# آليات مكافحة الإرهاب الالكتروني في البيئة العربية

## تجربة المملكة العربية السعودية

# Mechanisms of combating with Digital terrorism in Arab countries Saudi Arabia experience

سلامي اسعيداني*، ليلى فقيري

[1]جامعة محمد بوضياف المسيلة (الجزائر)، salami.saidani@univ-msila.dz

[2]جامعة محمد بوضياف المسيلة (الجزائر)، leila.feguiri@univ-msila.dz

تاريخ الاستلام: 2022/12/26 تاريخ القبول: 2022/12/30 تاريخ النشر: 2023/01/20

ملخص:

يعتبر الإرهاب قديم قدم التاريخ، إلا أن الإرهاب في الوقت المعاصر اتخذ بعداً جديداً مقلقا ومثيرا، خاصة بعد انتشار تقنيات الاتصال الحديثة بصورة متسارعة، بشكل مكن الإرهابيون من تنفيذ عمليات دموية مدمرة بأقل مجهود ودون تمكن الجهات الأمنية من منعهم ابتداء أو ضبطهم بعد ذلك. وكان لظهور شبكة المعلومات (الإنترنت) دور كبير في تنفيذ الإرهابيون لعملياتهم المدمرة عبر أليات كثيرة ستكون محور مداخلتنا، فضلا عن محاربتها محليا، إقليميا ودوليا.

كلمات مفتاحية: الآلية، المكافحة، الارهاب الالكتروني، البيئة، العرب

Abstract:

Terrorism dating back to many centuries in the history, but terrorism in the contemporary time has taken on a new disturbing and terrifying dimension, especially after the rapid spread of modern communication technologies, in a way that enabled terrorists to carry out bloody and destructive operations with minimal effort and without the security authorities being able to prevent them or arrest them after that. The emergence of the information network (the Internet) had a major role in the terrorists' implementation of their destructive operations through many mechanisms that will be the focus of our paper, as well as the fight and measures against them locally, regionally and internationally.

Keywords: Mechanism, Anti-terrorism, Digital terrorism, Arab's environment.

*المؤلف المرسل

**1-مقدمة:**

تعد ازمة الإرهاب في وقتنا الحالي من بين أهم الأزمات التي جميع الدول ويتخوف منه الأفراد. حتى أصبح جزءاً من رؤى الدول المستقبلية، ولا يكاد يمر شهر دون أن تقع عملية إرهابية في مكان ما من العالم، وأصبحت أنباء وأخبار الإرهاب تحتل الصدارة في وسائل الإعلام ومنصات الاتصال الرقمية، وتحظى بجذب انتباه المشاهدين والمتابعين، على اختلاف مستوياتهم الثقافية وميولهم السياسية ومواقع وجودهم على ظهر الأرض.

وللوقوف على هذه حيثيات هذه الأزمة الدولية بشكل يتناسب مع موضوع مشاركتنا، تأتي مداخلتنا لشرح الظاهرة نسبيا مع ابراز دول وجهود المملكة العربية السعودية ومؤسساتها الإقليمية والدولية في الموضوع.

## 1. الإرهاب الالكتروني: الماهية والأسباب

### 1.1 مفهوم الارهاب الالكتروني

لقد تعدت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والإيديولوجيات التي تعتنقها الدول اتجاهه.

نجد مثلا الاتفاقيات العربية لمكافحة تعرف الارهاب بأنه: كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه أو أغراضه يقع تنفيذا لمشروع اجرامي فردي أو جماعي من أجل القاء الرعب بين الناس أو ترويعهم بإيذاء أو الحاق الضرر بالبيئة أو بالمرافق العامة أو الخاصة أو تعريض الموارد الوطنية للخطر. (صابر، 2008)

بعد اطلاعنا على العشرات من التعاريف يمكن لنا ان نقف على تعريف جامع للإرهاب الارهاب الالكتروني بشكل عام بأنه: العدوان او التخويف او التهديد المادي او المعنوي الصادر من الدول أو الجماعات أو الافراد على الانسان في دينه أو نفسه أو عرضه أو ماله أو عقله بغير حق باستخدام الموارد

المعلوماتية والوسائل الالكترونية بشتى صنوف العدوان وصور الفساد. فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصالات والشبكات المعلوماتية من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

## 2.1. الإرهاب الإلكتروني: الأسباب، الخصائص والأهداف

### أ- أسباب ودوافع الإرهاب الالكتروني:

للإرهاب الإلكتروني أسباب ودوافع تختلف في درجة أهميتها حسب الاتجاهات السياسية والظروف الاقتصادية والاحوال الاجتماعية وكذلك الاختلاف الديني والعقائدي ويمكننا إيجاز أسباب ظاهرة الإرهاب فيما يأتي: (العطيات، 2012)

**أولاً: الدوافع الذاتية:**

تتعدد الدوافع الشخصية المؤدية للإرهاب، ويمكن بيان أبرزها فيما يلي:

1-افتقاد الشخص لأهمية دوره في الأسرة والمجتمع وفشله في الحياة الأسرية مما يؤدي الى اكتساب بعض الصفات السيئة ومن ضمنها عدم الشعور بالانتماء والولاء للوطن.

2-الرغبة في الظهور وحب الشهرة بحيث لا يكون الشخص مؤهلا فيبحث عما يؤهله باطلا فيشعر ولو بالعدوان والتخريب والتدمير.

3-نقمة الشخص على المجتمع الذي يعيش فيه نتيجة للظلم واهدار الحقوق.

**ثانيا: الدافع الذهنية والفكرية:**

تتنوع الدوافع الذهنية والفكرية المؤدية لظاهرة الإرهاب ويمكن بيان أهمها فيما يلي:

1- الجهل بمقاصد الشريعة الاسلامية المتمثل بالظن لا باليقين والتثبت، والفهم الخاطئ للدين، وتفسيره تفسير خاطئ، والجهل بقواعد الدين الحنيف وآدابه وسلوكه.

2- الانقسامات الفكرية المختلفة بين التيارات المتنوعة والمختلفة.

3- التطرف وهو أمر بالغ الخطورة في أي مجال من المجالات وخاصة المجالات الفكرية.

**ثالثاً: دوافع الأيديولوجية السياسية:** (محمد، 2015)

من أبرز الأسباب والدوافع الايديولوجية السياسية لظاهرة الإرهاب ما يأتي:

1- غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق العامة والتقصير في أمور الرعية.

2- معاناة بعض المجتمعات والشعوب الدولية من الظلم والاضطهاد والسيطرة الاستعمارية وسلب الأموال وخرق القوانين والمواثيق الدولية مما يدفع الشعوب الى التشدد والتطرف.

**أ- خصائص الإرهاب الإلكتروني وأهدافه**

**أولاً: خصائص الإرهاب الإلكتروني:**

يتميز الارهاب الالكتروني بعدة خصائص ومميزات منها: (العطيات، 2012)

1- الارهاب الالكتروني لا يحتاج عند ارتكابه الى العنف والقوة بل يتطلب حاسب الي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

2- يتميز الارهاب الالكتروني بانه جريمة ارهابية متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق اقليمي محدود.

3- صعوبة اكتشاف جرائم الارهاب الالكتروني ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مثل هذه الجرائم.

4- صعوبة الاثبات في الارهاب الالكتروني نظرا لسرعة غياب الدليل الرقمي وسهولة اتلافه وتدميره.

5- يتميز الارهاب الالكتروني بانه يتم بتعاون أكثر من شخص على ارتكابه.

6- مرتكب جريمة الارهاب الالكتروني يكون من ذوي الاختصاص في مجال تقنية المعلومات أو من شخص لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الحاسب الالي والشبكة المعلوماتية.

**ثانياً: أهداف الإرهاب الالكتروني:**(العطيات، 2012)

يهدف الإرهاب الإلكتروني إلى تحقيق جمله من الأهداف غير المشروعة ويمكننا بيان أبرز تلك الأهداف:

1. نشر الرعب والخوف بين الأشخاص والدول والشعوب المختلفة والإخلال بالأمن العام وزعزعة الطمأنينة

2 ـ إلحاق الضرر بالبنية التحتية المعلوماتية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة.

## 3ـ جمع الأموال اللازمة لتمويل العمليات الإرهابية

### 3.1. مظاهر الإرهاب الإلكتروني وأشكاله

#### أولا. تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب، وتبادل الأفكار والمعلومات صعباً في الواقع فإنه عن طريق الشبكات المعلوماتية تسهل هذه العملية كثيرا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين ويتبادل الحديث والاجتماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم لهم أتباعاً، وأيضاً عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الالكتروني. (Madhian، 2017)

وعلى الرغم من البريد الالكتروني (e-mail) أصبح من أكثر الوسائل استخداماً في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمناً وسرعة للإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم بل إن كثيرا من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها ويقوم الإرهابيون كذلك باحتلال البريد الالكتروني، والاستفادة منه في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الالكترونية. (Falcone، 2017)

فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة لمبادئها المنحرفة، والسيطرة على وجدان الأفراد واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة والتي تتعارض مع مصلحة المجتمع.

ويستخدم الإرهابيون الشبكة العالمية للمعلومات الانترنت بشكل يومي لنشر أفكارهم الهدامة ولتحقيق أهدافهم السيئة، ومن الممكن إبراز أهم استخداماتهم للشبكة فيما يلي: (الزين، 2015)

**أ: الاتصال والتخفي**

تستخدم الجماعات والمنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينهم نظرا لقلة تكاليف الاتصال والوسائل للاستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال للتخفي وذلك عن طريق البريد الالكتروني أو المواقع والمنتديات وغرف الحوار الالكتروني حيث وضع رسائل مشفرة تأخذ طابعاً لا يلفت الانتباه، فمن دون أن يضطر الإرهابي الإفصاح عن هويته كما أنها لا تترك أثراً واضحاً يمكن أن يدل عليه.

**ب: جمع المعلومات الإرهابية**

تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما أنها تعتبر موسوعة إلكترونية شاملة متعددة الثقافات ومتنوعة المصادر وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات ومواعيد الرحلات الجوية والمعلومات المختصة بسبل مكافحة الإرهاب؛ نظراً لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية.

**ج: التخطيط والتنسيق للعمليات الإرهابية**

العمليات الإرهابية عمل على جانب التعقيد والصعوبة فهي تحتاج الى تخطيط محكم وتنسيق شامل وتعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية حيث تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة في جو مريح، وبعيداً عن أعين الناظرين مما يسهل على الإرهابيين ترتيب تحركاتهم. (الزين، 2015)

**د: الحصول على التمويل**

من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية من خلال الاستفسارات والاستطلاعات

الموجودة على المواقع الالكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثم استجداؤهم بدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة رسائل البريد الالكتروني أو من خلال مساحات الحوار الالكترونية بطريقة ذكية وأسلوب مخادع بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية.

**هـ: التعبئة وتجنيد الإرهابيين**

تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها، وبث الأفكار والفلسفات التي تنادي بهم كما تسعى جاهدة الى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لدا من لديهم ميول واستعداد للانخراط في الأعمال التدميرية والتخريبية مما يوفر لديها قاعدة ممن تجمعهم نفس الأفكار والتوجهات فيسهل تجنيدهم لتنفيذ عمليات إرهابية في المستقبل. (الزين، 2015)

إن استقدام عناصر جديدة داخل التنظيمات الإرهابية يحافظ على بقائها واستمرارها لذا فإن الإرهابيين يقومون باستغلال تعاطف بعض أفراد المجتمع مع قضاياهم، فيجتذبونهم بأسلوب عاطفي وعبارات حماسية براقة، وذلك من خلال غرف الحوار والمنتديات والمواقع الالكترونية.

**و: التدريب الإرهابي الالكتروني**

تحتاج العمليات الإرهابية الى تدريب خاص ويعد التدريب من أهم هواجس التنظيمات الإرهابية وقد أنشئت معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام لكن مشكلة معسكرات التدريب الإرهابية أنها دائماً معرضة للخطر ويمكن اكتشافها ومداهمتها في أي وقت لذا فان الشبكة المعلوماتية بما تحتوه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب والتخطيط والتنفيذ كما قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل الى الإرهابيين في مختلف أنحاء العالم وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة. (العطيات، 2012)

**ي: إصدار البيانات الالكترونية**

تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة وذلك عن طريق المواقع الالكترونية أو بواسطة رسائل البريد الالكتروني أو من خلال منتديات الحوار وساحاته وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات ووصولها الى مختلف شرائح المجتمع

وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية اتجاهات متنوعة فتارة ترسم أهدافاً وخططاً عامة للتنظيم الإرهابي، وأحيانا تكون للتهديد والوعيد لشن هجمات إرهابية معينة في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار وتصريحات صادرة من جهات أخرى. (صابر، 2008)

**ثانيا. إنشاء المواقع الإرهابية الإلكترونية**

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات الانترنت لبث أفكارهم الضالة والدعوة الى مبادئهم المنحرفة ولإبراز قوة التنظيم الإرهابي، وللتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الالكتروني، وللتدريب الالكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد أنشات مواقع إرهابية الكترونية لبيان كيفية صناعة القنابل والمتفجرات والأسلحة الكيماوية الفتاكة ولشرح طرق اختراق البريد الالكتروني وكيفية اختراق وتدمير المواقع الالكترونية والدخول الى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات ونحو ذلك. (عياشي، 2006)

والموقع عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل ( hyber text mark up language html) ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العالمية (www browser) ويقوم بحل رموز (html) وإصدار التعليمات لإظهار الصفحات المكتوبة وإذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا بالنسبة للإرهابيين فان إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات الانترنت، لخدمة أهدافهم وترويج

أفكارهم الضالة أصبح سهلا وممكناً، ولذا فإن معظم التنظيمات الإرهابية لها مواقع الكترونية وهي بمثابة المقر الافتراضي لها. (Madhian، 2017)

ومن الأمثلة على بعض المواقع الالكترونية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية ما يأتي:

1- موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001، ومن خلاله تصدر البيانات الإعلامية للقاعدة.

2- ذروة السنام: وهي صحيفة الكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

3- صوت الجهاد: وهي مجلة نصف شهرية يصدرها ما يسمى تنظيم القاعدة في جزيرة العرب، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.

4- البتار: وهي مجلة عسكرية إلكترونية متخصصة تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد.

**ثالثا. الهجمات الممنهجة للإرهاب الالكتروني في عصر المعلومات:**

يمكن تقسيمها إلى ما يأتي: (Falcone، 2017)

**1- استهداف النظم العسكرية:**

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات ويعد هذا السيناريو من أخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، وتبدأ المرحلة الأولى من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي والصواريخ النووية.

**2- استهداف محطات توليد الطاقة والماء:**

أصبح الاعتماد على شبكات المعلومات وخصوصا في الدول المتقدمة من الوسائل المهمة لإدارة نظم الطاقة الكهربائية ويمكن للهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطيرة، وخصوصاً في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية فإن شبكات المعلومات المرتبطة

بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الالكتروني. (صابر، 2008)

**3- استهداف البنية التحتية الاقتصادية**

أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال مما يجعل هذه الشبكات نظرا لطبيعتها المترابطة وانفتاحها على العالم هدفاً مغرياً للمجرمين والإرهابيين، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالانطباعات السائدة والتوقعات والتشكيك في صحة هذه المعلومات، أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة وإضعاف الثقة في النظام الاقتصادي.

**4- استهداف نظم المواصلات**

ويتضمن هذا السيناريو اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج هبوط الطائرات وإقلاعها؛ مما قد ينجم عنه حصول تصادم فيما بينها، أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات، كما يحتمل تمكن قراصنة المعلومات من السيطرة على نظم التحكم بتسيير القطارات، وتغيير مواعيد الانطلاق بحيث تسود الفوضى أو تتصادم هذه القطارات فيما بينها وكذا بالنسبة للسفن والناقلات والغواصات البحرية. (Falcone، 2017)

**5- استهداف نظم الاتصالات**

ويشمل هذا السيناريو اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية وقد تمارس سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الإتصال بين أفراد المجتمع، ومؤسساته الحيوية الأمر الذي ينشر حالة من الرعب والفوضى، وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية، ولا يتوقف الأمر عند هذا الحد فقط بل هناك العديد من الأهداف الأخرى التي يمكن للمجرمين والإرهابيين المتمكنين من خلالها أن يشيعوا الفساد، وينشروا الفوضى فهناك على سبيل المثال شبكات المعلومات الطبية والتي يمكن من خلال مهاجمتها واختراقها، ومن ثم التلاعب بها حصول خسائر بشرية، ومن أمثلة ذلك في العالم الغربي ما قام به أحد المجرمين من الدخول

إلى سجلات المستشفيات والتلاعب بملفات المرضى بشكل أدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم، وما إلى ذلك يمكن لها أن تحدث آثاراً مدمرة على الصعيد الاجتماعي.

**رابعا. التهديد والترويع الالكتروني**

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ومن خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرقه؛ وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب محاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي لإبراز قوة التنظيم الإرهابية من ناحية أخرى. (محمد، 2015)

وقد يلجأ إرهابي (الإرهاب الالكتروني) إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية؛ بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الالكتروني إرسال الوسائل الالكترونية المتضمنة للتهديد (e-mails) وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية.

ولقد تعددت الأساليب الإرهابية في التهديد فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية ونحو ذلك.

**خامسا. التجسس الالكتروني**

يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الالكتروني بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والأنظمة الالكترونية التي جلبتها حضارة التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية وهي: التجسس العسكري والتجسس السياسي والتجسس الاقتصادي. (عياشي، 2006)

وفي عصر المعلومات ومع وجود وسائل التقنية الحديثة فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي، وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الالكترونية خاصة مع ظهور الشبكات المعلوماتية وانتشارها عالمياً، ومع توسع التجارة الالكترونية عبر الشبكة العالمية للمعلومات تحولت مصادر المعلومات التجارية إلى أهداف للتجسس الاقتصادي. (Madhian، 2017)

إن محاولة اختراق الشبكات والمعلومات والمواقع الالكترونية من قبل العابثين من مخترقي الأنظمة المعلوماتية (hackers) لا يعد إرهاباً، فمخاطر هؤلاء محدودة وتقتصر غالباً على العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع آمن، ويكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الإرهابية، وأجهزة الاستخبارات المختلفة من أجل الحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدول أخرى معادية، أو استغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة.

وتتجلى الخطورة في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية، ولا يمكن حتماً الاعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية، فهي ليست آمنة، ولا يمكن الاطمئنان لها تماماً. (Elnaim، 2013)

وتجدر الإشارة إلى أن الطرق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية؛ نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياحية والاقتصادية وهذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من اجل الإضرار بمصلحة المجتمع والوطن.

## 2. جهود المملكة العربية السعودية في مكافحة جريمة الإرهاب الإلكتروني

### 1.2. الهجمات الإرهابية الإلكترونية التي تعرضت لها المملكة العربية السعودية

يمكن التعرف على جهود المملكة العربية السعودية في مكافحة هذه الجريمة من خلال عرض لأبرز الهجمات التي تعرضت لها المملكة والسياسات التي اتخذتها لمكافحة هذه الجريمة وفقًا لما يلي:

أولا. تتمثل الهجمات الإلكترونية التخريبيَّة التي تهدد المملكة العربية السعوديّة في القرصنة، ونشر الفيروسات، وهجمات تعطيل الخدمات، ومع أن القراصنة قد يصلون إلى الكمبيوترات لعرض أو نسخ أو إدخال بيانات من دون إحداث ضرر كبير، فإن ناشري الفيروسات يفسدون عمدًا بيانات الكمبيوترات لإحداث أضرار اقتصاديَّة. من ناحية أخرى فإن هجمات معطِّلي الخدمات تجعل الكمبيوترات أو موارد الشبكات غير صالحة للاستخدام من قِبَل مستخدميها أو عملائها المعنيين. حدثت مثل هذه الهجمات التخريبية الإلكترونيَّة في المملكة العربية السعوديّة بشكلٍ متكرر وقد كلَّفتها حوالي 2.6 مليار ريال سعوديٍّ عام 2012، وفقًا لتقرير أصدرته شركة سيمانتك Symantec، وفيما يلي عرض لأبرز هذه الهجمات: (Elnaim، 2013)

ثانيا. عام 2016 واجهت السعودية موجة من الهجمات الإلكترونيّة التي أصابت هيئات حكوميّة وشركات قطاع خاص، وقد استخدمت هذه الهجمات برامج ضارة شبيهة بالبرامج المستخدمة في هجوم عام 2012 على شركة أرامكو السعوديّة، وتسببت في اضطراب واسع في البنى التحتيّة المهمّة. أثناء المؤتمر الدولي السنويِّ الثاني للأمن الإلكتروني بالرياض والذي انعقد في فبراير 2017، صرح المدير العام للمركز الوطنيِّ السعوديِّ للأمن الإلكتروني صالح إبراهيم المطيري بأن المملكة قد تعرضت لحوالي 100 هجوم إلكتروني أمنيٍّ يستهدف بنى تحتيّة مهمة، في محاولات لسرقة البيانات، وسببت انقطاعًا في الخدمات، خلال عام 2016، ومن بين تلك الهجمات، تم الإبلاغ عن هجوم إلكتروني على هيئة الطيران السعودية باستخدام برمجيات إزالة البيانات، ومن بين تلك البرامج الضارة قرص إزالة البيانات حصان طروادة شامون Shamoon الذي يعتبر أحد الفيروسات الحاسوبية المعقدة، والتي تم استخدامها ضد منظمات متعددة في المملكة العربية السعودية وخاصة في قطاع النفط.

ثالثا. في نهاية مايو 2015 تمكن أحد قراصنة الإنترنت من الهجوم على شبكات الجامعات السعودية وقام بسرقة العديد من المعلومات منها، متضمنة في ذلك التفاصيل الشخصية، والنتائج الأكاديمية بما يقرب من 4000 طالب جامعي.

رابعا. في أغسطس 2015 قام فريق سايبر أوف إيموشن، بقرصنة أكثر من 24 موقعًا حكوميًّا سعوديًّا على الإنترنت لفترة وجيزة.

خامسا. في يوليو 2015 هاجمت الدولة الإسلاميّة شبكة كمبيوتر حكومية ونشرت قائمة تحوي بيانات موظفين، منها أسماؤهم وأرقام هواتفهم وعناوين البريد الإلكتروني خاصتهم.

سادسا. في مايو 2013 قام الجيش الإلكتروني السوريّ بقرصنة عدة مواقع حكومية سعودية على الإنترنت في سلسلة من الهجمات الشبكيّة الكثيفة، ومن بين تلك الهجمات تعرضت الحواسيب الخاصة بالشرطة الوطنية إلى هجوم أدى إلى تعطيل العديد من طلبات الخدمة. (نرمين، 2018)

سابعا. الهجوم الإلكتروني على شركة أرامكو للبترول، وفيه أصيب أكثر من 30 ألف كمبيوتر في شركة البترول السعودية أرامكو بفيروس مدمِّر في شهر أغسطس عام 2012. دمّر الهجوم بيانات ومسح أقراصًا صلبة في أجهزة الكمبيوتر، ويعتقد أنه كان يهدف لوقف إنتاج البترول، وتحملت السعودية تكلفة إصلاح الضرر. (Falcone، 2017)

ثامنا. تعرض الموقع الرسمي لجامعة الملك سعود في عام 2012 للقرصنة على يد قرصان مجهول تم فيه قرصنة قاعدة بيانات تحوي 812 مستخدمًا، وقد تضمنت تلك البيانات أرقام الهواتف المحمولة، والعناوين، وكلمات المرور، وتم الإفصاح عنها باستخدام موقع مشاركة الملفات. (Kumar، 2012)

تاسعا. الهجوم الإلكتروني على وزارة الخارجية السعودية، والذي ترتب عليه تسريب عدد من الوثائق المهمة لعملاء دبلوماسيين في العديد من البلدان، وأكدت العديد من الدراسات أن ذلك التسريب كان الهدف الأساسي منه هو إدانة السياسة الخارجية السعودية، وذلك على الرغم من أن كافة المعلومات التي تم تسريبها لم تكن خارجة عن السياسة المعلنة لوزارة الخارجية، إلا أن المشكلة الرئيسة قد تمثلت في أن بعض المعلومات قد تم التلاعب به لتشويه الحقيقة وتم نشرها على الكثير من مواقع الشبكات الاجتماعية. (نرمين، 2018)

عاشرا. في يونية 2010 تعرض الموقع الخاص ببنك الرياض بالمملكة العربية السعودية لهجوم من جانب أحد قراصنة الإنترنت.

### 2.2. السياسات السعودية في مكافحة جريمة الإرهاب الإلكتروني:

للتصدي للهجمات الإلكترونية التي تتعرض لها المملكة العربية السعودية، والتي تمس كيانها وأمنها الوطني، اتخذت الحكومة العديد من الإجراءات والآليات، والتي يمكن تناولها كالآتي:

أولا. الجهود القانونية:

لمكافحة أي جريمة من الجرائم لابد أن يكون هناك بنية قانونية عقابية تحكمها، وأن يكون هناك جهة قضائية تطبق الجزاء على من يقوم بارتكابها، وهو ما تم في مكافحة جريمة الإرهاب الإلكتروني في السعودية، فعلى الرغم من أن المملكة تعتمد على القوانين الشرعية والتي تستند أصولها من كتاب الله والسنة النبوية، فإنها قد تمكَّنت من إصدار قانون خاص بمكافحة الجرائم الإلكترونية، وانضمت إلى الاتفاقية العربية الخاصة بمكافحة هذه الجريمة.

ثانيا. نظام مكافحة الجرائم المعلوماتية: تم إصدار القانون بموجب المرسوم الملكي رقم 17M بتاريخ السادس والعشرين من شهر مارس لعام 2007، ويتألف من 16 مادة؛ تشمل المادة الأولى بعض التعريفات الرئيسة، وتوضح المادة الثانية الهدف من القانون، وتضمن المواد من 3- 13 الجرائم والعقوبات، وتبين المادتين 14 – 15 دور الهيئات المختصة، أما المادة 16، فقد أوضحت تاريخ دخول القانون حيز النفاذ وقد حددته في مائة وعشرين يومًا من تاريخ نشره. وفيما يلي أبرز العقوبات الواردة في القانون. (المعلومات، 2007)

**ثالثا. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:**

تمت الموافقة على انضمام مصر للاتفاقية العربية لمكافحة جرائم تقنية المعلومات وقد انضمت المملكة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات في سبيل تعزيز التعاون بين الدول العربية لمكافحة جريمة الإرهاب الإلكتروني، علاوة على اقتناعها بضرورة "تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات."

**ثانيا . الجهود التنفيذية:**

- وزارة الاتصالات والمعلومات السعودية:

هي الوزارة المسئولة عن جميع وسائل الاتصال وتقنية المعلومة في المملكة العربية السعودية، وهي الجهة المخولة لها اقتراح مشاريع الأنظمة المتعلقة بالاتصالات وتقنية المعلومات ورفعها إلى مجلس الوزراء، وقد قامت الوزارة بإصدار العديد من القرارات المنظمة للتعاملات الإلكترونية منها: القرار رقم 7/ب/ 33181 بتاريخ 2003، المتضمن وضع خطة لتقديم الخدمات والمعاملات الحكومية، والقرار رقم 8189 م/ب/لعام 2005، الخاص بتشكيل لجنة داخل كل جهة حكومية للتعاملات الإلكترونية. (نرمين، 2018)

أسهمت الوزارة بصورة كبيرة في الجهود التي تبذلها الدولة لمكافحة جريمة الإرهاب الإلكتروني، من خلال اقتراحها للاستراتيجية الوطنية لأمن المعلومات الخاصة بالمملكة العربية السعودية في عام 2011.

تكونت الاستراتيجية من 90 صفحة، توضح رؤية واضحة للمملكة العربية السعودية، تنص على أن هدفها توفير بيئة رقمية آمنة وقوية، ويمكن القول بأن للاستراتيجية خمسة أهداف رئيسة هي: (Hathaway، 2017)

1. تطوير بنية تحتية لتكنولوجيا المعلومات آمنة ومرنة وموثوق فيها.
2. توفير موارد بشرية قادرة على تحقيق الأمن المعلوماتي بأعلى درجاته.
3. تهيئة بيئة لأمن المعلومات ملهمة قائمة على الثقة والشفافية والتعاون.
4. دعم خدمات الحكومة الإلكترونية ودعم البنية التحتية للمملكة من أجل الإيفاء بأهداف الأمن
5. تعزيز النمو الاقتصادي من خلال البحث والتطوير.

**-وزارة الداخلية:**

تعتبر وزارة الداخلية هي الوزارة المسئولة عن مراقبة شئون الأمن الداخلي، وفي هذا الصدد تسعى الوزارة إلى التصدي للجرائم الإلكترونية، وتقوم بعمل اجتماعات لبحث استعداداتها لمباشرة استقبال بلاغات الجرائم الإلكترونية، وأسلوب تحريز الأدلة الرقمية، وتحديد هوية المجرمين الرقميين، ومراقبة الإنترنت للأغراض الجنائية، ومن بين حالات الإرهاب الإلكتروني التي تصدت لها الوزارة. (نرمين، 2018)

**– خاتمة:**

ختاما، نعتقد أن الإرهاب أضحى ظاهرة عالمية حيث قامت المنظمات والجماعات الإرهابية لخطورتها الإجرامية بتوظيف طاقتها للاستفادة من الطبيعة الاتصالية لشبكه المعلومات في عملياتها الإرهابية وذلك من خلال بث أهدافها ومعتقداتها، والقيام ببعض الممارسات التي تهدد أمن الدول باستخدام وسائل التواصل الاجتماعي والتكنولوجيا الحديثة. فالعديد من الجماعات المتطرفة قد لجأت إلى القيام بأعمال التخويف والعدوان والتهديد المعنوي أو المادي، من خلال استخدام الوسائل الإلكترونية بهدف الاعتداء على الدول أو الأفراد، وهذا الأمر وضع المملكة العربية أمام تحدي عالمي واقليمي ساهم في اتخاذ الكثير من القرارات الناجحة والقوية بالغة الاهمية في التصدي ومواجهة الإرهاب الإلكتروني

**– قائمة المراجع:**


Cyber crime in Kingdom of Saudi .(December, 2013 12) .B. M. E Elnaim Arabia: The threat today and the expected future .(Vol. 3, No. 12, pp. 14-19) *In Information and Knowledge Management*، صفحة 16.

*Saudi Arabia's counterterrorism methods: A* .(2017) .Majed, M Madhian& ,.B United States: Naval Postgraduate School *.case study on homeland security* .Monterey

*Saudi Arabia's King Saud University Database Hacked.* .(2012 ,12 2) .M Kumar *. .The Hacker News*

*Kingdom of Saudi Arabia* .(2017) .Alsowailm, f Hathaway& ,.M., Spidalieri, F .Potomac Institute for Policy Studies :Virginia*..Cyber Readiness at a Glance*

*Second wave of Shamoon 2 attacks identified. Palo Alto* .(2017 ,1 1) .R Falcone *Networks Blog*. تم الاسترداد من https://unit42.paloaltonetworks.com/unit42-second- /wave-shamoon-2-attacks-identified.

سليمان، نرمين. (2018). *أثر الجرائم الإلكترونية على الأبعاد الداخلية للأمن القومي: دراسة حالة المملكة العربية السعودية خلال الفترة من 2006 إلى 2016*، ، ص *27*. القاهرة: جامعة القاهرة: دكتوراه بكلية الاقتصاد والعلوم السياسية.

عامر محمد. (2015). *الإرهاب الرقمي الماهية و سبل المكافحة*. القاهرة: دار أمال للنشر والتوزيع.

محمد، صابر. (2008). *الإرهاب الإلكتروني واستخدام القوة* . مصر: دار الدقهلية للنشر والتوزيع.

محمود العطيات. (2012). *الإرهاب الدولي في القانون المعاصر* . الفيوم: دار المحمدية للنشر.

مصطفى الزين. (2015). *الإرهاب الإلكتروني في التشريع الدولي المعاصر*. مصر: دار المجدلاوي للنشر والتوزيع.

هيئة الاتصالالات و نظ المعلومات. (2007). *نظام مكافحة الجرائم المعلوماتية رقم رقم M17*. usa: الامم المتحدة.

وفاق عياشي. (2006). *مكافحة الإرهاب بين السياسة والقانون31*. الجزائر: دار اللدوينة للنشر والتوزيع.