وزارة التعليم العالي والبحث العلمي
جامعة عمار ثليجي الأغواط
كلية الحقوق والعلوم السياسية
قسم الحقوق

جرائم الإرهاب الإلكتروني

مذكرة في إطار مقتضيات نيل شهادة الماستر في القانون الجنائي

إعداد الطلبة:

شقراني الطيب

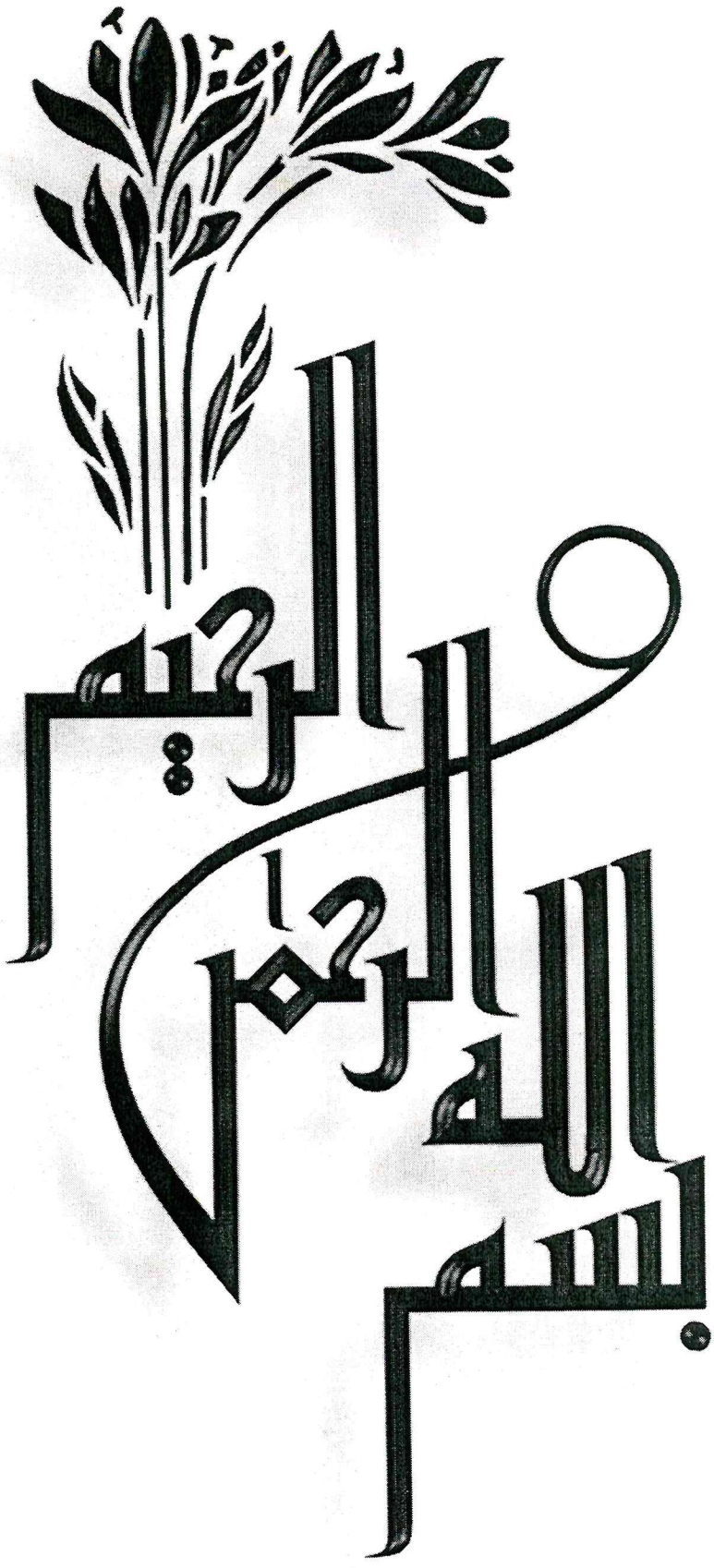
لجنة المناقشة

الأستاذ:.....بوزيدي أحمد تجاني.....رئيسا

الأستاذ:.....بوقرين عبد الحليم.....رئيسا

الأستاذ:.....بن صالح محمد الحاج عيسى.....عضوا مناقشا

السنة الجامعية: 2018/2017


بسم الله الرحمن الرحيم

إلى والدي روح جدتي رحمة الله عليها.

إلى عائلة شقراني رزقي شاهد بدون إستثناء

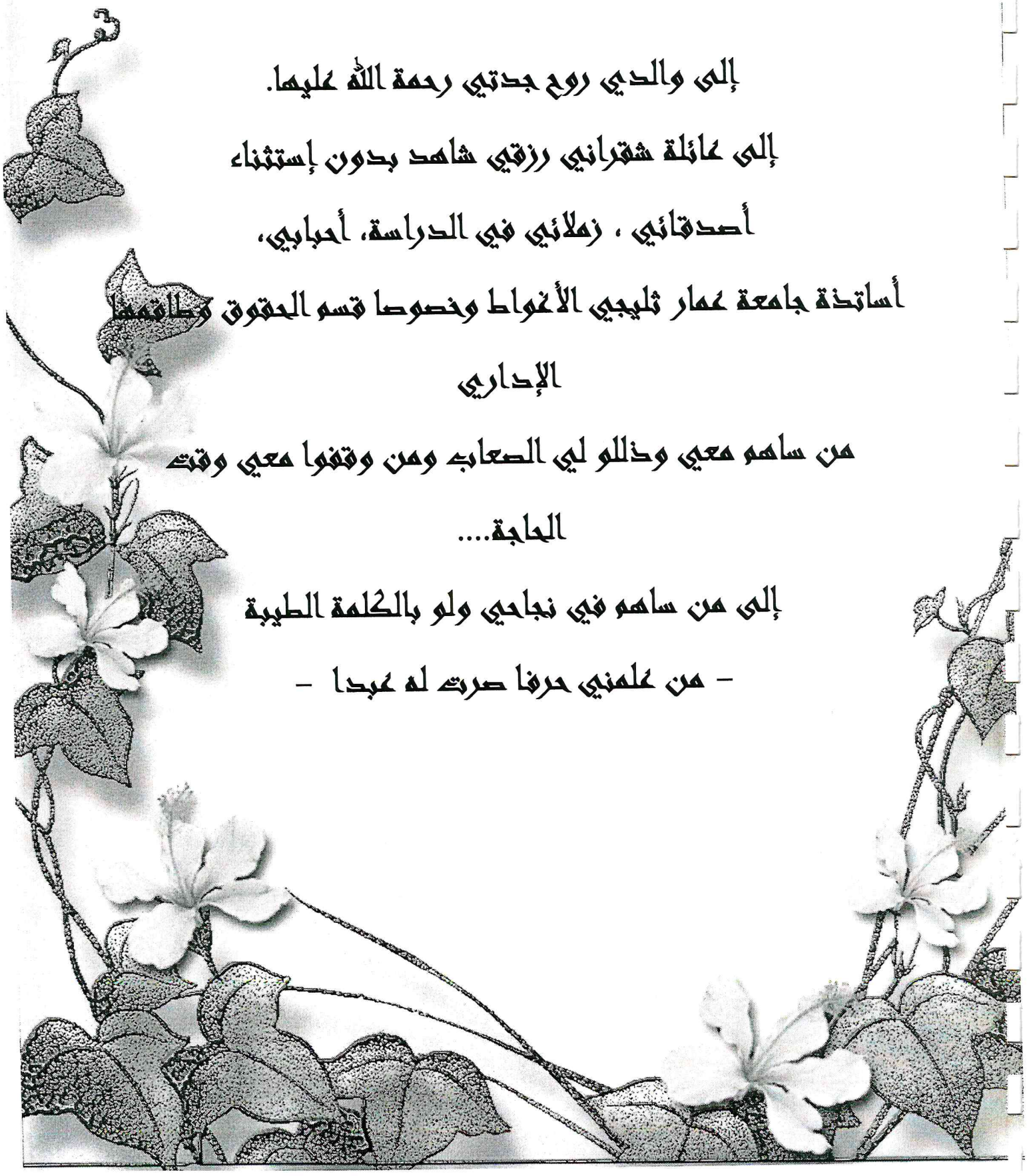
أصدقائي ، زملائي في الدراسة، أحبابي،

أساتذة جامعة عمار ثليجي الأغواط وخصوصا قسم الحقوق وطاقمها الإداري

من ساهم معي وذللو لي الصعاب ومن وقفوا معي وقت الحاجة....

إلى من ساهم في نجاحي ولو بالكلمة الطيبة

- من علمني حرفا صرت له عبدا -



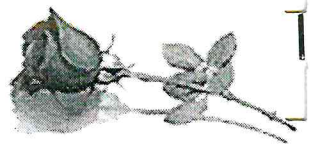
أولا أبدأ بحمد الله عز وجل حمدا كثيرا مباركا لا أحصي ثناء عليه وأصلي وأسلم على الحبيب المصطفى صاحب الشريعة والمنهاج عليه أفضل الصلاة وازكى التسليم.

قال رسول الله صلى الله عليه وسلم " من لم يشكر الناس لم يشكر الله، ومن أسدى اليكم معروفا فكافئوه، فإن لم يستطيعو فإدعو له"

تطبيقا لهذا الحديث النبوي الشريف يسرني في بداية هذه المذكرة أن أتوجه بالشكر الجزيل والثناء الخالص إلى أستاذي الفاضل: بوقرين عبد الحليم الذي أشرف على في تحضير هذه المذكرة، ووهبنا من وقته الثمين وشجعنا على ضرورة إنجاز وبدل لنا من نصائحه السديدة وتوجيهاته القيمة من اللحظة الأولى الغاية كتابة هذه الأسطر ما ذلل أمامنا الصعوبات الكثيرة.

كما أتقدم بالشكر إلى كل الأساتذة اللذين أشرفوا على تدريسنا وغيرهم ممن وقفوا إلى جانبنا فردا فردا دون أن ننسى الطاقم الإداري وكل من لم يبخل علينا بتقديم المساعدة من قريب أو بعيد في جمع المادة العلمية.

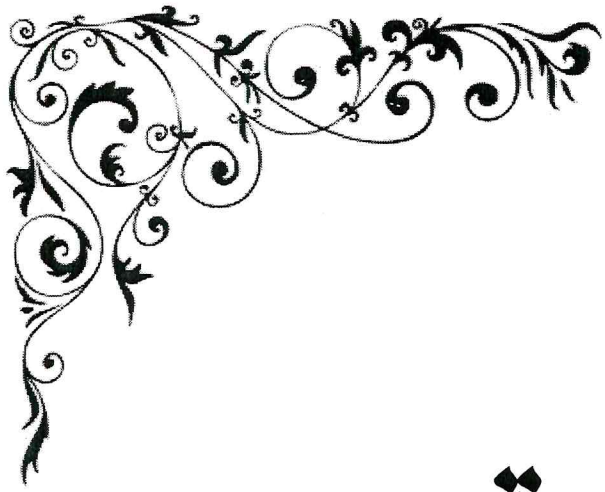
وأسال الله أن يجعل عملنا خالصا لوجهه الكريم وأن يتقبله منا، وأن يكتب لنا دائما التوفيق في كل أمورنا



يستحضرنا في مذكرتنا هذه قول العماد الأصفهاني

حين قال:

"إني رأيت لا يكتب أحدا كتابا في يومه إلا قال في غده : لو غير هذا لكان أحسن، ولو زيد هذا لكان يستحسن، ولو قدم هذا لكان أفضل ولو ترك هذا لكان أجمل، وهذا أعظم العبر، وهو دليل على استلاء جملة البشر"



مقدمة

مقدمة

مما لاشك فيه أن العالم يشهد تطورا هائلا في وسائل الاتصالات وتقنية المعلومات، حتى اصبح يطلق على هذا العصر عصر الثورة المعلوماتية وذلك لأن التغيرات السريعة والمتلاحقة المترتبة على التقدم العلمي والتعليمي شملت معظم جوانب الحياة، وكانت أشبه ما تكون بالثورة في حيا ة البشرية وأسلوب حياة الناس.

ولقد ترتبت على هذا الثورة الكبيرة والطفرة الهائلة التي جلبتها حضارة التقنية في عصر المعلومات بروز مصطلح الإرهاب الإلكتروني وتوسع استخدامه، وزيادة خطورة الجرائم الإرهابية وتعقيدها سواء من حيث تسهيل الاتصال بين الجماعة الإرهابية وتنسيق عملياتها، أو من حيث المساعدة على ابتكار أساليب وطرق إجرامية متقدمة وهو ما دعت إليه دول في وقت سابق إلى إبرام اتفاقيات لمكافحة الإجرام المعلوماتي على غرار اتفاقية بودابست العاصمة البحرينية عام 2001 عقب الهجمات التي تعرضت لها الو م أ في العام ذاته.

كما تم عقد مؤتمرات دولية في هذا الشأن حول حماية أمن المعلومات والخصوصية في قانون الأنترنيت على غرار المؤتمر الدولي الذي أنعقد بالقاهرة العاصمة المصرية سنة 2008.

وقد عاد اختيارنا لهذا الموضوع الى جملة من الاسباب الذاتية والموضوعية فأما الاسباب الذاتية فهي:

- نظرا للأحداث التي يشهد العالم والطفرة التكنولوجية (التي واكبتها التكنولوجيا (عالم الحاسوب الانترنت) في ظهور جرائم حديثة (جرائم العصر) الا هي جرائم المعلوماتية أو ما يعرف بالجريمة الالكترونية وماوكبها في التطور الإرهاب التقليدي الذي اصبح يعتمد على هذه المادة الحيوية.
- أما عن الأسباب الموضوعية: فهو قصد الوقوف على هاته الجريمة الخطرة (التي اصبحت تفتك بالدول والمجتمعات، محاولة الخروج بنتائج من خلال دراسة هذا

الموضوع والوقوف على جل النقاط التي تشكل هاته الجريمة من خلال النصوص القانونية على الصعيدين الوصية والعالمي).

- وعن الهدف من هاته الدراسة هو محاولة اكتشاف وتحديد معالم هاته الجريمة المستحدثة والتي تعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصالات وشبكات المعلومات وذلك من خلال تحديد مفهوم هاته الجريمة المستحدثة، وبيان أسبابها ودوافعها وتحديد خصائصها وأهدافها ومن ثم إبراز أهم مظاهرها وأشكالها.
- وعن الصعوبات التي لاقت هاته الدراسة تمثلت في شقين اثنين.

أولها: تشخيصي ناتج عن الارتباطات المهنية الممارسة وإن كانت من قبل العمل الممارس في هذا المجال وما شابهه.

أما الشق الثاني فيتمثل في ندرة المراجع الحديثة والآنية والتي تتوافق وسرعة تطور هاته الجريمة واتساع رقعتها على الصعيدين الوطني والدولي التي لمس مجالات عديدة، واسعة وحساسة.

- ومما سبق كان لا بد من طرح إشكالية يجيب عندها من خلال خطة منهجية نعالج به هذا الطرح ونقوم بإعطاء وصف وتحليل لهاته الجريمة وعليه تكون الإشكالية كالآتي: فيما يتمثل مفهوم جرائم الإرهاب الإلكتروني؟

وما هو الإطار القانوني الذي يضبط هاته الجريمة في مجال الحد منها؟

- وباعتبار جرائم الإرهاب الإلكتروني من مواضيع العصر والحديثة فاعتمدنا في دراستنا على المنهج الوصفي التحليلي وذلك من خلال الوصف الدقيق والشامل لهاته الجريمة من خلال تحديد المفاهيم والمنهج التحليلي من خلال التطرق إلى أسباب ودوافع مجالات هاته الجريمة المستحدثة مع إبراز خصائصها وأهم مظاهرها وأشكالها.

وتقتضي الاشكالية المتحورة حول جريمة الارهاب الالكتروني تقسيم الموضوع على النحو الاتي:

الخطة

الفصل الأول: مفهوم الإرهاب الإلكتروني

المبحث الأول: تعريف الإرهاب الإلكتروني ومميزاته.

المطلب الأول: تعريف الإرهاب الإلكتروني.

المطلب الثاني: مميزات الإرهاب الإلكتروني.

المبحث الثاني: أسباب الإرهاب الإلكتروني وآثاره.

المطلب الأول: أسباب الإرهاب الإلكتروني.

المطلب الثاني: آثار الإرهاب الإلكتروني

الفصل الثاني: الإطار القانوني الوطني والدولي في مجال مكافحة جرائم الإرهاب الإلكتروني .

المبحث الأول: الإطار القانوني الوطني والإقليمي في مكافحة جرائم الإرهاب الإلكتروني.

المطلب الأول: الإطار القانوني الوطني في مكافحة هاته الجريمة.

المطلب الثاني: الإطار الإقليمي لمكافحة هاته الجريمة.

المبحث الثاني: التعاون الدولي لمكافحة هاته الجريمة والتحديات الممارسة في هذا المجال.

المطلب الأول: مجال الإطار القانوني الدولي لمكافحة جرائم الإرهاب الإلكتروني

المطلب الثاني: التحديات الممارسة في هذا المجال.

خاتمة

الفصل الأول: مفهوم الإرهاب الإلكتروني

تتعرض في هذا الفصل المفهوم الارهاب الإلكتروني من خلال التعريف بهاتته الجريمة من خلال الجريمة حد ذاتها الإرهاب ومدى ارتباطه بالأنترنت في صورة مواكبته الرهيب الحامل في هذا المجال ومميزاته (أسبابه ودوافعه، خصائصه) و وأهدافه والمظاهر التي تتجالى بها هاته الجريمة.

ونباءا على ما تقدم فسيتم تقسيم الفصل الأول إلى المباحث التالية:

المبحث الأول: تعريف الإرهاب الإلكتروني ومميزاته.

المبحث الثاني: خصائص وأهداف ومظاهر الإرهاب الإلكتروني.

المبحث الأول: تعريف الإرهاب الإلكتروني ومميزاته.

لقد تعددت تعاريف الإرهاب واختلفت وتشابهت في نشأته، الاجتهادات ولم يصل المجتمع الدولي حتى الأن إلى تعريف جامع مانع متفق عليه للإرهاب.

ويرجع ذلك إلى تنوع أشكاله ومظاهره وتعدد أساليبه وانماطه واختلاف وجهات النظر الدولية والإتجاهات السياسية حوله وتباني العقائد والإيدولوجيات التي تعتنقها الدول، فيما يراه البعض إرهابا يراه البعض الأخر عمل مشروع ومباح كما أنا الإرهاب الإلكتروني مجموعة من السمات التي تختلف فيها عن بقية الجرائم وتمول دون اختلاطه بالإرهاب العادي.

ونستعرض لتعريف الإرهاب الإلكتروني ومميزاته على النحو التالي:

المطلب الأول: تعريف الإرهاب الإلكتروني

المطلب الثاني: مميزات الإرهاب الإلكتروني

المطلب الأول: تعريف الإرهاب الإلكتروني

إن ما يتميز به الإرهاب الإلكتروني عن (الإرهاب التقليدي بالطريقة العصرية المتماثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات إن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

ويشير الإرهاب الإلكتروني إلى عنصرين أساسين هما.

1- الفضاء الافتراضي

2- العالم الافتراضي

وهذا المكان الذي تعمل به أجهزة وبرامج الحاسوب والحواسيب المعلوماتية كما تنتقل فيه المعلومات الإلكترونية والإرهاب، وقد استفادت المنظمات الإرهابية من تلك التقنية وإستغلالها في إتمام عملياتها الإجرامية مما زاد من خطورتها، مما أصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية وإستخدماتها في تدمير البنية التحتية المعلوماتية التي تعتمد عليها الحكومات والشركاء الاقتصادية الكبرى.

كما تكمن خطورة الإرهاب الإلكتروني في سهولة استخدام الشبكات الرقمية وهو مستتر بعيدا عن أنظار السلطة حيث ازداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الألية والشبكات المعلوماتية، مما تجعلها سهل المنال[1]، فبدلا من استخدام المتفجرات، تستطيع الجماعات الإرهابية، من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الحيوية، وشل أنظمة القيادة والاتصالات أو قطع شبكات الإتصال بين الوحدات والقيادات المركزية أو تعطيل انظمة النخاع الجوي أو إخراج الصواريخ عن مسارها أو التحكم في خطوط الملاحة الجوية أو البرية أو البحرية أو شل محطات امتداد الطاقة أو الماء، أو اختراق النظام المرفي مما يضر بأعمال البنوك والأسواق العالمية[2]

ووفقا للتعريف الإلكتروني الذي قدمته دورثي دينيج أحد أبرز الباحثين في مجال الأمن الإلكتروني، يجمع مصطفى الإرهاب الإلكتروني Cyber Terrorisim ما بين مفهوم "الإرهاب" و "الفضاء الإلكتروني" ومن ثم فهو يشير إلى الامتدادات والتهديدات الموجهة لأجهزة الحاسب الألي والشبكات الإلكترونية والمعلومات الموجودة عليها بهدف إجبار المعلومات والمجتمعات على أفعال معينة لأغراض سياسية أو اجتماعية ولكن يشرط لكي يصنف هجوم ما بأنه إرهاب الكتروني[3].

أن ينتج عنه اضرار بالممتلكات أو الأفراد وخلق حالة من الخوف لدى الهدف، ومن ثم تخرج الهجمات التي تستهدف خدمات ليست على درجة كبيرة من الأهمية خارج إطار مفهوم الإرهاب الإلكتروني إذ لابد أن يكون الهدف حيويا وهاما بالنسبة لحياة المواطنين ولعمل الدولة، ويضاف إلى ذلك أن هجمات الإرهاب الإلكتروني لابد وأن تكون مدبرة ومخطط لها سابقا وتهدف إلى تدمير الهدف وإلحاقه بدرجة عالية من الضرر وليس فقط إحداث خلل في عمله.

---

[1] مصطفى يوسف كافي، جرائم الفساد، غسيل الأموال، السياحية، الإرهاب الإلكتروني، المعلوماتية، ط1، 2015، مكتبة المجتمع العريب للنشر والتوزيع، عمان، الأردن، ص143.

[2] د. مصطفى يوسف كافي، نفس المرجع، ص143.

[3] نوران شقيق، أثر التهديدات الإلكترونية على العلاقات الدولية، ط1، 2016، مصر القاهرة، ص3

- ويعود مفهوم الإرهاب الإلكتروني إلى بناية التسعينات نتيجة للزيادة الكبيرة في معدلات استخدام الانترنت والاعتماد عليه في إدارة شؤون الدول، مما أدى الى التخوف من أن يستخدم الإرهابيون هذه التكنولوجيا الحديثة في إحداث أضرار قد توفق في بعض الأحيان تلك الناتجة عن العمليات الإرهابية التقليدية[1].
- تزايدت هذه المخاوف من الإرهاب الإلكتروني بعد أحداث 11 سبتمبر لما يوفره الفضاء الإلكتروني من فرص للتنظيمات الإرهابية للقيام بهجمات تترتب عليها أضرار جسيمة[2].
- ولابد من التمييز بين الحرب الالكترونية والهجوم الإلكتروني فالحرب الإلكترونية تفترض وجود تفاعل ما بين فاعلين أو أكثر، بمعنى تلك الهجمات التي يقوم بها فاعل من فاعل أخر ليس لديه الرغبة أو القدرة على الرد على هذا الاعتداء لا يتخدل في إطار الحرب الإلكتروني.

المطلب الثاني: مميزات الإرهاب الإلكتروني

بالنظر الى طبيعة هاته الجريمة نجد أنها تتسم بمجموعة من الخصائص والمميزات ونحاول من خلال هذا المطب تلميذا فيمايلي:

- سهولة ارتكاب هذه الجريمة نظرا لاستخدام الوسائل ذات الطابع التقليدي.
- سهولة إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها.
- حرفية ارتكاب الجريمة مما يتطلب قدرا كبيرا من الذكاء والمعرفة من جانب ارتكابها وقدرا أكبر من الحرفية من جانب من يتولى الإشراف على جهود المكافحة.
- سرعة ارتكاب هذا النوع من الجرائم لاعتمادها على وسائل الإتصال الحديثة.
- أثار هذه الجريمة التي تتمثل في إحداث هزات كبيرة لمختلف المجالات لدى الدول.
- ترتكب الجرائم عبر الإنترنت بدقة بالغة نتيجة دقة أدوات الجريمة (شبكة الإنترنت).

[1] نوران شفيق، المرجع السابق، ص36.
[2] نوران شفيق،نفس المرجع ، ص39.

- جرائم تتسم بالغموض حيث يصعب إثباتها والتحقيق فيها مما هو الحال في الجرائم التقليدية.
- جريمة إلكترونية غير مادية[1].
- مرتكبو هذه الجرائم لهم صفات مميزة من حيث الثقافة والعلم التكنولوجي، فالمجرم في هذا النوع من الجرائم ليس عاديا فهو يرتكب جريمة متخصصة[2].
- جريمة قد تمتد إلى خارج حدود مرتكبيها إلى دولة أخرى.
- يسهل ارتكاب هذه الجريمة نظرا لأنها طابع تقليدي مما أنه من السهل إخفاء عالم الجريمة وصعوبة تتبع مرتكبيها[3].
- وتتشابه جماعات الإرهاب الإلكتروني Cyber Terrorisme مع القراصنة السياسيين في نوع الهجمات التي يقومون بها، إذ أن هجماتهم غالبا ما تكون مدفوعة بأهداف سياسية، غير أن نطاق الهجمات التي يقومون بها تختلف عن القراصنة، فالهدف الرئيسي الذي يسعى الإرهابيون الإلكترونيون إلى تحقيقه هو إلحاق الضرر بأهداف تمثل أهمية كبرى بالنسبة للدولة والمجتمع سواء اقتصاديا أم سياسيا أم تجاريا... إلى أخره في حين يكون هدف القراصنة السياسيين هو فقط الضغط السياسي دون إحداث أضرارا بالغة الضرورة.
- وقد تشترك هذه الجماعات في تلك الهجمات الإلكترونية التي تدعمها الدول أو تشارك في تسهيل العمليات التي تقوم بها الشبكات الإجرامية المنظمة.

وعادة ما تمتلك هذه الجماعات الإرهابية الإلكترونية مهارات عالية، وتعمل بشكل سري وتكون ممولة بشكل جيد وتكون له أهداف ايديلوجية وتشتغل المنظمات الإرهابية الأنترنت في عدة صور كالتالي:

---

[1] نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، دار الفكر الجامعي، الإسكندرية،2006،ص35

[2] محمد العلماء، جرائم الإنترنت والإحتساب عليها، دراسة منشور في الجامعة العربية للدراسات الأمنية والتدريب المجلة18، العدد36. منشورات أكادمية تأليف للعلوم الأمنية، الرياض، أكتوبر 2003، ص26.

[3] عبد الله علي محمودإجراءات جمع الأدلة في مجال سرقة المعلومات، منشور على الموقع الإلكتروني http//.www.qanoun.net

فهي تقوم باستخدامه باعتباره أنه وسيط لتحقيق التواصل فيما بينها مع التمتع بدرجة كبيرة من السرية ومن ثم يستطيع أعضاء هذه المنظمات تناقل المعلومات والأوامر فيما بينهم وتداول الأوامر التنفيذية والتخطيط للهجمات فضلا عن القيام بحملات لجمع الأموال لتنفيذها.

وبما أن الأنترنت يعتبر وسيط لتحقيق الإتصال فإن الأنترنت أيضا قد يتم استخدامه للدعاية، فهذه المنظمات والجماعات الإرهابية كثيرا ما تقوم باستخدام الإنترنت للدعاية لنفسها من خلال نشر بعض المعلومات والبيانات والفيديوهات الخاصة بها[1].

- كما أن الأنترنت حاليا يوفر مختلف المنظمات والجماعات وحتى الأفراد المعرفة التكنولوجية اللازمة للقيام بهجمات إلكترونية ولذلك يعتبر البعض أن الإنترنت قد أصبحت بمثابة معسكر تدريب افتراضي للإرهابيين لامتلاك القدرات التكنولوجية الازمة للقيام بالهجمات الإلكترونية إلا أن أراء المحللين تختلف في هذا الصدد فعلى سبيل المثال دانيال كيميدج يعتبر أن لجوء الجماعات وإنها هي قد أجبرت على ذلك بسبب افتقادها للتنظيم في حين يرى البعض الأخر أن لجوء الجماعات الإرهابية للفضاء الإلكتروني يصنف إليها مصدرا أخر من مصادر القوة خاصة وإن مارست هذه الهجمات في الدول المتقدمة
- مما سبق عرضه، يتضح مدى تعدد أشكال التهديدات الإلكترونية ومصادرها وآلياتها إلى حد يصعب معه حصرها بشكل كامل، وإنما فقط بيان أكثرها خطورة وانتشارا وتأثيرا في أمن الفواعل[2].
- ومن ثم بات الأمن الإلكتروني من أحد أهم أشكال الأمن التي تسعى الفواعل إلى تحقيقه والحفاظ عليه، وخاصة الدول التي قد تؤثر فيها هذه التهديدات على أمن الأفراد والشركات والمجتمع ككل. كما تسع دائرة الفضاء الإلكتروني لشمل كافة

[1] نوران شقيق، المرجع السابق، ص47.
[2] نوران شقيق، نفس المرجع ، ص48.

القطاعات، سواء على مستوى الفرد أم الدولة، فنجد أن دور الفضاء الإلكتروني يبدو بارزا في المجالات السياسية والاقتصادية والاجتماعية وغيرها، مما يزيد من المخاوف الأمنية حال وقوع أي هجوم أو اعتداء إلكتروني قد يضر بأي من هذه القطاعات الحيوية، ومن ثم، يمكن القول بأن الأمن الإلكتروني يجمع ما بين الأمن الإنساني والقومي، وهو ما يميزه عن الصور التقليدية لمفهوم الأمن.

غير أن مدى خطورة التهديدات الإلكترونية لا يتوقف فقط على تعدد أشكالها وأنواعها، وإنما أيضا على مدى خطورة الآثار المترتبة عليها، وهو ما يستوجب تحديد حجم الخسائر التي قد تحدثها الهجمات الإلكترونية وإلى أي مدى تستطيع أن تهد أمن الفواعل، وما إذا كانت قدرتها التدميرية تساوي أو تزيد في خطورتها عن التهديدات التقليدية[1].

- كما أن الإرهاب الإلكتروني في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب ألي متصل بالشبكة المعلوماتية فقط ومزود ببعض البرامج اللازمة.
- يتسم الإرهاب الإلكتروني بأنه عابر للدول والقارات، وغير خاضع لدولة معينة.
- صعوبة إثبات جرائم الإرهاب الإلكتروني، لغياب الدليل الرقمي من ناحية وسهولة إتلافه وتدميره من ناحية أخرى.
- أن مرتكب الإرهاب الإلكتروني في العادة من المتخصصين في مجال تقنية المعلومات ، أو لديه – على الأقل قدر من المعرفة والخبرة في التعامل مع الشبكات المعلوماتية.

كما أن أهدافه تتميز ب:

1- بنشر الخوف والرعب بين الأشخاص والدول، وتعريض سلامة المجتمع وأمنة للخطر.

2- الإخلال بالأمن المعلوماتي وزعزعة الطمأنينة.

[1] نوران شفيق، نفس المرجع السابق، ص48.

3- تدمير المبنى المعلوماتية التحتية، والإضرار بوسائل الاتصالات وتقنية المعومات[1].

4- الدعاية والإعلان وإثارة الرأي العام.

5- الاستلاء على الأموال.

[1] مصطفى يوسف كافي، المرجع السابق، ص 148.

المبحث الثاني: أسباب الإرهاب الإلكتروني وأثاره.

تختلف أسباب ودوافع الإرهاب الإلكتروني وأثاره وخطورته من حيث الأشكال والمصادر وتتراوح الخطورة بين البسيطة والمعقدة.

وهو ما سنحاول التطرق إليه من خلال الأسباب العامة للإرهاب الإلكتروني والأسباب الخاصة في المطلب الأول.

لنختم دراستنا في هذا المبحث بالتطرق إلى أثار الإرهاب الإلكتروني وخطورته في المطلب الثاني.

المطلب الأول: أسباب الإرهاب الإلكتروني.

إن الإرهاب الإلكتروني يختلف عن الإرهاب العادي من حيث منهجية العمل وذلك من خلال طريقة العمل والهدف في ظل ظهور ما يعرف بالعولمة إلا أن الأسباب والدوافع نشأت عصر السرعة والعالم الافتراضي غير المادي ومن هذه الأسباب تكمن فيما يلي:

أسباب الإرهاب الإلكتروني:

أولا: الأسباب العامة للإرهاب الإلكتروني:

تختلف أسباب الإرهاب ودوافعه تبعا لاختلاف الجهات السياسية والظروف الاقتصادية والأحوال الاجتماعية، والاختلاف الديني والعقائدي.

1- الدوافع الشخصية مثل:

أ. الرغبة في الظهور وحب الشهرة.

ب. الإحباط في تحقيق بعض الرغبات أو الوصول إلى المكانة المنشودة، وإحساس الشخص بأنه أقل من غيره وينظر إليه نظرة متدينة، فيلجأ إلى الإرهاب للخروج علا النظام.

ج. فشل الشخص في الحياة الأسرية، مما يؤدي إلى الجنوح وعدم الشعور بالانتماء والولاء للوطن.

د. الإخفاق الحياتي، إلى قد يكون إخفاقا في الحياة العلمية أو العملية، أو النواحي الوظيفية، أو التجارب العاطفية، مما يجعله يشعر بالفشل في الحياة[1].

2- الدوافع الفكرية مثل:

أ. الفراغ الفكري، والفهم الخاطئ للدين ومبادئه وأحكامه وآدابه، وسوء تفسيره.

ب. التطرف وخاصة في الأمور الفكرية.

3- الدوافع السياسية ونذكر منها:

أ. غياب العدالة الاجتماعية في بعض الدول، وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات في المرافق الأساسية، والاستيلاء على الأموال العامة

ب. اعتقاد الإرهابي انتهاك حقوقه وحرماته، وخرق القوانين والمواثيق الدولية، حيث أدى ذلك إلى التشدد والتطرف.

4- الدوافع الاقتصادية مثل:

أ. تفاقم الأزمات الاقتصادية في المجتمعات الدولية، بالإضافة إلى المتغيرات الاقتصادية العالمية، والاستغلال غير المشروع للموارد الاقتصادية لبلد معين.

ب. عدم إقامة تعاون دولي جدي من قبل الأمم المتحدة، وعدم إيجاد تنظيم عاجل ودائم لعدد من المشاكل العالمية، مثل اغتصاب الأراضي والاضطهاد[2].

ج. معاناة الأفراد من المشاكل الاقتصادية المتعلقة بالإسكان والفقر وغلاء المعيشة والتضخم في أسعار المواد الغذائية والخدمات الأساسية، وعدم تحسن دخل الفرد، مما يؤدي إلى تفشي روح التذمر ويدفع الشباب إلى التطرف والإرهاب.

[1] مصطفى يوسف كافي، المرجع السابق،ص 144.
[2] مصطفى يوسف كافي، نفس المرجع ص 145.

د. انتشار البطالة في المجتمعات المختلفة وعدم توفر فرص العمل، مما ساهم في ظهور جرائم السرقات والإرهاب. .. التقدم التقني للأنظمة المصرفية العالمية ومما أدى إليه من سهولة انتقال الأموال وتحويلها بين جميع أرجاء العالم عن طريق شبكة الانترنت، ساعد المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أهدافهم غير المشروعة.

5- الدوافع الاجتماعية مثل:

أ. التفكك الأسري، مما يؤدي إلى انتشار الأمراض النفسية والانحراف والإرهاب، خاصة وأن الترابط الأسري يحيط الأشخاص بشعور التعاون والتماسك.

ب. الفراغ النفسي والروحي والعقلي جعل الفرصة سانحة لقبول كل فكر هدام ومتطرف.

ثانيا: الأسباب الخاصة للإرهاب الإلكتروني وهي:

1. ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: حيث إن شبكات المعلومات مصممة بحسب الأصل بشكل مفتوح دون حواجز أمنية عليها، رغبة في تسهيل دخول المستخدمين. ويمكن للمنظمات الإرهابية استغلال الثغرات المتواجدة في الأنظمة الالكترونية والشبكات المعلوماتية، يفي التسلل إلى البني المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية[1].

2. عدم الوضوح الهوية الرقمية للمستخدم يجعل الفرصة سانحة للإرهابيين، حيث يستطيع محترف الحاسوب أن يتخفى تحت شخصية وهمية، ويشن بالتالي هجومه الإلكتروني بعيدا عن مراقبة السلطات العامة.

3 - سهولة استخدام شبكة المعلومات وقلة التكلفة مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون حاجة إلى مصادر تمويل، فشن هجوم إرهابي إلكتروني لا

[1] مصطفى يوسف كافي، المرجع السابق، ص146.

يتطلب أكثر من جهاز حاسب إلى متصل بالشبكة المعلوماتية ومزود با

فصعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب الإرهاب ا

تساعد المجرم على الإفلات من العقوبة

4- صعوبة اكتشاف و إثبات الجريمة الإرهابية ، خاصة في مجال جرائم الاختراق، مما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته.

5- غياب السيطرة والرقابة على الشبكات المعلوماتية، ولجوء المجرم الإرهابي إلى دول معادية لشن هجومه على الدول الأخرى[1].

اثار الهجمات الإلكترونية وخطورتها

تختلف التهديدات الإلكترونية من حيث أشكالها ومصادرها ودرجة خطورتها وتتراوح ما بين تهديدات بسيطة ومتوسطة ومعقدة، فالتهديدات البسيطة simple threats تتمثل في تلك الهجمات التي يستطيع أي فرد يمتلك قدرات تحليلية وتقنية بدائية القيام بها. تشير القدرات التحليلية إلى القدرة على تحديد الهدف المراد مهاجمته وتحليل نقاط الضعف الموجودة فيه والتي يمكن مهاجمتها. أما القدرات التقنية فتشير إلى امتلاك الآليات الإلكترونية من برامج وشبكات للقيام بالهجوم[2].

إذ يستطيع أي فرد أن يقوم بتحميل البرامج الخاصة بالقرصنة من الإنترنت وتحديد هدف ما لمهاجمته، دون الحاجة إلى وجود موارد خاصة أو هياكل مؤسسية للقيام بالهجوم. ولقد أصبح هذا النوع من الهجمات شائعا بشكل كبير على شبكة الإنترنت، وهناك نوع آخر من التهديدات يكون أكثر تقدما، وفيه يمتلك المهاجم معرفة واسعة بالهدف وأنظمة الأمان التي يطبقها و الأنظمة المشغلة للأجهزة الإلكترونية الخاصة به، ويستطيع وضع سيناريوهات مختلفة المهاجمته مما يمكنه من القيام بهجمات أكثر تعقيدا من الهجمات البسيطة.

[1] مصطفى يوسف كافي، المرجع السابق، ص147..
[2] نوران شقيق، المرجع السابق ص50.

غير أن هذه التهديدات، وعلى الرغم من خطورتها، لا ترقى إلى مستوى التهديدات المركبة أو المعقدة Complex threats والتي تعد أكثر تعقيدا وصعوبة في التنفيذ مقارنة التهديدات السابقة، ومن ثم فهي تمثل الخطر الأكبر على أمن الدول، هذا النوع من الهجمات لا يمكن القيام به من فرد أو مجموعة صغيرة من الخبراء، وإنما يتطلب الأمر مجموعات كبيرة وفرق مكونة من عدد كبير ممن يمتلكون قدرات ومعرفة بكافة الجوانب التقنية المعرفة الكاملة بطبيعة الشيكات، وأنظمة التشغيل، وأنظمة التحكم، وكيفية جمع المعلومات الاستخباراتية وتحليلها، ومن ثم فهي تحتاج إلى تدريب شديد التعقيد والقيام بتجارب على القيام بالهجوم وهو ما يتطلب كما كبيرا من الأموال والموارد والمعرفة التقنية و التحليلية.

إلا أن القدرة على القيام بأي هجوم ضد أي هدف تعتمد بالأساس على مدى توافر نقاط ضعف في النظام الإلكتروني الخاص به يمكن استغلالها. فهناك أنظمة إلكترونية تكون أكثر عرضة للهجمات الإلكترونية مقارنة بغيرها، ناهيك عن الهجوم الجزئي على هدف أو قطاع معي أو الهجوم الشامل (الحرب). وفيما يلي نوضح ما تشير إليه القابلية للتعرض للهجوم" Vulnerability في الأنظمة الإلكترونية والتي تختلف من مؤسسة الأخرى ومن نظام الكتروني لأخر[1].

القابلية للتعرض للهجوم:

لقد أصبحت تكنولوجيا المعلومات والاتصالات جزءا أصيلا من عمل الدول ومن بنيتها التحتية، ومحركا رئيسيا للتنمية الاجتماعية والاقتصادية، ولقد زادت أهمية الإنترنت وتكنولوجيا المعلومات والاتصالات على مدار الأربعة سنوات الماضية وخاصة بدءا من عام 2000، ليس فقط بالنسبة للحكومات، وإنما أيضا للقطاع الخاص، وما ترتب على ذلك من سهولة وصول الخدمات للأفراد والتي أصبحت تصل لأكثر من 2.5 مليار مواطن. وتصل نسبة مساهمة الإنترنت في الناتج المحلي الإجمالي في بعض الدول ل 8 بالمائة. وهو ما

[1] نوران شقيق، المرجع السابق، ص50.

ترتب عليه أن أصبحت المنافع الاقتصادية والتكنولوجية والسياسية والاجتماعية المرتبطة بالفضاء الإلكتروني في خطر نتيجة لشدة الاعتماد عليه.

فمن المتوقع أنه في العقد القادم سيصل الإنترنت إلى 60 بالمائة من السكان على مستوى العالم أي أكثر من 5 مليار مواطن، وسيصل ما بين أكثر من 50 مليار جهاز وسيسهم في الناتج المحلي الإجمالي ل 10 بالمائة من الدول النامية. وهو ما سيؤثر بدوره في الشئون الاقتصادية والسياسية والاجتماعية والأمن القومي للدول[1].

ولكن لابد وأن يتضمن أي نظام إلكتروني بعض نقاط الضعف التي يمكن استغلالها في شن الهجمات الإلكترونية. ولهذا السبب تقوم معظم المؤسسات بمحاولة وضع أنظمة للتأمين يكون الهدف منها هو محاولة معالجة نقاط الضعف هذه والتخفيف منها. ففي حالة التهديدات البسيطة، يتم استغلال نقاط الضعف الواضحة الموجودة في الأنظمة الإلكترونية الرئيسية التي لا ينصب اهتمام الدول والمنظمات على معالجتها[2].

كما أن الهجمات المتقدمة أيضا يتم فيها استغلال نقاط الضعف الظاهرة في الأنظمة الإلكترونية، إضافة إلى إمكانية الوصول إلى نقاط الضعف الأقل بروزا في نظام ما عن طريق استخدام التقنيات الحديثة. وفي هذا النوع من التهديدات، يتمكن المهاجم من استغلال نقاط الضعف في تطبيقات مشتركة ما بين عدد من المنظمات، وإن كان لا يمتلك القدرة في هذه الحالة على مهاجمتها جميعا بشكل متزامن. أما التهديدات المركبة، فيتم التوصل فيها إلى نقاط الضعف غير الواضحة داخل النظام، سواء في مؤسسة واحدة أم أكثر، ويمكن في هذه الحالة شن هجوم متزامن على كافة هذه المؤسسات.

ومن ثم يمكن القول بأن التهديدات البسيطة تقوم باستغلال نقاط الضعف المعروفة والواضحة، في حين أن التهديدات المتقدمة يتم فيها اكتشاف نقاط ضعف جديدة، ولكن يكون المهاجمون مقيدين في كيفية استغلالها، أما التهديدات المركبة فمن الممكن فيها

---

[1] Melissa E. Hathaway, Alexander Klimburg, (2012). Preliminary Considerations: On National Cyber Security. In Alexander Klimburg

[2] نوران شقيق، المرجع السابق، ص52.

التعرف على نقاط ضعف غير معروفة واستغلالها والقيام بهجمات الشبكات والأنظمة والمؤسسات. وتعتمد احتمالية نجاح أي تهديد با وطبيعة النظام الذي تتم مهاجمته، والاستراتيجيات المتبعة من قبل الهد

ومما يزيد من قابلية وقوع الهجمات الإلكترونية نقاط الضعف في الانظمه الإبحروبيه المختلفة، فالبرامج الخاصة بالحاسب الألي يتم تطويرها من خلال لغة برمجية معينة programming language ككود للحاسب الآلي. هذه الأكواد غالبا ما تتضمن بعض الأخطاء. فمع زيادة سرعة الحواسب الآلية أصبحت البرامج المشغلة أكثر تعقيدا، ولذا يحتوي البرنامج على ملايين السطور من الأكراد، والتي قد تتضمن بعض الأخطاء في أثناء تطويرها من قبل المبرمجين، هذه الأخطاء الكودية لا يمكن اكتشافها بسهولة حتى من تلك البرامج المصممة خصيصا لمراجعة الأكواد[2].

كما أن الأجهزة hardware سواء أجهزة الحاسب الآلي أو المعالج الدقيق micro processor و الدوائر الكهربية و الموزع router و أنظمة الاتصال وغيرها، والتي يتم تصنيعها وتجميعها في أكثر من دولة هي أيضا عرضة الهجمات الإلكترونية، فقد يتم تغبير أحد أجزائها سرا حتى لا تعمل بالشكل المطلوب أو أن تفسح المجال للبرامج الخبيثة، وقد يتم مهاجمة البرامج المشغلة لها لتحقيق ضرر مادي بالجهاز ذاته، كما حدث في حالة هجوم ستاكسنت Stuxnet.

ويضاف إلى هذه العوامل أن كل الأنظمة المسئولة عن تشغيل الإنترنت مفتوحة و غير مشفرة unencrypted، ومعظم المعلومات التي يتم إرسالها أيضا غير مشفرة باستثناء عدد محدود منها. كما أن مقدمي الخدمة يكون بإمكانهم الوصول إلى معلومات عن المواقع التي

(ed.), Naficantal Cyber Sectrify: Framework Maurital (op:1-34) NATO CCD COE Publication, Talin, pp:34

[1] Inving Lachow. (2009) Cyber Terrorismn; Menace of Myth? In Franklin D. Kramer et al (eds.). Cyberpower and National Security (437-463), Potorrac Books Inc. Pp:442-447[1]

[2] نوران شفيق، المرجع السابق، ص52.

يدخل إليها المستخدمون أو البريد الإلكتروني الخاص بهم وغيرها من المعلو

دورا في زيادة مخاطر التهديدات الإلكترونية[1].

فالطبيعة غير المركزية للإنترنت وغياب قواعد منظمة له تؤدي إلى زيادة احتما

الأنظمة الإلكترونية للهجمات. وكلما زاد اعتماد الدولة على الفضاء الإلكتروني في إدارة شئونها كلما زادت نقاط الضعف الإلكترونية لديها، من ثم زادت فرص تعرضها للهجوم الإلكتروني، ومع تزايد استخدام الإنترنت سواء من الشعوب أو الحكومات، باتت كثير من الدول تواجه عديدا من التهديدات الإلكترونية، ولذا تسعى لتطوير أنظمتها الدفاعية لتحسين قدرتها على مواجهة تلك المخاطر والتهديدات الإلكترونية، ولذا تسعى لتطوير أنظمتها الدفاعية لتحسين قدرتها على مواجهة تلك المخاطر والتهديدات.

وعليه، يمكن القول بأن المخاطر الناشئة عن الفضاء الإلكتروني تتسم بثلاث سمات رئيسية نوضحها كالتالي:

1- تتسم المخاطر الإلكترونية باتساع نطاقها وتعدد مستوياتها، فكل ما هو جزء من الفضاء الإلكتروني قد يكون هدفًا للهجمات الإلكترونية، ومن ثم فقد يؤثر ذلك في البنية التحتية الحيوية داخل الدولة، أو على النظام المالي لها، أو يؤدي إلى سرقة حقوق الملكية الفكرية أو سرقة المعلومات التي تقع على درجة كبيرة من الأهمية بالنسبة للدولة، أو تعطيل استخدام الدولة للآليات التكنولوجية في إدارة شئونها أو تدمير الأجهزة الإلكترونية ذات الصلة بالأمن القومي للدولة.

2- هذه المخاطر الأمنية تعد جزءًا من الفضاء الإلكتروني، بمعنى أنها تتم عن طريق استغلال نقاط الضعف في الأنظمة الإلكترونية وحتى أكثرها تعقيدًا أو من خلال البرامج الخبيثة القادرة على اختراق هذه الأنظمة ومن ثم، لا يمكن إيقاف هذه المخاطر كليًّا.

3- تتسم المخاطر الإلكترونية بتنوعها، سواء من حيث طبيعتها أم من حيث مصادرها، فقد تشنها دول أو منظمات إجرامية، أو أفراد، أو إرهابيين، وغيرهم.

[1] نوران شفيق، المرجع السابق، 53.

فطبيعة الفضاء الإلكتروني جعلت من المخاطر الأمنية الناتجة عن التفاعل عن التهديدات الأمنية التقليدية، وما يعزز من هذا الاختلاف هو اتساع الإلكتروني، حيث إنه يتخطى الحواجز الجغرافية والمكانية ومن ثم يجمع التي تمتلك مصالح ورؤى استراتيجية متنوعة. كما أن العولمة في مجال الفضاء الإلكتروني أصبحت من الأمور الحتمية، واعتماد الدول المتزايد على الأنظمة الإلكترونية لم يعد أيضًا من الممكن التراجع عنه، مما يزيد من المخاطر التي قد تتعرض لها الفواعل نتيجة لهذا الاعتماد المتزايد.

كما أن معدلات التطور في الفضاء الإلكتروني مرتفعة، ومن ثم يترتب على كل تطور ظهور نقاط ضعف جديدة تهدد أمن الفواعل. أي إن الفضاء الإلكتروني يتسم بديناميكيته. كما أن عدم القدرة على التأكد من هوية القائم بالهجوم هو أحد العوائق التي تواجه الفواعل في التعامل مع التهديدات الإلكترونية وهو ما يختلف عن التهديدات التقليدية[1].

فلقد صمم الإنترنت بدرجة عالية المرونة تفتح المجال إلى التطوير المستمر فيه وتحقيق درجة عالية من التواصل ما بين الأفراد والشبكات وتبادل المعلومات بتكلفة منخفضة. غير أن هذه التطورات المتلاحقة والمتسارعة أدت إلى ظهور عديدٍ من نقاط الضعف التي تستغل في القيام بهجمات إلكترونية. كما نتج عن طبيعة الإنترنت عديدٌ من التحديات الأمنية، إذ إنه قد صمم بحيث يكون نظامًا إلكترونيًّا يتسم باللامركزية يعمل فيه الأفراد والجماعات بسرية أي دون أن يكون هناك إمكانية للتعرف على هويتهم. وهنا تظهر مشكلة أن ينسب هجوم ما إلى طرف معين، ومن ثَم تصبح بعض الهجمات الإلكترونية غير قابلة للتتبع.

هذا التحدي المتمثل في صعوبة إسناد الهجوم لفاعل معين يمثل مصدر قوة للفواعل الدولية في مجال الفضاء الإلكتروني حتى تتسم عملياتهم بالسرية وعدم القدرة على التعرف على هويتهم ومن ثم معاقبتهم. إذ يصعب في هذه الحالات التعرف على هويتهم أو تعقبهم أو رد

[1] نوران شفيق، المرجع السابق، ص54.

هذه الهجمات خاصة وإن كان مصدرها أكثر من جهاز إلكتروني ومقدم للخدمة في أكثر من دولة.

كما تزايد استخدام الإنترنت حول العام ليس فقط على مستوى الأفراد ولكن أيضًا الدول. فلقد تطور الإنترنت بصورة سهلت استخدامه والتفاعل من خلاله واستخدام وظائفه. فهناك أكثر من 2 مليار مستخدم للإنترنت حول العالم، سواء في الدول النامية أم المتقدمة. وكلما زادت كفاءة الإنترنت وتطويره حيث يسهل استخدامه، زاد عدد مستخدميه، ومن ثم زادت المخاطر الأمنية التي قد يتعرض لها كافة هؤلاء المستخدمين. فهذه الزيادة المضطردة في استخدام الإنترنت تقدم مزيدًا من الأهداف والآليات للهجمات الإلكترونية.

كما أن هناك درجة عالية من الاندماج ما بين الشبكات المختلفة من خلال الإنترنت مما يزيد من مخاطر الهجمات الإلكترونية التي قد تؤدي إلى خسائر في الأموال، في الوقت، وفى الإنتاج، وفى المعلومات الهامة، أو حتى خسائر في الأرواح نتيجة للتأثير في الأنظمة الحيوية والبنى التحتية. فالبنى التحتية لأية دولة سواء المالية أو الإلكترونية أو الخاصة بالاتصالات وغيرها من أكثر الأهداف عرضة للهجمات الإلكترونية داخل الدولة خاصة في الدول المتقدمة[1].

المطلب الثاني: أثار الإرهاب الإلكتروني

تتمثل الهجمات الإلكترونية بشكل عام في مجموعة الاختراقات الموجهة الشبكات الحاسب الآلي لسرقة أو تغيير معلومات، أو تدمير النظام الإلكتروني، أو استخدام الشفرات الخبيثة والتي تنتقل من حاسب آلي إلى آخر وتقوم بتعطيل الوظائف التي تقوم بها تلك الأجهزة، أو إيقاف عمل الشبكات.

[1] نوران شقيق، المرجع السابق،ص55.

وباستخدام هذه الوسائل يستطيع القائمون بالهجوم الإضرار بالمؤسسات المالية، وأجهزة الاتصالات، والبنى التحتية، والمؤسسات الحكومية، والمستشفيات، وغيرها من الكيانات التي تعتمد بشكل كبير على أجهزة الحاسب الآلي في القيام بأعمالها الرئيسية. وهو ما يترتب عليه تعطيل المحركات الرئيسية لاقتصاد الدولة والإضرار بمواطنيها وتهديد أمنها القومي بشكل عام. ولذا تكون التداعيات الدولية لتلك الهجمات خطيرة وواسعة النطاق وتتخطى حيز الدولة لتؤثر في الأمن العالمي ككل.

ولقد أدى التزايد في درجة تعقيد وتشابك أنظمة البنى التحتية في عديد من الدول وتزايد اعتمادها على أجهزة الحاسب الآلي إلى زيادة قابلية تعرضها الهجمات الإلكترونية واتساع نطاق التأثيرات المحتملة المترتبة على هذه الهجمات. فعلى سبيل المثال، إذا اسفرت الهجمات الإلكترونية عن توقف الطاقة الكهربائية أو الاتصالات، قد يؤدي ذلك إلى تأثيرات متتالية على البنوك والمستشفيات والمؤسسات الحكومية[1].

ومن الخسائر التي قد تنتج عن الهجمات الإلكترونية، سواء بالنسبة للدول أو المنظمات أو الشركات هو انخفاض الإنتاجية، وانخفاض المبيعات، فضلا عن التكاليف المترتبة على عمليات الدفاع لصد الهجوم الإلكتروني، والجزاءات القانونية التي قد تتكبدها الشركات لعدم تقديم الخدمة للمستخدمين، وذلك في حالة تعرضها لهجمات الحرمان من الخدمة.

فوفقا لتقرير أعده مكتب التحقيقات الفيدرالي FBI ووكالة المخابرات المركزية الأمريكية CIA في عام 2003، لم تتمكن أغلب الجهات المعرضة الهجمات الحرمان من الخدمة من حساب الخسائر المترتبة عليها، وإن كانت ال 201 جهة التي استطاعت القيام بذلك قد قدرت الخسائر التي تكبدتها ب66.6 مليون دولار في خلال عام.

[1] نوران شقيق، المرجع السابق، ص56.

كما أن الهجمات على البنية التحتية الحيوية كتلك الخاصة بالطاقة، والاتصالات، والمواصلات، والأجهزة الحكومية، وخدمات الطوارئ وغيرها قد تؤدي إلى إصابات لبعض الأفراد أو خسائر في الممتلكات فضلا عن الخسائر الاقتصادية. وذلك لأن كثيرا من البنى التحتية كمولدات الطاقة، وأنابيب الغاز والبترول، وأنظمة معالجة المياه وتوزيعها، وغيرها أصبحت في عديد من الدول تعمل بطريقة إلكترونية من خلال أجهزة كمبيوتر وأنظمة التحكم الإشرافي والحصول على البيانات. تشير هذه الأنظمة إلى مجموعة الحواسب الآلية التي تقوم بمراقبة وتنظيم العمليات الخاصة بالبنية التحتية الحيوية للدولة كتلك الخاصة بشبكة الكهرباء. وعادة ما يتم توصيل هذه الأجهزة مباشر بالإنترنت حتى تعمل بكفاءة. وتعد هذه الأنظمة من أكثر الأهداف التي تتأثر بالهجمات الإلكترونية بشكل واضح وتترتب عليها آثار تدميرية واسعة النطاق نتيجة الارتباطها بالبنية التحتية الرئيسية داخل الدولة[1].

ولقد أصبحت أنظمة التشغيل هذه موصلة بشبكات اتصالات ليتم صيانتها وإدارتها وتحديثها عن بعد، وتعتمد بشكل متزايد على الإنترنت، ومن ثم تكون أكثر عرضة للهجمات الإلكترونية. كما أنه من الممكن أيضا أن يتم استخدام هجمات الحرمان من الخدمة في الحجر على إبداء طرف ما لرأيه أو نشر معلومات معينة كما حدث في ظل الحرب على العراق عندما هوجم موقع قناة الجزيرة الإخبارية بهجمات الحرمان من الخدمة الموزعة مما أدى إلى توقفه عن العمل.

ولبيان مدى خطورة التهديدات الإلكترونية على البنى التحتية، تم إجراء بعض الاختبارات على شبكات الطاقة، وتبين أنها قد تؤدي إلى توقف الشبكة تماما في حالة إصابتها بأحد البرامج الخبيثة، وذلك وفقا للاختبارات التي قام بها باحثون في معامل إداهو القومية في عام 2007.

[1] نوران شفيق، المرجع السابق، ص57.

ولكن اختلف الخبراء حول الدرجة التدميرية التي تتسم بها الهجمات الإلكترونية في حالة الدول المتقدمة. فالبعض اعتبر أن المجتمعات التي تعتمد بشكل كبير على التكنولوجيا الحديثة في إدارة شئون الدولة تكون أكثر عرضة اللهجمات الإلكترونية التي وإن تمت ستؤدي إلى آثار اقتصادية مدمرة على نطاق واسع، في حين يرى البعض الآخر أن التقدم التكنولوجي يمكن الدولة من التصدي لهذا النوع من الهجمات والتغلب على الآثار المترتبة عليها في وقت قصير.

كما أصبحت الأبعاد الإلكترونية واضحة في اغلب الصراعات السياسية والعسكرية وباتت الآثار المترتبة عليها لا تقل خطورة عن الهجمات التقليدية. إذا يمكن من خلال الهجوم الإلكتروني تدمير البنى التحتية للخصم أو التجسس عليه أو الضغط عليه سياسيا، وغيرها من الأهداف التي تنخفض تكلفة تحقيقها في الفضاء الإلكتروني عن العالم المادي. وهو الأمر الذي أدى بدوره إلى التأثير في أمن الفواعل وإضافة بعد آخر للتهديدات الأمنية التي تتعرض لها وهو البعد الإلكتروني[1].

فالاعتماد المتزايد على الفضاء الإلكتروني والتكنولوجيا الحديثة ترتب عليه تداعيات سياسية وأمنية وعسكرية تشير إلى أن الهجمات الإلكترونية ستلعب دورا بارزا في الصراعات ما بين الفواعل في السنوات المقبلة. وعلى الرغم من أن الهجوم الإلكتروني قد لا يكون له القدرة التدميرية ذاتها التي تتم بها القنابل أو الهجمات التقليدية، غير أن نجاح أية عملية أو هجوم يتوقف على مدى قدرته على تحقيق أهداف الطرف القائم بالهجوم. فإذا كان صاروخ باليستي وبرنامج خبيث كلاهما قادر على تدمير أو إيقاف هدف ما، سيكون الخيار الأقل تكلفة والأقل خطورة على المهاجم هو الخيار الإلكتروني. وتزداد خطورة الهجمات الإلكترونية مقارنة بالهجمات التقليدية إذ ما كانت موجهة إلى مولدات الطاقة، أو النظام المالي للدولة، أو الدفاع الجوي، وغيرها من الأهداف الحيوية التي تؤثر في الأمن القومي بصورة كبيرة ومباشرة.

[1] نوران شقيق، المرجع السابق، ص58.

ووفقا للتقارير شبه السنوية التي تعدها مؤسسة سيمانتيك [1] Symantec الحصر الهجمات الإلكترونية في أكثر من 200 دولة وإقليم من خلال شبكة سيمانتيك العالمية للاستخبارات، تم بإيقاف أكثر من 5، 5 مليار اعتداء إلكتروني في عام 2011، وهو ما يزيد عن عدد الهجمات الإلكترونية في عام 2010 بأكثر من 80 بالمائة[2].

ولقد صاحب هذا التزايد في الهجمات الإلكترونية استخدام الآليات متطورة في القيام بها، وما ساعد على انتشار البرمجيات الخبيثة بسهولة ما بين الأفراد هو زيادة استخدامهم لشبكات التواصل الاجتماعي، والتي تمثل هدفا لعديد من القراصنة. وشملت الاعتداءات عمليات التجسس ضد المؤسسات الحكومية والشركات الكبرى وحتى الشركات الصغرى والعاملين بها، والهواتف المحمولة، إلى آخره. كما ازدادت عمليات التجسس ضد المؤسسات الحكومية والصناعية وسرقة معلومات عن العملاء وذلك لتحقيق مكاسب مالية.

وأظهرت التقارير أنه حدث تزايد في عدد الهجمات الموجهة لهدف معين من متوسط 77 هجوم يوميا في عام 2010 إلى 82 في 2011 ولقد كان فيروس ستاكسنت في عام 2010 أبرز دليل على إمكانية أن تحدث الهجمات الإلكترونية خسائر مادية واضحة. وفي أكتوبر 2010 ظهر فيروس دوكو Duqu والذي تم من خلاله تحميل برامج تجسس تقوم بتسجيل ضربات المفاتيح keystrokes و غيرها من المعلومات. كما تعددت الاعتداءات التي تعرضت لها الصناعات والمنظمات غير الحكومية، فضلا عن القرصنة السياسية من قبل عدد من الجماعات أبرزها Anonymous و LulzSec.

كما تزايدت الهجمات المتقدمة المستمرة Advanced Persistent (Threats (APT كتلك التي تمت في مارس 2010 عن طريق سرقة 24 ألف ملف من وزارة الدفاع الأمريكية. هذا النوع من التهديدات يتم فيه استخدام آليات وتقنيات متطورة للتقليل من إمكانية الكشف عن هوية القائم بالهجوم، وتكون موجهة بالأساس إلى أهداف ذات أهمية

[1] شركة سيمانتك هي شركة تكنولوجية أمريكية عالمية، مقرها في كاليفورنيا بالولايات المتحدة، تأسست في عام ١٩٨٢ وتعمل في مجال برامج الأمن الخاصة بالحاسب الآلي وإدارة المعلومات

[2] نوران شفيق، المرجع السابق، ص59.

كبرى بالنسبة للدولة كمؤسسة الجيش أو الاستخبارات والمؤسسات الاقتصادية والبنى التحتية، والمنظمات ذات الأهمية الاستراتيجية، إلى أخره[1].

ولقد تعرضت عديد من القطاعات للهجمات الإلكترونية، وكان النصيب الأكبر منها للحكومة والقطاع العام بنسبة 20 بالمائة، ويليه القطاع الصناعي بنسبة 15 بالمائة ثم القطاع المالي 14 بالمائة. ولقد حدث في عام 2011 أكثر من 2، 187 مليون هجوم بهدف سرقة الهوية. ومن أكثر القطاعات التي تتعرض لاختراقات هي تلك المرتبطة بالرعاية الصحية، والتي وصلت فيها نسبة الاعتداءات إلى 43 بالمائة .

وبشكل عام، الهجمات الإلكترونية الأكثر خطورة دائما ما تكون مرتبطة بالبنية التحتية الحيوية للدول، أي مهاجمة الأنظمة الإلكترونية المشغلة للبنوك والاتصالات، والطاقة، وخدمات الطوارئ، والمؤسسات الحكومية، والمواصلات، وإمدادات المياه. فالهجمات الإلكترونية الموجهة لهذه القطاعات تستطيع أن تحدث أضرارا جسيمة بالمواطنين، وباقتصاد الدولة.

ومن الممكن أن تقوم الهجمات الإلكترونية بإرهاب المواطنين إذا ما تم استهداف أنظمة الطاقة في الدولة أو قطع الاتصالات، وغيرها من الهجمات التي تستهدف حرمان المواطنين والشركات والحكومات من الخدمات الأساسية، وهو ما قد يلعب دورا في ترويع المواطنين.

ومن الناحية الاقتصادية، من الممكن أن يؤدي هذا النوع من الهجمات إلى الإضرار بالبنية التجارية للدولة، وبالبورصة، وألحاق الضرر باقتصادها، وذلك نتيجة الاعتماد أغلب الأنشطة الاقتصادية على أجهزة الحاسب الآلي والإنترنت. ومن شأن ذلك أن يؤدي إلى فقدان الثقة في اقتصاد الدولة، وزيادة تكلفة القيام بأنشطة اقتصادية ومشروعات فيها.

[1] نوران شقيق، المرجع السابق، ص60.

وعلى الرغم من أن هذا لم يحدث بالفعل، إلا أن الهجمات الإلكترونية من الممكن أن تؤدي إلى القتل، كأن يتم استهداف قطاع المواصلات، وهو ما قد ينتج عنه اصطدام القطارات أو الطائرات، أو أن تستهدف السدود متسببة في فيضانات. كما ستتضاعف الآثار التدميرية إذا ما تم استهداف الأجهزة الطبية والمستشفيات وإتلاف أو تغيير المعلومات الخاصة بالمرضى. ولكن تبقى أكثر الآثار المترتبة على الهجمات الإلكترونية فاعلية هو استخدامها في استهداف أنظمة الإنذار المبكر مصحوبة بهجمات عسكرية، ومن ثم تعظيم القدرة التدميرية للهجمات التقليدية ذاتها. ومن ثم يمكن القول بأن الهجمات الإلكترونية في تزايد مستمر، ويتم تطويرها وتحديثها بشكل دوري بحيث أصبح من الصعب تجنب وقوعها، وبصورة جعلت الدفاع الإلكتروني أكثر تعقيدا وصعوبة.

ومما سبق تتضح خصوصية التهديدات الإلكترونية مقارنة بتلك التقليدية. ففي حين تنصب التهديدات العسكرية التقليدية على استهداف البشر والأجهزة بصورة مباشرة بغرض إلحاق أكبر قدر من الدمار بها، نجد أن الأسلحة الإلكترونية تستهدف بالأساس الأنظمة والشبكات التي تعتمد عليها الدول والشركات في إدارة شئونها وممارسة أنشطتها ويعتمد عليها الأفراد في كافة مناحي حياتهم. فحتى وإن لم يكن القتل المباشر أو الدمار المباشر هدفا من التهديدات الإلكترونية، وحتى وإن لم يكن من الممكن إحداث هذا النوع من الأثار بالنظر إلى طبيعتها، إلا أن الإخلال بأمن الفضاء الإلكتروني الذي بات من أبرز المساحات في التفاعلات الدولية والإنسانية في العصر الحديث، من شأنه أن يحدث أضرارا جسيمة تستهدف أسلوب الحياة نفسها من الممكن أن ترتب خسائر مالية واجتماعية أو حتى مادية لا يستهان بها[1].

وهنا يلاحظ أيضا أنه بالإضافة إلى كافة التأثيرات التي ناقشها هذا المبحث، أن التهديدات الإلكترونية من الممكن أن تحدث أثارا سلبية على عامل الثقة في المجتمعات، سواء ما بين الدولة ومواطنيها، أو بين شركة ما وعملاءها. فحتى وإن لم تكن التهديدات الإلكترونية قادرة

[1] نوران شفيق، المرجع السابق، ص61.

على إحداث أضرار مادية بعيدة المدى كتلك الناتجة عن التهديدات التقليدية، إلا أن بإمكانها أن تؤثر سلبا على علاقات الثقة في المجتمعات بشكل يهدد رؤية الأفراد للفضاء الالكتروني نفسه كمساحة آمنة للتفاعل والتواصل[1]. وهي المعضلة التي واجهت الكثير من المجتمعات التي شهدت هجمات إلكترونية متتالية، زعزع, الأفراد في قدرة الدولة على حمايتهم وحماية مؤسساتها من تلك التهديدات، ان الوقت ذاته بات الفضاء الإلكتروني يشكل جزءا رئيسيا من حياتهم أمسح من الصعب معه تقليل الاعتماد عليه بشكل جذري، أو الرجوع إلى المساحات التقليدية. ومن هنا تأتي أهمية تحقيق الأمن وخاصة بالنسبة للدول الأكثر اعتمادا على الفضاء الإلكتروني في إدارة خطورة التهديدات الإلكترونية على أمن الفواعل و المختلفة والآليات المستخدمة فيها وما يترتب عليها من آثار، نعرض في وبعد بيان التالي نماذج الاستراتيجيات تتبناها الدول لحماية أمنها في مواجهة ما قد ذ له من تهديدات أمنية إلكترونية، وبيان أوجه الشبه والاختلاف بينها، النظر تلك الدول إلى الفضاء الإلكتروني والآليات الإلكترونية في إدارة الدولية وتحقيق مصالحها، ومحورية الأمن الإلكتروني في استر الدفاعية.

[1] نوران شقيق، المرجع السابق، ص62.

الفصل الثاني

الإطار القانوني في مجال مكافحة جرائم الإرهاب الإلكتروني

يأتي تحقيق الأمن القومي في مقدمة مصالح الدول كافة بغض مكانتها على الساحة الدولية في ظل عالم تتطور فيه التهديدات الأمنية والمتغيرات الفائقة السرعة.

وسنحاول من خلال هذا الفصل التطرق إلى الإطار القانوني الوطني في مكافحة هاته الجريمة بالإضافة إلى بالإضافة إلى التعاون الإقليمي.

ثم ندرس في المبحث الثاني: التعاون الدولي لمكافحة الإرهاب الإلكتروني والتحديات الممارسة في هذا المجال.

المبحث الأول: الإطار القانوني الوطني والإقليمي في مكافحة جرائم الإرهاب الإلكتروني.

عرفت المادة 87 مكرر من قانون العقوبات[1] الأفعال التي تعد إرهابية أو تخريبية كل فعل يستهدف أمن الدولة وسلامتها وتتلخص هذه الأفعال في جرائم شلي العمومي والتي يكون الهدف منها:

- بث الرعب وخلق الجو.
- إنعدام الأمن سواء كان الإعتداء معنويا أو جسديا.
- التجهيز وعرقلة حركة المرور.
- الإعتداء على رموز الأمة ونبش القبور.
- الإعتداء ووسائل المواصلات الملكية والعمومية والخاصة والإستحواذ عليها بغير القانون.
- تعريض صحة الإنسان والحياة، أو البيئة للخطر ببث مواد محظورة في الماء أو الجو أو باطن الأرض.
- عرقلة عمل السلطات العمومية أو الإعتداء على حياو أعوانها، أو ممتلكاتهم أو عرقلة تطبيق القانون والتنظيمات.

ما يلاحظ من خلال المادة التالية التذكر التعريف الأوسع لمفهوم الإرهابي التقليدي وقياسا بالجرائم المستخدمة على الصعيد الوطني والدولي على غرار جرائم الكمبيوتر أو ما يعرف بجرائم الكمبيوتر أو ما يعرف بجرائم الإرهاب الإلكتروني فقد سعت الدولة الجزائرية للحد من هاته الجريمة المتطورة بتطوير انظمتها القانونية أستخدمت هياكل جذرية علا غرار الشرطة الإلكترونية بغرض التحقيق والتحري والحد من خطورتها.

وعليه سنحاول من خلال هذا المبحث التطرق إلى الإطار القانوني الوطني، هذا بالإضافة إلى القوانين الوطنية لدى على غرار الدولة الإمارات، السعودية، تونس....

من خلال المطلب الأول ثم نعرج إلى التعاون الاقليمي من خلال المطب الثاني.

[1] قانون العقوبات الجزائري.

المطلب الأول: الإطار القانوني الوطني في مكافحة جرائم الإرهاب الإلكتروني.

بالرجوع إلى نص المادة 87 مكرر من قانون العقوبات الجزائري[1] نجد أن الإرهاب التقليدي لايختلف عن ما يعرف بالإرهاب الإلكتروني المستحدث في عصر التكنولوجيا أو ما يعرف بالإرهاب الإلكتروني، فالإرهاب الإلكتروني من منطلق عنوان، تخويف، تهديد مادي معنوي، صادر من الدول أو الجماعات أو الأفراد على الإنسان بإستخدام الإمكانيات العلمية، والتقنية ووسائل الإتصال والشبكات المعلوماتية من أجل تخويف وترويع الأخرين والحاق الضرر بيهم أو تهديدهم.

كما كملت الدولة الجزائرية بتضافر المجهودات من خلال الميكانيزيات المستخدمة على غرار.

- الشرطة الإلكترونية، حيث يعمل هذا الجهاز على البحث في مختلف الجرائم الماسة بالكمبيوتر على الصعيدين الوطني والدولي على مختلف أشكالها وذلك من خلال التعاون الدولي على غرار التعاون الدولي والإقليمي في تسليم (المجرمين وتقديمهم للمحاكمة) "المنظمة الدولية للشرطة الجنائية" الأنتربول والأفربول، والتي تعني الدول الإفريقية، وهذا بناء على مختلف المراسلات التي تتم بين مختلف الأجهزة للدول والشرطة الجزائرية من خلال الأنتربول وفق إجراءات تتم من خلالها عمليات البحث الإستدلال إلى غاية المحاكمة وتسليم المجرمين وفق تنظيمات متفق عليها مسبقا.

  وهذا انطلاقا من الجانب الموضوعي والإجرائي لمعالجة هذا النوع من الجرائم.
- الوصف القانوني لهاته الجريمة من حيث كونها جريمة تقليدية تطورت من خلال التكنولويجيا المعاصرة والأسلوب المنتهج في ذلك
- ترتيبها في كونها جناية تستدعي وقت كبير لمعالجتها
- العقوبات المقررة لها.

[1] قانون العقوبات الجزائري.

- هذا بالإضافة إلى الجوانب الإجرائية للتمكن منها ومعالجتها وصولا إلى الجانب الدولي في التسليم والمحاكمة وفق شروط ونصوص قانونية وطنية وإتفاقيات دولية....

وعلى هذا الأساس بجد المشروع الجزائري:

- تعريف التعاون القضائي الدولي بين الدول من خلال التنسيق والتصديق على ذلك من خلال بين القوانين.
- م 46 من إتفاقية الأمم المتحدة على أن الدول الأطراف تتقدم لبعضها البعض أكبر قدر ممكن من المساعدة القانونية[1].

الإطار القانوني لمكافحة هاته الجريمة لدى دولة الإمارات العربية المتحدة.

يعتبر القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات هو الإطار القانوني لمكافحة هذا النوع المستجد من الجرائم.

ولعل هذا القانون يعتبر من القوانين الريادية والأولى في العالم العربي الذي ينظم مكافحة جرائم المعلوماتية.

وسوف نعرض لما تضمنه هذا القانون من أحكام وقواعد موضوعية وإجرائية في هذا الإطار.

- كل من أنشأ موقعا أو نشر معلومات على الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات لأية مجموعة تدعو لتسهيل وترويج برامج وأفكار من شأنها الإخلال بالنظام العام والأداب العامة يعاقب بالحبس لمدة لاتظيد على خمس سنوات[2].
- الجرائم الإرهابية عبر أو بإستخدام الإنترنت.

[1]. تنظيم إختصاص القوانين الجنائية الوطنية، ص70، مذكرة تسليم الجرمين الإرهابيين.
[2] أنظر (م20) من القانون المشار اليه

الإطار القانوني لمكافحة جرائم المعلوماتية والأنترنت في السعودية.

احتلت المركز السادس عالميا بين الدول التى تنطلق منها الهجمات الالكترونية نسبة إلى عدد مستخدمى الانترنت فى البلاد ، ومع زيادة انتشار الجرائم المرتبطة بالمعلوماتية فى المجتمع السعودى بدأت السلطات فى الإعداد لإصدار قانون جديد لمكافحة جرائم المعلوماتية ويتضمن مشروع القانون 16 مادة تتضمن السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد عن 500 ألف ريال أو بإحدى هاتين العقوبتين لكل شخص يرتكب أيا من جرائم التصنت على المعلومات المرسلة عن طريق الشبكة العالمية، كما يتضمن تجريم الدخول غير المشروع للمواقع الالكترونية لتغيير تصميماته أو تعديله أو إلغاءه أو إتلافه، وتصل مدة السجن إلى عشرة سنوات والغرامة إلى 5 ملايين ريال فى حالة إنشاء المواقع للمنظمات الإرهابية على الانترنت، كما تصل مدة السجن إلى 5 سنوات والغرامة إلى 3 ملايين ريال لكل من ينتج ما يمس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو تخزينه أو إرساله عن طريق الشبكة المعلوماتية[1].

يتضمن النظام الخاص بالجرائم المعلوماتية (16) مادة تتضمن السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد عن 500 ألف ريال أو بإحدى هاتين العقوبتين لكل شخص يرتكب أيا من جرائم التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون وجه حق أو التقاطه أو اعتراضه، أو الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعا[2].

كما يتضمن النظام تجريم الدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه، أو المساس بالحياة الخاصة بالآخرين

[1] عبد الله الكريم ع الله، المرجع السابق، ص81.
[2] عبد الله عبد الكريم عبد الله، نفس المرجع ، ص82.

عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، أو التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

وتصل مدة السجن إلى 10 سنوات والغرامة إلى 5 ملايين في حالة إنشاء المواقع للمنظمات الإرهابية على الشبكة العنكبوتية، أو الدخول إلى نظام معلوماتي أو أحد أجهزة الحاسب الآلي للحصول على معلومات وبيانات تمس الأمن الداخلي والخارجي للدولة أو اقتصادها الوطني، كما تصل عقوبة السجن إلى 3 سنوات والغرامة إلى مليونين لكل من يستولي لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند عن طريق الاحتيال أو انتحال شخصية غير صحيحة، أو الوصول إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات[1].

كما تصل مدة السجن إلى 4 سنوات والغرامة إلى 3 ملايين لكل من يدخل بشكل غير مشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تسريبها أو إتلافها أو إعادة نشرها وإيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدمير أو مسح البرامج أو البيانات الموجودة والمستخدمة فيها أو حذفها أو تسريبها أو إتلافها أو تعديلها أو إعاقة الوصول إلى الخدمة أو تشويشها أو تعطيلها بأي وسيلة كانت، وتصل مدة السجن إلى 5 سنوات والغرامة إلى 3 ملايين ريال لكل من ينتج ما يمس بالنظام العام أو الآداب العامة أو حرمة الحياة الخاصة أو إعداده أو إرساله أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي، أو إنشاء موقع على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري أو تسهيل التعامل به، أو إنشاء المواد المتعلقة بالشبكات الإباحية أو أنشطة الميسر المخلة بالآداب العامة ونشرها أو ترويجها أو إنشاء موقع للاتجار بالمخدرات أو المؤثرات العقلية أو ترويجها أو طرق تعاطيها أو تسهيل التعامل بها.

[1] عبد الله عبد الكريم عبد الله، المرجع السابق، ص82.

وفي هذا الإطار اقترح إضافة فقرة تتعلق بجرائم البلوتوث والتشهير عبر وسائل تقنيات المعلومات المختلفة من خلال ما يمس الحياة الخاصة عن طريق اساءة استخدام الهواتف النقالة المزودة بالكاميرات، أو التشهير بالأخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة، وتبني تعريف الحاسب الألي بشكل أدق وأشمل لكي تتم معاقبة من يسيئ استخدامه.

ويهدف هذا النظام القانوني إلى اعداد نظام يعالج جرائم المعلوماتية والحاسب والانترنت من خلال وضع ألية نظامية للحد من وقوع هذا النوع من الجرائم، وذلك بتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الإختصاص بمتابعتها وتطبيق العقوبات، وبما يؤدي إلى تحقيق الأمن المعلوماتي، وزيادة استخدامات الحاسب وشبكاته، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات والشبكات، وحماية المصلحة العامة والأخلاق والأداب العامة[1].

الاطار القانوني لمكافحة جرائم المعلوماتية والانترنت في تونس:

يحدد القانون التونسي الخاص بالمبادلات والتجارية الإلكترونية رقم 83 والمؤرخ في 9 أغسطس 2000 بعض الأحكام الخاصة بجرائم المعلوماتية والانترنت[2].

فالفصل 18 من القانون المشار اليه ينص على أنه يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بامضاء غيره بالسجن لمدة تتراوح بين 6 اشهر وعامين و بخطية تتراوح بين 1000 و 1000 دينار أو بأحدى هاتين العقوبتين. "

اما بموجب الفصل 49 فانه يعاقب كل مخالف لاحكام الفصول 20 و 26 و 29 والفقرة الثانية من الفصل 31 والفصل 34 والفقرة الأولى من الفصل 30 من هذا القانون بخطية تتراوح بين 500 و 5000 دينار.

[2] د.عبد الفتاح حجازي، مقدمة في التجارة الالكترونية العربية، الكتاب الأول: شرح قانون المبادلات والتجارة الالكترونية التونسي، دار الفكر الجامعي، الاسكندرية، 2004 ص255. .

وطبقا لاحكام الفصل 50 يعاقب كل من استغل ضعف أو جهل شخص في اطار عمليات البيع الالكتروني بدفعه للالتزام حاضرا أو آجلا بأي شكل من الأشكال، بخطية تتراوح بين 1000 و 20000 دينار، وذلك اذا ثبت من ظروف الواقعة أن هذا الشخص غير قادر على تمييز ابعاد تعهداته أو كشف الحيل والخدع المعتمدة بالالتزام أو اذا ثبت انه كان تحت الضغط مع مراعاة احكام المجلة الجنائية[1] .

وفي ذات السياق ينص الفصل 51 من القانون المشار اليه على أن يعاقب كل من مخالف لأحكام الفصلين 38 و 39 بخطية تتراوح بين 1000 و10000 دينار.

اما الفصل 52 فينص على أن يعاقب طبقا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الالكترونية واعوانه الذين يفشون أو يحثون أو يشاركون في افشاء المعلومات التي عهدت اليهم في اطار تعاطي نشاطاتهم باستثناء تلك التي رخص صاحب الشهادة كتابيا أو الكترونيا في نشرها أو الاعلام بها أو في الحالات المنصوص عليها في التشريع الجاري به العمل ومع حفظ الحقوق المدنية للمتضررين طبقا لأحكام الفصل 53 ، يمكن الوزير المكلف بالتجارة اجراء الصلح في المخالفات المنصوص عليها بالفصل 9 من هذا القانون والتي تتم معاينتها وفقا لأحكام هذا القانون، وايضا مع حفظ الحقوق المدنية للمتضررين، يمكن للوزير المشرف على الوكالة الوطنية للمصادقة الالكترونية اجراء الصلح في المخالفات المنصوص عليها بالفصل 45 من هذا القانون والتي تتم معاينتها وفقا لأحكام هذا القانون. وتكون طرق واجراءات الصلح وفق النصوص القانونية الجاري بها العمل والمنظمة للمراقبة الاقتصادية وخاصة القانون عدد 64 لسنة 1991 المتعلق بالمنافسة والاسعار والنصوص المنقحة والمتممة له، بدون المساس بحقوق الغير.

[1] عبد الله عبد الكريم عبد الله، المرجع السابق، ص86.

القانون العربي الاسترشادي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها قرار قرار (417، د2004/21م[1])

اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بقانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها نسبة إلى مقدم هذا المقترح وهو دولة الامارات العربية المتحدة، والذي كان قد اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495-د19-2003/10/8 ومجلس وزارة الداخلية العرب في دورته الحادية والعشرين.

وسوف نعرض لأحكام هذا القانون الاسترشادي حسب مواده.

المفاهيم المتضمنة في هذا القانون

نصت المادة (1) على ما يلي:

في تطبيق أحكام هذا القانون يقصد بالكلمات والعبارات الآتية المعاني الموضحة قرين كل منها:

- البيانات:
- كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الألي، كالارقام والحروف والرموز وما إليها..
- البرنامج المعلوماتي:

مجموعة من التعليمات والأوامر، قابلة للتنفيذ بإستخدام الحاسب الألي ومعدة لإنجاز مهمة ما.

- النظام المعلوماتي:

ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

[1] arabic.mjustice.dz

- الموقع:

مكان اتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

- الإلتقاط:

مشاهدة البيانات أو المعلومات أو الحصول عليها[1].

- **الإطار التجريمي والعقابي:**

من خلال محتوى الإطار التجريبي نجد أن القانون العربي الإرشادي يشدد بصفته عامة على مختلف الجرائم التي احتواها وإنتصبت في محتوى الانترنت بصفة عامة.

المطلب الثاني: التعاون الإقليمي للحد من هاته الجريمة

مركز الدفاع الإلكتروني التعاوني للتميز

في مايو 2008 وبعد حوالي عام من الهجوم على إستونيا، قام الحلف بإنشاء مركز الدفاع الإلكتروني التعاوني للتميز The Cooperative Cyber Defense Centre of Excellence ليكون مقره تالين، العاصمة الإستونية. الهدف الرئيسي من إنشاء هذا المركز هو التعزيز من قدرات الدفاع الإلكتروني للحلفاء، وزيادة الوعي بقضايا الأمن الإلكتروني وما يرتبط بها من تدريب وبحث وتطوير وتحليل وتبادل للاستشارات والخبرات. ومنذ إنشائه قام المركز بعقد عديد من الندوات الخاصة بالدفاع الإلكتروني لزيادة وعي الأعضاء بأهميتها. كما قام المركز بتنظيم أول مؤتمر عالمي في 2009 لمناقشة الهجوم الإلكتروني المعروف بشبكة الشبح GhostNet.

ولكن يلاحظ أن المركز لا يتبع الهيكل الرسمي للحلف، ولذا فإن النفقات الإدارية ونفقات العمل الخاصة به تتحملها إستونيا ومجموعة من الدول الراعية الأخرى بشكل فردي وليس من خلال ميزانية الحلف. وعلى الرغم من أن العضوية في المركز مفتوحة لكافة أعضاء الحلف، إلا أنها حاليا تضم 11 دولة فقط، وهي إستونيا ولاتفيا، وليتوانيا، وألمانيا، وهنجاريا،

[1] عبد الله عبد الكريم عبد الله، المرجع السابق، ص20.

وإيطاليا، وبولندا، وسلوفاكيا، وإسبانيا، وهولندا، والولايات المتحدة الأمريكية، ومن المتوقع أن تنضم كل من المملكة المتحدة وفرنسا وتركيا في عام 2014[1].

جهود تعاونية أخرى:

لم يكن إنشاء مركز الدفاع الإلكتروني هو المظهر الوحيد للتعاون ما بين أعضاء الحلف، وإنما تلا ذلك مجموعة من المبادرات التعاونية الأخرى. ففي

عام 2011 وافق وزراء دفاع الحلف على مراجعة السياسة الدفاع الإلكتروني – التي وضعت الأسس الخاصة بها في قمة براغ في 2002 وتمت صياغة خطة عمل لتنفيذها. وتقدم هذه الخطة رؤية مشتركة من قبل أعضاء الحلف لبناء القدرات الدفاعية اللازمة للحماية ضد الهجمات الإلكترونية.

وفي فبراير 2012 خصص الحلف مبلغ 58 مليون يورو وذلك لترسيخ قدرة الناتو على الرد الفوري على الهجمات الإلكترونية NATO Computer Incident Response Capability ليتم تفعيلها بشكل كامل في أكتوبر 2013 وفي العام ذاته تم تضمين الدفاع الإلكتروني في عملية التخطيط الدفاعي العام للحلف. وتلا ذلك إنشاء هيئة المعلومات والاتصالات، والتي ستنسق بين كافة الأجهزة التابعة للناتو لتوفير الحماية الكافية وتوفير النفقات على المدى الطويل.

. وفي يونيو 2013، عقد الحلف أول اجتماع مخصص فقط للدفاع الإلكتروني، اتفق فيه وزراء الدفاع على تأسيس فرق للرد الإلكتروني لحماية كافة الأنظمة والشبكات الإلكترونية للمنظمة. ولقد جاء هذا الاجتماع عقب تعرض الناتو لحوالي 2000 حالة اعتداء إلكتروني على الأجهزة التابعة له، وبعد اتهام الولايات المتحدة للصين بالتجسس الإلكتروني ضدها للاستيلاء على معلومات عسكرية وصناعية.

ويمكن القول بأنه على الرغم من أن الإطار الدفاعي للناتو هو من أنجح إن لم يكن الأنجح على الإطلاق– مقارنة بالمنظمات الدولية والإقليمية الأخرى، إلا أن هناك بعض العقبات

[1] نوران شفيق، المرجع السابق، ص102.

التي تقف في طريق زيادة فعالية واتساع نطاق تأثيره. فإحدى الإشكاليات التي تواجه الحلف في وضع استراتيجيات الدفاع الإلكتروني هو تحديد حجم المساعدات التي ستقدمها كل دولة من أعضاء الحلف لتطوير منظومته الدفاعية الإلكترونية.

إذ يختلف الأعضاء حول حجم المساعدة التي يجب تقديمها للدول التي تتعرض لهجمات إلكترونية. فالدول الصغيرة من مصلحتها الاستفادة من مساعدات الناتو في الدفاع الإلكتروني، في حين أن الدول الكبرى بالفعل تنفق أموالا طائلة على الدفاع الإلكتروني على المستوى الداخلي، وليس من مصلحتها توجيه نفقات ضخمة لميزانية الحلف لذات الهدف، كما أنها لا ترى أن جهود الدفاع الإلكتروني من خلال الناتو يمكن أن تكون بديلة عن الجهود الدفاعية الداخلية[1]. ومن ثم، قد تتردد في تقديم مساعدات ضخمة للحلف من خلال استقطاع جزء من ميزانيتها الداخلية للدفاع الإلكتروني، في حين أن جهود الحلف لن تغني بأي حال من الأحوال عن جهودها الداخلية.

يضاف إلى ذلك أن جهود الناتو في مجال الدفاع الإلكتروني لاتزال موجهة بالأساس لحماية أجهزة وشبكات الحلف، وتظل حماية البنى التحتية الحيوية للدول مسئولية وطنية من خلال ما يقدمه الناتو من مساعدات وتبادل للمعلومات والخبرات والقيام بالتدريبات. ويذكر أيضا أن التعاون مع الاتحاد الأوروبي يعد إحدى ركائز السياسية الإلكترونية الدفاعية للناتو من خلال المشاورات غير الرسمية التي تهدف إلى تعزيز التعاون في هذا المجال.

ثالثا: الاتحاد الأوروبي والأمن الإلكتروني:

يمثل الاتحاد الأوروبي مثالا آخر للتعاون الإقليمي لتحقيق الأمن الإلكتروني. إذ يسعى الاتحاد الأوروبي إلى تطوير استراتيجية دفاعية تهدف إلى حماية الدول الأعضاء من التهديدات الإلكترونية، وتعزيز التعاون ما بين الدول والتنسيق بينهم وخاصة فيما يتعلق بالجوانب التشريعية، فضلا عن تقوية البنية التحتية الإلكترونية الأجهزة الاتحاد والدول الأعضاء فيه.

[1]. نوران شفيق، المرجع السابق ص103.

ففي عام 2004 تم تأسيس هيئة الاتحاد الأوروبي لأمن المعلومات والشبكات European Union Agency for Network and Information (Security (ENISA وبدأت العمل في 2000، كخطوة في طريق تحقيق الأمن الإلكتروني للاتحاد الأوروبي. ولقد أسهمت الهيئة في تطوير الوعي بأهمية أمن الشبكات من قبل المواطنين والمستهلكين والشركات والقطاع العام. وتعد هذه الهيئة بمثابة محاولة من الاتحاد الأوروبي للاستجابة إلى قضايا الأمن الإلكتروني وضمان التعاون ما بين كافة الدول الأعضاء في تبادل المعلومات والمعرفة في هذا الصدد. فهي تساعد الدول الأعضاء ومؤسسات الاتحاد في مشاكل الأمن المعلوماتي وأمن الشبكات فيما يتعلق بالجوانب التقنية[1].

وفي عام 2010 قامت المفوضية الأوروبية بتبني أجندة إلكترونية تتضمن 14 خطوة لتحسين قدرة الدول الأوروبية على تجنب ورصد ومواجهة المشاكل المتعلقة بالشبكات الإلكترونية وبأمن المعلومات. وتم تأسيس فرق للاستجابة السريعة CERT للمؤسسات الأوروبية في يوليو 2011 والتي تعمل على حماية مؤسسات الاتحاد والتعاون أيضا مع فرق الاستجابة الخاصة بالدول الأعضاء[2].

ولقد تم تأسيس المركز الأوروبي للجريمة الإلكترونية European Cybercrime Centre والذي بدأ العمل فيه في يناير 2013 ليتولى مهمة الدفاع عن أجهزة الاتحاد الأوروبي ضد الجرائم الإلكترونية. كما يقوم أيضا بتقديم المساعدة والدعم للدول الأعضاء والأجهزة الاتحاد لبناء قدرات دفاعية إلكترونية والتعاون مع الشركاء العالميين[3].

كما يمثل التعاون العبر أطلنطي أحد أهم أسس المبادرات الأوروبية التحقيق الأمن الإلكتروني ومن أبرزها القمة التي عقدت في نوفمبر 2010 والتي أسست مجموعة عمل ما بين الولايات المتحدة والاتحاد الأوروبي للتعاون في تحليل مخاطر التهديدات والجرائم

---

[1] European Union Agency for Netwrok and Information Security. URL: https://www.enisa.europa.eu/about-enisa. Accessed on 15th March, 2014.

[2] European Cybercrime Centre

[3] Neil Robinson et al. Op. cit., pp:37-39

الإلكترونية. فالاتحاد الأوروبي لا يرى أن المخاطر المرتبطة بالفضاء الإلكتروني يمكن التصدي لها بمعزل عن المجتمع الدولي أو بجهود فردية من المنظمة.

وأصدرت المفوضية الأوروبية استراتيجية الأمن الإلكتروني للاتحاد الأوروبي في 4 فبراير 2013 ولقد كانت هذه الاستراتيجية بمثابة استجابة من الاتحاد الأوروبي للحاجة إلى دمج مجتمعات وجهات متعددة للعمل جنبا إلى جنب نحو تحقيق الأمن الإلكتروني على مستوى الاتحاد الأوروبي ووضع حجر الأساس للتعاون المستقبلي. وتضمنت هذه الاستراتيجية تأكيدا على ضرورة أن تمتلك كافة الدول القدرات الخاصة بالأمن المعلوماتي وأمن الشبكات وأن تتعاون وتتبادل المعلومات لحماية أمن الدول كافة. علاوة على ذلك، أكدت الاستراتيجية على ضرورة أن تشترك الهيئات التجارية وغير الحكومية في إدارة مبادى الإنترنت وجهود الأمن الإلكتروني[1].

رابعا: أمثلة أخرى للتعاون على المستوى الإقليمي :

يظهر التعاون الإقليمي في الدفاع الإلكتروني في أمثلة أخرى من المنظمات، وتأتي في مقدمتها منظمة شنغهاي للتعاون، والتي تأسست في 2001 وتضم في عضويتها الصين وكازخستان، وكراجستان وروسيا وطاجيكستان، وأوزباكستان، وتشارك فيه الهند وباكستان وإيران كمراقبين. ففي سبتمبر 2011 وقعت الدول الأعضاء اتفاقية للتعاون المشترك في مجال الأمن المعلوماتي ينظر إليها على أنها أساس للتعاون المستقبلي ما بين المنظمة والأمم المتحدة في الدفاع الإلكتروني.

وذكرت الاتفاقية في المادة الثانية منها الأسلحة المعلوماتية والإلكترونية وما يترتب على تطويرها والاستخدام الهجومي لها من مخاطر على أمن الدول.

كما أدرجت أيضا الاتفاقية مجموعة كبيرة من الجرائم التي اتفقت الدول الأعضاء على التعاون لمواجهتها، ومن بينها الجرائم الإلكترونية والإرهاب الإلكتروني وخاصة ذلك الذي

[1] نوران شفيق، المرجع السابق، ص105.

يستهدف البنى التحتية للدول، باعتبار أنها الخطر الأمني الأكبر الذي يهدد الدول الأعضاء.

وكذلك الحال بالنسبة لمنظمة الأسيان والتي صدر عنها بيان في عام 2009 بشأن التعاون لمحاربة الاعتداءات الإلكترونية والاستخدام الإرهابي والإجرامي للفضاء الإلكتروني. وأجريت ورشة عمل في مارس 2012 لبحث تطوير مجموعة من الإجراءات لبناء الثقة في الفضاء الإلكتروني وتعزيز الدور الذي تلعبه المنطقة في هذا الصدد.

المبحث الثاني: التعاون الدولي لمكافحة هاته الجريمة والتحديات الممارسة في هذا المجال.

لقد عملت الدول على غرار قوتها مكانتها الدولية على الحد من هاته الجريمة وهو ماسنحاول من خلال المبحث التطرق الى التعاون الدولي هاته الجريمة من خلال مطلبين.

المطلب الأول: التعاون الذي من خلال إتفاقية المجلس الأروبي وحلف الشمال الأطلنطي للأمم المتحدة وجهود تعاونية اخرى.

عن المطلب الثاني: التحديات الممارسة للحد من هاته الجريمة

المطلب الأول: التعاون الدولي للحد من جرائم الإرهاب الإلكتروني

سوف نتعرض هنا للقرارات والمعاهدات والأطر القانونية الدولية التي تعني بمكافحة جرائم المعلوماتية والأنترنت.

- القرار الصادر عن الأمم المتحدة بشأن الجرائم ذات الصلة بالكمبيوتر[1] وضع مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء إطارا دوليا في مكافحة جرائم الكمبيوتر فهو إذ يسلم بضرورة تطوير سبل ووسائل التعاون في المسائل الجنائية ورغبة منه في إستكمال العمل الذي أنجز في ميدان معايير الأمم المتحدة وقواعدها في ميدان العدالة الجنائية[2]، واذ يضع في اعتباره آن نظم الكمبيوتر كثيرا ما تستعمل لتخزين بيانات سياسة واقتصادية وطبية واجتماعية وشخصية تتسم بحساسية بالغة، وان هذه النظم قد تستخدم الاداء ومراقبة مهام معقدة كثيرا ما تنطوي على حالات قد تعرض للخطر الحياة وحقوق الانسان والحريات الأساسية، فانه واستجابة لهذه الاعتبارات وغيرها ونظرا إلى أن زيادة استخدام تكنولوجيا الكمبيوتر وشبكات الاتصالات السلكية واللاسلكية على نطاق العالم عن طريق الكمبيوتر بوصفها جزءا لا يتجزا من العمليات المالية والمصرفية الدولية قد تهيء ظروفا تيسر إلى حد كبير من ارتكاب العمليات الاجرامية داخل البلدان وفيما بينها مما

[1] هافانا 1990 ضمن مقررات القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة، ومعاملة السجناء.
[2] محمد الألفي، المسؤولية الجنائية عن الجرائم الاخلاقية عبر الانترنت، الكتب المصري الحديث للنشر، القاهرة، 2005، ص 174

يؤدي لازدياد اساءة استعمال الكمبيوتر كإحدى طرق الجريمة الاقتصادية وصعوبة الكشف عن الجرائم ذات الصلة بالكمبيوتر، وخصوصا بسبب السرعة التي يمكن أن ترتكب بها هذه الجرائم وايضا لزيادة النفاذ غير المصرح به إلى نظم الكمبيوتر وبياناته وبرامجه والاقدام دون اذن على استعمالها أو مراقبتها، أو التدخل فيها، أو ارتكاب افعال ضارة اخرى ذات صلة بنظمه وبياناته وبرامجه لكل هذه الاسباب اتي الاتفاق على هذا القرار.

ويلاحظ في هذا الاطار امكانية الربط بين الجريمة المنظمة وما يتصل بها من اساءة استعمال الكمبيوتر وان الكمبيوتر كثيرا ما قد تستخدمه الجريمة المنظمة لأغراض من قبيل غسل الأموال أو في ادارة الأصول المتحصلة بطريقة غير مشروعة.

وقد اتى هذا القرار متوائما مع قرارات وتقارير منظمة التعاون الاقتصادي والتنمية ولا سيما تقريرها الصادر عام 1986 وتوصية وتقرير مجلس أوروبا بشأن الجرائم المتعلقة بالكمبيوتر والمباديء التوجيهية التشريعية التي اعتمدتها اللجنة الوزارية لمجلس أوروبا في 13 ايلول / سبتمبر 1989 اضافة إلى مشروع المبادئ التوجيهية المتعلقة باستعمال ملفات البيانات الشخصية في نظم الكمبيوتر المعد من قبل اللجنة الفرعية لمنع التمييز وحماية الأقليات، مع ما يعني ذلك من اقتناع الدول المتفقة على اصدار هذا القرار ايمانا منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع الدولي والابعاد الدولية الاساءة استخدام الكمبيوتر والجرائم المتعلقة به .

وفي هذا الاطار فان ملامح هذا القرار تدور حول عدة أمور هي[1]:

1- التأكيد على أن وضع اطار قانوني دولي ملائم يتطلب بذل جميع الدول الأعضاء جهدا جماعيا .

2 - الطلب من الدول الأعضاء، في ضوء الاعمال المطلع بها فعلا في مجال الجرائم ذات الصلة بالكمبيوتر أن تكثف جهودها كي تكافح بمزيد من الفعالية عمليات اساءة استعمال

1 يونس عرب، جرائم الكمبيوتر والانترنت، ط1، منشورات اتحاد المصارف العربية بيروت، 2002، ص314.

الكمبيوتر التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر، اذا دعت الضرورة إلى ذلك،في التدابير التالية:

أ- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان أن تطبق الجزاءات والقوانين الراهنة، بشأن سلطات التحقيق وقبول الأدلة في الإجراءات القضائية على نحو ملائم وادخال تغييرات مناسبة اذا دعت الضرورة إلى ذلك. بالاضافة إلى وضع أحكام وإجراءات تتعلق بالتحقيق والأدلة للتصدي إلى هذا الشكل الجديد والمعقد من أشكال النشاط الاجرامي[1].

ناهيك عن أن مصادرة أو رد الأصول بصورة غير مشروعة والناجمة عن ارتكاب جرائم ذات صلة بالحاسوب هو امر جدير بالاهتمام.

ب – تحسين تدابير الأمن والوقاية المتعلقة بالحاسوب مع مراعاة حماية الخصوصية واحترام حقوق الانسان وحرياته الأساسية.

ج – اعتماد تدابير لزيادة وعي الجماهير والعاملين في الأجهزة القضائية وأجهزة انفاذ القوانين بالمشكلة وبأهمية مكافحة الجرائم ذات الصلة بالحواسيب.

د – اعتماد تدابير مناسبة لتدريب القضاة والمسؤولين والأجهزة المسؤولة عن منع الجرائم الاقتصادية والجرائم ذات الصلة بأجهزة الحاسوب والتحقيق فيها ومحاكمة مرتكبيها واصدار الأحكام المتعلقة بها.

هـ- التعاون مع المنظمات المهتمة بهذا الموضوع في وضع قواعد للآداب المتبعة في استخدام أجهزة الحاسوب والنفاذ إلى الشبكات.

و – اعتماد سياسات بشان ضحايا الجرائم المتعلقة بالكمبيوتر تنسجم مع اعلان الامم المتحدة بشان مباديء العدل المتعلقة بضحايا الاجرام والتعسف في استعمال السلطة،

[1] عبد الله عبد الكريم عبد الله، المرجع السابق ص110.

وتتضمن اعادة الممتلكات التي يتم الحصول عليها بطرق غير مشروعة، وتدابير لتشجيع الضحايا على ابلاغ السلطات المختصة بهذه الجرائم[1].

اتفاقية بودابست 2001 لمكافحة الجرائم المعلوماتية

الاتفاقية الاوروبية لمكافحة جرائم المعلوماتية «الجرائم الالكترونية»

بتاريخ 20 نيسان 2000 تقدمت اللجنة الاوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الكمبيوتر.

وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الأول وحتى اعداد مسودتها النهائية التي اقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم الالكترونية).

وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات واطلق ضمن مواقع عديدة اوروبية وامريكية على شبكة الانترنت لجهة التباحث وابداء الرأي. وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الاوروبي ومجلس أوروبا ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ اكثر من عشرة أعوام [2].

ملامح الاتفاقية

تتكون الاتفاقية من مقدمة واربعة فصول، فبعد أن استعرضت المقدمة اهداف الاتفاقية ومطلقاتها ومرجعاتها السابقة وما تقوم عليه من جخزد ارشادية وتوجيه وتدابير اقليمية ودولية، جاء الفصل الأول لتغطية المصطلحات الأساسية (مادة1). تتضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني، ثلاثة أقسام: الأول، ويضم المواد من 2-13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر، والقسم الثاني ويضم المواد من 14-21 وتتعلق بالقواعد الاجرائية والقسم الثالث ويضم المادة 22 وتعلق بالاختصاص. أما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون

[1] www.arablaw.com
[2] www.arablawinfo.com

الدولي، فقط تضمن قسمين، الأول تحت عنوان المبادئ العامة ويضم المواد من 22-27 والقسم الثاني ويتعلق بالنصوص الخاصة ويضم المواد من 29-35 أما الفصل الخامس فيتضمن الاحكام الختامية ويضم المواد من 36-48.

في هذا الاطار يذكر ان الجهود الأوروبية في هذا المجال بدأت عندما اصدر الاتحاد الأوروبي بتاؤيخ 11 مارس 1997 ارشادا يحمل الرقم 9/ ce/96 يتعلق بالحماية القانونية لقواعد البيانات، ويمتاز هذا الارشاد بأنه منح جميع قواعد البيانات بما فيها تلك غير الالكترونية الحماية القانونية اللازمة[1].

اسباب ابرام الاتفاقية

اكدت مقدمة الاتفاقية على الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر ومخاطرها المدمرة على الدول خاصة في ظل شيوع شبكات المعلومات وفي ظل التوسع والنماء الكبير لأنظمة الحوسبة المفتوحة ونقل وتدفق المعلومات، اضافة إلى التشديد على اهمية مكافحة كافة الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي السرية وسلامة المحتوى وتوفر المعلومات والنظم.

وقد اكدت مقدمة الاتفاقية على اتخاذ التدابير التشريعية والتنظيمية الضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على اهمية التعاون المحلي والاقليمي والدولي مع وجوب اقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الأساسية والسيادة.

ولان الاتفاقية جاءت حصيلة جهود دولية واقليمية فقد اكدت المقدمة على اهمية ما انجز من جهود في حقل جرائم الكمبيوتر من قبل الامم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد والاوروبي ومجموعة الدول الصناعية (مجموعة الثمانية) وبالنتيجة فان مقدمة مشروع الاتفاقية قد ركزت على عناصر اساسية ثلاث[2]:

[1] د. طوني عيسى، حماية برامج الكمبيوتر وقواعد البيانات، مقالة قانونية منشورة في مجلة العدل، قسم الدراسات، العدد 1999، منشورات نقابة المحامين في بيروت، ص132 [1]

[2] عبد الله عبد الكريم عبد الله المرجع السابق ص126.

الاول: يتمثل بأهمية التدابير التشريعية الموضوعية لمواجهة جرائم الكمبيوتر (نصوص التجريم الموضوعية).

الثاني: يتمثل بأهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة جرائم الكمبيوتر النصوص الإجرائية).

الثالث: يتمثل بأهمية التعاون الدولي والاقليمي في حقل مكافحة هذه الجرائم والانطلاق مما انجز من جهود دولية واقليمية في هذا الحقل[1].

المؤتمرات الدولية:

هناك عديد من المؤتمرات الدولية التي عقدت في السنوات الأخيرة وضمت عديدا من الدول لبحث سبل تحقيق الأمن الإلكتروني وتعزيز تعاون الدول في مجال تكنولوجيا المعلومات والاتصالات بشكل عام. ومن أهم تلك المؤتمرات المؤتمر الذي عقد في نوفمبر 2012 وعرف بمؤتمر لندن للفضاء الإلكتروني في المملكة المتحدة، والذي هدف إلى إجراء حوار سياسي حول القضايا الإلكترونية ينتهي إلى وضع أجندة المزيد من التعاون لتحقيق الأمن الإلكتروني، وذلك كإطار غير رسمي للحوار. ولقد تلا هذا المؤتمر، مؤتمر آخر عقد في بودابست في أكتوبر 2012 ضم 600 ممثل حكومي وممثلين عن القطاع الخاص، والمجتمع المدني وغيرهم[2].

وعقد مؤتمر آخر بعنوان "تحديات الأمن الإلكتروني" في برلين والذي تضمن ممثلين من القطاع الخاص والمجتمع المدني وأكاديميين، وحكوميين المحاولة الوصول إلى حلول تعاونية لمواجهة تحديات الأمن الإلكتروني بما في ذلك إجراءات بناء الثقة، والشفافية في الاستراتيجيات الدفاعية، وتطوير آليات إدارة الأزمات في الفضاء الإلكتروني.

[1] www.mctmnet.gov.om

[2] نوران شقيق، المرجع السابق، ص107.

وكذلك في نوفمبر 2012، معهد الأمم المتحدة البحوث نزع السلاح بالتعاون مع chatham house ومركز المعلومات والتدريب تم استضافت مؤتمرا دوليا لمدة يومين حول إمكانية أن تحقق إجراءات بناء الثقة استقرارا وأما في الفضاء الإلكتروني.

ولقد حدد الاتحاد العالمي للعلماء World Federation of Scientists مجموعة من المبادئ العامة للسلام الإلكتروني في إعلان أطلق عليه Erice Declaration للاستقرار والسلام الإلكتروني في أغسطس 2009، وأكد هذا الإعلان على الصلة الوثيقة ما بين السلام العالمي والاستقرار الإلكتروني، ويتمثل أهم ما جاء به من مبادئ في الآتي:

1- لابد وأن تدرك الحكومات أن القانون الدولي يضمن للأفراد حرية تداول المعلومات والأفكار وأن ذلك ينطبق على الفضاء الإلكتروني. ويكون أي تقييد فقط في الحالات التي يحددها القانون.

2- يجب أن تعمل كافة الدول مع بعضها بعضا لكي تصل إلى قواعد مشتركة للسلوك والتنسيق للوصول الى اطار قانوني عالمي يحكم الفضاء الإلكتروني يتضمن أحكاما إجرائية مشتركة وتعاونا في عمليات التحقيق بما لا يتعارض مع احترام الخصوصية وحقوق الإنسان. وعلى كافة الحكومات، ومقدمي الخدمة والمستخدمين احترام جهود تطبيق القانون الدولي ضد الجرائم الإلكترونية.

3- يجب أن تعمل الحكومات ومقدمو الخدمة والمستخدمون سويا على ضمان عدم استغلال الفضاء الإلكتروني في الإضرار بالمستخدمين.

4- على الحكومات والمنظمات والقطاع الخاص والأفراد أن يقوموا بتطبيق وحماية البرامج الأمنية الشاملة القائمة على قواعد ومبادئ عالمية متفق عليها باستخدام التكنولوجيا الحديثة[1].

5- أن يعمل مطورو البرامج والأجهزة على الوصول إلى تكنولوجيا آمنة تدعم من قدرة الأنظمة الإلكترونية على مقاومة مواطن الضعف فيها والتصدي للهجمات.

[1] نوران شفيق، المرجع السابق ص 111.

6- أن تتفاعل الحكومات تفاعلا نشطا مع الأمم المتحدة وجهودها في تعزيز الأمن الإلكتروني العالمي والسلام الإلكتروني لتجنب استخدام الفضاء الإلكتروني كمجال للصراع.

المطلب الثاني: التحديات الممارسة للحد من جرائم الإرهاب الإلكتروني.

تواجه المسألة الإجرائية في هاته الجريمة بعض العقبات لتفعيلها بشكل مؤثر، فالمسئولية الملقاة على عاتق سلطات الأمن في التوصل لمرتكب الجريمة الإلكترونية عظيمة الشأن، إذا أن ذلك يصطدم بالكيفية التي سيتم بها اكتشاف الجاني و بحث الوسائل المتبعة في اللحاق به و تعقبه و إثبات التهمة على الجاني .

و أوضح البداية إن أغلب الدول قد إتجهت لإستخدام الحاسب الآلي في تعقب المجرمين و مرتكبي الجرائم المعلوماتية ، و قد أصبح هذا الإتجاه هو الأساس الأمني في أغلب الدول لسهولة الكشف عن المجرم و تحديد بياناته ، و من أمثلة ذلك أجهزة الكشف عن البصمات التي تستخدم في بحث وتحديد بيانات مرتكب الجريمة ، و ذلك يتضح في أوروبا حيث فور أن يتم الكشف عن شخصية المجرم يتم التعامل معه و إذا كان خارج البلاد يخطر الإنتربول لضبطه[1].

و دور الحاسب الآلي لا يقتصر فقط على الكشف عن مرتكب الجريمة المعلوماتية فقط بل يمتد لكافة الجرائم ، سواء تم الإستعانة باحاسب الآلي لتحديد شخصية المجرم أو تعقب تبادل المعلومات بين أطراف الجريمة و تحديد مصدرها كجرائم المخدرات مثلا ، و تكنولوجيا الحاسب الآلي مهدت الطريق لكل من مرتكب الجريمة و متعقب المجرم في إستخدامها لتسهيل المهمة .

ومن اجراء ذلك أن نشأ في كل جهاز أمني قسم خاص تنحصر وظيفته في إستخدام الحاسب الآلي بكافة صورة ، سواء في التوصل للمجرمين أو اللحاق بهم أو إثبات التهمة عليهم، و هو ما سأتعرض له في الآتي:

---

[1] لواء دكتور قدرى عبد الفتاح الشهاوي ، الإستخبارات والإستدلالات وحقوق الإنسان وحرياته الأساسية، دار النهضة العربية، القاهرة،2006،ص240.

التوصل و الملاحقة للجاني وإثبات التهمة:

التوصل و الملاحقة للمجرم المعلوماتي

تشكل فكرة الوصول إلى الجاني في الجريمة الإلكترونية النتيجة المنتظرة من الحماية الإجرائية للمحل الإلكتروني ، فلابد أن يكون الحكم الصادر و المبني على الأدلة الجنائية المقدمة صحيحا[1] ، لأن خلو الحكم من المعطيات السليمة و المنطقية و التي تقود إلى حجية الحكم يعيبه بالبطلان ، و لذلك كان التوصل للجاني أساس نجاح الحماية الإجرائية و ما يترتب على ذلك من إجراءات .

ولما كانت تلك الفكرة من الصعوبة في التنفيذ في مجال الجريمة المعلوماتية نظرا للتقنية المقدمة و تطلب خبرة معينة في تنفيذها ، الأمر الذي يفرض على متبعها ظروف و خطوات معينة لابد أن ينتهجها الجهاز الأمني حتى تكون كافة الإجراءات المتبعة قانونية و مترابطة.

وفي البحث عن كيفية التوصل للجاني في الجريمة المعلوماتية الا أتعرض للجاني التقليدي والجريمة التقليدية ، فالبحث في سارق جهاز حاسب آلي أو من يقوم بإتلاف وحدات إلكترونية بشكل يدوي ليس مجال البحث، فتلك الجرائم هي جرائم تقليدية في مضمونها و إن اختلفت في المحل الواقع عليه الجريمة، و لكننا في دراستنا نبحث الجرائم غير التقليدية كسرقة المعلومات أو إتلاف وحدات التخزين على الحاسب الآلي باستخدام الفيروسات الإلكترونية لارتباط تلك الجرائم بالمعرفة والعلم التكنولوجي سيما وأن اكتشاف أغلب تلك الجرائم لا يكون إلا مصادفة.

ولذلك كان تحديد المعلومات والبيانات الجديرة بالحماية أساس الحماية الإجرائية و كان الكشف عن الجاني و التوصل إليه مرتبط بالبحث في معرفة كل المشتبه بهم للكيفية التي يتم التعامل بها في تلك المعلومات ، ففرض نطاق أمني لحماية المحل الإلكتروني هو خطوة

[1] سعيد عبد اللطيف إثبات جرائم الكمبيوتر والجرائم المرتكبة على الانترنت، دار النهضة العربية،القاهرة،1999،ص89.

جوهرية و أساسية في الحماية و يتم تحليل المخاطر التي قد تتعرض لها الأجهزة و العدو المترقب اقتحامه لها[1].

و في سبيل التفعيل الناجح لتلك الحماية لابد من تكاتف و مشاركة الجهاز الأمني بكاملة من مبرمجين و علماء و سلطات تنفيذ للتوصل إلى الجاني كل حسب الدور المنوط به، فالمبرمج هو من يستطيع كشف الإختراق الذي تم في الجهاز و تتبع مرتكبة ، أما السلطة التنفيذية هي المنوط بها تعقب المجرم و ضبطه لتقديمة للمحاكمة ، و كل ذلك لابد أن يقدم بشكل قانوني سليم حتى لا يشوب الإجراءات بطلان و كل إدارة أمنية لابد من تواجد فرق أمنية بها مختصة بذلك .

فتلك الفرق منوط بها جميع الحقائق العلمية للأزمة و كيفية مواجهتها و إعداد التصور المحتمل حدوثه أثناء المواجهة ، و ذلك لتأمين المنشأة أو المحل الإلكتروني من أي هجمات لاحقة ، و تقوم أجهزة الأمن المصرية بتكليف إدارات معينة في سبيل الوصول للجاني في الجريمة المعلوماتية ، و تقوم تلك الأجهزة جمع المعلومات و تلقي البلاغات .

و لما كانت الجريمة المعلوماتية بطبيعتها جريمة ممكنة الحدوث داخل جمهورية مصر العربية فهي جريمة دولية و عابرة للقارات أيضا ، و لذلك كان التعاون الدولي من أهم المفاتيح التي تساعد و تساهم بشكل فعال في مجال الحماية الإجرائية[2]، و هذا التعاون لابد أن يشمل المشاركة التشريعية و القضائية و التنفيذية حتى يمكن تنفيذه بشكل فعال .

و لذلك كانت المشاركة بين مختلف الدول لإنشاء جهاز أمني للحد من تلك الجرائم هو من الخطوات الأساسية للوصول إلى الجاني ، و كان تدعيم التعاون بين مختلف أجهزة الأمن ، و لذلك تم إنشاء شرطة متخصصة في جرائم الإنترنت بالولايات المتحدة الأمريكية تدعى "شرطة الإنترنت" لتلقي الشكاوى و تتبع منتهى البرامج و المواقع الإلكترونية على شبكة الإنترنت ، و تقوم مختلف الدول بإبلاغ الشرطة الدولية "الإنتربول"

[1] أيمن عبد الحفيظ ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة 2005، ص195.
[2] جميل عبد الباقي ، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة1992، ص225.

حال الكشف عن إحدى تلك الجرائم في حالة كون مرتكبها من دولة أخرى للمساعدة في القبض عليه .

يعتبر ملاحقة الجاني عقب التأكد من إرتكابه للجريمة الإلكترونية و الحصول على الدليل و التثبت منه إجراء طبيعي و متوقع ، إلا أن هذا الإجراء قد يصطدم بمبادئ حقوق الإنسان و التي أقرها الدستور المصري ، فقد ورد بالباب الثاني من الدستور المصري بالمادتين 34 أن الملكية الخاصة مصونة و المادة 36 و التي قررت عدم جواز المصادرة الخاصة للأموال إلا بحكم قضائي و المادة 41 المقررة للحق في الحرية الشخصية[1].

و بالبحث في تلك المواد نجد أن اللحاق بالمجرم مرتكب الجريمة الإلكترونية لهو من الصعوبة بمكان ، حيث أن إثبات التهمة على المتهم يستلزم فحص أجهزته الإلكترونية و إقتحام أسراره التكنولوجية ، و الحاق بالجاني في الجريمة المعلوماتية يختلف بعض الشئ عن اللحاق بالجاني في الجريمة التقليدية ، حيث أن الجاني في الجريمة التقليدية بمجرد ضبطه و ضبط الأداة المستخدمة في إرتكاب الجريمة يتم قطع أغلب الطريق لإثبات الإتهام عليه ، أما في الجريمة الإلكترونية لابد من التأكد من وجود البيانات المطلوبة في إدانة المتهم على الجهاز الخاص به ثم التيقن من إرتكابه للجريمة عن طريق الحاسب الآلي[2].

فأجهزة الأمن عقب تلقيها المعلومة تقوم بمراقبة الجهاز الخاص بالمبلغ و الإتصالات القادمة إليه ، ثم تتبع العنوان الإلكتروني المرسلة منه الرسالة و يلي ذلك وضع خطة أمنية تقليدية لضبط الجاني ، و كل ذلك لابد أن يكون في الإطار القانوني المشروع، ففي الولايات المتحدة الأمريكية تتحدد الإختصاصات عقب تلقي البلاغ فتقوم مجموعة بالتوجه للمكان و فحصة و تحديد الضرر الواقع و تدوين كافة المعلومات الموجودة على الحاسب الآلي مع عدم فصل الهواتف أو الأجهزة ، لتجنب ضياع البيانات التي تتلقاها الأجهزة و جدير بالذكر أن تلك الإجراءات المتبعة زادت بشكل ملحوظ عقب أحداث الحادي عشر من سبتمبر عام

[1]. لواء دكتور قدرى عبد الفتاح الشهاوي ، المرجع السابق ص 567
[2] أيمن عبد الحفيظ ، المرجع السابق ، ص 225

2001 فقد تم تطوير برنامج يدعى "كارنيفور" لتعقب و فحص كافه الرسائل الإلكترونية عبر الحاسب إذا ما تم الإشتباه في كونها تحمل معلومات إجرامية .

إثبات التهمة

يعد إثبات الجريمة الإلكترونية من الصعوبة بما كان لسهولة إخفاء معالمها، و إمكانية التخلص من آثارها[1]، و تختص الجهات الشرطية بتقديم الدليل المثبت للتهمة المنسوبة للمتهم ، و قد كفل النظام القانوني المصري أسوة بنظيرة الفرنسي مبدأ الإثبات الحر ، فلكل طرف في الجريمة الإلكترونية حرية إثبات التهمة أو نفيها ، و له في ذلك الحق في تقديم كافة الأدلة ، و لكن يثور البحث حول أنواع الأدلة المقدمة و مدى حرية القضاء في الأخذ بها و الإقتناع بجدواها .

فإذا ما تعرضت للبريد الإلكترونى و الرسائل الإلكترونية فالمشرع قد كفل الحماية لتلك الرسائل طالما أن لم يقصد إباحتها للجميع [2] ، و هذا الحق يهدف إلى حماية الحياة الخاصة ، إلا أنه قد يتعارض مع الصالح العام و مصلحة المجتمع و عليه فقد أباح المشرع ضبط الرسائل بالشروط سالفة الذكر[3].

و إذا ما تم البحث في حجية الدليل المقدم ضد المتهم و مدى جواز الأخذ به لابد من التفريق بين ما إذا كان ذلك الدليل مشروع أم باطل ، ففي القانون الجنائي لا يجوز الأخذ بالدليل الباطل ضد المتهم في الإدانة لأن ما بنى على باطل فهو باطل ولكن يكفي إستخلاص ثبوت التهمة، وفي ذلك قررت محكمة النقض من المقرر أنه لا يشترط في الدليل في المواد الجنائية أن يكون صريحا ودالأ مباشرة على الواقعة المراد إثباتها بل يكفي أن يكون استخلاص ثبوتها منه عن طريق الاستنتاج مما يتكشف من الظروف والقرائن وترتيب النتائج على المقدمات ، إلا أن الأمر يختلف في البراءة حيث أن المتهم مفترض فيه قرينة

[1] نبيلة هبه هروال ، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات ،دراسة مقارنة، دار الفكر الجامعي، الإسكندرية 2009ص 40.

[2] سعيد عبد اللطيف ، المرجع السابق ، ص 222

[3] سعيد عبد اللطيف، نفس المرجع، ص71

البراءة حيث القاعدة الفقهية " المتهم برئ حتى تثبت إدانته " ، و قد أكدت محكمة النقض ذلك في أحكامها حيث نصت الشرعية الإجرائية سواء ما اتصل منها بحيدة المحقق أو بكفالة الحرية الشخصية والكرامة البشرية للمتهم ومراعاة حقوق الدفاع جميعها ثوابت قانونية أعلاها الدستور والقانون وشرت على حمايتها القضاء ليس فقط لمصلحة خاصة بالمتهم وإنما[1] بحسبانها في المقام الأول تستهدف مصلحة عامة تتمثل في حماية قرينة البراءة وتوفير اطمئنان الناس إلى عدالة القضاء من أجل ذلك نص الدستور في المادة 41 منه على أن الحرية الشخصية حق طبيعي وهو مصونة لا تمس.

و على ذلك فالمحكمة في قرينة البراءة لها أن تأخذ بالدليل المقدم لها حتى و إن كان ذلك الدليل يشوبه البطلان حماية لحرية المتهم ، و إذا ما تعرضنا للبريد الإلكتروني و هو الأساس في أغلب جرائم الإنترنت و المعلومات حيث أن هذا البريد قد يحمل في مضمونة رسائل تحتوي على برامج تسبب إتلاف للحاسب الآلي أو تحويل غير مشروع للنقود أو خطط إجرامية ، و يكون أساس الإثبات في تلك الرسائل هو البيانات الإلكترونية للرسالة ، و التي تحمل مفردات الحاسب الآلي المرسل منه الرسالة (IP ADDRESS) و التي تقوم الشرطة بتعقبها للحصول على بيانات صاحب الجهاز و المكان المرسل منه تلك الرسالة.

وقد أباح المشرع المصرى جواز التعدي على سرية الحديث الخاص سواء المباشر أو غير المباشر ، ففي حالة الحديث المباشر أباح القانون للقاضى إصدار الإذن بالتسجيل و المشرع الفرنسي أباح ذلك دون تفرقه بين حديث خاص أو تليفوني[2].و إذا كان ذلك للمحادثات التليفونية أو الخاصة فهو أولى أن يكون للمحادثات عبر شبكة الإنترنت للوقوف على أي ضرر قد يقع .

و من الأمثلة في كيفية إثبات التهمة نحو المتهم ضبط و تفتيش الأجهزة الخاصة بالحاسب الآلي الخاص بالمتهم، و فحص وحداته الأساسية و هي وحدات الإدخال و وحدات التخزين

---

[1] نایر، نبیل عمر، الحماية الجنائية للمحل الإلكتروني للمحل الإلكتروني للجرائم المعلوماتية،دار الجامعة الجديدة للنشر2012،ص169.

2 محمود أحمد طه ، التعدي على حق الإنسان في سرية اتصالاته الشخصية بين التجريم والمشروعية ، دار النهضة العربية ، مطبعة جامعة طنطا 1993 ص 241

و التي يتم إستخدامها الحفظ البيانات و المعلومات و الكروت و البطاقات الممغنطة و التي يتم تسجيل البيانات عليها[1].

و لإثبات التهمة على المتهم لابد من بلوغ القاضي درجة اليقين من إرتكاب المتهم لتلك الجريمة و اليقين في تلك الحالة هو اليقين القضائي و ليس الشخصي[2] ، و يتم الوصول إلى ذلك اليقين عن طريق إستقامة الأدلة التي تحمل في مضمونها الإقناع و لا تكون درب من الخيال والمعرفة المطلوب توافرها لدى القاضي في الجريمة الإلكترونية تتطلب إلمام بعض القواعد العلمية التي تساعد في إدراك الكيفية التي تمت بها الجريمة، لبلوغ الإقتناع الكامل دون تأرجح بين البراءة والإدانة نحو المتهم وإلا كانت البراءة هي الحكم الواجب التطبيق.

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي الإسكندرية2006،ص396.
[2] .عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجيستير، دار الجامعة الجديدة، الإسكندرية2009، ص179.

خاتمة

خاتمة:

- يسود العالم إهتمام متزايد بثورة المعلومات وتكنولوجيا الإتصالات والتي أصبحت سمة هذا العصر فلقد أصبح العالم بمثابة قرية صغيرة يستطيع الإنسان أن يتبادل المعرفة خلال وقت قصير.

- ولقد أصبح من الثابت أن نشكل العالم اليوم هو انتاج العلم والتكنولوجيا فالدول التي تمتلك أدوات التكنولوجيا هي الدول التي تمتلك الغد.

- ونتيجة هذا التطور الهائل نتجت جرائم ترتبط بتقنية المعلومات مما أثار تحديات بالغة في حمل أنشطة المكافحة وأنشطة التحقيق والوصول الى مرتكبيها مما أثارت تحديات قانونية وفنية بشأن أليات مباشرة إجراءات التفتيش والضبط والتعامل مع الأدلة الرقمية الإلكترونية المتعلقة بهاته الجريمة.

- فهذه الجريمة (الإرهاب الإلكتروني) هي جريمة لا تترك أي أثر مادي في مسرح الجريمة، فلم تكن لهم القدرة على اتلاف أو تشويه او إضافة الدليل في فترة قصيرة.

إن تم استخلاص من بحثنا هذا هو أن الارهاب الالكتروني أفة وظاهرة دولية افتكت بالدول والشعوب وواكبت العصر من خلال استغلال التكنولوجيا الحديثة التي عمدت من خلالها تحطيم دول في ضرف وجيز وسريع من خلال الإبحار عبر مواقع شبكات الإنترنت.

فالإرهاب الإلكتروني كما هو معروف تقليديا في أثاره وأسلوبه نسج خيوطا وإرتبط شبكة الانترنت من خلال الإستغلال الأمثل للتكنولوجيا وهو ما أصبح يعرف بالإرهاب الحديث وعليه حاولنا من خلال بحثنا هذا التعرف على الإرهاب الحديث، وعليه حاولنا من خلال بحثنا هذا التعرف على الإرهاب الإلكتروني، مميزاته، أهدافه والجهود الوطنية الإقليمية وحتى الدولية للحد من هاته الجريمة المعاصرة والتحديات الممارسة في هذا المجال من خلال إبراز أهم القوانين الوطنية لدول صديقة وشقيقة وإتفاقيات إقليمية ودولية في هذا الصدد.

وعن الإستنتاجات المتوصل إليها من بحثنا هذا في الأتي:

- مما اثبتت فيه أن درائم الإرهاب الإلكتروني من الجرائم التي تمد الدول في مختلف المجالات.

- تتقدم وسائل إرتكاب هاته الجريمة بمستوى التقدم التكنولوجي والإلكتروني، وكلما حصلنا على نظام إلكتروني في جديث ومتطور إغتنم المجرمون المعلوماتيون (الإرهابيون) مزايا ومعطياته في أنشطتهم في أنشطتهم الإجرامية.

- تتضارب الجهود الوطنية والدولية ومن الممكن أن تتلاقى مثل هذه الجهود غير أن غياب القوانين المواكبة للتطور التقني والإفتقار إلى الحد الأدنى من الخبرة اللازمة لمواجهة هاته الجريمة، كل ذلك يجعل من جهود المكافحة هباء منشورا ما لم يتم الإسراع في تكوين إطار تشريعي ومؤسسي لمكافحة هذا النوع من الجرائم على المستوى الوطني والدولي بشكل أكثر فعاية وشفافية وعت التوصيات.

مما سبق ومن خلال بحثنا هذا وعن الصعوبات التي لاقتناء في جمع المادة العملية حول هذا الموضوع بالتحديد كان لازما:

- على الصعيد الوطني: بالنسبة للمشرع الجزائري تطوير المادة القانونية بما يتناسب التطورات التكنولوجية الحاصلة في هذا المجال بسن قوانين وإجراءات بما يتناسب ونوع الجريمة المستخدمة في هذا المجال.

- تضافر الجهود الوطنية والدولية والقيام بحملات تحسيسية بصفة دورية حول مخاطر الأنترنت عبر المدارس والجامعات...

- إستحداث وحذات خاصة على الصعيد الوطني في مجال البحث والتحري في مثل هاته الجرائم بالإضافة إلى القضاء المتخصص الذي لابد منه في هذا المجال بالإضافة إلى تقنين النصوص في مثل هاته الجريمة.

- تفعيل دور الاسر والمجتمع بكل بمخاطر الإنترنت والإستغلال العقلاني لها.

- تبادل الخبرات الأمنية والقانونية من خلال عقد لقاءات وندوات على الصعيد الوطني في مختلف المراكز التكونية والتعليمية والجامعات على المستوى الوطني وعقد مؤتمرات دولية وتبادل الخبرات في هذا المجال.

- عقد إتفاقيات بين الدول على الصعيدين الدولي والإقليمي تشمل مختلف الجوانب للحد من هاته الجريمة.

- زيادة الوعي لدى المتدرسين بمخاطر الانترنت من خلال دمجها في المقررات الدراسية بالإضافة إلى فاعلية الوظائف من خلال دورات التكوين لشغل الوظائف.

لنخلص في النهاية إلى أن جرائم الإرهاب الإلكتروني، ماهي إلا إحداث الحلقات السيئة في ثورة المعلومات والتي تحصد من خلالها الدول أشواطا نتيجة الزرع السيئ والتي تقطف ثماره المرير اليوم وغدا.

قائمة المراجع

قائمة المراجع

1- الكتب

1.أيمن عبد الحفيظ ، الإتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، القاهرة 2005.

2.جميل عبد الباقي ، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة1992.

3.سعيد عبد اللطيف إثبات جرائم الكمبيوتر والجرائم المرتكبة على الانترنت، دار النهضة العربية،القاهرة،1999.

طوني عيسى، حماية برامج الكمبيوتر وقواعد البيانات، مقالة قانونية منشورة في مجلة العدل، قسم الدراسات، العدد 1999، منشورات نقابة المحامين في بيروت.

4.عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجيستير، دار الجامعة الجديدة، الإسكندرية2009.

5.عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي الإسكندرية2006.

6.عبد الفتاح حجازي، مقدمة في التجارة الالكترونية العربية، الكتاب الأول: شرح قانون المبادلات والتجارة الالكترونية التونسي، دار الفكر الجامعي، الاسكندرية، 2004.

7.عبد الله علي محمودإجراءات جمع الأدلة في مجال سرقة المعلومات، منشور على الموقع الإلكترونيhttp//.www.qanoun.net

8.لواء دكتور قدرى عبد الفتاح الشهاوي،الإستخبارات والإستدلالات وحقوق الإنسان وحرياته الأساسية، دار النهضة العربية، القاهرة،2006.

9.محمد الألفي، المسؤولية الجنائية عن الجرائم الاخلاقية عبر الانترنت، الكتب المصري الحديث للنشر، القاهرة،2005.

10. محمد العلماء، جرائم الإنترنت والإحتساب عليها، دراسة منشور في الجامعة العربية للدراسات الأمنية والتدريب المجلة18، العدد36. منشورات أكادمية تأليف للعلوم الأمنية، الرياض، أكتوبر 2003.

11. محمود أحمد طه ، التعدي على حق الإنسان في سرية اتصالاته الشخصية بين التجريم والمشروعية ، دار النهضة العربية ، مطبعة جامعة طنطا 1993.

12. مصطفى يوسف كافي، جرائم الفساد، غسيل الأموال، السياحية، الإرهاب الإلكتروني، المعلوماتية، ط1، 2015، مكتبة المجتمع العريب للنشر والتوزيع، عمان، الأردن.

13. ناير، نبيل عمر، الحماية الجنائية للمحل الإلكتروني للمحل الإلكتروني للجرائم المعلوماتية، دار الجامعة الجديدة للنشر2012.

14. نبيلة هبه هروال ، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية 2009.

15. نبيلة هروال، الجوانب الإجرائية لجرائم الأنترنت في مرحلة جمع الإستدلالات، دار الفكر الجامعي، الإسكندرية،2006.

16. نواران شقيق، أثر التهديدات الإلكترونية على العلاقات الدولية، ط1، 2016، مصر القاهرة.

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

2- المراجع باللغة الفرنسية:

1. Adrian Croft. (June 4, 2013). NATO Boosts Cyber Defenses but Members Differ on its Role. Reuters.

2.Haly Laasme. (October, 2011). Estonia: Cyber Window into the Future of NATO. Joint Force Quarterly, Issue 63.

3.Jennifer A. Chandler Cyberspace:. (2003-2004). Security in Combatting Distributed Denial of Service Attacks. University of Ottawa Law & Technology Journal, Vol. 1.

4.Melissa E. Hathaway, Alexander Klimburg, (2012). Preliminary Considerations: On National Cyber Security. In Alexander Klimburg.

3- القوانين

- قانون العقوبات الجزائري.
- قانون 09/04 المؤرخ في 05/08/2009

4 - المواقع الإلكترونية

1. arabic.mjustice.dz
2. www.arablaw.com
3. www.arablawinfo.com
4. www.mctmnet.gov.om

فهرس المحتويات

فهرس المحتويات