

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول

### *The impact of information terrorism on the survival and future of nation- building.*

تاريخ الإرسال: 2021/12/14

تاريخ القبول: 2022/01/28

رفيق إيناس

جامعة محمد خيضر بسكرة

ines.rekik@univ-biskra.dz

#### ملخص:

ومكافحة الإرهاب الإلكتروني من خلال أعمالها ودوراتها وكذا إصدارها لقرارات واتفاقيات تضمن الحفاظ على كل من حقوق الدول والإنسان على السواء؛ ومن خلال ذلك تهدف هذه الورقة البحثية لمحاولة تحديد كافة الآليات الدولية والداخلية الكفيلة بضمان حق بقاء الدول وحمايتها من كافة الجرائم والتحديات الإلكترونية التي قد تتعرض لها. الكلمات المفتاحية: التطرف، الإرهاب، أمن الدول.

لا شك في أن الإرهاب قد أصبح يمثل أكبر تهديد للاستقرار الوطني والدولي على حد سواء، خاصة بعد اقترانه بالمجال الرقمي الافتراضي الذي يعتمد في الأساس على التسلسل إلى البنية التحتية الرقمية للدولة لعرقلة العمليات التنموية فيها وهذا ما جعله أكبر تهديد لأمن وبقاء الدول.

ونظرا لتلك الأهمية التي تحتلها دراسة موضوع التحديات الإلكترونية المستحدثة لأمن وبقاء الدول، اهتمت المنظمات الدولية هي الأخرى بتجريم and survival of States, international organizations have also been interested in criminalizing and combating cyber terrorism through their actions and sessions, as well as issuing resolutions and conventions to ensure the preservation of both state and human rights. This research paper aims to try to identify all international and internal mechanisms to ensure the survival of States and protect them from all cyber crimes and threats to which they may be exposed.

**Abstract:** There is no doubt that terrorism has become the greatest threat to both national and international stability, especially after it is associated with the virtual digital sphere, which relies mainly on infiltrating the state's digital infrastructure to disrupt the country's development processes, which has made it the greatest threat to the security and survival of states.

In view of the importance of studying the issue of the electronic challenges created for the security

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

**Keywords:** *extremism, terrorism, state security.*

لها الدول نجد تلك الصادرة عن الإرهاب الإلكتروني الذي ظهر في عدة بلدان في الآونة الأخيرة كعملية تطويرية للإرهاب التقليدي، حيث أصبح مفهوم الاستخدام غير المشروع للقوة في العلاقات الدولية لا يشمل فقط استخدام الأسلحة بكافة أنواعها، بل تعدى ذلك الحد لأن أصبح استخدام هجمات كمبيوتر واحد كقيل بتهديد بقاء وأمن والسلامة الإقليمية للدول.

لذلك أصبح موضوع الإرهاب الإلكتروني أحد المواضيع العامة التي تشغل فقهاء وباحثي العلوم القانونية والسياسية، ومن خلال هذا تهدف هذه الورقة البحثية لمحاولة تحديد كافة الآليات الدولية والداخلية التي استحدثتها الدولة الجزائرية الكفيلة بضمان حق بقاءها وحماية نظامها الأمني ووحدةها القومية الداخلية من كافة الجرائم والتنظيمات السببرانية والتهديدات الإلكترونية الخارجية التي قد تتعرض لها وهذا عن طريق الإجابة على الإشكالية التالية: ما مدى تأثير الإرهاب الإلكتروني على استقرار وأمن الدول؟ وسنقوم بالإجابة عن الإشكالية السابقة من خلال المحاور التالية:

المحور الأول: مفهوم الإرهاب الإلكتروني.

المحور الثاني: تأثير الجماعات الإرهابية على أمن وبقاء الدول:

المحور الثالث: إستراتيجية الأمم المتحدة ووكالاتها المتخصصة في مكافحة الإرهاب الإلكتروني.

المحور الأول: مفهوم الإرهاب الإلكتروني.

أثارت مسألة تحديد ماهية الإرهاب الدولي جدلا

### مقدمة:

شهد القرن العشرون العديد من التطورات التكنولوجية والتي طالت المجالات السلمية وغير السلمية، حيث شمل الجانب السلمي ذلك التطور في الاتصالات والمواصلات والراديو والتلفزيون والرسائل المكتوبة والاتصال عبر الأقمار الصناعية، والكمبيوتر بأجهاله المتعددة، وشبكة الاتصال العالمية، وكذلك المواصلات البرية والبحرية والجوية، وصولا إلى استخدام تلك التكنولوجيا في الأغراض العسكرية كثورة في الشؤون العسكرية والتطور في الأسلحة الخفيفة والمتفجرات، وأسلحة الدمار الشامل بأنواعها، وإن كانت أغلب الانجازات الحضارية التكنولوجية قد بدأت باستخدام الأسلحة، إلا أنه أضحى هناك مراحل وعمليات تقوم بها المجموعة الإرهابية باعتبارها أزر الملامح النظرية لتكنولوجيا الإرهاب.<sup>1</sup>

هذا وتعتبر الوسائل التكنولوجية أحد أهم الوسائل المساهمة في انتصار الجماعات الإرهابية على أمن الدول، وما يزيد من اتساع التحدي الذي يواجهه المختصون في القانون الدولي العام هو الغموض التي تكتنفه الهجمات السببرانية وعدم الاتفاق على تعريف محدد لها، في حين اجتهد الفقهاء في تحديد تعريف لهذا المصطلح ولأجل ذلك الغرض عرفها البعض على أنها تصرف يدور في عالم افتراضي قائم على استخدام البيانات الرقمية ووسائل الاتصال التي تعمل إلكترونيا، ومن ثم تطور هذا المفهوم ليشمل تحقيق أهداف عسكرية و أمنية مباشرة نتيجة اختراق مواقع إلكترونية حساسة.<sup>2</sup>

ومن بين مصادر الهجمات السببرانية التي تتعرض

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول — رقيق لينامس

لتحديد الأطراف هو السبب الرئيسي لعدم إمكانية الوصول إلى تعريف شامل للظاهرة. مثالا على التعريفات الملموسة المتأثرة بالمصالح المتضاربة هما وصف أفعال الفلسطينيين وأفعال إسرائيل. بينما كان هناك جدل كبير في الغرب حول كيفية استدعاء أفعال أرييل شارون، رئيس الوزراء الإسرائيلي والمفجرين الانتحاريين الفلسطينيين، لزعماء الدول الإسلامية الذين اجتمعوا في كوالالمبور في بداية أبريل 2002، من الواضح أن إسرائيل دولة إرهابية. لكن النظرة إلى الأعمال الفلسطينية أكثر غموضاً.<sup>4</sup>

إن كلمة الإرهاب في اللغة العربية مشتقة من الفعل رَهَبَ: بالكسر، يَرْهَبُ رَهْبَةً ورُهْبًا، بالضم، ورَهْبًا أي خاف، ورهب الشيء رهباً ورهبه: خافه. الرهبة: الخوف والفرع جمع بين الرغبة والرهبة. وفي حديث رضاع الكبير: فبقيت سنة لا أحدث بها رهبتة. قال ابن الأثير: هكذا جاء في رواية أي من أجل رهبتة، وهو منصوب على المفعول له. وأرهبه ورهبه: أي أخافه وفرعه. واسترهبه: استرعى رهبتة حتى رهبه الناس، وبذلك فسر قوله عز وجل: (واسترهبوهم وجاءوا بسحر عظيم)، أي أرهبوهم.<sup>5</sup>

### 1- التعريف الفقهي للإرهاب:

وبالنسبة للتعريف الفقهي للإرهاب الدولي فقد عرف الدكتور "إسماعيل صبري مقلد" بأنه: "الإرهاب الذي يتخطى الحدود السياسية للدول أو أنه الإرهاب الذي ينتج عنه ممارسة ردود فعل

كبيرا ضمن واقع العلاقات الدولية، بحيث لا يوجد تعريف للإرهاب متفق عليه بين دول العالم، لكن تم الإجماع على أن هناك فرق بين الإرهاب وبين المقاومة الشرعية التي تتم ضمن حركات التحرر.<sup>3</sup>

هذا ويعد الإرهاب الإلكتروني أحد التطورات العملية للإرهاب التقليدي والناجئ أساسا عن التطور العلمي وظهور الوسائل التكنولوجية، بحيث لم تعد فكرة الإرهاب مقترنة بالضرر المادي فقط، بل تعدى ذلك للضرر المعنوي أيضا ومنه لتحديد ماهية الإرهاب الإلكتروني وُجب التطرق لتعريفه، وأوجه الاختلاف بينه وبين مايتداخل معه من مصطلحات، وكذلك موقف القانون الدولي من ظاهرة الإرهاب الإلكتروني، لنقوم بعد ذلك إسقاط كل ذلك على ظاهرة إرهاب الدولة الإلكتروني.

### أولا- تعريف الإرهاب:

يعتبر تعريف الإرهاب العنصر الحاسم في تشكيل توجهات السياسة والقانون تجاه بلدان العالم، حيث تتطلب أخلاقيات العلاقات الدولية أن أي وصف محايد للظاهرة سيتم تطبيقه ومع ذلك، كما هو واضح إلى حد ما، فإن هذا نادراً ما يحدث في الواقع التطبيقي حيث أن مسألة تعريف الإرهاب من أفضل الأمثلة للميل إلى تضمين اهتمامات معينة في الأوصاف التي تبدو محايدة ما هو شرعي أو غير شرعي قانونا.

وربما يكون ربط المفهوم نفسه بالمصلحة المحددة

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

الدول وتمثل في الأعمال الإرهابية السيبرانية أو بما يعرف في الساحة الفقهية الدولية بـ "الإرهاب الإلكتروني الدولي"، حيث أضحت بعض الدول والمنظمات الإرهابية تستغل النظام الإلكتروني للدولة لأجل تهديد كيائها واستقرارها الأمني، كون أن الواقع التكنولوجي الذي طغى على العلاقات الدولية يفرض على الدولة التوجه نحو عصريته نظامها الإداري الداخلي والدولي والاعتدال فقط على الشبكة العنكبوتية في مختلف علاقاتها الدولية، ونتيجة لذلك فإن اختراق النظام المعلوماتي الإلكتروني للدولة كليل بتدمير اقتصادها وكيانها وحتى استقرارها.

### 2-التعريف العملي للإرهاب:

لقد اهتم العلماء بوضع تعريف ميداني للإرهاب، وأجمعوا على أن الظواهر الإرهابية أصبحت خطراً داهماً يهدد الأمن والسلم الدوليين، وظهر في ذلك ثلاث اتجاهات:

فيرى البعض أن الإرهاب يعتبر من الظواهر الاجتماعية المختلفة الأبعاد التي يختلط فيها العنصر النفسي بالعنصر الاجتماعي والثقافي والتاريخي والأمني والسياسي، وهذه العناصر تتميز بالغموض لذلك يعتقد هذا الاتجاه بعدم إمكانية وضع تعريف ميداني للإرهاب.

أما الاتجاه الثاني فيزعم بأنه يمكن تعريف الإرهاب كفعل مادي فقط يقوم به الإرهابيون تجاه سلامة أو أمن المواطنين أو المنشآت أو المرافق المرتبطة

وأصداء دولية قد يتسع تأثيرها أو يضيق بحسب الأحوال"، كما عرفه الدكتور "أحمد بلال عز الدين" بأنه: "استراتيجية عنف منظم ومتصل من خلال جملة من أعمال القتل والاختطاف وخطف الطائرات واحتجاز الرهائن وزرع المتفجرات، وما شابه ذلك بقصد أهداف سياسية".<sup>6</sup>

نلاحظ أن التعريف الأول لم يشمل كافة أنواع الإرهاب بل خصص ذلك الذي يتعدى حدود الدولة، ونرى أيضاً بأن الأعمال الإرهابية الدولية لا يمكن ربطها بالنطاق الإقليمي للدولة، بل المعيار الذي يمكن تصنيفه على أساسه العمل الإرهابي بأنه دولي هو معيار النتائج أو الآثار الناتجة عن تلك الأعمال الإرهابية كذلك لا يمكن ربط مصطلح الإرهاب عند تصنيفه على هذا الأساس اعتماداً على معيار ردود الأفعال الدولية حيث نجد أن الممارسات الواقعية الدولية يستند على المصلحة كأساس لتحديد إذا ما كانت الأفعال المرتكبة تعد إرهاباً دولياً وأهم مثال يمكن الاعتماد عليه في سبيل هذا هو الأفعال الصهيونية المرتكبة في الأراضي المحتلة الفلسطينية والتي اعتبرها فقهاء القانون الدولي على أنها أعمال إرهابية وفقاً لقواعد القانون الدولي.

أما بخصوص التعريف الثاني الذي قدمه الدكتور "أحمد بلال عز الدين" فنجد بأنه لم يواكب التطورات التي يشهدها المجتمع الدولي خاصة في المجال الإجرامي، حيث أصبحت المنظمات الإرهابية تعتمد على وسائل أشد خطورة من القتل والاختطاف والطائرات لأجل تهديد بقاء

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

بالدولة أو بالأفراد دون النظر إلى الدافع وراء ذلك الفعل. لكن هذا الاتجاه قد يؤدي للخلط بين مصطلح الإرهاب وبعض الظواهر المشابهة كالحرب الدولية والجريمة الدولية والحروب الأهلية الداخلية، والتطرف وكذلك حرب العصابات.

والموجّهة ضد أي الدولة والمقصود منها أو المحسوب خلق حالة من الرعب في عقول أشخاص معينين، أو مجموعة من الأشخاص أو عامة الناس. ومع ذلك، فإن اتفاقية عصبة الأمم لمنع ومعاينة الإرهاب لم تلتقى دعماً كافياً لدخولها حيز التنفيذ كما لم تتم إعادة النظر فيها عندما تمت كتابة ميثاق الأمم المتحدة 1945.<sup>9</sup>

وقد عرفته المادة الأولى من اتفاقية جنيف 1937 المتعلقة بـ" قمع ومعاينة الإرهاب" على أنه: "الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف أو تقصد خلق حالة من الرعب في أذهان أشخاص معينين، أو مجموعة من الأشخاص.

10

كذلك حاول مجلس الأمن تعريف الإرهاب حيث اعتبره بأنه: "كل عمل جرمي ضد المدنيين بقصد التسبب بالوفاة أو بالجروح البليغة أو أخذ الرهائن من أجل إثارة الرعب بين الناس أو إكراه حكومة أو منظمة دولية للقيام بعمل ما أو الامتناع عنه، وكل الأعمال الأخرى التي تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالإرهاب والتي لا يمكن تبريرها بأي اعتبار سياسي أو فلسفي أو إيديولوجي وعرقي أو ديني"<sup>11</sup>.

وبالرغم من أن هذا التعريف الصادر عن مجلس الأمن بخصوص الإرهاب الدولي إلا أنه قد أنتقد لعدم شموله للأنواع الجديدة للإرهاب كالإرهاب الرقمي غير أنه يعتبر ملزم لكافة دول العالم بما فيها

وفيما يتعلق بالرأي الثالث فيعتبر بأنه يمكن تعريف الإرهاب على أنه فكر إيديولوجي، حيث يشترط لتوافر الجريمة الإرهابية وجود فكر معين إيديولوجي من رواء أي جريمة إرهابية؛ فهم يربطون الإرهاب بالطابع السياسي أو العقائدي.<sup>7</sup>

### 3- جهود المنظمات الدولية العالمية والإقليمية

#### لتعريف الإرهاب.

واجمت المنظمات الدولية صعوبات كبيرة في محاولة منها لتعريف الإرهاب الدولي، والتي حالت دون الاتفاق على تعريف موحد وقد تعددت الآراء حول الأسباب التي أدت إلى هذه الصعوبات، حيث يرجعها البعض إلى تشعب الإرهاب وتعدد أشكاله وأهدافه وتناقضها، في حين يرجعها البعض إلى ممارسات الدول القوية، حيث تتخذ هذه الأخيرة من الإرهاب كطريقة لإخفاء العديد من الممارسات الإرهابية التي تقوم بها. وكذلك يندرج ضمن تلك الصعوبات محاولات بعض الدول لإدراج نضال الشعوب من أجل تحقيق تقرير مصيرها اعتماداً على القوة ضمن الأعمال الإرهابية.<sup>8</sup>

كان لعصبة الأمم في عام 1937 محاولة لتعريف "الأعمال الإرهابية" بأنها جميع "الأعمال الإجرامية

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

الدول غير الأعضاء في الأمم المتحدة وهو ما يعبر عن تطور تطور محسوس وهام في مسألة تعريف الإرهاب الدولي.

2 - اضطراب أي مرفق أو خدمة أساسية أو خلق حالة طوارئ.

3- إحداد تمرد عام في الدول.<sup>13</sup>

### ثانيا- تعريف الإرهاب الإلكتروني:

يتميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية بقصد الإطاحة بالنظام وتهديد البنية التحتية المعلوماتية للدول. وهو يشمل بذلك على عناصر هي: العمل الإرهابي والتنظيم، إضافة إلى العالم الافتراضي الذي يعتمد على التمثيل الرمزي والزائف للمعلومات.

ويعرف الإرهاب الإلكتروني بأنه: " العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى أصناف العدوان وصور الفساد، وبذلك يعتمد الإرهاب الإلكتروني أساسًا على استخدام الإمكانيات التقنية والعلمية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من إلحاق الأضرار بمختلف الأفراد والجماعات والدول، ومثال على ذلك فقد قدر مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت كلفة إصلاح الأضرار التي تسببها الفيروسات المعلوماتية بنحو 12 مليار

أما إقليميا تعد الاتفاقية العربية لقمع الإرهاب الصادرة عام 1998 عن جامعة الدول العربية، أول اتفاقية عربية تتضمن تعريف الإرهاب، من خلال المادة الأولى/2 والتي ورد فيها على أنه: "كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أغراضه، يقع تنفيذ المشروع إجرامي فرديا أو جماعيا، ويهدف إلى نشر الرعب بين الناس، أو ترويعهم، بإيذائهم أو تعريض حياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر."<sup>12</sup>

وبخصوص اتفاقية منظمة الوحدة الإفريقية لمنع الإرهاب ومحاربتة لسنة 1999 فقد عرفت العمل الإرهابي في المادة الأولى منها وحددته بأنه " كل فعل ينتهك القوانين الجنائية لدولة طرف، ويعرض للخطر حياة أو سلامة جسد أو حرية أي شخص أو أي عدد من الأشخاص أو يسبب لهم الأذى البالغ أو الموت، أو يلحق أضرار بالمتلكات الخاصة أو العامة أو بالبيئة أو التراث الثقافي أو الموارد الوطنية، ويكون القصد منه:

1 -تهديد أو إكراه أو إجبار أو إرغام أي حكومة أو جهاز أو مؤسسة أو مرفق عام على تنفيذ فعل أو الامتناع عن تنفيذه، أو تبني موقف معين أو تركه

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق لينامس

دولار أمريكي سنويًا.<sup>14</sup> من خلال هذه الطريقة يتم توسيع العناصر الإرهابيين وتجنيدهم المزيد من الجنود.<sup>15</sup>

### المحور الثاني: تأثير الجماعات الإرهابية على أمن الدول.

تمثل خطورة الجماعات الإرهابية الإلكترونية في إمكانية استخدامها للأنظمة والشبكات المعلوماتية لتدمير البنية التحتية الإلكترونية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى، وهناك ما يشير إلى إمكانية انهيار البنية التحتية للأنظمة والشبكات المعلوماتية في العالم كله، وليس في بعض المؤسسات والشركات الاقتصادية الكبرى أو بعض الدول المستهدفة.

فالإرهاب الإلكتروني أصبح خطراً يهدد العالم بأسره نتيجة سهولة استخدامه للسلح الرقمي فمثلاً تسبب قطع الكيبل البحري الذي يربط أوروبا بالشرق الأوسط في نهاية شهر يناير عام 2008، وما أعقبه من انقطاع كيبل آخر القريب من ساحل دبي وخليج عمان، حيث قدرت الخسائر المتولدة من ذلك والتي لحقت بقطاع الاتصالات والتعاملات الإلكترونية بمئات ملايين الدولارات.<sup>16</sup>

### أولاً-مظاهر تهديد الإرهاب الإلكتروني للدول:

يعتمد الإرهاب الإلكتروني أثناء قيامه بالعمليات الإجرامية المتسلسلة على أجهزة وبرامج الحاسوب والشبكات المعلوماتية التي تنتقل فيه البيانات الإلكترونية، ونظراً لارتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عن طريق الأقمار الصناعية

### ثالثاً- أهداف الإرهاب الإلكتروني.

يسعى الإرهاب الإلكتروني إلى تحقيق جملة من الأهداف غير المشروعة ويمكننا بيان أبرزها:

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 بالبنية التحتية للمعلوماتية الأساسية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة.

كذلك يهدف الإرهاب الإلكتروني إلى تهديد السلطات العامة للدول والمنظمات الدولية وابتزازها، والانتقام من الخصوم وجمع الأموال والاستيلاء عليها، مستعيناً في ذلك على بيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، في التعرف على الأشخاص 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

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

وشبكات الاتصال الدولية. فقد زادت الخطورة

الإجرامية للجماعات الإرهابية بتوظيفها تلك التقنية.<sup>17</sup>

وتتم عملية الاختراق الإلكتروني لبيانات الدول عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكنشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي. أما تدمير المواقع فهو الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (PC-Server) أو مجموعة نظم مترابطة شبكياً (Intranet) بهدف تخريب نقطة الاتصال أو النظام.<sup>19</sup>

كل هذه العمليات والهجمات تدعم مسبقاً بتدريبات خاصة من خلال معسكرات تدريبية سرية تنشأ لهذا الغرض، وما تتميز به تلك المعسكرات أنها ذات صبغة تقنية إلكترونية تعتمد على التدريب والتخطيط والتنفيذ الخفي، وهذا ما ساهم في زيادة خطورة الإرهاب الإلكتروني على أمن وبقاء الدول.<sup>20</sup>

### ثانياً- آثار الإرهاب الإلكتروني على الدول:

يقوم الإرهاب الإلكتروني عادة بتوجيه مختلف الأسلحة الإلكترونية للهجوم على الأنظمة المرتبطة

وتتكون البنية التحتية لتطوير قدرات الأسلحة الإلكترونية من جهاز كمبيوتر، أو هاتف محمول متصل بالإنترنت وسلسلة من البرمجيات الخبيثة وبرامج التجسس وما إلى ذلك. وتتطلب فقط هذه الأسلحة مهارات نادرة لإنتاجها وتحتاج فقط لمنصات بسيطة لإطلاقها وغير مرئية تتمثل في جهاز كمبيوتر ثابت أو محمول، موقع على شبكة الإنترنت (البريد الإلكتروني)، محرك للبحث، شبكة اجتماعية، خادم افتراضي أو مادي أو "سحابات بيانات"، تتجمع كلها في الكمبيوتر (جهاز الإطلاق). ويمكن تصميم الأسلحة الإلكترونية من أي مكان، ومن قبل أي شخص مثل القراصنة والجماعات الإرهابية، أو حتى دول متصارعة.<sup>18</sup>

هذا ويساعد البريد الإلكتروني كأحد البرمجيات المساعدة على التواصل بين مختلف الجماعات الإرهابية وتبادل المعلومات فيما بينهم، بل وأثبتت الدراسات العملية أن الكثير من العمليات الإرهابية التي حدثت خلال السنوات الأخيرة كان للبريد الإلكتروني فيها دور كبير في تبادل المخططات والأفكار بين القائمين بالعمليات الإرهابية. كذلك بالنسبة للمواقع الإلكترونية التي سهلت على الجماعات الإرهابية توسيع أنشطتهم لأبعد الحدود من خلال الاعتماد عليها في التخطيط والتنسيق للعمليات الإرهابية الهادفة لاختراق مختلف الأنظمة

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق لينامس

يستخدمها مجرمو الإنترنت لكسب الأموال، فإن عدد وتأثير هذه الهجمات يتزايد من عام لآخر وهو ما جعل قضية حماية المستخدمين أمراً أولوياً لدى الشركات.

كما أكدت شركة "كاسبرسكي" الرائدة في مجال الأمن المعلوماتي أن مجموعة من "الهكرز" تمكنوا من السيطرة على حسابات في مصارف عالمية، وسرقة نحو مليار دولار، إذ استخدموا تقنيات معقدة من أجل الوصول للحسابات، واستغل "الهكرز" 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.<sup>23</sup>

2- تهديد النظام السياسي للدول: 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 يهدد أمن الدول، كما تهدد 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 لمجلهم على إتيان أفعال معينة

بالفضاء الإلكتروني للدولة المعنية، ويستخدم في هذا الأسلحة الإلكترونية كأسلحة غير مرئية ولديها القدرة على التدمير الشامل لنظام الدولة بدون تهديد حقيقي للبنية التحتية لحياة الإنسان وبذلك عرف الهجمات الإلكترونية على أنها: " أعمال تقوم بها جماعات معينة بهدف اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".<sup>21</sup>

وتتمثل مختلف آثار الإرهاب الإلكتروني على الدول في النقاط التالية:

1- تهديد النظام الاقتصادي للدول: إن اختراق البنوك الداخلية للدول والتلاعب بمختلف الأرصدة الإلكترونية للدول تؤثر على ضمان الاستقرار الاقتصادي للدول كتحويل الجماعة الإرهابية الأرصدة المالية باستخدام بيانات البطاقات الائتمانية وسرقتها وكذلك اختراق نظام تحويل رؤوس الأموال الإلكتروني بين مختلف البنوك العالمية.<sup>22</sup>

وقد مُنيت عدد من الشركات والمصارف العملاقة بخسائر اقتصادية فادحة نتيجة القرصنة الإلكترونية التي واجهتها. فحسباً أشارت أحدث دراسة أجرتها مؤسسة B2B International وشركة كاسبرسكي لاب، والتي أعلنت عنها في الخامس عشر من أبريل 2015 فإن 25% من الشركات في منطقة الخليج تعتبر هجمات (DDoS) أحد أكبر ثلاثة تهديدات تواجه الشركات في المنطقة. و باعتبارها أحد أهم التقنيات الشائعة التي

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق لينامس

يخططون لاقتوافها.

مارس 2018، للتعرف على أكثر الدول العربية تعرضاً للهجمات الإلكترونية، وقد أكدت نتائج الدراسة بأن المملكة العربية السعودية تأتي في صدارة الدول العربية، محتلة المركز 17 عالمياً، وتبعها بعد ذلك الإمارات العربية المتحدة في المرتبة 18 عالمياً، ثم الجزائر في المرتب الثالث عربياً و 24 عالمياً بعد كل من المملكة العربية السعودية والإمارات العربية المتحدة من حيث التعرض للهجمات الإلكترونية.

كما أكد مركز الأمن السعودي في آخر إحصائيات له -إلى غاية كتابة هذه الأسطر- أنه في الربع الأخير من عام 2017 بنحو 7% مقارنة بالربع الثالث لنفس السنة، قد استهدفت أغلب التهديدات جهات حكومية وقطاعي الطاقة والاتصالات. أما الجزائر فقد صنفت من بين أكثر الدول العربية تضرراً من الهجمات الإلكترونية التي تعرضت لها، حيث يتعرض 44% من مستخدمي الانترنت في الجزائر لهجمات إلكترونية وهي النسبة الأعلى عالمياً.<sup>25</sup>

**ثالثاً- أسباب تمكن الإرهاب الإلكتروني من تهديد النظام الإلكتروني للدول.**

في الواقع أن وقوع عملية تدمير الإرهاب للمواقع والأنظمة الرئيسية الإلكترونية للدول تعود لعدة أسباب ساهمت في زيادة عدد تلك الهجمات وتطور مخاطرها، ولعل من بين أهم الأسباب هو ضعف الكليات السرية التي تستخدمها الدول

مثلا في عام 2010 ظهر ما عُرف باسم "إعصار ويكيليكس" إذ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم. وفي مارس 2014 هاجمت مجموعة "سايربريوت" الأوكرانية المواقع الإلكترونية لحلف الناتو، ما أدى إلى تعطيل مواقع الحلف لعدة ساعات". كما أعلن الكرملن أن قرصنة حاسوب شنوا هجوماً "عنيفاً" على موقع الرئاسة الروسية، وعطلوا العمل بموقع البنك المركزي الروسي. وأقر مفتش وحدة الجرائم الإلكترونية الأمريكي في أوت 2014، بأن قرصنة أجنبي تمكنوا من اختراق حاسبات تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية ومؤخراً أكدت صحيفة نيويورك تايمز في تقرير لها في 26 إبريل 2015 أن قرصنة روسيين اطلعوا 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 فيه يتواصلون يومياً مع أوباما، ومن خلال هذا الأرشيف تمكن القرصنة من قراءة رسائل تلقاها أوباما وهذا ما يهدد الأمن القومي الأمريكي.<sup>24</sup>

كما قامت شركة "فوريس الشرق الأوسط برصد وتتبع بيانات خريطة كاسبرسكي يوم الخميس 22

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

أنشئت بموجب القانون 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37، 32، و 40 من ق.إ.ج.ج. وتتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 2006/01/05. بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04.

2- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: والتي أنشئت بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. وتعمل الهيئة الوطنية على تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقائية، والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية، في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

3- المعهد الوطني للأدلة الجنائية وعلم الجرائم:

للدخول للأنظمة الخاصة بها، حيث في بعض الأحيان تستخدم أرقام أو حروف تسهل حفظها، كذلك نجد وضع برامج حماية للموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج والتي تعمل على التنبيه عند وجود حالة اختراق له.

كذلك نجد بأن عدم قيام الدول بالتحديث المستمر لأنظمة التشغيل لأجهزتها تساهم في الكثير من الأحيان في اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية. أو عدم القيام بالنسخ الاحتياطي للملفات والمجلدات الموجودة على أجهزة الدولة، يزيد من خطر احتمال فقدان بيانات هامة تعتمد عليها الدولة أثناء قيامها بمختلف مهامها الداخلية وكذلك في علاقاتها الخارجية مع كافة أشخاص القانون الدولي، هذا وبعد عام 2002 أكثر الأعراف اختراقاً فقد تضاقت فيه حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في مزودات الانترنت وانتشار الكثير من الفيروسات.<sup>26</sup>

لأجل هذا قامت الدولة الجزائرية باستحداث العديد من المراكز والهيئات التي تعمل على مكافحة الإرهاب الإلكتروني والتخفيف من مرتبتها الدولية والعربية باعتبارها تحتل المركز الثالث عربيا من حيث عمليات القرصنة الإلكتروني التي تتعرض لها، وتمثل هذه المراكز في:

1- الهيئات القضائية الجزائية المتخصصة: والتي

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

أولاً- جهود منظمة الأمم المتحدة في مكافحة الإرهاب الإلكتروني.

اهتمت دول العالم لمكافحة الإرهاب الإلكتروني تحت غطاء الأمم المتحدة نظراً لخطورة هذه المسألة على أمن وبقاء الدول، لذلك تم سن العديد من الاتفاقيات الدولية كاتفاقية فينا عام 1988 والتي حثت دول العالم على الدخول في اتفاقيات ثنائية ضد الإرهاب الإلكتروني. وبعدها تم عقد المؤتمر الثامن للأمم المتحدة في كوريا 1990 للنظر في نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية واقترح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة. كذلك أصدرت الجمعية العامة للأمم المتحدة العديد من القرارات التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداماً غير سلمي، كقرار الجمعية العامة في 19 ديسمبر 2001 بشأن إرساء الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا الإعلام والاتصال في الأعمال الإجرامية.<sup>28</sup>

وكذلك القرار رقم 49 لعام 2012 في دورتها رقم 67 والمتعلق بتسخير تكنولوجيا المعلومات والاتصالات لأغراض التنمية، كما أشادت الجمعية العامة في قرار آخر بضرورة تكاتف جهود الدول لمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية أو إرهابية وهي تعد محاولة أخرى للقضاء بكافة الأشكال على الإرهاب الإلكتروني الذي أضحي يهدد بقاء الدول.<sup>29</sup>

ويتكون من 11 دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاینات.

4-المديرية العامة للأمن الوطني: وتعمل على التصدي للجريمة الإلكترونية من عدة جوانب ومنها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعوية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الإلكترونية.<sup>27</sup>

المحور الثالث: استراتيجية الأمم المتحدة ووكالاتها المتخصصة في مكافحة الإرهاب الإلكتروني.

اهتمت منظمة الأمم المتحدة ووكالاتها المتخصصة بمسألة الإرهاب الإلكتروني كونه أضحي يهدد أمن وكيان الدول وهذا من خلال مختلف الأعمال التي تقوم بها والمجسدة في شكل قرارات ودوريات تصدرها، وفي هذا الصدد سنقوم بالتطرق لكل من جهود منظمة الأمم المتحدة في مكافحة الإرهاب الإلكتروني، وكذلك لدور الاتحاد الدولي للاتصالات في هذا الخصوص كأحد نماذج الوكالات المتخصصة في مكافحة الإرهاب الإلكتروني.

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق لينامس

واستراتيجيات تم اتباعها من خلال عدت قرارات تم إصدارها في هذا الخصوص، بهدف تحقيقها مبتغاها الأساسي وهو الحفاظ على السلم والأمن الدوليين.

### ثانيا- دور الاتحاد الدولي للاتصالات في مكافحة الإرهاب الإلكتروني:

يتم الاتحاد الدولي للاتصالات\* -وكالة متخصصة تابعة للأمم المتحدة- بتكنولوجيا الإعلام والاتصال، ويعتبر بأن من أهدافه الأساسية ضمان الأمن السيبراني<sup>31</sup>. فمن بين المهام التي يضطلع عليها الاتحاد تعزيز التعاون الدولي للخدمات الهاتفية السلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير إمكانات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية، كما يقوم الاتحاد بتقديم التوصيات الخاصة والدراسات الفنية المتخصصة في الاتصالات اللاسلكية وجمع المعلومات ونشرها من أجل بناء قدرات الدول الأعضاء - لاسيما الدول النامية- لتنسيق الاستراتيجيات الوطنية وحماية البنية التحتية للشبكات ضد المخاطر من خلال التوعية، والتقييم الذاتي، وبناء القدرات وتوسيع نطاق المراقبة والإنذار، وقدرات الاستجابة للحوادث للدول والجهات المعنية.<sup>32</sup>

وقد أصبحت قضايا الأمن المعلوماتي أحد المواضيع الهامة التي يتخصص في معالجتها، بما فيها الإرهاب الرقمي، ويتجسد ذلك من خلال مختلف

أما بالنسبة لمجلس الأمن فقد اهتم هو الآخر بمسألة مكافحة الإرهاب الرقمي من خلال عدة قرارات أصدرها في هذا الخصوص أهمها القرار رقم 1373 الصادر بتاريخ 28 سبتمبر 2001 الذي يعد أول قرار دولي يهتم بالإرهاب المعلوماتي الرقمي، حيث بموجبه تم تأسيس لجنة خاصة بالإرهاب تتكون من 15 خبيرا دوليا في مجال مكافحة الإرهاب من بينه الإرهاب الإلكتروني، كذلك خلال عام 2004 من خلال القرار رقم 1535 قام بإنشاء المديرية التنفيذية للجنة مكافحة الإرهاب، وكذلك القرار رقم 1822 الذي أشاد بضرورة التعاون بغرض مكافحة استغلال الإرهاب للتكنولوجيا في أغراض إرهابية، وكذلك القرار رقم 2255 الصادر في 2015، والذي أعرب من خلاله المجلس عن قلقه من تزايد استعمال الإرهاب للتكنولوجيا في جرائمه الإرهابية.

كذلك أكد عام 2017 من خلال القرار رقم 2395 لضرورة التعاون مع المديرية التنفيذية لأجل مكافحة استخدام الإرهابيين للإنترنت ووسائل التواصل الاجتماعي للترويج لأهدافهم الإرهابية.<sup>30</sup>

وهو ما يعتبر تأكيدا دائما من طرف المجلس على اهتمامه المستمر بقضية الإرهاب السيبراني. وبذلك تتضح الجهود السامية لمنظمة الأمم المتحدة في سبيل الاهتمام بموضوع الإرهاب الرقمي والمنبثق عن الإرهاب التقليدي، عن طريق خطط

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق لينامس

التقارير التي أصدرها والمتعلقة بمعايير الأمن المعلوماتي و التكنولوجيا في المجال الرقمي.

حيث أصدر الاتحاد الدولي للاتصالات خلال عام 2007 دليل الأمن السيبراني للبلدان النامية

والذي اشتمل على مجموعة الموارد اللازمة لتحقيق الأمن السيبراني، وتفادي مختلف الهجمات عبر الفضاء السيبراني كندمير أو سرقة بيانات حساسة للدول، أو كسر حماية البرمجيات، والتنصت الإلكتروني أو التجسس على أسرار الدولة، والتي تهدف غالباً لتهديد أمن وسلامة الدول.

وقد حدد الدليل مجموعة من الأعمال والأنشطة التي قام بها الإتحاد لمكافحة التهديدات السيبرانية والرسائل الاقتصادية وخاصة الإرهاب الرقمي المهدد لبقاء وأمن الدول والمدرجة في عدة مقررات من بينها:

**1. WTDC (2006 - )**  
الاستراتيجيات الإلكترونية وتطبيقات تكنولوجيا المعلومات والاتصالات: تهدف خطة العمل هذه إلى توفير فهم مشترك بين الدول لمسائل الرسائل السيبرانية، والتدابير المضادة التي يمكن اتخاذها ضد خطر هجمات الإرهاب الرقمي، ومحاولة الحد منها من خلال تبادل الخبرات الناجمة في هذا المجال بين الدول.

**2. المؤتمر العالمي لتنمية الاتصالات - 2006(WTDC-06) القرار 45 - آليات**

لتعزيز التعاون في مجال الأمن السيبراني، بما في ذلك مكافحة الرسائل الاقتصادية. الذي يكلف مكتب اتصالات التنمية بتنظيم اجتماعات للدول الأعضاء لمناقشة سبل تعزيز الأمن السيبراني.

**3. المؤتمر العالمي لتنمية الاتصالات - 2006 الملحق 2 بالقرار 2 - لجنة الدراسات 1**  
لقطاع تنمية الاتصالات المسألة 22 - تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني. والذي يهتم أساساً يبحث أفضل الممارسات من أجل إنشاء وتشغيل وسائل المراقبة والإنذار والاستجابة للحوادث والإصلاح، التي قد تستخدمها الدول الأعضاء من أجل بناء قدراتها الوطنية في هذا المضمار.

**4. القرار 130 - تعزيز دور الإتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات:** كذلك يهتم هذا القرار بمسألة تعزيز الأمن التكنولوجي من خلال انجاز بعض المشاريع المشتركة بين الدول من جهة و لجان قطاع التنمية العاملة في المجال الرقمي من جهة ثانية، لأجل تبادل الخبرات والمعلومات اللازمة لتفادي الهجمات السيبرانية المهددة للدول.<sup>33</sup>

كما تم في المؤتمر الإقليمي حول الأمن الإلكتروني في قطر خلال عام 2008 دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن الإلكتروني وحماية البنية التحتية الحرجة للمعلومات، والتي تعد بمثابة خطة أولى في سبيل التصدي للتحديات التي تواجهها

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

جراء اتصالها بتكنولوجيا الإعلام والاتصال.<sup>34</sup> ضمان استمرار الجماعة الإرهابية، وقد ساهمت

الوسائل التكنولوجية في تخفيف أعباء وتكاليف العمليات الإرهابية إذ يعد وجود جهاز كمبيوتر ثابت أو نقل ومجموعة من البرمجيات كافيًا لتهديد أمن وسلامة الدول.

وتتجسد آثارا الإرهاب الإلكتروني على أمن الدول وسلامتها الإقليمية من خلال مختلف التهديدات السياسية والاقتصادية الكفيلة بتدمير بعض أو جزء من البيانات الرقمية المهمة للدول، وهذا ناتج أساسا عن ضعف البرمجيات المعتمدة من طرف الدول والتي تعتمد عليها في محامها الوطنية والدولية اليومية.

وتحتل الجزائر المركز الثالث عربيا من حيث عدد عمليات السطو والقرصنة الإلكترونية التي تتعرض لها وهذا يجعلها في موقف حرج بين تحدي مواكبة التطور التكنولوجي الذي أصبح ضرورة حتمية من جهة، والآثار السلبية لتلك التكنولوجيا والمتجسدة في الخسائر الضخمة الناتجة عن عمليات السطو الإلكتروني، ولهذه الأسباب اهتمت الدول بإصدار جملة من المراكز التي تعمل أساسا على مكافحة عمليات القرصنة الإلكترونية.

وفي الأخير تقدم من خلال هذه الورقة البحثية البسيطة عدة توصيات تتجسد في:

1. ضرورة تفعيل مختلف الأجهزة الفنية الكفيلة بحماية أنظمة الدولة من

**الخاتمة:**  
تبين لنا من خلال هذه الدراسة أنه أصبح الإرهاب الإلكتروني هاجس يهدد بقاء الدول من خلال مختلف هجمات الجماعات المتطرفة عبر الانترنت، وهذا من خلال مختلف الوسائل التكنولوجية الحديثة التي تعتمد على عصري العتاد والبرمجيات بغرض الفتك بمختلف الأنظمة الإلكترونية للدول.

هذا ولم يتفق الفقهاء على تعريف واضح للإرهاب الإلكتروني، ربما هذا ناتج أساسا عن الاختلاف في تحديد تعريف الإرهاب التقليدي، لكن ما تم التوافق فيه هو عنصر التكنولوجية بحيث يعد إرهابا إلكترونيا كل جماعة تعتمد على التخطيط والتنسيق من خلال العتاد والبرامج التكنولوجية بغرض تهديد وخرق الأنظمة الداخلية للدول والمنظمات، هذا ولم يخلص القانون الدولي لتعريف واضح للإرهاب التقليدي ناهيك عن الإرهاب الإلكتروني، بالرغم من كل القرارات الدولية الصادرة في هذا الشأن سواء من طرف الأمم المتحدة أو المنظمات الدولية الأخرى.

ويعمل الإرهاب الإلكتروني لبلوغ جملة من الأهداف الاستراتيجية والتي أهمها التجسس على أنظمة مختلف الدول والاستيلاء على مبالغ مالية ضخمة من خلال الأرصاد المجمع لدى مختلف البنوك أو من مختلف البطاقات الائتمانية، هذا لأجل

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

<sup>2</sup> أحمد الفتلاوي: الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، 2016، ص 215.

<sup>3</sup> عادل صادق: الإرهاب الإلكتروني في الصراع الدولي، دار الكتاب الحديث، مصر، 2015، ص 95.

<sup>4</sup> Asta Maskaliunaité: **Defining Terrorism in the Political and Academic Discourse**, Balbic Defence Review, n° 8, vol 2, 2002, P36.

<sup>5</sup> ابن المنصور: لسان العرب، ط3، مج1، دار صادر، بيروت، لبنان، د.س.ن، ص 436.

<sup>6</sup> العزاوي: موقف القانون الدولي من الإرهاب والمقاومة المسلحة، دار الحامد للنشر والتوزيع، عمان، الأردن، ص 29.

<sup>7</sup> يوسف ملا جمعة الياقوت: الإرهاب، ب.د.ن، 2010، ص 22-18.

<sup>8</sup> حسين العزاوي: المرجع السابق، ص 29.

<sup>9</sup> Alex Schmid: **Terrorism - The Definitional Problem**, Case Western Reserve Journal of International Law, vol 36, issue2, 2004, P385.

<sup>10</sup> المادة الأولى من اتفاقية جنيف المتعلقة بـ" قمع ومعاقة الإرهاب"، الصادرة خلال عام 1937.

<sup>11</sup> قرار مجلس الأمن الدولي رقم 1566، جلسة رقم 5053، الصادر بتاريخ 8 أكتوبر 2004.

<sup>12</sup> الاتفاقية العربية لمكافحة الإرهاب: الصادرة خلال عام 1998. المادة 01.

<sup>13</sup> عبد الرحيم بن بوعيدة: الاتفاقيات الدولية المتعلقة بمكافحة الإرهاب في مجال الطيران المدني، مقالة متاحة على الرابط التالي: <https://www.iasj.net>، تاريخ الإطلاع 2018/03/29 على الساعة 21:30، ص 5.

<sup>14</sup> علي عدنان الفيل: الإرهاب الإلكتروني، مجلة الجامعة الخليجية، قسم القانون، العدد 2، جامعة الموصل، العراق، 2010، ص 19.

<sup>15</sup> أيسر محمد عطية: دور الآليات الحديثة للحد من الجرائم المستحدثة - الإرهاب الإلكتروني وطرق مكافئته- مقالة

الاختراق، وكذلك العمل على وضع أرقام سرية معقدة لتلك الأنظمة الرقمية، تتكون من رموز وأشكال وأرقام وأحرف بالدمج فيما بينها كطريقة لتقليل القرصنة الإلكترونية.

2. كذلك يجب على الدول وضع نسخ احتياطية للملفات الهامة كسبيل لضمان عدم فقدانها في حالة ما تم خرق أو إتلاف النسخ الأصلية.

3. ضرورة إيجاد نظام قانوني دولي موحد ضمن المنظومة القانونية للأمم المتحدة في سبيل مواجهة ومكافحة الإرهاب الإلكتروني من خلال معاهدة دولية جماعية، وكذلك تعزيز التعاون الدولي في هذا المجال.

4. كذلك نوصي بضرورة تفعيل مختلف القرارات الدولية التي تبنتها مختلف المنظمات والأجهزة العالمية كسبيل للتصدي للإرهاب الإلكتروني، وهذا عن طريق إنشاء شرطة دولية إلكترونية تعمل على التصدي لعمليات القرصنة الإلكترونية التي تتعرض لها الدول.

### الهوامش والمراجع:

<sup>1</sup> عادل عبد الصادق: الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والإستراتيجية، القاهرة، مصر، 2009، ص 90.

## تأثير الإرهاب المعلوماتي على بقاء ومستقبل بناء الدول ——— رقيق ليناس

- <sup>28</sup> رائد العدوان: المعالجة الدولية لتضايي الإرهاب الإلكتروني، مقالة مقدمة خلال الدورة التدريبية للفترة بين 2-2013/02/27، الرياض، ص.ص 09، 10.
- <sup>29</sup> قرار الجمعية العامة للأمم المتحدة رقم 70/125، الصادر خلال دورتها السبعون، في 16 ديسمبر 2015.
- <sup>30</sup> أطلع على مختلف قرارات الأمم المتحدة من خلال الموقع الرسمي لها على شبكة الانترنت: <http://www.un.org>.
- \* نشأ الاتحاد الدولي للمواصلات بمقتضى اتفاقية باريس عام 1865 تحت اسم "اتحاد التلغراف الدولي" ثم عدّل ليصبح "الاتحاد الدولي للاتصالات السلكية واللاسلكية"، وفي عام 1947 انضم الاتحاد للأمم المتحدة ليصبح أحد الوكالات المتخصصة التابعة لها.
- <sup>31</sup> تقرير الاتحاد الدولي للاتصالات: الصادر عن الأمانة العامة للاتحاد الدولي للاتصالات، الصادر في مارس 2011، المصدر [www.itu.int](http://www.itu.int) الموقع الرسمي للاتحاد، تاريخ الاطلاع 04 أبريل 2018، على الساعة 20:10.
- <sup>32</sup> سامر مؤيد عبد اللطيف: نوري رشيد الشافعي، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، جامعة كربلاء، العراق، 2016، ص.25.
- <sup>33</sup> الاتحاد الدولي للاتصالات: دليل الأمن السيبراني للبلدان النامية، طبعة 2007، ص.ص 130-133.
- <sup>34</sup> سامر مؤيد عبد اللطيف: نوري رشيد الشافعي، المرجع السابق، ص.25.
- مقدمة خلال ملتقى الجرائم المستحدثة في ظل المتغيرات والتحول الإقليمي والدولية، خلال الفترة بين 2-2014/09/4، كلية العلوم الإستراتيجية، عمان، الأردن، 2014، ص 9.
- <sup>16</sup> رقد عيادة الهاشمي: المرجع السابق، ص 12.
- <sup>17</sup> رقد عيادة الهاشمي: الإرهاب الإلكتروني، كتاب إلكتروني الكتروني متاح على الرابط التالي: <https://www.mizandz.com/2017/11/pdf.htm>، ص 12.
- <sup>18</sup> عادل عبد الصادق: أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة وحدة الدراسات المستقبلية، الإسكندرية، مصر، ص.ص 55، 56.
- <sup>19</sup> بوحداء سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية للعلوم السياسية، الجزائر، 2017.
- <sup>20</sup> علي عدنان الفيل: المرجع السابق، ص.15.
- <sup>21</sup> عادل عبد الصادق، المرجع السابق، ص 55.
- <sup>22</sup> أيمن حسين: الإرهاب الإلكتروني أخطر معارك حروب الفضاء، مقال متاح على الرابط الإلكتروني التالي: <http://alwatan.com/details/166324>، تاريخ اطلاع يومك 2018/04/04 على الساعة 20:15.
- <sup>23</sup> بوحداء سارة: أثر الإرهاب الإلكتروني على أمن واستقرار الدول، مقالة متاحة على الموقع الإلكتروني لجامعة قاصدي مرباح ورقلة: <https://manifest.univ-ouargla.dz> تاريخ الإطلاع يوم 2017/04/06 على الساعة 08:00، ص.10.
- <sup>24</sup> نفس المرجع: ص 11.
- <sup>25</sup> نزمين عباس، الدول العربية الأكثر تعرضاً للهجمات الإلكترونية، مقال متاح على الرابط التالي: <https://www.forbesmiddleeast.com>، آخر إطلاع يوم: 2018/04/06، على الساعة 02:00.
- <sup>26</sup> علي عدنان الفيل: المرجع السابق، ص.18.
- <sup>27</sup> فضيلة عاقل: الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال المؤتمر الدولي الرابع عشر المتعلق بالجرائم الإلكترونية المنعقد بين يومي 24-25 مارس 2017، مركز جيل البحث العلمي، لبنان، 2017، ص 130.