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية، ونحو ذلك.[1]

يكون هذا من خلال بث عدد من النشرات والفيديوهات التي تظهر قوة وقسوة الجماعات الإرهابية، وصور تعذيب وقتل من يخالف أوامرها وتعليماتها، واستخدام وسائل الاتصال والانترنت من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم وتدمير مرتكزات التنمية في البلاد ونشر الفوضى والدمار لأهداف فاسدة ومنحرفة ونشر الإشاعات الكاذبة بين الناس مما يؤدي لنشر الخوف والهلع بين الجمهور.[2]

هذا وتعتمد جل التنظيمات الإرهابية في نشر رسائلها عبر مختلف صفحاتها الالكترونية على نظرية الرعب كمنهج يرمي إلى تسويق مختلف المضامين الدعائية لها، حيث أصبحت الشبكات الاجتماعية في الوقت الحالي تلعب دورا كبيرا في تغذية ودعم ظهور العنف والإرهاب والتطرف وذلك من خلال استغلال الإرهابيين لها في تسويق أغراضهم.[3]

[1]– العجلان عبد الله بن عبد العزيز بن فهد، المرجع السابق، ص61–62.

[2]– علي بوعمرة، المرجع السابق، ص 19 .

[3]– المرجع نفسه، ص19.

ثانيا: التجسس الالكتروني

التجسس الالكتروني أو ما يعرف بحرب التجسس المعلوماتي في حين عبارة عن عدة طرق باختراق المواقع الالكترونية، ومن ثم سرقة بعض المعلومات والتي قد تكون في قائمة الأهمية والخطورة للطرق الملتقى والصورة منه.[1]

هذا ويعتبر التجسس من أقدم وأخطر الأنشطة الاستخباراتية التي مارسها الإنسان قديما في مختلف الميادين خاصة الحروب، إذ أنه تطور عقب الطفرة التي حققتها التكنولوجيا والإعلام واستخدام الحواسب الآلية وشبكات الانترنت، وأصبح الهاجس الأكبر للدول ومن أكثر الجرائم خطورة التي تستهدف المعلومات المخزنة في شبكات المعلومات، إذ أن خطورته لا تكمن في استخدام الانترنت بل في ضعف الرسائل الأمنية المختصة في حماية الشبكات الخاصة بالمؤسسات والهيئات.[2]

ويقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية كما تستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية وهي التجسس العسكري، والتجسس الشخصي والتجسس التجاري، ممثلا في التجسس العسكري تحاول المنظمات الإرهابية اختراق حواسيب وزارت الدفاع للدول المعنية، ذلك قصد الحصول على معلومات عسكرية مثل عدد قوات ونوعية تسليحها وأماكن توجيهها... الخ.

كما تتم عملية التجسس الالكتروني بعدة طرق منها استخدام برنامج التجسس مثل برنامج الحصان طروادة وبرامج تسجيل المفاتيح والأبواب الخلفية وبرامج مراقبة الانترنت، وغرف الدردشة.....الخ، ومن أشهر الطرق شيوعا استعمال وسيلة البريد، حيث يقوم الضحية بفتح المرافقات المرسلة ضمن رسالة غير (**E-mail**)الإلكتروني معروفة المصدر أو باستعمال أسلوب إخفاء المعلومات داخل المعلومات أخرى عادية داخل

[1]- حسنين شفيق، المرجع سابق، ص168.

[2]- علي بوعمرة، المرجع السابق، ص20.

الحاسوب ومن ثم يجد وسيلة لتهريب تلك المعلومات العادية في مظهرها، وبذلك لا يشك أحد بأن هناك معلومات حساسة يتم تهريبها.[1]

المطلب الثالث: الركن المعنوي لجريمة الإرهاب الالكتروني

الركن المعنوي لجريمة الإرهاب الالكتروني نجد فيه كل من القصد الجنائي العام والقصد الجنائي الخاص الذي فصلنا من خلال هذا المطلب كل واحد منهم على حدى.

الفرع الأول: القصد الجنائي العام

يخبر القصد الجنائي عن الإرادة الخبيثة للجاني في مخالفة المسار القانوني على النحو الصحيح الذي رسمه المشرع فقد عرفه الفقه على أنه " العلم بعناصر الجريمة وإرادة ارتكابها" ومن هذا نرى أنه للقصد الجنائي العام عنصرين أساسين يمثلان في العلم والإرادة.[2]

فالعلم هو "حالة ذهنية أو قدر من الوعي يسبق تحقيق الإرادة و يعمل على إدراك الأمور على نحو صحيح مطابق للواقع " وهي الحالة التي يكون فيها الجاني على دراية تامة بمكونات الجريمة وأن السلوك الذي أتى به المجرم فإذا اختفى العلم انعدم القصد الجنائي، أما فيما يخص جريمة الإرهاب الإلكتروني فهي علم الجاني بارتكابه سلوك مجرم قانونا المتمثل في فعل السفر والتمويل والتجنيد وعلمه بالوسيلة المستعملة فين2 ارتكاب هذه الأفعال وهي تكنولوجيا الإعلام والاتصال.[3]

أما الإرادة فهي نشاط نفسي يتجه إلى تحقيق غرض عن طريق وسيلة معينة فالإرادة ظاهرة نفسية ذات طبيعة مادية، تحدث في العالم الخارجي من آثار ما يشبع به الإنسان حاجاته المتعددة، وهي تنصب على السلوك الإجرامي باستخدام الوسائل

---

[1]- يزيد بوحليط، المرجع السابق، ص2014-215.

[2]- غلاف كريمة، جرلال زوهرة، المرجع السابق،ص 48.

[3]- المرجع نفسه، ص 48.

الإلكترونية والذي يهدف إلى إثارة الرعب والخوف بين الناس وتعريض سلامة المجتمع بين للخطر، وهذا يعني أنه في حراسة الإرهاب الإلكتروني لابد من اتجاه إرادة المجاني إلى استخدام الوسائل الإلكترونية لتنفيذ هذه الأفعال لأغراض إرهابية.[1]

الفرع الثاني: القصد الجنائي الخاص

يكون القصد الجرمي خاصا إذ تطلب فيه المشرع إلى جانب العلم والإرادة عن دافع معين، وهو استهداف غاية يحددها القانون، وجريمة الإرهاب باستخدام الوسائل الإلكترونية يكون فيها هدف الجاني وغايته إثارة الرعب والخوف بين الأفراد.[2]

فالقصد الجنائي الخاص في جريمة الإرهاب باستخدام الوسائل الإلكترونية يكون الهدف الأخير والنهائي للجاني باستخدام الوسائل الإلكترونية هو الإخلال بالنظام العام عن طريق بث الذعر وإثارة الخوف والاضطراب بالمجتمع ويري الباحث أن جريمة الإرهاب باستخدام الوسائل الإلكترونية من الجرائم المقصورة التي يشترط لقيامها توافر القصد الجرمي.[3]

[1]– مصطفى سعد حمد مخلف، المرجع السابق، ص80–81.

[2]– المرجع نفسه، ص81.

[3]– المرجع نفسه ، ص 82.

الفصل الثاني:

جهود مواجهة

الإرهاب الإلكتروني

من لقد أصبح الإرهاب الإلكتروني يشكل خطرا كبيرا بالنسبة للدول التي تعتمد في إدارتها واقتصادها وأمنها على تقنية المعلومات حيث أصبحت هذه الأخيرة تشكل هاجسا كبيرا بعدما اتخذتها المنظمات الإرهابية كوسيلة لنشر غايتها، وبعد الزيادة الرهيبة في خطورة هذه الجريمة وانتشارها الواسع كان لابد من اتخاذ التدابير وتكثيف الجهود بين التشريعات وإبرام الاتفاقيات وتكوين المنظمات الدولية والإقليمية لمواجهة ومكافحة هذه الجريمة، لذا فقمنا بتخصيص هذا الفصل لجهود مواجهة الإرهاب الإلكتروني الذي تناولنا من خلاله في المبحث الأول (مكافحة الإرهاب الإلكتروني على المستوى الدولي) أما المبحث الثاني فخصصناه (للجهود الوطنية لمكافحة الإرهاب الإلكتروني).

المبحث الأول: مكافحة الإرهاب الإلكتروني على المستوى الدولي

إن الإرهاب الإلكتروني جريمة عابرة للحدود وهي تشكل خطرا على أمن الدول وقد فرضت خطورته على الحكومات اتخاذ التدابير اللازمة وسن تشريعات من أجل التصدي لهذه الجريمة سواء على المستوى الدولي أو الإقليمي، لذا قمنا بتقسيم هذا المبحث إلى مطلبين حيث خصصنا المطلب الأول لمكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية والإقليمية، أما المطلب الثاني فخصصناه للمكافحة على مستوى المنظمات الدولية.

المطلب الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية والإقليمية

إن الخوف والرعب الذي ينشره الإرهاب الإلكتروني دفع كل من الاتفاقيات الدولية على التعاون من أجل نص مختلف المواد لمكافحة الإرهاب الإلكتروني وكذلك هو الحال بالنسبة للمنظمات الإقليمية التي حاولت بدورها التعاون على مكافحة هذه الجريمة إقليميا، لذا سوف نتناول في الفرع الأول مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية والفرع الثاني مكافحة الإرهاب الإلكتروني على المستوى الإقليمي.

الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية

سنتطرق في هذا الفرع لمكافحة الإرهاب الإلكتروني في كل من اتفاقية إساءة استعمال تكنولوجيا المعلومات، واتفاقية بودابست.

أولا: اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات

أُصدرت الاتفاقية العالمية لمكافحة إساءة استعمال تكنولوجيا المعلومات رقم (63/55) في 12 أبريل 2000 من قبل الجمعية العامة لمنظمة الأمم المتحدة وهذا نتيجة لتزايد الجرائم المرتكبة عبر الانترنت، وقد كان هدف هذه الجمعية الدعوة إلى

الانضمام إلىجميع الاتفاقيات ذات الصلة بغية تكثيف الجهود لمحاربة الجريمة العابرة للحدود الوطنية ومنها الإرهاب الإلكتروني، والعزم على أن تكفل إتاحة منافع التكنولوجيا الجديدة وخاصة تكنولوجيا المعلومات والاتصالات للجميع بما يتفق مع التوصيات الواردة في الإعلان الوزاري الصادر من الدورة الموضوعية للمجلس الاقتصادي والاجتماعي للأمم المتحدة لعام 2000. [1]

كما تشير أيضا على أن قرار الجمعية العامة رقم (121/45 المؤرخ في 14 ديسمبر 1990) أيد توصيات مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، والذي دعا الدول أن تكثف جهودها لمكافحة إساءة استعمال الحواسيب بفعالية أكبر.[2]

نصت المادة 1 من اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55 لسنة 2000 في الفقرات (أ–د) على ما يلي:

أ–" ينبغي للدول أن تكفل عدم توفير قوانينها وممارستها فيها ملاذ أمن للذين يسيئون استعمال تكنولوجيا المعلومات لأغراض إجرامية "

ب–" ينبغي أن تنسق جميع الدول المعنية للتعاون في مجال إنفاذ القانون لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة بإساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية " [3]

ج–"ينبغي أن تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية "

[1]– علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق، ص330.

[2]– عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2019، ص47–48.

[3]– شاشوة ياسمينة، المرجع السابق، ص74.

د-" ينبغي تدريب العاملين في مجال نفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية "[1]

ثانيا: اتفاقية بودابست

تُعرف اتفاقية بودابست بالاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية، وقد وضعت هذه الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية، وعرضت للتوقيع في بودابست في 2001/11/23 ودخلت حيز التنفيذ في 2004، وهذه الاتفاقية متاحة أمام أية دولة من دول العالم للانضمام إليها.[2]

تشمل الاتفاقية 48 مادة موزعة على 4 فصول، تناول الفصل الأول تعريف المصطلحات المستخدمة، وتناول الفصل الثاني الإجراءات الواجب اتخاذها على المستوى المحلي في مجال قانون العقوبات والإجراءات الجنائية وقواعد الاختصاص القضائي، والأخير الشروط الختامية القضائي، ويهدف الفصل الثالث إلى تنظيم التعاون الدولي، ويضم الفصل الرابع والأخير الشروط الختامية[3].

وفي إطار هذا التعاون نصت الاتفاقية على أن " تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الإلكتروني لهذه الجرائم، " كما أنه يمكن لأي طرف في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل

[1]- شاشوة ياسمينة، المرجع السابق، ص74.

[2]- نجيب بن عمر عوينات، الإرهاب الإلكتروني: المفهوم والجهود الدولية والإقليمية لمكافحته، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، معهد العالي للإعلامية، الكاف جامعة جندوبة، تونس، العدد السادس، جوان2017، تاريخ الصدور: 2017/04/20، ص18.

[3]- نجيب بن عمر عوينات، المرجع نفسه، ص18.

الاتصال السريع مثل الفاكس أو البريد الإلكتروني على أن تستوفي تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك. [1]

الفرع الثاني: مكافحة الإرهاب الإلكتروني على المستوى الإقليمي

وسنتناول في هذا الفرع كل من الإتحاد الأوروبي وجامعة الدول العربية

أولا: جهود الاتحاد الأوروبي لمكافحة الإرهاب الإلكتروني

في عام 2002 اعتمد مجلس الإتحاد الأوروبي القرار الإطاري (2002/475/JHA) الصادر في 13 حزيران / يونيه 2002 بشأن مكافحة الإرهاب والذي يوحد تعريف الجرائم الإرهابية في جميع دول الأعضاء في الإتحاد الأوروبي عبر طرح تعريف محدد ومشترك لمفهوم "**الإرهاب**" ويُؤسس قواعد للولاية القضائية لضمان إمكانية ملاحقة الجرائم الإرهابية قضائيا بفاعلية، ويُبين تدابير محددة فيما يخص ضحايا الجرائم الإرهابية، وفي إطار التصدي لخطر الإرهاب المتزايد بما يشمل استخدام تكنولوجيا جديدة مِثل الانترنت، عدل القرار الإطار(2002/475/JHA) في عام 2008 ليتضمن على وجه التحديد أحكاما بشأن التحريض العلني على ارتكاب جرائم إرهابية، والتجنيد و التدريب بغرض الإرهاب، وفي ذلك القرار أتى مجلس الإتحاد الأوروبي أيضا على ذِكر قرار مجلس الأمن رقم 1624 (2005) الذي دعا فيه المجلس الدول أن تحظر بنص القانون التحريض على ارتكاب عمل إرهابي أو أعمال إرهابية وأن تمنع ذلك التصرف[2].

ويوفر القرار الإطاري (2008/919/JHA) سند للملاحقة القضائية بشأن نشر الدعاية الإرهابية والدراية الفنية اللازمة لصنع القنابل عبر الانترنت، إذ كان هذا النشر متعمدا ومستوفيا لشروط الجرائم المذكورة، وتستند تعديلات القرار الإطاري (2002/475/JHA) فيما يتعلق بالتحريض العلني والتجنيد والتدريب إلى أحكام مشابهة

[1]– نجيب عمر عوينات، المرجع السابق، ص18.

[2]– مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الانترنت لأغراض إرهابية، تقرير منشور على الموقع : https://www.unodc.org/، تاريخ التصفح: 2022/05/03، الساعة 18:55، ص22.

في اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، وقد استحدث القرار الإطاري (2008/919/JHA) جرائم جديدة فيما يتعلق بالسلوكيات التي قد تؤدي إلى أعمال إرهابية بغض النظر عن الوسائل أو الأدوات التكنولوجية التي ترتكب هذه الجرائم عبرها، وكما هو الحال في اتفاقية مجلس أوروبا المتعلقة بمنع الإرهاب، تشمل أحكام القرار الإطاري (2008/919/JHA) الأنشطة التي تُمارس عن طريق الانترنت وإن كانت غير مخصصة لها. [1]

ثانيا: جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني

تصدت جامعة الدول العربية كمنظمة إقليمية عربية للأنشطة غير المشروعة المرتكبة بواسطة تقنية المعلومات وأن ميثاقها لا ينص صراحة على مكافحة الإرهاب وما يرتبط به من تفرعات، ولكن المادة (2) منه أوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها، وهذا ما تنطوي عليه وسائل الإرهاب الإلكتروني مِن تجاوزات وإخلال السلطة وسيادة الدول عبر التعرض لنظم المعلومات بالمؤسسات السيادي، فضلا عن إمكانية استغلال المعلومات الحساسة وتوظيفها ضد مصالح الدول العربية المستهدفة الأمر الذي يستدعي الدول العربية لمواجهة مثل هذه الأنشطة الإرهابية في الفضاء الإلكتروني، وهو اتجاه أكدته المادة (3) من الميثاق حينما خولت مجلس الجامعة بتقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن والسلم، ويمكن اعتبار الاعتداء على نظم المعلومات التي تعتمده المؤسسات الرسمية للدول العربية ومحاولة تدميرها أو الإضرار بها وإشاعة الرعب والتحريض ضد النظام القائم التي تتم عبر آليات الإرهاب الإلكتروني من صور العدوان وفقا لقواعد القانون الدولي وميثاق منظمة الأمم المتحدة [2].

[1]– مكتب الأمم المتحدة المعني بالمخدرات والجريمة، المرجع السابق، ص23.

[2]– شاشوة ياسمينة، المرجع السابق، ص100.

أسفرت جهود الجامعة العربية للتصدي للأنشطة غير المشروعة بواسطة التقنية الإلكترونية عن إصدار مجلس وزراء العرب القرار رقم (229 سنة 1999) متعلق بإصدار القانون الجزائي العربي كقانون عربي نموذجي، إذ أن ابرز ما يمكن رصده من جهود على صعيد منظمة جامعة الدول العربية في مضمار التصدي لجرائم الإرهاب الإلكتروني وجرائم الحاسوب هو اعتماد مجلس وزراء العدل العرب لهذا القانون والذي تضمن فصلاً خاصًا بالاعتداء على حقوق الأشخاص الناتج عن المعلوماتية[1] .

المطلب الثاني: مكافحة الإرهاب الإلكتروني في المنظمات الدولية

إن المنظمات الدولية في سعي دائم للحفاظ على الأمن الدولي وذلك بعد الانتشار الرهيب للجرائم خاصة بعد اقترانها بالشبكة المعلوماتية، مما سهل و سرع انتشارها فكان لابد من التدخل السريع من أجل الحد منها خاصة بعد ظهور الإرهاب الإلكتروني الذي سارعت كل من منظمة الأمم المتحدة ومجموعة الدول الثمانية بوضع مجموعة من القرارات والقوانين من أجل مكافحته.

الفرع الأول: جهود كل من منظمة الأمم المتحدة و مجموعة الدول الثمانية

سوف نتناول في هذا الفرع ما تم إصداره من هاتين المنظمتين.

أولا: منظمة الأمم المتحدة

أصدرت الأمم المتحدة مجموعة من القوانين عبر جمعيتها العامة التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال و المعلومات استخداما غير سلمي، ففي 22 نوفمبر 2002 اتخذت قرار بشأن التطورات في ميدان المعلومات والاتصالات السلكية و اللاسلكية في سياق الأمن الدولي، وفي ديسمبر من نفس السنة اتخذت قرار إرساء ثقافة عالمية لأمن الفضاء الإلكتروني واعتبر من القرارات الهامة التي

[1]– شاشوة ياسمينة، المرجع السابق، ص100–101.

استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث الدول والمنظمات الدولية والإقليمية على تكثيف التعاون الدولي لمجابهة الإرهاب الإلكتروني[1].

وقد أكدت تقارير و قرارات صادرة عن الأمم المتحدة مؤخرًا تأكيدا خاصا على أهمية مكافحة استخدام الانترنت في أغراض إرهابية باعتبارها جزءًا رئيسيا من أي إستراتيجية شاملة لمكافحة الإرهاب، ففي تقرير الأمين العام المقدم للجمعية العامة عن عام 2006 والذي حمل عنوان "**الإتحاد في مواجهة الإرهاب توصيات لإستراتيجية عالمية لمكافحة الإرهاب**" أفاد الأمين العام صراحة بأن القدرة على إيجاد الأموال ونقلها، وعلى حيازة الأسلحة وتجنيد الكوادر وتدريبها على الاتصال خاصة باستخدام الانترنت هي كلها عناصر أساسية بالنسبة للإرهابيين، واستطرد الأمين العام مؤكدًا على أن الانترنت قد باتت أداة تتسارع وتيرة توسع الإرهابيين في استخدامها في تجنيد الأفراد ونشر المعلومات والدعاية، الأمر الذي لابد من مواجهته بعمل منسق بين الدول الأعضاء مع احترام حقوق الإنسان والتقيد بالالتزامات الأخرى التي يفرضها القانون الدولي[2].

هذا وقد نبه مجلس الأمن في القرار ذي العدد (1963 لعام 2010) إلى "**ازدياد استخدام الإرهابيين التكنولوجيا الجديدة للمعلومات والاتصالات وخاصة الإنترنت لأغراض التجنيد عبر الإنترنت وكذلك التحريض على دعم الأعمال الإرهابية**" بوصفها أنماط مستحدثة الاستخدامات الإرهابيين للإنترنت لمعطيات الشبكة الدولية للمعلومات، وكان القرار ذي العدد(2255 في شباط عام 2015) أكثر شمولا لطرق استخدام الإرهابيين للإنترنت في أنشطتهم الإرهابية، إذ تضمن "**الإعراب عن قلقه من تزايد لجوء الإرهابيين إلى استعمال**

[1]– سارة بوحادة، مداخلة حول أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية للعلوم السياسية، الجزائر، ص13.

[2]– مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق، ص18.

تكنولوجيا المعلومات ولاسيما شبكة الإنترنت من أجل تسيير الأعمال الإرهابية والتحريض الإرهاب أو تجنيد مرتكبيها أو تمويلها"[1].

وفي مؤتمر منظمة الأمم المتحدة الثاني عشر لمنع الجريمة و العدالة الجنائية عام (2010)، عُقد هذا المؤتمر في سلفادور–البرازيل من (12–19 نسيان عام 2010) تحت عنوان إستراتيجيات شاملة في تحديات عالمية والذي نظم منع الجريمة و العدالة الجنائية وتطورها في عالم متغير، وتضمن جدول الأعمال ثمانية بنود وكان من ضمنها جرائم الإنترنت، والتعاون الدولي في مكافحة هذه الجريمة[2] .

ثانيا: مجموعة الدول الثمانية

عملت مجموعة الدول الثمانية على مكافحة الإرهاب الإلكتروني من خلال الإعلانات والمؤتمرات والملتقيات والاجتماعات حيث سعت إلى تعزيز الحرية والديمقراطية وحقوق الإنسان والتعاون الدولي في القضايا المتعلقة بالانترنت حيث أنشأت الفريق الفرعي للجرائم الإرهابية الإلكترونية التقنية في قمة مجموعة (G–8) في (11/10/2004) حيث تم اعتماد وزراء العدل والداخلية التابعين لبلدان المجموعة في اجتماعاتهم المختلفة آلية لمكافحة العديد من جرائم الإنترنت.[3] وتستند إلى المبادئ التالية:

- ✓ التنسيق بين جميع الدول المعنية بملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بصرف النظر عن مكان حدوث الضرر
- ✓ عدم إتاحة ملذات آمنة للمعتدين على تكنولوجيا المعلومات، تدريب الموظفين المكلفين بتنفيذ القوانين، إضافة لتجهيزيهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية

[1]– نايف أحمد ضاحي الشمري، عمر عباس خضير العبيدي، جرائم الأمن السيبراني واليات مكافحتها في إطار القانون الدولي، 5 International Legal Issues Conferenc – ILIC2020 – ISBN (978–9922–90–5)، (1–5)، ص406.

[2]– المرجع نفسه، ص406.

[3]– شاشوة ياسمينة، المرجع السابق، ص82.

العالمية.[1] كما ناقشت مجوعة الدول الثماني في (موسكو-روسيا) سنة 2006 الجريمة الإرهابية الإلكترونية وقضايا الفضاء الإلكتروني وأصدرت بيان موسكو الذي تم التأكد فيه على منع الأعمال الإجرامية المحتملة واتخاذ التدابير الضرورية، وكذلك اجتمع وزراء العدل و الداخلية لدول (G-8) في 23-25 ماي عام 2007 في (ميونيخ ألمانيا) واتفق الأعضاء على العمل من خلال الأطر القانونية لتجريم أشكال معينة بشأن استخدام الإنترنت لأغراض إرهابية[2]

وفي عام 2011 في فرنسا أصدرت أيضا الدول الثمانية الجزء الثاني من الإعلان في قضايا الإنترنت في البنود (4 إلى 22) حيث أكدت فيه أن شبكة الإنترنت أصبحت ضرورية في كافة أنحاء العالم، حيث تلعب دورًا في نمو المجتمعات واقتصاديات الدول وتعزيز الحرية والديمقراطية وحقوق الإنسان حيث دعى الإعلان إلى تعزيز التعاون داخل جميع المحافل الدولية التي تتناول حركة الانترنت.[3]

الفرع الثاني: جهود المنظمات العالمية المتخصصة

وهما المنظمة العالمية للملكية الفكرية ومنظمة التعاون الاقتصادي

أولا: المنظمة العالمية للملكية الفكرية

تم التوقيع على الاتفاقية المنشئة لها في ستوكهولم "**1967**"، وأصبحت تابعة لأمم اعتبارا من عام 1974، تشجع هذه المنظمة على توقيع معاهدات دولية جديدة والتنسيق بين التشريعات القومية وتقديم المساعدات القانونية للدول النامية بهدف حماية الملكية الفكرية وتنميتها، ومع تزايد حاجة المنظمة على غرار باقي المنظمات لحماية البرامج شكلت مجموعة عمل تضم عددًا من الخبراء بهدف حماية برامج الحواسيب من التهديد أو

[1]- شاشوة ياسمينة، المرجع نفسه، ص82

[2]- المرجع نفسه، ص82.

[3]- المرجع نفسه، ص83.

الهجوم الإلكتروني حيث أفضى ذلك بعد سلسلة من الاجتماعات إلى انتهاج أغلب الدول والميل إلى برامج الحاسوب لقوانين حماية حق المؤلف.[1]

ثانيا: منظمة التعاون الاقتصادي و التنمية (OECD)

تسعى منظمة التعاون الاقتصادي والتنمية (OECD) بأول مبادرة دولية لها أن تتعامل مع المشكلات المتمثلة بالاعتداء على الأموال المعلوماتية والمتكونة من مجموعة الأدوات المكونة للحاسوب والبرامج و البيانات والتي يترتب عليه مشكلات قانونية.[2]

إن الهدف من هذه المنظمة من هذه المنظمة تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتَناغُم التطور الاقتصادي مع التنمية الاجتماعية يظهر اهتمام هذه المنظمة بالجرائم الإرهابية الإلكترونية الدولية من خلال وضعها لعديد من الأدلة التي تبناها مجلس المنظمة مع توصية الأعضاء بالالتزام بها في سبيل مكافحة الإرهاب الإلكتروني، كما عملت أيضا على إرسال استبيان إلى الدول الأعضاء فيها لتحديد مفهوم جرائم الحاسوب وتعريفها مع تبيين أفعال جرائم الإرهاب الإلكتروني وتكييف نصوص الاتفاقيات الدولية لمكافحة هذه الأنشطة المستحدثة، وقامت هذه المنظمة في عام 1983 بعقد اجتماع في باريس للبحث في جرائم الإرهاب الإلكتروني.[3]

[1]– علي بوعمرة، المرجع السابق، ص40.

[2]– يونس عرب، جرائم الكومبيوتر والإنترنت، ط1، اتحاد المصارف العربية، بيروت، 2002، ص322 .

[3]– المرجع نفسه، ص322.

المبحث الثاني: الجهود الوطنية لمكافحة الإرهاب الإلكتروني

بعدما تطرقنا إلى ماهية الإرهاب الإلكتروني تعرفنا على الخطر الذي يشكله هذا الأخير مما دفع دول العالم إلى تكثيف الجهود من أجل مكافحته.

ومن خلال هذا المبحث سنعرض مختلف الجهود التي بذلتها الدول في سبيل مكافحة هذه الجريمة التي باتت تشكل خطرا على أمنها واستقرارها لذا تطرقنا إلى 3 مطالب الأول خصصناه لدول الغربية والثاني لدول العربية أما الثالث فتناولنا فيه الجهود الوطنية.

المطلب الأول: جهود بعض الدول الغربية لمكافحة الإرهاب الإلكتروني

إن مكافحة الإرهاب الإلكتروني أصبحت ضرورة حتمية خاصة وأنه يهدد أمن الدول واستقرارها، ومن خلال هذا الخطر الذي يشكله عملت التشريعات الدولية على وضع قوانين لمكافحته، ونذكر من هذه الدول ما يلي:

- **الولايات المتحدة الأمريكية:** لقد أجرت الولايات المتحدة الأمريكية تجربة واسعة فيما يخص تأثيرات الإرهاب الإلكتروني، حيث أنشأت هيئات أمنية حكومية تراقب البريد الإلكتروني، وهي تتألف من عدة مراكز وأقسام تختص بمكافحة جرائم كثيرة أهمها: جرائم الإرهاب، الجريمة المنظمة عبر الوطنية، جرائم التهريب وغسل الأموال، كذلك إنشاء وكالة الاستخبارات (CIA) لمجموعة منظمة تتعاطى مع جوانب تخص الإرهاب الإلكتروني أطلقت عليها اسم "**مركز حرب المعلومات**" Informations (War's Center) والذي يعمل دون توقف. [1]

ومن جهة أخرى، فإنه يجب الإشارة بأن الرئيس الأمريكي السابق بوش الابن، قام بإصدار القرار الرئاسي 13231 المؤرخ في 2001/10/16 بشأن حماية البنية التحتية

[1]– توفيق شريخي، المرجع السابق، ص66.

الحساسة في عصر المعلومات، والذي قام بموجبه بإنشاء مجلس يضم ثلاثين رئيسا لشركات مساهمة منشورة حول أمن النظام المعلوماتي في الدولة.[1]

وقد قام المشرع الأمريكي بإصدار قانون جديد, و هو القانون الوطني 2001 المؤرخ في 2001/10/26 والذي كان له تأثير امتد إلى استحداث تعديلات في التشريعات النافذة المفعول على المستوى الفدرالي في الولايات المتحدة .[2]

وهناك العديد من الخطوات الأخرى التي اعتمدت عليها الولايات المتحدة الأمريكية لمكافحة جريمة الإرهاب الإلكتروني نذكر منها:

- ✓ عمد البنتاغون إلى إنشاء وحدة عسكرية متخصصة عهد إليها بمهمة تحصين الفضاء المعلوماتي الأمريكي وتأمين شبكات الاتصال الحساسة في الولايات المتحدة ضد أي حرب إرهابية محتملة[3].
- ✓ إصدار قانون تعزيز أمن المعلومات في 2002، ووضع الإستراتيجية الوطنية لتأمين الفضاء الإلكتروني في 2003[4].

- **فرنسا:** التهديد الإرهابي لم يكن ينظر إلى قُوته وخُطورته حيث عرف تغييرًا عميقًا في طبيعته، وسريا على نهج معظم شركائها كيفت فرنسا مجهوداتها في هذا السياق الجديد، وقد عزز قانون 23 كانون الثاني 2006 حول مكافحة الإرهاب الاستجابة لمتطلبات الوقاية وفق المتغيرات السريعة في وسائل النقل وتقنيات الاتصالات، وقد أسفرت هذه الجهود عن وضع إستراتيجية طويلة الأجل تم عرضها ضمن الكتاب الأبيض لمواجهة الإرهاب، وهذا الكتاب هو ثمرة تفكير بين

[1]– هروال نبيلة، المرجع السابق، ص357.

[2]– المرجع نفسه، ص357.

[3]– ياسمينة شاشوة، المرجع السابق، ص69.

[4]– المرجع نفسه، ص69.

المهنيين ورجال المخابرات والقضاة والمسئولين الحكوميين والصحفيين والأكاديميين[1].

إن هذا الكتاب الأبيض هو وثيقة جاءت واضحة المعالم ومحددة الأهداف ومهمة على مستوى الرؤية الإستراتيجية التي رُسِمَت لها، ورغم أنها لا تتبنى الرؤية الأمريكية في الحرب ضد الإرهاب، إلا أنها من خلال كتابها الأبيض تعكس تماما مدى جُهوزيتها أمام الخطر الحاذق بالدولة حيث سارعت إلى مواجهة الموقف عبر عدة مسارات[2].

وقد التجأت فرنسا ابتداء في محاربة الإرهاب إلى قانون العقوبات وقانون الإجراءات الجنائية مع الأخذ بنظام قانون يخالف القواعد العامة واعتبار العمل الإرهابي وصفا له ولذاتيته القانونية، ولم يترتب عن مخالفة القواعد العامة في نصوص قانوني العقوبات والإجراءات الجنائية أي نقد جوهري من جانب المجلس الدستوري الفرنسي الذي أكد في 3 سبتمبر 1986 أن نصوص محاربة الإرهاب تجد تبريرها في الطابع الخاص للإرهاب. [3]

وفي 23 يناير 2006 صدر في فرنسا قانون مكافحة الإرهاب الفرنسي مُتمثلا في إجراء تعديلات على القانون رقم 73 الصادر في 21 يناير 1995 بشأن التوجيه ووضع البرامج في مجال الأمن، وبمقتضى القانون الصادر سنة 2006 طرأ نوعان من التعديلات المباشرة على قانون العقوبات الفرنسي، ومن بين هذين النوعين التغيير الذي مس شأن الجماعات الإرهابية وذلك بتشديد العقاب على مديريها والتوسع في تجريم هذه

[1]– أبو عمار، ميلود عبد الرحمان بنعتيك، الإرهاب المعلوماتي، مداخلة المؤتمر الدولي لمكافحة جرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية 2015، السعودية، الرياض، متوفر على الموقع: http://search.mandumah.com/Record/690587 ، تاريخ التصفح: 16 ماي 2022 على الساعة 15:51، ص147.

[2]– المرجع نفسه، ص147.

[3]– المرجع نفسه، ص146.

الجماعات بالنظر إلى الجرائم التي تحظر لها في المواد (421_21 و 421_5/ 1 و421_6). [1]

وباستحداث قانون الإجراءات الجنائية المادة 706_24 تضمن تعديلات نصت على مركزية محاكم تطبيق العقوبات بباريس بشأن المحكوم عليهم في جرائم إرهابية وإنشاء محاكم جنايات متخصصة للأحداث الإرهابية (المادة 706_25). [2]

- **اليابان:** دعت الحكومة اليابانية إلى التصدي بسرعة لخطر الإرهاب الإلكتروني بعد اختراقات عديدة لأنظمة الكومبيوتر، على غرار الموقع الحكومي الياباني ومحو بيانات هامة تتضمن إحصاءات متعلقة بالسكان ومعلومات مهمة أخرى[3].
- **روسيا:** قدمت روسيا في العام 2015 على مشروع " **أمن المعلومات الدولية** " والتي أكدت فيها الحاجة إلى معاهدة دولية جادة تعني بالفضاء الإلكتروني، نظرا لما تقتضيه ظروف العصر الراهن والتحولات الإلكترونية السريعة[4].
- **ألمانيا:** اهتمت الدولة الألمانية إلى حد كبير بتأمين أنظمة الكومبيوتر وقاعدة البيانات العامة والحكومية خاصة بعد اعتداءات 11 سبتمبر، فقد ركز المكتب الاتحادي للأمن وتكنولوجيا المعلومات على كل ما يتعلق بتأمين البنية التحتية لتكنولوجيا المعلومات[5].
- **السويد:** صدر قانون البيانات السويدي عام 1973 م، والذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم

[1]– أبو عمار، ميلود عبد الرحمان بنعتيك، المرجع السابق، ص146.

[2]– المرجع نفسه، ص146.

[3]– علي عدنان الفيل، المرجع السابق، ص106.

[4]– توفيق شريخي، المرجع السابق، ص68.

[5]– المرجع نفسه، ص68.

الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول الغير مشروع عليها. [1]

- **بريطانيا:** أقرت بريطانيا قانون مكافحة التزوير والتزييف عام 1971 م، والذي شمل في تعاريفه الخاصة تعريف أداة تزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى [2].
- **دَوْلَتَيْ المجر و بولندا:** يوجد في كل من المجر و بولندا قوانين خاصة بجرائم الحاسب الآلي والإنترنت توضح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي أو إفشاء كلمات السر أو الأكواد الخاصة بالبرامج، كما تعطي الشاهد أيضا الحق في الامتناع عن طبع المعلومات المسترجعة من الحاسب الآلي متى كان ذلك إلى إدانته أو إدانة أحد أقاربه، بل تذهب القوانين الجنائية المعمول بها في بولندا إلى أبعد من هذا حيث أنها تنص على أن لا يقابل ذلك أي إجراء قسري أو تفسيره بما يضر المتهم[3].

المطلب الثاني: مكافحة الإرهاب الإلكتروني في بعض الدول العربية

لم تقتصر مكافحة الإرهاب الإلكتروني على الدول الغربية فحسب، بل امتدت لتشمل أيضا الدول العربية ومن بين هذه الدول نذكر ما يلي:

- **السعودية:** صدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات

[1]– رفد عيادة الهاشمي، الإرهاب الإلكتروني، ط1، دار أمجد للنشر والتوزيع، الأردن، 2019، ص32.

[2]– المرجع نفسه، ص33.

[3]– المرجع نفسه، ص 34.

واللوائح كقرار مجلس الوزراء رقم (163) في 1417/10/24 هـ، الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها ومن ذلك:

1. الامتناع من الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الانترنت، أو إلى أي معلومات خاصة، أو مصادر معلومات دون الحصول على موافقة المالكين أو من يتمتعون بحقوق الملكية لتلك الأنظمة و المعلومات و المصادر
2. الامتناع عن إرسال أو استقبال معلومات مشفرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية
3. الامتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح
4. الامتناع عن إشراك الآخرين في حسابات الاستخدام، أو اطلاعهم على الرقم السري للمستخدم
5. الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها. [1]

كما تم إصدار أنظمة تحد من جرائم الإرهاب الإلكتروني، وفي هذا السياق تم إقرار نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/17 وتاريخ 1428/3/8 هجري بناء على قرار مجلس الوزراء رقم (79) وتاريخ 1428/3/7 هجري الذي فرض عقوبات بالسجن والغرامة أو كليهما معا على كل شخص ينشأ موقعا لمنظمات إرهابية على شبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أو نشر كيفية صنع المتفجرات. [2]

وفي هذا السياق تنُص المادة السابعة من هذا القانون على أنه "يُعاقب بالسجن مدة لا تزيد على عشر سنوات و بغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يقوم بإنشاء موقع منظمات إرهابية على الشبكة المعلوماتية، أو أحد

[1] علي بوعمرة، المرجع السابق، ص49.

[2] – المرجع نفسه، ص50.

أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات أو أداة تستخدم في الأعمال الإرهابية"[1].

- **الأردن:** بعد التفجيرات التي تعرضت لها فنادق العاصمة "**عَمان**" في العام 2005، والتهديدات الإرهابية التي تزداد يوما بعد يوم خصوصا في ظل اكتساح التكنولوجيا الرقمية لكل نقطة في العالم، وعلى الرغم من أن القوانين الأردنية كانتمِن قبل تفتقد لإشارة واضحة و صريحة لما يسمى الإرهاب الإلكتروني، إلا أنها أشارت إلى كل أشكاله وكل ما ينطوي تحته.[2]
- تُعتبر الأردن من السَباقين في المصادقة والتوقيع على الاتفاقيات والبروتوكولات المتعلقة بقمع الإرهاب بشتى أنواعه حيث أنه:
- صَادق على الاتفاقية العربية لمكافحة الإرهاب في العام 1998
- وقَع على اتفاقية محاربة الجريمة المنظمة عبر الوطنية (اتفاقية باليرمو) في العام 2002.
- صَادق على اتفاقية الأمم المتحدة لقمع تمويل الإرهاب في العام 2003
- وقَّع على الاتفاقية العربية لمكافحة غسل الأموال وتمويل الإرهاب في العام 2010.

كما أَبرمت الأردن في إطار التعاون الثنائي أكثر من اتفاقية ذات طابع أمني تضمنت نُصوصا تكفل محاربة الجريمة المنظمة والإرهاب بما فيها الإرهاب الإلكتروني مع كل من سوريا، العراق، المجر، ايطاليا، إسبانيا.... وفي العام 2010 أصدرت الأردن قانون جرائم أنظمة المعلومات.[3]

---

[2]– توفيق شريخي، المرجع السابق، ص70.

[3]– المرجع نفسه، ص70.

كما قامت الحكومة الأردنية بإنشاء العديد من المراكز بُغية تحقيق استراتيجياتها الأمنية ومنها:

- شُعبة الجرائم الإلكترونية وإدارة البحث الجنائي التابعة لمديرية الأمن، تتضمن إنشاء قسم خاص بالإسناد والتحقيق الفني في العام 2008، ويعني بالتحقيق في جرائم تكنولوجيا المعلومات والاتصالات والانترنت
- مركز"**الملك عبد الله آل ثاني**" للتصميم و التطوير، ويعني بالبحث والتطوير في مجال الأنظمة الدفاعية أنشئ بموجب إرادة ملكية من الملك عبد الله آل ثاني

المركز الوطني لتكنولوجيا المعلومات، أنشئ سنة 2003 بموجب قانون توظيف موارد تكنولوجيا المعلومات الوطنية خلفا لمركز المعلومات الوطني 1993[1].

وفي عام 2012 أصدر المركز "**الإستراتيجية الوطنية لضمان أمن المعلومات و الأمن السيبراني**" والتي تتضمن إجراءات ضمان أمن نظم المعلومات التحتية والحيوية وتعني بعدة نقاط أهمها:

- تعزيز الأمن الوطني الأردني من خلال منع هجمات الإرهاب الرقمي والقرصنة للبنية التحتية للمعلومات الأردنية.
- تقليل المخاطر المتعلقة بالبيئة التحتية وشبكة المعلومات الحكومية من خلال تقليل نقاط الضعف.
- زيادة الوعي حول مخاطر الإرهاب الإلكتروني وضرورة استتباب أمن المعلومات وأهميته للأمن القومي.

وبهذا تكون الأردن قد قطعت شوطا كبيرا في التصدي للإرهاب الإلكتروني.[2]

- **سوريا:** تعتبر من بين الدول التي أصدرت قوانين بشأن مكافحة الإرهاب الإلكتروني، فقد صدر فيها قانون" **التواصل على الشبكة ومكافحة الجريمة**

[1]- توفيق شريخي، المرجع السابق، ص70.

[2]- المرجع نفسه، ص70-71.

المعلوماتية "، وتضمن الفصل الثالث منه تحت "**عنوان مكافحة الجريمة المعلوماتية** " المواد 15 حتى 23 وفيها تعداد للجرائم وموضوعه، وقد قسم هذا الفصل الجرائم الإلكترونية إلى جنح وجنايات، لكنه لم يتناول الجريمة الإرهابية الإلكترونية مباشرة ولكنه نص في المادة 30 منه ضمن الفصل الخامس تحت عنوان" **أحكام عامة و ختامية** " على تشدد العقوبات وفق القواعد العامة للتشديد المنصوص عليها في قانون العقوبات النافذ في الحالات التالية: إذا كان موضوع الجريمة يمس الدولة أو السلامة العامة، وإذا جرى ارتكاب الجريمة بواسطة عصابة منظمة. [1]

- **مصر:** صدر في الجمهورية العربية المصرية قانون "**في شأن مكافحة جرائم تقنية المعلومات**" تضمن في الباب الثالث منه الجرائم الإلكترونية أو الجرائم المعلوماتية من المادة 13 إلى المادة 33، وكان القانون المصري قبل ذلك نص في المادة 15 منه على أنه يعاقب كل من قام بطريقة مباشرة أو غير مباشرة، ويقصد ارتكاب جريمة إرهابية في الداخل أو الخارج، بإعداد أو تدريب أفراد على صنع واستعمال الأسلحة التقليدية أو الغير تقليدية، أو وسائل سلكية أو اللاسلكية أو الإلكترونية أو أية وسيلة أخرى، إذا هنا المشرع المصري قد لاحظ إمكانية استخدام الانترنت وهو من الوسائل الإلكترونية للقيام بعمل إرهابي.[2]
- **قطر:** صدر القانون رقم 14 لسنة 2014 المتعلق بمكافحة الجرائم الإلكترونية الذي نص صلب المادة 5 منه على أن "**يُعاقِب القانون بالحبس مدة لا تتجاوز ثلاث سنوات و الغرامة 500 ألف ريال لإدارة موقع يبيع**

[1]– نجاة رامز أبو شقرا، جرائم الإرهاب الإلكتروني في ظل محدودية النص، رسالة مقدمة لنيل درجة الماجستير، القانون الجزائي، كلية الحقوق والعلوم السياسية، جامعة بيروت العربية، 2020، ص11–12.

[2]– المرجع نفسه ، ص12.

تنظيما إرهابيا" أو نشر أخبار تعرض الدولة للخطر أو ترويج الأخبار الكاذبة ضد سلامة الدولة "، أو تسهيل الاتصال بقيادة و أعضاء الجماعات الإرهابية أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تضييع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية. [1]

- **السودان:** صدر قانون جرائم المعلوماتية لسنة 2007 الذي نص في الفصل الخامس منه على أنه "**كل من ينشئ أو ينشر أو يستخدم موقعا على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابية تحت أي مسمى لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة أو بالعقوبتين معا**".[2]

المطلب الثالث: مكافحة الإرهاب الإلكتروني في التشريع الجزائري

إن الجزائر شأنها شأن الدول الأخرى بعد معاناتها الطويلة من الإرهاب أصبحت ذات خبرة في التعامل معه، لذلك فإنه بعد بروز الإرهاب الإلكتروني سارعت مباشرة إلى سن نصوص قانونية لمكافحته والتخلص منه، لذا خصصنا هذا المطلب لدراسة هذه الجريمة داخل الوطن وقد تطرقنا إلى ما يلي:

الفرع الأول: واقع الإرهاب الإلكتروني في الجزائر

صرح القائد العام للدرك الوطني الجزائري السابق في كلمة له ألقاها بمناسبة افتتاح الندوة الدولية حول "**الأمن السيبراني**"، حيث قال أن" **الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر، من خلال تنامي مظاهر الترويج لكل أشكال العنف**

[1]– نجيب بن عمر عوينات، المرجع السابق، ص22.

[2]– المرجع نفسه، ص21.

ولإرهاب والتطرف باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الإلكترونية" لذلك دعا إلى إطلاق خلايا أمنية متخصصة من أجل حماية المواطن الجزائري وخاصة عنصر الشباب.[1]

أما التنظيم الإرهابي "**داعش**" فله أزيد من 50 ألف موقع إلكتروني، 90 ألف باللغة العربية على موقع التواصل الاجتماعي "فيسبوك" و40 ألف بلغات أخرى، ورغم الخطورة الكبيرة التي يخلفها هذا التنظيم عبر مواقعه إلا أن تأثيره على المجتمع الجزائري كان قليلا، فقد كشف السيد محمد عيسى وزير الشؤون الدينية والأوقاف السابق أن التجنيد الإلكتروني لداعش في الجزائر عن طريق شبكة الانترنت ومواقع التواصل الاجتماعي لم يتجاوز 100 شاب جزائري.[2]

إن هاته الحصيلة رقم ضئيل إذا ما قُورِن بعدد المجندين من دول عربية أخرى، وهذا يعود لنتائج العشرية السوداء التي عاشاها الجزائريون نهاية القرن الماضي.[3]

الفرع الثاني: إجراءات الوقاية لمكافحة الإرهاب الإلكتروني

سنتطرق من خلالها إلى عنصرين مهمين آلا وهما:

أولا: إنشاء مراكز التوجيه العسكري

إن الأزمات التي مرت بها الكينونة الجزائرية في القرن الماضي قد أظهرت بشكل جلي التحديات الأمنية الخطيرة التي مر بها العالم النظام الأمني الجزائري على غرار بقية الأنظمة لدول العالم الثالث خلال فترة التحول من الحرب الباردة إلى ما بعد هذه الحرب،

[1]– بن مرزوق عنترة، الكر محمد، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والاجتماعية، العدد 38، جوان2018، ص37.

[2]– المرجع نفسه ، ص37.

[3]– المرجع نفسه، ص37.

وذلك من حيث بنائها وطرق التقرب منها والتحدي الوحيد الذي يواجهه النظام الأمني الجزائري على غرار النظام العالمي هو التهديدات التي يثيرها الإرهاب الحديث.[1]

وعلى هذا الأساس يأتي مركز التوجيه العسكري في عمليات مكافحة الإرهاب، وهي مقاربة إجرائية للحصول على نتائج إستراتيجية أو أثر عملياتي على التنظيمات الإرهابية المنتشرة إلكترونيا وحدوديا على وجه التحديد وذالك من خلال تطبيق تعاون مضاعف ومتعدد الجوانب على أوسع مدى للقدرات العسكرية والغير عسكرية، وهذه المقاربة تعتبر مقاربة تكيفية تتخذ شكلا متداخلا لتمتد وتشمل الأبعاد الميدانية والعملياتية والإستراتيجية لأي اشتباك.[2]

إن هذا الأساس المتين لهذه العمليات يتضمن خلق بعض الأحداث وحسن الاستفادة منها، وبالرجوع إلى الهدف الأساسي لمركز التوجيه العسكري الجزائري في مكافحة الإرهاب هو على المستوى الإستراتيجي أو السياسي فإن هذا يؤدي إلى مفهوم عمق الإستراتيجية وبأن الحرب نفسها هي ببساطة امتداد للسياسة بوسائل أخرى وهذا يتطلب الحاجة إلى توجيه سياسي حول إطار إستراتيجي، بحيث يجري التخطيط للعمليات المجدية في مركز التوجيه العسكري الجزائري في عمليات مكافحة الإرهاب والتي يمكن تعريفها بالتطبيق المتماسك والمترابط لكافة الموارد القومية وعلى مختلف الأصعدة الوطنية توجهها الأهداف الإستراتيجية، والجدوى من هذا المفهوم هو إعطاء القادة ذوي الفكر الواسع القدرة على تحديد هدف التنظيمات الإرهابية بطريقة تسهل تحقيق الهدف كاملا للإستراتيجية الحاذقة وهو "**استلام الجماعات الإرهابية دون قتال**"، ما يعرف بالشلل الإستراتيجي للخصوم.[3]

---

[1]– بلهول نسيم، مفهوم المذهب العسكري الجزائري لثنائية بيئة الضبط العملياتي والدين في مكافحة الإرهاب، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، العدد الأول 2015، ص16.

[2]– المرجع نفسه، ص16.

[3]– المرجع نفسه، ص17.

وبالنظر إلى تزايد حجم التهديدات الإرهابية الخطيرة على الجزائر، تم في نهاية 2014 استحداث لجنة أمنية مشتركة متخصصة في مجال مكافحة الإرهاب من طرفي وزارتي الداخلية والدفاع، بالإضافة إلى تعقب المنتديات الجهادية في مسعى جديد يأتي في ظل تنامي المخاطر الأمنية، وعلى خلفية تزايد نشاط شبكات التجنيد التي تم تفكيكها من طرف وحدات الدرك الوطني ومصالح الأمن والجيش في العديد من ولايات الجمهورية، وبعدما كشفت أيضا الكثير من التحريات الأمنية الدقيقة عن وجود صفحات بمواقع التواصل الاجتماعي تروج للأفكار الجهادية المتطرفة، وتعمل أيضا في الجهة المقابلة على استقطاب مقاتلين مفترضين عبر الانترنت في سبيل الالتحاق بصفوف الجماعات الإرهابية في كل من العراق وسوريا وليبيا.[1]

ثانيا: إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها

لقد عرفت الجزائر أزيد من 100 جريمة إلكترونية سنة 2014 وتضاعف هذا العدد خلال السداسي الأول لسنة 2015، حيث سجلت المصالح الأمنية أزيد من 200 جريمة إلكترونية متنوعة، وفي هذا الإطار عملت الدولة الجزائرية على تأسيس الهيئة الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها في 9 أكتوبر 2015، بعدما وقع رئيس الجمهورية على مرسوم رئاسي يقضي بإنشاء هذه الجديدة والتي تعد بمثابة سلطة إدارية مستقلة لدى وزير العدل، كما تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسئولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقاء.[2]

كما تضم الهيئة قضاة وضباطا تابعين لمصالح الاستعلامات العسكرية والدرك والأمن الوطنيين، وأعوانا من الشرطة القضائية وفقا لأحكام قانون الإجراءات الجزائية،

[1]– بلهول نسيم، المرجع السابق، ص17.

[2]– علي بوعمرة، المرجع السابق، ص55.

وتكلف هذه الآلية الجديدة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الحديثة، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام.[1]

وهنا على سبيل المثال كمحاربة كل المضامين الإرهابية المتطرفة التي تدعو إلى الغلو الديني أو تسعى إلى تجنيد الشباب الجزائري في صفوفها، كما تعمل هذه الهيئة على جمع المعلومات والتزويد بها من خلال الخبرات القضائية وضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي واستثناء هيئات وطنية أخرى.[2]

الفرع الثالث: النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني و النتائج المحققة في هذا الإطار

قد خصصنا هذا الفرع للكشف عن النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني، والنتائج المتوصل لها.

أولا: النصوص القانونية الخاصة بمكافحة الإرهاب الإلكتروني

تندرج مكافحة الإرهاب الإلكتروني في الجزائر ضمن مكافحة الجريمة السيبرانية بكافة أشكالها، مع أنه يوجد غموض وعدم دقة في النصوص القانونية الوطنية في تعريف هذا النمط من الجرائم المستحدثة، لقد تنبه المشرع الجزائري إلى ضرورة جعل المنظومة القانونية مواكبة للتطور الحاصل في تكنولوجيا المعلومات والاتصال في هذا الصدد، صدر القانون رقم 15/04 المتعلق بالمعالجة الآلية للمعطيات (نوفمبر2004)، ثم

[1]- علي بوعمرة، المرجع السابق، ص56.

[2]- المرجع نفسه، ص56.

القانون رقم 09_04 لسنة 2009، والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[1]

ومن التدابير المتخذة من قبل الحكومة الجزائرية ما يتعلق بالوقاية الإلكترونية التي تشمل كما حددها القانون 09_04 الوقاية من جرائم الإرهاب والماس بأمن الدولة، الوقاية من التعدي على أنظمة معلومات يكون هدفه المساس بالدفاع الوطني، ما تقتضيه التحريات والتحقيقات القضائية والمساعدات القضائية الدولية، كما نص القانون على قواعد تفتيش منظومات المعلومات وحجز المعطيات في إطار التحريات.[2]

كما نص قانون العقوبات على عقوبات بالسجن والغرامة المالية، تختلف باختلاف الجريمة المرتكبة، مثال ذلك المادة 394 مكرر، مع مضاعفة العقوبة بالنسبة للجرائم التي تمس أمن الدولة والدفاع الوطني بنص المادة 394 مكرر3 . [3]

واهتمت وزارة الدفاع الوطني بحفظ الأمن السيبراني، عبر وضع سياسات وبرامج واستحداث آليات لمكافحة الجريمة السيبرانية وحماية البيئة التحتية للمعلومات ، تعبئة عدد من الأجهزة المتخصصة لحماية أمن الفضاء السيبراني والوقاية من الجريمة مثل: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ، هيئات ذات اختصاص إقليمي تعني بالجرائم الإلكترونية الواقعة خارج الحدود الوطنية والتي تمس الأمن الوطني، المعهد الوطني للأدلة الجنائية، وعلم الإجرام،المديرية العامة للأمن الوطني. [4]

وقد صدر القانون رقم 20_05 (آفريل 2020) المتعلق بالوقاية من التميز ومكافحتهما، ليشكل تكملة لجملة القوانين والنصوص المتعلقة بمكافحة الإجرام ولإجرام

---

[1]– عبد القادر جعيجع وزهرة تيغزة، تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني واستراتيجيات المواجهة، مجلة دفاتر السياسة والقانون، المجلد 13 العدد الأول، الجزائر، 2021، ص552.

[2]– المرجع نفسه ، ص552.

[3]– المرجع نفسه ، ص552.

[4]– المرجع نفسه ، ص552.

الإلكتروني، ويهدف إلى أخلقة الحياة العامة مع توصية بإنشاء مرصد وطني للوقاية من التمييز وخطاب الكراهية، ينص القانون على تدابير وعقوبات متنوعة تمس كذلك من يستخدم تكنولوجيا الإعلام والاتصال (وهنا إشارة إلى شبكات التواصل الاجتماعي) بغرض الدعاية والكراهية ونشر العنف، مع التنديد في جريمة استخدام هذه التكنولوجيا لنشر العنف في المجتمع. [1]

وكتقييم لبعض الجهود الدولية في مجال مكافحة الإرهاب الإلكتروني يمكن القول إن استمرار التطور التكنولوجي والاستخدام المتزايد لشبكة الانترنت من بين أهم التحديات التي تقف في وجه سياسات واستراتيجيات الدول، إلى جانب عدم وجود تعريف جامع للإرهاب الإلكتروني، والثغرات القانونية بالنسبة لهذا النوع من الجرائم، مِثل غياب العنصر المادي أحيانا وصعوبة كشف الجريمة في حينها، يضاف إلى ذلك غياب سياسة تشريعية موحدة في مجال الإرهاب الإلكتروني كما هو الحال لدى الدول العربية. [2]

ثانيا: النتائج المحققة في إطار مكافحة الإرهاب الإلكتروني في الجزائر

تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني، وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال من معالجة أكثر من 1000 جريمة إلكترونية، منها 30 بالمائة على مواقع التواصل الاجتماعي. [3]

هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016، وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بتهديدات إرهابية بإسم تنظيم داعش الإرهابي، لتسفر جهود البحث والتحري

[1]– ، عبد القادر جعيجع وزهرة تيغزة، المرجع السابق، ص552–553.

[2]– المرجع نفسه ، ص553.

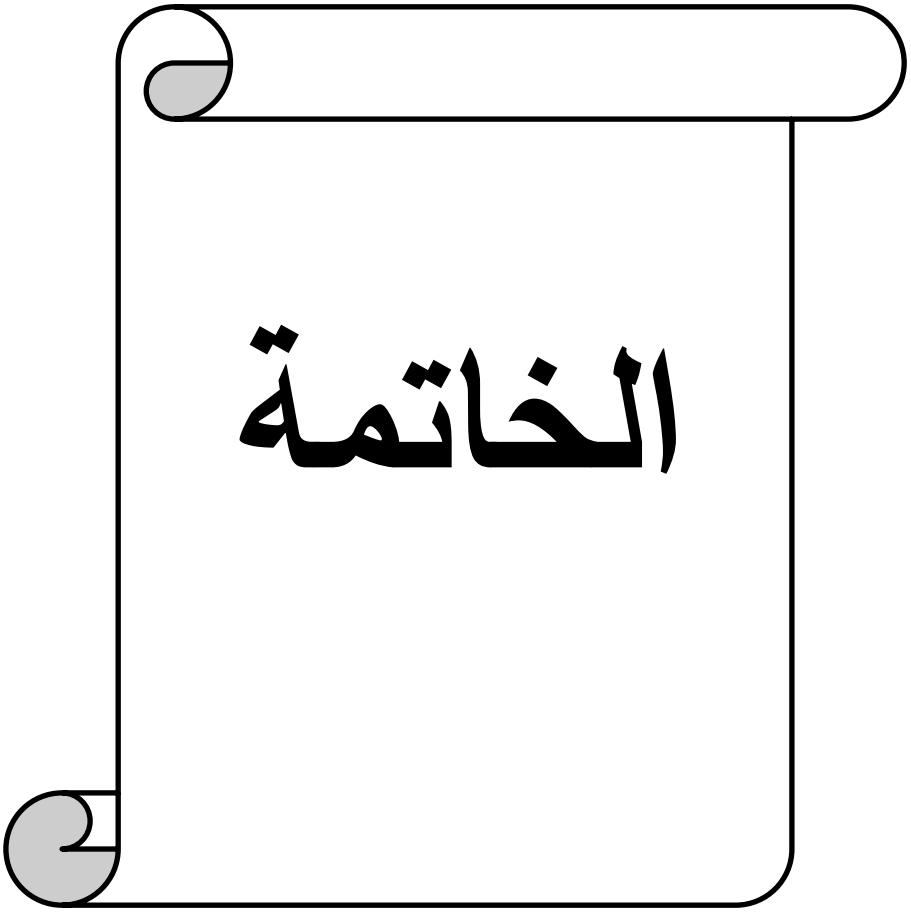
[3]– بن صويلح أمال، المرجع السابق، ص9.

والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء. [1]

هذا وقد استطاع الجيش الإلكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليبيا، كما تمكن من فك شفرات الرسائل المتبادلة، وما يزيد عن 30 خلية تسعى لاستقطاب الشباب لتجنيده عبر مواقع الانترنت ومنصات التواصل الاجتماعي خاصة الفيس بوك والتويتر لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة، وتلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية إلى جانب اتصالات محلية ودولية. [2]

[1]– بن صويلح أمال، المرجع السابق، ، ص9.

[2]– المرجع نفسه، ص9.


الخاتمة

الخاتمة:

إن الإرهاب الإلكتروني جريمة معلوماتية كانت نتيجة للتطور الحاصل في المجال العلمي و هو امتداد لجريمة الإرهاب التقليدي، حيث أن مجرمي الإرهاب سلكوا طريقا جديدا لتنفيذ هجماتهم وغاياتهم الإرهابية إذ أنهم اتخذوا الانترنت والحاسب الآلي وسيلة لذلك، وبالرغم من أن الإرهاب الإلكتروني جريمة جديدة إلا أنه انتشر بشكل كبير وفي مدة قصيرة وأصبح يشكل خطرا جسيما، وذلك نظرا لما ينجم عنه من أضرار سواء على الأفراد أو الدول، وهذا استدعى بالضرورة تكاتف وتضامن الدول من أجل سن تشريعات سواء على المستوى الدولي أو الوطني من أجل الحد أو القضاء على هذه الجريمة ومما سبق لنا دراسته نستنتج أن:

- لم يتمكن الفقهاء من وضع تعريف جامع ومانع للإرهاب الإلكتروني، إلا أنهم استطاعوا معرفة حجم الخطر الذي يشكله هذا الأخير، وتوصلوا إلى هدفه الأساسي ألا وهو نشر الرعب والخوف.
- الإرهاب الإلكتروني له مجموعة من الدوافع والأسباب المؤدية له.
- الخطر الذي تشكله هذه الجريمة كبير جدا، فهو يستهدف الفئة الشبابية ويستدرجهم لتنفيذ العمليات الإرهابية من خلال وسائل الاتصال وتقنية المعلومات مما يزيد من حدة خطورته سواء على الأفراد أو الدول.
- الإرهاب الإلكتروني هو وجه آخر يكشف السلبيات الناتجة عن التقدم العلمي على مستوى العالم.
- هو جريمة فائقة الخطورة تستهدف العالم بأسره وكان لابد من اتخاذ مختلف الإجراءات والتدابير من طرف المنظمات والاتفاقيات الدولية أو الإقليمية من أجل سن تشريعات لمكافحة هذا النوع من الجرائم، وكذلك هو الحال بالنسبة للدول التي لجأت إلى وضع مجموعة من القوانين لمواجهة الإرهاب الإلكتروني، وهو بالضبط

ما قامت به السلطات الجزائرية التي طالما كثفت جهودها من أجل القضاء على الإرهاب الإلكتروني وسن من خلاله مجموعة القوانين الرادعة له.

ومن أهم التوصيات التي توصلنا إليها:

- لابد من إيجاد تعريف جامع ومانع لجريمة الإرهاب الإلكتروني.
- من المهم نشر الوعي بين الناس بخطورة هذه الجريمة وتحذيرهم من الأضرار الناتجة عنها.
- البحث عن كل الأسباب المؤدية للإرهاب الإلكتروني والوقوف بالند لها
- ضرورة تكثيف الجهود بين الدول والمنظمات للحد من انتشار هذه الجريمة الإلكترونية.
- حث الفئات المستهدفة على أخلاقيات استخدام الانترنت لتجنب الوقوع في هذه الجريمة،مع ضرورة إدخال المنهج الأخلاقي في المنظومات التربوية لتوعية بالمخاطر التي تولدها الانترنت.
- لابد من تعاون السلطات القضائية في مختلف الدول لتبادل الخبرات فيما بينهم لمكافحة الإرهاب الإلكتروني.
- أما على المستوى الوطني فمن الضروري إطلاق خلايا أمنية متخصصة من أجل حماية المواطن الجزائري خاصة عنصر الشباب من مخاطر الإرهاب الإلكتروني مع ضرورة مواكبة التطور التكنولوجي لمسايرة أساليب ارتكاب هذه الجريمة والحد منها.
- يجب سن قوانين خاصة بالإرهاب الإلكتروني دون ربطه بالإرهاب العادي.

قائمة المصادر

والمراجع

المصادر والمراجع

أولا: المصادر.

-القرآن الكريم .

- القوانين والمراسم .

1. القانون رقم 04/09 المؤرخ في 5 غشت سنة 2009، يحتوي على القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال، الجريدة الرسمية، العدد 47.
2. المرسوم الرئاسي رقم 55/02 مؤرخ في 5 فبراير 2002 تتضمن التصديق يتحفظ على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، الجريدة الرسمية، العدد 9، الصادر في 2002/02/10 .

ثانيا: المراجع.

أولا: الكتب .

1. حسنين شفيق،-الإعلام الجديد والجرائم الإلكترونية التسريبات. التجسس الإلكتروني، الإرهاب الإلكتروني-، دار الفكر والفن للطباعة والنشر والتوزيع، مصر، 2014.
2. رفد عيادة الهاشمي، الإرهاب الإلكتروني، ط1، دار أمجد للنشر والتوزيع، الأردن، 2019
3. عادل عبد الصادق، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، ط2، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2003.
4. عبد الرحمن بن عبد الله السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، ط1، جامعة الإمام بن سعود الإسلامية، 2004.
5. عبد القادر زهير النقوزي، مفهوم القانوني لجرائم الإرهاب الداخلي والدولي، منشورات حلبي الحقوقية، الطبعة الأولى، بيروت، 2008.

6. علاء صراط الغامدي، الحرب النفسية للإرهاب الجديد، دار المنشأة المعارف، الإسكندرية، مصر، 2006.
7. علي عدنان الفيل، الإجرام الإلكتروني، دراسة مقارنة، ط1، مكتبة زين الحقوقية والأدبية، لبنان، 2011 .
8. مصطفى يوسف كافي، الإدارة الإلكترونية، دار ومؤسسة رسلان للطباعة والنشر، سوريا، دمشق، 2011 .
9. مصطفى يوسف كافي، جرائم (الفساد–غسيل الأموال–السياحة–الإرهاب الإلكتروني–المعلوماتية)، الطبعة الأولى، مكتبة المجمع العربي للنشر والتوزيع، عَمان–الأردن، 2014.
10. هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، دار الكتب العلمية للنشر، لبنان، 2005.
11. يونس عرب، جرائم الكومبيوتر والانترنت، ط1، اتحاد المصارف العربية، بيروت، 2002 .
12. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة، كلية الحقوق والعلوم السياسية، جامعة 8 ماي 1945، قالمة، الجزائر،2019.

ثالثا: الرسائل والمذكرات

1. إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني، دراسة مقارنة، رسالة مقدمة لنيل درجة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، العراق، 2012 .
2. بن صفية وداد، تأثير المتغير التكنولوجي على الفواعل الدولية الجديدة الإرهاب الإلكتروني نموذجا، مذكرة لنيل شهادة الماستر الأكاديمي، تخصص إستراتيجية وعلاقات دولية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2018/2017.

3. توفيق شريخي، الإرهاب الإلكتروني وتأثيره على أمن الدولة، مذكرة لنيل شهادة الماستر أكاديمي، تخصص إستراتيجية وعلاقات دولية، جامعة محمد بوضياف، مسيلة، الجزائر، 2018/2017 .

4. خلود عبد الرحيم العالول، الإرهاب الإلكتروني، بحث علمي قانوني لنيل لقب أستاذة في المحاماة نقابة المحامين، فرع دمشق، الجمهورية السورية.

5. سارة جلاب، سياسة مكافحة الإرهاب (دراسة مقارنة بين الجزائر والولايات المتحدة الأمريكية)، مذكرة تكميلية لنيل شهادة الماستر، تخصص سياسات عامة مقارنة، كلية الحقوق والعلوم السياسة، جامعة العربي بن المهيدي، في 2015/2014 .

6. شاشوة ياسمينة، الإرهاب الإلكتروني بين مخاطره وآليات مكافحته، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية ح.ع.س، جامعة أكلي محند أولحاج، البويرة، 2020/2019 .

7. علي بوعمرة، جريمة الإرهاب الإلكتروني، مذكرة مقدمة ضمن متطلبات لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة 2021/2020 .

8. عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2019 .

9. غلاف كريمة، جرلال زوهرة، جريمة الإرهاب الإلكتروني، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة عبد الرحمن ميزة، بجاية، 2019./2018 .

10. نجاة رامز أبو شقرا، جرائم الإرهاب الإلكتروني في ظل محدودية النص، رسالة مقدمة لنيل درجة الماجستير، القانون الجزائي، كلية الحقوق والعلوم السياسية، جامعة بيروت العربية، 2020 .

11. هاجر عون، الإرهاب الإلكتروني، مذكرة تكميلية لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، جامعة العربي بن المهيدي، أم البواقي، 2015-2016 .
12. هروال هيبة نبيلة، جرائم الانترنت، أطروحة دكتوراه، كلية.ح.ع.س، جامعة أبي بكر، بالقايد، تلمسان، 2014/2013.
13. مصطفى سعد حمد مخلف، جريمة الإرهاب عبر الوسائل الإلكترونية "دراسة مقارنة بين التشريعين الأردني والعراقي"، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2017.

ثالثا: المجلات والمقالات

1. بلهول نسيم، مفهوم المذهب العسكري الجزائري لثنائية بيئة الضبط العملياتي والدين في مكافحة الإرهاب، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، العدد الأول، 2015 .
2. بن مرزوق عنترة، الكر محمد، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والاجتماعية، العدد 38، جوان 2018 .
3. عبد القادر جعيجع وزهرة تيغزة، تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني واستراتيجيات المواجهة، مجلة دفاتر السياسة والقانون، المجلد13 العدد الأول، الجزائر، 2021 .
4. نجيب بن عمر عوينات، الإرهاب الإلكتروني: مفهوم الجهود الدولية والإقليمية لمكافحته، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، معهد العالي للإعلامية، الكاف جامعة جندوبة، تونس، العدد السادس، تاريخ الصدور :2017/04/20 .
5. سليماني مباركة، الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، العدد08ج01، جوان2017.

رابعا: المداخلات و الملتقيات

1. أبو عمار، ميلود عبد الرحمان بنعتيك، الإرهاب المعلوماتي، مداخلة المؤتمر الدولي لمكافحة جرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية 2015، السعودية، الرياض، متوفر على الموقع: http://search.mandumah.com/Record/690587، تاريخ التصفح: 16 ماي 2022 على الساعة 15:51.
2. بن صويلح أمال، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام، الملتقى الدولي حول الإجرام السيبراني، المفاهيم والتحديات خطوة هامة نحو مكافحة الإرهاب الإلكتروني للجزائر، جامعة قالمة، يومي 11-12 أفريل 2017 .
3. سارة بوحادة، مداخلة حول أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية للعلوم السياسية، الجزائر .
4. العجلان، عبد الله بن عبد العزيز بن فهد، الإرهاب المعلوماتي، مداخلة في المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية-ICACC- كلية علوم الحاسب والمعلومات- نوفمبر 2015، المملكة العربية السعودية، الرياض، متوفر على الموقع: http://search.mandumah.com/Record/690587، تاريخ التصفح: 14 ماي 2022، الساعة: 13:30.
5. نايف أحمد ضاحي الشمري، عمر عباس خضير العبيدي، جرائم الأمن السيبراني واليات مكافحتها في إطار القانون الدولي، مداخلة ضمن ملتقى دولي، 5th International Legal Issues Conference - ILIC2020 - ISBN(978-9922-90-5-1) .

خامسا: المواقع الإلكترونية

1. مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الانترنت لأغراض ارهابية، تقرير منشور على الموقع: https://www.unodc.org/، تاريخ التصفح: 2022/05/03، الساعة 18:55.

الفهرس

فهرس المحتويات

العنوان	الرقم
مقدمة	3-1
الفصل الأول: ماهية الإرهاب الالكتروني	
المبحث الأول: الإطار المفاهيمي الإرهاب الالكتروني	06
المطلب الأول: مفهوم الإرهاب الالكتروني	06
الفرع الأول: تعريف الإرهاب الالكتروني	06
الفرع الثاني:خصائص الإرهاب الالكتروني	10
الفرع الثالث: أهداف الإرهاب الالكتروني	10
الفرع الرابع: تمييز الإرهاب الالكتروني عن المفاهيم المشابهة	11
المطلب الثاني: أسباب الإرهاب الالكتروني ومخاطره	15
الفرع الأول: أسباب الإرهاب الالكتروني	15
الفرع الثاني: مخاطر الإرهاب الإلكتروني	20
المبحث الثاني: أركان الإرهاب الالكتروني	24
المطلب الأول: الركن الشرعي لجريمة الإرهاب الالكتروني	24
الفرع الأول: تجريم الإرهاب الالكتروني في التشريع الجزائري	24
الفرع الثاني: تجريم الإرهاب الالكتروني في بعض تشريعات الدول العربية	25
المطلب الثاني: الركن المادي لجريمة الإرهاب الالكتروني	26
الفرع الأول: إنشاء مواقع إرهابية الكتروني	26
الفرع الثاني: تدمير المواقع الالكترونية	27
الفرع الثالث: التهديد و التجسس الالكتروني	28
المطلب الثالث: الركن المعنوي لجريمة الإرهاب الالكتروني	31
الفرع الأول: القصد الجنائي العام	31
الفرع الثاني: القصد الجنائي الخاص	32
الفصل الثاني: جهود مكافحة الإرهاب الالكتروني	

المبحث الأول: مكافحة الإرهاب الالكتروني على المستوى الدولي	35
المطلب الأول: مكافحة الإرهاب الالكتروني في الاتفاقيات الدولية والاقليمية	35
الفرع الأول: مكافحة الإرهاب الإلكتروني في الاتفاقيات الدولية	35
الفرع الثاني: مكافحة الإرهاب الالكتروني على المستوى الاقليمي	38
المطلب الثاني: مكافحة الإرهاب الالكتروني في المنظمات الدولية	40
الفرع الأول: جهود كل من منظمة الأمم المتحدة ومجموعة الدول الثمانية	40
الفرع الثاني: جهود المنظمات العالمية المتخصصة	43
المبحث الثاني: الجهود الوطنية في مكافحة الإرهاب الالكتروني	45
المطلب الأول: جهود بعض الدول الغربية لمكافحة الإرهاب الالكتروني	45
المطلب الثاني: مكافحة الإرهاب الالكتروني في بعض الدول العربية	49
المطلب الثالث: مكافحة الإرهاب الالكتروني في التشريع الجزائري	54
الفرع الأول: واقع الإرهاب الالكتروني في الجزائر	54
الفرع الثاني: إجراءات الوقاية لمكافحة الإرهاب الالكتروني	55
الفرع الثالث: النصوص القانونية الخاصة بمكافحة الإرهاب الالكتروني والنتائج المحققة في هذا الإطار	58
الخاتمة	63
قائمة المصادر والمراجع	66
فهرس	73

الملخص:

لقد أصبح الإرهاب الالكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الانترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، و تتفاقم هذه المخاطر بمرور كل يوم لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الالكترونية، ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الالكتروني والحد من أثاره الجسيمة على الأفراد والمنظمات، الأمن القومي و السيادة الوطنية للدول و زعزعة استقرار المجتمعات و تماسكها.

Summary :

Electronic terrorism has become an obsession that scares the world ،which has become vulnerable to attacks by terrorists on the Internet who are engaged in sabotage activities from anywhere in the world ،These dangers are exacerbated every day because modern technology alone can not protect people from electronic terrorist operations ،States to take measures and precautions to confront electronic terrorism and reduce its effects on individuals and organization ،national security and national sovereignty of States and the destabilization of societies and cohesion.