الإرهاب الإلكتروني وأثرة في أمن الدول.. السعوديَّة إنموذجاً

*رؤى خليل سعيد خليل

*باحثة من العراق
باحثة في مركز حمورابي

المقدمة

إنَّ ظهورِ الحاسبات الآلية التي أدت إلى تغيير شكل الحياة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوماً بعد يوم، سواء في المؤسسات المالية، أم المرافق العامة، أم المجال التعليمي، أم الأمني أم غير ذلك، إلا أنه وإن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد، فإنَّ الوجه الآخر والمتمثِّل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة ومنها الإرهاب الإلكتروني أصبح خطراً يهدِد العالم بأسره، إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق.

إن أكثر الأنظمة التقنية تقدماً وأسرعها تطوراً هي الأنظمة الأمنية، وعلى الرغم سرعة تطورها إلا أنها أقل الأنظمة استقراراً وموثوقية، نظراً لتسارع وتيرة الجرائم الإلكترونية وأدواتها والثغرات الأمنية الُّتي لا يمكن أن يتمَّ الحد منها على المدى الطويل، فمجال أمن المعلومات في الإنترنت آخذ في التطور بشكل كبير تماشُّياً مع التطور في الجريمة الإلكترونية.

من مظاهر تهديد الإرهاب الالكتروني لأمن الدولة، عملُ الجماعاتِ الإرهابيةِ على نشر أفكارهم وقيمهم على شبكات التواصل الإجتماعي، وضمٌّ أكبر قدُر ممكن من الأفراد وتجنيدهم وتعليمهم كيفية استخدام المتفجرات واختراق المواقع الالكترونية وغيرها من العمليات الإجرامية غير المشروعة، إضافة إلى اختراق الشبكات الحساسة للدول والتجسس عليها وإرسال رسائل تهديد للدول لقبول مطالبهم.

فنتيجة لجملة هذه التهديدات المتنوعة، يتوجب على المجتمع الدولي بمختلف أشكاله تبني مجموعة من الإستراتيجيات لمواجهة الإرهاب الالكتروني، وتحقيق أمن واستقرار الدول.

أهميَّة البحث

إزداد خطر الإرهاب الالكتروني نتيجةً لاستخدام الدولة التكنولوجيا المتطورة في مختلف الميادين، لإتصافها بسهولة الاستخدام ورخص التكلفة بهدف تحقيق الرخاء والتقدم البشري، لكن الجماعات الإرهابية استغلت الظروف وبدأت تشن هجمات على مختلف القطاعات السياسية، الاقتصادية العسكرية والاجتماعية من خلال إختراقها المواقع الالكترونية لرؤساء الدول والحكومات والوزارات والتجسس عليها وتدميرها، والإطلاع

على مختلف المعلومات الأساسية للدولة خاصة الأمنية منها، إضافة إلى المؤسسات الاقتصادية كالبنوك والبورصات العالمية، مما يؤثر سلبا في الأمن الاقتصادي للدولة. فلم تقتصر الهجمات على الجوانب السياسية والأمنية والاقتصادية فقط، بل مسَّت أيضا الجوانبَ الإجتماعيةَ والثقافيةَ بتدمير مواقع المستشفيات ومصانع توليد الطاقة الكهرباء ،الماء، الغاز، والعمل أيضا على نشر ثقافة التطرف الديني في أوساط الشباب وطمس الهوية واجتذابهم إلى المنظمات الإرهابية مما يهدّد الأمن الإجتماعي.

إشكاليَّة البحث

الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر المقبل، نظراً لتعدُّد أشكاله وتنوُّع أساليبه واتّساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الفوضى، مع توفير قدر كبير من السلامة والأمان للإرهابيين. وعليه فالإشكالية المطروحة: ما الإرهاب الإلكتروني وأهدافه وأساليبه؟ وكيف أثَّر الإرهابُ الإلكتروني في أمن واستقرار الدول؟ وكيف تعاملت السعودية مع الإرهاب الالكتروني؟

فرضية البحث

في ظل مختلف هذه التهديدات الأمنية المختلفة لأمن الدولة عامة والمجتمع خاصة، عملت وحدات المجتمع الدولي على إتخاذ الإستراتيجيات كافة لمواجهة ظاهرة الإرهاب الالكتروني وتحقيق أمن واستقرار الدول. فارتبط أمن واستقرار الدول بمدى تأثير مخاطر الإرهاب الالكتروني.

المبحث الأول: الإطار النظري للإرهاب الإلكتروني

يتميّز الإرهابُ الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

والحرب الالكترونية هي جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بوساطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات سواء لإرتكابها أم للتحقيق فيها.

اولا: تعريف الإرهاب الالكتروني وأسبابه

توسَّعت الحرب في المدة الأخيرة لتستخدم أرقى التطورات التكنولوجية في المجالات جميعها، ولا شكَّ في أنَّ تطور التقنيات الإلكترونية كان من أهم المجالات التي حاولت الحرب استخدامها، بل إن الجيوش والقوى الأخرى المُهتمَّة بالأعمال الحربية تستخدم التقنيات الإلكترونية المتطورة حتى في حالات السلام، إمّا استعداداً لأي حرب أو من أجل الدفاع وجمع المعلومات.

والحرب الالكترونية هي جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بوساطة الحاسب الآلي من خلال شبكة الانترنت وهي تتطلب إلماماً خاصَّاً بتقنيات الحاسب الآلي ونظم المعلومات سواء لإرتكابها أم للتحقيق فيها [1].

1 - إسراء جبريل رشاد مرعي، الجرائم الإلكترونية.. الأهداف - الأسباب - طرق الجريمة ومعالجتها، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، 30/4/2017، http://democraticac.de/?p=35426.

أمَّا الأمن الإلكتروني فهو مجموع الوسائل التقنية والتنظيمية والإدارية التي يتمُّ استخدامُها لمنع الاستخدام غير المصرَّح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني [2]. ويمكن أن يشمل مفهوم "الأمن الإلكتروني" الإجراءات الرامية إلى اختراق منظومات "العدو" بهدف الحماية منه وليس الحرب عليه، فهو على ذلك مفهوم وقائي ودفاعي أصلاً.

2 - منى الاشقر جبور، السيبرانية.. هاجس العصر، المركز العربي للبحوث القانونية والقضائية، مصر، ص28

أمَّا عن الإرهاب الإلكتروني لا يوجد تعريف جامع مانع لمفهوم الإرهاب الالكتروني وذلك نتيجة لحداثة المفهوم وغياب تعريف دقيق لمفهوم الإرهاب في حد ذاته، ففي هذا الإطار نحاول التطرق لبعض التعريفات للإرهاب الالكتروني. فلا بدَّ من الإشارة إلى أن الإرهاب والإنترنت مرتبطان بطريقتين: الأولى ممارسة الأعمال التخريبية لشبكات الحاسوب والإنترنت. والثانية أن الإنترنت أصبحت منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف،

وللاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم.

عرَّفه جيمس لويس James Lewiss على أنه :"استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة مثل : الطاقة والنقل ،أو بهدف ترهيب الحكومة والمدنيين" [3].

يُعرَّف "الإرهابُ الإلكتروني" بأنه:" العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان، في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد" [4]. فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

أسباب الإرهاب الإلكتروني [5]

– ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: مما يُمكّن المنظمات الإرهابية من التسلل إلى البنية التحتية وتخريبها، وذلك نتيجة لإتصاف شبكات المعلومات بالانفتاح وغياب القيود والحواجز الأمنية واحتوائها على ثغرات معلوماتية بهدف التوسع وتسهيل الدخول.

– غياب الهوية الرقمية :إذ يقوم الإرهابي بشن هجومات إلكترونية بهوية وشخصية وهمية بدون مخاطرة.

– سهولة الاستخدام وقلّة التكلفة: بمعنى أنه للقيام بالهجوم الإلكتروني لا بدَّ من توفر حاسوب متطور متصل بشبكة معلوماتية متطورة فهو لا يكلف جهداً ولا يستغرق وقتا.

– غياب الآليات القانونية للسيطرة والرقابة على الشبكات المعلوماتية: فغياب الاتفاقيات الدولية والتشريعات الوطنية الخاصة بالإرهاب الالكتروني يؤدي إلى زيادة انتشار الظاهرة وتوسعها

3– Alix DESFORGES، " Cyberterrorisme : quel périmètre ?"، Fiche de l'Irsem n° 11، décembre 2011 ، p.03. file:///C:/Users/sarra/Downloads/Fiche__n11__p – rimetre__cyberte – rorisme%20(2).pdf 03/02/2017 à 08:39.

4 – أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته". محاضرة ألقيت بملتقى دولي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية ،أيام 04–02 /09/2014، ص09.

5 – بوحادة سارة، أثر الإرهاب الالكتروني على أمن واستقرار الدول، المدرسة الوطنية العليا للعلوم السياسية –الجزائر، ص7.

في مختلف دول العالم.

صعوبة اكتشاف وإثبات الجريمة الإرهابية: القناع الالكتروني والمهارة الفنية كفيلان بإخفاء أثر المجرم.

– صعوبة اكتشاف وإثبات الجريمة الإرهابية: القناع الالكتروني والمهارة الفنية كفيلان بإخفاء أثر المجرم.

– تستطيع أن تلحق الضرر بعدد أكبر من الأفراد مقارنة بالهجمات التقليدية وهو ما يساعدها على جذب الاهتمام الإعلامي والحكومي مما يمكّنها من تحقيق أهدافها .

ثانياً: خصائص الإرهاب الإلكتروني وأهدافه:

يتميّز الإرهاب الإلكتروني بعدد من الخصائص والصفات التي يختلف فيها عن بقية الجرائم، وتحولً دون اختلاطه بالإرهاب العادي، ومن الممكن إيجاز أهم تلك الخصائص والصفات فيما يلي[6] :

1 – إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسوب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

2 – يتّصف الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود.

3 – صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.

4 – صعوبة الإثبات في الإرهاب الإلكتروني، نظراً لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.

5 – يتميّز الإرهاب الإلكتروني بأنه يتمُّ عادة بتعاون أكثر من شخص على ارتكابه.

6 – أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي

6 – 1. عبدالله بن عبدالعزيز بن فهد العجلان، "الإرهاب الإلكتروني في عصر المعلومات" بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في 4–2 جوان 2008، ص14.

الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.

اما أهداف الإرهاب الإلكتروني [7]:

7 – المصدر نفسه السابق.

يهدف الإرهاب الإلكتروني إلى تحقيق جملة من الأهداف غير المشروعة ويمكننا بيان أبرز تلك الأهداف في ضوء النقاط الآتية:

1 – نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة.

2 – الإخلال بالنظام العام، والأمن المعلوماتي، وزعزعة الطمأنينة.

3 – تعريض سلامة المجتمع وأمنه للخطر.

4 – إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة.

5 – تهديد السلطات العامة والمنظمات الدولية وابتزازها.

6 – الإنتقام من الخصوم.

7 – الدعاية والإعلان، وجذب الانتباه، وإثارة الرأي العام.

8 – جمع الأموال والإستيلاء عليها.

لكل هذه الأسباب والدوافع أصبح الإرهاب الإلكتروني هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية، لذلك عُدّت هذه الثوابت قاعدةً أساسيةً في التحكم في المستقبل العلمي للدول المتقدمة.

فإن عالم الانترنت يجتذب المنظمات الإرهابية لافتقاره عناصر

الرقابة، كما أنه بيئة مناسبة لممارستهم الإرهابية ونشر الأفكار المتطرفة التي تسيطر على وجدان الأفراد لإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض و مصلحة المجتمع أو القيام بأعمال تخريبية بشكل يخفي هويتهم المباشرة وبشكل أبسط مما يقوم به الإرهابيون الفعليون، ففي حين يحتاج الإرهاب الفعلي إلى أسلحة وتحركات سرية قد تصيب أو تخفق، فضلاً عن التكاليف المادية لإنجاح هذه العمليات، يحتاج الإرهاب الإلكتروني إلى بعض المعلومات فقط ليستطيع اقتحام الحواجز الإلكترونية، كما أن تكاليف القيام بهذه الهجمات لا تتجاوز جهاز حاسوب والدخول إلى الشبكة العنكبوتية.

يُعد الإرهاب الإلكتروني تهديداً لأمن واستقرار الدول وذلك نتيجة لاستخدام الدول التكنولوجيا المتطوّرة في البِنية التحتية وتطوير المؤسسات الرسمية وغير الرسمية وجعلها إلكترونية، فهذا ما سهل على الجماعات الإرهابية إختراق هذه المواقع وتهديدها ونشر الرعب والخوف لتحقيق أهدافها، باستخدام الانترنت للاتصال والتلقين وكسب أكبر عدد ممكن من المتعاطفين معهم.

فظهر التزاوج بين الانترنت والإرهاب بشكل أكبر وضوحاً بعد أحداث الحادي عشر من أيلول 2001م، فقد انتقلت المواجهة ضد الإرهاب من مواجهة مادية مباشرة واقعية إلى الفضاء الإلكتروني، حيث أصبحت الانترنت من أشدِّ وأكبرِ الأسلحة الفتاكة.

المبحث الثاني: الإرهاب الإلكتروني تحد لأمن الدول

يُعدُّ الإرهاب الإلكتروني تهديداً لأمن واستقرار الدول وذلك نتيجة لاستخدام الدول التكنولوجيا المتطوّرة في البنية التحتيَّة وتطوير المؤسسات الرسمية وغير الرسمية وجعلها إلكترونية، فهذا ما سهَّل على الجماعات الإرهابية إختراقَ هذه المواقع وتهديدها ونشر الرعب والخوف لتحقيق أهدافها، باستخدام الانترنت للاتصال والتلقين وكسب أكبر عدد ممكن من المتعاطفين معهم.

اولا: إستخدام الجماعات الإرهابيَّة للأنترنت، وأثر ذلك في أمن الدول.

تعمل الجماعات الإرهابية على استخدام تكنولوجيا متطورة لنشر مبادئهم وتصوراتهم ، والقيام بعدّة أعمال تخريبية عن طريق شبكات الانترنت للوصول إلى أهدافها المرجوَّة، وذلك من خلال ما يلي[8]:

8 – عبد الله بن عبدالعزيز بن فهد العجلان، "الإرهاب الإلكتروني في عصر المعلومات" بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة في 4-2 جوان 2008 ، ص ص 19-16.

* أمثلة عن المواقع الالكترونية للجماعات الإرهابية :

-1موقع النداء: الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001م، ومن خلاله تصدر البيانات الإعلامية للقاعدة. -2 ذروة السنام: وهي صحيفة إليكترونية دورية للقسم الإعلامي لتنظيم القاعدة. -3 صوت الجهاد: وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، تصدر بصيغتي : (word)،(pdf) وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.

1 – الإتصال : تستخدم الجماعاتُ الإرهابيَّةُ الانترنت للاتصال فيما بينهم وتمويل عملياتهم من مناطق مختلفة قد تبعد مئات الكيلومترات عن منطقة العملية الإرهابية، نظراً لسرعتها وقلَّة تكلفتها مقارنة بالوسائل الأخرى، إضافة إلى وفرة المعلومات إذ تُعدُّ شبكةُ الانترنت موسوعةً الكترونية غنيَّةً بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، مواقعَ المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات، ومواعيد الرحلات الجوية الدولية، والمعلومات المختصَّة بسبل مكافحة الإرهاب، وغيرها من المعلومات التي تُعدُّ بمثابة الكنز الثمين بالنسبة للإرهابيين.

2 – نشر الأفكار المتطرفة: تعمل الجماعاتُ الإرهابية لنشر التطرف من خلال مواقع التواصل الإجتماعي وغرف الدردشة مع مختلف شرائح المجتمع خاصة فئة الشباب لإستغلالهم في العمليات الإرهابية، إضافة إلى وجود عدّة مواقع إرهابية، فمثلاً هناك تقرير كَشَفَ أن التنظيم الإرهابي لداعش لديه 90 ألف صفحة باللغة العربية على موقع التواصل الإجتماعي الفايسبوك و40 ألف بلغات أخرى ، إضافة إلى موقعه الذي دشنه التنظيم بسبع لغات لإبتزاز الشباب وضمّهم لصفوفهم فحوالي 3400 شاب إنضمَّ إلى داعش عن طريق حملات التنظيم الالكترونية. فحسب جمعية آفاق للأمن الداخلي لتونس أن المواقع الإلكترونية ذات التوجّه المتطرّف والإرهابي تستقطب نحو ألف شاب في السَّنة وهو يعادل 3 شبان يوميا ، وهو رقم مرتفع يعكس خطورة الظاهرة التي تزداد حدّتُها وهم يمثلون حوالي 40٪ من مجموع الشباب المستقطب وهم من الطلبة والتلاميذ المتفوقين الذين تتراوح أعمارهم بين 17 و28 سنة الذين يدرسون الاختصاصات العلمية :الطب ،الفيزياء والكيمياء إذ تقوم هذه الجماعات باستثمار مهاراتهم العلمية لأغراض تخريبية [9].

9– إيهاب شوقي ، الإرهاب الالكتروني و جرائمه، من الموقع: http://www.anntv.tv/new/showsubject.aspx?id=121062

3 – التخطيط والتنسيق : تستخدم الجماعات الإرهابية الانترنت للتخطيط والتنسيق فيما بينهم وتدبير الهجمات الإرهابية، ففي 2001 تمَّ التخطيط بشكل مكثف لهجمات 11 سبتمبر عبر الرسائل الالكترونية العادية وغرف الدردشة لتحديد مهام كل عنصر. كما

نجحت داعش في التخطيط والتنسيق لعملياتها الإرهابية الكبرى في أوروبا، وخاصة في فرنسا وبلجيكا، من خلال شبكات المعلومات ومواقع التواصل الاجتماعي لا يمكن رصدها، بل وتمحى بعد قراءتها مباشرة من خلال أجهزة ألعاب الفيديو المتصلة عبر الإنترنت، وأدَّت هذه العمليات الإرهابية لمقتل نحو مئتي شخص في تشرين الثاني 2015، وفشلت أجهزة المخابرات الأوروبية في رصد العمليات قبل وقوعها لكنها اكتشفت هويات منفذيها من خلال هواتفهم المحمولة ومكالماتهم المتبادلة مع أفراد المنظمة [10].

10 – أيمن حسين ،"الإرهاب الالكتروني أخطر معارك حروب الفضاء": من الموقع : تم تصفحه يوم 01-02-2017 على الساعة 12:14 http://alwatan.com/details/166324 تاريخ النشر:14/01/2017.

4 – التلقين الإلكتروني: تسعى الجماعات الإرهابية من خلال الوسائل الالكترونية إلى تقديم إرشادات وطرق صنع القنابل اليدوية والأسلحة الكيمياوية الفتاكة وأساليب التفخيخ والتفجير.

تسعى الجماعات الإرهابية من خلال الوسائل الالكترونية إلى تقديم إرشادات وطرق صنع القنابل اليدوية والأسلحة الكيمياوية الفتاكة وأساليب التفخيخ والتفجير.

5 – التمويل الإلكتروني: تحظى الجماعات الإرهابية بتمويل إلكتروني باستغلالها أصحاب القلوب الرحيمة لدفع تبرعات مالية لأشخاص اعتباريين يمثلون واجهة لهؤلاء الإرهابيين، بطريقة ماكرة لا يشك فيها المتبرع بأنه يساعد الجماعات الإرهابية.

ثانياً: مظاهر تهديد الإرهاب الإلكتروني لأمن الدول:

تفاقمت ظاهرة الإرهاب الإلكتروني في الآونة الأخيرة وأثّرت سلباً في أمن الدول في مختلف الميادين، إذ تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق الآثار التي استخدمت فيها المتفجرات، مما يلحق أضرارا بالمؤسسات المالية، وأجهزة الاتصال والبنى التحتية والمؤسسات الحكومية وغيرها من الكيانات التي تعتمد بشكل كبير على شبكة الانترنت، والذي يؤدي بدوره إلى تعطيل المحركات الرئيسة للدولة والإضرار بمواطنيها وأمنها القومي. ومن تداعيات الإرهاب الالكتروني على أمن الدول ما يلي :

- تهديد أمني سياسي : تعمل المنظمات الإرهابية على إلحاق الشلل

بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها. مما يهدّد أمن الدول ، كما تهدّد شخصيات سياسية بارزة في المجتمع بالقتل ، أو بالقيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، إضافة لاختراق البريد الإلكتروني لرؤساء الدول وكبار الشخصيات السياسية وهتك أسرارهم والإطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية، أو تهديدهم لحملهم على إتيان أفعال معينة يخطّطون لاقترافها.

مثلا في إيطاليا عام 1998م تعرضت عدة وزارات وجهات حكومية ومؤسسات مالية لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها [11]، وفي عام 2010 ظهر ما عُرف باسم "إعصار ويكيليكس" إذ تمَّ استغلال شبكة الإنترنت العالمية في تسريب وثائق تحتوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقُنصلياتها الخارجية بدول العالم [12]. وفي آذار 2014 هاجمت مجموعة "سايبر بيركوت" الأوكرانية المواقع الإلكترونية لحلف الناتو، ما أدى إلى تعطيل مواقع الحلف لعدة ساعات". كما أعلن الكرملن أن قراصنة حاسوب شنوا هجوماً "عنيفاً" على موقع الرئاسة الروسية، وعطلوا العمل بموقع البنك المركزي الروسي. وأقرَّ مفتش وحدة الجرائم الإلكترونية الأمريكي في عام 2014، بأن قراصنة أجانب تمكنوا من اختراق حاسبات تابعة للهيأة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية ومؤخراً أكدت صحيفة نيويورك تايمز في تقرير لها في 26 نيسان 2015 أن قراصنة روسيين إطَّلعوا على رسائل إلكترونية للرئيس الأمريكي باراك أوباما العام الماضي، بعدما تمكنوا من اختراق الشبكة الإلكترونية غير السرية للبيت الأبيض، واطلعوا على أرشيف الرسائل الإلكترونية لموظفين في البيت الأبيض يتواصلون يومياً

وفي عام 2010 ظهر ما عُرف باسم «إعصار ويكيليكس» إذ تم استغلالُ شبكة الإنترنت العالمية في تسريب وثائق تحتوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقُنصلياتها الخارجية بدول العالم

11 - حسن بن سعيد بن سيف الغافري ،الإرهاب الالكتروني .من الموقع
http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=1&PID=9&LID=5

12 - شيريهان نشأت المنيري ،"مخاطر جرائم الانترنت على استقرار النظام الدولي"، مجلة السياسة الدولية، من الموقع
http://www.siyassa.org.eg/NewsQ/2450.aspx

مع أوباما، ومن خلال هذا الأرشيف تمكَّن القراصنةُ من قراءة رسائل تلقاها أوباما [13] وهذا ما يهدّد الأمن القومي الأمريكي.

13 – الإرهاب الالكتروني ...هل يتحول إلى مصدر التهديد الأول في العالم، من الموقع http://alkhaleejonline.net/articles/1430728333185670700/ تاريخ النشر: 04/05/2015

أمَّا أمنياً تعمل الجماعات الإرهابية على التسلل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلّها لصالحها، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها[14] .

14 – عبدالله بن عبدالعزيز بن فهد العجلان، مرجع سبق ذكره ،ص22.

• تهديد اقتصادي: اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، وتعطيل عمليّات التحويل المالي، مما يُلْحقُ الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة، وإلحاقَ الأذى بالاقتصاد الوطني، وتعديلُ ضغط الغاز عن بُعد في أنابيب الغاز لتفجيرها، ونُظم السلامة في المصانع الكيمياوية لإحداث أضرار بالناس، ومن أمثلتها قيام بعض الإرهابيين بتحويل ملايين الدولارات من بعض الحسابات الشخصية لكبار العملاء بعد إختراق نظام التحويلات الدولي بين البنوك، وقيام بعض الهاكرز المحترفين بسرقة بيانات بطاقات الإئتمان من بعض أكبر مراكز التسوق الإلكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقات، وكذلك قيام بعض المنظمات الإرهابية بالعمل على تدمير اقتصاد إحدى دول الشرق الأوسط بشراء سندات دولية لتلك الدولة من داخلها عبر البورصات العالمية وبيعها بالخارج بأسعار أقل من قيمتها مما أدى إلى إنهيار عملتها . . . ولتوفير تمويل لأعمالها الإرهابية في الدول التي تمَّ بيع السندات فيها [15].

15 – أيمن حسين ، مصدر سبق ذكره.

كما مُني عددٌ من الشركات والمصارف العملاقة بخسائر اقتصادية فادحة نتيجة القرصنة الإلكترونية التي واجهتها. فحسبما أشار أحدثُ دراسة أجرتها مؤسسة B2B International وشركة كاسبرسكي لاب، والتي أعلنت عنها في الخامس عشر من نيسان 2015 فإن 25 % من الشركات في منطقة الخليج تُعدُّ

هجمات (DDoS) أحد أكبر ثلاثة تهديدات تواجه الشركات في المنطقة. و بَعدّها أحد أهمّ التقنيات الشائعة التي يستخدمها مجرمو الإنترنت لكسَب الأموال، فإن عدد وتأثير هذه الهجمات يتزايد من عام لآخر وهو ما جعل قضية حماية المستخدمين أمراً أولوياً لدى الشركات. وقبل السادس من شباط 2015، أكدت شركة "كاسبرسكي" الرائدة في مجال الأمن المعلوماتي أن مجموعة من "الهاكرز" تمكنوا من السيطرة على حسابات في مصارف عالمية، وسرقة نحو مليار دولار، إذ استخدموا تقنيات معقدة من أجل الوصول للحسابات، واستغل "الهاكرز" ثغرة بأنظمة أجهزة الحاسوب في المصارف تمكنوا خلالها من نسخ بيانات الحسابات في مدة لا تتجاوز 20 ثانية واستغلوها من أجل تحويل الأموال بسرعة فائقة [16].

16 – الإرهاب الالكتروني ...هل يتحول إلى مصدر التهديد الأول في العالم؟، مصدر سبق ذكره.

• تهديد إجتماعي : يؤثّر الإرهاب الالكتروني في حياة المدنيين ورفاهيتهم وحتى ثقافتهم كالتالي:

– تُوجّه المنظمات الإرهابية رسائلَها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهاربها، وذلك بهدف شن حملات نفسية ضد الدول العدوَّة ، فهي تعرض أفلاماً مرعبة للرهائن والأسرى أثناء إعدامهم ، مما يؤثّر في المدنيين.

– إختراق صفحة إلكترونية لمستشفى وتهديد حياة المرضى فيه عن طريق التلاعب بأنظمة العلاج عن بُعد بهدف قتل المرضى، وأيضا في مصانع غذاء الأطفال لتغيير مُستويَات نسب المواد الغذائيّة بهدف قتل الأطفال.

– شن عمليات إرهابية على المواقع الحيوية، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، فمثلا في كانون الثاني 2008 تمَّ قطع الكابل البحري الذي يربط أوروبا بالشرق الأوسط والكابل القريب من ساحل دبي وخليج عمان، مما أدى إلى خسائر بقطاع الاتصالات والتعاملات الإلكترونية أو شل محطات إمداد الطاقة والماء، إذ تشير مصادر كلية الحرب الأميركية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى

موت ما بين 70 إلى 90 ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية [17].

17 – أيمن حسين، مرجع سبق ذكره.

ثالثاً: الجهود الدوليَّة لمكافحة الإرهاب الإلكتروني.

عملت وحدات المجتمع الدولي على اتخاذ عدة استراتيجيات لمكافحة الإرهاب الالكتروني وتحقيق الأمن و الاستقرار.

1 – الإستراتيجيات الدولية والإقليميَّة:

أصدرت الأمم المتحدة مجموعة من القرارات عبر جمعيتها العامة التي توضّح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداما غير سلمي ، ففي 22 تشرين الثاني 2002 اتخذت قراراً بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي ، وفي كانون الاول من نفس السنة إتّخذت قرار إرساء ثقافة عالمية لأمن الفضاء الالكتروني وعدّ من القرارات الهامة التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث الدول والمنظمات الدولية والإقليمية على تكثيف التعاون الدولي لمجابهة الإرهاب الإلكتروني [18].

18 – نوران شفيق ،أثر التهديدات الإلكترونية على العلاقات الدولية ،(القاهرة :المكتب العربي للمعارف ،2015)،ص.108.

وفي 2004 تمَّ إنشاء مجموعة الخبراء الحكومية GCE بهدف مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدِف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية، كما شكَّل الأمين العام للأمم المتحدة كوفي عنان في 2004 فريقا دوليا لدراسة قضية إدارة الانترنت [19] .

19 – رائد العدوان ،"المعالجة الدولية لقضايا الإرهاب الإلكتروني"، محاضرة ألقيت في دورة تدريبية بعنوان توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ،الرياض، فيفري 2016، ص ص 10-09.

كما ساهمت مجموعة الدول الصناعية هي الأخرى في مجابهة الإرهاب الالكتروني بإنشاء مجموعة فرعية للجريمة عالية التقنية وتبنت ما عرف بالمبادئ العشرة حول مكافحة جرائم الكومبيوتر ، وفي عام 2000 صدرت مسودة اتفاق عالمي حول مكافحة الإرهاب الالكتروني من جامعة ستاندفورد بهدف الوصول إلى تعاون دولي لمواجهة هجمات الفضاء الالكتروني [20].

20 – المصدر نفسه.

2 – الإستراتيجية الدولية :

أنشأت الولايات المتحدة الأمريكية مؤسسة مركز حماية البنية الأساسية القومي ومقرها الدور 11 من مقر مكتب التحقيقات الفيدرالية ، بلغت ميزانية المركز 1.5 مليار دولار للإعداد والمنع والاكتشافات والاستجابة، أي ربط جميع شبكات الأمن الالكتروني للمراقبة والإشراف، وأن تصبح المخابرات الأمريكية ومجلس الأمن القومي متحدين في هدف مشترك مع مكتب التحقيقات الفيدرالية [21]. وفي مصر يجري العمل في وزارة الاتصالات والمعلومات لإصدار نظام عن الجريمة الإلكترونية، يتضمن عقوبات رادعة لمن يقوم من الأفراد أو المؤسسات بتزوير أو إفساد مستند إلكتروني على الشبكة، أو الكشف عن بيانات ومعلومات بدون وجه حق، وغيرها من صور الجريمة الإلكترونية. ففي 2002 صدر القرار الوزاري رقم 13507 بإنشاء إدارة لمكافحة جرائم الحاسوب وشبكات المعلومات ويساهم في مكافحة الإرهاب الالكتروني. أما في الأردن فيجري العمل لإعداد تنظيم يتعلق بخصوصية المعلومات وسريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر الشبكات العالمية للمعلومات، كما تساهم الأردن في إعداد مشروع حول قانون مكافحة جرائم تقنية المعلومات وما في حكمها، والمقدم إلى الإدارة العامة للشؤون القانونية في جامعة الدول العربية [22].

21 – مصطفى محمد موسى ،الإرهـــاب الالـكـتروني دراسة قانونية –أمنية – نفسية –اجتماعية .(الأردن : دار الكتب والـوثـائـق القومية ،ط.01 ،2009) ص. 298.

22 – مصطفى يوسف كـافي وآخـرون ،الإعـلام و الإرهـاب الالـكـتروني، (الأردن: دار الإعصـار العلمي للنشر والـتـوزيـع ،ط.01 ، 2015.)، ص.167.

المبحث الثالث: الأساليب التي تستخدمها الدول لمكافحة الإرهاب الإلكتروني

لقد أصبح الإرهابُ الإلكتروني أكثرَ ضراوةً لاعتماده على التكنولوجيا المتطورة للأنترنت، التي ساعدت المنظمات الإرهابية في التحكم الكامل في اتصالاتهم البينية، مما زاد من اتّساع مسرح عملياتهم الإرهابية. وينبغي عند وضع آليات لمواجهة انتشار الجماعات الإرهابية عبر مواقع التواصل الإجتماعي الإلكتروني أن يُراعى في طرحها البعد الرسمي الحكومي والشعبي عبر منظمات المجتمع المدني، كما ينبغي أن تُراعى الأبعاد السياسية والقانونية والدينية والاقتصادية للظاهرة.

الإرهاب الإلكتروني من الجرائم العابرة للدول والقارات،

والتحقيق فيها وإثباتها أمر غاية في التعقيد، بالنظر إلى سرعة غياب الدليل الرقمي من جهة، وسهولة إتلافه وتدميره من جهة أخرى.

23 – عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مصدر سبق ذكره.

وتنقسم أساليب مكافحة الإرهاب الإلكتروني إلى قسمين رئيسين:

أ ـ أساليب الوقاية من الإرهاب الإلكتروني [23]:

في ضوء الصعوبات التي تواجه التحقيق في جرائم الإرهاب الإلكتروني، تضطلع الوقاية من هذه الجريمة بأهمية كبيرة بين رجالات الفقه والقانون كوسيلة من وسائل مكافحة الإرهاب الإلكتروني

في ضوء الصعوبات التي تواجه التحقيق في جرائم الإرهاب الإلكتروني، تضطلع الوقاية من هذه الجريمة بأهمية كبيرة بين رجالات الفقه والقانون كوسيلة من وسائل مكافحة الإرهاب الإلكتروني، إعمالاً لقاعدة "درهم وقاية خير من قنطار علاج".

وإذا أردنا أن نتحدث عن طرق الوقاية من جرائم الإرهاب الإلكتروني، يبرز إلى حيز الوجود الدور الذي يمكن أن يلعبه الإعلام الرسمي وغير الرسمي في مواجهة المواقع التي تروّج للفكر المتطرف والإرهاب على شبكة الانترنت.

فالإعلام يلعب دوراً محورياً هاماً في مكافحة الإرهاب الإلكتروني، ودور الإعلام يجب أن ينصبَّ بالدرجة الأولى على الجوانب الإنسانية التي تهمُّ المواطنين والأفراد في الدول، ويدخل في هذا النطاق تركيز الإعلام على ضحايا الإرهاب، وفئاتهم وأعدادهم، والتركيز على الضحايا من الأطفال والنساء، حتى تكون الرسالة الإعلامية في هذا الشأن قوية وفعّالة ومؤثرة في نفوس الجمهور والمواطنين.

ونشير في هذا الصدد إلى نقطة غاية في الأهمية، وهي ضرورة إيجاد وخلق منظومة تعاون كامل ومطلق بين وسائل الإعلام وأجهزة الأمن على اختلاف مسمياتها لمواجهة الإرهاب الإلكتروني، ومن هنا يأتي دور الأجهزة الأمنية في حال رصدها لمثل هذه المواقع التي تغذي الفكر المتطرف والإرهاب، بأن تزود أجهزة الأمن وسائل الإعلام بالمعلومات المناسبة في هذا الشأن.

ومن المهم الانتباه إلى مسألة تعامل وسائل الإعلام مع العمليات الإرهابية والإنتاج الإلكتروني للمنظمات الإرهابية، فالنية الحسنة هنا لا تكفي، إذ يقوم الإعلام المعادي للإرهاب في بعض الأحيان بالترويج لهذا الإرهاب عن غير قصد عبر نقل بياناته بهدف التشهير بها. كما أن ما نعدّه نحن سلبياً ومجال انتقاد، يعدّه الإرهابيون إيجابياً ويرتاحون لترويجه من الإعلام المعادي للإرهاب، وإن كان هدف هذا الإعلام النقد، مثال ذلك انتقاد "جهاد النكاح" و"حوريات الجنة" قد يُساهم في ترويج هذه المفاهيم وتوسيع شبكة اصطياد الشباب من الإرهابيين.

لذا نؤكد في هذا المجال أن دور الإعلام يجب أن لا يقتصر على الإعلام الموجّه ضد الجماعات المتطرفة أو الإرهاب، إنما يجب أن يمتدَّ ليشمل وضع ضوابط خاصة بالتغطية الإعلامية للجماعات الإرهابية والمتطرفة، ومثل هذه الضوابط يجب أن تأخذ بعين الاعتبار وعلى سبيل المثال لا الحصر ما يلي:

1 – عدم التوسع والمبالغة في نشر البيانات والتهديدات الصادرة عن الجماعات الإرهابية من خلال شبكة الانترنت، نظراً لما يتركه ذلك من آثار سلبية في نفوس الجمهور، وما قد يتركه الخوف لديهم من اندفاع نحو تبني أفكارهم والانخراط في صفوفهم.

2 –عدم تسليم وسائل الإعلام بكل ما ينشر من الإرهابيين أو الجماعات المتطرفة على المواقع الإلكترونية، وعدم عدّها مصدراً من مصادر الإعلام الموثوقة.

3 – تركيز الإعلام على ضحايا الإرهاب من الأطفال والنساء وكبار السن، والآثار السلبية التي يتركها مثل هذا الأمر على أسر الضحايا.

4 –إبراز دور الأجهزة الأمنية في مكافحة الإرهاب الإلكتروني والتصدي له، وبشكل يولّد لدى الجمهور ثقة أكبر في قدرة أجهزة الأمن للتصدي للإرهاب الإلكتروني، وتعزيز فكرة أن أجهزة الأمن هي الحصن المنيع الذي يجب مساندته للقضاء على

هذا النوع من الجرائم.

5 –التركيز في الوقاية من الإرهاب لدى المؤسسات الإعلامية والأمنية على آراء مختصين واستشاريين في العلوم ذات الصلة، كعلم النفس الاجتماعي والسياسي وعلم الاجتماع السياسي (سوسيوبوليتيك) وعلم الاجتماع الثقافي والباحثين الدينيين الموضوعيين.

6 – تعزيز الثقة بين المواطن وأجهزة الأمن، عبر إلتزام هذه الأجهزة بالدقة في عملها وعدم اللجوء إلى مجرد الشك أو التقارير الكيدية بحق المواطنين، وأن تقوم القيادات الأمنية على مختلف المستويات بمراقبة سلوك عناصر الأمن والشرطة وغيرهم من الفعاليات المختصة في تعاملهم مع المواطنين.

7 – تعظيم دور المواطن في التصدي لجرائم الإرهاب الإلكتروني، وخلق الشعور لدى الجمهور بأن هذا الدور لا يقلُّ أهمية عن دور باقي أجهزة الدولة، بل إن الدور الذي يلعبه المواطن يفوق في أهميته باقي الأدوار، لأن المواطن من أهم الفئات المستهدفة بالإرهاب الإلكتروني، والذي تسعى الجماعات الإرهابية أو المتطرفة من وراء استخدام الانترنت إلى استدراجه وتجنيده لخدمة مصالحها وأهدافها.

ب ـ أساليب العلاج من الإرهاب الإلكتروني [24]:

من الضرورة أن تكون هناك بيئة تشريعية تعالج هذا النوع من الجرائم، فما لم يكن هناك غطاء تشريعي أو نص قانوني يجرّم هذا النوع من الأفعال لا يمكن الحديث عن آليات التحقيق في جرائم الإرهاب الإلكتروني، فالتحقيق من حيث الأصل يهدف إلى كشف ملابسات وحيثيات جريمة مرتكبة، فإذا كان الفعل الذي ينطبق عليه وصف الإرهاب الإلكتروني غير مجرّم فإنه لا مجال للحديث عن التحقيق في هذا النوع من الأفعال.

إن إجراءات التحقيق في جرائم الإرهاب الإلكتروني لا تختلف كثيراً عن إجراءات التحقيق في الجرائم الأخرى، من حيث

24 – د.أسماء الحسين، أسباب الإرهاب والعنف والتطرف دراسة تحليلية، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الجزء الثالث، الطبعة الأولى، (الرياض: جامعة الإمام محمد بن سعود الإسلامية، 1425هـ – 2004م).

الإجراءات القانونية الشكلية والتقنيات المستخدمة في كشف الجرائم وجمع أدلتها، إلا أن التعقيدات التي ترافق جرائم الإرهاب الإلكتروني وصعوبة إثباتها وجمع أدلتها، يجعل من التحقيق في هذا النوع من الجرائم صعباً، ويلقي على كاهل فرق التحقيق أعباءاً كبيرة، فجرائم الإرهاب الإلكتروني لا تنتهي بمجرد إلقاء القبض على الجاني أو الجناة، بل يبقى خطر هذه الجرائم قائماً حتى بعد اكتشافها وإلقاء القبض على فاعليها لوجود عناصر أخرى لم يتمّ إلقاء القبض عليها، إذ تبدأ تلك العناصر بالتحرك لطمس وإخفاء وتدمير الحقائق التي من شأنها أن تدين الجناة من رفقائهم الذين تمَّ إلقاء القبض عليهم، ناهيك عن الدور الذي يمكن أن تقوم به تلك الجماعات للتأثير في مجريات التحقيق من خلال اختلاق أدلة مصطنعة تقود التحقيق في اتجاه معين، أو تهديد المحققين أو الشهود.

ولا بدَّ هنا من التركيز على الأمور الأساسيَّة التالية:

1 ــ إيجاد وتجهيز وإعداد فرق متخصصة للتحقيق في هذا النوع من الجرائم، وتأهيلهم وتدريبهم على الوسائل الحديثة للتحقيق في جرائم الإرهاب الإلكتروني.

2 ــ مراجعة التكتيكات والتدريبات المعتمدة لمكافحة الإرهاب بشكل دوري، وتعديل ما يلزم لكي تتناسب و متطلبات مكافحة التهديدات الإرهابية المستقبلية على الساحة العالمية.

3 ــ ينبغي على الأجهزة الأمنية أن تفرض رقابة صارمة على الجناة المدانين في جرائم الإرهاب الإلكتروني خلال مدة وجودهم داخل السجون.

4 ــ تطبيق مبدأ العزل والفصل، وذلك بعزل المحكومين في هذا النوع من الجرائم عن غيرهم من المحكومين لتجنب خطورة التأثير في غيرهم من السجناء.

5 ــ زرع المصادر داخل السجون وخصوصاً في المهاجع التي يوجد فيها المحكومون في قضايا الإرهاب الإلكتروني، ورصد زوار المحكومين في جرائم الإرهاب الإلكتروني ومتابعتهم

ومراقبتهم.

6ــ تطبيق برامج إصلاح وتأهيل خاصة بالمحكومين في هذا النوع من الجرائم، بحيث تهدف هذه البرامج إلى إعادة تأهيل النزيل ومحاولة الاستفادة منه وتجنيده لحساب الدولة، وبالتالي يكون مصدراً هاماً من مصادر جمع المعلومات عن الجماعات الإرهابية أو المتطرفة.

المبحث الرابع: إستراتيجيَّة السعوديَّة في مواجهة الإرهاب الإلكتروني

إنَّ حكومة المملكة العربية السعودية تولي اهتماماً كبيراً بتطوير وتعزيز أنظمة الحماية ومكافحة الإرهاب الإلكتروني، عبر منظومة متطورة للقيادة والسيطرة والأمن السيبراني، بهدف حماية البنية الحيوية للقطاعات الاقتصادية الاستراتيجية، إلى جانب كبرى المنشآت الصناعية في المملكة. وأن حماية البنية التحتية الحيوية أضحت من أولويات الحكومات والشركات في العالم، وإحدى مقوّمات الاستقرار والاستدامة الاقتصادية، في ظل تصاعد عمليات القرصنة والاختراقات الإلكترونية والإرهاب السيبراني.

أوَّلاً: ضوابط مواجهة السعوديَّة الإرهاب الإلكتروني

لقد صدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصَّت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح، كقرار مجلس الوزراء رقم (163) في 24 10 1995ـ الذي ينصُّ على إصدار الضوابط المنظمة لإستخدام شبكة الإنترنت والاشتراك فيها، ومن ذلك [25]:

1 – الإمتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الإنترنت، أو إلى أي معلومات خاصة، أو مصادر معلومات دون الحصول على موافقة المالكين، أو من يتمتعون بحقوق الملكية لتلك الأنظمة والمعلومات

25 – عبد الرحمن بن عبد الله السند ، وسائل الإرهاب الإلـكـتروني وحكمها في الإسلام وطرق مكافحتها من الموقع : http://shamela.ws/browse.php/book-1244/page-20

أو المصادر.

2 – الإمتناع عن إرسال أو استقبال معلومات مشفَّرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية.

3 – الإمتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح.

4 – الإمتناع عن إشراك الآخرين في حسابات الاستخدام، أو إطلاعهم على الرقم السري للمستخدم.

5 – الإلتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.

6 – الإمتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها.

7 – الإمتناع عن الاستخدام المكثّف للشبكة بما يشغلها دوماً، ويمنع الآخرين من الاستفادة من خدماتها.

8 – الإلتزام بما تصدره وحدة خدمات (الإنترنت) بمدينة الملك عبد العزيز للعلوم والتقنية من ضوابط وسياسات لاستخدام الشبكة.

9 – نصَّ القرار على تكوين لجنة دائمة برئاسة وزارة الداخلية وعضوية وزارات: الدفاع، والمالية، والثقافة والإعلام، والاتصالات وتقنية المعلومات، والتجارة، والشؤون الإسلامية، والتخطيط، والتعليم العالي، والتربية والتعليم، ورئاسة الاستخبارات، ومدينة الملك عبد العزيز للعلوم والتقنية، وذلك لمناقشة ما يتعلق بمجال ضبط واستخدام (الإنترنت) والتنسيق فيما يخصُّ الجهات التي يراد حجبها، ولها على الأخص ما يأتي:

أ – الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة

عبر الخط الخارجي للإنترنت والتي تتنافى و الدين الحنيف والأنظمة.

ب- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية.

وهذا القرار يبيّن مبادرة المملكة العربية السعودية وسعيها لتنظيم التعاملات الإلكترونية وضبطها.

ولقد بدأت المملكة العربية السعودية في عقد دورات تدريبية، هي الأولى من نوعها حول موضوع مكافحة جرائم الحاسب الآلي بمشاركة مختصين دوليين، وتقدر تكلفة جرائم الحاسب الآلي في منطقة الشرق الأوسط بحوالي 600 مليون دولار، 25% من هذه الجرائم تعرض لها أفراد ومؤسسات من السعودية خلال عام 2000م فقط، وفيما تعمل لجنة سعودية حكومية مكوَّنة من وكلاء الوزارات المعنية بهذا الموضوع على الانتهاء من إنجاز مشروع نظام التجارة الإلكترونية، فهي مكلفة أيضاً بوضع النظم والبيانات، وتقييم البنية التحتية، وجميع العناصر المتعلقة بالتعاملات الإلكترونية، وتأتي هذه الاستعدادات للحدّ من انتشار هذا النوع من الجريمة محليًّا بعد فتح باب التجارة الإلكترونية فيها، خاصة أن العالم يعاني من انتشارها بشكل واسع بعد أن تطوَّرت بشكل لافت للنظر فيما يخصُّ ماهية هذا النوع من الجرائم، ومرتكبيها، وأنواعها ووسائل مكافحتها، إلى جانب الأحكام والأنظمة التي تحدُّ من ارتكابها [26].

26 - عمر الزبيدي، السعودية تعقد دورات لمكافحة جرائم الكمبيوتر بعد خسائر تقدر بأكثر من 150 مليون دولار لحقت بمؤسساتها الوطنية، جريدة الشرق الأوسط، العدد: 8196، يوم الاثنين 7/5/2001.

وتهدف الإجراءات في المملكة العربية السعودية إلى تنمية معارف ومهارات المشاركين في مجال مكافحة الجرائم التي ترتكب عن طريق الكمبيوتر، أو عبر شبكة الحاسب الآلي، وتحديد أنواعها ومدلولاتها الأمنية، وكيفية ارتكابها، وتطبيق الإجراءات الفنية لأمن المعلومات في البرمجيات وأمن الاتصالات في شبكات الحاسب الآلي، والإجراءات الإدارية لأمن استخدام المعلومات، ويرتكبُ هذا النوعُ من الجرائم بوساطة عدّة فئات مختلفة، ولعلَّ الفئة الأخطر من مرتكبي هذا النوع من الجرائم هي فئة الجريمة

المنظمة التي يستخدم أفرادها الحاسب الآلي لأغراض السرقة أو السطو على المصارف والمنشآت التجارية، بما في ذلك سرقة أرقام البطاقات الائتمانية والأرقام السرية ونشرها أحياناً على شبكة الإنترنت، كما تستخدم هذه الفئة الحاسب الآلي لإدارة أعمالها غير المشروعة كالقمار والمخدرات وغسيل الأموال، وعلى رغم تنوع الفئات التي ترتكب هذه النوعية من الجرائم إلا أن الطرق المستخدمة في الجريمة تتشابه في أحيان كثيرة [27].

27 – عبد الله بن شرف الغامدي: المملكة مهتمة بتطوير أنظمة الحماية ومكافحة الإرهاب الإلكتروني، المؤتمر العالمي لحلول القيادة والسيطرة، جامعة الملك سعود ووزارة الدفاع ومركز القيادة والسيطرة ومركز التميز لأمن المعلومات في الجامعة، الرياض، 12 أكتوبر 2017.

ولذلك فإن أجهزة الأمن بحاجة إلى الكثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر، خاصة في مسرح الجريمة، حتى يكون رجل التحقيق قادراً على التعامل مع الأدوات الإلكترونية من أجهزة وبرامج.

وكما ذكرنا سابقاً يجري العمل في المملكة العربية السعودية لإصدار عدد من الأنظمة التي تضبط التعاملات الإلكترونية وتُجرّم الاعتداء والعدوان الإلكتروني.

ثانياً: الإستراتيجيَّة الوطنيَّة للأمن السيبراني السعودي

يعمل المركز الوطني السعودي للأمن الإلكتروني ضمن استراتيجية قائمة على التعاون والتنسيق مع القطاعات الحكومية والمنشآت الحيوية بالمملكة كشركاء مُهمين في تحقيق أهداف الأمن الإلكتروني بالمملكة.

يعمل المركز الوطني السعودي للأمن الإلكتروني ضمن استراتيجية قائمة على التعاون والتنسيق مع القطاعات الحكومية والمنشآت الحيوية بالمملكة كشركاء مُهمين في تحقيق أهداف الأمن الإلكتروني بالمملكة.

سيشكل المركز النقطة المحورية لتنسيق الجهود الوطنية في تحديد ومراقبة المخاطر الإلكترونية، وتقديم الإرشادات والتوصيات اللازمة لحماية شبكات الاتصالات وأنظمة المعلومات الوطنية، ومشاركة البيانات المتعلقة بالتهديدات، وتنسيق عمليات الاستجابة والمعالجة للحوادث الإلكترونية.

أهداف الإستراتيجيَّة الوطنيَّة السعوديَّة للأمن السيبراني[28]

تَهدُف الهيأةُ الوطنيةُ إلى تعزيز حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة

28 – د.صالح بن ابراهيم المطيري، المركز الوطني للأمن الالكتروني السعودي، المؤتمر العالمي للحلول القيادة والسيطرة، بناء القدرات المحلية، مركز التميز للامن والمعلومات، جامعة الملك سعود، السعودية.

وبرمجيات، وما تقدّمه من خدمات، وما تحتويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، ومستهدفة التأسيس لصناعة وطنية في مجال الأمن السيبراني تُحقّقُ للمملكة الريادةَ في هذا المجال انطلاقاً مما تضمنته رؤية المملكة العربية السعودية 2030. وتتلخص الأهداف فيما يلي:

- تعزيز الأمن السيبراني للدولة.
- حماية مصالح المملكة الحيوية.
- حماية أمن المملكة الوطني.
- حماية البنى التحتية الحساسة في المملكة.

فتُعدُّ الأهدافُ الإستراتيجيَّة بمثابة الأداة لتنفيذ رؤية ورسالة المركز الوطني للأمن الالكتروني، وهي كالآتي [29]:

29 - - زياد جيوسي، الهيئة الوطنية للأمن السيبراني الأمثل لحماية الأمن الشخصي، المؤتمر، الخامس لأمن وسلامة المعلومات في الفضاء السيبراني، https://carjj.org/

1. تمكين الجهات الحكومية والمنشآت الحيوية من الاستعداد بشكل أفضل للحماية من الهجمات الالكترونية. من خلال مساعدة الجهات الحكومية والمنشآت الحيوية للاستعداد بشكل أفضل للحماية من الهجمات الالكترونية و التصدي لها على المستوى الوطني.
- تمكين الجهات الحكومية و المنشآت الحيوية على الحصول على معلومات استباقية للتصدي للهجمات.

- تزويد الجهات الحكومية والمنشآت الحيوية بقدرات عملية وفعّالة للمراقبة الالكترونية.

- تعزيز التواصل و التعاون في حماية الفضاء الإلكتروني بين الجهات الحكومية والمنشآت الحيوية.

2. تعزيز الوضع العام للفضاء الإلكتروني، من خلال العمل على تعزيز فهم مخاطر الأمن الالكتروني وإيضاح آلية التعامل مع الحوادث الالكترونية،

- تفعيل أفضل الممارسات العالمية في الفضاء الإلكتروني في المملكة

العربية السعودية.

– زيادة الوعي العام حول مخاطر الفضاء الالكتروني.

3. بناء وتعزيز قدرات المركز الداخلية، بناء القدرات الداخلية لتعزيز دور المركز للقيام بالمسؤوليات المناطة به بشكل عملي وفعّال:

– تطوير وإدارة المركز وفقا للمبادرات التنفيذية والتوجّه الاستراتيجي للمركز.

– تحديد و إدارة المتطلبات التشغيلية للمركز.
– تسخير موارد المركز لتطوير و تحسين أداء العمل.

الخدمات الرئيسة للمركز الوطني للأمن الإلكتروني:
1. توكيد المعلومات والجاهزية، مراجعة البنية المعمارية لأمن المعلومات. قياس مستوى النضوج الأمني. تطوير وإدارة المعايير الأمنية. إدارة المخاطر.

2. مشاركة المعلومات الأمنية الاستباقية، جمع المعلومات الأمنية وتحليلها (Threat Intelligence)، نشر النتائج (التحذيرات) للقطاعات الحكومية والمنشآت الحيوية.

3. عمليات الدراية الأمنية، المراقبة و الاستنتاج، رصد وتقييم الهجمات الالكترونية.

4. الإستجابة للحوادث والاستشارات التقنية، التحقيق الرقمي للحوادث الالكترونية ومعالجتها، تحليل الأدلة الجنائية الرقمية.

تحديات الحماية من الهجمات الإلكترونية
– صعوبة الوثوق بأنظمة المعلومات وأجهزة الاتصالات
– الحماية ليست أنظمة تقنية فقط وإنما هي منظومة متكاملة (الحوكمة ،الاستراتيجيات والسياسات، والعنصر البشري).

– صعوبة تحقيق الحماية مما يتطلّب إدارة للمخاطر تراعي التوازن بين الحماية والمراقبة والإستجابة للحوادث.
ضوابط الأمن Security Controls ومنع الإختراق
– هناك عدّة أطر عامة وخاصة تحتوي على ضوابط لحماية شبكات الاتصالات وأنظمة المعلومات من الهجمات الإلكترونية .
– تلك الأطر تحتوي على قوائم طويلة من الضوابط الأمنية والتي يستلزم تطبيقها وقتاً و جهداً كبيراً .
– إستعان بعض الدول بقائمة مختصرة بأهم الضوابط الأمنية والتي تمَّ وضعها بقائمة Critical Controls بحيث: تمنع 80% أو أكثر من الاختراق ، لا يحتاج إلى وقت أو جهد كبير للتطبيق.

الخاتمة

يعدُّ الإرهاب الالكتروني تهديدا أمنيا الكترونيا، خاصة بزيادة استخدام التكنولوجيا المتطورة في مختلف المجالات ،من خلال استخدامها بشكل سلبي من طرف الجماعات الإرهابية وقيامها بهجوم واعتداء الكتروني على مختلف القطاعات الحيوية للدولة، مما ينتج عنها خسائر فادحة تمسُّ جميع الميادين خاصة الأمني منها . هذا ما يوجب على وحدات المجتمع الدولي اتّخاذ التدابير اللازمة كافة لمجابهة هذه الأخطار أو الحدّ منها .

إنٍ من أبرز ما توصلت إليه في البحث الآتي:

أولًا: إن التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة يجب أن تخضع للأحكام الشرعية المستمدة من الكِتاب والسُّنة، وفي ضوء تلك الأحكام تقوم الجهات المعنية بوَضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة، كما تقوم الهيآت القضائية والأمنية والحقوقية بتنزيل تلك الأحكام واللوائح على القضايا المختلفة، وفض النزاعات الناتجة عنها.
ثانيًا: يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، وتعليم الطرق ,والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات

وغير ذلك.

رابعاً: حجب المواقع الضارة والتي تدعو إلى الفساد والشر، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق من الأساليب المجدية والنافعة لمكافحة الإرهاب الإلكتروني.

خامساً: على الرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية والتي تعدُّ وسيلةً من وسائل مكافحة الإرهاب الإلكتروني، فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الإلتزام بتلك الأحكام لا يزال في مراحله الأولية، وما تمَّ في هذا الشأن لا يتجاوز مجموعةً من القرارات المنفصلة واللوائح الجزئية التي لا تستوعب القضايا المُستجدَّة في أعمال تقنية المعلومات كما لا توجد بصورة منظمة ومعلنة أقسام أمنية، ومحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة.

سادساً: إن أجهزة الأمن تحتاج إلى كثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر والوقاية منها، وتطوير إجراءات الكشف عن الجريمة، خاصة في مسرح الحادث، بحيث تتمكن من تقديم الدليل المقبول للجهات القضائية، وأيضاً يلزم نشر الوعي العام بجرائم الكمبيوتر، والعقوبات المترتّبة عليها، واستحداث الأجهزة الأمنية المختصة القادرة على التحقيق في جرائم الكمبيوتر، والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

سابعاً: على مستوى دول العالم ومع مواكبة التطور الهائل لتقنية المعلومات سُنَّت أنظمة لضبط التعاملات الإلكترونية، وتضمنت تلك الأنظمة عقوبات للمخالفين في التعاملات الإلكترونية ومكافحة الإرهاب الإلكتروني.