جامعة أكلي محند أولحاج – البويرة

كلية الحقوق والعلوم السياسية

قسم القانون العام

الإرهاب الإلكتروني بين مخاطره وآليات مكافحته

مذكرة تخرج ضمن متطلبات نيل شهادة المـاستر في الحقوق

تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبة:
- شاشوة ياسمينة

إشراف الأستاذ:
- د/ لونيسي علي

لجنة المناقشة

الأستاذ: .....رئيسا

الأستاذ: د/. لونيسي علي.....مشرفا ومقررا

الأستاذ:.....ممتحنا

السنة الجامعية: 2020/2019.

إهـــــداء

"تهادوا تحابوا"؛ حديث نبوي شريف.

اهدي ثمرة جهدي إلى من تنحني هامتي له خجلا أبي

إلى من علمتني وهنا على وهن أمي

إلى من أشد بهم ظهري إخواني وأخواتي ..نجيب وسام كنزة سليمان

إلى كل أهلي و أقاربي صغيرهم و كبيرهم

إلى صديقات عمري تنهينان سهام آسيا سارة فريدة

إلى كل الأصدقاء وزملاء

وإلى كل من ساندوني ووقفوا معي لأتمم هذا العمل المتواضع

شكر وتقدير

"لا يشكر الله من لم يشكر الناس"؛ حديث نبوي شريف.

الشكر أولا؛ الله سبحانه وتعالى عرفانا واعترافا. عرفانا؛ فلا عطاء إلا بإذنه ولا مجد إلا بتقديره. واعترافا؛ فالكمال لله والتواضع صفة النبلاء

وأتقدم بجزيل الشكر والتقدير إلى أساتذتي الأفاضل، إلى كل من علمني حرفا، إلى كل من أرشدني إلى العلم.

كما أتقدم بالشكر الجزيل إلى الأستاذ المشرف "لونيسي علي" خاصة؛ على تفضله للإشراف على هذا العمل وعلى نصائحه وإرشاداته القيمة، ولجنة المناقشة عامة؛ عن قبولهم لمناقشة وتقييم هذا العمل الأكاديمي والتي سوف لن تبخل علينا بتوصياتها وتصويباتها القيمة.

واشكر كل من ساهم من بعيد أو من قريب في إنجاز العمل محل الطرح؛ سواء بالعمل أو الدعاء.

قائمة أهم المختصرات:

أولا: باللغة العربية

ص : صفحة

ص ص :من الصفحة إلى الصفحة

ط :طبعة

د ن ط: دون طبعة

ج ج د ش :الجمهورية الجزائرية الديمقراطية الشعبية.

ثانيا: باللغة الفرنسية

P : page

مقدمة

ظهرت الجريمة بظهور الجنس البشري وأخذت تتطور تبعا له، فأصبحت سلوكا ملازما للطبيعة البشرية الأمر الذي جعلها تأخذ أبعادا وأشكال مختلفة، ومن بين هذه الجرائم الجريمة الإرهابية[1]، التي عانت منها المجتمعات البشرية عبر التاريخ وزادت حدة هذه المعاناة في العصر الحديث، نتيجة تطور علمي وتكنولوجي الذي شهده العالم والذي أدى إلى ظهور ثورة معلوماتية هائلة شملت معظم جوانب الحياة.

بما في ذلك العالم الإجرام الذي عرف تطورا كبيرا ببروز مجموعة من الجرائم المستحدثة التي تعتمد على أساليب متطورة، ومن أبرز هذه الجرائم ما اصطلح عليه بالإرهاب الالكتروني أو المعلوماتي الرقمي

حيث يعتبر الإرهاب الالكتروني من أبشع وأخطر الجرائم التي ترتكب عبر الانترنت وتهدد العالم بعصره الآلي، حيث يستغل الساحة المعلوماتية أو الفضاء الالكتروني من خلال إنشاء حسابات خاصة بإرهاب في مواقع الانترنت لنشر التطرف والفكر الإرهابي في العالم والتواصل بين أعضائها حول كيفية اختراق وتدمير المواقع ونشر الفيروسات والتجسس على الدول لكشف أسرارها وابتزازها لتحقيق أغراض إرهابية والحصول على تمويل نشاطها الإرهابي وتدمير البنية التحتية لدول[2].

ويعتبر هذا الإرهاب المعاصر النسخة الالكترونية عن الإرهاب التقليدي، فمن حيث التنظيم فهو عابر للحدود الإقليمية، متعدد الجنسيات لا تجمعه قضية وطنية أو قومية بل إيديولوجية سياسية أو دينية، ويهدف إلى تحقيق أكبر الخسائر المادية والبشرية في ظرف وجيز جدا وبسرعة البرق، مستعملا في ذلك أسلحة رقمية جد متطورة[3]،

---

[1]–إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1، مركز الديمقراطي العربي لدراسات إستراتيجية والسياسية والاقتصادية، برلين، ألمانيا،2018، ص01

[2]–أمير فرج، الجرائم المعلوماتية على شبكة المعلومات، دار المطبوعات الجامعية، الإسكندرية، 2008، ص128

[3]–إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1، مركز الديمقراطي العربي لدراسات إستراتيجية والسياسية والاقتصادية، برلين، ألمانيا،2018، ص01

وتعتبر التقنية الحديثة السلاح الأشد فتكا الذي يستخدمه الإرهابي المعلوماتي في تنفيذ هجماته واعتداءاته على الأمن والسلم الدوليين، والفضاء الالكتروني مجالا خصبا ولتواصل فيما بينهم والاستعداد لأعمالهم المدمرة [1]

وبناء على كل ما يشكله الإرهاب إلكتروني من مخاطر وتهديدات على العالم اجمع سعيت معظم الدول سواء الغربية أو الأجنبية إلى مكافحة هذا الإجرام الخطير الذي صاحب سوء استعمال التقنيات الحديثة.

وتكمن أهمية دراسة هذا الموضوع في إلقاء الضوء على الإرهاب الرقمي المعاصر من خلال تحديد مفهومه وخصائصه وحجم مخاطر التي يخلفها وانعكاساته على المجتمعات، وتمييزه عن الجرائم المتصلة به وتبيان آليات المكافحة والوقاية منه سواء فنيا /تقنيا/قانونيا على الصعيد الدولي أو الإقليمي، حيث يعتبر من أخطر أشكال الإرهاب وأكثرها استحداث أو انتشارا في ظل التطور التكنولوجي وتنامي استخدام شبكة الانترنت.

وتهدف دراسة هذا الموضوع إلى إلقاء الضوء على ظاهرة وبيئة الإرهاب الالكتروني وعرض أهم مخاطر وأثار ناجمة عن الإرهاب الالكتروني بهدف توعية وتنبيه الأفراد ومجتمعات منه، والاطلاع على مستجدات والمتغيرات الالكترونية وذلك بمعرفة طرق واليات الوقاية منه، إضافة دراسة بسيطة لرصيد المعرفي المتعلق بهذا الموضوع.

وأثارنا دراسة موضوع الإرهاب الالكتروني للعدة أسباب منها الشخصية والموضوعية فتنطوي أهم الأسباب الشخصية كوني طالبة في الحقوق والعلوم السياسية ويندرج موضوع الدراسة في مجال تخصصي القانون الجنائي والعلوم الجنائية، واهتمامي الشخصي بموضوع الإرهاب الالكتروني وما يرتبط به من استراتيجيات واليات مكافحته وميولي الجامحة ورغبتي الملحة في الغوص أكثر ومعرفة تفاصيله وحيثياته.

[1]–غلاف كريمة، جرلال زوهرة، جريمة الإرهاب الالكتروني، مذكرة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، تخصص قانون جنائي وعلوم جنائية، جامعة عبد الرحمان ميرة، بجاية، 2019/2018، ص03

وتتمثل الأسباب الموضوعية في كونه من المواضيع الحديثة التي تستحق بذل الجهد للبحث فيه كونه ظاهرة متعددة الأبعاد عميق عمق المخاطر التي يسببها وعمق الشبكة التي يعتمد عليها وتمثل الأساس في منطلقاته فهو كأخطبوط بأذرع عديدة يمس كل القطاعات الحيوية والحساسة والبنية التحتية ويستعمل الفضاء الالكتروني كساحة لصراع والحرب والتهديد والأمر الذي حفزنا على البحث فيه كونه من المواضيع التي شغلت اهتمام الرأي العام العالمي والإقليمي ومعرفة جهود الدولية والإقليمية في هذا المجال.

ومن خلال ما سبق يتبادر إلى أذهاننا طرح الإشكالية التالية: فيما تكمن مخاطر الإرهاب الالكتروني وما هي آليات مكافحته؟

وللإجابة على هذه الإشكالية تم الاعتماد على المنهج الوصفي التحليلي لوصف جريمة الإرهاب الالكتروني من خلال تحديد بعض المفاهيم واهم السمات التي تتميز بها جريمة محل الموضوع، والمنهج التحليلي الذي يوافق طريقتنا في الإجابة على تساؤلاتنا

وعليه ارتأينا تقسيم هذا البحث إلى فصلين، الفصل الأول تناولنا فيه الإطار العام للإرهاب الالكتروني، حيث تطرقنا في (المبحث الأول) لماهية الإرهاب الالكتروني، ومخاطر الإرهاب الالكتروني وأثاره في (المبحث الثاني)، كما تناولنا في الفصل الثاني مكافحة الإرهاب الالكتروني حيث خصصنا (المبحث الأول) لمكافحة الإرهاب الالكتروني على الصعيد الدولي والإقليمي و (المبحث الثاني) آليات مواجهة الإرهاب الالكتروني.

الفصل الأول:

الإطار العام للإرهاب الإلكتروني

لقد شهدت البشرية عبر القرون الماضية تطورات عديدة مست كل المجلات بما في ذلك عالم الإجرام عامة وجريمة الإرهاب خاصة ،حيث ظهر الجيل الأول من الإرهاب ذو الطابع القومي في أواخر القرن التاسع عشر بحيث اجتاح القارة الأوربية في صورته التقليدية و في فترة الحرب الباردة ظهر الجيل الثاني منه ذو الطابع الإيديولوجي بإفرازه صراعات بين المعسكرين الغربي و الشرقي ، و في ظل التطورات الصارخة لتكنولوجيا و انفجار المعلوماتي ظهر جيل ثالث من الإرهاب تحت اسم الإرهاب الالكتروني كتهديد أمني جديد للدولة و المجتمعات العابرة للحدود، إذ تستخدم التقنيات الحديثة لشن هجومات إرهابية بهدف نشر الخوف و الرعب[1].

وللإحاطة بمعالم هذه الظاهرة قسمنا هذا الفصل إلى مبحثين تناولنا في (المبحث الأول) ماهية الإرهاب الالكتروني وفي (المبحث الثاني) مخاطر الإرهاب الالكتروني وأثاره.

[1]– إيمان بن سالم، المرجع السابق ، ص01

المبحث الأول: ماهية الإرهاب الالكتروني

يعد الإرهاب الالكتروني من الجرائم التي استغلت الجانب السلبي لتطور الهائل في وسائل الاتصال وثورة الانترنت وتكنولوجيا التي حولت العالم إلي قرية صغيرة خالية من الحدود الجغرافية وسياسية.

وجعلت المعلومات في متناول الجميع (الكبير، القاصر، الجاهل، المثقف، المجرم...) من بينهم الإرهابيين الذين يستخدمونهم في تنفيذ أنشطتهم الإرهابية وأعمالهم التخريبية. وبذلك ساهمت عوامل التحضر السريع وسهولة استخدام هذا السلاح أي ما يعرف بالإرهاب الالكتروني إلي انتشاره الهائل وارتفاع نسبة ضحاياه وشدة أثره و ضرره.

فالإرهاب الالكتروني يتميز عن غيره من أنواع الإرهاب في استخدام الموارد المعلوماتية والوسائل الالكترونية وكذا في طبيعته ونطاقه ووسائله وحتى في خصوصية مرتكبيه.

ومن خلال هذا المبحث سنقوم بدراسة مفهوم الإرهاب الالكتروني ودوافعه في (المطلب الأول) ومظاهر الإرهاب الالكتروني ووسائله في (المطلب الثاني).

المطلب الأول: مفهوم الإرهاب الالكتروني ودوافعه

يعتبر الإرهاب من بين الظواهر التي تأثرت بتطور الحاصل في مجال التقنيات والتكنولوجيات الحديثة. حيث أن التزاوج بين الإرهاب وتكنولوجيا أسفر عن نوع جديد من أخطر أنواع الإرهاب على الأمن وسلامة المجتمعات، وهو من بين الجرائم المستحدثة إلا وهو الإرهاب الإلكتروني أو الرقمي بحيث تعددت تسمياته.

ونحاول من خلال هذا المطلب تقديم تعريف الإرهاب الالكتروني في (الفرع الأول) ثم سنتطرق في (الفرع الثاني) إلي صور الإرهاب الالكتروني وفي (الفرع الثالث) دوافع وأسباب هذا الإرهاب.

الفرع الأول: تعريف بالإرهاب الالكتروني

لقد تعال مؤشر الجرائم على مستوى الدولي في القرن الأخير نتيجة ظهور الثورة المعلوماتية، وإفرازها لعديد من الجرائم المستحدثة التي لم يسبق وان عرفها العالم، إذ تعتمد على أساليب متطورة مما أدى إلي تزايد أخطارها وعلى رأسها الإرهاب الالكتروني.قبل التعرض إلى تعريف هذا الأخير باعتباره جريمة عصرية توجب علينا أولا التطرق إلي تعريف الجريمة التقليدية للإرهاب، باعتبار الإرهاب الالكتروني امتداد لها.

أولا: المقصود بالإرهاب التقليدي

أن من أهم القضايا الجدلية على المستوى الدولي، هو عدم الوصول إلي تعريف جامع ومانع متفق عليه للإرهاب بشكل عام ولعل السبب في ذلك يعود الى تشعب فكرة الإرهاب وتنوع أشكاله ومظاهره وتعدد أسبابه ودوافعه وأنماطه، واختلاف وجهات النظر الدولية والسياسية حوله فما يراه البعض عملا إرهابيا يراه البعض الأخر عملا مشروعا، وعليه كثرت الدراسات حول الإرهاب وانعقدت العديد من المؤتمرات في شانه وتم التوقيع على العديد من الاتفاقيات الدولية والإقليمية لمكافحته وتعددت المحاولات لتعريفه[1].

أ) تعريف الإرهاب لغة (terrorism)

نجد أن معاجم اللغة الحديثة تقول أن الإرهاب كلمة مشتقة من فعل المزيد ارهب أم مرهب فهما يؤديان نفس المعنى وهو الخوف وفزع ،فيقال ارهب فلان فلانا بمعنى اخافه أو أفزعه أما الفعل المجرد رهب، يرهب ،رهبة ،ورهبا فيعني خاف أما فعل المزيد بتاء هو ترهب فيعني انقطع للعبادة في صومعته و يشتق منه الراهب و الراهبة و الرهبانية و كذلك يستعمل الفعل لتوعد ، يقال ترهب فلان فلانا أي توعده ، و أن كلمة رهبة ينحدر أصلها من كلمة لاتينية ومنها انتقلت فيما بعد إلى اللغات الأخرى، لدرجة أصبحت

[1]–محمد حسن عمر برواري، غسيل الأموال وعلاقته بالمصارف والبنوك، دراسة مقارنة، ط1، دار قنديل لنشر والتوزيع، عمان، 2013 ص182

مشتقاتها (الإرهابي ، الإرهاب ،الأعمال الإرهابية ،الإرهاب المضاد، الإرهاب السياسي ،الداخلي ،الدولي)مشتقات واسعة الانتشار عموما [1].

ولا يختلف معنى الإرهاب كثيرا في اللغة الإنجليزية عن نظيره في اللغة العربية فافعل (terrorize) يعني الشعور بفزع أو الخوف الشديد وكلمة (terrorisme)تعني استعمال العنف من اجل تحقيق أهداف سياسية أو إرغام الحكومة بقيام بعمل ما. وهي مشتقة من كلمة (terror) حيث نجد في اللغة العربية كلمة(terreur) ترادفها كلمة رعب وذعر أو رهبة كما ترادفها اصطلاحا كلمة إرهاب.[2]

ب) تعريف الإرهاب اصطلاحا

على الرغم من آن تحديد تعريف موحد للإرهاب يعد خطوة أساسية وهامة لتوصل إلى مكافحة هذا الوباء الخطير الذي يهدد الأمن وسلم الدوليين. إلا انه من الإشكاليات العويصة ومن أصعب الجوانب التي تواجه دراسة ظاهرة الإرهاب بصفة عامة رغم العديد من المحاولات لتعريفه وهذا يعود إلي تطور المستمر لهذا المصطلح مما جعل الفقهاء عاجزون لتوصل والاتفاق على تعريف واحد.

سنحاول التطرق لتعريف الاصطلاحي من خلال عرض مجهودات التي بذلها الفقه، اذ دخلت فكرة الإرهاب عالم الفكر القانوني لأول مرة في المؤتمر الأول لتوحيد القانون العقابي الذي انعقد في مدينة وارسو في بولندا عام 1930و منذ ذلك الوقت لم تتوقف المحاولات الفقهية لوضع تعريف جامع للإرهاب.

1) تعريف الإرهاب على الصعيد العربي

عرف الدكتور عبد العزيز سرحان"الإرهاب على انه كل اعتداء على الأرواح والأموال والممتلكات العامة والخاصة، بمخالفة أحكام القانون الدولي العام بمصادره

[1]– محمد حسن عمر برواري ، المرجع السابق، ص182

[2]–المرجع نفسه، ص182

المختلفة، بما في ذلك المبادئ العامة للقانون بمعني الذي تحدده المادة 38 من النظام الأساسي لمحكمة العدل الدولية "[1].

كما عرفه أيضا احمد جلال عز الدين بأنه "عنف منظم ومتصل بقصد خلق حالة من التهديد العام الموجه إلى دولة أو جماعة سياسية والذي ترتكبه المنظمة بقصد تحقيق أهداف سياسية" [2] . بينما عرفه الدكتور محمد إبراهيم زياد على انه " اللجوء إلى العنف أو تهديد بالعنف من جانب جماعة ترمي إلى تحقيق هدف يتعارض مع أهداف السلطة التشريعية "[3]. كما انه جاء في الموسوعة السياسية أن الإرهاب هو استخدام العنف الغير القانوني أو التهديد به بغية تحقيق هدف سياسي"[4].

2) على الصعيد الغربي (الأجنبي)

عرف دافيد"david" الإرهاب على انه " كل عنف مسلح يرتكب بغرض سياسي او اجتماعي أو فلسفي أو إديلوجي أو ديني،ينتهك المبادئ المستقرة للقانون الإنساني التي تجرم استخدام قاسية أو تدميرية أو مهاجمة أهداف بريئة دون أن يكون لذلك ضرورة عسكرية"[5] ومن جهة أخرى يعرف الفقيه "wardlaw"الإرهاب على انه " استخدام العنف أو التهديد من فرد أو جماعة تعمل أما لصالح سلطة قائمة أو ضدها،عندما يكون الهدف من ذلك العمل هو خلق حالة من القلق الشديد لدى مجموعة من الضحايا المباشرة

---

[1]–لونيسي علي، اليات مكافحة الإرهاب الدولي بين فعالية القانون الدولي وواقع الممارسات الدولية الانفرادية، رسالة دكتورة في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص21

[2]–عبد القادر زهير النقوزي، مفهوم القانوني لجرائم الإرهاب الداخلي والدولي، منشورات حلبي الحقوقية، ط1، بيروت، 2008، ص21

[3]–محمد إبراهيم زيد، مقدمة في علم الاجرام وعلم العقاب، دار الهدى للمطبوعات، الإسكندرية، 2008، ص228

[4]–ليندا بن طالب، غسيل الأموال وعلاقتها بمكافحة الارهاب، دراسة مقارنة، دار الجامعة الجديدة لنشر، الإسكندرية، 2011، ص142

[5]– هارون فتوسي، الجريمة الإرهابية على ضوء قانون العقوبات الجزائري، مذكرة ماستر في القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن لمهيدي، ام لبواقي،2014/2013، ص10

للإرهاب وإجبار تلك المجموعة على موافقة على مطالب لمرتكبي العمل إرهابي " [1] كما اقر الفقيه فيجيه "vigima" أن الإرهاب هو استخدام العنف كأداة لتحقيق الأهداف السياسية " [2]

ثانيا: تعريف الإرهاب الالكتروني

إذا سلمنا بفكرة مفادها أن مفهوم الإرهاب كمصطلح تقليدي أصبح واضح إلى حد ما، فإن الارهاب الإلكتروني كمفهوم مستحدث يكتنفه الكثير من الغموض، وذلك أنه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه ومن حيث دور الفاعل فيه وطبيعة سلوكه [3]

وان غياب تعريف موحد لإرهاب متعمد إن صح التعبير وذلك بسبب عدم رغبة الدول في تقديم تعريف شامل من اجل سد الثغرات والفراغ القانوني الذي صاحب التطور التكنولوجيا المعلومات السريع، لذلك غالبا ما نجد التعريفات تأتي فضفاضة غير محددة من اجل إمكانية احتوائها لأي فعل من الأفعال الإرهابية الجديدة ممكنة الحدوث. ويستنبط تعريف الإرهاب الالكتروني من التعريفات السابقة للإرهاب العام، حيث نلاحظ أن مبدأ تجريم الإرهاب واحد وهو العنف والتهديد.

أ) المقصود بالإرهاب الالكتروني:

مع أن الارهاب الالكتروني أصبح شائعا في السنوات الأخيرة، وبات خطرا كبيرا على الصعيد الدولي ولاسيما مع التطور السريع لتقنيات الاتصال واعتماد المتزايد للبشر على الانترنت، إلا انه لا يوجد لحد الآن تعريف عالمي متفق عليه لهذه الظاهرة، فقد تعددت التعريفات التي تناولته.

---

[1]– احمد محمد رفعت، الإرهاب الدولي، دار النهضة العربية، القاهرة، 2006، ص216

[2]– عصام عبد الفتاح عبد السميع مطر، جريمة الإرهابية، دار الجامعة الجديدة لنشر، الإسكندرية، جمهورية مصر العربية، 2005، ص39

[3]– أسامة احمد المناعسة، جلال محمد الزعبي، جرائم التقنية نظم المعلومات الالكترونية، دراسة مقارنة، ط2، دار الثقافة لنشر والتوزيع، عمان، الأردن،2014، 321

يتألف مصطلح الإرهاب الالكتروني (cyberterrorisem)من كلمتين كلمة (cyber)تعني الانترنت و (terrorisem)و تعني الإرهاب ،ولقد ظهر هذا المصطلح عقب التطورات الكبيرة التي حققتها تكنولوجيا المعلومات واستخدام الحواسب الآلية والانترنت في الإدارة معظم شؤون الحياة. حيث نجد أن الغرب أول من تفطن لهذا الإرهاب الرقمي أو ما يسمى سيبراني أو المعلوماتي أو الشبكي حيث تعددت تسمياته، فأول من استخدام كلمة الارهاب الالكتروني هو "Barry Collin "في فترة الثمانينات واقر بصعوبة إعطاء تعريف شامل للإرهاب التكنولوجي وعرفه انه "هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو إيدلوجية وان الهجمة يجب أن تكون ذات أثر مدمرو تخريبي مكافئ للأفعال المادية للإرهاب "

وفي بداية التسعينات صدر تقرير عن الأكاديمية الوطنية الأمريكية للعلوم عن أمن الكمبيوتر جاء فيه: " نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة على أجهزة الكمبيوتر، حيث غدا بإمكان الإرهابيين إحداث تدمير كبير بالاعتماد على لوحة المفاتيح أكثر من استخدام القنبلة، وقد يتسبب ذلك في بيرل هاربر الكتروني جديد [1]

ولقد ظهر الإرهاب الالكتروني بشكل علني في الولايات المتحدة الأمريكية عندما قام الرئيس بيل كلينتون سنة 1996 بتشكيل لجنة حماية منشآت البنية التحتية، التي توصلت إلى أن مصادر الطاقة والاتصالات وكذا شبكات الكمبيوتر ستكون هدف الأول للهجمات الإرهابية، ولكن هذه الأخيرة لم تعرفه اكتفت بدراسة الظاهرة ومحاولة فهم سياسة تفكير الإرهاب الالكتروني والطرق التي يتخذها في تنفيذ عماليته بحيث تظهر الدراسة شغف

[1]–عادل عبد الصادق، استخدام الإرهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015، ص104

الإرهابيين في استخدام شبكة الانترنت في عملياتهم الإرهابية، مظهرين بذلك براعتهم في التفوق على أي تقنية مستخدمة.[1]

وفي هذا الصدد قامت وكالة المخابرات المركزية الأمريكية بتعريف الإرهاب الالكتروني على انه "أي هجوم تحضيري ذو دوافع سياسية موجهة ضد نظم المعلومات والتي تنتج عن العنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين"[2]

في حين عرفه مركز الحماية البنية التحتية القومية الأمريكية "انه عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية ولا السلكية ينتج عنه تدمير وتعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو إيدلوجية ".[3]

كما نلاحظ أيضا أن الاتحاد الأوربي بدوره يقر بجرائم الإرهاب الالكتروني من خلال الاتفاقية بودابست ولكنه لم يعرفه، اكتفى بتعريف الإرهاب بشكل عام سنة2002على انه "كل عمل يرتكب بهدف ترويع الأهالي، أو إجبار أو تدمير الهياكل الدستورية أو الاقتصادية أو الاجتماعية لدولة ما أو هيئة دولية ما أو زعزعة استقرارها"، وبعدما قامت دول الأعضاء بتعريفات غير موفقة للإرهاب الالكتروني أتي الاتحاد بهذا التعريف الشامل للإرهاب.[4]

حيث أن فرنسا عرفت الإرهاب الالكتروني على انه "كل هجوم الغرض منه الحصول على معلومات المرتبطة بالغير وإمكانياته واستراتيجياته التي يتخذها لدفاع عن

---

[1]– نجاري بن حاج علي فايزة، الاليات القانونية للإرهاب الالكتروني، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016، ص24

[2]–عادل عبد الصادق، المرجع السابق، ص106

[3]–توفيق مجاهد، طاهر عابسة، جريمة الإرهاب في ضوء احكام الاتفاقية العربية لمكافحة جرائم التقنية المعلومات، لعام 2010، مجلة العلوم القانونية والسياسية، المجلد 09، العدد03، ديسمبر 2018، جزائر، ص82

[4]–عادل عبد الصادق المرجع نفسه، ص106

نفسه أو تدمير نظم المعلوماتية أو نشر المعلومات الزائفة من اجل تضليله بتوظيف التكنولوجيا الحاسب الآلي وتكنولوجيا المعلومات والانترنت "[1]

كما عرفته إيطاليا انه "كل جماعة إرهابية تستعمل الوسائل التكنولوجيا كالانترنت من اجل الدعاية لنشاطاتهم أو التعريف بأهدافهم أو التنسيق أو التبادل المهارات والخبرات والأساليب، أو جمع التبرعات من اجل تمويل عماليتهم الإرهابية " [2]

بإضافة إلى أن بعض الدول العربية أيضا حاولت إعطاء تعريف الإرهاب الالكتروني

حيث عرفته مصر على انه "الاستخدام الغير القانوني للقوة أو الضعف ضد الأفراد وممتلكات بغية الإرهاب والتهديد لإرغام الحكومة أو السكان المدنيين أو أي فئة أخرى على القبول بهدف سياسي أو اجتماعي أو اقتصادي"

كما عرفته المملكة السعودية على انه "أي فعل يرتكب متضمن استخدام الحاسب الآلي أو شبكة المعلوماتية أو استخدام التقنيات الرقمية المخالفة لأحكام النظام ومن أنواعه السب، التشهير، والابتزاز، والإباحة وكذلك الشائعات وما يتعلق بأمور المالية كاعتداء على البطاقات البنكية بأشكالها واختلاسها "[3]

كما عرفه عادل عبد الصادق بأنه "يعني العدوان أو التخويف أو تهديد ماديا أو معنويا باستخدام الوسائل الالكترونية الصادرة من دول أو جماعات أو الأفراد عبر الفضاء الالكتروني أو أن يكون هدفا لذلك العدوان بما يؤثر على الاستخدام السلمي له "[4]

---

[1] –Pitter BELLEY, Hached attacked, abused digital crime exposed, London. Regan Page, 2002. p 107.

[2] – Steven FURNELL, Cyber crime vandalizing the information society. London. Addison, cuesely. 2002. p 253.

[3] – نجاري بن حاج علي فايزة، المرجع السابق، ص29.28

[4] –عادل عبد الصادق، الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة، ط1، مركز الاهرام للدراسات السياسية والاستراتيجية , 2009، ص109

وهناك من عرفه انه "هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا توجه من اجل الانتقام والابتزاز أو الإجبار أو التأثير على الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة وبتالي لكي يلقب الشخص ما بأنه إرهابي على الانترنت وليس مخترقا فقط فلا بد من أن تؤدي الهجمات التي يشنها إلي عنف ضد الأشخاص أو على الأقل تحدث أذى كافيا من اجل نشر الخوف والرعب.[1]

ولقد عرفه الفقه انه" خرق للقانون يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف إثارة اضطراب خطير في نظام العام عن طريق شبكة المعلومات العلمية الانترنت "[2]

ومن خلال ما تم عرضه نلاحظ أن كل المجتمع الدولي اقر واعترف بهذا التهديد الجديد. الذي يعتبر حديث العهد ولكنه سريع الانتشار و الالتهاب بتسارع تقدم التكنولوجيا المعلومات والاتصالات الرقمية والانترنت، فلإرهاب الالكتروني حظي باهتمام كبير على مستوى المجتمع الدولي بآسره و لكن هناك من لم يتطرق إلى تعريفه و اكتفى بتحديد السلوكيات الإجرامية المرتكبة بتقنيات الحديثة و هذا ينطبق على الاتفاقيات و التشريعات الدولية ،ونلاحظ أن المشرع الجزائري هو الأخر اكتفي بتصدي لظاهرة الإرهاب باستخدام تكنولوجيات الإعلام و الاتصال اثر تعديل قانون العقوبات بالقانون 16. 02 و إضافة مادتين 87 مكرر 11 و 87 مكرر 12 لمواجهة الإرهاب الالكتروني و لم يقدم تعريف لهذه الظاهرة .[3]

ورغم كل التعريفات الواردة بحق الإرهاب الالكتروني إلا أنها تبقى غامضة وغير كاملة ولم يتم تناولها بشكل عملي جدي، وسنأخذ بالتعريف الأقرب لصواب وهو تعريف المجمع الفقه الإسلامي "العدوان أو تخويف أو تهديد ماديا ومعنويا باستخدام الوسائل

[1]–علي عدنان الفيل، الاجرام الالكتروني، ط1، مكتبة زين الحقوقية والأدبية، لبنان،2011، ص60

[2]–اسراء طارق جواد، كاظم الجابري، جريمة الإرهاب الالكتروني، دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق ن جامعة البحرين، العراق،2012، ص23

[3]–غلاف كريمة، جرلال زوهرة، مرجع السابق، ص15

الالكترونية الصادر من الدول أو جماعات أو أفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الفساد في الأرض"[1]

وفي الأخير نستنتج أن الإرهاب الالكتروني هو كل فعل من أفعال العنف أو التهديد أي كانت بواعثه وأغراضه يقع تنديدا لمشروع إجرامي أو جماعي باستخدام وسائل الكترونية [2]

ب) خصائص الإرهاب الالكتروني

بناء على ما تم عرضه سابقا من التعريفات مختلفة للإرهاب سواء من قبل الفقه أو غيره يظهر لنا جليا انفراد الإرهاب الإلكتروني بمجموعة من الخصائص التي تميزه عن غيره من أنواع الإرهاب، ويمكن إجمال هذه الخصائص في النقاط التالية:

1. عصري يستخدم التقنيات وتكنولوجيا الحديثة: يتميز هذا الإرهاب عن الارهاب التقليدي باستعمال الوسائل الالكترونية وحدوثه في بيئة هادئة خالية من القوة والعنف فهو لا يتطلب أكثر من حاسب آلي مرتبط بانترنت وبعض البرامج الأزمة

2. عابر للحدود: يتميز بأنه عابر للحدود والقارات فهو لا يخضع لأي نطاق جغرافي معين لأنه يتم في بيئة الكترونية

3. صعوبة اكتشاف جرائم الإرهاب الالكتروني:وهذا يعود إلى نقص الخبرة لدى الجهات الأمنية والقضائية في التعامل في مثل هذه الجرائم المستحدثة دائمة التطور والتغير وغالبا ما تحدث جرائم لا يعلمون بوقوعها أصلا

4. صعوبة إثبات جرائم الإرهاب الالكتروني:وهذا يعود إلي سهولة إتلاف الدليل الرقمي إن وجد أصلا

[1]–امير فرج يوسف، الجرائم الدولية للأنترنت، ط1، المركز القومي للإصدارات القانونية، مصر، 2011، ص139

[2]–عادل عبد الصادق، الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة، المرجع السابق، ص109

5. ذكاء وخبرة مرتكب جريمة الإرهاب الإلكتروني: غالبا ما يكون مرتكب هذه الجريمة يتسم بقدر عالي من الذكاء والحيطة ومن ذوي الاختصاص في مجال التقنية المعلومات او خبير في مجال الحاسب الآلي وشبكة المعلوماتية

6-تعدد مرتكبي الجريمة الإرهاب الالكتروني غالبا ما يتم بتعاون أكثر من شخص على ارتكابه (منظمات والجماعات الإرهابية).[1]

ثالثا: تمييز الإرهاب الالكتروني عن غيره عن غيره من المفاهيم

إن مصطلح الإرهاب الالكتروني يتشابه ومرتبط نوعا ما ببعض المصطلحات التي تتمثل في الإرهاب التقليدي، جريمة الالكترونية، القرصنة، حرب المعلومات، جريمة المنظمة ... سنحاول عرض أهم أوجه التشابه والاختلاف بينهم.

أ) تمييز الإرهاب الالكتروني عن الإرهاب العادي

إن الفكرة الأساسية في تجريم الإرهاب ثابتة تتمثل في خوف المترتب على استخدام العنف وان الهدف من كل أنواع الإرهاب نشر الخوف والفزع داخل المجتمع وبما إن الإرهاب الالكتروني يعتمد على العنف الالكتروني باستخدام تطبيقات الانترنت والخدمات المتصلة بها فان الإرهاب التقليدي هو نفسه الإرهاب الالكتروني إلا انه يستخدم الحاسب الآلي كمصدر للهجمات إذن الاختلاف بينهما يكمن في الطريقة العصرية في استخدام الموارد المعلوماتية ووسائل الالكترونية التي جلبتها تقنية عصر المعلومات.[2]

ب) تمييز الإرهاب الإلكتروني عن الجريمة الالكترونية

أدى التطور الحاصل في مختلف مجالات الحياة وكثرة استخدام الحاسبات الآلية إلى ظهور الجرائم ذات طبيعة الكترونية أطلق عليها عدة تسميات منها جرائم المعلوماتية،

[1]- مصطفى يوسف كافي، الإدارة الالكترونية،د.ط، دار ومؤسسة رسلان لطباعة والنشر، سوريا، دمشق، 2011، ص441

[2]- نور الله تلة، الإرهاب بالوسائل الالكترونية، مذكرة ماجستير في القانون الجزائي كلية الحقوق، جامعة دمشق،2015-2016، ص26-27

جرائم الكترونية، جرائم التقنية العالية .... الخ.[1] ولقد خصص لها المشرع الجزائري القسم السابع من القانون 15.04 معدل لقانون العقوبات المعنون "المساس بأنظمة المعالجة الآلية للمعطيات" من خلال إضافة المواد 394مكرر إلى 394مكرر 8.[2]

ولقد اصطلح المشرع الجزائري على الجريمة المعلوماتية مصطلح تكنولوجيا الإعلام والاتصال عند استحداثه لقانون 04.09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وعرفها بموجب المادة 2 منه "الجرائم المساس بأنظمة المعالجة للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية أو نظام الاتصالات الالكترونية ".[3]

إذن لتكون الجريمة معلوماتية يجب أن ترتكب بواسطة منظومة معلوماتية أو نظام اتصال الكتروني حسب المادة 2 من القانون 04.09 ومن هنا نلاحظ أن الجريمة الالكترونية والإرهاب الكتروني يشتركان في

1. في الوسيلة المستعملة في ارتكابهما أي التكنولوجيا الحديثة وتعدان من الجرائم ذات طبيعة مشتركة
2. كلاهما من الجرائم المستحدثة والعابرة للحدود الوطنية والإقليمية
3. يعتبران من الجرائم التي تهدم القيم
4. ومن الجرائم السلمية لا يتطلبان العنف والقوة في ارتكابهما
5. سهولة الارتكاب وقلة التكلفة
6. يشتركان في خصوصية المجرم الذي يمتاز بذكاء والفطنة

[1]– حسين شفيق، –الاعلام الجديد والجرائم الالكترونية التسريبات. التجسس الالكتروني. الإرهاب الالكتروني، دار الفكر والفن، بدون بلد النشر ،2015 ص17

[2]– الامر رقم 66–156، المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات، ج ج د ش، جريدة الرسمية، ال عدد49، مؤرخ في 19جوان 1966، المعدل والمتمم

[3]– القانون رقم 09–04 المؤرخ في 5غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، الجريدة الرسمية، العدد 47

ورغم كل نقاط التشابه بينهما إلا أنهما يختلفان في الهدف فالجريمة المعلوماتية تسعى لتحقيق الربح بينما الإرهاب بإضافة إلى الربح يسعى لتحقيق أغراض سياسية، ثقافية، دينية . كما أن المجرم المعلوماتي اقل خطورة من المجرم الإرهابي المعلوماتي.[1]

ج) تمييز الإرهاب الالكتروني عن قرصنة:

جريمة القرصنة والاختراق هي " عصيان مدني الكتروني يحتوي رموز سياسية بهدف تعزيز الإيدلوجية السياسية فاختراق بشكل عام هو القدرة على الوصول للهدف بطريقة غير مشروعة عن طريق الثغرات في نظام الحماية الخاص بالهدف "[2]

وتهدف هذه الجرائم للاستيلاء على المكاسب المادية المحدودة والتسلية أو الإزعاج، هدف القرصان هو العبور الأنظمة والبيانات في حين الإرهاب الالكتروني هو استخدام الإمكانيات التقنية والعلمية واستغلال قدرات الحاسوب وشبكات المعلوماتية.[3]

د) تمييز الإرهاب الالكتروني عن حرب المعلومات:

يمكننا التميز بينهما من خلال التعرض إلى تعريف حرب المعلومات وهي "استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل المعلومات الخصم وعماليته مبنية على المعلومات والنظم المعلوماتية وشبكات الحاسب الآلي الخاصة به، وكذلك الحماية من خطر الهجوم من قبل الخصم لإحراز التقدم على الأنظمة العسكرية والاقتصادية "

كما أنها تنقسم إلى نوعين

---

[1]–غلاف كريمة، جرلال زوهرة، جريمة الإرهاب الالكتروني، مرجع سابق، ص ص27،28

[2]–عبد الله بن عبد الغزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم الى المؤتمر الدولي الأول حول حماية امن المعلومات والخصوصية في قانون الانترنت المنعقد من2 الى 4 يونيو، القاهرة، مصر، 2008، ص12

[3]– احمد فلاح العموش، مستقبل الإرهاب في هذا القرن، مطابع جامعة نايف للعلوم الأمنية، الرياض ،2006، ص ص9495

. حرب معلومات هجومية: تقوم بها في الغالب الدولة أو أجهزة استخباراتها لأهداف سياسية وعسكرية أو غيرها حيث يستحوذ المهاجم على المعلوماتية ونظمها ويقوم بسرقة البرامج الكمبيوترية أو يقوم بتخريب أو تعطيل نظم معلوماتية.

أما حرب المعلومات الدفاعية: تعمل على حدود الوقاية من إعمال تخريبية التي قد تتعرض لها وتختلف الوسائل الدفاعية باختلاف أدوات التخريب والمعلوماتية وطبيعة الإضرار التي قد تحدثها.[1]

ومن أبرز أوجه التشابه بينهما:

. هي عمليات تتم عبر شبكة الانترنت وبواسطة الحاسب الآلي

. صعوبة اكتشافها وفي الغالب ما يفلت المجرم من العقاب بسب غياب الأدلة

. قلة التكلفة

. ذكاء وخبرة مرتكبيها

ورغم العلاقة الوثيقة التي تظهر بينهما إلا انه هناك اختلاف بينهما حيث ان حرب المعلومات ما هي إلا أداة يمكن لفاعلون في الإرهاب الالكتروني استخدامها في تنفيذ أهدافهم ويمكن أن تتحول بحد ذاتها لإرهاب الكتروني بناء على من يقف وراء استخدامها كجماعات الإرهابية، وليس كل سوء استخدام للفضاء الالكتروني إرهابا.[2]

و) تمييز الإرهاب الالكتروني عن الجريمة المنظمة:

كان يطلق على الجريمة المنظمة مصطلح عصابات المافيا وهي من بين الجرائم التي تطورت باحتكاكها بالتطور التكنولوجي الحاصل في العالم،ولقد عرفت على انها "ظاهرة إجرامية التي يكون ورائها جماعات معينة تستخدم العنف أساسا لنشاطها الإجرامي بهدف الربح وقد تمارس نشاطها وطنيا أو خارجيا أو تكون لها علاقات بمنظمات إجرامية

[3]– عادل عبد الصادق، الإرهاب الالكتروني القوة في العلاقات دولية نمط جديد وتحديات مختلفة، ط2، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة ،2009، ص ص136،135،133

[2]– المرجع نفسه، ص136

متشابهة لها في الدول الأخرى " [1]،وانطلاقا من ان "كل جريمة إرهابية جريمة منظمة ولكن ليس كل جريمة منظمة حدثا إرهابيا "[2].

يمكننا القول إن الجريمة المنظمة والإرهاب الالكتروني متداخلين ولتمييز بينهم استعرض أهم أوجه التشابه بينهما

1. كلتهما جرائم تطورت بفضل احتكاكهما بتكنولوجيا العصر ويعتمدان على وسائل الاتصال الحديثة
2. يعتبران من الجرائم العالمية العابرة للحدود
3. يسعيان إلى بث الرعب والخوف في نفوس لتحقيق الأهداف
4. يتشابهان من حيث القواعد التي تحكم نظامها الداخلي (التعاون والتخطيط)
5. يسعيان لإيجاد ممول لأعمالهما الإجرامية واستقطاب أعضاء جدد

من بين أهم نقاط لاختلاف الجوهرية بينهما:

. يختلفان في الهدف غاية الجريمة المنظمة استخدام العنف لكسب المصالح الشخصية وأرباح مادية أما الإرهاب أهدافه غير محددة سواء سياسية أو دينية أو مادية ...

. الجريمة المنظمة تشترط عنصر الاستمرارية والجماعة على عكس الإرهاب الذي يمكن أن يرتكب في إطار فردي

. تشهير بأعمال الإرهابية عن طريق الإعلام على عكس الجريمة المنظمة التي ترتكب بسرية

. اعتراف الدولة بإرهاب ككيان من خلال التفاوض مع مجرميها على عكس الجريمة المنظمة.[3]

---

[2]– مجراب دوادي، الأساليب الخاصة للبحث والتحري في الجريمة منظمة، أطروحة الدكتورة، كلية الحقوق، تخصص قانون عام، جامعة يوسف بن خدة، الجزائر 2015–2016 ص09

[2]– محمد امين بشرى، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث جامعية نيل العربية للعلوم الأمنية، الرياض، 2004، ص146

[1]– غلاف كريمة، جرلال زوهرة، المرجع السابق، ص ص30،31

الفرع الثاني: صور الإرهاب الالكتروني

يرتبط الإرهاب الالكتروني بتقدم التكنولوجي في كافة مجالات الحياة وفي العالم بأسره وبذلك اتخذ إبعاد جديدة وازدادت خطورته على المجتمعات الدولية[1].

فمصطلح الإرهاب الالكتروني ينطلق من عالمين العلم المادي الذي يشير إلى العالم الملموس قضايا والظواهر المتعددة منها الطاقة، الكهرباء، الضوء والعالم الافتراضي يشير إلى التمثيل الرمزي المجازي للمعلومات وهو المكان الذي تتم فيه العمليات الإرهاب الالكتروني التدمير والتخريب[2].

ويعرف الإرهاب الالكتروني بتعدد أشكاله وصوره بحكم انه ينشط في عالم افتراضي غير المرئي لذا يصعب رصده وحصره فلا يتخذ طابعا ونمطا واحدا فقد تكون مستقلة بحد ذاتها كجريمة عادية ولكن بارتباطها بعناصر الإرهاب وأساليبه وأهدافه خطره تعد حينها جريمة إرهابية وسنحاول تسليط الضوء على بعض صور الإرهاب الالكتروني.

أولا: جريمة غسيل الأموال

تعد ظاهرة غسيل الأموال من الجرائم المستحدثة المحظورة قانونيا، فهناك إجماع دولي على تحريمها مما دفع مرتكبيها إلى استخدام تقنيات الحديثة ووسائل المتطورة لتمويه و التعتيم و التضليل عبر شبكة معقدة من ترتيبات و إجراءات وعلى درجة عالية من السرية ومما لاشك فيه أن استخدامها لتلك التقنيات ووسائل المتطورة جعلها من اخطر الجرائم وأكثرها شرا على الاقتصاد العالمي ، وذلك بارتباطها بكافة أشكال الجريمة المنظمة و اخصها تجارة السلاح و المخدرات ... الخ و دعم المنظمات الإرهابية بصورة مباشرة ، فهي ترتبط بأنشطة غير مشروعة و عمليات مشبوهة . وتعتبر من الجرائم ذات

[1]–عبد الرحمان سند، وسائل الإرهاب الالكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، ج1، د.ط، الرياض، 2004، ص224

[2]–عمر الفاروق، تأملات في بعض صور الحماية الجنائية لبرامج الحاسوب الالي، بحث مقدم الى مؤتمر الكويت، مجلة المحامي ،1989، ص57

الطابع الدولي فتزداد انتشارا يوما بعد يوم رغم كل الجهود الدولية والإقليمية المبذولة لمواجهتها([1]).

أ) تعريف جريمة غسيل الأموال

لقد تعددت تعريفات جريمة غسيل الأموال نتيجة لحداثتها وسرعة انتشارها في جميع أنحاء العالم، الأمر الذي جعلها تحضي باهتمام مختلف المؤتمرات وتشريعات والفقهاء الذين سارعوا إلى محاولة تحديد مفهومها فهناك من عرفها على أنها "**تحويل أو نقل الأموال التي يتم الحصول عليها بطرق غير مشروعة أو متهربة من التزامات قانونية إلي أشكال أخرى من أشكال الاحتفاظ بثروة لتغطية على مصادرها والتجهيل بها** " [2]

وعرفها البعض الأخر على أنها " أي عملية من شانها إخفاء المصدر الغير المشروع الذي اكتسبت منه الأموال "[3]

ونلاحظ ان المشرع الجزائري خصص القسم السادس مكرر من قانون العقوبات لجرائم تبيض الأموال واعتبر كل الأفعال الواردة في المادة 389 مكرر[4]، تبيضا للأموال "يعتبر تبيضا للأموال:

1. تحويل الممتلكات ...
2. إخفاء أو تمويه ...
3. اكتساب الممتلكات أو حيازتها ...
4. المشاركة في ارتكاب ...

[1]–حامد عبد اللطيف عبد الرحمن، جريمة غسيل الأموال وسبل مكافحتها، رسالة ماجستير، مملكة البحرين ،2012، ص

[2]–سيد احمد عبد الخالق، الآثار الاقتصادية والاجتماعية لغسيل الأموال، د ن ط، دار النهضة العربية، القاهرة ،1997، ص03

[3]–محمد فتحي عيد، الإجرام المعاصر، د ن ط، منشورات أكاديمية نايف للعلوم الأمنية، الرياض،1999، ص280

[4]–انظر المادة 389 مكرر من قانون العقوبات

وبذلك يكون المشرع الجزائر يقد تبنى المفهوم الذي جاءت به اتفاقية الأمم المتحدة لمكافحة الاتجار الغير المشروع بالمخدرات والذي يشمل تبيض الأموال متأتية من أي جريمة كانت.[1] حيث عرفته كما يلي سنة 1988 "عملية تحويل الأموال أو نقلها مع العلم أنها مستمدة من أية جريمة بهدف إخفاء أو تمويه المصدر الغير المشروع للأموال أو بقصد مساعدة أي شخص متورط في ارتكاب مثل هذه الجريمة على الإفلات من العواقب القانونية لأفعاله"[2]

ب) علاقة الإرهاب الالكتروني بجريمة غسيل الأموال

لقد أثبتت مختلف الدراسات وجود علاقة بين غسيل الأموال بصورتها التقليدية او المعاصرة بحركات الإرهاب والتطرف والعنف الداخلي.

ولقد أدى استعمال الوسائل التقنية الحديثة في جريمة غسيل الأموال إلى تسهيل إجراء العديد من العمليات المصرفية و تحويل الأموال في دقائق معدودة مما يصعب رصد حركة هذه الأموال كما ساهمت مواقع الانترنت في تبيض و تسهيل حركة الأموال الغير المشروعة [3].

ويعد التبيض إحدى الركائز الضرورية التي يعتمد عليها الإرهاب لتمويل أعمالهم وأنشطتهم الإجرامية، وهناك علاقة وطيدة بينها خاصة باحتكاك كل منهما بتكنولوجيا الحديثة وتظهر هذه العلاقة بصفة مباشرة بانتهاج الإرهابيون الإجرام المنظم في أعمالهم الإرهابية إلى جانب الاتجار بمعادن نفسية، والأسلحة والمخدرات وغيرها من المصادر

[1]–شراك عماد، بن عطاء الله طارق، ظاهرة تبييض الأموال في ظل التشريع الجزائري، مذكرة ماستر، تخصص إدارة ومالية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، جلفة،2016.2017، ص7.6

[2]–اتفاقية الأمم المتحدة لمكافحة الاتجار الغير المشروع في المخدرات، فينيا، 1988، مادة 3

[3]–كتب علاء رضوان ، علاقة غسيل الأموال بالجرائم الالكترونية ،المقال متوفر على موقع https://www.youm7.com ، تاريخ النشر:2019/11/10، 9:00م، تاريخ التصفح 2020/08/29، الساعة 11:30

الأخرى الغير المشروعة بهدف الحصول على الأموال المشروعة يوظفونها الإتمام أعمالهم.[1] .

كما أن هذه العلاقة الوثيقة بينهما تدفع الارهابين للجوء لبعض أجهزة المخابرات و التجسس و استخدام الأموال الهاربة ، التي يتحصل عليها مختلف المجرمين كتجار المخدرات وتبيضها و استخدامها في تمويل الجماعات الإرهابية أو تأسيسها من اجل مزاولة أعمالها الغير المشروعة و عماليتها التخريبية و تدميرية الموجهة إلى أنظمة أو الحكومات معينة في مختلف الدول ، عن طريق استخدام شبكة المعلوماتية و ذلك بتأسيس مواقع الكترونية و قنوات فضائية لدعم تلك التنظيمات الإرهابية و تضليل الرأي العام، ومع اتساع نطاق العلاقة بينهما نصت الاتفاقيات الدولية في الآونة الأخيرة إلى إدراج جرائم الفساد و الإرهاب ضمن جرائم غسيل الأموال بهدف تجفيف منابع الفساد و الإرهاب.

ثانيا) جريمة التجسس الالكتروني:

يعد التجسس من أقدم وأخطر الأنشطة الاستخباراتية التي مارسها الإنسان قديما في مختلف الميادين خاصة الحروب.

ولقد تطور عقب الظفرة التي حققتها التكنولوجيا الإعلام واستخدام الحواسب الإلية وشبكات الانترنت،وأصبح الهاجس الأكبر لدول من أكثر الجرائم خطورة التي تستهدف المعلومات المخزنة في شبكات المعلومات[2]، ولا تكمن خطورته في استخدام الانترنت بل في ضعف الرسائل الأمنية المختصة في حماية الشبكات الخاصة بالمؤسسات والهيئات.

---

[1]–مصطفى طاهر، المواجهة التشريعية لظاهرة غسيل الأموال متحصلة من جرائم المخدرات، ط2، طبع على نفقة المؤلف، القاهرة، 2004، ص144

[2]– بن بادة عبد الحليم، بوحادة محمد سعد، جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة، متوفر على الموقع:https://www.elmizaine.com، تاريخ النشر :3يوليو2020، تاريخ التصفح 29 /2020/08، ساعة 14:05

وفي هذا العصر أصبحت الحدود الجغرافية مستباحة بأقمار التجسس والبث الفضائي، الأمر الذي أصبح يهدد سيادة الدول، خاصة إذا كان من يستخدمها هم الإرهابيين[1].

لان الخطر الحقيقي في التجسس لا يكمن في العابثين أو المخترقين فمخاطر هؤلاء تعد محدودة وتقتصر عادة على العبث أو إتلاف المحتويات التي يمكن استعادة النسخة المخزنة منها في الغالب، ولكن الخطر الأكبر يظهر من خلال استخدام الإرهاب لهذه الجريمة على الأشخاص أو الدول أو المنظمات أو الهيئات الدولية أو الوطنية.

وتستهدف عمليات التجسس الإرهابي ثلاثة أهداف رئيسية وهي التجسس العسكري والسياسي والاقتصادي،حيث تقوم التنظيمات الإرهابية وأجهزة الاستخبارات المختلفة بحصول على أسرار ومعلومات الدولة من ثم إفشائها لدول أخرى معدية أو استغلالها بما يضر المصلحة العامة للوحدة الوطنية لدولة[2].

ثالثا) جريمة التهديد والقصف الالكتروني

أ) التهديد الالكتروني

تستغل الجماعات الإرهابية شبكة الانترنت العالمية من اجل بث الرعب والخوف في نفوس الأفراد والدول ولقد تعددت الأساليب التي تستعملها في التهديد عبر الانترنت سوء بتهديد الضحية بنشر صور خاصة أو مقاطع فيديو أو فضح معلومات سرية مقابل دفع مبالغ نقدية طائلة، ويمكن أيضا استخدامه للإفصاح عن المعلومات السرية خاصة بشركة أو مكان عمل و يحدث ذلك عن طريق استدراج الضحايا عن طريق البريد الالكتروني أو مواقع التواصل الاجتماعي التي تستخدم من قبل كل الفئات العمرية[3]،كما يهدد بقتل

[1]–غادة نصار، الإرهاب والجريمة الالكترونية، العربي لنشر والتوزيع، قاهرة،2017، ص30

[2]–الزبن، بدرة هوميل، الإرهاب في الفضاء الالكتروني، رسالة دكتورة، كلية القانون، جامعة عمان العربية،2012، ص ص178،177

[3]–سليمان الطعاني، الوجيز في التربية الإعلامية، ط1، دار الخليج لنشر والتوزيع، الأردن، عمان، 2020، ص ص109،108

الشخصيات السياسية في الدولة أو بتفجير مراكز سياسية أو تدمير البنية التحتية المعلوماتية عن طريق نشر الفيروسات لإتلاف الأنظمة المعلوماتية ...الخ.[1]

ب) القصف الالكتروني

هو أسلوب الهجوم على الشبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الالكترونية إلى مواقع هذه الشبكات مما يزيد الضغط على قدرتها على استقبال الرسائل من متعاملين معها والذي يؤدي إلي وقف عمل الشركة، وعادة ما تلجا هذه المنظمات الإرهابية إلي تدمير البني التحتية الخاصة بأنظمة المعلومات في العالم بأسره.[2]

الفرع الثالث: دوافع الإرهاب الالكتروني

الإرهاب ظاهرة لم تولد صدفة، بل نتيجة تراكمية،لأسباب ودوافع متعددة ومتنوعة ومتشابكة تتحكم في ارتكابه، وهي عينها أسباب ظاهرة الإرهاب عموما فقد تكون سياسية أو اقتصادية أو فكرية ... الخ والى جانب هذه الأسباب فان الإرهاب الالكتروني ينفرد بجملة من الأسباب الخاصة التي جعلت منه موضوعا مناسبا وسلاحا سهلا للجماعات ومنظمات الإرهابية[3]. ونلاحظ أن تداخل وتشابك دوافع الإرهاب يعود إلى الطبيعة المعقدة والمركبة لظاهرة التي نحن بصددها.

أولا: الأسباب العامة للإرهاب

وهي ذاتها أسباب الإرهاب التقليدي وذلك يعود لكون الإرهاب الالكتروني نوع من أنواع الإرهاب وشكلا من أشكاله وتختلف هذه الأخيرة باختلاف الظروف والجهات

[1]–إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1، مركز الديمقراطي العربي لدراسات إستراتيجية والسياسية والاقتصادية، برلين، ألمانيا،2018، ص21

[2]–سليمان الطعاني، المرجع السابق، ص109

[3]–علي عدنان، الفيل، الإرهاب الالكتروني، مجلة الجامعية الخليجية، جامعة الخليج: كلية الحقوق، العدد 2، 2010، ص8

السياسية والأحوال المعيشية والاختلاف الديني والعقائدي...الخ فما يصلح على مجتمع ما قد لا يصلح بضرورة على غيره من المجتمعات[1].

أ) الأسباب الشخصية

1. الرغبة في الظهور إلي العالم وحب الشهرة والدعاية والمال فشعار، الجماعات الإرهابية "ارهب عدوك ونشر قضيتك"[2].

2. الرغبة في الانتقام من المجتمع نتيجة ما تعرض له الشخص من ظلم وتهميش وقهر وفقر.

3. الخلل والاضطراب النفسي لشخص حيث تتشكل لديه عقد نفسية تتمثل في الشعور بالنقص المادي والجسماني واحتقاره من قبل المجتمع.

4. الفشل في كل جوانب الحياة سواء الأسرية أو الدراسية أو الوظيفية أو العاطفية مما يولد شعور عدم الانتماء والولاء لوطنه وهذا ما يدفعه إلى الولوج إلى عالم الجريمة والانحراف والإرهاب[3].

ب) الأسباب الفكرية

1. الفهم والتفسير الخاطئ لدين ومبادئه وأحكامه وآدابه

2التطرف والتعصب الديني والفكري. [4]

3. جهل والأمية وعدم كفاية التعليم وكذا نقص دور التربوي وتهذيبي للمدارس[5]

---

[1]–مصطفى يوسف كافي، الإدارة الالكترونية، المرجع السابق، ص438

[2]–نسيب نجيب، التعاون الدولي لمكافحة الإرهاب، مذكرة نيل شهادة ماجستير في القانون الدولي، جامعة مولود معمري، تيزي وزو، 2009، ص40

[3]–الهويدي عمر، مكافحة جرائم الإرهاب، دار وائل لنشر، عمان، 2011، ص54

[4]–مصطفى يوسف كافي، الإدارة الالكترونية، المرجع السابق، ص439

[5]–أمير فرج، جريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، ط1، مكتبة الوفاء القانونية، الإسكندرية،2011، ص224

ج) الأسباب السياسية

1. ما تمارسه الدول ضد مواطنيها: من انتهاك في الحقوق والحريات وتهميش وفرض سياسات غير عادلة والاستيلاء على الأموال العامة وعدم المساواة في توزيع الثروات والخدمات الوطنية.[1]

2. غياب الديمقراطية وحرية الرأي والتعبير والشفافية يولدون الرغبة في التغير وغضب في الشوارع

3. تهميش الجماعات الإسلامية من قبل بعض الدول العربية والإسلامية والوقوف في وجهها وتصدي لأربابها وحصر نشاطها وتجميد عطائها مما أدى إلى ظهور منظمات سرية والغضب الشديد انصب في شكل إرهاب.

4. خرق القوانين ومواثيق الدولية أدى إلى التطرف [2]

د) الأسباب الاقتصادية

1. تفاقم المشاكل والأزمات الاقتصادية في مختلف المجتمعات والاستغلال الغير المشروع للموارد الاقتصادية

2. تفاوت الطبقي والاجتماعي وعدم المساواة فهناك الغنى الشديد والفقر المميت

3. انتشار البطالة والفقر وأزمات السكن وغلاء المعيشة والتضخم في أسعار مواد الغذائية والخدمات الأساسية مما أدى إلى التطرف والإرهاب

4. التقدم في أنظمة المصرفية مما سهل تحويل وانتقال الأموال حول العالم عن طريق انترنت مما ساعد منظمات الإرهابية على استغلال الفرصة من اجل تحقيق أهدافها غير المشروعة.[3]

---

[1]–مصطفى يوسف كافي، مرجع نفسه، ص439

[2]–عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، المرجع السابق، ص11

[3]– المرجع نفسه، ص ص439 ،440

و) الأسباب الاجتماعية

1. التفكك الأسري والاجتماعي والطفولة المضطربة مما يؤدي إلى الأمراض نفسية وانحراف والإرهاب

2. الجهل والفراغ النفسي والعقلي جعل الفكر يتقبل كل الأفكار التطرف والعنف [1]

ثانيا) الأسباب الخاصة للإرهاب الالكتروني

الدوافع التي ينفرد بها الإرهاب الالكتروني تتمثل في:

أ) ضعف البنية المعلوماتية للشبكات وقابليتها للاختراق

أن الشبكات المعلوماتية مصممة في الأصل بشكل مفتوح بدون قيود أو حواجز أمنية وذلك رغبة في توسيع وتسهيل الدخول المستخدمين، وتحتوي الأنظمة الالكترونية والشبكات المعلوماتية على ثغرات تستغلها المنظمات الإرهابية وتتسلل بواسطتها إلى البني المعلوماتية التحتية وتمارس عملياتها التخريبية.

ب) غياب الحدود الجغرافية وتدني مستوى المخاطرة

إن غياب الحدود المكانية في الشبكة المعلوماتية وعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعد فرصة مناسبة للإرهابيين، حيث يستطيع محترف الحاسوب أن يقدم نفسه بهوية والصفة التي يرغب بها، ويتخفى تحت أي شخصية وهمية، ومن ثم يشن هجومه الالكتروني وهو نسترخ في منزله أو في أي مكان من هذا العالم دون مخاطرة وبعيدا عن أعين الناظرين.[2]

[1]–مصطفى يوسف كافي، المرجع السابق، ص440

[2]–عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف ومصنفات الفنية، دار الثقافة لطباعة والنشر، 1999، ص83

ج) سهولة استخدام وقلة التكلفة

من سمات الشبكة المعلوماتية كونها سهلة الاستخدام، قليلة التكلفة فهي لا تكلف لا جهدا كبيرا ولا تستغرق وقتا طويلا، مما هيا للإرهابيين فرصة ثمينة للوصول إلي أهدافهم المشروعة ومن دون الحاجة إلي مصادر تمويل ضخمة[1].

د) صعوبة اكتشاف واثبات الجريمة الإرهابية

إن صعوبة الإثبات تعد من أقوى الدوافع المساعدة على ارتكاب الجريمة الإرهاب الالكتروني فاغلبا لا يعلم أصلا بوقوع الجريمة معلوماتية خاصة في بعض جرائم الاختراق وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل تنفيذ الجريمة.

و) الفراغ التنظيمي والقانوني وغياب السيطرة والرقابة على الشبكات المعلوماتية

إن الفراغ الشديد والقصور الملحوظ الذي تعاني منه التنظيمات والقوانين العالمية حول الإرهاب الالكتروني والجرائم المعلوماتية يعد من أهم الأسباب الرئيسية لتفشي وانتشار الإرهاب الالكتروني، وان غياب القوانين واللوائح تجريميه ردعية عالمية متكاملة جعلت المجرمين يشنون هجوماتهم من بلدان تعاني قصور وفراغ قانوني على بلدان توجد فيها قوانين صارمة في هذا المجال مما أدى إلي ظهور مشكلة تنازع القوانين وقانون الواجب تطبيق. كما أن انعدام جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مداخلها ومخارجها يعد سببا في تفشي ظاهرة الإرهاب الالكتروني، إذ يمكن لأي شخص الدخول ووضع ما يريد في الشبكة وكل ما يمكن لجهة الرقابة فعله هو منع الوصول إلى المواقع المحجوبة أو إغلاقها أو تدميرها بعد نشر المجرم لنا يريده.

وكل هذا جعل الإرهاب الالكتروني الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية[2].

---

[1]– عفيفي كامل عفيفي ، المرجع السابق، ص85

[2]–عبد الله عبد العزيز بن فهد العجلان، مرجع سابق، ص 12

المطلب الثاني: مظاهر الإرهاب الالكتروني ووسائله

يرتبط الإرهاب الإلكتروني بالمستوى المتقدم الذي باتت وسائل الاتصالات والتقنية المعلومات تلعبه في جميع مجالات الحياة وفي العالم بأسره.

ويبقى من الصعب علينا تحديد مظاهر ووسائل الإرهاب الالكتروني جميعا، فطبيعته تتطلب لامحدودية لأنه يستخدم التكنولوجيا التي تتطور يوما بعد يوم، ومن خلال هذا المطلب سنحاول تبيان أبرز مظاهر الإرهاب الالكتروني في (الفرع الأول) أما (الفرع الثاني) سنتناول فيه أهم وسائل وأساليب الإرهاب الالكتروني فحين سنتطرق في (الفرع الثالث) إلي أهداف الإرهاب الالكتروني.

الفرع الأول: مظاهر الإرهاب الالكتروني

إن الإرهاب الالكتروني يستهدف التقنية في القرن الواحد والعشرين والذي يؤثر على القوة الإنتاجية و الثقة في المجتمعات و من ابرز مظاهر الإرهاب الالكتروني تبادل المعلومات الإرهابية و نشرها من خلال شبكة المعلوماتية، و إنشاء مواقع إرهابية الكترونية.

أولا: تبادل المعلومات الإرهابية ونشرها من خلال شبكة المعلوماتية

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب وتبادل الآراء والأفكار والمعلومات صعبا في الواقع، فانه عن طريق شبكات المعلوماتية تسهل هذه العملية كثيرا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين،ويتبادلون الحديث والاستماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا إتباعا وأنصار عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الالكترونية[1].

[1]–عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، متوفر على الموقع التالي: http://www.shaimaaatalla.com، تاريخ النشر 2009/07/27، تاريخ التصفح 2020/08/30، الساعة:19:18

أ) الاتصال والتخفي وجمع المعلومات الإرهابية

تستخدم الجماعات و المنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الاتصال و التنسيق فيما بينهم ،نظرا لقلة تكاليف الاتصال و الرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى ،كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال و التخفي ، وذلك من طريق البريد الالكتروني أو المواقع و منتديات و غرف الحوار الالكتروني ،حيث يمكن وضع رسائل مشفرة تأخذ طابعا لا يلفت الانتباه ، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته ، كما أنها لا تترك أثرا وضحا يمكن أن يدل عليه ، وتمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما أنها تعتبر موسوعة الكترونية شاملة متعددة الثقافات ،و متنوعة المصادر و غنية بالمعلومات الحساسة التي يسعى الإرهابيين للحصول عليها كمواقع المنشئات النووية، و مصادر تولي الطاقة، و أماكن القيادة و السيطرة و الاتصالات و مواعيد الرحلات الجوية الدولية و المعلومات المختصة بسبل مكافحة الإرهاب و نحو ذلك من المعلومات التي تعتبر بمثابة كنز بالنسبة للإرهابيين ، نظرا لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية [1].

ب) التخطيط والحصول على تمويل للعمليات الإرهابية:

العمليات الإرهابية تعرف أنها عمل صعب ومعقد ، في هي تحتاج إلى التخطيط المحكم، و التنسيق الشامل، و تعتبر الشبكة العلمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية، حيث تتيح لهم حرية التخطيط الدقيق و التنسيق الدقيق لشن هجومات إرهابية محددة، في جو مريح و بعيدا عن أعين الناظرين مما يسهل للإرهاب ينترتيب تحركاتهم و توقيت هجماتهم .ومن خلال شبكة المعلوماتية العالمية و عن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية من خلال الاستفسارات و لاستطلاعات الموجودة

[1]–علي عدنان الفيل، المرجع السابق، ص80

على المواقع الالكترونية ، يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة و القلوب الرحيمة و من ثم يتم استجداؤهم لدفع تبرعات مالية للأشخاص اعتبارين يكونون واجهة لهؤلاء الإرهابيين ، يتم ذلك بواسطة رسائل البريد الالكتروني أو من خلال ساحات الحوار الالكترونية ، بطريقة ذكية و أسلوب مخادع لا يشك حتى المتبرع انه يساعد إحدى التنظيمات الإرهابية[1].

ج) التدريب الإرهابي الالكتروني

تحتاج المنظمات الإرهابية إلى تدريب خاص. ويعد التدريب أهم الهواجس التنظيمات الإرهابية، حيث انشات معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام لكن المشكلة تكمن في اكتشافها و مداهمتها في أي وقت ، لذا فان الشبكة المعلوماتية بما تحتويه من خدمات و مميزات أصبحت وسيلة مهمة لتدريب الإرهابي ،كما قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب و التخطيط و التنفيذ و التخفي، و هذه الأدلة يمكن نشرها على شبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم ، وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من الكم الهائل من المواقع و المنتديات و الصفحات التي تحتوي على كتيبات و إرشادات تبين كيفية تصنيع القنابل و المتفجرات و المواد الحارقة و الأسلحة المدمرة [2].

ثانيا: إنشاء مواقع إرهابية الكترونية

إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم فسرعان ما يغير نمطه الالكتروني غدا، ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان الكتروني مختلف، بل تجد لبعض المنظمات

[1]–السامي علي عياد، جريمة المعلوماتية واجرام الانترنت، ط1، دار الفكر الجامعي، الإسكندرية،2007، ص49

[2]–mohamed bozabar، la criminaliteinformatiquesurl internet، journal of law academic، n°01، voulum26 ،faculté de droit، universite kowit,2002، p24

الإرهابية آلاف المواقع حتى يضمنوا انتشارا أوسع،وحتى لو تم الحصول على بعض هذه المواقع أو تعرضت بعضها لتدمير تبقى مواقع الأخرى يمكن الوصول إليها.

أ) تدمير المواقع والبيانات الالكترونية ونظم المعلوماتية

تقوم التنظيمات الإرهابية بشن هجومات الكترونية، بقصد تدمير المواقع و البيانات الالكترونية و النظم المعلوماتية و إلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها و تستهدف الجماعات الإرهابية ثلاثة أهداف أساسية غالبا وهي أهداف عسكرية و سياسية و اقتصادية، وفي عصر ثورة المعلومات نجد الأهداف الثلاثة وعلى رأسها مراكز القيادة و التحكم العسكرية، ثم مؤسسات ذات المنافع كمؤسسات الكهرباء و المياه و من ثم تأتي المصارف و الأسواق المالية و ذلك الإخضاع إرادة الشعوب و المجتمعات الدولية [1].

وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماما دون تدمير المواقع او اختراقها بشكل دائم، فالمتغيرات التقنية، وإلمام المخترق بثغرات في التطبيقات والتي بنيت في معظمها على أساس تصميم المفتوح لمعظم الأجزاء، سواء كان ذلك في مكونات نقطة الاتصال أو في الشبكة أو في البرمجة، جعلت الحيلولة دون الاختراقات صعبة جدا، بالإضافة أن هناك منظمات إرهابية يدخل ضمن عملها ومسؤوليتها الرغبة في الاختراق وتدمير المواقع ومن المعلومان لدى المؤسسات من إمكانيات وقدرات ما ليس لدى الأفراد.

ويستطيع القراصنة الحواسب الالكترونية التوصل إلى المعلومات السرية والشخصية واختراق خصوصية وسرية المعلومات بسهولة، وذلك راجع إلى التطور المذهل في عالم الحاسب الآلي والشبكات المعلوماتية ويصاحبه تقدوه أعظم في الجرائم المعلوماتية وسبل ارتكابها، ولاسيما وان مرتكبها ليسوا مستخدمين عاديين بل قد يكونوا خبراء في مجال الحاسبة الالكترونية.

[1]–موزة مزروعي، الاختراقات الالكترونية خطر كيف تواجهه، مجلة الأفاق الاقتصادية، العدد 9، الإمارات المتحدة، 2008، ص59

ب) سيناريوهات المحتملة للإرهاب الالكتروني

لقد قام خبراء الجرائم الالكترونية والأمن المعلوماتي أكثر من سيناريو محتمل للهجمات الإرهابية وأودعوها في بحوث ودراسات والتقارير التي تعالج هذه المسالة وهي

1) استهداف نظم العسكرية:

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، المرتبطة بشبكات المعلومات و يعد هذا السيناريو من اخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، و تبدأ المرحلة الأولى من هذا السيناريو باختراق منظومات الخاصة بالأسلحة الإستراتيجية و نظم الدفاع الجوي، وصواريخ النووية، فقد تتوفر لدى الإرهابي المعلوماتي فرصة فك الشفرات سرية لتتحكم بنظام تشغيل منصات إطلاق الصواريخ الإستراتيجية و الأسلحة الفتاكة، فيحدث ما لا يحمد عقباه على المستوى العالمي[1].

2) استهداف محطات توليد الطاقة والماء

أصبح الاعتماد على الشبكات المعلومات وخصوصا في الدول المتقدمة، من الوسائل المهمة لإدارة نظم الطاقة الكهربائية،ويمكن لهجمات على مثل هذا النوع من الشبكات المعلومات أن تؤدي إلى نتائج خطيرة، ولاسيما في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية ولذلك فان شبكات المعلومات مرتبطة بشكل مباشر أو غير مباشر بطاقة الكهربائية وتعد من الأهداف الأولى التي قد يستهدفها الإرهاب الالكتروني.

ويشمل هذا السيناريو مباشرة سلسلة من الهجمات المعلوماتية التي تنهض بمهام تحكم بشبكات توزيع الطاقة الكهربائية الوطنية وينشأ على مثل هذه الهجمات تعطيل عدد

[1]–حسين شفيق، الإعلام الجديد والجريمة الالكترونية.التسريبات، التجسس الالكتروني، الإرهاب، المرجع السابق، ص201

من مرافق الحياة في البلاد، وسيادة الفوضى نتيجة انعدام مصادر الطاقة الكهربائية و شل الحركة في عموم البلاد، وكذا بنسبة لشبكات مصادر المياه و طرق توزيعها[1].

3) استهداف البنية التحتية الاقتصادية

أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال و الأعمال ،مما يجعل هذه الشبكات نظرا لطبيعتها المترابطة ، و انفتاحها على العالم ، هدفا مغريا للمجرمين و الإرهابيين و مما يزيد من الإغراء الأهداف الاقتصادية و المالية، كما أنها تتأثر بشكل ملموس بالانطباعات السائدة و التوقعات و التشكيك في صحة هذه المعلومات أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة ، و أضعاف الثقة في النظام الاقتصادي و يشمل هذا السيناريو إحداث خلل واسع في نظم الشبكات التي تتحكم بسريان أنشطة المصاريف و الأسواق المال العالمية ،و نشر الفوضى في الصفقات التجارية الدولية، فضلا عن ذلك يمكن إحداث توقف جزئي أو كلي في منظومات التجارة و الأعمال، إذ تتعطل الأنشطة الاقتصادية و تتوقف عن العمل.

4) استهداف نظم المواصلات

ويتضمن هذا السيناريو اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية و إحداث خلل في برامج هبوط الطائرات و إقلاعها، مما قد ينجم عنه حصول تصادم فيما بينهما أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلي مدرج المطار، كما يحتمل تمكن قراصنة المعلومات من السيطرة على النظم التحكم بتسيير القطارات، وتغيير مواعد الانطلاق فتسود الفوضى أو تتصادم هذه القطارات فيما بينها، وكذلك بالنسبة لسفن والناقلات والغواصات البحرية[2].

[1]– حسين شفيق، المرجع السابق، ص201.202

[2]– المرجع نفسه، ص202

5) استهداف نظم الاتصالات

ويشمل هذا السيناريو اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية وقد تمارس سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية الأمر الذي ينشر حالة من الرعب والفوضى وعدم القدرة على متابعة تداعيات الهجومات الإرهابية المعلوماتية، ومن أمثلة ذلك في العالم الغربي ما قام به أحد المجرمين من الدخول إلى سجلات المستشفيات وتلاعب بملفات المرضى بشكل أدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بنسبة لهم. كما أن رسالة واحدة تنشر مثلا بالبريد الالكتروني مفادها أن هناك دماء ملوثة في المستشفى كفيلة أن تحدث أثار مدمرة على الصعيد الاجتماعي [1].

الفرع الثاني: وسائل الإرهاب الالكتروني

أهم ما يميز الإرهاب الالكتروني عن غيره هو استخدامه لكل الوسائل التقنية الحديثة في تنفيذ مخططاته وتدويلها سواء فيما يتعلق بالتخطيط أو التمويل أو التبرير أو التنفيذ، وتكمن أهم وسائل الإرهاب الالكتروني في[2]:

أولا) البريد الالكتروني

تعد خدمة البريد الالكتروني من أهم وأخطر خدمات الاتصال وتبادل المعلومات السرية التي استفاد منها الإرهاب في تنفيذ العمليات ونشر الأفكار وجمع التبرعات المادية وأشارت الدراسات إلى أن هناك 3 مليار رسالة الكترونية يتم تبادلها يوميا، ومن أبرز الدوافع لاستخدام البريد الالكتروني كونه مجانا ولا يتطلب الحصول عليه سوى ادخال بعض البيانات الشخصية.

[1] – حسين شفيق، المرجع السابق، ص202،203

[2] –حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم السياسية، جامعة ديالي، عدد خاص، ص ص331،332

ثانيا) تصميم الموقع

حيث يمكن من خلال تصميم المواقع ومنتديات وغرف الدردشة خاصة أن تكون ساحة اللقاء التي يمكن أن تجمع عدة أشخاص وبوقت واحد لتبادل المعلومات وتجنيد الإرهابيين جدد والتدريب الالكتروني من خلال تعليم طرق تساعد على شن الهجمات إرهابية، حيث تستخدم بعض المنظمات الإرهابية ألاف المواقع لكي يضمنوا الانتشار الواسع لأفكارهم.

ثالثا) تدمير المواقع

من خلال عدد من الأفراد الذين يمتلكون المهارات المتقدمة في برامج الحاسوب والتي يمكن من عن طريقهم إرسال عدد كبير من الملفات إلى المواقع المراد تدميره بنفس الوقت مما يربك الموقع لعدم قدرته على استيعاب هذه الملفات والتي تؤدي بدورها إلى تدمير الموقع.

رابعا) أنظمة الهاكرز الاختراق

يوجد عدد من البرامج التي يستطيع الإرهاب من خلالها أن يتجسس عن طريق الملف الذي يعمل كمستقبل للمعلومات ،فمع ظهور عصر المعلومات الرقمي و الوسائل التقنية أصبحت حدود الدول مستباحة أمام الأقمار الاصطناعية و البث الفضائي ، ويمكن النفاذ إلى أي موقع من خلال اسم المستخدم و الرمز السري تخوله بان يكون الشخص الوحيد الذي يمكن أن يدخل إلي أجهزة الحواسيب ومن أشهر البرامج الهاكرز Web cracker4 و net buster و net bus hascporf و عملية الاختراق الالكتروني يمكن أن تتم من أي مكان في العالم دون الحاجة إلى تواجد القرصان في الدولة التي يتم اختراق موقعها .

خامسا) الهاتف المحمول

هذا النوع من الوسائل منتشر بشكل كبير حيث يمكن من خلاله تفجير السيارات المفخخة و العبوات اللاصقة والتي تم برمجتها مع أجهزة الهاتف المحمول.

الفرع الثالث: أهداف الإرهاب الالكتروني

يهدف الإرهاب الالكتروني إلى تحقيق جملة من الأهداف الغير المشروعة و تكمن في [1]:

. نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة

. الإخلال بنظام العام والأمن المعلوماتي وزعزعة الطمأنينة

. تعريض سلامة المجتمع وأمنه للخطر

. إلحاق الضرر بالبنى التحتية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات أو بأموال أو المنشئات العامة والخاصة

. تهديد السلطات العامة والمنظمات الدولية وابتزازها

الانتقام من الخصوم

. الدعاية والإعلام وجذب انتباه وإثارة الرأي العام

. جمع الأموال أو الاستيلاء عليها.

[1]–حسين شفيق، الإعلام الجديد والجريمة الالكترونية، التسريبات، التجسس الالكتروني، الإرهاب، المرجع السابق، ص ص190،191

المبحث الثاني: مخاطر الإرهاب الالكتروني وأثاره

لقد ازداد وجه الإرهاب قبحا عما كان عليه في الماضي نتيجة التطور الكبير الذي شهدته وسائل الإعلام والاتصال و كثرة مستخدمي الانترنت في العالم [1].

حيث دخل الإرهاب حقبة جديدة أسهمت في إعادة النظر في أشكاله الحالية ، فلم يعد يقتصر على نمطه التقليدي الذي يمكن استهدافه و لكنه بات عابر للحدود على نحو يصعب السيطرة عليه بغلق الحدود أو تأمينها، ولقد تغيرت خطط الإرهاب وأدواته وأساليبه المستخدمة ولاح في الأفق "شبح الإرهاب الالكتروني" [2]الذي أصبح هاجسا يهدد العالم بأسره فلم يعد هناك شيء يثير الذعر لدى أجهزة مكافحة الإرهاب في العالم أكثر من الرعب و الخوف منه،[3] نظرا لما يسببه من مخاطر و أثار وخيمة على الأفراد والدول والمؤسسات فهو يستهدف البنية التحتية المعلوماتية و القطاعات الحيوية في الدول ومن هنا سنحاول من خلال هذا المبحث التطرق إلى أهم مخاطر الإرهاب الالكتروني في (المطلب الأول) ودراسة أثار الإرهاب الالكتروني في (المطلب الثاني)

المطلب الأول: مخاطر الإرهاب الالكتروني

الإرهاب الالكتروني هو الأكثر تمثيلا وتجسيدا وتعبيرا عن العولمة ويشكل هذا النوع أحدث وأخطر أنواع الإرهاب فتكا على الأطراف الفاعلة من الدول[4]. ويعتبر هذا الإرهاب وليد إحداث 11 سبتمبر 2001 التي جاءت لتظهر للعالم الارتباط بين الإرهاب والانترنت والمخاطر الكبيرة له، و التي تتفاقم يوم بعد يوم والتقنية الحديثة غير قادرة على

---

[1]–سعود شرفات، الإرهاب الالكتروني رعب على الأبواب، متوفر على الموقع: https://hafryat.com، تاريخ النشر:2018/03/01، تاريخ التصفح:2020/09/02، الساعة: 10:27

[2]– عبد الستار عبد الرحمن، الإرهاب السيبراني خطر يهدد العالم، متوفر على الموقع:https://imctc.org/Arabic ، تاريخ النشر :2020/02/23، تاريخ التصفح:2020/09/02، الساعة:10:33

[3]– سعود شرفات، الإرهاب الالكتروني رعب على الأبواب، متوفر على الموقع:https://hafryat.com، تاريخ النشر:2018/03/01، تاريخ التصفح:2020/09/02، الساعة: 10:35

[4]– سعود شرفات، المرجع السابق

حماية الناس من الهجمات الإرهابية، وتزداد خطورة هذا الإرهاب على الدول المتقدمة التي تستخدم نظام الحكومة الالكترونية (الإدارة الالكترونية)ومن هنا أثارنا تقسيم هذا المطلب إلى 3 فروع محاولين التطرق إلى بعض أهم مخاطر الإرهاب الالكتروني حيث خصصنا الفرع الأول لمخاطر الإرهاب الالكتروني على الأفراد و الفرع الثاني لمخاطر الإرهاب الالكتروني على الدول و المؤسسات و الفرع الثالث مخاطر الإرهاب الالكتروني على التجارة الالكترونية

الفرع الأول: مخاطر الإرهاب الالكتروني على الأفراد

الإرهاب الالكتروني هو إرهاب الغد إرهاب المستقبل نظرا لتعدد أشكاله وتنوع أساليبه وكثرة مخاطره.[1]

فلا تقتصر مخاطره على الدول والمؤسسات فقط بل تمتد لتشكل خطرا وتهديدا لسلامة وامن وراحة الفرد،فبظهور الحاسبات الآلية تغير شكل الحياة في العالم و أصبح من أساسياتها في الألفية الجديدة و لكن هذا الاختراع العبقري تحول إلي لغم داخل كل بيت خاصة بعد استخدامه في الدخول إلى شبكة المعلومات الدولية " الانترنت" [2].

ومن هنا فان الحفاظ على خصوصية في الحياة كل شخص أضحى من المستحلات لوجود الإرهاب الالكتروني الذي يهدد هذه الخصوصية من خلال التجسس على البريد الالكتروني واختراق صفحات خاصة في مواقع التواصل الاجتماعي و بتالي ابتزاز الأفراد، كما انه من خلال الانترنت يقوم بنشر أفكار التطرف و العنف ويعزل الفرد عن البيئة الأسرية و الاجتماعية مما يؤدي إلى عيوب في الشخصية و بتالي يسهل استقطاب و تجنيدهم خاصة فئة الشباب وعدمي النضج و الوجدان ويهدم الأخلاق و

[1]–سعود شرفات، الإرهاب السيبراني خطر يهدد العالم، مرجع سابق

[2]– عبد الحميد إبراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي وجرائم المنظمة: ما هو رد فعل القطاع الخاص، دورة تدريبية مكافحة الجريمة الإرهابية المعلوماتية، كلية تدريب، قسم برامج التدريبية، 2006، ص27

القيم من خلال نشر وصناعة مواقع إباحية كما انه يوجه رسائل للجمهور و الإعلام بهدف ترويعهم و تخويفهم من خلال عرض أفلام مرعبة لرهائن و الأسرى أثناء إعدامهم.

أولا) التهديد والابتزاز المعلوماتي

يتمثل الإرهاب الالكتروني الموجه ضد الأفراد كل التصرفات التي يقوم بها من خلال وسائل التكنولوجيا (الانترنت، الهاتف، الفاكس...) مهما كان نوعها أو حجمها ضد الشخص الطبيعي، ومن بين أهم مخاطر الإرهاب الالكتروني على الأفراد نجد التهديد والابتزاز المعلوماتي، حيث شهدت شبكة الانترنت حالات للابتزاز المعلوماتي، من قبل أشخاص تمكنوا بوسيلة أو بأخرى من اختراق نظام الأمن للبريد الالكتروني أو التنصت أو التجسس على حلقات الدردشة عبر مواقع التواصل الاجتماعي[1]. وفي الغالب ما يستهدف هذا النوع من الإرهاب الشخصيات المعروفة سواء الحكومية أو العسكرية أو الفنية ... حيث تتيح الانترنت والتكنولوجيا وسائل مبتكرة للابتزاز نذكر منها:

انتحال الشخصية الأفراد من اجل الاستفادة من سمعتهم أو مالهم أو صلاحياتهم أو بهدف استدراجه ملل بوح بأسرارهم من خلال إنشاء حسابات مزورة من اجل التعارف ثم فضحهم واستغلالهم وتشويه سمعتهم ونشر المعلومات السرية والصور الشخصية عنهم بهدف المساس بكرامتهم وتهديدهم، ونذكر على سبيل المثال بعض حالات التهديد وابتزاز الأشخاص

. التهديد بالوثائق المزورة التي يتم تزويرها الكترونيا

. الولوج إلى أسرار المهنية (سير الأشخاص ...)

. نصب والاحتيال والتزوير بشتى الأشكال ...[2]

[1] علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، دار منشاة المعارف، الإسكندرية، مصر،2006، ص09

[2] – جعفر حسن جاسم الطائي، الإرهاب المعلوماتي واليات الحد منه، مجلة العلوم القانونية والسياسية، عدد خاص جامعة ديالي، ص499

ومن الأمثلة على الابتزاز الشخصيات المعروفة ما حدث في أمريكا حيث نفذ مخترقون "هاكرز" المعروفون باسم "ار ايفيل" تهديدهم لرئيس الأمريكي دونالد ترامب "بنشر غسيله القذر" من خلال تسريب 169 رسالة الكترونية تتحدث عن ترامب إذا لم يدفع فدية تقدر ب 42 مليون دولار وحسب تصريحاتهم تحصلوا على هذه المعلومات الخطيرة باختراق مكتب المحاماة شهير الذي يمثل العديد من الفنانين المشهورين أمثال ليدي قاقا ومادونا حيث قاموا بتسريب معلومات خطيرة عليهم. ولقد صنف مكتب التحقيقات الفدرالي (اف،بي، أي) أنها عمل إرهابي سيبراني أي الكتروني.[1]

ثانيا) المواقع الإباحية

يعتبر نشر المواقع الإباحية التي تهدم القيم والمبادئ جانب من جوانب خطورة الإرهاب الالكتروني على الأفراد[2]، حيث أصبح الانتشار الواسع لصور والأفلام الإباحية على شبكة الانترنت يشكل قضية ذات اهتمام عالمي في الوقت الراهن فحين تعد صناعة الإباحة جريمة في الكثير من دول العالم خاصة التي تستهدف أو تستخدم الأطفال[3].

وينتمي معظم منتجي هذه المواد إلى فئتين واسعتين هم المتربصون جنسيا بأطفال وكذلك مجموعات الإجرام المنظم التي تسعى إلى كسب أرباح طائلة من خلال الترويج لمثل هذه الصور، فهناك مواقع تحاول استدراج مرتاديها بتقديم خدمة إرسال الصور الجنسية مجانية يوميا على عناوينهم بريدية أو مواقع التواصل الاجتماعي الخاصة بهم

[1]–محمد عطايا، فوربس: الهاكرز يبدأون بنشر الجزء الأول لتسريبات ترامب و يطلبون فدية42 مليون دولار، متوفر على الموقع: https://www.masrawy.com، تاريخ النشر:2020/05/18، تاريخ التصفح:2020/09/02، الساعة:11:50

[2]–بن يحي الطاهر الناعوس، مكافحة الإرهاب الالكتروني ضرورة بشرية و فريضة شرعية، مكتبة الألوكة ،2015، ص08

[3]– علي جابر حسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية لنشر والتوزيع، د.ب.ن، 2018، ص77

فحين يقوم المتأثرين بهذه المواقع بدفع مبلغ محدد أو اشتراك شهري أو سنوي مقابل مشاهدة والاستفادة من خدمات هذه المواقع[1].

فلقد أتاحت شبكة الانترنت أفضل الوسائل لتوزيع هذه الصور الفاضحة و الأفلام الخليعة بكل علني فاضح يقتحم بيوت و مكاتب الأفراد، يجعل كل مستخدم الانترنت معرض لتأثر بها لكنه يشكل خطرا حقيقيا على الأطفال و مراهقين [2]، بحيث أوضحت دراسة (adist) أن إدمان المواقع الإباحية يؤدي إلي أثار مدمرة و نتائج وخيمة كارتفاع جرائم الاغتصاب بصفة عامة و اغتصاب الأطفال بصفة خاصة و العنف الجنسي و فقد العائلة لقيمتها و مبادئها و احتقار النساء بدل احترامهن[3]

ثالثا) استقطاب وتجنيد الشباب

يعد تجنيد الأفراد عامة و الشباب خاصة من بين اكبر مخاطر الإرهاب الالكتروني ، و تتمثل عملية التجنيد في جمع حشد من الأشخاص و استقطابهم و استخدامهم قسرا أو طواعية بغرض الانضمام و الالتحاق بالجماعات الإرهابية مهما كان غرضها عن طريق إعدادهم ماديا و معنويا لخدمة هذه الجماعات محلية كانت أو دولية [4]، أما عملية تجنيد الشباب فهي تتم عن طريق أساليب قهرية قسرية لإقناع وذلك بإتباع مراحل و شروط لاقتناص الشباب ليجد نفسه عضوا في الجماعات الإرهابية .

ولقد أدى انتقال الإرهاب من بيئة مادية طبيعية إلى بيئة افتراضية في انتشاره بسرعة الضوء في كامل بقاع العالم فأصبح من الصعب القضاء عليه كما تحولت شبكة الانترنت إلى أداة فعالة حيث أصبحت تغني عن معسكرات التدريب[5]، كما تحول العالم

---

[1]–عبد الصبور عبد القوي على مصري، منال عبد اللاه عبد الرحمن، محكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، مكتبة القانون واقتصاد، الرياض، 2012، ص67

[2]–المرجع نفسه، ص68

[3]– عبد الصبور عبد القوي على مصري ، المرجع السابق، ص69

[4]– ايمان بن سالم، المرجع السابق، ص22

[5]– المرجع نفسه، ص ص 23،24

الرقمي إلى مسرحا أمنا لدعة التطرف والعنصرية وأداة تخدم أفكارهم الضالة بإضافة الى فعاليتهم في تجنيد الشباب وتوسيع رقعة التطرف فاتخذوا شبكة الانترنت معبرا لبث ونشر أفكارهم المتطرفة سواء كانت سياسية أو دينية أو عنصرية[1].

حيث تعتبر شبكة الانترنت سلاحا تعتمد عليه الجماعات الإرهابية في تجنيد الشباب عن طريق

. المواقع التواصل الاجتماعي: الفيسبوك وتويتر ومنتديات وغرف الدردشة

. رسائل الدعاية والإعلام

. الألعاب الالكترونية[2].

الفرع الثاني: مخاطر الإرهاب الالكتروني على المؤسسات والدول

منذ بداية الألفية الثانية لم يعد هناك شيء يثير الذعر لدى الأجهزة الأمنية و الاستخبارية و أجهزة مكافحة الإرهاب في العالم أكثر من الذعر و الرعب من الإرهاب الالكتروني [3]، الذي لا تقتصر أثاره الكارثية فقط على خسائر في الأرواح بل امتد إلي خسائر الاقتصادية و اجتماعية و سياسية و ثقافية بغض النظر عن إذا كانت الدولة صغيرة أو كبيرة، قوية أو ضعيفة

ونتيجة اعتماد الإرهاب الالكتروني على الإمكانيات العلمية والتقنية واستغلال وسائل الاتصال وشبكات المعلوماتية فهو يشكل بذلك مخاطر كبيرة على الدول ومؤسساتها.

أولا:مخاطر الإرهاب الالكتروني على المؤسسات

يعد الإرهاب الالكتروني من أكبر المخاطر التي تهدد المؤسسات من خلال اختراق شبكات اتصالاتها والنفاذ إلى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها المختلفة،وفي ظل المنافسة التي تشهدها معظم الأسواق الحالية أصبح التجسس

---

[1]– ايمان بن سالم، المرجع السابق، ص26

[2]– المرجع نفسه، ص27.28.29.30

[3]– سعود شرفات، الإرهاب الالكتروني خطر على الأبواب، مرجع سابق، موقع:https://hafryat.com ، الساعة: 14:26

على مختلف أنشطة الشركات مصدر قلق حقيقي[1]، وقد تم اختراق شبكة المعلومات لبعض البنوك السودانية في إطار حملة شنت ضد السودان ضمن ما سمي بتمويل العمليات الإرهابية.

ومن بين مظاهر الخطر الأخرى للإرهاب على المؤسسات إسقاط موقع المؤسسة على الانترنت وذلك بان يصوب عليه العديد من الرسائل المولدة تلقائيا التي تظل تنهمر إلى أن تصل إلى حد يعجز الموقع تماما عن ملاحقتها ليسقط وبتالي تسقط معه جميع المعاملات التجارية والمالية الالكترونية التي يوفرها موقع المؤسسة لعملائه وشريكاته

ومن الرسائل الأخرى التي تتعرض لها المؤسسات فك شيفرة الحماية السرية للبيانات التي تتبادلها مع الآخرين خارج المؤسسة من عملاء ووكلاء وما شابه، وقد سبق أن عرف العالم تهديد حيث قام شاب من النرويج بنشر برنامج في عدة أسطر يمكن به فك الشيفرة الرقمية التي تبث بها أفلام عبر الشبكة وهو دليل الإرهاب في السطو على المؤسسات وهو التهديد نفسه الذي تواجهه حماية الملكية الفكرية[2].

ثالثا: مخاطر الإرهاب الالكتروني على الدول

ان الإرهاب الالكتروني نشاط أو هجوم متعمد يمتلك دوافع سياسية تسعى لتأثير على الدولة والرأي العام العالمي ويستخدم الفضاء الالكتروني بوصفه عاملا مساعدا ووسيطا في تنفيذ العمل الإرهابي.[3]

ولقد ظهر الارتباط بين الانترنت والإرهاب بشكل واضح في الآونة الآخرة وانتقلت المواجهة ضد الإرهاب والإرهابيين من مواجهة مادية مباشرة إلى مواجهة الكترونية وتحولت الحروب الوقعة إلى حروب رقمية وأصبحت الانترنت من اشد الأسلحة فتكا

---

[1]–علاء صراط الغامدي، المرجع السابق، ص15

[2]–جعفر حسن جاسم الطائي، مرجع السابق، ص500

[3]–نور بنداري عبد الحميد فايد، دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية، دراسة حالة "داعش"، متوفر على الموقع، https://democraticac.، تاريخ النشر 2016/07/19، تاريخ التصفح: 2020/09/06، الساعة: 21:21

وهدما إذ ما استخدمت الأغراض سيئة وتحقيق نوايا إرهابية [1] وتتمثل خطورة جرائم الإرهاب الإلكتروني على الدول فيما يمكن أن يترتب عليها من أضرار جسيمة وخسائر مالية ضخمة كتعطيل عمليات التحويل المالي.

أو الدخول إلى شبكات التحكم في المرافق العامة مما يتسبب في شلل البنى التحتية الأساسية، بل واحتمال تدميرها كليا[2] إذ أصبحت الدول معرضة لما يسمى بالدمار الشامل بسبب استخدام الأسلحة البيولوجية المعلوماتية متمثلة في جيوش الفيروسات التي تكثر في حدود الدول وتحطم البنية المعلوماتية [3]يتميز الإرهاب عن غيره بالاعتماد على الموارد المعلوماتية والأسلحة الالكترونية في تنفيذ عماليته، ومن أبرز وهذه الأسلحة القنابل الالكترونية مثل

. تعطيل الاتصالات والتشويش عليها والتنصت على المكالمات وبث معلومات مضللة وتقليد الأصوات خاصة أصوات القادة العسكريين الإصدار أوامر خطيرة . استهداف شبكات الحاسوب بالتخريب عن طريق نشر الفيروسات . مسح الذاكرة الخاصة بأجهزة المعادية . منع تدفق الأموال وتغيير مسار الودائع ...الخ [4]

ومن بين المخاطر الأخرى المرعبة للإرهاب الالكتروني التي تهدد البشرية حسب (باري كولين)

. الوصول عن بعد إلى أنظمة التحكم بمصانع الحبوب وتغير مستويات مكملات الحديد للإضرار بصحة المستهلكين

. إجراء تعديلات عن بعد في معالج حليب الأطفال الرضع للإضرار بهم

---

[1]–Mann, David & Sutton, Mike, Net crime, Brit. J. criminal, vol 38,No 2 ,spring 1998,p220

[2]– هشام محمد رستم، الإرهاب الدولي، دار النهضة العربية، القاهرة، مصر، 2003، ص106

[3]–جعفر حسن جاسم الطائي، المرجع السابق، ص500

[4]–عبد الستار عبد الرحمن، الإرهاب السيبراني خطر يهدد العالم، متوفر على موقع:https://imctc.org/Arabic/Article، تاريخ النشر:2020/02/23، تاريخ التصفح:2020/09/06، الساعة:21:57

. تعطيل المصارف والمعاملات المالية الدولية والبورصات لإفقاد الثقة في النظام

. تغير مكونات صناعة الأدوية عن بعد لدى شركات الأدوية

. تغيير الضغط في خطوط الغز واحمال شبكة الكهرباء مما يوقع انفجارات والحرائق المروعة

. مهاجمة أنظمة التحكم في الحركة الجوية وجعل الطائرتين مدنيتين تتصادمان عن طريق الولوج إلي أجهزة استشعار في قمرة القيادة الطائرة وهذا ممكن في خطوط السكك الحديدية أيضا [1]

إن الإرهاب يشكل هاجسا حقيقيا وتهديدا لكل الدول فهو يهدد أمنها وسياستها واقتصادها ... فلقد شهد العالم بأسره بروز الإرهاب الالكتروني على ارض الواقع لأول مرة سنة 2000م حينما أدى فيروس "I Love you " إلى إتلاف معلومات تقدر ب 10 مليارات دولار أمريكي، كما شهد أيضا كيف تم تحويل الطائرات المدنية في تفجير برجي التجارة العالميين في أمريكا فيما عرف بهجمات 11 سبتمبر 2001 حيث تمكن الإرهابيين من استغلال التكنولوجيا المعلومات المتطورة في التخطيط و التنفيذ هذه العملية التي تشكل اكبر اختراق معلوماتي أسفر عن سقوط آلاف الضحايا في تاريخ الولايات المتحدة ، الأمر الذي أدي ب 30 دولة إلى توقيع اتفاقية مكافحة الإجرام المعلوماتي في العاصمة المجرية بودابست من نفس العام ، بينما ففي عام 2003 أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسوب و قدر مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الانترنت كلفة إصلاح الإضرار التي سببتها فيروسات المعلوماتية نحو 12مليار دولار.[2]

[1]–عبد الستار عبد الرحمن، المرجع السابق

[2]–ايمن حسن، الإرهاب الالكتروني أخطر معارك حروب الفضاء، متوفر على الموقع: http://alwatan.com ، تاريخ النشر:2017/01/14، تاريخ التصفح:2020/09/06، الساعة: 21:59

الفرع الثالث: مخاطر الإرهاب الالكتروني على التجارة الالكترونية

يعتبر الإرهاب الالكتروني وليد الاستخدامات الضارة التكنولوجيا المتطورة والانترنت حيث تعتمد الجماعات الإرهابية في ممارسة أعمالها التخريبية على الفضاء الالكتروني الذي أصبح بيئة مناسبة لها، حيث نجد انه من مميزات الإرهاب الالكتروني انه مقر امن وصعب الإثبات وقليل التكلفة فهو لا يحتاج إلى أكثر من جهاز حاسوب متصل بشبكة الانترنت كما انه يدعى بجريمة الناعمة نظرا إلى انه لا يحتاج إلى العنف، فيقوم الإرهابي وهو في قمة الراحة في منزله أو مقهى ...

وأساسا تكمن خطورته في سهولة استخدامه مع شدة أثره وضرره فهو يشكل خطر على كل القطاعات الحيوية في الدول وكل الجوانب سوء الاقتصادية أو السياسية أو الأمنية ... وما يهمنا نحن مخاطر هذا الإرهاب على التجارة الالكترونية.

أولا) المخاطر الأمنية للإرهاب الالكتروني على التجارة الالكترونية

تتفاقم يوما بعد يوم مخاطر الإرهاب الالكتروني نظرا لاستعماله لتكنولوجيات الحالية بإضافة إلى الثغرات الأمنية المتعددة في التعاملات التجارية الالكترونية وتتجلى أهم هذه المخاطر في

أ) القرصنة أو تعطيل نظام المعلومات

تعتبر الفيروسات وسيلة هجوم شائعة لإتلاف معطيات التعاملات التجارية من قبل الإرهابيين ولكن هناك عدة مخاطر للقرصنة أو تعطيل نظام المعلومات تتبين فيما يلي:

1) خرق الحماية المادية:ويتم ذلك عن طريق

. التفتيش في المخلفات التقنية: ويقصد بها بحث الإرهابيين في مخلفات المؤسسة عن شيء يساعدهم في الاختراق نظام المعلوماتي للمؤسسات التجارية والمالية مثل أوراق مكتوب عليها كلمة السر أو مخرجات الكمبيوتر أو أقراص الصلبة المرمية بعد استعمالها أو ما شابه ذلك

. الالتقاط السلكي: هو توصيل السلك المادي مع شبكة توصيلات النظام لجهة استراق السمع بطريقة سهلة أو معقدة تبعا لنوع الشبكة أو طرق التواصل المادي.[1]

2) خرق الحماية المتعلقة بأشخاص وشؤون الموظفون: وذلك

. التخفي بانتحال شخصية موظف: وهو استخدام الإرهابي لوسائل التعريف العائدة للموظف المخول له هذا الاستخدام كاستغلال أحد الإرهابيين لكلمة سر أحد العمال، واستغلال صلاحيات مخولة للموظف من خلال اقتناص شخصيته ...[2]

. البرمجيات الخبيثة: ويقصد بها الفيروسات كفيروس حصان الطروادة (trojanhorses) أو القنابل المنطقية (logic bombe) تقوم هذه الهجمات بتدمير المواقع الالكترونية لشركات التجارية مخلفة خسائر بملايين مثل ما فعل فيروس "الشيفرة الحمراء" الذي الحق أكبر الخسائر في بيئة الكمبيوتر والانترنت مقارنة بغيره من الأعمال الإرهابية[3].

ب)استغلال الشبكات الاجتماعية المعلوماتية

لا تكمن المخاطر الحقيقية للانترنت بشكل عام الإرهاب الالكتروني بشكل خاص فيما هو ظاهر كالتجسس، الفيروسات، مواقع السرقة الملكية الفكرية، نشر مواقع الإباحية، مواقع الترويج للإرهاب ومواقع العنف وانتحار وإدمان الألعاب الالكترونية ومخاطر الصحية...

بل فيما هو كامن وخفي مثل ما تؤديه شبكات الاجتماعية ويجهله معظمنا ونلخص هذه المخاطر فيما يلي:

---

[1]– نجاري بن حاج علي فايزة، المرجع السابق، ص43

[2]– سعاد إكرام عوض، التزوير المعلوماتي، دراسة نقدية لمختلف القوانين الوضعية، منشاة المعارف، الإسكندرية، 2008، ص146

[3]– المرجع نفسه، ص147

1) مخاطر الشبكة الاجتماعية الفيسبوك (Facebook)

إن ظهور وانتشار شبكة الفيسبوك، جعل الحياة لا خصوصية لها فقد عمل الفيسبوك على البحث في بيانات المستخدمين ورسائلهم وتعليقاتهم وحتى محادثات الخصة بين الأفراد، ويعتبر اكبر موقع التواصل الاجتماعي من حيث المسجلين فيه بقاعدة بيانات تضم 90 مليون مستخدم وعليه فان معظم الشركات التجارية العالمية ليس بمعزل عنه ما يجعل تعاملاتها الاقتصادية وصفقاتها التجارية معرضة لتجسس وكذا تشويه سمعتها بنشر معلومات أو صور كان يقوم شخص بفتح حساب باسم احد مدراء الشركة و تشويه سمعته يسبب عدة مشاكل لا حصر لها [1].

2) مخاطر محرك غوغل(Google)

يعتبر أهم محرك بحث في العالم إذ يحتوي على المليارات المعلومات التي يتم تحميلها أو تغييرها من ثانية إلى أخرى وكذا سرعة تقديم الأجوبة والمعلومة ناهيك عن عدد الصفحات اللامتناهية جعلت منه أهم وسيلة لبث أفكار الإرهابيين واستفادة من الشروحات صنع المتفجرات وكيفية قرصنة المواقع والحصول على كلمات السر وغيرها من الموضوعات الموجودة فيه ولقد تلقت شركة (Google) العديد من الشكاوى على انتهاك خصوصية الأفراد من خلال ما يتم نشره من أمور غير قانونية وذلك لعدم وجود رقابة كافية.[2]

3) مخاطر خدمة الفيديو (you tube)

لقد استغل المجرمين والإرهابيين هذه الخدمة من اجل عرض مختلف جرائمهم من اجل نشر الرعب والخوف بين الأفراد من خلال عرض جرائم القتل، وكذا مهاراتهم في

[1]– فايز الشهري، الطرح الفكري على شبكة الانترنت المراحل والرموز، د. د. ن، مصر، د ب ن، ص96

[2]– B–HOFMAN, THE USE of the internet by Islamic Extremists testemony the house of permanent، may 2006، p102.

تحويل رؤوس الأموال من بنوك عالمية لحساباتهم الخاصة دون رصدهم وتصوير اعترافاتهم بوجوه غير مكشوفة.[1]

ج) تأثير التجسس على التجارة الالكترونية

تسعى الجماعات الإرهابية من خلال التجسس على المعلومات الصناعية والمالية والتجارية إلى ضرب مواقع القوى الاقتصادية لدولة ما والضغط عليها من خلال ابتزازها بطلب فدية أو إطلاق سراح الرهائن[2]

كما تعتبر الشبكة العنكبوتية سوق مفتوح لجميع الدول تتم من خلالها التعاملات بمبالغ ضخمة تصل إلى مليارات الدولارات مما يجعل جانب الاقتصادي للأنترنت الأكثر خطورة، لان الهدف الأساسي للإرهاب هو المال والثاني أن الهجمات الموجودة ضد نظم المعلومات الاقتصادية لها تأثير كبير على الرأي العام [3]

ثانيا) المخاطر التجارية للإرهاب الالكتروني

إعمال الإرهاب الالكتروني لا تنحصر فقط في كل ما هو تهديد أمنى بل تتعدى ذلك لتصل إلى التهديدات تجارية تزعزع النظام الاقتصاد والتجارة الالكترونية الدوليين وهذه النشطة تتمثل في:

أ) موقع الشبكة المعلوماتية في المعاملات التجارية

إن الإرهاب الجديد أصبح أكثر خطورة لاعتماده على التكنولوجيا التي ساعدته في التحكم الكامل باتصالات الأفراد، مما زاد اتساع سرعة عملياتهم و بالتالي أصبح من الصعب مكافحة هذا الإرهاب الجديد ،غير انه تبقى الوظيفة الرئيسية لتجسس على

1- Raul ATAYLOR. Maestros ormisogvnistis? Gender and the social construction of haking, y- vonne tweaks, Williampubliching, 2003, p140.

[2]– حكيم غريب، مكافحة الاشكال الجديدة للإرهاب الدولي، رسالة دكتورة، كلية العلوم السياسية و العلاقات الدولية، جامعة الجزائر 03 ، الجزائر ،2014، ص840

[3]–سهيلة خليل غازي، معوقات التجارة الرقمية في الدول العربية، دار الوفاء لنشر، القاهرة، مصر، 2003، ص106

التعاملات الاقتصادية منع التبادلات التجارية عن طريق وسائل التكنولوجيا ،تحويل رؤوس الأموال ،التجسس على المحادثات عبر الهاتف و الانترنت، التطلع على الوثائق الرسمية، مهاجمة المراكز الرئيسية الاقتصادية بتخريب الحواسب أو نظم الاتصال أو قاعدة البيانات كل هذه التصرفات تمس بصفة مباشرة بالتجارة الالكترونية [1].

وهذه الأخيرة جعلت من العالم قرية صغيرة، وفرت الوقت وجهد وخلقت علاقات اقتصادية بين مختلف دول العالم، كما أن التجارة الالكترونية أحد أهم الوسائل التي تحاول النهضة باقتصاد العالمي على عكس الإرهاب الالكتروني الذي يقوم بالعكس تماما.

ب) اختراق الإرهاب الالكتروني لموقع التجارة الالكترونية

إن التهديدات التي تواجه التجارة الالكترونية في تزايد مستمر كلما تطورت التكنولوجيا نذكر منها:

1) انتهاك نظام الحماية السرية لتجارة الالكترونية

يقوم الإرهاب الالكتروني بالوصول إلى المعلومات المالية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، ذلك راجع لتطور الهائل لجهاز الحاسوب، وخصوصية مرتكبو الجريمة المعلوماتية فهي ترتكب بواسطة خبراء كمبيوتر وليس أشخاص عاديين [2]

2) إتلاف مواقع التجارة الالكترونية باستخدام الفيروسات

بما أن التجارة الالكترونية تعتمد في تصرفاتها على نظام الحاسب الآلي المتصل بالشبكات المعلومات كأحد الآليات التي يتم من خلالها ممارسة مختلف النشاطات التجارية والالكترونية، فان الفيروس المعلوماتي الذي ينشط هو الأخر على نفس مستوى

[1]– حكيم غريب، المرجع السابق، ص860

[2]– علاء صراط الغامدي، الحرب النفسية للارهاب الجديد، المرجع السابق، ص50

التجارة الالكترونية، يتميز بخاصيتين في غاية الخطورة أولها الانتقال والانتشار والثانية التدمير.

تما بخصوص انتقال و انتشار الفيروس، فهو ينتقل من جهاز إلى أخر بسرعة يساعده في ذلك وجود وسائل اتصال حديثة، أما بخصوص اثر الفيروس في التدمير فانه يرتبط ببرنامج معين يدخل إليه المستخدم وبعد تاريخ و ساعة معينة يبدأ الفيروس في التدمير الذي يشمل مسح البيانات المخزنة، ومن أعراض الإصابة بالفيروس بطئ نظام التشغيل ,ضيق سعة التخزينية كما يؤدي إلي تشويش المعلومات وكذا ادخلا معلومات غير صحيحة [1].

ج) بطاقات الدفع الالكترونية (بطاقة الائتمان)

بموجب بطاقات الدفع يمكن لحاملها بسحب مبالغ نقدية من المكينات سحب النقود الخاصة بالبنوك أو أن يقدمها كأداة وفاء لسلع والخدمات لشركات والتجار وتصدر البطاقة في حدود ثمن مالي معين لا يجوز تجاوزه وهذه البطاقات منها ما هو محلي لا يتجوز استعماله حدود الدولة التي تصدر فيها ومنها ما هو عالمي يستخدم في كل دول العالم، وهناك بطاقة ذهبية التي تمنح صاحبها سقفا انتمائيا عاليا، وأطراف العملية المصرفية تتم عن طريق هذه البطاقات هم بنك العميل حامل البطاقة، وكذلك حامل البطاقة والتاجر وبنك التاجر [2]

وتتمثل الاستعمالات الغير القانونية لهذه البطاقة:

. إساءة استعمال بطاقات الدفع الالكتروني من حامل البطاقة، كتقديم مستندات مزورة للحصول على بطاقة ائتمان أو كاستعمال البطاقة بعد نهاية مدة صلاحيتها او استعمالها رغم الغاء البنك لها.

[1]–نجاري بن حاج علي فايزة، المرجع السابق، ص54

[2]– محمد سليمان احمد، أساسيات الاستثمار الالكتروني تحليل الأعراف المالية، ط2، منشاة المعارف، الإسكندرية، مصر، 2005، ص76

. إساءة استعمال البطاقة من طرف الغير كسرقة البطاقة واستعمالها أو سرقة الرقم السري الخاص بصاحب البطاقة واستخدامه.

. تلاعب التاجر في بطاقات الوفاء كاستعماله بطاقات ليس لها أرصدة كافية للصرف أو قبول بطاقات مزورة من العملاء

. تلاعب موظفي البنك المصدر للطاقة بالاتفاق مع حامل البطاقة أو التاجر أو مع غيرهما كالسماح بتجاوز حد البطاقة في السحب أو تجاوز مدة الصلاحية.

. التلاعب في بطاقات الائتمان عن طريق شبكة الانترنت باختراق لخطوط الاتصالات العالمية أو الحصول على الأرقام السرية والمعلومات عن المواقع أو إنشاء مواقع وهمية على أنها مواقع أصلية ويتلقى طلبات المعاملات الخاصة بالتجارة الإلكترونية يتم الحصول على المعلومات المتضمنة فيها

. اختراق أرقام البطاقات عن طريق استعمال معدلات رياضية وإحصائية بهدف تحصيل أرقام الطاقات الائتمانية المملوكة للغير واستعمالها في المعاملات غير مشروعة.[1]

المطلب الثاني: آثار الإرهاب الالكتروني

الإرهاب ظاهرة تقشعر لها الأبدان حوت بين جنباتها الكثير والكثير من الآلام والأوجاع لدرجة استقطبت اهتمام الشعوب والحكومات في كل دول العالم. وأصبح يمثل بجميع أشكاله تهديدا وخطرا لسلام والأمن الدوليين نظرا لما له من أثار وخيمة على امن المواطنين واستقرارهم وعلى الإمكانيات الاقتصادية والهيبة السياسية للدولة في محيطها الإقليمي والدولي[2]. ومن خلال هذا المطلب سنسلط الضوء على أهم الآثار للإرهاب

[1]– محمد فاتح محمود المغربي، التجارة الالكترونية، ط1، دار الجنان لنشر والتوزيع، عمان، الأردن، 2016

[2]– حسن بن سعيد بن سيف الغافري، الإرهاب الالكتروني الخطر قادم، متوفر على موقع:http://althawrah.ye/archives/72153، تاريخ النشر:2014/02/14، تاريخ التصفح:2020/09/02، الساعة18:34

الالكتروني حيث سنتناول في (الفرع الأول) أثار الإرهاب الالكتروني على الآمن والسلم وفي (الفرع الثاني) أثار الإرهاب الالكتروني على العلاقات الدولية وفي (الفرع الثالث) أثار الأخرى للإرهاب الالكتروني.

الفرع الأول: آثار الإرهاب الالكتروني على الأمن وسلم

تعد الآثار دائما نتائج لأسباب معينة، وأيضا تدل عليها بمعنى أن النتيجة هي مجموعة من الأسباب التي تفاعلت وأفرزت هذه النتيجة، ولذى من خلال النتائج يمكن الوصول إلى الآثار، وتحديد مفهوم الآثار له أهمية لبيان خطورة الموضوع محل الدراسة وأبعادها على الحياة الإنسانية في جميع جوانبها وتأثيرها على القواعد التي تنظم حياة المجتمعات على المستوى الدولي، ولا يخفى على احد خطورة الجرائم الإرهابية الالكترونية التي بلغت من القسوى و الفظاعة حدا لا يطاق حتى أصبحت الجرائم العادية أمامها أهون وارحم[1].

وان الإرهاب الالكتروني ذو طابع دولي، وهو بذلك يشكل تهديدا على امن الدول ومنشأتها المختلفة و عليه فهو امتداد للجريمة العابرة للقارات، حيث تبنت الجرائم الإرهابية عبر الوسائل الالكترونية في الآونة الأخيرة أشكالا ذات أثار ضارة على العلاقات الدولية وأصبحت تهدد الأمن و السلم الدوليين، و يتصور حدوث هذا إذا قامت شبهات اتجاه دولة ما بأنها قامت بإيواء و تجنيد الإرهابيين عبر الوسائل الالكترونية وتحريضهم ضد الدول عبر هذه الوسائل، فان العلاقة بينها و بين الدولة المتضررة من الإرهاب تتأثر سلبا، وتتوقف أو ربما تمتد إلى المقاطعة[2].

ومن الأمثلة التطبيقية التي قامت بها داعش والقاعدة من استغلال الوسائل الالكترونية للأعمال إرهابية أدت إلى توتر العلاقات الدولية وتهديد الأمن والسلم الدوليين،

[1]– عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة، أطروحة دكتورة، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2012، ص98

[2]– المرجع نفسه، ص110.111

العمل الذي قام به موقع "ويكيليكس" "والذي يعرف الصراع الالكتروني ذو طبيعة ناعمة". وذلك أدى إلى الصراع الدولي الالكتروني للحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية من خلال تسريب المعلومات والأسرار واستخدامها عبر منصات إعلامية بما يؤثر على العلاقات الدولة، فان هذا الصراع من شانه أن يهدد السلم العالمي باعتباره حربا الكترونية بين الدول مما يحدث خلل بنظام الأمن والسلم الدوليين[1].

حيث خلفت العمليات الالكترونية أثار كبيرة في بنية المجتمعات دول العالم، و استطاعت هذه العمليات تقسيم الدول مذهبيا و طائفيا عرقيا، وذلك من اجل تحقيق هدف هذه الظاهرة المتمثلة بضرب المؤسسات و الأفراد لنيل من الأمن و السلم الدوليين، حيث أخذت الدول على عاتقها القيام بما هو ممكن من اجل تحقيق السلام والاستقرار داخل دولها من خلال الدعوة إلى ضرورة مواجهة الإرهاب الالكتروني الذي اخذ يضرب دولا مختلفة مخلفا أثار وتهديدات وتداعيات تمس الأمن و السلم الدوليين، ومما يستدعي ضرورة العمل على تنسيق الجهود المشتركة من اجل مكافحة الإرهاب الالكتروني، من خلال قاعدة معلومات و برامج عمل مشتركة للقضاء عليه عبر محاربة الفكر المتطرف الذي اخذ ينتشر، والعمل على تحقيق اكبر قدر ممكن من التعاون الدولي لحصر هذه الظاهرة و الحد من انتشارها ، ومن ثم إعادة نشر السلام و المحافظة على الأمن و السلم الدوليين و الاستقرار في المجتمع الدولي [2].

الفرع الثاني: آثار الإرهاب الالكتروني على العلاقات الدولية

إن من آثار الإرهاب الإلكتروني التأثير على مستوى العلاقات الدبلوماسية الدولية من خلال جمع المعلومات والتنصت والتجسس وتسهيل النشاطات السرية في العلاقات

[1]–عمر عباس خضير العبيدي، الإرهاب الالكتروني في نطاق القانون الدولي، رسالة ماجستير في القانون العام ، كلية الحقوق، جامعة تكريت، العراق، 2019، ص92

[2]– أيمن عبد الكريم حسين، الإرهاب ودوافعه وتداعياته على الأمن والسلم الدوليين مركز البيان لدراسات والتخطيط، بغداد،2018، ص05

الدولية، مثل عميلة الاغتيالات، وتزايدت العلاقة بين التكنولوجيا والأمن وأصبح لا يعترف بالحدود الإقليمية أو العالمية ولقد أدت ظاهرة الإرهاب الإلكتروني إلى تحول جزء من العالم من الطابع المادي إلى عالم رقمي إلكتروني، حيث أصبح الفضاء الإلكتروني مجالا جديدا للتفاعلات الدولية سواء أكانت تفاعلات صراعية أم تعاونية، مما أثر على الغير طبيعة القوة وبروز تهديدات الفضاء الإلكتروني، وأثر بدوره على استراتيجيات الأمن القومي للدول ، والسعي إلى الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني لمنع تعرض بنيتها التحتية والحيوية للخطر، ومنثم دخول المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيت طبيعتها وأنماط استخدامها وطبيعة الفاعلين

وقد أحدث الفضاء الإلكتروني آثارا وتغيرات في طبيعة القوة وعناصرها وأنماط استخدامها، وتتميز القوة الإلكترونية بالتحرك في مسارات متداخلة، وتعمل على نقل عملية التأثير من وإلى الفضاء الإلكتروني، إذ يتمثل المسار الأول في انتقال الأحداث من أرض الواقع إلى الفضاء الإلكتروني أما لتصفية الصراعات وأما لاستخدامه لبت العنف والتحريض والكراهية، ويتمثل المسار الثاني في انتقال عناصر التهديد من الفضاء الإلكتروني إلى أرض الواقع عن طريق تأثير ما يتم نشره من معلومات وشائعات وغيره على المجتمع ، ويتمثل المسار الثالث في استخدام الفضاء الإلكتروني كوسيلة إعلام تنقل كل ما يحدث داخلية وعالمية، مما يؤدي إلى ردود أفعال عالمية مؤيدة ومعارضة،[1] وكذلك التأثير على العلاقات الدولية من حيث وقوع هذه الجرائم من دولة إلى الدولة أخرى وتعريضها للخطر نتيجة حدوث العمل الإرهابي في إقليمها، وتأثيره على مصالح دول أخرى كوقوعه على أعضاء السلك الدبلوماسي أو على وسائل نقل أجنبية أو على رعايا عدة دول[2].

[1]–نوران شفيق، آثر التهديدات الالكترونية على العلاقات الدولية، مكتب العربي للمعارف، القاهرة، 2015، ص1080

[2]–عادل عبد الصادق، الإرهاب قوة في العلاقات الدولية نمط جديد وتحديات مختلفة، ط1، المرجع السابق، ص44

ومن الأمثلة التطبيقية للآثار على العلاقات الدولية ومنها في جولية عام (2010)، أفاد مكتب الإدارة الشخصية التابع للحكومة الأمريكية أن قراصنة تمكنوا من سرقة بيانات قرابة أربعة ملايين موظف فيدرالي، إذ اتهم مسؤولون أمريكيون حكومة الصين بالوقوف خلف هذه العملية التي تعد الفاجعة الأكبر في تاريخ البلاد، وعد الخبراء أن الهدف من هذه العملية هو تحسين مستوى الصين لقدراتها على تجنيد جواسيس نظرا لأهمية المعلومات المسروقة التي تمكنهم من الوصول إلى أسرار أمن الدولة [1].

الفرع الثالث:الآثار الأخرى للإرهاب الالكتروني

يعد الإرهاب الإلكتروني من أهم وأحدث الجرائم التي فرضت نفسها على المشرع الدولي والتي تستدعي مواجهتها بتشريعات دقيقة لا تسمح لمرتكبيها بالإفلات من العقاب، وتتجلى أهمية تجريم هذا النمط من السلوك المنحرف فيما تسببت به الجريمة الإرهابية الإلكترونية من آثار اقتصادية واجتماعية وسياسية، ومن آثار الإرهاب الإلكتروني التهديد في أمن واستقرار الدول[2].

تظهر آثار خطورة الإرهاب الإلكتروني في جميع المجالات السياسية والاقتصادية والاجتماعية والأمنية والنفسية ، فمن الناحية الأمنية والنفسية يفضي إلى عدم الشعور بالأمن والطمأنينة ليحل بدلها الخوف والقلق وفقدان الثقة وهو ما يؤدي إلى تفشي الأمراض النفسية من جراء هذه الجرائم ، ومن آثار الإرهاب الإلكتروني على الناحية السياسية فأنه يهدد الوحدة الدولية بالتفكك فضلا عن النيل من سمعة الدول وهيبتها أمام الرأي العام الدولي ويضعف أو ينعدم ثقلها السياسي إلى غير ذلك من التأثيرات ، وعن الآثار الاقتصادية فان العمليات الإرهابية تؤثر على التنمية الاقتصادية للدولة نتيجة لشلل الذي يصيب عجلة الإنتاج فضلا عن تحويل نفقات كبيرة كانت في طريقها لتوسيع

[1]– محمد محي الدين عوض، تشريعات مكافحة الإرهاب في الوطن العربي، أكاديمية نايف العربية، للعلوم الأمنية، 1999، ص92

[2]– محمود رجب فتح الله، الوسيط في الجرائم معلوماتية، دار الجامعة الجديدة، الإسكندرية،2019، ص514

مجالات التنمية فتتحول من المجال الأمني، إلى غير ذلك من الآثار في مختلف المجالات ، ومن هذه النتائج أو الآثار قد لا تظهر مباشرة بعد العمل الإرهابي تمنها ما هو متعلق بالجانب السياسي ومنها ما هو متعلق بالجانب الاجتماعي ومنها ما هو المتعلق بالحياة الاقتصادية ومنها ما يتعلق بجانب الأمني والنفسي [1].

سنتناول الآثار الأمنية والنفسية على نقطتين هما ما يأتي

أولا) الآثار النفسية لأعمال الإرهاب الإلكتروني:

أن الضغوط النفسية التي يتعرض لها أفراد المجتمع وحدوث حالة الاضطرابات والاختلال في القيام الأسرة بوظائفها وإدارة حياتها اليومية والتخطيط لمستقبلها والخوف المتزايد وعدم وضوح الرؤية المستقبلية النتيجة الأعمال الإرهابية، جميعها عوامل تعد مقومات بناء الشخصية ونموها وتترك أثار نفسية سيئة لدى أفراد المجتمع، وربما لا تظهر إلا بعد فترات طويلة، ويمكن تحديد أهم الآثار النفسية التي يتركها الإرهاب الإلكتروني فيما يأتي:

1-زيادة الأمراض النفسية على الفرد نتيجة عيشه حالة قلق وتوتر واضطراب مستمر وصراع النفسي دائم بسبب الوضع الناجم عن هذه الأعمال الإرهابية والاعتداءات الوحشية العشوائية على الوسائل الالكترونية

2-تأثر الأطفال نفسيا بما يشاهدونه من إحداث إرهابية عبر الوسائل الإلكترونية خاصة الآثار الدموية التي يخلفها الإرهاب وبشكل أخص إذا كان الضحايا من أسرة الطفل، إذ يصاب الطفل جلسات نفسية و عصبية وسلوكية قد تستمر معه فترة زمنية طويلة وتأثر على سلوكه[2].

[1]- عمراني كمال الدين، المرجع السابق، ص103

[2]- محمد عبد الله العميري، موقف الإسلام من الإرهاب، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض،2004، ص80

3-التهديد بعدم الاستقرار لدى الأشخاص نتيجة الاكتئاب والقلق مما ينعكس على سلوكياتهم وتعاملهم مع الآخرين، الأمر الذي يؤدي إلى ضعف العلاقات بين أفراد المجتمع القائمة على أساس الثقة والاطمئنان الغير[1]

ومن الأمثلة التطبيقية للآثار النفسية ، هي لعبة على شبكة الإنترنت تسمى (الحوت الأزرق) ، حيث ظهرت هذه اللعبة في عام (2013) في روسيا وتكون مسموحة في معظم البلدان ، وتتكون اللعبة من تحديات لمدة (50) يوما ، وفي التحدي النهائي يطلب من اللاعب الانتحار ، وتحتاج هذه اللعبة الاتصال بشبكة الإنترنت حيث ينبغي على اللاعب إرسال صورة أو فيديو يدل على إتمام المهمة لكي يتابع التحدي التالي ، حيث حكم على شخص عام(2017) بالسجن لمدة ثلاث سنوات بعد محاكمته في سيبيريا بتهمة التحريض على الانتحار عبر شبكة الاجتماعية الروسية (فكونتاكتي)[2].

ثانيا) الآثار الأمنية لظاهرة الإرهاب الإلكتروني على المستوى الدولي:

إن فقدان نعمة الأمن والاستقرار من أبرز أثار الإرهاب الإلكتروني وأخطاره في المجال الأمني إذ تعد تلك النعمة من أجل نعم اللِه تعالى وأعظمها على عباده ، وفي قوله تعالى في محكم كتابه الكريم "وَضَرَبَ الله مَثَلاً قَرْيَةً كَانَتْ أمِنَةً مُطْمَئِنَّةً يَأْتِيهَا رِزْقُهَا رَغَدًا مِنْ كُلّ مَكَانِ فَكَفَرَتْ بِأنْعَمْ اللِهَ فأذَاقَهَا الُله لِبَاسَ الجُوعِ وَالْخَوْفِ بِمَا كَانُواْ يَصْنَعُونَ"[3]، فالأمن أساس الرخاء والاستقرار والنماء ، وما ذلك إلا لأهمية الأمن والاطمئنان في حياة البشر دون استثناء ، والإرهاب الإلكتروني في حقيقته ما هو إلا جريمة بشعة تلحق الضرر بالأفراد والمجتمعات وأنظمة الحكم على حد سواء ، وهو ما يشعر المواطنين بالخوف وعدم الاطمئنان على أنفسهم وأعراضهم وأموالهم، حيث تأتي الآثار الأمنية الإرهاب الإلكتروني في مقدمة الآثار السلبية المباشرة في أي مجتمع ، إذ

[1]-عبد الله عبد الكريم عبد الله، جرائم المعلوماتية الانترنت (الجرائم الالكترونية)، ط1، منشورات حلبي الحقوقية، بيروت،2007، ص ص32،33

[2]- محمود رجب فتح الله، المرجع السابق، ص522

[3]- السورة النحل، الآية 112

يمثل الإرهاب الإلكتروني رسالة مباشرة من مرتكبيها يوجهونها إلى من يختلفون معهم عن طريق إرهاب الناس والفزع على نطاق واسع عبر الوسائل الإلكترونية ، وترويج الأفكار والشائعات على هذه الوسائل لضرب المجتمعات الدولية ، وذلك لانعدام الثقة وخلق جو مشحون بين المواطنين والشعوب والدول مما يؤدي إلى إشعال الفتنة والنار بين الدول ، وزعزعة الأمن والاستقرار والفوضى في أوساط المجتمع الدولي.[1]

إن مكافحة الإرهاب الإلكتروني يتطلب ضرورة اتخاذ إجراءات أمنية على مختلف الأصعدة الدولية، وذلك لأن هذا الإرهاب الإلكتروني يشكل قضية تهم المجتمع الدولي بأسره وظهوره يؤدي إلى عدم الاستقرار وانعدام الطمأنينة والشعور بالخوف على الأنفس، مما يتطلب من المجتمع الدولي مضاعفة جهودها الأمنية لطمأنه المواطن والحد من انتشار الجريمة الإرهابية الإلكترونية، ويمكن أن نجمل أهم الآثار الأمنية التي يخلفها الإرهاب الإلكتروني فيما يأتي

1-انعدام الشعور بالأمن الإلكتروني وعدم الطمأنينة والخوف في مجال الحياة العادية نتيجة حالة القلق الدائم الذي يعيش الفرد، حيث لا يدري متى سيصيبه الخطر الناتج عن الإرهاب الإلكتروني[2]

2 . نشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية مما يؤثر على شعبية رجال الأمن الالكتروني والمسؤولين عنه والنيل من سمعتهم وفقدان الثقة بالقوانين والأنظمة التي تنظم الأمن الإلكتروني وتساهم في تحقيقه في المجتمع [3]

3-تعمل الجماعات الإرهابية عبر الوسائل الإلكترونية إلى التحكم بالأنظمة الأمنية من خلال فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية

[1]- علي بن فايز الجحني، خطاب العنف الإرهابي قنواته وآثاره، جامعة نايف للعلوم الأمنية، الرياض،2008، ص8

[2]-عمراني كمال الدين، المرجع السابق، ص110

3-عبد العزيز لطفي جاد الله، امن المجتمع الالكتروني بين السياسة الالكترونية والتعاون الدولي في إطار مواجهة الجرائم الالكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2017، ص264

والأسلحة الفتاكة وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجي وشب هدف عزلها على قوات والنفاد إلى النظم العسكرية واستخدامها التوجيه جنود إلى نقطة غير أمنة قبل قصفها و تفجيرها[1]

ومن الأمثلة التطبيقية على أثار الأمنية، ما حدث في آذار عام (2014) عندما هاجمت مجموعة "سايبربيركوت" الأكرانية المواقع الالكترونية التالية لحلف الناتو، مما أدى إلى تعطيل مواقع الحلف لعدة ساعات، وهنا:وهذا ما يخلف أثار على مستوى الحماية الأمنية وزعزعت الأمن والعلاقات الدبلوماسية الدولية.[2]

[1]– السيد عبد الفتاح علي، مكافحة الجرائم الالكترونية بين نظم المعلوماتية والإعلام البديل، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2017، ص65

[2]– عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق، ص22

الفصل الثاني:

مكافحة الإرهاب الالكتروني

يعاني المجتمع الدولي في كل شبر من أرجائه في هذا العصر من جرائم مستحدثة التي غطت على الجرائم التقليدية[1]، حيث بات الإرهاب الالكتروني وما يفرزه من مشاكل وتهديدات الشغل الشاغل للمجتمع الدولي[2]، وفي ظل زيادة خطورة هذا الإرهاب الجديد وانتشاره الرهيب أصبحت محاربته ضرورة حتمية تستوجب على دول تكثيف جهودها بسن تشريعات وإبرام الاتفاقيات وإنشاء منظمات الدولية والإقليمية لمكافحة هذا الوحش الذي أضحى من أكبر التحديات التي تواجهها الدول.

وسنتناول في هذا الفصل مكافحة الإرهاب الالكتروني على الصعيد الدولي (المبحث الأول) واليات مكافحة الإرهاب الالكتروني (المبحث الثاني)

[1] – عبد الله عبد العزيز يوسف، التقنية والجرائم المستحدثة،جامعة نايف العربية للعلوم الأمنية، الرياض، 1999، ص201

[2] – يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، منشورات مركز كوردستان لدراسات الإستراتيجية، السلمانية 2008، ص03

المبحث الأول: مكافحة الإرهاب الالكتروني على الصعيد الدولي والإقليمي

يعد الإرهاب الالكتروني أحد أكبر المشكلات التي تواجهها الدول والمجتمعات في عصرنا الحاضر، فرغم أن الإرهاب، كجريمة محلية ودولية، كان موجودا منذ القدم إلا أنه لم يتسع من حيث المدى ولم يشكل تهديدا خطيرا على المجتمعات إلا في السنوات الأخيرة.[1]

وان خطورة هذا الإرهاب فرضت على الحكومات تطوير وسائلها وقدراتها لتصدي لتهديداته المختلفة بتوفير التقنيات اللازمة للحماية وتقنين قواعد وتشريعات على مستوى الإقليمي والدولي. وان الطابع العالمي لهذه الظاهرة زادها تعقيد في شان مكافحتها دوليا، خاصة مع عدم وجود إطار قانوني دولي واضح يتناول هذه الظاهرة المستحدثة[2].ولقد حضي الإرهاب الالكتروني باهتمام كبير على كافة الأصعدة سواء الدولي أو الإقليمي إذ عقدت في شانه العديد من الاتفاقيات وندوات مختلفة وتسابقت جل الدول الكبرى إلى سن تشريعات بهدف الحد منه.

من هنا سنتناول في هذا المبحث أهم الجهود ومحاولات للحد من الإرهاب الالكتروني حيث تطرقنا في (المطلب الأول) إلى الجهود الدولية لمكافحة الإرهاب الالكتروني وجهود الإقليمية لمكافحة الإرهاب الالكتروني (المطلب الثاني)

المطلب الأول: الجهود الدولية في مكافحة الإرهاب الالكتروني

لقي الإرهاب الالكتروني اهتماما عالميا كبيرا، بشهادة العالم اجمع على جسامة وخطورة هذا الإرهاب بعد أحداث 11 سبتمبر 2001 مما دفع المجتمع الدولي الى تكثيف الجهود وسن معظم الدول الكبرى تشريعات وقوانين رادعة للحد من القصور الجنائي في

[1]– عبد الله عبد العزيز يوسف،المرجع السابق، ص201

[2]– نور الله تله، المرجع السابق، الإرهاب بالوسائل الالكترونية، ص110

مواجهته وإبرام العديد من اتفاقيات وإنشاء منظمات دولية في الشأن مكافحة هذا النمط الإجرامي العابر للحدود

ولدراسة هذه الجهود الدولية سنقسم هذا المطلب إلى 3 فروع سنتناول في (الفرع الأول) مكافحة الإرهاب الإلكتروني في الدول الغربية و (الفرع الثاني) مكافحة الإرهاب الالكتروني في الاتفاقيات الدولية و (الفرع الثالث) مكافحته في منظمات الدولية

الفرع الأول: مكافحة الإرهاب الالكتروني في الدول الغربية

سنعرض فيما يلي بإيجاز تجارب بعض الدول الغربية في مواجهة الإرهاب الكتروني من خلال قوانينها واستراتيجياتها الوطنية

أولا: الولايات المتحدة الأمريكية

تعد الولايات المتحدة من الدول السباقة في محاربة ظاهرة الإرهاب بالوسائل الإلكترونية، من خلال قوانينها الوطنية أو من خلال سعيها لعقد اتفاقيات دولية بهذا الخصوص، أو من خلال إنشاء الأجهزة المختصة بمكافحة الإرهاب بالوسائل الإلكترونية. حيث تميزت الإستراتيجية الأمريكية لمكافحة الإرهاب الإلكتروني بطابع استباق الهجمات المحتملة، وانصبت هذه الإستراتيجية في بادئ الأمر على المجال العسكري، حيث عمد البنتاغون سنة 2005 إلى إنشاء وحدة عسكرية متخصصة، عهد إليها بمهمة تحصين الفضاء المعلوماتي الأمريكي، وتأمين شبكات الاتصال الحساسة في الولايات المتحدة ضد أي حرب إرهابية محتملة[1]. وتعد الولايات المتحدة الأمريكية من أولى الدول التي أصدرت قوانين لمكافحة الإرهاب الإلكتروني، ففي أكتوبر 2001، أصدرت اتفاقية لمكافحة الإرهاب المعلوماتي، والتي وسعت من خلالها سلطات البحث

[1]–عبد المجيد حلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية، مكافحة جرائم الإرهاب المعلوماتية، في فترة 2006/4/139، المغرب القنطرة، 2006، ص22

والتحقيق والمراقبة الإلكترونية[1]، وتعمل الحكومة الفيدرالية الأمريكية جاهدة على سن تشريعات متطورة لمكافحة هذه الأنماط المستجدة للظاهرة الإرهابية، بحيث تحاول تقنين استخدام محرك البحثMSN– Google . Yahoo في مجموعة من الشركات[2].

وهناك خطوات عديدة اتخذتها الولايات المتحدة لمكافحة الجريمة والإرهاب الإلكتروني منها[3]:

1–إصدار قانون تعزيز أمن المعلومات 2002

2–وضع الإستراتيجية الوطنية لتأمين الفضاء الإلكتروني 2003

3–أنشأت وزارة العدل الأمريكية لجنة مكافحة الإرهاب الإلكتروني

4–كما تم إنشاء لجنة حماية البنية التحتية الحساسة في الولايات المتحدة، والتي أسست مجموعة خاصة تتناول جوانب الإرهاب الإلكتروني وأطلقت عليها اسم: مركز حرب المعلومات

5–كما تم إنشاء المركز القومي لحماية البنية التحتية ومركز تحليل وتبادل المعلومات، وبرنامج وغيرها من المبادرات.

ثانيا: بريطانيا

تعد المملكة المتحدة البريطانية هي أخرى من أولى الدول التي سارعت إلى محاربة الإرهاب الالكتروني، حيث قامت بتحقيقات أولية على يد لجنة القانون الأسكتلندي ضمنتها مذكرة استشارية نشرت عام 1982، وفي عام 1987 تم إعداد نشاط مماثل

[1]–محمد سيد سلطان، الحماية الدولية والقانونية للبيئة الالكترونية من الجريمة والإرهاب، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة: المفاهيم والتشريعات والتطبيقات، منعقد في الرياض، 2010/04/7.6، ص19

[2]–عبد المجيد حلاوي، المرجع السابق، ص22

[3]–محمد سيد سلطان، المرجع السابق، ص20.19

أعدته لجنة القانون عام 1988، وقد أسفر عن هذه الأنشطة توصيات وضع بناء عليها قانون إساءة استخدام الحاسب الالي الذي تمت الموافقة عليه في عام 1990[1].

ولقد عرف القانون البريطاني رقم 2000 لمكافحة الإرهاب والمعروف ب (terrorism act) الذي دخل حيز التنفيذ في فبراير 2001م، الإرهاب تعريفا موسعة ليشمل أفعال القرصنة المعلوماتية التي من شأنها إزعاج أو خلق اضطراب داخل النظام الإلكتروني وتضمن القانون 2000 (terrorism act) ثماني أقسام ، وضعت فيه قوانين مكافحة الإرهاب في مدونة واحدة ، وقد طرأ عليه مجموعة من التعديلات منها : في سنة 2009 م صدر تعديل لقانون مكافحة الإرهاب تضمن أفعال جديدة عدت تشجيعا للإرهاب ، حيث عد تشجيعا للإرهاب نشر التصريحات التي يمكن أن تفهم من الجمهور بأنها تشجيع مباشر أو غير مباشر ، أو تحريض على ارتكاب الإرهاب ، أو التجنيد الأعمال إرهابية ، كما تضمن هذا القانون جرائم التدريب على الإرهاب والتحضير له وقرر مجلس النواب البريطاني في أوائل افريل2012 م طرح ومناقشة قانون يسمح بموجبه لأحد وكالات المخابرات البريطانية بمراقبة كل الاتصالات الهاتفية والرسائل الإلكترونية والنصية والأنشطة التي تمارس على شبكة الإنترنت لمعالجة ظاهرة الإرهاب الإلكتروني ، مما أثار جدلا واسعا حول انتهاك الحرية الشخصية سواء في بريطانيا أو في العالم [2].

ثالثا: فرنسا

تعتبر التجربة الفرنسية في مكافحة الإرهاب من بين أهم التجارب التي يحتذى بها على الصعيد الإقليمي (الاتحاد الأوربي) فلقد سعت للاستعداد المبكر ولمواجهة الفعالة للإرهاب الالكتروني، حيث سن المشرع الفرنسي القانون رقم 88/19 المؤرخ في 05

[1]– صباح كزيز، أمال كزيز، الإرهاب الالكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، رقم 1، العدد8 ، 2008 ،ص321

[2]–نور الله تلة، المرجع السابق، ص140

فيفري1988و الخاص بالجرائم المعلوماتية و الحريات و ضمه القانون الفرنسي في المادة462 منه ، و جرم مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريقة غير مشروعة المادة02/462 ، كما شدد العقوبة في الأحوال التي ينجم عنها هذا الولوج المحو أو تعديل في معطيات آليا،، واستعمال المستندات ، و عاقب على هذه الجرائم بعقوبة السجن أو الغرامة و خضع هذا القانون لتعديلات منها عام 1993، بحيث و سعت من نطاق السلوكيات محل التجريم إضافة إلى تعديل بعض العقوبات لتحقيق المزيد من الأبعاد الردعية [1].

أصدرت الحكومة الفرنسية قانونا لمكافحة الإرهاب علم 2009 يسمح بمراقبة الهواتف والإنترنت، وزرع كاميرات مراقبة في الأماكن العامة وملاحقة أي فرنسي يسافر للتدرب على أعمال إرهابية خارج البلاد حتى ولو لم يرتكب أي عمل مسيء في فرنسا، وحتى لو لم يمض شبابه على الأراضي الفرنسية، وذلك بتهمة تشكيل عصابة إجرامية تهدف لارتكاب عمل إرهابي، وهي جريمة يعاقب عليها بالسجن عشر سنوات والغرامة 225 ألف أورو[2].

وفي نوفمبر 2014 تم تعديل القانون الفرنسي،الذي نص على منع الفرنسيين من السفر للانضمام للجماعات الجهادية في سورية بعد انضمام مئات الفرنسيين لتنظيم داعش،ومصادرة جواز سفر وبطاقة هوية كل من أمضى بين ستة أشهر وعامين بها، ومنع المشتبه بانضمامهم لتنظيم " داعش " من دخول فرنسا، ومراقبة السلطات المواقع الالكترونية التي تدعو للتطرف، ومطالبة مديرها بمسح المحتويات المتشددة وحظر المواقع التي تدافع عن الإرهاب[3].

[1]–رائد عدوان، المرجع السابق، ص ص 12–13

[2]–نور الله تلة، المرجع السابق ، ص141

[3]– المرجع نفسه، ص ص141–142

و في مارس 2015، خرج إلى النور قانون جديد باسم " تعزيز مكافحة الإرهاب"، و وافق عليه البرلمان، و ينص القانون على جواز اختراق من وصفهم ب" الإرهابيين المحتملين" و مراقبتهم من خلال اذونات إدارية دون الحاجة إلى موافقة قضائية ، اللجوء إلى أجهزة لتسجيل كلام الأشخاص وصورهم ، أو البرامج معلوماتية يلتقط البيانات المعلوماتية "، ما سيسمح العناصر الاستخبارات بوضع ميكروفونات وكاميرات تجسس وغيرها أينما يرون ذلك ضروريا ، بما في ذلك إقامة مراكز تتبع هواتف المشتركين التي تسمح باعتراض الاتصالات في مربع معين ، سواء من اتصالات مشتبه بهم أو المقربين منهم والتنصت عليهم ، ويلزم القانون مشغلو خطوط الهواتف ومزودو الإنترنت بتسليم السلطات كل ما يمكن أن يجمعوه من بيانات[1] .

وفي 23 أفريل 2015 تما إبرام اتفاق بين الحكومة الفرنسية وكبار مشغلي الإنترنت لمكافحة الإرهاب الإلكتروني والتصدي للمواقع الجهادية، ويهدف الاتفاق إلي التصدي لمحاولات نشر التطرف والتعصب على الإنترنت، ووضع آلية سريعة لسحب المضامين ذات الطابع الإرهابي، فضلا عن تشكيل مجموعة عمل مشتركة بين وزارة الداخلية الفرنسية ومشغلي الإنترنت، وانضم إلى الاتفاق كل من شركات غوغل وفيس بوك وميكروسوفت وآبل وتويتر، إضافة إلى الجمعية الفرنسية للشركات المزودة لخدمة الإنترنت لهذا الاتفاق، وقد حجبت وزارة الداخلية الفرنسية خمسة مواقع تمجد الإرهاب عبر الإنترنت، في مسابقة منذ تبني قانون" تعزيز مكافحة الإرهاب "، وصدر أمر الحجب عن مكتب الجريمة المرتبطة بتكنولوجيا المعلومات والاتصال[2].

الفرع الثاني:مكافحة الإرهاب الالكتروني في الاتفاقيات دولية

إن شساعة وبشاعة الإرهاب الالكتروني بات أمرا ملحوظا ومحسوسا على الصعيد العالمي، ويتبين ذلك من خلال الإحصائيات المروعة التي تبين حجم المخاطره والخسائر

[1]– نور الله تلة المرجع السابق ، ص142

[2]– المرجع نفسه ، ص ص 142–143

الناجمة عنه، و يتفاوت تأثيره من دولة إلى أخرى بحسب اعتمادها على التقنية العالمية المعلوماتية، فهو يشكل بذلك تهديدا للأمن القومي و الاقتصاد الوطني، وفي إطار مكافحته عمل المجتمع الدولي بجهد كبير لتصدي و القضاء عليه بكل أشكاله من خلال إبرام اتفاقيات دولية التي لعبت دورا كبيرا في محاربته بوضع أحكام قانونية بغية الحصول مرتكبي تلك الجرائم على جزاء رادع من خلال إلزام الدول بتجريم الجرائم الإرهابية الالكترونية ونلاحظ إن معظم الاتفاقيات الدولية مبرمة في هذا الشأن، أبرمت قبل أحداث 11 سبتمبر 2001 أو بعدها [1]ومنها :

أولا: اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55 لسنة 2000

قامت الجمعية العامة لمنظمة الأمم المتحدة في 12 أفريل 2000 بإصدار اتفاقية عالمية لمكافحة إساءة استعمال تكنولوجيا المعلومات الأغراض إجرامية رقم (55/ 63) بعد تزايد الجرائم المرتكبة عبر الإنترنت وما تثيره من مشاكل، حيث أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في هذا الشأن.

حيث إن الجمعية العامة تشير إلى إعلان منظمة الأمم المتحدة بشان الألفية التي عقدت فيه الدول الأعضاء لمكافحة الإرهاب الدولي والمخدرات والدعوة إلى الانضمام إلى جميع الاتفاقيات الدولية ذات الصلة ، وتكثيف جهودها لمكافحة الجريمة العابرة للحدود الوطنية بجميع أبعادها ، ومنها الإرهاب الإلكتروني ، والعزم على أن تكفل إتاحة منافع التكنولوجيا الجديدة ،وبخاصة تكنولوجيا المعلومات والاتصالات للجميع ، بما يتفق مع التوصيات الواردة في الإعلان الوزاري الصادر من الدورة الموضوعية للمجلس الاقتصادي والاجتماعي للأمم المتحدة لعام 2000[2]. كما تشير أيضا على إن قرار الجمعية العامة

[1]–سجاد خليفة خزعل تميمي، المواجهة الدولية والوطنية لجريمة تمويل الإرهاب، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2017، ص116

[2]– علي عدنان الفيل، الإجرام الالكتروني، المرجع السابق، ص330

رقم (121/45المؤرخ 14 ديسمبر 1990)،أيد توصيات مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين،والذي دعى الدول أن تكثف جهودها لمكافحة إساءة استعمال الحواسيب بفعالية أكبر [1].

ولقد نصت المادة 1 من هذه الاتفاقية في الفقرات (أي) على ما يلي:

(أ)"ينبغي للدول أن تكفل عدم توفير قوانينها وممارساتها فيها ملاذا أمن للذين يسيئون استعمال تكنولوجيا المعلومات الأغراض إجرامية "

(ب)"ينبغي أن تنسق جميع الدول المعنية للتعاون في مجال إنفاذ القانون لدى التحقيق والمقاضاة في القضايا الدولية المتعلقة بإساءة استعمال تكنولوجيا المعلومات الأغراض إجرامية ".

(ج)"ينبغي أن تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة إساءة استعمال تكنولوجيا المعلومات الأغراض إجرامية".

(د) "ينبغي تدريب العاملين في مجال النفاذ القوانين وتجهيزهم بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية"

(ز)"ينبغي لنظم المساعدة المتبادلة أن تضمن التحقيق في الوقت المناسب في إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية وجمع الأدلة في مثل هذه الحالات وتبادلها في الوقت المناسب"(ي)"تقضي مكافحة إساءة استعمال تكنولوجيا المعلومات الأغراض إجرامية وضع حل ولتأخذ في الاعتبار حماية حريات الأفراد وحمايتيهم الخاصة والمحافظة على قدر الحكومات على مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية"[2]

---

[1]–عمر عباس خضير العبيدي، الإرهاب الالكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق،2019، ص ص47–48

[2]–انظر المادة 1، من اتفاقية مكافحة إساءة استعمال التكنولوجيا الأغراض إجرامية رقم (63/55) في 2000/04/12، والصادرة عن منظمة الأمم المتحدة، الجلسة العامة 2000/12/4/81

ولقد دعت المادة (2) إلى" **أخذ هذه التدابير المذكورة أعلاه في الاعتبار في جهودها الرامية إلى مكافحة إساءة استعمال تكنولوجيا المعلومات الأعراض إجرامية** "[1]، وكذلك قررت المادة (3) على "**إبقاء مسالة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية على جدول أعمال دورتها السادسة والخمسين،ضمن البند المعنون (منع الجريمة والعدالة الجنائية)**"[2].

ونلاحظ أن هذه الاتفاقية لم تنص بشكل صريح على جريمة الإرهاب الإلكتروني، ولكن جاءت لمكافحة الجرائم المرتكبة عبر الإنترنت التي تنتمي الى دائرتها جرائم الإرهاب الإلكتروني

ثانيا: اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001والبروتوكول الملحق بها

أ) اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001

تعتبر اتفاقية بودابست أول وأبرز اتفاقية تختص بالجرائم الالكترونية، وهي أوروبية المنشأ ولكنها ذات طابع عالمي،وقد وقعت عليها (21) دولة أوروبية بالإضافة إلى كندا وأمريكا وجنوب أفريقيا،وتعكس هذه الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ومجلس أوروبي في التصدي لمكافحة الإرهاب الالكتروني والجريمة المعلوماتية[3]، حيث وقع وزراء خارجية دول أعضاء مجلس أوروبا على هذه الاتفاقية في 5نوفمبر 2001 وهي نتيجة لعمل استمر لمدة 4 سنوات[4].

[1]–انظر المادة 2، من اتفاقية مكافحة إساءة استعمال التكنولوجيا المعلومات لأغراض إرهابية لسنة2000

[2]– انظر المادة 3، من اتفاقية مكافحة إساءة استعمال التكنولوجيا المعلومات لأغراض إرهابية لسنة 2000

[3]–عمر عباس خضير عبيد، المرجع السابق، ص50

[4]–محمد سيد سلطان، المرجع السابق، ص22

تم توقيع هذه الاتفاقية، بسبب المخاوف والقلق إزاء سوء استخدام شبكات الانترنت والمعلومات الالكترونية، ومن اجل توفر ما يلزم لردع أي عمل موجه ضد سرية نظم الحاسوب والشبكات والبيانات[1].

وتتكون هذه الاتفاقية من 48 مادة، أكدت فيها على ضرورة التزام دول الأعضاء بتسليم المجرمين وتبادل المساعدات في تحقيق وجمع الأدلة واتخاذ تدابير تشريعية التي تمكنها من الوفاء بالالتزامات، وهدف من إبرامها وضع سياسة جنائية مشتركة بين الدول المجلس بهدف حماية ممتلكاته من الجريمة الالكترونية من خلال اعتماد تشريعات ملائمة وتقرير التعاون الدولي[2].

وتتألف الاتفاقية من مقدمة وأربعة فصول:فقد أكدت المقدمة على أهمية ما أنجز من جهود في حقل المعلوماتية من قبل منظمة الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوروبي ومجموعة الدول الصناعية.وبالنتيجة فإن مقدمة هذه الاتفاقية استعرضت أهدافها ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهود إرشادية وتوجيهية وتدابير إقليمية ودولية،وتضمن الفصل الأول تعريف بعض المفاهيم منها نظام الحاسوب و بياناته، أما الفصل الثاني جاء تحت عنوان:الجوانب الموضوعية والإجرائية للجرائم المعلوماتية (المواد2-22) معالجة النصوص الموضوعية لجرائم الكمبيوتر، والجوانب الإجرائية الجرائم المعلوماتية،وجاء الفصل الثالث: بعنوان الأحكام المتعلقة بالجرائم المعلوماتية عابرة الحدود (المواد23 -35)والمتعلقة بالاختصاص والتعاون الدولي، أما الفصل الرابع جاء بالأحكام الختامية (المواد 36. 48)[3].

[1]- عمر عباس خضير عبيد، المرجع السابق، ص50

[2]-نور الله تلة، المرجع السابق، ص ص155-156

[3]-عمر عباس خضير عبيد، المرجع السابق، ص ص50-51

لقد حثت هذه الاتفاقية الدول الأعضاء على تجريم بعض الأعمال الإرهابية عبر الوسائل الالكترونية التي وصفتها بغير المشروعة في تشريعاتها داخلية،ولقد تضمنت الاتفاقية عدة مجموعات من الجرائم الإلكترونية[1]، وهي على النحو الآتي:

- المجموعة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات الإلكترونية.
- المجموعة الثانية: الجرائم المرتبطة بالحاسوب الإلكتروني
- المجموعة الثالثة: الجرائم المرتبطة بالمحتوى الإلكتروني.
- المجموعة الرابعة: الإرهاب الإلكتروني.

نستنتج من خلال المذكرة التفسيرية لاتفاقية بودابست في (8 فيفري 2001) ان الهدف من هذه الاتفاقية بموادها من (2-13)، هو تحسين أو إصلاح وسائل منع وقمع الإجرام المعلوماتي، وسنتناول بعض من مواد هذه الاتفاقية فيما يخص الجرائم الإرهابية الإلكترونية، ومنها ما يأتي:

نصت المادة (2) من هذه الاتفاقية على جريمة الولوج أو الدخول غير القانوني، أما المادة(3) فنصت على جريمة الاعتراض غير القانوني، و تنص المادة (4) على جريمة الاعتداء على سلامة البيانات، أما المدة (5) فنصت على جريمة الاعتداء على سلامة النظام أما المادة (6) نصت على جريمة إساءة استخدام أجهزة الحاسوب، فحين نصت المادة (7) على جريمة التزوير المعلوماتي :(التزوير المتصل في الحاسوب الآلي)،أما المادة (8) فنصت على جريمة الاحتيال المعلوماتي (الاحتيال المتصل في الحاسوب الآلي)، و المادة (10) نصت على الجرائم المتصلة بالاعتداءات الواقع على الملكية الفكرية والحقوق المجاورة

أما المادة (11) تضمنت الشروع والاشتراك، فحين نصت المادة(12) على مسؤولية الأشخاص المعنوية، ولقد نصت المادة(13) على الجزاءات والإجراءات

[1]-خالد حسن احمد لوطفي، الجرائم الانترنت بين القرصنة الالكترونية والابتزاز الالكتروني، ط1، دار الفكر الجامعي، الإسكندرية ،2018، ص54

التشريعية المعاقبة على الجرائم السابقة[1].**ب) البروتكول الإضافي لاتفاقية بودابست لسنة (2001)بالجرائم الإرهابية الإلكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر ، ستراسبورغ 2003/01/28 والصادر عن مجلس أوروبا – سلسلة المعاهدات الأوروبية رقم (189)** :سندرس ما جاء في المادة (6) من هذا البروتكول ، حيث تضمنت هذه المادة ارتكاب جرائم دولية منها أفعال تشكل جرائم إبادة جماعية وجرائم ضد الإنسانية ، كما هي معروفة في القانون الدولي ، وكما أقرتها القرارات النهائية الملزمة للمحكمة العسكرية التي أنشأت بموجب اتفاقية لندن بتاريخ (8 / أوت/1945)، أو قرارات أي محكمة دولية أخرى أنشأت بموجب وثائق دولية ذات صلة ويقر باختصاصها ذلك الطرف " فإن هذه الجرائم إذا وقعت عبر الوسائل الإلكترونية (كتجنيد الأطفال) تعتبر جرائم إرهاب إلكتروني تدخل ضمن الجرائم أعلاه [2].

الفرع الثالث: مكافحة الإرهاب الالكتروني في منظمات الدولية

تسعى المنظمات الدولية كغيرها من الاتفاقيات والمؤتمرات والقاءات الدولية والإقليمية إلى إرساء قواعد قوية لبناء إستراتيجية فعالة لمكافحة الإرهاب الالكتروني ومواكبه التطورات حاصلة في شان هذا النمط الإجرامي الجديد، حيث تم عقد عديد من منظمات الدولية لتي تؤدي دورا ملحوظا في إطار مكافحة الأعمال الإرهابية التي تتم عبر شبكة الإنترنت، والتي تلحق الإضرار بالنظام الاجتماعي والأخلاقي للدول من جراء الاستخدام السيئ لأجهزة الاتصال الحديثة ، وعلى رأسها منظمة الأمم المتحدة وبعض المنظمات العالمية المتخصصة الأخرى [3].

---

[1]– عمر عباس خضير عبيد، المرجع السابق، ص ص51–57

[2]–إيهاب سنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الالكترونية (بودابست 2001) والبرتوكول الملحق بها، دار النهضة العربية، القاهرة،2009، ص80

[3]–عمر عباس خضير العبيدي، المرجع السابق، ص66

أولا: منظمة الأمم المتحدة ومجموعة الدول الثمانية (8- G)العالمية :

أ) جهود منظمة الأمم المتحدة:

إن منظمة الأمم المتحدة تبذل جهودا فاعلة ليست بقليلة في مجال مكافحة الإرهاب الإلكتروني، وذلك من اجل منع أي محاولة اعتداء من قبل الإرهابي الإلكتروني على أمن الدولة وأفرادها، وتظهر جهودها من خلال المؤتمرات التي تعقد برعايتها والخاصة بمنع الجريمة ومعاملة السجناء[1]، وكذلك مؤتمرات الجمعية الدولية لقانون العقوبات التي تعقد كل خمس سنوات، إذ تسعى منظمة الأمم المتحدة من خلال هيئاتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة، وكان المؤتمر السابع المنعقد بميلانو (عام 1980) كانطلاقة في هذا الشأن، والذي أكد على الاستفادة من التطورات العلمية والتكنولوجية في مواجهة هذه الظاهرة الإجرامية المتعلقة بالحاسوب الآلي [2]، وفي المؤتمر التاسع برعاية منظمة الأمم المتحدة في القاهرة (سنة1995) تم التأكيد على وجوب حماية مخاطر التكنولوجيا ، ووجوب التنسيق والتعاون بين الدول ، وفي المؤتمر العاشر لمنع الجريمة في بودابست جرى اعتبار جرائم الحاسوب الآلي نمطا جديدا من الجرائم المستحدثة مع وجوب العمل للحد من أعمال القرصنة الإلكترونية ، وأقرت الجمعية العامة للأمم المتحدة في الدورة (56 /285) في (31 جانفي عام 2002) قرارا يدعو إلى استخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية ، وجاء هذا بعد سلسلة من القرارات الدولية لتنبيه الرأي العام العالمي وتنمية الوعي بحجم المخاطر هذه الجرائم[3] .

[1]–علي يوسف شكري، المنظمات الدولية، ط1، دار الصفاء لنشر والتوزيع، عمان، 2012، ص ص97،98

[2]–مريم محمد حسن، التنظيم القانوني لجريمة التجسس المعلومات، رسالة ماجستير، كلية القانون، جامعة كوفة، العراق،2016، ص162

[3]–عمر عباس خضير عبيد، المرجع السابق، ص67

أصدرت الجمعية العامة للأمم المتحدة القرار رقم (95/45) الصادر في (14/12/1990) والذي يتعلق بالمعطيات الحساسة والتي تعني كل معلومة تؤدي إلى التفرقة العنصرية أو التميز بشكل عام بين البشر مثل معلومات عن العرق، اللون، الآراء السياسية، الآراء الفلسفية .... الخ)[1]، وفي 12 أفريل 2000 وقعت منظمة الأمم المتحدة على اتفاقية خاصة بمكافحة إساءة استعمال التكنولوجيا الإجرامية، بسبب تزايد الجرائم المرتكبة عبر الإنترنت مشاكل التي تثيرها، ولقد أكد الاتفاقية على الحاجة إلى التعزيز والتنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[2].

وفي عام 2010 حذر مجلس الأمن في القرار رقم(1963) من "ازدياد استخدام الإرهابيين التكنولوجيا الجديدة للمعلومات والاتصالات وخاصة الإنترنت لأغراض التجنيد عبر الإنترنت وكذلك التحريض على دعم الأعمال الإرهابية"، وجاء في فيفري2015 القرار رقم(2255) أكثر شمولا لطرق استخدام الإرهابيين للأنترنت في أنشطتهم الإرهابية، إذ تضمن "الإعراب عن قلقه من تزايد لجوء الإرهابيين إلى استعمال تكنولوجيا المعلومات ولاسيما شبكة الإنترنت من أجل تسيير الأعمال الإرهابية والتحريض على الإرهاب أو تجنيد مرتكبيها أو تمويلها" [3].

وفي مؤتمر منظمة الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية عام (2010)، عقد هذا المؤتمر في سلفادور –البرازيل من (19–12 أفريل2010) تحت عنوان استراتيجيات شاملة في تحديات عالمية والذي نظم منع الجريمة والعدالة الجنائية

[1]–محروس نصر غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، العدد 24، الإصدار 9، العراق ،2011، ص118

[2]– نجيب بن عمر عوينات، الإرهاب الالكتروني: مفهوم الجهود الدولية والإقليمية لمكافحته، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، معهد العالي للإعلامية، الكاف جامعة جندوبة تونس، العدد6، تاريخ الصدور2017/04/20، ص ص17–18

[3]– عمر عباس خضير العبيدي، المرجع السابق، ص68

وتطورها في عالم متغير، وتضمن جدول الأعمال ثمانية بنود وكان من ضمنها جرائم الإنترنت، والتعاون الدولي في مكافحة هذه الجريمة [1].

ولم ينص ميثاق منظمة الأمم المتحدة صراحة على تجريم استخدام المعلومات كأداة إرهابية ضمن ما يعرف بالإرهاب الإلكتروني، إلا أن روح الميثاق يتفق مع تجريم استخدامه بوصفه انتهاك لما ورد في الميثاق بخصوص "التهديد أو استخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة "، ومع الأخذ في الاعتبار أن الميثاق جاء لمكافحة النزاعات المسلحة، على اعتبار أن الإرهاب الإلكتروني واستخدام حرب المعلومات يقعان ضمن العدوان ، حيث إن هذا النوع من الإرهاب لا يتفق مع السيادة الدولية ، لأنه يهدد العلاقات الدولية باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد منظمة الأمم المتحدة[2] .

ونستنتج إن الأمم المتحدة في إطار مكافحة الإرهاب الالكتروني والجرائم المتصلة بالكمبيوتر والفضاء الرقمي أخذت بثلاثة محاور وهي:

-التنبيه من مخاطر الإرهاب الجديد ونشر وتطوير الوعي الدولي عبر سلسلة من الجهود.

-ضمان حرية التعبير وتنقل الحر للمعلومات والأفكار والمعرفة في شبكة المعلومات مع وجوب مراقبة الانترنت من اجل الحفاظ على الأمن والسلم الدوليين.

-وضع استراتيجيات علمية شاملة لمواجهة ومكافحة مخاطر الإرهاب الالكتروني على ارض الواقع.[3]

---

[1]- عمر عباس خضير العبيدي، المرجع السابق، ص69

[2]-توفيق شريخي، الإرهاب الالكتروني وتأثيره على امن الدولة، مذكرة ماستر، تخصص إستراتيجية وعلاقات دولية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة، الجزائر، ص60

[3]- توفيق شريخي، المرجع السابق، ص62

ب) مجموعة الدول الثماني (8-G)

عملت مجموعة الدول الثمانية على مكافحة الإرهاب الالكتروني من خلال الإعلانات والمؤتمرات وملتقيات والاجتماعات وسعيت إلى تعزيز الحرية والديمقراطية وحقوق الإنسان والتعاون الدولي في قضايا المتعلقة بالانترنت.

حيث أنشأت مجموعة الدول الثمانية (8- G) الفريق الفرعي للجرائم الإرهابية الإلكترونية التقنية في قمة مجموعة(8- G) في (2004/10/11) ، تم اعتماد وزراء العدل والداخلية التابعين لبلدان مجموعة في اجتماعاتهم المختلفة آلية لمكافحة العديد من جرائم الإنترنت والتي تستند إلى المبادئ التالية:

1-التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بصرف النظر عن مكان حدوث الضرر.

2-عدم إتاحة ملذات آمنة للمعتدين على تكنولوجيا المعلومات، تدريب الموظفين المكلفين بتنفيذ القوانين.

3-تجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالمية.[1]

ولقد أصدرت مجموعة الدول الثماني (8- G)عام 2005 بيان عن اجتماعها أكدت فيه على أن وكالات إنفاذ القانون تستجيب بسرعة لتهديدات الجريمة الإرهابية الإلكترونية والحوادث الخطيرة ، وفي اجتماع أخر للمجموعة في(موسكو - روسيا) سنة 2006ناقشت الجريمة الإرهابية الإلكترونية وقضايا الفضاء الإلكتروني Cyberspace ، وأصدرت بيان موسكو الذي تم التأكيد فيه على منع الأعمال الإجرامية المحتملة واتخاذ التدابير الضرورية، وكذلك اجتمع وزراء العدل والداخلية لدول (8- G)في23-25 ماي عام 2007 في (ميونخ ألمانيا) : واتفق الأعضاء على العمل من خلال الأطر القانونية لتجريم أشكال معينة بشأن استخدام الإنترنت لأغراض إرهابية ،اجتمعت الدول الثمانية

[1]-خالد حسن احمد لطفي، الإرهاب الالكتروني آفة العصر الحديث والآليات القانونية لمواجهة، ط1، دار الفكر الجامعي، الإسكندرية،2018، ص159

أيضا في (إيطاليا) سنة 2009، حيث التقى وزراء العدل والداخلية في روما (28-30 ماي 2009) ، وأصدرت القمة بيان تضمن جرائم الإنترنت والأمن السيبراني ، وأشار البيان الذي قدم لمفوضية منظمة الأمم المتحدة لمنع الجريمة والعدالة الجنائية إلى أن التقدم التكنولوجي أسفر عن إساءة استعمال الشبكات الاجتماعية ، وخدمات التشفير، وأن الهجمات الإجرامية الجديدة المتطورة الأخرى على أنظمة المعلومات تشكل تحديات إضافية تواجه إنفاذ القانون [1]، و في عام 2011 في فرنسا أصدرت الدول الثمانية الجزء الثاني من الإعلان في قضايا الإنترنت في البنود (4 إلى 22) وأكدت فيه أعلى أن شبكة الإنترنت أصبحت ضرورية في كافة أنحاء دول العالم ، حيث تلعب دور في نمو المجتمعات واقتصاديات الدول ومصدر للتعليم وتعزيز الحرية والديمقراطية وحقوق الإنسان، ودعي الإعلان الى تعزيز التعاون داخل جميع المحافل الدولية التي تتناول حركة الإنترنت[2].

ثانيا: المنظمات العالمية المتخصصة

أ) منظمة التعاون الاقتصادي والتنمية (OECD):

تسعى هذه المنظمة بأول مبادرة دولية لها أن تتعامل مع المشكلات المتمثلة بالاعتداء على الأموال المعلوماتية والمتكونة من مجموعة الأدوات المكونة للحاسوب والبرامج والبيانات والتي يترتب عليه مشكلات قانونية، حيث تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية، يظهر اهتمام هذه المنظمة بالجرائم الإرهابية الإلكترونية الدولية ، من خلال وضعها لعديد من الأدلة و القواعد الإرشادية التي تتصل بتقنية المعلومات ، ويعد الدليل المتعلق بحماية الخصوصية و قواعد نقل البيانات من أول الأدلة التي تبناها مجلس

[1]-مجمع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الالكترونية، البحث الحائز على المركز الأول لمسابقة جائزة الأمير نايف عبد العزيز للبحوث الأمنية، عمان،2016، ص ص67-69

[2]- خالد حسن احمد لطفي، المرجع السابق، ص160

المنظمة، مع التوصية الأعضاء بالالتزام بها في سبيل مكافحة جرائم الإرهاب الإلكتروني، كما عملت أيضا على إرسال استبيان إلى الدول الأعضاء فيها لتحديد مفهوم جرائم الحاسوب وتعريفها، مع تبين الأفعال 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،[1] وإصدار تقرير بعنوان الجريمة المرتبطة بالحاسوب وتحليل السياسة الجنائية، إذ استعرض التقرير القوانين الجنائية القائمة، والمقترحات الخاصة من الدول الأعضاء، وتضمن أيضا تقرير الحد الأدنى لأعمال سوء استخدام الحاسوب التي يجب على المجتمع الدولي أن يجزمها ويضع لها عقوبات رادعة للحد منها.

ب) الاتحاد الدولي للاتصالات: تم إنشاء هذه المنظمة بمقتضى اتفاقية باريس عام (1965) تحت اسم اتحاد (التلغراف الدولي)، ثم عدل الاسم ليصبح الاتحاد الدولي للاتصالات السلكية واللاسلكية، إذ انضم الاتحاد الدولي للاتصالات إلى منظمة الأمم المتحدة وأصبح إحدى الوكالات المتخصصة في عمل الاتصالات المنضوية تحت مظلة منظمة الأمم المتحدة، فأصبح بمثابة ملتقى دولي رئيسي لهذه المنظمة، ويضم في عضويته (482) عضوا من الشركات العالمية والصناعية العاملة في القطاعين العام والخاص[2].

في تونس عام 2005 عقدت قمة عالمية لمجتمع المعلومات وضرورة التعاون الدولي في محاربة الجرائم الإرهابية الإلكترونية، التي أكدت على ضرورة تنسيق الاتحاد الدولي للاتصالات آلية لبناء الثقة والأمن في مجال استخدام تكنولوجيا الاتصال والمعلومات، وذلك عبر إطلاق برنامج الأمن الإلكتروني العالمي الذي أعده الاتحاد

[1]–يونس عرب، جرائم الكمبيوتر والانترنت، ط1، اتحاد المصارف العربية، بيروت ،2002، ص322

[2]–خليل حسين، التنظيم الدولي النظرية العامة والمنظمات العالمية، ط1، دار المنهل اللبناني، بيروت، 2010، ص ص454-455

الدولي للاتصالات بهدف اقتراح استراتيجيات للتوصل إلى حلول لتعزيز الثقة والأمن في المجتمع المعلوماتي، ومن أهداف للاتحاد الدول للاتصالات، عقد المؤتمر الدولي حول الأمن الإلكتروني الدولي بالتعاون مع مكتب الاتحاد الدولي للاتصالات في دولة قطر في شباط عام (2008)، وتم دعوة جميع الدول لوضع وتنفيذ إطار قانون الأمن الإلكتروني الدولي، وكذلك حماية البنية التحتية الحرجة للمعلومات، وهذه تعد خطوة أولى في سبيل التصدي للتحديات التي تواجهها الدول جراء اتصالها بتكنولوجيا المعلومات والاتصالات[1].

ج) المنظمة العالمية للملكية الفكرية الويبو(WIPO)

تهدف هذه المنظمة الدولية إلى دعم الملكية الفكرية في جميع أنحاء العالم، وتعد من أهم المنظمات العالمية التي انشات في هذا الشأن، فهي تسعى إلى المساعدة الدولية من أجل حماية حقوق المبدعين وأصحاب الملكية الفكرية بنوعيها الملكية الصناعية والملكية الأدبية والفنية، ومع تزايد الحاجة العالمية لحماية البرامج من خطر الإرهاب الإلكترونية شكلت هذه المنظمة مجموعات عمل تضم عددا من الخبراء بهدف حماية برامج الحاسوب الآلي. ففي عام (1996)، أبرمت اتفاقية ما بين منظمة التجارة العالمية والمنظمة العالمية للملكية الفكرية، وذلك من أجل التعاون المشترك في مجال الملكية الفكرية لاسيما ما يتعلق منها بتطبيق نصوص اتفاقية (تريبس)، وقد عقدت فعلا اتفاقية أولى عام (1998)، تلتها اتفاقية أخرى عام (2001) ، وتهدف اتفاقية (تريبس) في مجملها إلى تعزيز دور الدول المتقدمة واصفاف الدول النامية في مجال الملكية الفكرية ، كما تعمل على إبطال عجلة التقنيات في الدول النامية لاسيما الدول العربية، وذلك بتعزيزها لسيطرة مفهوم الربح على المصنفات الأدبية والفكرية بعيدا عن توخي مفاهيم التوزيع العادل في نشر تلك التقنيات، كذلك فرض حصار تكنولوجي عليها .[2]

[1]–عمر عباس العبيدي، مرجع السابق، ص71

[2]–عمر عباس خضير عبيد، المرجع السابق، ص73–74

المطلب الثاني: الجهود الإقليمية لمكافحة الإرهاب الالكتروني:

بعد تفطن العالم بأسره لمخاطر الإرهاب الالكتروني،باتت مكافحته ضرورة حتمية على المجتمع الدولي، حيث تكاتفت الجهود على المستوى الدولي لتصدي والوقاية من هذا الوباء الخطير، ولقد تطلبت الحاجة إلى اقتراح خطط واستراتيجيات إقليمية، للوقاية منه على الساحة الإقليمية أيضا.

ولدراسة هذه الجهود سنقسم هذا المطلب على ثلاثة فروع ندرس في (الفرع الأول) مكافحة الإرهاب الالكتروني في تشريعات العربية، وفي (الفرع الثاني) مكافحة الإرهاب الإلكتروني في المنظمات الإقليمية. إما في(الفرع الثالث) مكافحة الإرهاب الإلكتروني في المؤتمرات الإقليمية

الفرع الأول: مكافحة الإرهاب الالكتروني في تشريعات الدول العربي

عملت المجتمعات والدول عبر فترات متلاحقة في سن تشريعات ونصوص من اجل مكافحة الجرائم الالكترونية عامة وجرائم الإرهابية الالكترونية خاصة، ولقد انتبهت الدول العربية إلى مخاطر المجال الالكتروني بعد الظروف التي مر بها العالم العربي بما سمي (ثورات الربيع العربي) وما أعقب ذلك من استخدام التنظيمات الإرهابية المتطرفة للفضاء الإلكتروني

أولا: الإرهاب الالكتروني في الجزائر: بعد ما عاشته الجزائر من ويلات الإرهاب في الفترة السابقة أصبحت معروفة بتجربتها في مكافحة الإرهاب، إذ أشاد بها المجتمع الدولي بمجموع الإجراءات التشريعية المتخذة في هذا المجال، وتبعا لنفس السياسة الأمنية تحاول الجزائر مواكبة التطور التكنولوجي بتحصين الترسانة القانونية بمجموعة من الإجراءات في مكافحة الإرهاب الجديد أي الإرهاب الإلكتروني

رجوعا إلى كون الجزائر تحاول تبني فكرة التجارة الإلكترونية في تعاملاتها الاقتصادية المستقبلية، وبما أن الإرهاب الإلكتروني ينشط على نفس مستوى التجارة

الإلكترونية من حيث الوسائل، تدارك المشرع الجزائري الفراغ القانوني في مجال الإرهاب الإلكتروني عموما والإرهاب عبر الانترنيت خصوصا بموجب القانون رقم 04-15 [1]، المعدل لقانون العقوبات.

نجد المادة (394مكرر) تجرم كل دخول غير مصرح به عن طريق الغش على المنظومة المعلوماتية، سواء منس ذلك الدخول أو البقاء في كامل المنظومة أو جزء منها، أما المادة (394 مكرر 1)، تجرم كل عملية إتلاف وتدمير للمعطيات ،وتليها المادة(394 مكرر 2) تجرم كل عملية استيلاء على المعطيات ، كما نصت مواد القسم السابع مكرر من قانون العقوبات، وخاصة المادة (394 مكرر 2) فقرة ثانية على تجريم أفعال الحيازة الإفشاء و النشر التي ترد على المعطيات الآلية، بأهداف المنافسة غير المشروعة، الجوسسة الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة، إضافة إلى ما نصت عليه المادة (394 مكرر 6) بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محل الجريمة من الجرائم المنصوص عليها في القسم السابع من قانون العقوبات[2].

تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة (394 مكرر 6) والمتمثلة في مصادرة الأجهزة والبرامج والوسائل المستخدمة، وإغلاق المواقع والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنيت الذي ترتكب فيه الجرائم بشرط علم مالكه.

أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي:

---

[1]--قانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن قانون العقوبات، جريدة الرسمية، عدد17، الصادر في 2004/11/10

[2]-انظر المادة 394 مكرر 2 ومكرر6، من القانون رقم 04-15 المؤرخ في 2004/11/10 المتضمن قانون العقوبات

-حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة او تخريب النظام.

_إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام.

ولقد دفع القصور الذي عرفه القانون رقم 04-15 والمعدل لقانون العقوبات الذي نص على حماية جزئية نسبية لأنظمة المعلومات ، من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ، بالمشرع الجزائري إلى إصدار القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها جمع هذا القانون بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة و التدخل السريع التحديد مصادرها والتعرف على مرتكبيها [1]

يتضمن القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على 06 فصول أهمها:

الفصل الثاني الذي جسد أحكام خاصة بمراقبة الاتصالات الإلكترونية، وقد راعي في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، إذ نص القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو في حالة توفر المعلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام،أو بمقتضيات التحريات والتحقيق، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[2]

[1]-قانون رقم 09-04 مؤرخ في 2009/02/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47، صادر في 2009/02/16

[2]-انظر المادة 04 من القانون رقم 09-04، المرجع السابق

– أما الفصل الخامس فقد أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة

يعد القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مجالا شاملا في ميدان مكافحة الإرهاب الإلكتروني، إذ جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب على شبكة الانترنيت، وجهاز الحاسوب الآلي.

وفي هذا السياق من الضروري أن تجتهد الدول العربية في وضع قوانين وطنية المكافحة الإرهاب الإلكتروني، وأن تسارع في إصدارها للتزايد الخطير لهذه الظاهرة وما تحمله من تهديدات وآثار تدميرية على الأفراد والمجتمعات وحقوق الإنسان[1]

ثانيا: الإرهاب الالكتروني في القانون الأردني

تصدى المشرع الأردني لتجريم الأفعال الإرهابية الالكترونية المستخدم فيه الحاسوب والانترنت، وذلك من خلال:

أ)الإرهاب بالوسائل الإلكترونية بموجب نص قانون منع الإرهاب

أصدرت الحكومة الأردنية في2006/11/01 قانون منع الإرهاب، الذي شمل التعريف في طياته الإرهاب الالكتروني ، حيث عرف العمل الإرهابي في هذا القانون بأنه : "كل عمل مقصود يرتكب بأي وسيلة كانت يؤدي إلى قتل أي شخص أو التسبب بإيذائه جسديا أو إيقاع أضرار في الممتلكات العامة أو الخاصة أو في وسائط النقل أو البيئة أو البنية التحتية أو في مرافق الهيئات الدولية أو البعثات الدبلوماسية ، إذا كانت الغاية منه الإخلال بالنظام العالم وتعريض سلامة المجتمع وأمنه للخطر أو تعطيل تطبيق أحكام

[1]–انظر المادة 13و 14 من القانون نفسه

الدستور أو القوانين أو التأثير على سياسة الدولة أو الحكومة أو إجبارها على عمل ما أو الامتناع عنه أو الإخلال بالأمن الوطني بواسطة التخويف أو الترهيب أو العنف" . يمكننا القول إن هذا التعريف يشمل بطياته الإرهاب بالوسائل الإلكترونية بشكل ضمني[1].

ب) الإرهاب بالوسائل الإلكترونية بموجب نص قانون جرائم أنظمة المعلومات رقم / 30لسنة 2010:

وبتعدد الجرائم الالكترونية واتساع نطاقها، اضطر المشرع الأردني لإصدار قانون خاص بجرائم أنظمة المعلومات رقم / 30 / لسنة 2010، فقد نصت المادة 10 من هذا القانون على أنه" كل من استخدم نظام المعلومات أو الشبكة أو أنشأ موقعا إلكترونية لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة".وبإمعان النظر فيما تضمنته هذه المادة نجد أنها حصرت مواجهة الإرهاب بالوسائل الإلكترونية بإنشاء مواقع تروج وتدعم الأعمال الإرهابية أو تستخدم وسيلة لتمويلها، وهذه لا تمثل سائر مفردات وصور أنشطة الإرهاب بالوسائل الإلكترونية، وبالتالي يجب على المشرع الأردني ان يتوسع في صور تجريم استخدام نظم المعلومات أو الشبكة أو المواقع الإلكترونية للقيام بأعمال إرهابية ليشمل جوانب الإرهاب بالوسائل الإلكترونية كلها[2]

ثالثا: الإرهاب الإلكتروني في بعض الدول العربية الأخرى

لقد سنت العديد من الدول العربية الأخرى تشريعات وقوانين في إطار تجريم الإرهاب بالوسائل الالكترونية (الإرهاب الالكتروني)[3]:

[1]– نور الله تله، المرجع السابق، ص ص134–135

[2]– نور الله تله، المرجع السابق، ص ص135–136

[3]–رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، دورة تدريبية حول: توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، ص ص 16–17

في سوريا صدر قانون التوقيع الإلكتروني وخدمات الشبكة فضلا عن تقديم قانون مكافحة الإرهاب في 26 جوان 2012 إلى مجلس الشعب السوري، والذي يعرف المنظمة الإرهابية ويجزم العمل الإرهابي وتمويل الإرهاب بما فيها استعمال وسائل الاتصال والمعلومات.

وفي سلطنة عمان المرسوم السلطاني رقم 2007/8 الخاص بقانون مكافحة الإرهاب والذي يشير بصورة ضمنية للإرهاب الإلكتروني كأحد صور الإرهاب، والمرسوم السلطاني رقم 2008/69 الخاص بقانون المعاملات الإلكترونية، كما أصدرت السلطنة قانون مكافحة جرائم الحاسب الآلي.

أما في المغرب فصدر ظهير شريف رقم 1-07-129 صادر في 30 نوفمبر 2007 لتنفيذ القانون رقم 53/05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية،وكذلك القانون رقم 03/03 المتعلق بمكافحة الإرهاب الصادر في 28 ماي 2003 الذي عرف الإرهاب بجميع أشكاله وأشار في البند السابع (7) منه إلى الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.

الفرع الثاني: الاتفاقيات الإقليمية في مكافحة الإرهاب الالكتروني

إن الحماية الفضاء الإلكتروني و الوقاية من ظاهرة الإرهاب عامة و الإرهاب الالكتروني خاصة، تتم من خلال وضع استراتيجيات وسياسات والخطط تندرج في البرامج التنفيذية الوطنية والإقليمية والدولية بوصفها أحد الوسائل الرئيسية لمواجهة جرائم الإرهاب الإلكتروني ، و بعد دراستنا سابقا للاتفاقيات الدولية المبرمة في هذا الشأن سنحاول في هذا الفرع التطرق إلى الاتفاقيات الإقليمية لمكافحة الإرهاب الالكتروني ، حيث إن مجلس أوروبا أول من تبنى مبادرة تشريع اتفاقية لمكافحة الجرائم الإرهابية الإلكترونية عام

(2001) ، وتعد هذه الاتفاقية رائدة لدعم وتعزيز جهود مجلس التعاون لدول الخليج العربي في مكافحة الجريمة الإرهابية الإلكترونية[1].

ولأجل هذا سنقسم هذا الفرع على نقطتين وهما ما يأتي

أولا: اتفاقية الاتحاد الأفريقي لعام 2014

أبرمت هذه الاتفاقية بموافقة رؤساء الاتحاد الأفريقي(AU)عليها وتدخل حيز التنفيذ بمصادقة 15 دولة عليها، ولقد جاءت لتعالج المشاكل الواقعة عبر الإنترنت على هذه القارة كالتجارة الإلكترونية، وحماية البيانات، والجرائم الإرهابية الإلكترونية، والأمن السيبراني إذ تتيح هذه الاتفاقية للدول الأعضاء سن قوانين وطنية بموجب هذه الاتفاقية لمكافحة الجرائم الإرهابية الإلكترونية[2].

ولقد جاء في المادة (18) من هذه الاتفاقية، حماية أصحاب البيانات، ولهم الحق في إخبارهم، قبل أن يتم مشاركة البيانات الخاصة بهم مع أطراف ثالثة، كما نصت المادة (3/25) على الأمن السيبراني وحقوق الإنسان، حيث جاءت أقسام الأمن السيبراني في الاتفاقية لتحمي حقوق الإنسان، ويجب على الحكومات أن تكفل الميثاق الأفريقي لحقوق الإنسان، والشعوب وغيرها من الحقوق الأساسية الأخرى مثل حرية التعبير والحق في الخصوصية، والحق في محاكمة عادلة في القوانين الجديدة ، وجاءت المادة (1/26) ثقافة المجتمع للأمن السيبراني ، وكذلك جاء نص المادة (2/28) لتدعيم سيادة القانون من قواعد الأمن السيبراني، وكذلك إصرار الاتفاقية على أن توقع الحكومات اتفاقية المساعدة القانونية المتبادلة، وذلك لوضع المعايير الدولية لتبادل البيانات بطريقة فعالة، وكذلك حظرت الاتفاقية استخدام الحاسوب الآلي للإساءة لشخص ما الأسباب العرق أو الدين أو الأصل القومي العرقي أو الديني أو الرأي السياسي، وكذلك يجب على (15)

[1]–عمر عباس خضير العبيدي، المرجع السابق، ص58

[2]–درار نسيمة، الامن المعلوماتي وسبل المواجهة مخاطرة في التعامل الالكتروني، دراسة مقارنة، أطروحة الدكتورة، كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد تلمسان الجزائر، 2017. ص ص 285–286

دولة من دول الأعضاء ال (54) أن تشير إلى الاتفاقية في أحكامها، ثم يجب أن تمرر القوانين المنفذة للاتفاقية في كل دولة من الدول الأعضاء وتنشر على الإنترنت[1].

ثانيا: الاتفاقيات العربية لمكافحة الإرهاب الإلكتروني

سنتناول الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010 والقانون العربي الإسترشادي لمكافحة تقنية المعلومات وما في حكمها لعام 2004على النحو الآتي:

1) الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010

توصلت جهود العربية في مكافحة الجرائم الإرهابية الإلكترونية إلى توقيع اتفاقية عربية لمكافحة جرائم تقنية المعلومات في نهاية عام (2010)، والتي تهدف إلى تعزيز التعاونبين الدول العربية في مجال مكافحة الجرائم الإرهابية الإلكترونية، وتتكون هذه الاتفاقية من (43) مادة، منها (21) مادة في باب التجريم، وثمانية مواد إجرائية تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين ، وضبط المواد المخزنة على الحواسيب الشخصية والأجهزة التقنية ويتكون الفصل الرابع من (14) مادة تنظم التعاون بين الدول الأعضاء في تبادل معلومات المستخدمين، حيث يكون نطاق سريان هذه الاتفاقية إقليميا [2]. وتضمنت الاتفاقية المذكورة الأحكام الموضوعية والمتمثلة في تجريم الأفعال المكونة الجرائم تقنية المعلومات وهي الاختراق، والاعتراض، والاعتداء على سلامة البيانات والملكية الفكرية، وإساءة استخدام وسائل تقنية المعلومات، والتزوير، والاحتيال، والإباحية، وجرائم تقنية المعلومات المتعلقة بالإرهاب الإلكتروني، وغسل الأموال والمخدرات، والإتجار بالجنس البشري والأسلحة، والاستخدام غير المشروع

[1]–درار نسيمة، المرجع سابق، ص ص288–289

[2]–صفاء كاظم غازي الجياشي، جريمة قرصنة البريد، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة بابل، العراق،2016، ص46

الأدوات الائتمان والوثائق الإلكترونية ، فضلا عن تشديد العقوبات على الجرائم التقنية التي ترتكب بواسطة تقنية المعلومات [1].

فقد تضمنت المادة (11) من هذه الاتفاقية التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع، فضلا عن ذلك تجريم أفعال إنتاج أو عرض أو توزيع أو تشفير أو نشر أو شراء أو بيع أو استيراد مواقع إباحية أو مخلة بالحياء بواسطة تقنية المعلومات، وكذلك تم تجريم المقامرة والتحريض على الدعارة والفجور وجرائم الآداب العامة، بالإضافة إلى الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد أو التشهير والسب والقذف والإساءة إلى السمعة بواسطة تقنية المعلومات[2].

وكذلك تضمنت المادة (10) من الاتفاقية العربية لتقنية المعلومات على أنه الجرائم المتعلقة بالإرهاب والمرتبة بواسطة تقنية المعلومات ومنها ما يأتي:[3]

1-نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.

2-تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.

3-نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.

4 -نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

[1]-رامي متولي القاضي، مكافحة الجرائم المعلوماتية في تشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة،2011، ص75

[2]-المرجع نفسه، ص76

[3]-المرجع نفسه، ص ص76-77

2) القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام2004:

توجت جهود الدول العربية لمواكبة التطورات التكنولوجية والمعلوماتية التي يشهدها العالم بإصدار قانون عربي نموذجي موحد لمكافحة جرائم تقنية المعلومات ، ولقد اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما يسمى بقانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها ، وتم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم (495 / د 19- 2003/10/8) كما تم اعتماده من مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (418/د2004/31) ويتكون هذا القانون من (27) مادة [1].

ووفقا للقانون المذكور يمكن تجريم الأفعال الآتية، واعتبارها من جرائم الإرهاب الإلكتروني إذا مست مصالح محمية قانونا:

. الدخول غير المشروع بقصد إلغاء أو حذف أو تدمير أو إنشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية[2].

– إعاقة أو تشويش أو التعطيل العمد وبأي وسيلة عن طريق الشبكة المعلوماتية او أحد أجهزة الحاسوب الآلي وما في حكمها، والوصول إلى الخدمة أو الدخول الى أجهزة أو برامج أو مصادر البيانات أو المعلومات[3].

[1]–محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت والأحكام الموضوعية والأحكام الجزائية، ط1، منشورات حلبي الحقوقية، بيروت، 2011، ص125

[2]–انظر المادة 3 من القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها والصادر عن الأمانة العامة لجامعة الدول العربية، (القرار 2004/417)

[3]–انظر المادة 7 من القانون العربي الإسترشادي لمكافحة جرائم التقنية أنظمة المعلومات وما في حكمها

. استعمال الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها من تهديد أو ابتزاز الشخص آخر لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعا[1].

. استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقة ائتمانية وما في حكمها بقصد استخدامها في الحصول على بيانات الغير أو أمواله[2].

إنتاج أو إعداد أو إرسال أو خزن ما من شأنه المساس بالنظام العام أو الآداب العامة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي[3].

– إنشاء أو نشر موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها بقصد الإتجار بالجنس البشري أو تسهيل التعامل فيه.[4]

– إنشاء أو نشر موقع على شبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها وأعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أدوات تستخدم في الأعمال الإرهابية[5].

– الدخول العمد بغير وجه حق إلى موقع أو نظام مباشر أو عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسوب الآلي وما في حكمها بقصد الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو بث أفكار تمس ذلك[6].

---

[1]– انظر المادة 9 من القانون العربي الإسترشادي لمكافحة جرائم التقنية أنظمة المعلومات وما في حكمها

[2]–انظر المادة 10 من القانون نفسه.

[3]–انظر المادة 13 من القانون نفسه.

[4]– انظر المادة 17 من القانون نفسه.

[5]–انظر المادة 21من القانون نفسه.

[6]–انظر المادة 32من القانون نفسه.

الفرع الثاني: مكافحة الإرهاب الالكتروني في منظمات الإقليمية

رغم أن التشريعات الإقليمية ومنها التشريعات العربية، متأخرة في مواكبة المستجدات التشريعية العالمية المتعلقة بجرائم الحاسوب الآلي الهادفة إلى حماية المعلوماتية من جرائم الإرهاب الإلكتروني، إلا أنها أدت دورا بارزا في مكافحته من خلال جهود السوق الأوربية المشتركة، فصدر عن البرلمان الأوروبي عدة قرارات منها القرار (1979/4/8) الخاص في حماية الفرد في مواجهة التطور المعلوماتي[1]، وفي إطار الجهود الدولية ظهرت منظمات إقليمية على غرار منظمة الأمم المتحدة ساهمت في مكافحة الإرهاب الإلكتروني، إذ كان أبرز هذه المنظمات الاتحاد الأوروبي.

وسنتناول من خلال هذا الفرع نقطتين كما يلي.

أولا: لاتحاد الأوروبي في مكافحة الإرهاب الإلكتروني:

لقد بذل الاتحاد الأوروبي جهود فعالة لمكافحة الجرائم الإرهابية الإلكترونية بكل أشكالها، ففي عام (1981) أثمرت هذه الجهود بتوقيع دول الاتحاد على اتفاقية تتعلق بحماية الأشخاص في مواجهة المعالجة الإلكترونية ذات الصبغة الشخصية، و من أهم الجهود التي بذلها الاتحاد الأوربي لمواجهة الجريمة الإلكترونية ومكافحتها هي وضع قواعد إرشادية عام (1985) خاصة بتحديد أنماط جرائم الحاسوب، ونبهت هذه القواعد المشرعين إلى ضرورة تحديد الأنشطة غير المشروعة المرتبطة باستخدام الحاسوب الآلي ، وعلى ضرورة التوازن بين مواجهة الحاجة للحماية الجنائية ضد هذه الأنشطة من جهة وحماية الحق في المعلومات وحريات الأفراد من جهة أخرى[2].

[1]–وليد الزيدي، القرصنة على الانترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة لنشر والتوزيع، الأردن،2003، ص128

[2]–صغير يوسف، الجرائم المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري، الجزائر، 2013، ص101

وفي عام (1989) أصدر الاتحاد الأوروبي توصيات خاصة بالجرائم الإرهابية الإلكترونية، وتمت الموافقة عليها من لجنة وزراء المجلس الأوربي، وتضمنت الحد الأدنى من الأنشطة غير المشروعة المتعلقة بالحاسوب ودعت إلى تجريمها وتمثلت هذه الأنشطة بما يأتي[1]:

1-التواصل غير المرخص به بما في ذلك التغلب على الإجراءات أو التدابير الأمنية والاعتراض غير المرخص لإرسال البيانات سواء كان ذلك من داخل النظام أو خلافه.

2-تجريب البيانات أو البرامج .

3-غش الحاسوب وتزويره.

4-إعادة الإنتاج غير المرخص لبرامج الحاسوب.

وبعد انتباه الاتحاد الأوروبي لضرورة وضع إطار قانوني عام للجرائم الإرهابية الإلكترونية، ولذلك شكلت لجنة الخبراء الفحص الجرائم الإرهابية الإلكترونية ، وتوفير حماية أكثر فاعلية من الناحيتين الإجرائية والموضوعية ، وتساعد هذه اللجان العديد من اللجان الفرعية المتخصصة في التقنية المعلوماتية والمكلف بإجراء الدراسات البحثية والمسحية، وفي (25 أفريل2000)، اجتمع مجلس الاتحاد الأوروبي في "ستراسبورغ " ووجهة الدعوة إلى حماية المجتمعات الأوربية من الجرائم الإرهابية الإلكترونية ووضع التشريعات الملائمة لمكافحتها، بالنص على تجريم الأفعال التي تشمل إتلاف قواعد البيانات ووظائف الحاسوب الآلي وأنظمته أو التزوير فيها أو الاحتيال وعقوبة المتسبب بذلك، حتى الشروع في مثل هذه الجرائم والمساهمة فيها، وضمان التعاون الدولي في مجال التحقيق وتبادل المعلومات لتحقيق الأمن الإلكتروني، وكل هذا بعد أن توجت جهود

[1]-مريم محمد حسن، التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، كلية القانون، جامعة كوفة، العراق،2016، ص169

الاتحاد الأوربي في إصدار اتفاقية تتعلق بالجرائم المعلوماتية اتفاقية بودابست السنة (2001) .[1]

ومن الجهود الأوربية أيضا اهتمام لجنة الوزراء الاتحاد الأوروبي بالمشكلات الخاصة بالجرائم الإرهابية الإلكترونية من خلال الإشارة في توصياتها المتعددة إلى تشجيع الدول الأوروبية على تبني سياسات مشتركة تهدف إلى تحقيق التفاهم والتعاون في مكافحة جرائم الإرهاب الإلكتروني، ومن هذه التوصيات توصية رقم (85/10) الخاصة بالتطبيق العملي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية، وبشأن اعتراضا لاتصالات السلكية واللاسلكية ، والتوصية رقم (88/2) بشأن القرصنة في مجال التأليف والحقوق المجاورة وحقوق النشر، والتوصية رقم (87/15) التي تنظم استخدام البيانات الشخصية في قطاع الشرطة، والتوصية رقم (95/4) بشأن حماية البيانات الشخصية في مجال خدمات الاتصال وخاصة الخدمات التليفونية، وكذلك التوصية رقم (89/9) بشأن الجرائم المتعلقة بالكمبيوتر التي تقدم الإرشادات للهيئات التشريعية الوطنية فيما يتعلق بتعريف جرائم معينة تتعلق بالكمبيوتر، وأخيرا التوصية رقم (13/95) التي تتعلق بمشكلات قانون الإجراءات الجنائية ذات الصلة بتكنولوجيا المعلومات[2].

ومن الجهود الأوروبية لمكافحة الإرهاب الإلكتروني أيضا، ما أشار إليه القرار الصادر عن مؤتمر وزراء العدل الأوروبيين الحادي والعشرين الذي عقد في " براغ" (11.10/ 6 / 1997) الذي أوصى لجنة الوزراء بدعم العمل الخاص باللجنة الأوروبية فيما يتعلق بتحقيق التقارب بين القوانين الجنائية للدول الأوروبية بشأن الجرائم الإرهابية الإلكترونية ، ويعود لهذا القرار الفضل بالتمكن من استخدام الوسائل التقنية الفعالة في البحث والتحقيق في هذه الجرائم وكذلك القرار الصادر عن مؤتمر وزراء العدل الأوروبيين

[1]–خالد حسن احمد لطفي، المرجع السابق، ص176

[2]– رامي متولي القاضي، المرجع السابق،64–65

الذي عقد في لندن (2000/6/8.9)، والذي تضمن حث الدول الأوروبية على متابعة الجهود لإيجاد الحلول الملائمة لتمكين الدول الأوروبية من الانضمام إلى اتفاقية بودابست لسنة (2001)، والإقرار بضرورة الحاجة إلى التعاون الدولي بشأن مكافحة جرائم الإرهاب الإلكتروني .[1]

ثانيا: جهود جامعة الدول العربية لمكافحة الإرهاب الإلكتروني:

تصدت جامعة الدول العربية كمنظمة إقليمية عربية للأنشطة غير المشروعة المرتكبة بواسطة تقنية المعلومات، وان ميثاقها لا ينص صراحة على مكافحة الإرهاب وما يرتبط به من تفرعات، ولكن المادة (02) منه أوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها، وهذا ما يتقاطع بالضرورة مع ما تنطوي عليه وسائل الإرهاب الإلكتروني من تجاوزات وإخلال السلطة وسيادة الدول عبر التعرض لنظم المعلومات المرتبطة بالمؤسسات السيادية ، فضلا عن إمكانية استغلال المعلومات الحساسة وتوظيفها ضد مصالح الدول العربية المستهدفة، الأمر الذي يستدعي الدول العربية لمواجهة مثل هذه الأنشطة الإرهابية عبر 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 والسلام ، 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] .

إن اهتمام جامعة الدول العربية يبدو متأخرا على صعيد العمل الميداني، حيث بدأت عام (1983) الجهود العربية المشتركة في مكافحة الإرهاب بالتوصل إلى الإستراتيجية

[1]–رشيد صبحي جاسم محمد، الإرهاب والقانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة بغداد، العراق، 2003، ص208

[2]–خالد حسن احمد لطفي، مرجع السابق، ص177

الأمنية العربية التي أقرها مجلس وزراء الداخلية العرب، والتي تضمنت ضرورة الحفاظ على أمن المواطن العربي من المحاولات العدوانية للإرهاب والتخريب الموجهة من الداخل والخارج، وفي إطار الخطة الأمنية تشكلت لجنة الجرائم المنظمة وتناولت في اجتماعها الأول موضوع جرائم الإرهاب الإلكتروني[1].

أسفرت جهود الجامعة العربية للتصدي للأنشطة غير المشروعة بواسطة التقنية الإلكترونية،عن إصدار مجلس وزراء العرب القرار رقم (229سنة 1999) متعلق بإصدار القانون الجزائي العربي الموحد كقانون عربي نموذجي، إذ أن أبرز 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 فصلا خاصة بالاعتداء على حقوق الأشخاص الناتج عن المعلوماتية[2].

إن المحاولات والجهود العربية متواصلة لسد الفراغ التشريعي الحاصل في القوانين الجنائية الموجودة ، ومن أجل مواجهة هذا النوع من الجرائم المستحدثة ، فلقد خصصت الجامعة العربية الاجتماع الثاني عشر للجنة المختصة بالجرائم المستحدثة في عام (2009) لموضوع (التزوير في مجال بطاقات الائتمان)، وقد أعدت الأمانة العامة لجامعة الدول العربية مشروع اتفاقية عربية حول جرائم الحاسوب تنفيذا للتوصية الصادرة عن الاجتماع الحادي عشر للجنة المختصة بالجرائم المستحدثة، وقد تمت المناقشة من قبل لجنة مشتركة من مجلسي وزراء الداخلية والعدل العرب، إذ عقدت حتى الآن عدة اجتماعات الوضع المشروع في صيغته النهائية في ضوء ملاحظات الدول الأعضاء، حيث يذكر إلى أنه الحد الآن لم تتكلل هذه الجهود باعتماد هذه الاتفاقية [3].

---

[1]–سامر مؤيد عبد اللطيف، الإرهاب الالكتروني وسبل مواجهته، بحث منشور في مجلة كربلاء العلمية، العدد 14، العراق، 2016، ص31

[2]–عمر عباس خضير العبيدي، المرجع السابق، ص80

[3]–رامي متولي، المرجع السابق، ص74–75

المبحث الثاني: آليات مواجهة الإرهاب الالكتروني

شكلت قضية مكافحة الإرهاب بصورته التقليدية أهم قضايا التي ركزت عليها أغلب الأجندات الأمنية للدول على مدار سنوات طويلة، غير أنه مع التطورات التكنولوجية التي شهدها العالم حديثا وقع تغيير كبير سواء على مستوى تطور الظاهرة أو على مستوى آليات المكافحة، فلم تعد ظاهرة الإرهاب مقتصرة على جانبها التقليدي فقط بل تعدته التشمل ظاهرة الإرهاب الالكتروني كأحد أخطر الجرائم التي برزت بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكارا هدامة تدعو إلى العنف والتطرف، ما أدى إلى دق ناقوس الخطر لدى السلطات و المؤسسات الدولية للبحث عن الآليات و التدابير لمكافحة والوقاية من هذا الوحش الذي يترصد بكافة المجتمع الدولي .

وسنحاول من خلال هذا المبحث دراسة طرق وتدابير مكافحة الإرهاب الالكتروني فخصصنا (المطلب الأول) لمكافحة الإرهاب الالكتروني فنيا و (المطلب الثاني) لمكافحة الإرهاب الالكتروني قانونيا، عسكريا فكريا

المطلب الأول: مكافحة الإرهاب الالكتروني فنيا

يعد الإرهاب الالكتروني تحديا امنيا، تعمل الدول على مواجهته والحد منه وذلك عن طريق استخدام مجموعة من الإجراءات الفنية التقنية والتدابير الاحترازية الوقائية التي يمكن لها أن تقلل بشكل كبير من مخاطر هذا الإرهاب، وتتمثل هذه الإجراءات في إجراءات الحماية الفنية الأساسية التي سنتناولها في (الفرع الأول) وأنظمة الحماية الفنية من الاعتداءات الالكترونية في (الفرع الثاني)

الفرع الأول: إجراءات الحماية الفنية الأساسية

إن استخدام مجموعة من الإجراءات الأساسية يمكن لها أن تقلل بشكل كبير من مخاطر الإرهاب بالوسائل الإلكترونية والجريمة المعلوماتية، وتوفير بيئة إلكترونية آمنة

نسبية، وتتمثل هذه الإجراءات التي يجب مراعاتها: التدريب ونشر الوعي الإلكتروني، وتفعيل الرقابة الإلكترونية وأنظمة الحجب والترشيح [1]

أولا:التدريب والتوعية

تتطلب مكافحة الإرهاب الالكتروني في الفضاء الإلكتروني، مواجهته من خلال تدريب المسؤولين عن مكافحة الإرهاب على استيعاب السياسات الأمنية الإلكترونية، والتركيز على دحض أفكار الإرهابيين وعزلهم عن المجتمع، مع بث أفكار مضادة لما يروجون له، من خلال إنشاء مواقع التوعية العديدة وعدم ترك الساحة الإعلامية ساحة حرة لهم[2].

أ): التدريب

إن التدريب مقوم أساسي لبناء الخبرات والمهارات، خاصة في ظل التقدم المتواصل لتكنولوجيا الحاسب الآلي والإنترنت، الأمر الذي يفرض على جهات إنفاذ القوانين، وخاصة المسؤولة عن مكافحة الإرهاب، أن تسير في خطوات متناسقة مع هذا التطور، حتى يتم التصدي للجرائم الإلكترونية والإرهاب بالوسائل الإلكترونية.

فيجب أن يكون رجال القضاء والنيابة العامة على درجة كبيرة من الإلمام بالحوسبة الرقمية والكفاءة والمعرفة والقدرة على متابعة الجرائم الإلكترونية والإرهاب الإلكتروني، واستخلاص الأدلة منها، وهذا لا يتم إلا بالتدريب الذي يشمل جوانب الجرائم الإلكترونية كلها، من حيث كيفية إنشاء المواقع وإدارة الشبكات ونقاط الضعف وأماكن الاختراق الشبكات المعلومات وطرق الحصول على أدلة والتعاون الدولي في هذا المجال[3].

[1]– نور الله تله، المرجع السابق ص164

[2]– المرجع نفسه، ص163

[3]– فراس طحان، الإرهاب الالكتروني وسبل مكافحته، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، العدد الثاني ،2011، ص379

ب) إنشاء مواقع التوعية

للجماعات الإرهابية مواقع عديدة على شبكة الإنترنت، وتبث من خلالها جميع الأفكار الضالة والسامة، وتعمل جاهدة على استقطاب أكبر عدد من الشباب، وبالتالي تجدر الإشارة إلى أهمية عدم ترك الساحة الإلكترونية لتلك الجهات، أي ضرورة إيجاد البديل القوي والمنافس على شبكة الإنترنت، والبدء بإنشاء المواقع والمنتديات التي تخدم المجتمع وتنير أفكار الشباب وتحارب الجماعات الإرهابية وتكشف كذب ما يروجون له من أفكار هدامة،هذا من جهة ، وتعمل على تثقيف المستخدمين الذين يستخدمون شبكة الإنترنت من جهة أخرى لتجنب مخاطر الإرهاب الالكتروني والوصول للاستخدام الأمثل لشبكة، أي نشر الوعي التكنولوجي بكيفية التعامل مع الإنترنت والحاسوب .

فعادة لا يهتم المستخدم بحيثيات الحماية مما يتسبب بنتائج غير مرغوبة، بل علاوة على ذلك غالبا ما يعد المستخدمين إجراءات الحماية ضربا من الإزعاج أكثر منه مساعدة ووقاية. أي أنه كما يستطيع الإرهابيين استخدام شبكة الإنترنت بكفاءة، كذلك يستطيع صانعو السلام، استخدام الإنترنت لمجابهتهم، والمقصود هو نشر الأفكار السامية والمتحضرة التي تدعو إلى السلام والمحبة والتعايش السلمي، أي ما يسمى المواجهة اللينة مع الإرهاب عبر دحض أفكاره، وعزله عن المجتمع، مع بث أفكار مضادة لما يروج له الإرهابيين، وإتاحة الفرصة أمام حرية التعبير [1]

ج) تفعيل دور الإعلام

ضرورة الإقرار بأهمية دور وسائل الإعلام الرسمية وغير الرسمية في بلورة إستراتيجية للتصدي لمزاعم الإرهابيين وتشجيع وسائل الإعلام على وضع قواعد إرشادية للتقارير الإعلامية والصحفية مما يحول دون استفادة الإرهابيين منها [2].

[1]– نور الله تلة، المرجع السابق، ص ص164-165

[2]– المرجع نفسه، ص166

حيث يعمل الإرهاب بالوسائل الإلكترونية على خدمة البعد الإعلامي للجماعات الإرهابية، من خلال استخدام شبكة الإنترنت كحاضن لنشاطها الإعلامي، فالجماعات الإرهابية لا يهمها عدد الضحايا الذين قتلوا بقدر ما يهمها كم من الناس شاهدوا وتفاعلوا مع الحادثة الإرهابية، كما يعمل أيضا على تضخيم الصورة الذهنية القوة وحجم الجماعات الإرهابية،ويلعب الإعلام دور محوريا مهما في مكافحة الإرهاب بالوسائل الإلكترونية، فلا يجب أن يقتصر دور الإعلام على الإعلام الموجه ضد الجماعات الإرهابية، إنما يجب أن يمتد ليشمل وضع ضوابط خاصة بالتغطية الإعلامية للجماعات الإرهابية، مثل عدم التوسع والمبالغة في نشر التهديدات الصادرة عن الجماعات الإرهابية من خلال شبكة الإنترنت، نظرا لما يتركه ذلك من أثار سلبية في نفوس الجمهور، وأيضا عدم تسليم وسائل الإعلام بكل ما ينشر من قبل الإرهابيين على المواقع الإلكترونية، وعدم عدها من مصادر الإعلام الموثوقة[1] .

ثانيا: تفعيل المراقبة الإلكترونية وأنظمة الحجب

من الضروري على الحكومات والدول فرض الرقابة والسيطرة على كل ما يقدم من خلال شبكة الإنترنت، في إطار إيجاد بيئة إلكترونية خالية من الجريمة والإرهاب

أ) المراقبة الإلكترونية

يجب على الدول فرض رقابة على كل ما يقدم عبر شبكة الإنترنت، لمنع الدخول للمواقع التي يتضمن محتواها مواد تتعلق بالإرهاب، فضلا عن مراقبة الاتصالات عبر شبكة الإنترنت والبريد الإلكتروني بهدف ضبط المجرمين وتفتيشهم، وجمع الأدلة لإدانتهم وتقديمهما للمحاكمة.

ويجب أن تكون هذه المراقبة مشروعة وتحقق التوازن بين حق الأفراد في الخصوصية وحق المجتمع في مكافحة الجريمة.

[1]–سعد عطوة الزنط، الإرهاب الالكتروني وإعادة صياغة استراتيجيات الأمن القومي، مؤتمر الجرائم المستحدثة. كيفية إثباتها ومواجهتها، مصر، 15–16ديسمبر 2010، ص22

لا تعني الرقابة المنع من استخدام شبكة الإنترنت، لكنها تدبير وقائي،لمنع وقوع الجرائم، فالرقابة على الإنترنت هي التحكم في النشر والوصول إلى المعلومات على الإنترنت، وتستخدم الرقابة تقنية تعتمد على الجدار الناري أو البروكسي، ويتم ذلك من خلال إجبار المتعاملين مع الشبكة على المرور عبر خوادم البروكسي قبل الوصول إلى الشبكة.

فمزودات خدمة الإنترنت تتسلم وتنظم كل الطلبات، وتستخدم برامج تحسس الرقم الخاصIP، مما يعطي بعض البيانات عن المستخدم حتى لو استخدم اسم وهمي لدخول الشبكة، ويوجد برامج عدة للمراقبة الإلكترونية وبرامج متخصصة بجمع الأدلة والقرائن من رسائل البريد الإلكتروني. فعلى سبيل المثال، توظف الصين مليوني شخص لمراقبة الأنشطة على شبكة الإنترنت، حيث تعد شبكة الإنترنت في الصين من أكثر الشبكات التي تشهد سيطرة ورقابة حكومية صارمة في العالم، حيث تعد مواقع الإنترنت تحت الرقابة الجبرية الدائمة، بل وصل الأمر إلى حد التدخل لحذف التعليقات ذات الحساسية بصورة روتينية على مواقع الشبكات الاجتماعية[1].

ب) أنظمة الحجب

من أهم ما يجب توافره في هذا الصدد حجب المواقع الضارة التي تدعو إلى الشر والفساد، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق، والقيام بالإجراءات كلها بما في ذلك ترشيح المحتوى[2].

ولقد جاء في بعض الدراسات أن الدول التي تفرض قوانين صارمة في منع المواقع الضارة والهدامة تنخفض فيها نسبة الجرائم[3].

[1]– نور الله تلة، المرجع السابق، ص 167–168

[2]–عبد الرحمن بن عبد الله سند، المرجع السابق، ص23

[3]– المرجع نفسه ، ص24

الفرع الثاني: أنظمة الحماية الفنية من الاعتداءات الالكترونية

تتم الحماية الفنية من الاعتداءات الإلكترونية سواء كانت إرهابية أو غيرها، بوسائل فنية عدة منها[1]:

– تشفير البيانات المهمة المنقولة عبر الإنترنت، سواء كانت منقولة عبر وسائل الاتصالات أو عبر الألياف البصرية، بحيث يتم تشفير البيانات، ثم إعادتها إلى وضعها السابق عند وصولها إلى الطرف المستقبل، ويتم اللجوء إلى تشفير البيانات والمعلومات إذا كانت مهمة، لأن عملية التشفير مكلفة.

– إيجاد نظام أمنى متكامل يقوم بحماية البيانات والمعلومات.

– توفير برامج الكشف عن الفيروسات لحماية الحاسب والبيانات والمعلومات من الإضرار بها.

– عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية.

– عمل نسخ احتياطية من البيانات تخزن خارج مبنى المنظمة.

– استخدام وسائل حديثة تضمن دخول الأشخاص المصرح لهم فقط إلى أقسام مركز الحاسب الآلي، كاستخدام أجهزة التعرف على بصمة العين، أو اليد أو الصوت.

–استخدام كلمة مرور ، حيث تعد كلمة المرور من أبسط أشكال الحماية ويفضل اختيار كلمة مرور ذات بنية قوية ، ويجب مراعاة تغييرها الدوري. وسندرس في هذا الفرع عن بعض هذه الوسائل بشيء من الإيجاز.

أولا: نظام التحقق من الهوية

يشير مفهوم التعرف بالهوية إلى التعرف الإيجابي الدقيق بهوية مستخدمي الشبكة ومضيفاتها، وتطبيقاتها، وخدماتها، ومصادرها.

[1]– عبد الرحمن بن عبد الله سند، المرجع السابق، ص29

يوجد تقنيات عدة للتحقق من الهوية وخصوصا أساليب التحقق البيولوجي من الهوية، بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص، حيث تعتمد هذه الأنظمة على تسجيل معلومات عن بصمات الأصابع والوجوه،والأصوات، وقزحية وشبكية العين، التوقيع اليدوي، وغيرها.

يمكننا أن ننظر إلى هذه التقنية على أنها تعتمد على شيء لا يمكن نسيانه أو فقده أو تركه في مكان غير آمن، مثل البطاقات الممغنطة أو كلمات السر.

لكن تبقى كلمة السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعا للتحقق من الهوية، وهنالك وسائل كثيرة يمكن إن استخدامها، تعتمد هذه الوسائل أساسا على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم.[1]

ثانيا: خدمات الأدلة

برمجيات خدمات الأدلة هي عبارة عن قواعد بيانات خاصة، ذات مستوى عال من الأمان عادة، ومصممة لجمع وإدارة المعلومات المتعلقة بمستخدمي الشبكة، ولا يقتصر دور هذه البرمجيات على جمع كلمات السر وأسماء المستخدمين، بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين، ويتم استخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بمكوناتها جميعها كالتطبيقات، والأجهزة الخادمة،والمجلدات، وحتى شكل الشاشة التي يستعملها المستخدم، وتدار كلها بشكل مركزي من مكتب مدير الشبكة دون الحاجة للقيام بأية زيارات إلى الأجهزة أو المستخدمين[2].

ثالثا: استخدام التشفير لحماية المعلومات الهامة

يعتبر التشفير عملية تحويل المعلومات إلى شيفرات غير مفهومة، تبدو بدون معني، لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة.

---

[1]–نور الله تله، المرجع السابق، ص175–176–

[2]–حسن بن احمد الشهري، المرجع السابق، ص17

يعتبر التشفير سلاح ذو حدين، حيث أنه يوفر الحماية للبيانات، لكن إذا فقد المفتاح السري أو البرنامج الذي شفر المحتوى، فلا فائدة ترجى من المحتوى المشفر[1].

رابعا: الجدار الناري:

هو فلتر يسمح بالتعاملات والتبادلات المرغوب فيها فقط، حيث تعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالاعتماد على مجموعة من السياسات، حيث تقوم بتصفية حركة حزم البيانات بالسماح بمرور الحزم الواردة من المصادر المعروفة والموثوق بها، ومنع الحزم الواردة من جميع المصادر الأخرى وكذلك السماح بتشغيل الخدمات اللازمة لأعمال المؤسسية ومنع تشغيل الخدمات الأخرى[2].

ويوجد ضمن فئة الجدران النارية صنفان،الأول: هو الجدران النارية المؤسسية التي تقوم بحماية تطبيقات المؤسسات،والثاني: هي الجدران النارية الشخصية، والجدران النارية في تطور مستمر وذلك ردا على تطور القراصنة ومحاولات اختراقها أو تعطيلها[3].

خامسا:الشبكات الافتراضية الخاصة

لا توجد طريقة أكثر أمنا من الشبكات الافتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى الشبكة، وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ من خلالها إلا من يقوم بتحديده مدير الشبكة، وفي هذه الحالة يمكن للمستخدمين المعينين النفاذ إلى الشبكة عبر الإنترنت، وإسقاط الحزم الواردة من أية جهات أخرى غير هؤلاء المستخدمين[4].

---

[1]–نور الله تله، المرجع السابق، ص176–178

[2]– زكريا احمد عامر، حماية الشبكات الرئيسية من الاختراق والبرامج الضارة، رسالة ماجستير، جامعة النيلين، كلية الدراسات العليا، السودان، 2011، ص39

[3]– نور الله تلة، المرجع السابق، ص179

[4]– سعيد عطوة الزنط، المرجع السابق، ص16

المطلب الثاني: مكافحة الإرهاب الالكتروني قانونيا، فكريا، عسكريا

رغم أهمية إجراءات الحماية الأساسية وأنظمة الحماية الفنية من الاعتداءات الإلكترونية وضرورة تواجدها، إلا أنها لا تكفي لجعل الإنترنت مكانا أمنا، حيث كشف الواقع أن أكبر الأنظمة المعلوماتية، وأكثرها توفيرا الحماية الفنية تم اختراقها، فلا بد من طرق أخرى تساعد في مواجهة هذا الإرهاب.

وسنتناول في هذا المطلب طرق أخرى لمواجهة الإرهاب الالكتروني حيث سندرس في (الفرع الأول) مواجهة الإرهاب الالكتروني قانونيا وفي (الفرع الثاني) مواجهته فكريا و (الفرع الثالث) مواجهته عسكريا

الفرع الأول: مواجهة الإرهاب الالكتروني قانونيا

سنت العديد من دول العالم قوانين لمكافحة الجرائم الإلكترونية بعد أن ظهر جليا مدى سرعة انتشارها و فداحة الخسائر الناتجة عنها وأجمع أغلب هذه القوانين أن هذه الجرائم ما هي إلا تعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام الوسائل التقنية وخصص جزء كبير من هذه القوانين لعقوبات رادعة لجرائم الإرهاب الالكتروني الذي يمتد أثره ليس على دولة معينة بحد ذاتها بل يمتد ليشمل المجتمع الدولي بأسره و فيما يلي بيان أسماء بعض دول العالم التي ست قوانين لمكافحة هذه الجريمة [1]

السويد، الولايات المتحدة الأمريكية،أستراليا،كندا،الصين، مقاطعة هونج كونج التابعة للصين، مملكة الدنمارك، فرنسا، ألمانيا، جمهورية إيرلندا.الهند، اليابان وغيرها العديد- من دول العالم التي أضافت إلى قانونها الجزائي ملحقا خاص المكافحة الجرائم الإلكترونية ومنها (لبنان،البحرين،الجزائر،المغرب،تونس،الأردن،مصر،السودان وهناك ثلاث دول

[1]–حسن بن احمد الشهري، الإرهاب الالكتروني حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد الرابع، العدد الثامن، 2015، ص20

عربية فقط هي السعودية والإمارات وعمان التي سنت قوانين مستقلة لمكافحة الجرائم المعلوماتية[1].

ولقد سعت معظم هذه الدول إلى مكافحة ومواجهة الإرهاب الالكتروني بشتى الطرق حيث[2]

– قام الإنتربول بأعضائه المائة وثمان وسبعين بعمل جبار لمحاربة جرائم الإرهاب الإلكتروني خاصة والجرائم الالكترونية عامة،وتقييم العديد من الدورات الأعضائه وكذلك العديد من مجالات التدريب.

– مجلس أوروبا في إطار سعيه لمواجهة الجرائم الإلكترونية سن القانون الإسترشادي لمكافحة جرائم الحاسب الآلي وهو إطار يجمع 45دولة ولم يقتصر على الدول الأوروبية بل شمل أمريكا وكندا واليابان وعدد من الدول الإفريقية وأمريكا الجنوبية

–منظمة جنوب شرق آسيا وضعت الخطوط العريضة لتبادل المعلومات والخبرات بخصوص مواجهة الجرائم الالكترونية عامة وجرائم الإرهاب الالكتروني خاصة بل وقعت على إنشاء وحدة إقليمية لهذه الدول لمكافحة الجرائم الالكترونية

– وافقت الجامعة العربية على اعتماد قانون دولة الإمارات العربية المتحدة كقانون استرشادي لقانون مشابه للقانون الإسترشادي لدول أوروبا لمكافحة جرائم الإرهاب الالكتروني.[3]

جامعة نايف العربية للعلوم الأمنية انطلاقا من تخصص الجامعة كجامعة تهتم بالأمن الشامل وتختص كذلك بتنفيذ الجانب العلمي من الخطط والاستراتيجيات الأمنية العربية لمكافحة الإرهاب التي أقرت ، من وزراء الداخلية في الدول العربية وتم الانتهاء من تنفيذ الخطة المرحلية الرابعة الإستراتيجية في العام 2009وتنفذ الجامعة العديد من

[1]– حسن بن احمد الشهري، المرجع السابق، ص20

[2]–المرجع نفسه، ص20

[3]– المرجع نفسه، ص20

مناشط العلمية المعتمدة ضمن الخطط كما نفذ تعدد امن الدورات التدريبية والندوات العلمية والمحاضرات العلمية والدراسات والأبحاث الميدانية وتمكنت من الاستفادة من الخبرات الدولية حيث نظمت العديد ومن الأنشطة العلمية في مجال مكافحة الإرهاب في كل من فرنسا وألمانيا و إسبانيا و النمسا وإيطاليا وهولندا والتشيك والصين كما ضمت مناهجها العلمية العديد من المقررات الدراسية التي تناولت مشاكل وأنواع الإرهاب وطرق مواجهته.[1]

الفرع الثاني: المواجهة الفكرية

إذا كانت مشكلات التنظيمات الإرهابية والجرائم الإلكترونية مشكلات فكرية فيجب أن تعتمد الإجراءات المحلية والإقليمية والدولية على الوسائل الفكرية الفنية والقانونية في مواجهة هذه المشكلات وأن تقتصر الإجراءات الأمنية على الخارجين على القانون فقط لأن الاعتماد على الإجراءات الأمنية وحدها إلي نتائج عكسية فعندها انطلقت الطائرات الأمريكية لضرب أفغانستان انطلقت معها حركة تنظيم القاعدة على الانترنت المنظمات الأخرى الحليفة لها. واكتملت تلك الحلقة باحتلال العراق، وليكتسب تنظيم القاعدة أرضا جديدة لبث أفكاره التنظيمية المعادية للولايات المتحدة وللغرب بوجه عام، من هنا فقد زادت المواقع الإرهابية التنظيم القاعدة على الانترنت من 13 موقعا عام 2001 لتصل إلى ما يقارب 2000 موقع في عام 2006 وفق بعض التقديرات. السبيل الأمثل لمواجهة مثل هذه الظاهرة يكمن في:

1-الاستخدام الأمثل لوسائل الإعلام من خلال:نشر الأفكار المعتدلة وتجنب نشر أعمال العنف أو الأفكار المتطرفة 2-كشف مواقع المتطرفين ومناقشة أفكاره موبيان ما تشتمل عليه من مخلفات.

[1]-حسن بن احمد الشهري، مرجع السابق، ص20

3-التوسع في إنشاء المواقع البديلة لنشر الوسطية والاعتدال ومحاربة الأفكار المتطرفة.

4-تشكيل لجان وطنية لحماية الشباب وتحصينهم من الأفكار المتطرفة

5-إعداد وتنفيذ برامج إعادة تأهيل المتطرفين فكريا وعمليا.

6-اتخاذ الإجراءات الفنية المناسبة لحماية المواقع المعتدلة واختراق المواقع المتطرفة وتغذيتها بالأفكار المعتدلة.

7-وضع معاير دولية لأمن المعالجة الآلية للبيانات.

8-التدابير الملائمة لحل المشكلات الاختصاص القضائي التي تثيرها جرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية.

8-الاتفاقية الدولية تنطوي على نصوص وتنظيم الإجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق الدول [1]

الفرع الثالث:مواجهة استخباراتية وعسكرية للإرهاب الالكتروني

تتم المواجهة العسكرية للإرهاب الالكتروني:

أولا: بتقوية ودعم أجهزة جمع المعلومات والاستخبارات: تستطيع الدولة للمحافظة على أمن مواطنيها تسخير الأموال لتقوية أجهزة جمع المعلومات عن الإرهابيين والجماعات الإرهابية ليس هذا فحسب لابد من تجنيد عناصر ذو خبرة في مجال أنظمة المعلومات وإنشاء المواقع الإلكترونية وبرمجة الحاسب الآلي وغيرها من تقنياته المختلفة.

ثانيا: الردع واستخدام القوة: هو خيار صعب تقوم به الدول ضد القواعد الإرهابية. باغتيال اتقياداتهم وتصفيتهم والتضيق عليهم.وتجفيف منابع مصادرهم البشرية والمالية. إن اللجوء لهذا خيار يكون عندما ينشر و يتوسع الإرهاب الالكتروني بشكل كبير،و

[1]- حسن بن احمد الشهري، المرجع السابق، ص20

مرتكبو هذا النوع من الإرهاب يصعب جدا الوصول إليهم بسبب استعمالهم لأسماء مستعارة و صعوبة تحديد أماكنهم [1].

[1]–حسن بن احمد الشهري، المرجع السابق، ص19–20

خاتمة

خاتمة

إن الإرهاب الالكتروني وليد التطور العلمي الهائل ومن مفجرات الثورة التكنولوجيا حيث يعد من الجرائم المستحدثة الذي يعتمد على الموارد المعلوماتية على عكس الإرهاب التقليدي، وهو إرهاب المستقبل،والهاجس الأكبر لدول التي أصبحت عرضة لهجمات الإرهابيين والجمعات المتطرفة الذين يمارسون نشاطهم التخريبي في أي مكان وزمان، فهو عالمي لا تربطه أي حدود جغرافية ، ورغم قصر تاريخه إلا انه انتشر بسرعة النار في الهشيم ويتعالى مؤشر مخاطره يوم بعد يوم ،لان التقنية و حدها غير قادرة على حماية الناس من العمليات الإرهابية الالكترونية والتي سببت أضرار جسيمة على الأفراد والدول، مما يستدعي تضافر الجهود الدولية و إقليمية و الوطنية لوضع استراتيجيات هادفة لمكافحة هذا الخطر الداهم أو التقليل من حدة أثره و ضرره.

ومن خلال ما سبق دراسته نستنتج:

- إن التزاوج بين الإرهاب والحاسبات الآلية والانترنت يعد إجراما خطيرا في عصر قيام الحكومات المعلوماتية التي تعتمد على الشبكات الرقمية في تسيير قطاعتها الحيوية

- وان جرائم الإرهاب الالكتروني ما هي إلا امتداد للجريمة الإرهابية المادية التقليدية وصورة من صوره، بل هي نسخة الكترونية لها، وان معالم هذا الإرهاب لم تبرز إلى العالم إلا بعد أحداث 11سبتمبر 2001 التي ضربت الولايات المتحدة الأمريكية

- وان المجتمع الدولي لم يتوصل إلى تعريف جامع ومانع للإرهاب الالكتروني ولكن اتفق على تحديد الهدف منه الذي يتجسد في نشر الخوف والرعب والفزع باستعمال الوسائل التكنولوجيا حيث يُعرف انه العدوان أو تخويف أو تهديد المادي أو المعنوي الصادر عن الدول أو الأفراد أو الجماعات على الإنسان في دينه أو نفسه أو ماله أو عقله بغير حق باستخدام الموارد المعلوماتية ووسائل الالكترونية بشتى أصناف العدوان والفساد في الأرض.

– وتعد الوسائط الالكترونية بمختلف أنواعها من بريد الالكتروني ومواقع التواصل الاجتماعي المسرح المفضل للجمعات الإرهابية المتطرفة لنشر وبث أفكارهم المتطرفة والهدامة وتجنيد الشباب وتمويل أنشطتهم بحيث أصبحت ملاذا أمنا وسلاحا سهلا لتنفيذ أعمالهم وأغراضهم الإرهابية.

– و للإرهاب المعلوماتي أسباب ودوافع متعددة و متنوعة هي عينها

– ويعد إرهاب الرقمي إرهاب الحاضر والمستقبل والخطر القادم، نظرا لتعدد أشكاله وتنوع أساليبه وشدة أثره وضرره واتساع مجال الأهداف التي يمكن أن يستهدفها من خلال وسائل الاتصالات وتقنية المعلومات بأقل تكلفة وجهد ممكنين وبقدر عال من الراحة

– ولقد أصبح هذا الإرهاب الهاجس الأكبر الذي يرعب العالم نظرا لفداحة المخاطر التي يسببها سواء على الأفراد أو الدول ومؤسساتها ومختلف الأنشطة الحيوية وانعكاساته السلبية على عجلة التقدم في العالم اجمع

– ويعد ظاهرة عالمية جد خطيرة، تستهدف المجتمع الدولي برمته، مما أدى إلى حتمية عقد اتفاقيات ومنظمات إقليميا ودوليا وإنشاء وبناء أجهزة ومراكز مختصة وصياغة القوانين والتشريعات اللازمة على مستوى الدوال في إطار مكافحة هذه لظاهرة

– رغم خطورة الإرهاب الالكتروني إلا انه هناك بعض التدابير والإجراءات المكافحة التي اعتمدت عليها الدول للحد من أثر هذه الظاهرة وهي المكافحة الفنية بواسطة الإجراءات الحماية الأساسية (تدريب والتوعية، تفعيل المراقبة الالكترونية وأنظمة الحجب) وإجراءات الحماية الفنية من الاعتداءات الالكترونية (نظام التحقق من الهوية، خدمات الأدلة، الجدار الناري...الخ)، المكافحة القانونية والفكرية والعسكرية.

– القصور التشريعي فيما يخص الإرهاب الالكتروني .

ومن أهم الملاحظات والتوصيات التي توصلنا إليها:

– ضرورة إعطاء تعريف موحد لجريمة الإرهاب الالكتروني يشمل كل السلوكيات المجرمة لهذه الجريمة

– الرفع من درجة الوعي لدى الشعوب بخلق ثقافة اجتماعية عن الجرائم المعلوماتية بصفة عامة وجرائم الإرهاب الالكتروني بصفة خاصة

– عقد مؤتمرات علمية تحسيسية بمخاطر الإرهاب الالكتروني وتدابير مكافحته في الجامعات

– تعزيز التعاون الدولي والتشريعي والقضائي والأمني مع الدول الأكثر خبرة بالجرائم الالكترونية لمكافحة الإرهاب الالكتروني

– تخصيص شرطة قضائية خاصة وخبراء ذو كفاءة عالية في مجال الانترنت وتدريبهم على التعامل مع الجرائم الالكترونية ذات الطبيعة الفنية والعلمية معقدة

– تفعيل دور الإعلام الرسمي وغير الرسمي، حيث يلعب دورا محوريا مهما في مكافحة الإرهاب بالوسائل الالكترونية

– ضرورة التنسيق وتبادل المعلومات والخبرات بين الأجهزة المعنية بمكافحة الإرهاب بالوسائل الالكترونية في دول العالم

– حث الدول على عقد اتفاقيات الدولية خاصة بمكافحة الإرهاب الالكتروني والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الإرهاب والجرائم المعلوماتية

– يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن مناهج الدراسية في تعليم ما قبل الجامعي

– العمل على تعديل التشريعات الداخلية بما يتلاءم مع مكافحة الإرهاب الالكتروني وسد الثغرات التي تكتنف هذا الإرهاب

– الاهتمام بالجانب الوقائي لمكافحة الإرهاب الالكتروني وعمل بمقولة "الوقاية خير من العلاج "

– ودعوة الدول العربية إلى إبرام اتفاقية شاملة لمكافحة الإرهاب الالكتروني تحتوي على تعريف موحد لهذا الإرهاب وتحديد صوره الإجرامية واليات التعاون في المجال القضائي والأمني وتبادل المعلومات والخبرات وملاحقة تسليم المجرمين الإرهابيين وإنشاء مراكز لمراقبة الاتصالات وشبكة الانترنت

– أما على المستوى الوطني ندعو المشرع الجزائري إلى تجريم جريمة الإرهاب الالكتروني في نصوص خاصة وفصلها عن الإرهاب التقليدي ووضع عقوبات رادعة تتناسب مع حجم وخطورة هذه الجريمة

– يتعين إدخال مادة "أخلاقيات استخدام الانترنت" ضمن مناهج الدراسية في تعليم ما قبل الجامعي

– العمل على تعديل التشريعات الداخلية بما يتلاءم مع مكافحة الإرهاب الالكتروني وسد الثغرات التي تكتنف هذا الإرهاب

– الاهتمام بالجانب الوقائي لمكافحة الإرهاب الالكتروني وعمل بمقولة "الوقاية خير من العلاج "

قائمة المراجع

أولا: المصـــــادر

-القرآن الكريم

ثانيا: المراجـــــع

أولا: الكتب

1. أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، د ن ط، مطابع جامعة نايف للعلوم الأمنية، الرياض ،2006
2. احمد محمد رفعت، الإرهاب الدولي، دار النهضة العربية، القاهرة، 2006، ص216
3. أسامة احمد المناعسة، جلال محمد الزعبي، جرائم التقنية نظم المعلومات الالكترونية، دراسة مقارنة، ط2، دار الثقافة لنشر والتوزيع، عمان، الأردن،2014
4. أمير فرج يوسف، الجرائم الدولية للانترنت، ط1، المركز القومي للإصدارات القانونية، مصر، 2011
5. أمير فرج، الجرائم المعلوماتية على شبكة المعلومات، دار المطبوعات الجامعية، الإسكندرية، 2008.
6. أمير فرج، جريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، ط1، مكتبة الوفاء القانونية، الإسكندرية،2011
7. إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، ط1، مركز الديمقراطي العربي لدراسات إستراتيجية والسياسية والاقتصادية، برلين، ألمانيا،2018
8. أيمن عبد الكريم حسين، الإرهاب ودوافعه وتداعياته على الأمن والسلم الدوليين مركز البيان لدراسات والتخطيط، بغداد،2018
9. إيهاب سنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الالكترونية (بودابست 2001) والبرتوكول الملحق بها، دار النهضة العربية، القاهرة،2009

10. بن يحيي طاهر الناعوس، مكافحة الإرهاب الالكتروني ضرورة بشرية و فريضة شرعية، مكتبة الالوكة،2015

11. حامد عبد اللطيف عبد الرحمن، جريمة غسيل الأموال وسبل مكافحتها، رسالة ماجستير، مملكة البحرين ،2012

12. حسين شفيق، –الإعلام الجديد والجرائم الالكترونية التسريبات. التجسس الالكتروني، الإرهاب الالكتروني–، دار الفكر والفن، بدون بلد النشر ،2015

13. خالد حسن احمد لطفي، الإرهاب الالكتروني آفة العصر الحديث والآليات القانونية لمواجهة، ط1، دار الفكر الجامعي، الإسكندرية،2018

14. خالد حسن احمد لوطفي، الجرائم الانترنت بين القرصنة الالكترونية والابتزاز الالكتروني، ط1، دار الفكر الجامعي، الإسكندرية ،2018

15. خليل حسين، التنظيم الدولي النظرية العامة والمنظمات العالمية، ط1، دار المنهل اللبناني، بيروت، 2010

16. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في تشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة،2011

17. السامي علي عياد، جريمة المعلوماتية وإجرام الانترنت، ط1، دار الفكر الجامعي، الإسكندرية،2007

18. سعاد إكرام عوض، التزوير المعلوماتي، دراسة نقدية لمختلف القوانين الوضعية، منشاة المعارف، الإسكندرية، 2008

19. سليمان الطعاني، الوجيز في التربية الإعلامية، ط1، دار الخليج لنشر والتوزيع، الأردن، عمان، 2020

20. سهيلة خليل غازي، معوقات التجارة الرقمية في الدول العربية، دار الوفاء لنشر، القاهرة، مصر، 2003

21. سيد احمد عبد الخالق، الآثار الاقتصادية والاجتماعية لغسيل الأموال، د ن ط، دار النهضة العربية، القاهرة ،1997
22. السيد عبد الفتاح علي، مكافحة الجرائم الالكترونية بين نظم المعلوماتية والإعلام البديل، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2017
23. عادل عبد الصادق، استخدام الإرهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015
24. عادل عبد الصادق، الإرهاب الالكتروني القوة في العلاقات دولية نمط جديد وتحديات مختلفة، ط2، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة ،2009
25. عادل عبد الصادق، الإرهاب الالكتروني قوة في العلاقات الدولية نمط جديد وتحديات جديدة،ط1، مركز الأهرام للدراسات السياسية والإستراتيجية , 2009
26. عبد الرحمان بن عبد الله سند، وسائل الإرهاب الالكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، ج1، د ن ط، الرياض، 2004
27. عبد الصبور عبد القوي على مصري، منال عبد اللاه عبد الرحمن، محكمة الرقمية والجريمة المعلوماتية، دراسة مقارنة، مكتبة القانون واقتصاد، الرياض، 2012
28. عبد العزيز لطفي جاد الله، امن المجتمع الالكتروني بين السياسة الالكترونية والتعاون الدولي في إطار مواجهة الجرائم الالكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2017
29. عبد القادر زهير النقوزي، مفهوم القانوني لجرائم الإرهاب الداخلي والدولي، منشورات حلبي الحقوقية، الطبعة الأولى، بيروت، 2008
30. عبد الله عبد العزيز يوسف، التقنية والجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999

31. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية الانترنت (الجرائم الالكترونية)، ط1، منشورات حلبي الحقوقية، بيروت،2007
32. عصام عبد الفتاح عبد السميع مطر، جريمة الإرهابية، دار الجامعة الجديدة لنشر، الإسكندرية، جمهورية مصر العربية، 2005
33. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف ومصنفات الفنية، دار الثقافة لطباعة والنشر، 1999
34. علاء الصراط الغامدي، الحرب النفسية للإرهاب الجديد، دار منشاة المعارف، الإسكندرية، مصر،2006
35. علي بن فايز الجحني، خطاب العنف الإرهابي قنواته وأثاره، جامعة نايف للعلوم الأمنية، الرياض،2008
36. علي جابر حسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية لنشر والتوزيع،2018
37. علي عدنان الفيل، الإجرام الالكتروني، ط1، مكتبة زين الحقوقية والأدبية، لبنان،2011
38. علي يوسف شكري، المنظمات الدولية، ط1، دار الصفاء لنشر والتوزيع، عمان، 2012
39. غادة نصار، الإرهاب والجريمة الالكترونية، العربي لنشر والتوزيع، قاهرة،2017
40. فايز الشهري، الطرح الفكري على شبكة الانترنت المراحل والرموز، دون دار النشر، مصر، دون بلد النشر.
41. لهويدي عمر، مكافحة جرائم الإرهاب، دار وائل لنشر، عمان، 2011
42. لیندا بن طالب، غسيل الأموال وعلاقتها بمكافحة الإرهاب، دراسة مقارنة، دار الجامعة الجديدة لنشر، الإسكندرية، 2011

43. محمد إبراهيم زيد، مقدمة في علم الإجرام وعلم العقاب، دار الهدى للمطبوعات، الإسكندرية، 2008

44. محمد أمين بشرى، التحقيق في الجرائم المستحدثة، مركز الدراسات والبحوث جامعية نيل العربية للعلوم الأمنية، الرياض، 2004

45. محمد حسن عمر برواري، غسيل الأموال وعلاقته بالمصارف والبنوك، دراسة مقارنة، طبعة الأولى، دار قنديل لنشر والتوزيع، عمان، 2013 ص182

46. محمد سليمان احمد، أساسيات الاستثمار الالكتروني تحليل الأعراف المالية، ط2، منشاة المعارف، الإسكندرية، مصر

47. محمد عبد الله العميري، موقف الإسلام من الإرهاب، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض،2004

48. محمد فاتح محمود المغربي، التجارة الالكترونية، ط1، دار الجنان لنشر والتوزيع، عمان، الأردن، 2016

49. محمد فتحي عيد، الإجرام المعاصر، د ن ط، منشورات أكاديمية نايف للعلوم الأمنية، الرياض،1999

50. محمد محي الدين عوض، تشريعات مكافحة الإرهاب في الوطن العربي، أكاديمية نايف العربية، للعلوم الأمنية،1999

51. محمود رجب فتح الله، الوسيط في الجرائم معلوماتية، دار الجامعة الجديدة، الإسكندرية،2019

52. مصطفى طاهر، المواجهة التشريعية لظاهرة غسيل الأموال متحصلة من جرائم المخدرات، ط2، طبع على نفقة المؤلف، القاهرة، 2004

53. مصطفى يوسف كافي، الإدارة الالكترونية، د ط، دار ومؤسسة رسلان لطباعة والنشر، سوريا، دمشق، 2011

54. نوران شفيق، آثر التهديدات الالكترونية على العلاقات الدولية، مكتب العربي للمعارف، القاهرة، 2015

55. هشام محمد رستم، الإرهاب الدولي، دار النهضة العربية، القاهرة، مصر، 2003

56. وليد الزيدي، القرصنة على الانترنت والحاسوب، التشريعات القانونية، ط1، دار أسامة لنشر والتوزيع، الأردن،2003

57. يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، منشورات مركز كوردستان لدراسات الإستراتيجية، السلمانية 2008

58. يونس عرب، جرائم الكمبيوتر والانترنت، ط1، اتحاد المصارف العربية، بيروت 2002،

ثانيا: الرسائل والمذكرات

1 أطروحات الدكتورة

1. حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، رسالة دكتورة، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، الجزائر ،2014

2. –درار نسيمة، الأمن المعلوماتي وسبل المواجهة مخاطرة في التعامل الالكتروني، دراسة مقارنة، أطروحة الدكتورة، كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد تلمسان الجزائر،2017

3. الزبن، بدرة هوميل، الإرهاب في الفضاء الالكتروني، رسالة دكتورة، كلية القانون، جامعة عمان العربية،2012

4. عمراني كمال الدين، السياسة الجنائية المنتهجة ضد الجرائم الالكترونية، دراسة مقارنة، أطروحة دكتورة، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2012

5. غازي عبد الرحمن رشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة دكتورة، كلية الحقوق، الجامعة الإسلامية، لبنان،2004

6. لونيسي علي، آليات مكافحة الإرهاب الدولي بين فعالية القانون الدولي وواقع الممارسات الدولية الانفرادية، رسالة دكتورة في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012

7. مجراب دوادي، الأساليب الخاصة للبحث والتحري في الجريمة منظمة، أطروحة الدكتورة، كلية الحقوق، تخصص قانون عام، جامعة يوسف بن خدة، الجزائر 2016-2015

2 رسائل ماجستير

1. إسراء طارق جواد، كاظم الجابري، جريمة الإرهاب الالكتروني، دراسة مقارنة، رسالة ماجستير في القانون العام، كلية الحقوق ن جامعة البحرين، العراق،2012

2. رشيد صبحي جاسم محمد، الإرهاب والقانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة بغداد، العراق، 2003

3. سجاد خليفة خزعل تميمي، المواجهة الدولية والوطنية لجريمة تمويل الإرهاب، رسالة ماجستير، كلية الحقوق، جامعة تكريت، العراق، 2017

4. صغير يوسف، الجرائم المرتكبة عبر الانترنت، رسالة ماجستير، كلية الحقوق، جامعة مولود معمري، الجزائر، 2013

5. صفاء كاظم غازي الجياشي، جريمة قرصنة البريد، دراسة مقارنة، رسالة ماجستير، كلية القانون، جامعة بابل، العراق،2016

6. عمر عباس خضير العبيدي، الإرهاب الالكتروني في نطاق القانون الدولي، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة تكريت، العراق، 2019

7. محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت والأحكام الموضوعية والأحكام الجزائية، ط1، منشورات حلبي الحقوقية، بيروت، 2011

8. مريم محمد حسن، التنظيم القانوني لجريمة التجسس المعلومات، رسالة ماجستير، كلية القانون، جامعة كوفة، العراق،2016

9. مريم محمد حسن، التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، كلية القانون، جامعة كوفة، العراق،2016

10. نسيب نجيب، التعاون الدولي لمكافحة الإرهاب، مذكرة نيل شهادة ماستر في القانون الدولي، جامعة مولود معمري، تيزي وزو، 2009

11. نور الله تلة، الإرهاب بالوسائل الالكترونية، مذكرة ماجستير في القانون الجزائي كلية الحقوق، جامعة دمشق،2015-2016

3 مذكرات ماستر

1. توفيق شريخي، الإرهاب الالكتروني وتأثيره على امن الدولة، مذكرة ماستر، تخصص استراتيجية وعلاقات دولية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، مسيلة، الجزائر، 2018/2017

2. شراك عماد، بن عطاء الله طارق، ظاهرة تبييض الأموال في ظل التشريع الجزائري، مذكرة ماستر، تخصص إدارة ومالية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، جلفة،2017/2016

3. غلاف كريمة، جرلال زوهرة، جريمة الإرهاب الالكتروني، مذكرة الماستر، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، تخصص قانون جنائي وعلوم جنائية، جامعة عبد الرحمان ميرة، بجاية، 2019/2018

4. نجاري بن حاج علي فايزة، الآليات القانونية للإرهاب الالكتروني، مذكرة ماجستير في القانون الدولي لإعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2016

5. هارون فتوسي، الجريمة الإرهابية على ضوء قانون العقوبات الجزائري، مذكرة ماستر في القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن لمهيدي، أم لبواقي،2014/2013

ثالثا: المقالات

1. توفيق مجاهد، طاهر عابسة، جريمة الإرهاب في ضوء أحكام الاتفاقية العربية لمكافحة جرائم التقنية المعلومات، لعام 2010، مجلة العلوم القانونية والسياسية، المجلد 09، العدد03، ديسمبر 2018، جزائر

2. –حسن بن احمد الشهري، الإرهاب الالكتروني حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد الرابع، العدد الثامن، 2015

3. حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم السياسية، جامعة ديالي، عدد خاص

4. صباح كزيز، أمال كزيز، الإرهاب الالكتروني وانعكاساته على الأمن الاجتماعي، مجلة التراث، رقم 1، العدد 8، 2008

5. علي عدنان، الفيل، الإرهاب الالكتروني، مجلة الجامعية الخليجية، جامعة الخليج: كلية الحقوق، العدد 2، 2010

6. فراس طحان، الإرهاب الالكتروني وسبل مكافحته، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، العدد الثاني ،2011

7. موزة مزروعي، الاختراقات الالكترونية خطر كيف تواجهه، مجلة الأفاق الاقتصادية، العدد 9، الإمارات المتحدة، 2008

8. نجيب بن عمر عوينات، الإرهاب الالكتروني: مفهوم الجهود الدولية والإقليمية لمكافحته، مجلة الأستاذ الباحث لدراسات القانونية والسياسية، معهد العالي للإعلامية، الكاف جامعة جندوبة تونس، العدد 6، تاريخ الصدور 2017/04/20

رابعا: أعمال الندوات والمؤتمرات

1.رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، دورة تدريبية، توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب، الرياض، السعودية،23-27فيفري2013

2.سامر مؤيد عبد اللطيف، الإرهاب الالكتروني وسبل مواجهته، بحث منشور في مجلة كربلاء العلمية، العدد 14، العراق، 2016

3.سعد عطوة الزنط، الإرهاب الالكتروني وإعادة صياغة استراتيجيات الأمن القومي، مؤتمر الجرائم المستحدثة. كيفية إثباتها ومواجهتها، مصر، 15-16ديسمبر 2010

4.عبد الحق باسو، الإرهاب المعلوماتي في القانون المغربي الدولي، دورة تدريبية، مكافحة الجرائم الإرهابية المعلوماتية، المغرب ن قنطيرة، 2006.04.09

5.عبد الحميد إبراهيم محمد العريان، العلاقة بين الإرهاب المعلوماتي وجرائم المنظمة: ما هو رد فعل القطاع الخاص، دورة تدريبية مكافحة الجريمة الإرهابية المعلوماتية، كلية تدريب، قسم برامج التدريبية، 2006

6.عبد الله بن عبد الغزيز بن فهد العجلان، الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية امن المعلومات والخصوصية في قانون الانترنت، المنعقد من2 إلى 4 يونيو، القاهرة، مصر، 2008

7.عبد المجيد حلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية، مكافحة جرائم الإرهاب المعلوماتية، في فترة 2006/4/13.9، المغرب القنطرة، 2006

8.عمر الفاروق، تأملات في بعض صور الحماية الجنائية لبرامج الحاسوب الآلي، بحث مقدم إلى مؤتمر الكويت، مجلة المحامي ،1989

9.مجمع البحوث والدراسات الأكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الالكترونية، البحث الحائز على المركز الأول لمسابقة جائزة الأمير نايف عبد العزيز للبحوث الأمنية، عمان،2016

10. محروس نصر غايب، الجريمة المعلوماتية، بحث منشور في مجلة التقني، العدد 24، الإصدار 9، العراق ،2011

11. محمد سيد سلطان، الحماية الدولية والقانونية للبيئة الالكترونية من الجريمة والإرهاب، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلوماتية الآمنة: المفاهيم والتشريعات والتطبيقات، منعقد في الرياض، 2010/04/7.6

خامسا: النصوص القانونية والاتفاقيات الدولية

1) النصوص القانونية الوطنية

1. الأمر رقم 156/66، المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات، ج ج د ش، جريدة الرسمية، العدد49، مؤرخ في 19جوان 1966، المعدل والمتمم

2. القانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن قانون العقوبات، جريدة الرسمية، عدد17، الصادر في 2004/11/10

3. قانون رقم 09-04 المؤرخ في 2009/02/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47، صادر في 2009/02/16.

القوانين والاتفاقيات الدولية

الاتفاقيات الدولية:

1. الاتفاقية العربية لمكافحة الجرائم المعلوماتية، لسنة 2010 وما في حكمها، الصادرة عن جامعة الدول العربية
2. اتفاقية مكافحة إساءة استعمال التكنولوجيا الأغراض إجرامية رقم (63/55) في 2000/04/12، والصادرة عن منظمة الأمم المتحدة، الجلسة العامة 2000/12/4/81
3. اتفاقية بودابست لمكافحة الجرائم المعلوماتية، لسنة 2001، الصادرة عن مجلس أوروبا رقم 185 في 2001/11/23 والبروتوكول الإضافي لها سنة 2003
4. اتفاقية الأمم المتحدة لمكافحة الاتجار الغير المشروع بمخدرات،فينيا، 1988
5. اتفاقية الاتحاد الإفريقي فيما يتعلق في مجال الأمن السيبراني وحماية البيانات الشخصية عام 2014

القوانين الأجنبية

1. القانون العربي الإسترشادي (نموذجي) لمكافحة جرائم التقنية أنظمة المعلومات وما في حكمها 417/د21/2004
2. قانون جرائم الأنظمة المعلومات ،رقم 30 لسنة 2010 ،الأردن

المواقع الالكترونية

1. حسن بن سعيد بن سيف الغافري، الإرهاب الالكتروني الخطر قادم، متوفر على موقع:http://althawrah.ye/archives/72153، تاريخ النشر:2014/02/14، تاريخ التصفح:2020/09/02، الساعة18:34

2. ايمن حسن، الإرهاب الالكتروني أخطر معارك حروب الفضاء، متوفر على الموقع:http://alwatan.com/details/166324، تاريخ النشر:2017/01/14، تاريخ التصفح:2020/09/06، الساعة: 21:59

3. عبد الستار عبد الرحمن، الإرهاب السيبراني خطر يهدد العالم، متوفر على موقع:https://imctc.org/Arabic/ArticleDet، تاريخ النشر:2020/02/23، تاريخ التصفح:2020/09/06، الساعة:21:57

4. نور بنداري عبد الحميد فايد، دور و سائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية، دراسة حالة "داعش"، متوفر على الموقع،https://democraticac.de/?p، تاريخ النشر 2016/07/19، تاريخ التصفح:2020/09/06،الساعة:21:21

5. محمد عطايا، فوربس: الهاكرز يبدأون بنشر الجزء الأول لتسريبات ترامب و يطلبون فدية42 مليون دولار، متوفر على الموقع:https://www.masrawy.com، تاريخ النشر:2020/05/18، تاريخ التصفح:2020/09/02، الساعة:11:50

6. سعود شرفات، الإرهاب الالكتروني رعب على الأبواب، متوفر على الموقع:https://hafryat.com/en/node/1678، تاريخ النشر:2018/03/01، تاريخ التصفح:2020/09/02، الساعة: 10:27

7. سعود شرفات، الإرهاب الالكتروني خطر على الأبواب، مرجع سابق، موقع:https://hafryat.com/en/node/1678، الساعة: 14:26

8. سعود شرفات، الإرهاب الالكتروني رعب على الأبواب، متوفر على الموقع:https://hafryat.com/en/node/1678، تاريخ النشر:2018/03/01، تاريخ التصفح:2020/09/02،الساعة:10:35

9. عبد الستار عبد الرحمن، الإرهاب السيبراني خطر يهدد العالم، متوفر على الموقع:https://imctc.org/Arabic/Art ،تاريخ النشر:2020/02/23، تاريخ التصفح:2020/09/02، الساعة:10:33

10. عبد الله بن عبد العزيز بن فهد العجلان،الإرهاب الالكتروني في عصر المعلومات ، متوفر على الموقع التالي:http://www.shaimaaatalla.com ، تاريخ النشر 2009/07/27،تاريخ التصفح 2020/08/30،الساعة:19:18

11. كتب علاء رضوان ، علاقة غسيل الأموال بالجرائم الالكترونية ،المقال متوفر على موقع https://www.youm7.com ،تاريخ النشر:2019/11/10، 9:00م، تاريخ التصفح 2020/08/29، الساعة 11:30

12. بن بادة عبد الحليم، بوحادة محمد سعد، جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة، متوفر على الموقع:https://www.elmizaine.com، تاريخ النشر:3يوليو2020، تاريخ التصفح 29 /2020/08، ساعة 14:05

المراجع الأجنبية

1. Mann, David & Sutton, Mike, Net crime, Brit. J. criminal, vol 38,No 2 ,spring 1998,p220
2. mohamed bozabar, la criminaliteinformatiquesurl internet, journal of law academic ,n°01,voulum26,faculte de droit, universite kowit,2002
3. Pitter BELLEY, Hached attacked, abused digital crime exposed, London. Regan Page, 2002.
4. Raul ATAYLOR. Maestros ormisogvnistis? Gender and the social construction of haking, y- vonne tweaks, Williampubliching, 2003
5. Steven FURNELL, Cyber crime vandalizing the information society. London. Addison, cuesely. 2002. P

فهرس المحتويات

فهرس المحتويات:

العنوان	الصفحة
قائمة أهم المختصرات	
الإهداء	
شكر وتقدير	
مقدمة	02
الفصل الأول: الإطار العام للإرهاب الالكتروني	06
المبحث الأول: ماهية الإرهاب الالكتروني	07
المطلب الأول: مفهوم الإرهاب الالكتروني ودوافعه	07
الفرع الأول: التعريف بالإرهاب الالكتروني	08
أولا: المقصود الإرهاب التقليدي:	08
ثانيا: تعريف الإرهاب الالكتروني	11
ثالثا: تمييز الإرهاب الالكتروني عن غيره عن غيره من المفاهيم	17
الفرع الثاني: صور الإرهاب الالكتروني	22
أولا: جريمة غسيل الأموال	22
ثانيا: جريمة التجسس الالكتروني	25
ثالثا: جريمة التهديد والقصف الالكتروني	26
الفرع الثالث: دوافع الإرهاب الالكتروني	27
أولا: الأسباب العامة الإرهاب	27
ثانيا: الأسباب الخاصة للإرهاب الالكتروني	30
المطلب الثاني: مظاهر الإرهاب الالكتروني ووسائله	32
الفرع الأول: مظاهر الإرهاب الالكتروني	32
أولا: تبادل المعلومات الإرهابية ونشرها من خلال شبكة المعلوماتية	32
ثانيا: إنشاء مواقع إرهابية الكترونية	35

الفرع الثاني: وسائل الإرهاب الالكتروني	38
أولا: البريد الالكتروني	38
ثانيا: تصميم الموقع	39
ثالثا: تدمير المواقع	39
رابعا: أنظمة الهاكرز الاختراق	39
خامسا: الهاتف المحمول	39
الفرع الثالث: أهداف الإرهاب الالكتروني	40
المبحث الثاني: مخاطر الإرهاب الالكتروني وأثاره	40
المطلب الأول: مخاطر الإرهاب الالكتروني	41
الفرع الأول: مخاطر الإرهاب الالكتروني على الأفراد	42
أولا: التهديد والابتزاز المعلوماتي	42
ثانيا: المواقع الإباحية	44
ثالثا: استقطاب وتجنيد الشباب	45
الفرع الثاني: مخاطر الإرهاب الالكتروني على المؤسسات والدول	46
أولا: مخاطر الإرهاب الالكتروني على المؤسسات	46
ثانيا:مخاطر الإرهاب الالكتروني على الدول	47
الفرع الثالث: مخاطر الإرهاب الالكتروني على التجارة الالكترونية	49
أولا: المخاطر الأمنية للإرهاب الالكتروني على التجارة الالكترونية	50
ثانيا: المخاطر التجارية للإرهاب الالكتروني	53
المطلب الثاني: أثار الإرهاب الالكتروني	56
الفرع الأول: أثار الإرهاب الالكتروني على الأمن وسلم	57
الفرع الثاني: أثار الإرهاب الالكتروني على العلاقات الدولية	58
الفرع الثالث:الآثار الأخرى للإرهاب الالكتروني	60
أولا: الآثار النفسية لأعمال الإرهاب الإلكتروني:	61
ثانيا: الآثار الأمنية لظاهرة الإرهاب الإلكتروني على المستوى الدولي:	62

الفصل الثاني: مكافحة الإرهاب الإلكتروني	66
المبحث الأول: مكافحة الإرهاب الالكتروني على الصعيد الدولي والإقليمي	67
المطلب الأول: الجهود الدولية في مكافحة الإرهاب الالكتروني	68
الفرع الأول: مكافحة الإرهاب الالكتروني في الدول الغربية	68
أولا: الولايات المتحدة أمريكية	68
ثانيا: بريطانيا	69
ثالثا: فرنسا	70
الفرع الثاني:مكافحة الإرهاب الالكتروني في الاتفاقيات دولية	73
اولا: اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55 لسنة 2000	73
ثانيا: اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001والبروتوكول الملحق بها	75
الفرع الثالث: مكافحة الإرهاب الالكتروني في منظمات الدولية	78
أولا: منظمة الأمم المتحدة ومجموعة الدول الثمانية (8– G)العالمية	79
ثانيا: المنظمات العالمية المتخصصة	83
المطلب الثاني: الجهود الإقليمية لمكافحة الإرهاب الالكتروني	86
الفرع الأول: مكافحة الإرهاب الالكتروني في الدول الإقليمية العربية	86
أولا: الإرهاب الالكتروني في القانون الأردني	86
ثانيا: الإرهاب الإلكتروني في القانون المصري	89
ثالثا: الإطار التشريعي في الجزائر	91
الفرع الثاني: الاتفاقيات الإقليمية في مكافحة الإرهاب الالكتروني	92
أولا: الاتفاقية الأمريكية لعام 1999، واتفاقية الاتحاد الأفريقي لعام 2014	92
ثانيا: الاتفاقيات العربية لمكافحة الإرهاب الإلكتروني	93
الفرع الثالث: مكافحة الإرهاب الالكتروني في منظمات الإقليمية	97
أولا: المنظمات الإقليمية لمكافحة الإرهاب الإلكتروني	97
ثانيا: المؤتمرات الإقليمية لمكافحة الإرهاب الإلكتروني	100

المبحث الثاني: مكافحة الإرهاب الالكتروني	102
المطلب الأول: مكافحة الإرهاب الالكتروني فنيا	102
الفرع الأول: إجراءات الحماية الفنية الأساسية	104
أولا: التدريب والتوعية	104
ثانيا: تفعيل المراقبة الالكترونية وأنظمة الحجب	106
الفرع الثاني: أنظمة الحماية الفنية من الاعتداءات الالكترونية	109
أولا: نظام التحقيق من الهوية	109
ثانيا: خدمات الأدلة	109
ثالثا: استخدام التشفير لحماية المعلومات الهامة	110
رابعا: الجدار الناري	110
خامسا: الشبكات الافتراضية	110
المطلب الثاني: مكافحة الإرهاب الالكتروني قانونيا، فكريا، عسكريا	111
الفرع الأول: مواجهة الإرهاب الالكتروني قانونيا	111
الفرع الثاني: المواجهة الإرهاب الالكتروني فكريا	113
الفرع الثالث: مواجهة الإرهاب الالكتروني عسكريا	114
خاتمة	116
قائمة المصادر و المراجع	121
فهرس المحتويات	136