

التطور الدولي في مكافحة الإرهاب السيبراني

**The international Development in combating
cyberterrorism**رانيا حداد*، جامعة عباس لغرور خنشلة، الجزائر، 

haddad.rania@univ-khenchela.dz

تاريخ الارسال: 2025-01-22 تاريخ القبول: 2025-03-15 تاريخ النشر: 2025-03-19

Abstract

In recent decades, terrorism has posed a grave threat to international security and peace. As its tactics, goals, and reach have evolved, and with the backdrop of rapid technological advancements, terrorism has morphed into a new form: cyberterrorism. This emerging global criminal phenomenon has prompted increased international attention and concerted efforts to combat it. This research paper seeks to analyze the existing international legal framework for countering cyberterrorism and to explore avenues for international cooperation. It will examine the role of security and intelligence cooperation mechanisms between states. Both descriptive and analytical approaches will be employed in this study

Keywords: international terrorism, cyberterrorism, counterterrorism, technological development, security cooperation mechanisms.

ملخص

شكل الإرهاب خلال العقود الأخيرة تحديا خطيرا يهدد الأمن والسلم العالميين، ومع تطور أساليبه وأهدافه وتجاوزه لحدود الجغرافية للدولة الواحدة مع مراعاة التطور التكنولوجي الرهيب في شتى المجالات أصبح بذلك الإرهاب يتخذ شكلا جديدا ألا وهو الإرهاب السيبراني الذي يعد ظاهرة إجرامية عالمية مستحدثة وشديدة الخطورة، مما أدى إلى تزايد الاهتمام الدولي بمكافحته وتظافر الجهود الدولية لمواجهة هذا التحدي، وعليه تهدف هذه الورقة البحثية إلى تحليل مضامين الإطار القانوني الدولي المرصود لمكافحة الإرهاب السيبراني وكذا إبراز سبل التنسيق والتعاون الدولي من خلال مناقشة دور آليات التعاون الأمني والاستخباراتي بين الدول، بالاعتماد في معرض هذه الدراسة على كل من المنهج الوصفي وكذا التحليلي.

الكلمات المفتاحية: الإرهاب الدولي، الإرهاب السيبراني ، مكافحة الإرهاب، التطور التكنولوجي، آليات التعاون الأمني.

مقدمة:

يشهد العصر الرقمي تطوراً متسارعاً في جميع المجالات، بما في ذلك الجريمة والتهديدات الإرهابية، فقد تحول الفضاء السيبراني إلى ساحة جديدة لصراعات لا تقل أهمية عن الصراعات التقليدية، وعليه يعد الإرهاب السيبراني من أخطر التحديات الأمنية التي تواجه العالم في العصر الرقمي مع التطور المتسارع للتكنولوجيا وزيادة اعتماد المؤسسات والدول على الأنظمة الرقمية والبنية التحتية للمعلوماتية، أصبحت الهجمات السيبرانية أداة خطيرة في يد الجماعات الإرهابية، بحيث تستهدف هذه الهجمات المنشآت الحيوية والخدمات الأساسية مما يؤدي إلى شل الحياة العامة وإلحاق أضرار أمنية واقتصادية وحتى اجتماعية بالغة الخطورة.

من هنا تبرز الحاجة الملحة إلى تطوير استراتيجيات فعالة لمكافحة الإرهاب السيبراني، بحيث تعمل على الجمع بين التدابير التقنية والتشريعية والقضائية في إطار التعاون الدولي، وتتطلب هذه الاستراتيجيات المرصودة لمكافحة هذه الظاهرة الإجرامية المستجدة فهماً عميقاً لطبيعة التهديدات السيبرانية وأساليب عمل المنظمات الإرهابية في الفضاء الرقمي وهذا بغية التوصل إلى تطوير قدرات الدفاع السيبراني وتعزيز الوعي الأمني لجميع الدول.

ومن هذا المنطلق برزت الحاجة إلى دراسة هذا الموضوع لعدة دواعي أبرزها الانعكاسات الخطيرة لهذا الموضوع البالغ حساسية وتأثيره العميق على المستوى الاستراتيجي والسياسي وكذا الاقتصادي والاجتماعي، ناهيك عن أن دراسة هذه الظاهرة الإجرامية المستجدة تفتح المجال أمام التعمق في فهم وتحليل الاستراتيجيات الدولية المرصودة لمواجهة الأنماط الإجرامية الجديدة المتأنية عن التطور التكنولوجي الرهيب والمختلفة تماماً عن الجرائم التقليدية.

وعليه تستهدف هذه الدراسة بالأساس البحث في مفهوم الإرهاب السيبراني وأساليبه من جهة ومن ثمة التطرق إلى السياسات والاستراتيجيات الدولية لمكافحة الإرهاب السيبراني،

للوصول في ختام هذا البحث إلى حل للإشكالية التالية: ما مدى نجاعة الاستراتيجيات الدولية المرصودة لمكافحة الإرهاب السيبراني في ظل تزايد التهديدات التكنولوجية وتعدد البيئة الرقمية العالمية؟.

وتندرج تحت نطاق هذه الإشكالية مجموع التساؤلات الفرعية التالية:

- ما مفهوم الإرهاب السيبراني ؟
- ماهي سبل تطوير التعاون الدولي في مجال مكافحة الإرهاب الدولي ؟

وسنعمد في دراسة هذا الموضوع على العناصر الممنهجة التالية:

المحور الأول: الإطار المفاهيمي للإرهاب السيبراني.

أولاً: مفهوم الإرهاب السيبراني.

ثانياً: وسائل الإرهاب السيبراني.

المحور الثاني: الإطار الإجرائي لمكافحة الإرهاب السيبراني.

أولاً: المساعي الدولية لمكافحة الإرهاب السيبراني.

ثانياً: المساعي الإقليمية لمكافحة الإرهاب السيبراني.

1. الإطار المفاهيمي للإرهاب السيبراني.

سنتناول من خلال هذا العنصر تحديد مفهوم شامل لمصطلح الإرهاب السيبراني

وكذا تحديد مجموع الأساليب المتبعة فيه من قبل الجماعات الإرهابية.

1.1 مفهوم الإرهاب السيبراني.

إن تحديد مفهوم الإرهاب السيبراني يقتضي منا تحليل مكونات هذا المصطلح وتقسيمه

للإلمام بمختلف جوانبه الفقهية والاصطلاحية كما سيلي تبينه.

1.1.1 تعريف الإرهاب.

يعرف الإرهاب على أنه الاستخدام الغير مشروع للعنف، أو استعماله بغرض التهديد

أو الاغتيال والتشويه وأعمال التعذيب والتخريب، من أجل تحقيق هدف سياسي بحث قد

يتمثل في إحباط روح العزيمة والمقاومة لدى الأفراد وكذا المؤسسات، أو قد يهدف إلى تحصيل المعلومات أو الأموال، ويمكن القول بصفة عامة أنه سعي الجماعات الإرهابية إلى تحقيق أهدافها من خلال استعمال وسائل الإكراه ضد الأطراف الأخرى. (الكيالي، 1994، صفحة 153).

من خلال هذا التعريف يمكن إبراز أهم صفات الإرهاب وهي كالتالي:

- استعمال العنف أو التهديد من خلاله.
- تترتب آثار نفسية عن الأفعال الإرهابية تتجسد في زرع الرعب والفرع. (وليد عبد الحي، 2015، صفحة 377)
- أعمال العنف المنظمة.
- الغاية السياسية لإرهاب.
- التحول في أسلوب الصراع من القتال العسكري إلى الأسلوب الإرهابي.
- الهدف الغير مباشر للإرهاب هو التأثير على شريحة أوسع من الفئة المستهدفة للضحايا المباشرين.
- يؤثر الإرهاب بشكل أوسع على الجانب النفسي أكثر منه على الجانب المادي. (وليد عبد الحي، 2015، صفحة 377)

2.1.1 تعريف السيبرانية:

يعتبر هذا المصطلح حالياً من أكثر المصطلحات رواجاً في قاموس الأمن الدولي، ويدل هذا المصطلح على مجموع من الأنظمة والتقنيات المتطورة والحديثة التي يتم من خلالها حماية الأنظمة والشبكات الإلكترونية للهيئات والمؤسسات ومختلف قطاعات الدولة التي تحتوي على قواعد مخصصة لتخزين وحفظ البيانات والمعلومات بغرض حمايتها من الهجمات السيبرانية بغير وجه حق. (قره، 2019)

3.1.1 تعريف الإرهاب السيبراني:

استعمل مصطلح الإرهاب السيبراني لأول مرة عن طريق Barry Collin, حيث عرفه بأنه عبارة عن هجوم إلكتروني يهدف إلى تهديد الحكومات أو الاعتداء عليها من أجل السعي نحو تحقيق أهداف سياسية أو إيديولوجية أو دينية، ويكون لهذه الاعتداءات أثر تدميري وتخريبي يضاهي الأفعال الإرهابية في شكلها المادي. (N.E.Emery, 2005, p. 80) كما تناوله كذلك بالتعريف James Lewiss, حيث عرفه على أنه استعمال أدوات الحاسوب وشبكاته بصدد عمليات تهدف إلى تدمير وتخريب البنى التحتية المهمة في الدول مثل البنى الخاصة بالطاقة ومجال النقل، أو قد يكون الهدف منه ترهيب الأفراد المدنيين وكذا الحكومات. (DESDORGES, 2011, p. 03)

كما يمكن تعريف الإرهاب السيبراني بأنه مجموع الأفعال التي تستهدف الاعتداء أو الترهيب والتهديد سواء المادي أو المعنوي ضد الدول أو الأفراد في مقتضيات الدين أو العرض أو العقل أو المال دون وجه حق من خلال استخدام الوسائل المعلوماتية والتكنولوجية. (عطية، 04_02/09/2014، صفحة 09)

من خلال جملة التعريفات السالفة الذكر يمكن صياغة التعريف التالي:

الإرهاب السيبراني هو الاستخدام الغير مشروع للوسائل الإلكترونية وقواعد البيانات التي تحوزها الدول وشن هجمات إلكترونية تقنية ضدها، قد يكون هدفها سياسي أو إيديولوجي ضد الدولة بشكل مباشر أو يهدف ترويع الأفراد وزرع الرعب في نفوسهم.

2.1. وسائل الإرهاب السيبراني.

بغية تحقيق الأهداف المسطرة من قبل الجماعات الإرهابية، تعتمد هذه الأخيرة في تنفيذ عملياتها الإجرامية على مجموعة من الوسائل التقنية، وعليه سنستعرض من خلال هذه العناصر أبرز الوسائل المستعملة في تنفيذ الهجمات الإرهابية السيبرانية:

أ- اختراق وتخريب المواقع الإلكترونية:

تستهدف بعض المنظمات الإرهابية تدمير واختراق بعض المواقع الإلكترونية كأسلوب لشن هجماتها، وتستهدف من خلال هذا الإجراء إلى تسريب البيانات والمعلومات وهذه العمليات تتم عن بعد دون الحاجة إلى وجود المخترق ضمن الحدود الجغرافية للدولة المستهدفة. (الزنت، 16/15 ديسمبر 2010، الصفحات 3-5)

ب- التجسس الإلكتروني:

تقوم الجماعات الإرهابية بالتجسس على المنظمات والدول وحتى الأفراد عن طريق استخدام التقنيات الإلكترونية، وتشمل عمليات التجسس الإرهابي الإلكترونية ثلاثة محاور رئيسية وهي التجسس العسكري، السياسي والاقتصادي. (مباركة، 2010، صفحة 348)

ج- التهديد والترهيب الإلكتروني:

تستهدف المنظمات الإرهابية من خلال الوسائط الإلكترونية وشبكة المعلومات العالمية نشر الرعب والخوف لدى الأفراد والحكومات ومحاولة تهديدهم وإخضاعهم لرغباتها وأهدافها الإرهابية من جهة، ومن جهة أخرى تستهدف الحصول على الأموال وفرض كيائها الإرهابي من خلال إرسال الرسائل التهديدية عبر وسائل التواصل الإلكترونية. (مباركة، 2010، صفحة 347)

د- إنشاء مواقع إلكترونية:

قد يمثل العمل الإرهابي الإلكتروني للجماعات الإرهابية في إنشاء أو استحداث مواقع افتراضية هدفها تمثيل هذه الجماعات، حيث تقوم من خلال هذه المواقع الإلكترونية ببث مقاطع تعلن من خلالها ضلوعها في شن عمليات إرهابية ومسؤوليتها في ذلك، وتعلن من خلالها كل الأعمال الإرهابية والأخبار المتعلقة بهذه التنظيمات من خلال استغلال التقنيات

والوسائل الإلكترونية وزرع الرعب والهلع لدى الأفراد وحتى الدول. (مباركة، 2010، صفحة 347)

2. الإطار الإجرائي لمكافحة الإرهاب السيبراني.

أمام تزايد الخطورة الإجرامية للأفعال الإرهابية المندرجة في غطاء الإرهاب السيبراني، يجد المجتمع الدولي ككل نفسه أمام حتمية تظافر الجهود والمساعي الدولية وكذا الإقليمية في مجال التنسيق والعمل على مكافحة هذه الظاهرة الإجرامية المستفحلة على المستوى العالمي، وعليه سنناقش من خلال هذه الجزء من الدراسة الجهود الدولية وكذا الإقليمية المرصودة في مجال مكافحة الإرهاب السيبراني.

1.2. المساعي الدولية لمكافحة الإرهاب السيبراني.

أ- اتفاقية مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55:

في إطار مكافحة الإرهاب السيبراني عمدت الجمعية العامة لهيئة الأمم المتحدة إلى إصدار اتفاقية عالمية بتاريخ 2000/04/12 لمكافحة إساءة استخدام تكنولوجيا المعلومات وتوظيفها لأغراض إجرامية، وهذا جاء كنتيجة فرضتها الزيادة الملحوظة في المظاهر الإجرامية القائمة على استخدام الانترنت والوسائل التقنية، وهذا ما أدى بالضرورة إلى تكثيف الجهود الدولية لمحاربة هذه المظاهر الإجرامية المستحدثة، وفي ذات السياق أكد إعلان منظمة الأمم المتحدة بخصوص الألفية الذي عقده دول الهيئة بخصوص مكافحة الإرهاب الدولي وجرائم المخدرات وتكثيف المجهودات في إطار مكافحة الجرائم المنظمة العابرة للحدود الوطنية بمختلف أبعادها وخاصة ما تعلق منها بالإرهاب الإلكتروني، مع التأكيد على منح مجال الاستفادة من منافع التكنولوجيا الحديثة للجميع مع إلزامية التقيد بما يتماشى مع مقتضيات الإعلان الوزاري الصادر عن دورة المجلس الاقتصادي والاجتماعي التابع لهيئة الأمم المتحدة، كما حرصت هيئة الأمم المتحدة إلى التأكيد على تظافر الجهود والمساعي الدولية في إطار

المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين في مجال مكافحة الاستعمال الغير مشروع لتقنيات الحواسيب والانترنت. (العبيدي، 2019، الصفحات 47-48)

وقد جاء في مضمون المادة الأولى من هذه الاتفاقية النص على ما يلي:

- يجب على الدول أن لا توفر إطارا تشريعيا بموجب قوانينها الداخلية يعطي غطاء لحماية من يستخدم التكنولوجيا بهدف ارتكاب أفعال إجرامية.
- على مجموع الدول تكثيف الجهود والعمل على التنسيق المشترك فيما يتعلق بالإجراءات القضائية المتعلقة بمتابعة المجرمين الضالعين في جرائم إلكترونية.
- العمل على التنسيق وتبادل المعلومات بين الدول في مجال محاربة المظاهر الإجرامية المرتبطة بالتكنولوجيا.
- تدريب وتجهيز الأفراد المعنيين بمكافحة الجرائم المعلوماتية.
- ضمان إجراء التحقيقات اللازمة بخصوص جرائم المعلوماتية في ظرف قياسي.
- ضمان حماية وتكريس حقوق وحرية الأفراد بصدد العمل على مكافح الجرائم المرتبطة بالإنترنت. (المادة 1، اتفاقية مكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية رقم 63/55، 2000)

ب_ اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية:

تعتبر هذه الاتفاقية من أبرز الاتفاقيات المبرمة في شأن مكافحة الجرائم المعلوماتية ولها طابع عالمي، تم التوقيع عليها من قبل 24 دولة أوروبية بالإضافة إلى جنوب إفريقيا وكندا والولايات المتحدة الأمريكية، وتمثل هذه الاتفاقية مجموع المساعي والجهود المبذولة من طرف الاتحاد الأوروبي والمجلس الاقتصادي الأوروبي فيما يتعلق بمكافحة الإرهاب الإلكتروني على وجه التحديد وكذا الجرائم المعلوماتية. (العبيدي، 2019، صفحة 22)

وقد أدرجت هذه الاتفاقية مجموع الأفعال التي تصنفها على أنها من قبيل الأعمال الإرهابية السيبرانية والتي يتم تنفيذها من خلال الوسائل الإلكترونية، وهي كالتالي:

- المجموعة الأولى: تتضمن الأفعال المجرمة التي يكون هدفها أمن المعلومات الإلكترونية.
 - المجموعة الثانية: تتضمن الأفعال المتعلقة بالحواسيب الإلكترونية.
 - المجموعة الثالثة: تتضمن الأفعال المتعلقة بالمحتوى الإلكتروني.
 - المجموعة الرابعة: تتضمن الأفعال المرتبطة بعمليات الإرهاب الإلكتروني. (اتفاقية بودابست لمكافحة الجرائم المعلوماتية، 2001)
- 2.2. المساعي الإقليمية لمكافحة الإرهاب السيبراني.

أ- الجهود المبذولة على صعيد الاتحاد الأوروبي: جاءت الجهود المبذولة من قبل الاتحاد الأوروبي في شأن مكافحة الإرهاب السيبراني في شكل اتفاقية موقعة من طرف دوله سنة 1981، وتتعلق هذه الاتفاقية بحماية الأفراد من مخاطر الجرائم الإلكترونية ذات الطابع المعلوماتي الشخصي، حيث تبنى الاتحاد الأوروبي من خلال الاتفاقية النص على مجموعة من الارشادات المتعلقة بتحديد أنواع وأشكال الجرائم المتعلقة بالحاسوب سنة 1985، كما أكدت هذه الاتفاقية كذلك على ضرورة التوفيق ما بين حماية الحقوق والحريات الشخصية للأفراد ودواعي التحقيقات الجنائية المتعلقة بالجرائم المعلوماتية. (صغير، 2013، صفحة 101)

كما قام الاتحاد الأوروبي في ذات السياق بإصدار مجموع توصيات تتضمن الأفعال المدرجة ضمن الجرائم الإلكترونية، والتي شملتها موافقة اللجنة الوزارية التابعة للاتحاد الأوروبي، حيث تم تحديد مجموع الأفعال الغير مسموح أو مرخص بها وكذا الجهات المشبوهة وكل الأفعال التي تدخل في تكوين أفعال إجرامية إلكترونية. (حسن، 2016، صفحة 169)

ونجد كذلك جهود الاتحاد الأوروبي بارزة في هذا المجال من خلال اهتمامه بقضايا الإرهاب السيبراني والجرائم المرتبطة به عبر عدة توصيات صادرة منه بهدف حث دول الاتحاد إلى إدراج سياسات مشتركة فيما بينها تعمل على التنسيق والتعاون في مجال مكافحة الإرهاب السيبراني، ومن بين هذه التوصيات نذكر التوصية رقم 89/9 المعنية بجرائم أجهزة الكمبيوتر

والتي تعطي التوجيهات المناسبة للجهات التشريعية في الدول فيما يتعلق بتجريمها بموجب القوانين الداخلية لها. (القاضي، 2011، صفحة 75)

ب_ الجهود المبذولة على مستوى الاتحاد الإفريقي:

تم تبني اتفاقية الاتحاد الإفريقي لسنة 2014، والموقعة من قبل رؤساء الاتحاد والمصادق عليها من قبل 15 دولة، حيث تضمنت هذه الاتفاقية آليات وجهود مكافحة التهديد السيبراني الموجه ضد القارة الإفريقية والذي يستهدف التجارة الإلكترونية وقواعد البيانات المحمية، كما أكدت هذه الاتفاقية على ضرورة التزام الدول أثناء تصديها للجرائم السيبرانية بحماية وضمان الحقوق الفردية والخصوصية مع تكريس الحق في المحاكمة العادلة وضمان كل الحقوق والحريات المكرسة للإنسان، كما تبنت هذه الاتفاقية كذلك طرح موضوع التنسيق والعمل الدولي في إطار مكافحة الهجمات السيبرانية وكذا المساعدة المتبادلة بين مختلف الأطراف في إجراءات المتابعة والتحقيق حسب نص المادة 2/28 منها، كما نوهت هذه الاتفاقية على المحافظة والالتزام بالغرض الذي وضعت من أجله هذه الاتفاقية ألا وهو مكافحة الجرائم السيبرانية وعدم الحيد عن أهدافها لدوافع شخصية أو سياسية. (دزار، 2017، صفحة 285 إلى 289)

خاتمة

في ظل التطور المتسارع للتكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في شتى مناحي الحياة، بات الإرهاب السيبراني يشكل تهديدا وجوديا للأمن العالمي، بفضل سهولة الوصول إلى التقنيات الحديثة وإمكانية تطويرها وتوفر شبكات الإنترنت أصبح من السهل على الجماعات الإرهابية استغلال هذه الأدوات لتنفيذ هجمات واسعة النطاق تستهدف البنى التحتية الحيوية والاقتصادية للدول وتثير الرعب والهلع بالنسبة للأفراد، مما يؤثر بطبيعة الحال وبشكل سلبي على استقرار المجتمعات وكذا يهدد الأمن القومي للدول.

وعليه يمكن القول أن مفهوم الإرهاب شهد تحولاً جذرياً مع بروز الإرهاب السيبراني على الساحة الرقمية العالمية، حيث انتقل من الاعتماد على أفعال العنف المادية إلى استغلال الفضاء الإلكتروني كساحة جديدة للصراع، فالإرهاب السيبراني بخصائصه الفريدة من السرعة والمرونة والقدرة على الوصول إلى أهداف بعيدة، يمثل تحدياً جديداً للأمن القومي للدول، ويستدعي تطوير استراتيجيات جديدة لمواجهةته على المستوى الدولي والإقليمي.

وعليه تم التوصل من خلال هذه الدراسة البحثية إلى النتائج التالية:

أولاً- الدور المحوري للتكنولوجيا: أظهرت هذه الدراسة الدور الفعال الذي تلعبه التكنولوجيا في تمكين الجماعات الإرهابية من تحقيق أهدافها من خلال استعمال الانترنت لتسهيل التواصل بين أفرادها وكذا زرع الرعب عبر المواقع والمنصات الإلكترونية وتمكين هذه العصابات من اختراق مراكز البيانات والمعلومات لمختلف المنظمات والدول.

ثانياً- تنوع التهديدات الإرهابية السيبرانية: حيث تم استعراض تنوع الوسائل التي تقوم من خلالها الجماعات الإرهابية بشن هجماتها السيبرانية حيث تتراوح ما بين نشر خطابات التهديد والترويع بالنسبة إلى الأفراد إلى حد تهكير واختراق المواقع والأرضيات الرقمية الرئيسية للدول.

ثالثاً- أهمية التعاون الدولي: لقد أكدت الدراسة على أهمية التعاون الدولي في مجال مكافحة الإرهاب السيبراني، حيث يتطلب هذا التحدي جهوداً مشتركة بين الدول وجميع الفاعلين على الساحة الدولية لمواجهة هذه الظاهرة الإجرامية العابرة للحدود.

ومن أهم التوصيات المقترحة في ذات السياق ما يلي:

- ضرورة تكثيف الجهود لتعزيز الوعي بخطورة الإرهاب السيبراني لدى الأفراد والمؤسسات الحكومية والخاصة.
- تنمية القدرات الوطنية في مجال الأمن السيبراني من خلال التدريب والتأهيل المستمر للمختصين في مجال المكافحة.

- يجب تطوير المنظومة التشريعية الدولية وكذا الداخلية للدول لمواكبة التطورات في مجال الإرهاب السيبراني.
 - تعزيز التعاون الدولي والتنسيق وتبادل المعلومات في مجال الاستخبارات ومكافحة الجرائم السيبرانية.
 - تشجيع البحث العلمي في مجال الأمن السيبراني لتطوير تقنيات جديدة للكشف عن الهجمات السيبرانية والتصدي لها.
- ختاماً، فإن مكافحة الإرهاب السيبراني تتطلب جهوداً متضافرة من جميع الفاعلين في المجتمع الدولي للتصدي لمخاطر هذه الظاهرة الإجرامية شديدة الخطورة.
- الهوامش:

- DESDORGES, A. (2011). Cyberterrorism: quel périmètre! Récupéré sur les fiches de l'irsem n°11:
<https://www.google.com/search?q=alix+desforges+Cyberterrorism%3A+quel+p%C3%A9rim%C3%A8tre!%2C+fiche+de+l%27irsem+n%C2%B011&oq=alix+desforges+Cyberterrorism%3A+quel+p%C3%A9rim%C3%A8tre!%2C+fiche+de+l%27irsem+n%C2%B011&aqs=chrome..69i57j0j7&sourceid=c>
- N.E.Emery. (2005). The Myth of Cyberterrorism. Peregrine technical solution ,vol 4 ,n 1.
- اتفاقية بودابست لمكافحة الجرائم المعلوماتية (2001).
<https://rm.coe.int/budapest-convention-in-arabic/1680739173>

- الزنط، س. ع. (15/16). ديسمبر. (2010) الإرهاب الإلكتروني وإعادة صياغة استراتيجيات الأمن القومي. مؤتمر الجرائم المستحدثة: كيفية اثباتها ومواجهتها. مصر: المركز القومي للبحوث الاجتماعية والجنائية.
- العبيدي، ع. ع. (2019). الإرهاب الإلكتروني في نطاق القانون الدولي. رسالة ماجستير. كلية الحقوق، العراق.
- القاضي، و. م. (2011). مكافحة الجرائم المعلوماتية في تشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية الطبعة الأولى. القاهرة: دار النهضة العربي.
- الكيالي، ع. ا. (1994). الموسوعة السياسية الجزء 7. بيروت: المؤسسة العربية للدراسات والنشر.
- المادة 1، اتفاقية مكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية رقم (12 04 2000). 55/63 منظمة الأمم المتحدة الجمعية العامة.
- بيلي برايسون، و اسامة محمد اسبر. (2017). موجز تاريخ كل شيء تقريبًا (الإصدار الثانية). القاهرة: العبيكان للنشر.
- حسن، م. م. (2016). التنظيم القانوني لجريمة التجسس المعلوماتي. رسالة ماجستير. كلية القانون جامعة الكوفة، العراق.
- درار، ن. (2017). الأمن المعلوماتي وسبل المواجهة: مخاطرة في التعامل الإلكتروني دراسة مقارنة. أطروحة دكتوراه. كلية الحقوق جامعة أبو بكر بلقايد تلمسان، الجزائر.
- صغير، ي. (2013). الجرائم المرتكبة عبر الانترنت. رسالة ماجستير. كلية الحقوق جامعة مولود معمري، الجزائر.

- عطية، آ. م. (2014/09/02_04). دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهتها. ملتقى دولي حول الجرائم المستحدثة في ظل المتغيرات والتحوليات الإقليمية والدولية .
- قره، ف. (2019, 08 28). الأمن السيبراني. Récupéré sur <https://political-sciencyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A> :
- مباركة، س. (2010). جوان. (الإرهاب الإلكتروني وطرق مكافحته. مجلة الحقوق والعلوم السياسية العدد 08 الجزء 01,
- وليد عبد الحفي، و. (2015). فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني. عمان الأردن: دار الحامد للنشر والتوزيع.