# الإرهاب الالكتروني: بين عولمة الجريمة وضرورة المكافحة

# Cyber-Terrorism: between the Globalization of Crime and the Need to Combat

**بعجي عبد النور[1]*، مالك نسيمة[2]**

[1] كلية الحقوق جامعة الجزائر-1 ، abdennour.bdj@gmail.com

[2] كلية الحقوق جامعة الجزائر-1 ، nassimamelek@gmail.com

تاريخ الاستلام: 2022/01/17 تاريخ القبول: 2022/03/26 تاريخ النشر: 2022/06/20

**ملخص:**

تعد ظاهرة الإرهاب الالكتروني شكل من العولمة الاجرامية التي تمنح للإرهابي فرص أكثر في العالم السيبراني، فالإرهاب في الأصل جريمة كلاسيكية من جرائم القانون العام والتي تأخذ ثوب جديد تحت مسمى "الإرهاب الالكتروني" وعليه هناك خصوصية لهذه الظاهرة الإجرامية، وفي هذا الصدد توصلت الدراسة إلى أن المشرع الجزائري جرم استخدام الإرهابيين ومناصريهم لتكنولوجيات الإعلام والاتصال عملا بالالتزامات الدولية، إلا أنه لا يعد كافيا ويجب تبني أسلوب الوقاية وتجريم جميع صور الارهاب الالكتروني الأخرى.

**كلمات مفتاحية:** الإرهاب الالكتروني، عولمة الارهاب، التجنيد، تمويل سفر، الإرهابيين الأجانب.

**Abstract:**

Cyberterrorism is a globalization crime that gives the terrorists more opportunities in the cyberspace, this study found a local legislator has criminalized the use of ICT by terrorists, and in this regard to confront the privacy of cyber-terrorism in application of international obligations, but it is not sufficient and the method of prevention must be adopted and all other acts of cyber-terrorism should be criminalized.

**Keywords:** cyberterrorism; globalization; Recruitment; foreign terrorists**.**

* **المؤلف المرسل**

**1. مقدمة :**

يعد الإرهاب الإلكتروني ظاهرة إجرامية عابرة للحدود الوطنية نتجت عن التطور الرهيب في التكنولوجيا والاعتماد عليها في نواحي الحياة التي يعجز الإنسان بمفرده عن أدائها ولاسيما الخدمات الحيوية في الدول المتطورة، ويمكن القول بأن العالم أصبح قرية صغيرة عبر تطور وسائل الاتصال الحديثة، ونجم عن هذا الأخير مجتمع معلوم يعتمد في نشاطه على تكنولوجيات الإعلام والاتصال من وسائل التواصل الاجتماعي والبريد الإلكتروني، ومؤخرا بروز الذكاء الاصطناعي، وقبل ظهور الثورة الرقمية كان المجرم الكلاسيكي يعتمد على التخطيط والتنقل والقوة للقيام بالأعمال الإجرامية ومن بينها الأعمال الإرهابية من تفجيرات وقتل للأبرياء واستهداف للممتلكات بغرض تغيير النظام السياسي، وبفعل ما تقدمه التكنولوجيا اصبح يعتمد الإرهابي على الوسائل الإلكترونية التي تسهل القيام بإجرامه متى أراد وبسهولة عبر لوحة المفاتيح أو نقر بالماوس، ويعد اول استعمال للإرهاب الإلكتروني في أحداث 11 سبتمبر 2001 التي ابانت على التأثير العالمي الذي يمكن أن يحدثه هجوم إرهابي منظم على مختلف القطاعات وعلى الرغم من أن الهجوم كان هجومًا جسديًا بشكل أساسي، فقد أثيرت فكرة استخدام أجهزة الكمبيوتر والشبكات لتنظيم مثل هذا الهجوم عبر استخدام الفضاء الإلكتروني لتنفيذ أنشطة إرهابية.

ويشكل الإرهاب الالكتروني ظاهرة بالغة الأهمية لما ينطوي عليه من تهديدات تمس الدول نظرا لعالمتيه بحيث يكون أقرب للجريمة المنظمة، وأصبحت التنظيمات الإرهابية تستغل الفضاء السيبراني من أجل استقطاب المؤيدين وتجنيدهم بسهولة، مما يستوجب البحث في خصوصية هذه الجريمة، ويعزز ذلك ظهور تنظيم الدولة الذي دق ناقوس الخطر من زيادة تدفق المقاتلين الإرهابيين الأجانب إلى الشرق الأوسط، حيث صدر قرار مجلس الأمن رقم 2178 (2014) الذي اعتبر "نقطة تحول في الجهود المبذولة على المستوى العالمي للحد من تهديد المقاتلين الإرهابيين الأجانب" وتم اعتماده بالإجماع، ويلزم جميع البلدان بسن قوانين تجرم السفر أو محاولة السفر لأغراض إرهابية، ويطالب الدول بقمع ومنع التنظيم والتجنيد والنقل وتجهيز المقاتلين الإرهابيين الأجانب بالإضافة إلى تمويل أنشطتهم، ومن هذا نطرح الإشكالية التالية: كيف يمكن التصدي لظاهرة استخدام تكنولوجيات الاعلام والاتصال من قبل

الإرهابيين في ظل عدم وجود تعريف موحد للإرهاب بصفة عامة من جهة والالتزام بقرار مجلس الأمن رقم 2178 (2014) من جهة أخرى ؟

وللإجابة على هذه الإشكالية والالمام بمختلف جوانب الموضوع، تم تقسيم الموضوع إلى قسمين، القسم الأول يتناول عولمة مفهوم الإرهاب الالكتروني، ونتناول فيه مفهوم الإرهاب الالكتروني، ثم خصائص الإرهاب الالكتروني، أما القسم الثاني فيتناول مكافحة الإرهاب الالكتروني، ثم مفهوم استخدام تكنولوجيات الإعلام والاتصال في الإرهاب، واستخدام تكنولوجيات الإعلام والاتصال في الأعمال المسهلة للسفر لأنشطة إرهابية، وبعدها التطرق في الخاتمة إلى نتائج الدراسة وبعض التوصيات.

ولدراسة الموضوع نقترح فرضيتين، تتمحور الأولى في اعتبار الإرهاب الإلكتروني نوع من الجرائم الإلكترونية تخضع الى النصوص التجريمية نفسها التي تخضع لها الجرائم الالكترونية، والثانية في كون الإرهاب الالكتروني ذو طبيعة معقدة واجرام مستحدث تستوجب معالجته في نصوص قانونية خاصة تطبيقا للالتزامات الدولية في هذا المجال.

وتهدف الدراسة الى بيان أن الإرهاب تأثر بالعولمة من خلال استخدام تكنولوجيات المعلومات والاتصال والذي نتج عنه خصوصية لهذه الجريمة، تحديدا في الركن المادي للجريمة بحيث يرتكب الإرهابي اجرامه عبر الفضاء السيبراني الذي يعد مسرح جريمته، كما تعد جريمة معولمة سواء من ناحية المفهوم الذي في ظل غياب تعريف للإرهاب يصعب حصر مفهومه، وإبراز عالمية الإرهاب من خلال خصائصه المستمدة من الفضاء السيبراني، واستقراء مختلف النصوص القانونية التي جرمت صور الإرهاب الالكتروني على ضوء الالتزامات الدولية وفي مقدمتها قرار مجلس الأمن رقم 2178 (2014) ومعرفة النقائص وإيجاد الحلول المناسبة.

وفي هذا الصدد اعتمدت على المنهجين التحليلي والوصفي من أجل استقراء النصوص القانونية والاتفاقيات الدولية وقرارات الأمم المتحدة.

## 2. عولمة مفهوم الإرهاب الإلكتروني

أثرت التكنولوجيا على الظاهرة الإجرامية وغزت جميع مناحي الحياة مما نتج عنه ظهور أنواع من الجرائم المعولمة والحديثة، وأصبح الإرهابي يلجئ إلى تقنية المعلومات لتحقيق اغراضه، "الإرهاب الإلكتروني" والذي تعددت أنواعه ومفاهيمه والاستجابة القانونية على المستوى الدولي والتشريعات الوطنية في الوقاية منه ومكافحته، وفي هذا المبحث نعالج ماهية الإرهاب الإلكتروني، ثم خصائص هذا الاجرام المستحدث.

### 1.2 مفهوم الإرهاب الإلكتروني:

يعد الإرهاب الإلكتروني من الجرائم المستحدثة التي اثرت عليها العولمة من خلال التكنولوجيا التي جعلت من العالم قرية صغيرة، وسهلت من طرق ارتكاب الإجرام ولعل أخطره هو الإرهاب الذي يحصد أرواح الأبرياء ويسبب خسائر فادحة في الأموال والممتلكات، وأمام هذه التحديات يستوجب علينا تحديد مفهوم لظاهرة استعمال التكنولوجيا من قبل الإرهابي، واستعراض خصائصها المميزة لها عن باقي الجرائم.

#### 1.1.2. تعريف الإرهاب الالكتروني في الفقه

ظهرت عبارة الإرهاب الإلكتروني أول مرة في منتصف الثمانينات والذي يتألف من "الإنترنت" و "الإرهاب" من خلال دراسة للباحث "Barry Collin" والتي توصل فيها إلى صعوبة تحديد تعريف لظاهرة الإرهاب الذي تستعمل فيه التكنولوجيا وكذا تحديد دور الكمبيوتر والأنترنت في العمل الإرهابي، ومنذ ذلك الحين تم استخدام مصطلح "الإرهاب الإلكتروني" على نطاق واسع، حيث يجمع بين اثنين من أكبر مخاوف هذا القرن: الفضاء الإلكتروني والإرهاب[1]، وفي سنة1980 أستخدم المصطلح للإشارة إلى الهجمات الإلكترونية التي تطال اقتصاد الولايات المتحدة الأمريكية من خلال دراسات ولعل ابرزها تقرير الأكاديمية الوطنية الأمريكية للعلوم عن أمن الكمبيوتر، والذي جاء فيه بأن الولايات المتحدة الأمريكية في خطر، لاعتمادها بشكل متزايد على أجهزة الكمبيوتر في إدارة الخدمات الحيوية والذي يجعلها عرضة لهجوم إلكتروني متعمد، وهذا ما يجعل من إرهابي الغد قادرًا على إحداث المزيد من الضرر باستخدام لوحة المفاتيح أكثر من القنبلة،[2]وعموما لا يزال الإرهاب السيبراني ظاهرة حديثة جدًا يصعب فهمها، لأنه يستغل المفاهيم التي تتأرجح بين العلوم السياسية وعلم الإجرام وعلم الاجتماع والفلسفة واللاهوت وعلوم

الكمبيوتر وحتى الخيال العلمي[3]، وبالرجوع الى المؤلفات العلمية نجد أن الباحثين في معالجة ظاهرة الإرهاب الإلكتروني عرفت بأنها ذلك التقارب بين علم التحكم الآلي والإرهاب أو التزاوج بين الإرهاب والتكنولوجيا،[4]وتميز الباحثة"Talihamrm" بين الإرهاب الإلكتروني الموجه نحو الهدف، وبقصد به جميع الهجمات التي ترتكب ضد أجهزة الكمبيوتر والشبكات والمعلومات، والإرهاب الإلكتروني الموجه بالأدوات يقصد به جميع الإجراءات التي تستخدم الإنترنت أو أجهزة الكمبيوتر لتنظيم الأعمال الإرهابية وإتمامها على أنها إرهاب إلكتروني[5]، وبالتالي فإن الأنشطة المتنوعة مثل جمع الأموال والاستطلاع والاتصالات والدعاية جميعها يمكن أن تعتبر إرهابًا إلكترونيًا إذا تم إجراؤها عبر الإنترنت لأغراض الإرهاب، ويتخذ "Denning Dorothy" منهج ضيق في تعريفه للإرهاب الإلكتروني بمناسبة شهادة أدلى بها أمام مجلس النواب الأمريكي، ويعتبره نقطة التقاء الإرهاب والفضاء الإلكتروني، وعموما يعني الهجمات غير القانونية والتهديدات التي تطال أجهزة الكمبيوتر عندما تتم بهدف تحقيق أهداف سياسية أو اجتماعية، كما أنه لتصنيف الهجوم على أنه إرهاب إلكتروني، يجب أن يؤدي إلى عنف ضد الأشخاص أو الممتلكات أو على الأقل التسبب في ضرر كافٍ لتوليد الخوف،كما ان تلك الهجمات التي تعطل الخدمات الثانوية لن تكون كذلك[6]، وينطلق الباحث "Pollitt Mark" من عنوان مفاده: "الإرهاب الإلكتروني هل هو حقيقة أم خيال؟"، ليتوصل من خلال دراسته إلى وضع تعريف شامل للإرهاب الإلكتروني، بانه: "هجوم متعمد ذو دوافع سياسية يستهدف المعلومات والبرامج والبيانات وأنظمة الكمبيوتر التي تؤدي إلى عنف ضد أهداف مدنية من قبل مجموعات أو عملاء سريين[7]، وعليه يجمع بين تعريف وزارة الخارجية الأمريكية للإرهاب وتعريف الفضاء السيبراني، وبذلك يكون الحد من القدرات المادية للبنية التحتية للمعلومات الوسيلة القادرة على الحد من إمكانية التدمير المادي لها، ومن هذه التعريفات يتضح بأن الفقه لم يتفق على تعريف موحد للإرهاب الإلكتروني، والمتفق عليه أن مصطلح "الإرهاب الإلكتروني" حصل على إجماع بأنه تعبير عن ظاهرة إجرامية جديدة من الإرهاب تهدف إلى تحقيق نتائج الإرهاب التقليدي من خلال استخدام تكنولوجيا المعلومات.

### 2.1.2. تعريف الإرهاب الإلكتروني في الاتفاقيات والقرارات الدولية

تناولت الاتفاقيات الدولية ظاهرة الإرهاب الالكتروني، وفي هذا الصدد تعد اتفاقية بودابست الأولى من نوعها التي تتعلق بالجرائم الإلكترونية والتي تم اعتمادها تحت رعاية مجلس أوروبا سنة2001 في العاصمة المجرية[8]، ونصت على عدة جرائم في الفضاء السيبراني، ومع ذلك لم تطرق الاتفاقية لمفهوم الإرهاب الإلكتروني، وبالرجوع إلى اتفاقية الأمن المعلوماتي شنغهاي عرفت الإرهاب المعلوماتي[9] بأنه استخدام مصادر المعلومات و/أو التأثير عليها في فضاء المعلومات لأغراض إرهابية، ويكمن مصدر هذا التهديد في المنظمات الإرهابية والأشخاص الضالعين في أنشطة إرهابية الذين يقومون بأعمال غير مشروعة، وتشمل سماته استخدام شبكات المعلومات من قبل المنظمات الإرهابية للقيام بأنشطة إرهابية واستقطاب مؤيدين جدد إلى صفوفها[10]، وحصرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ظاهرة "الإرهاب الإلكتروني" في استخدام تقنية المعلومات للأعمال الإرهابية، وعددتها المادة15 بأن: "الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات: نشر أفكار ومبادئ جماعات إرهابية والدعوة لها؛ تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية؛ نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية؛ نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.".

وفيما يتعلق بقرارات الأمم المتحدة توجد العديد منها التي تتعلق بالإرهاب بشكل عام، ولم تخص الإرهاب الإلكتروني بأي قرار إلى غاية سنة2006 حين اعتمدت الجمعية العامة قرار تحت عنوان: "إستراتيجية الأمم المتحدة لمكافحة الإرهاب"،[11]ونصت في المادة12 على أن الدول تعمل على: " .. (ب). استخدام الإنترنت كأداة لمكافحة تفشي الإرهاب، مع التسليم في الوقت نفسه بأن الدول قد تحتاج إلى المساعدة في هذا الصدد"، ولم تستخدم فرقة العمل المعنية بتنفيذ مكافحة الإرهاب التابعة للأمم المتحدة بشكل صريح مصطلح الإرهاب الإلكتروني، وانما وضعت تحليل حول إمكانية استخدام الأنترنت بقصد ارتكاب أعمال إرهابية[12]، وتناولت وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات بدول مجلس التعاون الخليجي[13]، في المادة 29 على ضرورة معاقبة من يقوم بإنشاء

مواقع الكرتونية أو نشر معلومات عن طريق الشبكة الإلكترونية أو إحدى وسائل تقنية المعلومات، من أجل تسهيل الاتصالات بين أعضاء جماعة إرهابية، أو بقصد ترويج أفكارها أو تمويلها..، وبالتالي استندت في التعريف إلى الوسيلة المستعملة، وفي إطار الجمعية العامة تم اعتماد قرار "أنشطة منظومة الأمم المتحدة في مجال تنفيذ إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب"، ويوجز هذا القرار الاتجاهات والتحديات في المشهد العالمي المتطور للإرهاب، ويتضمن التهديدات والتحديات الناشئة عن شن هجمات باستعمال الذكاء الاصطناعي والطائرات المسيرة بدون طيار أو الهجمات الإلكترونية[14].

## 2.2 خصوصية الإرهاب الإلكتروني:

يعد الإرهاب الإلكتروني بمثابة جريمة منظمة والتي لا يمكن لرجال إنفاذ القانون من السيطرة عليها، وهذا الاعتبار لا يكون مطابق لأبعد الحدود لأنه يجب الحديث عن السمات المميزة للعنف الذي يعد جريمة إرهاب كلاسيكية وتحوله بفعل التزاوج مع تقنيات التكنولوجيا إلى كيان جديد يدعى بـ" الإرهاب الإلكتروني" له من السمات ما تميزه عن باقي الجرائم المنظمة.

### 1.2.2. ترابط الإرهاب الالكتروني مع الجريمة الإلكترونية

يرتبط الإرهاب الالكتروني بالجريمة الالكترونية لأن ظهوره كان في منتصف التسعينيات عندما أصبحت شبكة الويب العالمية جزءًا لا يتجزأ من حياة الناس[15]، ويتم استخدام الإنترنت على نطاق واسع كوسيلة للنشر من قبل القراصنة والإرهابيين، وينشر القراصنة في المجلات الإلكترونية ويضعون مواقع الويب بأدوات برمجية ومعلومات حول القرصنة من تفاصيل حول نقاط الضعف في الأنظمة الشائعة مثلا: Microsoft Windows، وبرامج لاختراق كلمات المرور وحزم البرامج لكتابة فيروسات الكمبيوتر وغيرها،[16]وبالتالي تستخدم الجماعات ذات التوجه السياسي تقنيات القرصنة للانخراط في ضربات أكثر خطورة ضد الحكومات والمنظمات السياسية، وقد تنتهك هذه الهجمات القانون ولكنها لا تسبب بالضرورة الخوف أو القلق بين عامة الناس، ونتيجة ذلك، فإن نشاط القرصنة يشبه أشكال معينة من إجراءات الاحتجاج في العالم الحقيقي مثل التخريب المتعمد وتدمير الممتلكات الخاصة لتعزيز أجندة

سياسية، بينما يجب أن يكون عمل الإرهاب الإلكتروني مدفوعًا بأجندة سياسية أو أيديولوجية ويسعى إلى بث الخوف أو الإكراه أو تخويف الحكومة أو شعبها، كما يجب أن تؤدي نتائج الإرهاب الالكتروني إلى خسائر في الأرواح بمعنى ضرر في العالم الحقيقي، والذي يشكل دور رئيسي في النتيجة الجرمية للإرهاب التقليدي،[17] ويمكن أن يرقى الإرهاب السيبراني إلى حرب المعلومات دون اشتراطه لوقوع الضرر الذي يوجد في الإرهاب التقليدي لأن المستعمل لحرب المعلومات هو في الأصل إرهابي، ومن جهة أخرى يعد مصطلح "حرب المعلومات" بمثابة مفهوم عام يشمل عناصر متنوعة من الحرب النفسية والمعلومات المضللة والدعاية والحرب الإلكترونية أو حرب الكمبيوتر[18].

### 2.2.2. سمات الإرهاب الالكتروني

يتميز الإرهاب الذي يتم عبر وسائل التكنولوجيا والمعلومات بمجموعة من السمات تميزه عن باقي الجرائم نوجزها كالآتي:

أ-الإعلام الآلي أداة الإرهاب الإلكتروني:

لا يحتاج الإرهاب الإلكتروني في ارتكابه إلى العنف والقوة بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج الإلكترونية[19]، فالإرهاب التقليدي يستخدم القوة والعنف التي تتجلى في العالم الخارجي أو التهديد بها، بينما الإرهاب الإلكتروني يستعمل القوة اللينة بصورة أكبر حيث المعلومات والأفكار والتأثير في الرأي العام حيث الفكرة تحرك القوة داخل الفضاء الإلكتروني، ويتم الاستفادة مما يتيحه الفضاء الإلكتروني من سرعة الانتشار وتوافر وسائل يمكن استخدامها كأسلحة رخيصة ونسب نجاحها مرتفعة، وأيضا كوسيلة إعلام[20].

ب- يستند الإرهاب الإلكتروني إلى العامل الفردي والحماسة:

يتميز الإرهابي الذي يستعمل التكنولوجيا بأن لديه أهداف محددة في الاعتبار عندما يهاجم النظام المعلوماتي، فهو على عكس المتسللين أو الخصوم الساذجين، سيحاول الإرهابي الإلكتروني استهداف المضيف أو النظام المحدد الذي يجب اختراقه لإنجاز مهمته، وبالتالي يجب أن يكون الإرهابي الإلكتروني محترفًا ومبدعًا وذكيًا للغاية من أجل أن يبحث عن طرق حديثة وأصلية لتحقيق هدفه،[21] وبالتالي يكون

مرتكب الإرهاب الإلكتروني في العادة من المتخصصين في مجال تقنية المعلومات[22]، وفي الغالب يهدف مجرمو الإنترنت إلى جني الأموال، في حين أن الإرهابيين الإلكترونيين قد يكون لديهم مجموعة من الدوافع ويسعون في كثير من الأحيان إلى إحداث تأثير مدمر، ولا سيما على البنية التحتية الحيوية[23]، ويكون ذلك من أجل تخويف أو إجبار حكومة أو شعبها على تحقيق أهداف سياسية أو اجتماعية، والتي تعد بمثابة قوى محركة للإرهاب الإلكتروني، في حين أن المجرمين العاديين أو المهاجمين قد لا تكون الدوافع سياسية أو دينية أو اجتماعية[24].

ج-الإرهاب الإلكتروني جريمة عابرة للحدود الوطنية:

تعد السمة البارزة للجرائم الإلكترونية بأنها عابرة للحدود فقد يكون المجرم في قارة وتقع الجريمة في قارة أخرى[25]، ولا يكون الإجرام محصورا في الدوافع السياسية فقط، بل يتسم بنزاعين أحدهما عنيف باستخدام القدرات الهجومية والدفاعية عبر الفضاء السيبراني من أجل تعطيل شبكات نظم المعلومات والبنية التحتية باستخدام الأسلحة الإلكترونية عبر الفضاء السيبراني من قبل أحد الفاعلين داخل مجتمع المعلومات العالمي، والنوع الآخر يتسم بطابع مرن للصراع والمنافسة على الوصول إلى تأثير المعلومات على المشاعر والأفكار التي تطلق حربًا نفسية من خلال وسائل الإعلام[26].

د- صعوبة اكتشاف جرائم الإرهاب الإلكتروني:

يعد استخدام الوسائل الإلكترونية المستحدثة أداة تساعد المجرمين في ارتكاب العديد من الجرائم دون إمكان القبض عليهم، ومثال ذلك أن استخدام البريد الإلكتروني كوسيلة اتصال بين المجرمين، يتعذر منه مراقبتهم على النحو الذي يحدث في الاتصالات السلكية واللاسلكية، كذلك فإن عمليات التحويلات المالية الإلكترونية قد تتم بين الجناة والذين قد يكونوا فرادى أو جماعات بغرض تمويل العمليات الإجرامية أو المخططات الإرهابية دون أن يتم اكتشافها[27]، ويتطلب تدريب سلطات التحري وجهات التحقيق والقضاة بحيث تتوافر لديهم القدرة الفنية التي تمكنهم من القيام بأعمال وظائفهم المختلفة بشأن هذا النوع من الجرائم التي ترتكب باستخدام الوسائل الإلكترونية المتقدمة.

### 3.2.2. الإرهاب الالكتروني جريمة قائمة بذاتها؟

يعد الإرهاب الالكتروني بمثابة جريمة من جرائم القانون العام في قانون العقوبات، والتي تأثرت بتكنولوجيات الاعلام والاتصال لتأخذ صورة مستحدثة من الإرهاب، ويعزز هذا الطرح القانون09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في نص مادته الثانية بأن: "1- الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية."، وبالتالي الجرائم الموصوفة بأفعال إرهابية أو تخريبية في القسم الرابع مكرر من قانون العقوبات يمكن تعدادها من ضمن جرائم الإرهاب الالكتروني في مفهوم القانون09-04 في مادته الثانية إذا ارتكبت أو سهل ذلك عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية. وعليه يمكن القول بأن " الإرهاب الالكتروني هو في الأصل جريمة تقليدية وبفعل تكنولوجيات المعلومات والاتصال أخذت شكل جديد"، وبالرجوع إلى النموذج القانوني لجريمة الإرهاب الالكتروني أي الأركان الثلاثة للجريمة، نجد خصوصية في الركن المادي، الذي يتكون من استخدام الوسائل الالكترونية في السلوك الإرهابي، والذي لا يشترط أن يترتب عليه نتيجة جرمية أو علاقة السببية بالبحث عن نسبة السلوك الإجرامي للفاعل حتى يتم تجريم الإرهاب باستخدام الوسائل الالكترونية من سلوك مادي، كونها من جرائم الخطر وليس الضرر، كما أن المشرع الجزائري حدد حصرا سلوكيات الإرهاب الالكتروني في المادتين87مكرر11 و87مكرر12 من قانون العقوبات مما لا يفتح المجال لاعتبار سلوكيات أخرى تحت طائفة الإرهاب الإلكتروني، ونخلص بأن جريمة الإرهاب الإلكتروني في سلوكها الإجرامي تثير خصوصية، والتي بموجبها يمكن القول بأن" الإرهاب الالكتروني جريمة قائمة بذاتها" وهذا الطرح ندعمه من خلال ما سوف نوضحه في النقاط القادمة باعتبار أن تجريم هذه السلوكيات جاء كإلتزام لقرار مجلس الأمن رقم 2178 (2014)، ومن جهة أخرى شرط استخدام تكنولوجيات الإعلام والاتصال في السلوك المادي في حالة عدم توافره يجعلنا أمام جريمة إرهاب تقليدية لم يكن منصوص عليها من قبل ضمن القسم الرابع مكرر من قانون العقوبات، ومن ناحية الركن الشرعي يتوفر من خلال وجود نصوص قانونية

تحدد بدقة اركان جريمة الإرهاب الالكتروني في نصوص المواد السابق ذكرها عملا بمبدأ الشرعية في المادة الأولى من قانون العقوبات "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون"، ويتحقق الركن المعنوي للجريمة من قصد عام بعلم الجاني بارتكاب سلوك مجرم قانونا في فعل السفر والتمويل والتجنيد من خلال تكنولوجيات الإعلام والاتصال، واتجاه إرادته لاستخدامها في تنفيذ هذه السلوكيات لأغراض إرهابية أي قصد خاص.

## 3. مكافحة الإرهاب الالكتروني

يستدعي مكافحة الإرهاب الالكتروني تجريم استخدام تكنولوجيات الإعلام والاتصال من قبل الإرهابيين وفق ما جاء عن الأمم المتحدة والفرق التابعة لها في مكافحة الإرهاب، وإدراج الالتزامات الناتجة عن قرارات الأمم المتحدة التي جاءت بموجب الفصل السابع من ميثاق الأمم المتحدة في القوانين الداخلية، ونستعرض كالآتي:

### 1.3 مفهوم استخدام تكنولوجيات الإعلام والاتصال في الإرهاب:

نبين مفهوم استخدام تكنولوجيات الإعلام والاتصال من قبل الإرهابيين ومعالجة المشرع لهذا المصطلح، كالآتي:

#### 1.1.3. المدلول التقني لتكنولوجيات الإعلام والاتصال

عرفت تكنولوجيات الإعلام والاتصال عدة تسميات ووصفت بأنها التكنولوجيات الحديثة للمعلومات والاتصال NTIC ثم حذفت كلمة الحديثة من التسمية لتصبح تكنولوجيا المعلومات والاتصال TIC ثم مع بداية استخدام الأنترنت في التسعينات تم اختصارها إلى تسمية TI،[28]وهي بمثابة حلقة وصل بين نقطتين أو أكثر بينهما مسافة معينة وذلك عن طريق استخدام ما يسمى بتكنولوجيات المعلومات، وتستعمل من أجل وصف الإجراءات الخاصة بنقل المعلومات من نقطة إلى أخرى بواسطة الوسائل التكنولوجية[29].

### 2.1.3. المدلول القانوني لتكنولوجيات الاعلام والاتصال

تشكل خطر كبير على الأمن والسلم الدوليين مما دفع مجلس الأمن إلى اصدار قرارات في هذا الشأن، وأكد القرار2161 (2014)[30]على أن انتشار العولمة بالمجتمعات أدى إلى استعمال التكنولوجيات الجديدة في مجال المعلومات والاتصالات لاسيما شبكة الأنترنت في تيسير الأعمال الإرهابية وكذلك استعمالها في التحريض على ارتكاب أعمال إرهابية وتجنيد مرتكبيها وتمويلها والتخطيط لها، ويشير القرار2178 (2014)[31] من خلال البند07 بأن الجماعات الإرهابية يتم تمويلها وتسليحها وتدبير شؤونها أو تجنيد أفراد لها أو دعم اعمالها وأنشطتها بأي طريقة كانت بما في ذلك تكنولوجيات المعلومات والاتصال كشبكة الأنترنت أو وسائل التواصل الاجتماعي أو اي وسيلة أخرى، وتكون هنا تكنولوجيات الإعلام والاتصال بمثابة وسيلة لتسهيل الأنشطة الإرهابية.

وصادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[32] التي عددت صور الجرائم الإرهابية المرتكبة بواسطة تقنية المعلومات، ولم تستعمل مصطلح " تكنولوجيات الاعلام والاتصال"، مع وجود تقارب في المعنى والدلالة على استعمال التكنولوجيا والأنترنت وغيرها من الوسائل، وفي هذا الصدد عرفت الاتفاقية في المادة02 من البند01 تقنية المعلومات بأنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لاسلكيا في نظام أو شبكة"، وفي البند05 النظام المعلوماتي بأنه: "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"، وعلى مستوى القانون الداخلي، تناول القانون09-04 الذي يتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في البند الأول من المادة02 في معرض حديثه عن تعريف للجرائم المتصلة بتكنولوجيات الإعلام والاتصال بأن الوسيلة التي ترتكب بها هذه الجرائم هي المنظومة المعلوماتية أو نظام للاتصالات السلكية، ويستنتج منه بأن المفهوم الضيق لمصطلح "تكنولوجيات الإعلام والاتصال" ينحصر في نقطتين أساسيتين أو مفهومين، وهذا ما تناولت نفس المادة تعريفه في البند "ب" بأن : " منظومة معلوماتية: أي نظام منفصل أو مجموعة

من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، وفي البند "و" بأن: " الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"، وبالتالي فالمشرع في قانون الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لم يضع تعريف محدد وواضح لهذا المصطلح لأنه يعد من بين المصطلحات التقنية، ويمكن وضع تعريف لها من ما سبق شرحه بأنها الأنظمة المعلوماتية[33] التي تعالج بطريقة ألية المعلومات، وجميع الوسائل الإلكترونية التي تنتقل عبرها المراسلات ومختلف المعلومات.

### 2.3 طرق تجريم الإرهاب الإلكتروني في القانون الجزائري:

جاءت عدة قرارات عن الامم المتحدة لتحذر من خطورة استعمال الأنترنت من قبل الإرهابيين وخصوصا بعد هجمات 11 سبتمبر 2011 في الولايات المتحدة الأمريكية، وحددت المادة02 من القانون رقم09-04 المتعلق بتكنولوجيات الإعلام والاتصال ومكافحتها[34] في الفقرة "أ" بأن: "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات واي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية."

ويفهم من فحوى النص بأن الصيغة القانونية التي جاء بها واسعة تشتمل على جميع الجرائم التي تقع على نظام المعالجة الآلية للمعطيات المنظمة في قانون العقوبات من خلال القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويطلق عليها الجرائم السيبرانية أو الإلكترونية، وتوصف بأنها جميع الجرائم المرتكبة على شبكات الاتصالات السلكية واللاسلكية، والتي تلعب فيها أجهزة الكمبيوتر أو الشبكات دور أدوات الأهداف أو مسرح الجريمة[35]، والجرائم التي تستعمل تكنولوجيا الإعلام والاتصال بمثابة وسيلة لارتكاب إجرامها سواء عبر منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وبالرجوع إلى قانون العقوبات نجد أن البند الأخير من المادة87 مكرر11 استعمل مصطلح "استخدام تكنولوجيات

الإعلام والاتصال" والذي يكون محدد في ارتكاب الأفعال الإرهابية المنصوص عليها في الفقرات 1و2و3 من نفس المادة، ونعالجها كالآتي:

### 1.2.3. استخدام تكنولوجيات الإعلام والاتصال في السفر لأنشطة إرهابية:

يكتسب الإرهابيون التقنيات التي توفرها التكنولوجيا بهدف الوصول إلى تنويع نشاطاتهم، وجعلها تتميز بالكفاءة والفعالية، بحيث يتسنى تنفيذها بعدد أقل من الأشخاص ونتائج أفضل، وبالتالي يمكن لشخص واحد أن يجند المزيد من الأعضاء الجدد، كما أن تقنيات الشبكات التي تتميز بالتنوع والتعدد مدفوعة إلى حد كبير من قبل المستهلكين والأسواق التجارية في جميع أنحاء العالم، وليس من العملي إبقاء هذه الأنواع من التقنيات بعيدة عن أيدي الإرهابيين، ويمكن ببساطة شراء هذه التقنيات من الرفوف،[36] ومن هذا تتجلى خطورة استخدام الإرهابيين ومناصريهم لتكنولوجيات الإعلام في نشر الفكر المتطرف المؤدي للإرهاب بكافة أنواعه، وتجنيد الآخرين لارتكاب أعمال الإرهاب وتحريضهم على ذلك، من خلال قنوات منها شبكة الإنترنت وتمويل وتسهيل سفر المقاتلين الأجانب والأنشطة التي يضطلعون بها بعد ذلك، وجاء القرار 2178 (2014) الذي اتخذه مجلس الأمن في ديباجته ليؤكد على الخطر الشديد والمتنامي الذي يشكله المقاتلون الإرهابيون الأجانب وحدد لهم تعريف بأنهم: "الأفراد الذين يسافرون إلى دولة غير التي يقيمون فيها أو يحملون جنسيتها بغرض ارتكاب أعمال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو توفير تدريب على أعمال الإرهاب أو تلقي ذلك التدريب، بما في ذلك في سياق النزاعات المسلحة"، ويشدد على ضرورة أن تعمل الدول الأعضاء في إطار من التعاون على منع الإرهابيين من استغلال التكنولوجيات والاتصالات والموارد في التحريض على دعم الأعمال الإرهابية مع الحرص في الوقت نفسه على احترام حقوق الإنسان والحريات الأساسية.

وعددت المادة87مكرر11 صور للأنشطة الإرهابية ومن بينها ما جاءت به الفقرة الأولى من تجريم للسفر ونصت بأنه: ".. كل جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها."، وفي الفقرة الأخيرة: " يستخدم تكنولوجيات الإعلام والاتصال لارتكاب

الأفعال المذكورة في هذه المادة"، وبالتالي تستخدم تكنولوجيات الإعلام والاتصال في تسهيل السفر الذي يكون غرضه أنشطة إرهابية.

وحددت المادة نفسها في الفقرة الأولى نطاق تجريم السفر لغرض الإرهاب، بحيث يطبق نص المادة على الجزائري والأجنبي الذي يأتي جريمة السفر لأغراض إرهابية أو يستخدم تكنولوجيات الإعلام والاتصال في ارتكابها، وجاءت عبارة "الأجنبي" تنفيذا لما اشار إليه القرار 2322 (2016) بعد استمرار تدفق المجندين إلى تنظيم الدولة وتنظيم القاعدة والجماعات المرتبطة بهما، والذي أكد بدوره على ضرورة تطبيق القرار2178(2014) للحد من ذلك من خلال منع وقمع تجنيد أو تنظيم أو نقل أو تجهيز المقاتلين الإرهابيين الأجانب وتمويل سفرهم وانشطتهم، ويعد الأجنبي مقيم بصفة شرعية إذا كان حائز على بطاقة المقيم من قبل ولاية إقامته لمدة سنتين، والتي تبين أنه ثبت إقامته الفعلية والمعتادة والدائمة في الجزائر، وغير المقيم الذي يعد عابر للإقليم الجزائري أو الذي يقيم فيه لمدة لا تتجاوز تسعين يوما[37].

ويكون القصد الخاص من السفر هو ارتكاب الأعمال الإرهابية، والتي عددها المشرع الجزائري من خلال المادة87 مكرر، أو بقصد خاص من خلال التدبير أو الإعداد أو المشاركة أو التدريب أو تلقي تدريب على الأعمال الإرهابية، وتعد أعمال التدبير أو الإعداد أو المشاركة بمثابة أعمال مساعدة أو معاونة في قانون العقوبات الجزائري، ومنصوص عليها في القواعد العامة التي تحكم الاشتراك في الجريمة في المواد من42 إلى44 قانون العقوبات، وتعد بمثابة حشو في المادة87مكرر11 تطبيقا لقرارات الأمم المتحدة التي أتخدت بموجب الفصل السابع من ميثاق الأمم المتحدة ويقع على الدول الأعضاء الالتزام بتطبيقها كما سبق بيانه من قبل، ونشير إلى أنه كان على المشرع الجزائري وضع تعريف لمصطلح التدريب أو تلقي تدريب، مثلما تم إدارجه في البروتوكول الإضافي لاتفاقية مجلس أوروبا لمنع الإرهاب[38]حيث نصت المادة 03 في البند الأول على أنه: ( لأغراض هذا البروتوكول يعني "تلقي تدريب للإرهاب": تلقي تعليمات بما في ذلك الحصول على المعرفة أو المهارات العملية من شخص آخر في صنع أو استخدام المتفجرات أو

الأسلحة النارية أو غيرها من الأسلحة أو المواد الضارة أو الخطرة، أو في الوسائل أو الطرق بغرض تنفيذ جريمة إرهابية أو المساهمة في ارتكابها).

**2.2.3. استخدام تكنولوجيات الإعلام والاتصال في الأعمال المسهلة للسفر لأنشطة إرهابية:**

اعتبارها وسيلة تسهيل للسفر سواء من خلال توفير وجمع الأموال أو التمويل، وكذا تنظيم السفر، كالآتي:

**أ- تكنولوجيا الإعلام والاتصال وسيلة توفير وجمع للأموال أو تمويل للسفر:**

ورد في نص المادة87مكرر11 تجريم لأفعال "التوفير والجمع" و"التمويل" في الفقرتين2 و3، ويعد التوفير بمثابة إيجاد للمصادر التي يتم جمع الأموال منها، أما جمع الأموال بمعنى تحصيلها من مصادر مختلفة، ويعد القائم بجمع الأموال ليس هو من يعمل على توفيرها، بالتالي تظهر ضرورة تجريم كل فعل على حدى، ومن جانب آخر يعد التوفير والجمع للأموال بمثابة أعمال تندرج تحت المفهوم العام لـ "التمويل"، ويكون التوفير بمثابة وسيلة مباشرة، بينما الجمع وسيلة غير مباشرة للتمويل، وهذا ما أكدته المادة 05 الفقرة الأولى من البروتوكول الإضافي لاتفاقية مجلس أوروبا لمنع الإرهاب، والتي عرفت "تمويل السفر إلى الخارج لغرض الإرهاب" بأنه: توفير أو جمع للأموال كليًا أو جزئيًا بأي وسيلة كانت سواء بشكل مباشر أو غير مباشر، وذلك لتمكين أي شخص من السفر إلى الخارج لغرض الإرهاب، ويعد ماورد في الفقرتين2 و3 السابق ذكرها بمثابة تطبيق مباشر لما جاء به القرار1373(2001)، والذي أتخذ بموجب الفصل السابع من ميثاق الأمم المتحدة، وحث على ضرورة:

(أ). منع ووقف تمويل الأعمال الإرهابية؛ (ب). تجريم قيام رعايا هذه الدول عمدا بتوفير الأموال أو جمعها، بأي وسيلة، بصورة مباشرة أو غير مباشرة، أو في أراضيها لكي تستخدم في أعمال إرهابية، أو في حالة معرفة أنها سوف تستخدم في أعمال إرهابية.

وبالرجوع إلى قانون العقوبات لانجد تعريف لـ "التمويل" في المادة87 مكرر4، ويبقى الامر محال للقوانين الخاصة المكلمة لقانون العقوبات في التجريم، وفي هذا الصدد تناول قانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما[39] في المادة03 منه تعريف لجريمة تمويل الإرهاب، بنصه على أنه: ( يعتبر مرتكبا لجريمة تمويل الإرهاب ويعاقب بالعقوبة المقررة في المادة87مكرر4 من قانون العقوبات كل من

يقدم أو يجمع أو يسير بإرادته بطريقة مشروعة أو غير مشروعة باي وسيلة كانت بصفة مباشرة أو غير مباشرة أموالا بغرض استعمالها شخصيا كليا أو جزئيا لارتكاب أو محاولة ارتكاب جرائم موصوفة بأفعال إرهابية أو مع علمه... يعد تمويل الإرهاب فعلا إرهابيا).

**ب– تكنولوجيا الإعلام والاتصال وسيلة تنظيم أو تسهيل للسفر:**

جرمت المادة87مكرر11 في الفقرة الثالثة تنظيم وتسهيل السفر لارتكاب أنشطة إرهابية، لكن لم تحدد معنى أو نطاق لأعمال التنظيم والتسهيل، وبالتالي يرجع في ذلك للأحكام العامة التي تتعلق بالمساهمة في الجريمة في صورة المساعدة أو المعاونة، ونجد أن المادة06 الفقرة الأولى في البروتوكول الإضافي لاتفاقية مجلس أوروبا لمنع الإرهاب عرفت "تنظيم أو تسهيل السفر إلى الخارج بغرض الإرهاب" بأنه أي عمل من أعمال التنظيم أو التسهيل يساعد أي شخص في السفر إلى الخارج لغرض الإرهاب.

**4. خاتمة:**

من خلال دراستنا للموضوع في الإرهاب الالكتروني نجد بأنها ظاهرة مستحدثة تأثرت بما تقدمه العولمة من أساليب جديدة تقوم على استخدام الأنترنت وتكنولوجيات الاعلام والاتصال في ارتكاب الأعمال الارهابية وتسهيلها، كما أنها مفهوم صعب التعريف نظرا لأنها تجمع بين خصائص نوعين من الاجرام، وفي ظل عدم وجود تعريف موحد للإرهاب في حد ذاته والخصائص التي يوفرها الاجرام الالكتروني، يكون التصدي لهذه الظاهرة عبر تجريم نوع محدد من الأفعال كما فعل المشرع الجزائري غير كافي، وتوصلنا للنتائج التي نوجزها كالآتي:

– الإرهاب الإلكتروني جريمة عالمية تتعدى حدود الدولة الواحدة ويصعب اكتشافها وعادة ما يكون المجرمون من المختصين في مجال تقنية المعلومات أو لديه قدر من المعرفة والخبرة في التعامل مع الشبكات المعلوماتية.

– توجد صكوك دولية عديدة جرمت فئات من الإرهاب إلا أنه لا يوجد صك عالمي في مكافحة الإرهاب بصورة عامة نظرا لغياب تعريف موحد للإرهاب، ولا بصورة خاصة فيما تعلق بالإرهاب الإلكتروني.

– لم يضع المشرع الجزائري تعريف محدد وواضح لـ "تكنولوجيات الإعلام والاتصال" لأنه يعد من بين المصطلحات التقنية، وعرف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– التزمت الجزائر بتطبيق القرار 2178 (2014) من خلال إدراج المادة87مكرر11 والمادة 87مكرر12 والذي جاء على وجه الإلزام نظرا لخطورة استخدام الإرهابيين ومناصريهم لتكنولوجيات الإعلام والاتصال.

ومن ثم توصلت الدراسة للتوصيات التالية:

– سن قانون يتعلق بالإرهاب بشكل عام وتجريم جميع أفعال الإرهاب الإلكتروني، وضرورة التعريف بالمصطلحات التي جاءت بها المادة87مكرر11 لأنها تثير الغموض وتفتح الباب نحو خلق جرائم أخرى من طرف القاضي الجزائي، وذلك عملا بما جاء به قرار مجلس الأمن ومقتضيات تطبيق مبدأ الشرعية.

– تبني اسلوب الوقاية من خلال الضغط على شركات التكنولوجيا لإزالة المحتوى المتطرف وتعطيل الشبكات المتطرفة على الإنترنت من أجل تهيئة المجال للرسائل البديلة، وكذا إعاقة سفر الإرهابيين بجمع البيانات المتعلقة بسجلات أسماء الركاب والمعلومات المسبقة عن الركاب واستخدامها لمنع سفر الإرهابيين عبر الحدود.

– ضرورة المصادقة على الاتفاقية المتعلقة بالجريمة الإلكترونية "بودابست".

– توعية الشباب بخطورة المحتوى العنيف والمتطرف وإشراكه في الحرب على الإرهاب من خلال منصات التواصل الاجتماعي والأنترنت والندوات والأبحاث العلمية والإشهار على مختلف القنوات التلفزيونية.

## 5. الهوامش:

[1] . Collin, B. C. (1997, March). The future of cyberterrorism: Where the physical and virtual worlds converge. *Crime and Justice International*, 1997, 13(2): p15-18.

[2] . National Research Council, C. O. R. P. O. R. A. T. E. (1991). Computers at risk: Safe computing in the information age. National Academy Press, p07.

[3] . Du Québec, S., & Fortin, F. (2013). *Cybercriminalité : Entre inconduite et crime organisé*. Presses inter Polytechnique, Canada, p286.

[4] . Akhgar, B., Staniforth, A., & Bosco, F. (Eds.). (2014). Cyber crime and cyber terrorism investigator's handbook. Syngress, p11.

[5] . Taliharm, A. M. (2010). Cyberterrorism : In theory or in practice ? Defence Against Terrorism Review. 3 (2), p64.
[6] . Denning, D. E. (2000). Cyberterrorism : Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. Focus on Terrorism, 9, p71.
[7] . Pollitt, M. M. (1998). Cyberterrorism—fact or fancy?. Computer Fraud & Security, 1998(2), p09.
[8]. منير محمد الجهيني، ممدوح محمد الجهيني، (2006)، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية (مصر)، ص180.
[9] . Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO, (June 2002), available at: http://eng.sectsco.org/load/207508/, accessed 20 Avril 2021.
[10] . ibid, Annex 1 and 2.
[11] . UNITED NATIONS. The United Nations Global Counter-Terrorism Strategy. A/RES/60/288. 2006.
[12] . United Nations Counter-Terrorism Implementation Task Force, (February 2009), Countering the Use of the Internet for Terrorist Purposes, Working Group Report, p05.
[13]. وثيقة الرياض، سنة2013، النظام (القانون) الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية، الأمانة العامة: مجلس التعاون الخليجي، الرياض.
[14]. قرار الجمعية العامة، أنشطة منظمة الأمم المتحدة في مجال تنفيذ استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب،https://undocs.org/ar/A/72/840، 25أفريل2021، 12:35سا.
[15]. Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. Terrorism and Political Violence, 24(2), p338.
[16] . Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism : The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, p251.
[17]. Holt, T. J. op.cit., p340.
[18] . Du Québec, S., & Fortin, F, Op.cit., p287.
[19]. محمد علي سويلم، (2018)، جرائم الإرهاب والإرهاب الإلكتروني: دراسة مقارنة، المصرية للنشر والتوزيع، مصر، ص230.
[20]. عادل عبد الصادق، (2009)، الارهاب الالكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، القاهرة: مصر، ص112.
[21]. Schudel, G., Wood, B., & Parks, R. (2000, October). Modeling behavior of the cyber-terrorist. In submitted for consideration by the 2000 IEEE Symposium on Security and Privacy, p03.
[22]. مصطفى يوسف كافي، (2011)، الإدارة الإلكترونية، رسلان للطباعة والنشر والتوزيع، سوريا، ص441.

[23] . MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). Cyber security countermeasures to combat cyber terrorism. In Strategic intelligence management. Butterworth-Heinemann. p236.

[24]. Veerasamy, N., Grobler, M., & Von Solms, B. (2012). Building an ontology for cyberterrorism, p08.

[25]. غادة نصار، (2017)، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة: مصر، ص14.

[26] . Adel Abdel-Sadek, (march2013), Cyber Terrorism and The Use of Power in International Relation New Pattern and new challenge, Arab center for cyberspace research, second edition, p05.

[27]. محمد محي الدين عوض، (1993)، مشكلات السياسة الجنائية المعاصرة، مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة: مصر، ص360.

[28]. ماهر عودة الشمايلة وآخرون، (2015)، تكنولوجيا الإعلام والاتصال، دار الإعصار للنشر والتوزيع، ص100.

[29]. ياسر عبد الرحمن خلف، (2017)، تكنولوجيا الإعلام والاتصالات، الجنادرية للنشر والتوزيع، ص21.

[30] . UN Security Council, Security Council resolution 2161 (17 June 2014), on threats to international peace and security caused by terrorist acts, S/RES/2161, available at: https://www.undocs.org/S/RES/2161%20(2014), accessed 5 June 2021.

[31] . UN Security Council, Security Council resolution 2178 (24 September 2014), on threats to international peace and security caused by foreign terrorist fighters], S/RES/2178, available at: https://www.undocs.org/S/RES/2178%20(2014), accessed 5 June 2021.

[32]. مرسوم رئاسي 14-252، المؤرخ في 8سبتمبر سنة2014، التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة 21 ديسمبر سنة2010، الجريدة الرسمية الجزائرية، العدد57 الصادرة في28 سبتمبر سنة2014، ص04.

[33]. أنظر: قانون رقم15-03، المؤرخ في أول فبراير سنة2015، يتعلق بعصرنة العدالة، الجريدة الرسمية الجزائرية، العدد06 الصادرة في 10فبراير سنة2015، ص04: أنظر المادة02، والمادة03.

[34]. قانون 09-04، المؤرخ في5غشت سنة2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد47 صادرة في 16غشت سنة2009، ص05.

[35] . Du Québec, S., & Fortin, F, Op.cit., p14.

[36]. Don, B. W., Frelinger, D. R., Gerwehr, S., Jackson, B. A., & Landree, E. (2007). Network technologies for networked terrorists: assessing the value of information and communication technologies to modern terrorist organizations, (Vol. 454). Rand Corporation, summary -xvi-.

[37]. أنظر: المادة16 من القانون08-11، ممضي في 25 يونيو سنة2008، يتعلق بشروط دخول الأجانب إلى الجزائر وإقامتهم بها وتنقلهم فيها، الجريدة الرسمية الجزائرية، العدد 36 الصادرة في 02 يوليو سنة2008، ص04.

[38] . Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Council of Europe Treaty Series - No. 217, Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168047c5ea, accessed 12june2021.

[39]. قانون 15-06، المؤرخ في 15فبراير سنة2015، يعدل ويتمم القانون رقم05-01 المؤرخ في 6فبراير سنة2005، المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية الجزائرية، العدد08 الصادرة في 15فبراير سنة2015، ص04.