

## جريمة الإرهاب الإلكتروني: الأسباب وآليات العلاج.

بن مرزوق عنتره  
أستاذ محاضراً  
جامعة محمد بوضياف – المسيلة.

### ملخص:

شكلت التكنولوجيا الحديثة أحد العوامل الهامة التي ساهمت في انتشار جريمة الإرهاب الإلكتروني. والتي تعتبر أحد أخطر الجرائم التي تهدد أمن واستقرار الدول والمجتمعات. وسنحاول من خلال هذه الدراسة تحليل هذه الجريمة بالتطرق لأهم مسبباتها وسبل الوقاية منها ومكافحتها.

### Abstract:

La technologie moderne a été l'un des facteurs importants qui contribuent à la propagation du crime de cyber-terrorisme. C'est l'un des crimes les plus graves qui menacent la sécurité et la stabilité des États et des sociétés. dans le cadre de cette étude ,nous essaierons d'analyser ce crime en s'attaquant à ses principales causes et à ses moyens de la prévenir et de la combattre.

الكلمات المفتاحية: الإرهاب الإلكتروني- الإجرام الإلكتروني- الاختراق المعلوماتي- السياسة الوقائية- السياسة العلاجية...

### مقدمة:

شكلت قضية مكافحة الإرهاب بصورته التقليدية القضية الرئيسية التي ركزت عليها أغلب الأجنادات الأمنية للدول على مدار سنوات طويلة، غير أنه مع التطورات التكنولوجية التي شهدتها العالم حديثاً وقع تغير كبير سواء على مستوى تطور الظاهرة أو على مستوى آليات المكافحة، فلم تعد ظاهرة الإرهاب مقتصرة على جانبها التقليدي فقط بل تعدتها لتشمل ظاهرة الإرهاب الإلكتروني كأحد أخطر الجرائم التي برزت بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الإلكترونية التي تحمل أفكاراً هدامة تدعو إلى العنف والتطرف.

وأمام زيادة انتشار الظاهرة وتزايد ضررها كان على الدول ضرورة تغيير سياساتها الأمنية المعتمدة على الأسلحة التقليدية والعمل على انتهاز سياسات أكثر تكيفاً مع التطورات التكنولوجية بالاعتماد على الأسلحة الإلكترونية في حروبها الجديدة.

هذه الدراسة ستحاول التطرق لطبيعة جريمة الإرهاب الإلكتروني وأهم مسبباتها وآليات مكافحتها وذلك من خلال طرحها للتراسلات التالية:

- ماهي أبرز التغيرات التي فرضتها الثورة التكنولوجية الحديثة على ظاهرة الإرهاب؟ وكيف ساهمت في نقلها من المفهوم التقليدي إلى المفهوم الجديد؟

- كيف وظفت التنظيمات الارهابية وسائل الاتصال الحديثة في خدمة أجندها الإجرامية؟
- ماهي أهم الأسباب الدافعة للوقوع في هذه الجريمة؟ وماهي الأدوات المستخدمة في ذلك؟
- ماهي أهم الآليات الكفيلة بالتصدي لهذه الجريمة الخطيرة التي اتسع انتشارها وازداد خطرها؟
- الإجابة عن هذه التساؤلات تتطلب منا ضرورة تناول العناصر التالية:
- إشكالية تحديد مفهوم الإرهاب بين التصور التقليدي والتصور الحديث.
- التنظيمات الإرهابية والتوظيف اللاعقلاني لوسائل الاتصال الحديثة.
- التنظيمات الارهابية والإجرام الإلكتروني: دراسة في الأسباب والعناصر المستخدمة.
- آليات التصدي لجرائم الإرهاب الإلكتروني بين الإجراءات الوقائية والأساليب العلاجية.
- 1- إشكالية تحديد مفهوم الإرهاب بين التصور التقليدي والتصور الحديث:

تعتبر مهمة تحديد المصطلحات أول تحد يواجهه المفكرون ويتعرض له الباحثون في جميع التخصصات وفي شتى الدراسات، وذلك لما تطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين فرقاء المجتمع العلمي يمكن تعميمها على جميع الحقول المعرفية، ويعتبر مصطلح الارهاب الالكتروني واحدا من هذه المصطلحات التي تعرف تعددا في التعريفات المقدمة لها.

لم يرد لفظ الارهاب terrorism مستقلا بذاته في المعاجم العربية القديمة التي خلت من هذه الكلمة بحكم أنها من الكلمات الحديثة الاستخدام، غير أنها عرفت الفعل رهب رهبة ورهبا أي خاف، والرهبة هي الخوف والفرع، والرهبوت تعني الخوف العظيم، وما تجدر الإشارة إليه أن لفظ الإرهاب في اللغة العربية لا يحمل مضامين الرعب، التي يقوم على أساسها ذلك اللفظ في اللغة الانجليزية. وقد جاء مفهوم الإرهاب في القرآن الكريم بمعان متعددة تتفاوت ما بين الخوف والفرع والرهبة أو الخشية من الله والخشوع له، كما تعني أيضا الردع العسكري، ولم يرد في القرآن الكريم ما يدل على معنى استخدام الرعب لتحقيق أهداف سياسية كما جاء في معظم المعاجم الحديثة. أما لفظ الإرهاب terrorism بمعناه اللغوي المعاصر المرتبط باستخدام العنف violence فترجع أصوله إلى لفظ رعب terreur الذي ورد لأول مرة في اللغة الفرنسية عام 1355م في كتابات الراهب Bersuire، وذلك اشتقاقا من اللفظ اللاتيني Terrere الذي يعني في الأصل خوفا أو قلقا متناهيا نتيجة تهديد غير محدود أو مألوف أو متوقع<sup>1</sup>.

في موسوعة السياسة يعرف الإرهاب بأنه استخدام العنف غير القانوني أو التهديد به بأشكاله المختلفة كالإغتيال والتشويه والتعذيب والتخريب والنسف بغية تحقيق هدف سياسي معين مثل كسر روح المقاومة لدى الأفراد وهدم المعنويات لدى الهيئات والمؤسسات، أو وسيلة من وسائل الحصول على المعلومات أو المال، وبشكل عام استخدام الإكراه لإخضاع طرف مناوئ لمشينة الجهة الإرهابية. أما في قاموس علم الجريمة Criminology of Dictionary A فهو نمط من العنف يتضمن الاستخدام المنظم للقتل أو التهديد باستخدامه أو الأذى الجسدي والتدبير لإنزال الرعب أو الذعر بجماعة مستهدفة لأوسع مدى من الضحايا الذين أنزل بهم الرعب لإشاعة أجواء من الرعب<sup>2</sup>.

أما في القاموس السياسي يعرف الإرهاب بأنه محاولة نشر الذعر والفرع لأغراض سياسية، كما أن الإرهاب وسيلة تستخدمها حكومة استبدادية لإرغام الشعب على الخضوع والاستسلام لها.<sup>3</sup>

وأمام تعدد تعاريف الإرهاب واختلافها قام الكاتب Schmid Alex في كتابه الإرهاب السياسي Terrorism Political بمراجعة مائة تعريف للإرهاب من قبل خبراء وباحثين في هذا المجال وخلص إلى وجود عناصر مشتركة بين هذه التعاريف على النحو التالي:<sup>4</sup>

- مفهوم تجريدي بدون جوهر.
- لا يكفي تعريف واحد لحصر جميع استخدامات المصطلح.
- العديد من التعريفات المختلفة تشترك في عوامل عامة
- معنى الإرهاب مستمد من الضحية المستهدفة.

هذا بالنسبة لمفهوم الإرهاب أما الإرهاب الإلكتروني Cyberterrorism الذي جاء نتيجة الثورة التكنولوجية التي شهدها العالم الحديث ، فرغم الاهتمام الإعلامي والأكاديمي به في السنوات الأخيرة إلا أن بداية استخدامه كمصطلح كان خلال فترة الثمانيات علي يد باري كولن Collin Barry الذي عرفه بأنه «التقاء ما بين الفضاء السيبراني والإرهاب»<sup>5</sup> ثم تطور المفهوم بعد ذلك فقد عرفه مارك بوليت Mark Poliit عام 1997، وهو وكيل خاص لمكتب التحقيقات الفدرالي، بأنه: «هجوم متعمد، ذو دوافع سياسية ضد المعلومات وأنظمة الكمبيوتر، وبرامج الكمبيوتر، وبيانات الأهداف التالية ضد العنف من جانب المجموعات المعادية للوطنية أو وكلائهم السريين»<sup>6</sup>.

في حين عرفه Denning Dorothy بأنه شن هجمات ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها، بهدف تهريب حكومة أو شعب ما بناء على أهداف سياسية أو اجتماعية غير مشروعة. ولكي يعتبر ذلك إرهاب لابد أن يؤدي إلى ترويع وإكراه الحكومات والأشخاص والممتلكات أو على الأقل التسبب في الضرر والخوف، وكذلك إحداث ضحايا وإيذاء بدني وانفجار وأضرار اقتصادية جسيمة والهجوم على البنية الأساسية وإعاقة عمل الخدمات الأساسية.<sup>7</sup>

ويعرفه جيمس لويس Lewiss James كذلك على أنه " استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنية التحتية الوطنية المهمة مثل: الطاقة والنقل والعمليات الحكومية، أو بهدف تهريب حكومة ما أو مدنيين"<sup>8</sup>

واعتبرته وكالة التحقيقات الفدرالية I.B.F. بأنه مصطلح حديث يعني استعمالاً - أو التهديد باستعمال - غير مشروع للعنف ضد أشخاص أو ممتلكات لتخويف أو إجبار حكومة أو المدنيين كلهم أو بعضهم لتحقيق أهداف سياسية أو اجتماعية.<sup>9</sup>

وبرز الإرهاب الإلكتروني لأول مرة عام 2000 حينما أدى انتشار فيروس الكمبيوتر "I love you" إلى إتلاف معلومات قدرت قيمتها بنحو 10 مليارات دولار أمريكي، كما عزت الولايات المتحدة هجمات 11 سبتمبر عام 2001 إلى الربط بين الهجمات وبين الجريمة الإلكترونية وهو الأمر الذي دعا ثلاثين دولة إلى التوقيع على أول اتفاقية دولية لمكافحة الإجرام المعلوماتي في العاصمة المغربية بودابست من نفس العام، بينما في عام 2003 أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسوب، وقدر "مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت" كلفة إصلاح الأضرار التي تسببها فيروسات المعلوماتية بنحو 12 مليار دولار أمريكي سنوياً. وفي أكتوبر 2012 الأمم المتحدة عرفت الإرهاب الإلكتروني بأنه "استخدام الانترنت لنشر

أعمال إرهابية"، وفي الآونة الأخيرة اتهم تقرير أميركي الجيش الصيني بالوقوف وراء شبكات قرصنة تستخدم في حرب، بما يعني أن الجرائم الإلكترونية تشكل خطراً كبيراً على استقرار الدول، وارتقت لمفهوم "الإرهاب الإلكتروني" "CyberTerrorism" الذي يُمثل تهديداً واضحاً للأمن القومي للدول، حيث أصبحت البنية التحتية لأغلب المجتمعات الحديثة تُدار عن طريق أجهزة الحاسب الآلي والإنترنت، وهو ما يُعرضها لهجمات مُتعددة من "الهاكرز" و"المُخترقين" بشكل عام، ومن أجهزة المخابرات والمنظمات الإرهابية بشكل خاص.<sup>10</sup>

وكخلاصة لما تم تقديمه من تعريفات يمكن القول أن الإرهاب الإلكتروني يعني «العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشق صنوفه وصور الإفساد في الأرض».<sup>11</sup>

## 2- التنظيمات الإرهابية والاستغلال اللاعقلاني لوسائل الاتصال الحديثة:

تعتبر الإنترنت سلاحاً ذو حدين، إما وسيلة من وسائل نشر الخير والعلم والتواصل بين البشر، وإما أداة من أدوات نشر الفساد والشرور بينهم، وفي العصر الحديث اعتبرها العديد من المختصين أنها أكثر أسلحة التنظيمات الإرهابية تهديداً لأمن واستقرار المجتمعات، حيث تم توظيفها من أجل التحريض على نشر الكراهية والتطرف والعنف والقتل وسفك الدماء بدعوى الجهاد المقدس، وهي بذلك الوسيلة المثلى التي تعتمد عليها هذه التنظيمات في التعبئة والتجنيد لها، على أساس أنها تقوم بتحقيق الهدف في أسرع وقت وبأقل تكلفة. وهذا ما يفسر تزايد عدد المنضمين لها.

فقد أكد تقرير للخبير الأمني في قضايا الإرهاب الرقي جيف باردين jeff bardin أن التنظيم الإرهابي «داعش» له أزيد من 50 ألف موقع إلكتروني، 90 ألف صفحة باللغة العربية على موقع التواصل الاجتماعي «فيس بوك»، و40 ألفاً بلغات أخرى، وهذا ما ساهم في تجنيده حوالي 3400 شاب شهرياً عبر حملاته الإلكترونية.<sup>12</sup>

وقد أشار الخبير المصري في شؤون الجماعات الإسلامية ومؤسس «الجهة الوسطية لمواجهة العنف والتطرف»، صبرة القاسمي، إن هناك نحو 82 ألف صفحة على الإنترنت تحت إدارة تنظيم داعش، تتوزع ما بين صفحات في مواقع التواصل الاجتماعي المختلفة والمنتديات ومواقع إلكترونية أخرى. وأن مهمة تلك الصفحات هي الترويج للتنظيم، فضلاً عن استقطاب المزيد من العناصر الشبابية للانضمام له. كما أكد الباحث في شؤون الحركات والجماعات المتطرفة ماهر فرغلي الذي اعتبر أن قرابة 60 في المئة من العناصر الإرهابية في تنظيم داعش في الوقت الحالي تم استقطابها من خلال الشبكة العنكبوتية، ومواقع التواصل الاجتماعي، مشيراً إلى أن مشاركة تنظيم داعش بـ40 تغريدة يومياً على موقع التواصل الاجتماعي تويتر، تؤكد اهتمام التنظيم بالشبكة العنكبوتية، حيث إن هناك نحو 210 صفحات ومجموعات على مواقع التواصل الاجتماعي للخلايا الإرهابية في سوريا والعراق فقط.<sup>13</sup>

ولا يتوقف أمر استخدام الإنترنت منذ نشوء تنظيم داعش الإرهابي فقط، بل يرجع إلى سنوات مضت، ولعل من أهم المواقع الإلكترونية التي كانت تدعو إلى التعبئة والتجنيد والدعوة إلى الانضمام إلى التنظيمات الإرهابية مايلي:<sup>14</sup>

موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001م، ومن خلاله تصدر البيانات

الإعلامية للقاعدة.

ذروة السنام: وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

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

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

3- التنظيمات الإرهابية والإجرام الإلكتروني: دراسة في الأسباب والعناصر المستخدمة.

الإرهاب ظاهرة واحدة سواء بصفته التقليدية أو بصفته الحديثة، وهي ظاهرة معقدة ومركبة وشاملة، متعددة الأسباب متنوعة الآليات والعناصر المستخدمة، وسنحاول من خلال هذا العنصر التطرق إلى أهم أسباب بروز ظاهرة الإرهاب الإلكتروني وأهم العناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية.

- أسباب الإرهاب الإلكتروني:

أسباب الإرهاب الإلكتروني لا تختلف كثيراً عن أسباب الإرهاب بصفة عامة، وهي أسباب تتعدد وتختلف تبعاً لاختلاف الجهات السياسية والظروف الاقتصادية والأحوال الاجتماعية، والاختلاف الديني والعقدي، لذلك فإن ما يصدق على مجتمع قد لا يصدق بالضرورة على غيره من المجتمعات. ويمكننا إيجاز أهم الأسباب المؤدية إلى بروز ظاهرة الإرهاب الإلكتروني فيما يلي<sup>15</sup>.

- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها، رغبة في تسهيل دخول المستخدمين، وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية، ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية.

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

- سهولة استخدام شبكة المعلومات وقلة التكلفة: مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون الحاجة إلى مصادر تمويل، فشن هجومي إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة، فصعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تساعد المجرم على الإفلات من العقوبة.

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

- الفراغ التنظيمي والقانوني وغياب السيطرة والرقابة على الشبكات المعلوماتية، ولجوء المجرم الإرهابي إلى دول معادية لشن هجومه على الدول الأخرى.

كل هذه الأسباب شجعت على انتشار ظاهرة الإرهاب الإلكتروني التي أصبحت الوسيلة المثلى في العمل الإجرامي للتنظيمات الإرهابية المختلفة.

#### - العناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية:

كشفت دراسة أعدها جابريال ويمن خبير الإرهاب الدولي الأمريكي بجامعة هارفرد بالولايات المتحدة الأمريكية عن كيفية استغلال الجماعات الإرهابية لشبكة الانترنت من أجل تحقيق أغراضهم الخبيثة كمايلي:<sup>16</sup>

- **التنقيب عن المعلومات:** إن شبكة الانترنت في حد ذاتها تعتبر مكتبة إلكترونية هائلة الحجم، وتكتظ بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها مثل أماكن المنشآت النووية، والمطارات الدولية، والمعلومات المختصة بسبل مكافحة الإرهاب، وبذلك يكون 80% من مخزونهم المعلوماتي معتمداً في الأساس على مواقع إلكترونية متاحة للكل، دون خرقاً لأي قوانين أو بروتوكولات الشبكة.

- **الاتصالات:** تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بينها، وذلك نظراً لقلة تكاليف الاتصال باستخدام الانترنت، مقارنة بالوسائل الأخرى، كما أنها تتمتع بوفرة المعلومات التي يمكن تبادلها، وقد أصبح عدم وجود زعيم ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية، وكل هذا بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية.

- **التعبئة وتجنييد إرهابيين جدد:** إن استخدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها واستمرارها، وهم يستغلون تعاطف الآخرين من مستخدمي الانترنت مع قضاياهم، ويجتذبون هؤلاء السذج بعبارات براقية وحماسية من خلال غرف الدردشة الإلكترونية، ونحن نعلم أن تسليحة الشباب والمراهقين هي الجلوس بالساعات الطويلة في مقاهي الانترنت للثرثرة مع جميع أنواع البشر في مختلف أنحاء العالم.

- **إعطاء التعليمات والتلقين الإلكتروني:** يمتلئ الانترنت بكم هائل من المواقع التي تحتوي على كتيبات وإرشادات تشرح طرق صنع القنابل، والأسلحة الكيماوية الفتاكة، وعند استخدام محرك البحث «غوغل» Google عام 2005 للبحث عن مواقع تضم في موضوعاتها كلمات مثل «إرهابي terrorist» و«دليل» handbook، فكانت نتائج البحث ما يقرب من ثمانية آلاف موقع.

- **التخطيط والتنسيق:** تعتبر شبكة الانترنت وسيلة للاتصال باللغة الأهمية بالنسبة للمنظمات الإرهابية، حيث تتيح لهم حرية التنسيق الدقيق لشن هجمات إرهابية محددة، ويضيف ويمن أن أعضاء منظمة القاعدة البارزين اعتمدوا بشكل مكثف على الانترنت في التخطيط لهجمات 11 سبتمبر، ويستخدم الإرهابيون الرسائل الإلكترونية العادية email وغرف الثثرة chat rooms، لتدبير الهجمات الإرهابية وتنسيق الأعمال والمهام لكل عنصر إرهابي.

- **الحصول على التمويل:** يستعين الإرهابيون ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، في التعرف على الأشخاص ذوي القلوب الرحيمة ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين، يمثلون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة البريد الإلكتروني بطريقة ماهرة لا يشك فيها المتبرع بأنه يساعد إحدى المنظمات الإرهابية.

#### 4- آليات التصدي لجرائم الإرهاب الإلكتروني بين الإجراءات الوقائية والأساليب العلاجية:

أمام التهديدات والمخاطر المتزايدة التي تخلفها استخدام التكنولوجيا الحديثة فقد بات لزاما على مختلف الدول البحث عن آليات وميكانيزمات يمكن من خلالها التخفيف من حدة التهديدات الناجمة عن جرائم الارهاب الالكتروني، وذلك من خلال الاعتماد على سياسة أمنية فعالة تضع مسألة توفير الأمن السيبراني على رأس أولوياتها واستراتيجياتها.

ذلك أن هدف الأمن السبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات.<sup>17</sup> وهذا يتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به.<sup>18</sup>

وأمام هذه التحديات فقد بات لزاما على أي دولة تريد المحافظة على أمنها واستقرارها وسيادتها أن تهتم اهتماما بالغاً بمسألة تحقيق وتطوير أمنها السيبراني بما يساعدها على تجنب أخطار جرائم الارهاب الالكتروني، وذلك عن طريق اعتمادها لسياسات وقائية وأخرى علاجية.

#### - أساليب الوقاية من الإرهاب الإلكتروني:

من أهم الأساليب التي يمكن الاعتماد عليها للوقاية من الإرهاب الالكتروني مايلي:

- اعتماد سياسة وقائية بنشر ثقافة الأمن السيبراني وزيادة الوعي المجتمعي بمختلف المخاطر والتهديدات التي تفرضها الثورة التكنولوجية الحديثة، وتحصين أفراد المجتمع ضد كل الأفكار الهدامة التي تنشرها مختلف المواقع الالكترونية ووسائل التواصل الاجتماعي، وذلك من خلال حجب وإزالة تلك المنشورات والمواقع الالكترونية المروجة للفكر الإرهابي عبر الانترنت وملاحقة المؤيدين لها.

- تحديث البنية التحتية لتقنية المعلومات والاتصالات وحمايتها، وتحديد نقاط القوة والضعف الموجودة في التشريعات القانونية المتعلقة بمكافحة جرائم الارهاب الالكتروني، والعمل على تجاوز عقبات تطبيقها.

- تفعيل دور وسائل الإعلام في مواجهة الفكر الإجرامي للتنظيمات الإرهابية على شبكة الانترنت، والتحذير من مختلف المواقع المحرّضة على العنف والداعية للتعصّب والتجنيد للفكر المتطرف، مع ضرورة التعاون مع الجهات الأمنية في الحصول على المعلومات اللازمة المساعدة على مواجهة هذا النوع من الإرهاب في إطار تشجيع ما يعرف بالإعلام الأمني.

- بث أعمال تلفزيونية حول ضحايا الإرهاب والنتائج المدمرة المترتبة على استخدام الانترنت في تشجيعه والترويج له، والتعامل بيقظة وحذر مع ما تنشره التنظيمات الإرهابية على المواقع الالكترونية المختلفة.

- إقامة مؤتمرات فكرية حول مواضيع الإرهاب الالكتروني، ووضعها ضمن المقررات الدراسية من أجل تنشئة أجيال تنبذ الإرهاب بشتى أشكاله، مع الحرص على تشجيع البحوث العلمية حول الظاهرة بما يؤدي إلى دحض الفكر التطرفي.

- نشر قيم المواطنة والتسامح والفكر الوسطي وتعزيز مكانة المؤسسات الأمنية في نفوس المواطنين، من خلال التشهير لانجازاتها في مجال مكافحة جرائم الإرهاب الالكتروني .

- الاستفادة من خبراء عالميين مجال مكافحة الجرائم الالكترونية من أجل المساهمة في تكوين مختصين من ذوي المهارات العالية

والدراية والاطلاع والتحكم الدقيق في التكنولوجيا الحديثة.

- الاستفادة من تجارب الدول الرائدة في مجال تحقيق الأمن السيبراني، والتعرف على أفضل التقنيات العالمية المنتهجة في مكافحة الجرائم الالكترونية من قرصنة وتجسس وإرهاب الكتروني...إلخ
- نشر ثقافة الترويج للأخطار المترتبة عن الاستخدام السيء للإنترنت، مع معرفة ما يترتب عن ذلك من عقوبات شديدة رادعة بإمكانها منع تشجيع الانضمام للتنظيمات الإرهابية والترويج لها.
- أساليب العلاج من الإرهاب الإلكتروني:

من أهم الأساليب التي يمكن الاعتماد عليها في مكافحة الإرهاب الإلكتروني مايلي:

- من الضرورة أن تكون هناك بيئة تشريعية تعالج هذا النوع من الجرائم، فما لم يكن هناك غطاء تشريعي أو نص قانوني يجرم 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 مجرم فإنه لا مجال للحديث عن التحقيق في هذا النوع من الأفعال.<sup>19</sup> كما انه لابد من تشديد العقوبات ضد كل من ثبت في حقه القيام بهذا الجرم.
- وقد صاغ الكاتب بدر أحمد في دراسته الموسومة «بالإرهاب الإلكتروني: أدواته وآثاره..أساليب الوقاية والعلاج» مجموعة من الآليات لعلاج ظاهرة الإرهاب الإلكتروني، تمثلت فيمايلي:<sup>20</sup>
- مراجعة التكتيكات والتدريبات المعتمدة لمكافحة الإرهاب بشكل دوري، وتعديل ما يلزم لكي تتناسب مع متطلبات مكافحة التهديدات الإرهابية المستقبلية على الساحة العالمية.
- ينبغي على الأجهزة الأمنية أن تفرض رقابة صارمة على الجناة المدانين في جرائم الإرهاب الإلكتروني خلال فترة تواجدهم داخل السجون.
- تطبيق مبدأ العزل والفصل، وذلك بعزل المحكومين في هذا النوع من الجرائم عن غيرهم من المحكومين لتجنب خطورة التأثير في غيرهم من السجناء.
- زرع المصادر داخل السجون التي يتواجد فيها المحكومون في قضايا الإرهاب الإلكتروني، ورصد زوار المحكومين في جرائم الإرهاب الإلكتروني ومتابعتهم ومراقبتهم.
- تطبيق برامج إصلاح وتأهيل خاصة بالمحكومين في هذا النوع من الجرائم، بحيث تهدف هذه البرامج إلى إعادة تأهيل النزير ومحاولة الاستفادة منه وتجنيدده لحساب الدولة، وبالتالي يكون مصدراً هاماً من مصادر جمع المعلومات عن الجماعات الإرهابية أو المتطرفة.
- سن القوانين أو التشريعات الخاصة التي تسد كافة الثغرات التي تكتنف جريمة الإرهاب الإلكتروني وسبل التحقيق فيها، كالقوانين المتعلقة بكيفية اكتشاف الأدلة الإلكترونية، وحفظها، والأدلة التي تقبل قانوناً لإثباتها.
- إحداث هيئة وطنية من الخبراء والمختصين تعمل على وضع وتطوير استراتيجيات وطنية للأمن الإلكتروني تركز على حماية البنية التحتية لشبكات المعلوماتية والنظم البرمجية وتنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة: الأمنية والتشريعية والقضائية

والفنية، وذلك من أجل الحد من جرائم الإرهاب الإلكتروني قدر المستطاع، والعمل على ضبطها، وإثباتها بالطرق القانونية. - السعي لإيجاد منظومة قانونية دولية تحت مظلة الأمم المتحدة يعهد إليها توثيق وتوحيد جهود الدول في مكافحة ومواجهة الإرهاب الإلكتروني.

- عقد الاتفاقيات بين الدول بخصوص جرائم الإرهاب الإلكتروني وتنظيم كافة الإجراءات المتعلقة بالوقاية من هذه الجريمة وعلاجها وتبادل المعلومات والأدلة في شأنها، بما في ذلك تفعيل اتفاقيات تسليم الجناة في جرائم الإرهاب الإلكتروني. - تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضد دول أو جهات أخرى خارج هذه الأراضي.

- ضرورة أن تكون هذه المواقع الإرهابية مصدر معلومات كبيرة للأجهزة الأمنية، من حيث علاقات الإرهابيين والفكر الإرهابي والخطط الإرهابية ودراسة البيانات الصادرة عن أرباب الإرهاب، لمعرفة خططهم واستراتيجياتهم حتى تتمكن الأجهزة الأمنية من مواجهة الإرهاب في المستوى الفكري نفسه واللوجستي إن لم تتفوق عليهم بواسطة استخدام أسلحتهم ومواقعهم. - قيام مزودي خدمة الانترنت بالإبلاغ عن النشاط الإرهابي الملموس إن شعروا بأنه يتضمن التهديد لأي شخص أو مؤسسة. - الدفع بعناصر أمنية للانضمام إلى هذه المواقع بهدف إفساد خططها أو تدميرها، أو نشر تصحيح للمعلومات الواردة فيها، حتى لا يثق. على الأقل. من يدخل هذه المواقع بالعاملين فيها، فلا يدري هل هم أهل فكر أم جهات أخرى، حيث ستفقد هذه المواقع مصداقيتها وبريقها وحيويتها وتصبح بدلاً من أن تخترق هي المواقع الرسمية تصبح هذه المواقع نفسها مخترقة من قبل بعض الشباب الموثوق بهم وطنياً وفكرياً ودينياً، للدخول والمحاورة وتشيتت جهود أهل الفكر الضال والإرهاب. - التنسيق مع إدارات المواقع ومحركات البحث أمثال (جوجل، وياهو، ويوتيوب، ووندوز لايف، ومكتوب، والفيسبوك) وغيرها لمنع دخول الإرهابيين لهذه المواقع، وعدم استخدام مواقعهم كوسيلة لنشر الفكر الإرهابي، والحذر من أن تكون هذه المواقع حامية وحاملة للإرهاب، وهذا بلا شك يتطلب تعاوناً دولياً وإقليمياً ومحاصرة حقيقية للفكر الإرهابي، حيث إن هذا الفكر الخبيث سريع التشكل وسريع الالتفاف.

- بناء وتطوير وتفعيل مراكز ومؤسسات مكافحة الإرهاب الدولي في إطار القطاعين العام والخاص على مستوى العالم.

#### خاتمة:

في الأخير وانطلاقاً من كل ما سبق يمكن القول أن مسألة مكافحة الإرهاب الإلكتروني يعد أحد أهم التحديات الجديدة التي فرضتها التطورات التكنولوجية المتسارعة، ولذلك فعلى الدول والمجتمعات بذل المزيد من الجهود حتى تنجح في مجال مكافحة مختلف المخاطر التي يفرزها الفضاء الإلكتروني، والتي يأتي على رأسها الإرهاب الإلكتروني وغيره من التهديدات التي يمثل الانتصار عليها انتصاراً للإنسانية جمعاء.

فالانترنت يجب أن تبقى فضاءاً لنشر ومشاطرة العلوم والمعرفة وأداة للإبداع والتقارب والتعاون بين الأفراد والشعوب و الدول، وليس وسيلة وأداة تهديدية تستغلها الجماعات الإرهابية من أجل بلوغ أهدافها الإجرامية ونشر أفكارها التطرفية، كما أشار إلى ذلك السيد وزير الشؤون المغربية والإتحاد الإفريقي وجامعة الدول العربية، السيد: عبد القادر مساهل في كلمته خلال

أشغال الورشة الدولية حول دور الإنترنت والشبكات الاجتماعية في مكافحة التطرف والإرهاب الإلكتروني والوقاية منهما.<sup>12</sup>  
قائمة المراجع:

- الكتب باللغة العربية:

- اسماعيل عبد الفتاح عبد الكافي، الإرهاب ومحاربه في العالم المعاصر. القاهرة: الهيئة العامة لقصور الثقافة، 2007.
- جهاد عودة، محمد عبد العظيم الشيمي، أيمن زكي، مدخل لظاهرة الارهاب في مصر والمملكة العربية السعودية: تجارب استراتيجية. القاهرة: المكتب العربي الحديث، 2015.
- محمد الحميري، أصول إرهاب الحوثيين والقاعدة في اليمن. القاهرة: المكتب العربي للمعارف، 2015.
- مصطفى يوسف كافي، الإدارة الإلكترونية. دمشق: دار رسلان للطباعة والنشر والتوزيع، 2012.
- الملتقيات العلمية:

- أيسر محمد عطية، «دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته». ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية. عمان خلال الفترة 02-04 سبتمبر 2014.

- محمد محمد الألفي، تشريعات مكافحة جرائم الارهاب الالكتروني: الأحكام الموضوعية والأنماط. ورقة عمل مقدمة في الندوة العلمية حول: القوانين العربية والدولية في مكافحة الإرهاب. المنعقدة بالرياض خلال الفترة 15-17 أبريل 2013.

- الجرائد:

- أمنية عادل، الإنترنت يلقي بآلاف الشباب في جحيم الجماعات الارهابية. جريدة البيان، العدد 12660، الصادر بتاريخ 15 فيفري 2015.

- الكتب باللغة الاجنبية:

- Bradley, K.Ashley. **Anatomy of Cyberterrorism :Is America vulnerable .?A Research Paper Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements ,February.2003**
- Joanna F .DeFranco ,**What Every Engineer Should Know About Cyber Security and Digital Forensics.** Boka Raton : CRC press, 2014.
- John Arquilla,David Ronfeldt, **Networks and Netwars: The Future of Terror, Crime, and Militancy.** USA ; Rand publication, 2001.
- M N Sirohi, **Cyber Terrorism and Information Warfare.** Delhy ; Alpha Editions, 2015.
- Newton Lee, **Counterterrorism and Cybersecurity: Total Information Awareness.** 2<sup>nd</sup>Ed. Switzerland ; Springer International Publishing, 2015.
- Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, **Critical Information Infrastructure Security.** Berlin ;

Springer, 2013.

- Ushie Henry Ekpe, The Impact of Terrorism (Including Cyber Terrorism) and Threats of Terrorism on International Business (or Nation Sate). **Journal of the International Relations and Affairs Group**, Volume 3, Issue 1, 2013.

#### المواقع الالكترونية:

- إيهاب شوقي، الإرهاب الإلكتروني وجرائمه. من موقع:

<http://www.assakina.com/awareness-net/rebounds.81251/html>

- أيمن حسين، الإرهاب الإلكتروني أخطر معارك حروب الفضاء. جريدة الوطن الأردنية. من موقع:

<http://alwatan.com/details166324/>

- بدر أحمد، الإرهاب الإلكتروني: أدواته وآثاره.. أساليب الوقاية والعلاج. من موقع:

<http://baathparty.sy/site/arabic/index.php?node&552=cat&15369=>

- محمود خليل، 50 ألف موقع إلكتروني لداعش.. والإرهاب يحاصر الإنترنت. من موقع:

<http://www.alittihad.ae/details.php?id=64991&y=2015&article=full>

#### الهوامش:

1 محمد الحميري، أصول إرهاب الحوثيين والقاعدة في اليمن. القاهرة: المكتب العربي للمعارف، 2015، ص ص 08-09.

2 جهاد عودة، محمد عبد العظيم الشبيبي، أيمن زكي، مدخل لظاهرة الارهاب في مصر والمملكة العربية السعودية: تجارب استراتيجية. القاهرة: المكتب العربي الحديث، 2015، ص ص 18-19.

3 اسماعيل عبد الفتاح عبد الكافي، الإرهاب ومحاربه في العالم المعاصر. القاهرة: الهيئة العامة لقصور الثقافة، 2007، ص 20.

4 جهاد عودة، محمد عبد العظيم الشبيبي، أيمن زكي، مرجع سابق الذكر، ص 19.

5 John Arquilla, David Ronfeldt, **Networks and Netwars: The Future of Terror, Crime, and Militancy**. USA; Rand publication, 2001, P281.

6 Ushie Henry Ekpe, The Impact of Terrorism) Including Cyber Terrorism (and Threats of Terrorism on International Business) or Nation Sate. (**Journal of the International Relations and Affairs Group**, Volume 3, Issue 1, 2013, P38.

7 M N Sirohi, **Cyber Terrorism and Information Warfare**. Delhy; Alpha Editions, 2015, P01.

8 Newton Lee, **Counterterrorism and Cybersecurity: Total Information Awareness**. 2ndEd, Switzerland; Springer International Publishing, 2015, P225.

9 Bradley, K. Ashley. **Anatomy of Cyberterrorism: Is America vulnerable**. ?A Research Paper Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, February, 2003 P06.

10 أيمن حسين، الإرهاب الإلكتروني أخطر معارك حروب الفضاء. جريدة الوطن الأردنية. من موقع:

<http://alwatan.com/details/166324>

11 أيسر محمد عطية، «دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته». ورقة مقدمة في الملتقى العلمي:

الجرائم المستحدثة في ظل المتغيرات والتحوليات الإقليمية والدولية. عمان خلال الفترة 02-04 سبتمبر 2014، ص 09.

12 محمود خليل، 50 ألف موقع إلكتروني لداعش.. والإرهاب يحاصر الإنترنت. من موقع:

<http://www.alittihad.ae/details.php?id=64991&y=2015&article=full>

13 أمنية عادل، الإنترنت يلقي بآلاف الشباب في جحيم الجماعات الارهابية. جريدة البيان، العدد 12660، الصادر بتاريخ 15 فيفري 2015، ص 32-33.

14 إيهاب شوقي، الإرهاب الإلكتروني وجرائمه. من موقع:

<http://www.assakina.com/awareness-net/rebounds/81251.html>

15 مصطفى يوسف كافي، الإدارة الإلكترونية. دمشق: دار رسلان للطباعة والنشر والتوزيع، 2012، ص ص 440-441.

16 محمد محمد الألفي، تشريعات مكافحة جرائم الارهاب الإلكتروني: الأحكام الموضوعية والأنماط. ورقة عمل مقدمة في الندوة العلمية حول:

القوانين العربية والدولية في مكافحة الإرهاب. المنعقدة بالرياض خلال الفترة 15-17 أبريل 2013، ص ص 06-08.

17 Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, **Critical Information Infrastructure Security**. Berlin ; Springer, 2013, P 03-02.

18 Joanna F. DeFranco, **What Every Engineer Should Know About Cyber Security and Digital Forensics**. Boca Raton : CRC press, 2014. P40.

19 أيسر محمد عطية، مرجع سابق الذكر، ص 27.

20 بدر أحمد، الإرهاب الإلكتروني: أدواته وآثاره... أساليب الوقاية والعلاج. من موقع:

<http://baathparty.sy/site/arabic/index.php?node=552&cat=15369&>

21 وكالة الأنباء الجزائرية، الارهاب الإلكتروني: «الجزائر حريصة على حماية أمنها». من موقع:

<http://www.algpress.com/article-50021.htm>