تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني وإستراتيجيات المواجهة.

The evolution of terrorism and its reflection on the stability of societies: A reading in the phenomenon of Cyber-Terrorism and coping strategies

عبد القادر جعيجع*
مخبر البحوث و الدراسات في العلاقات الدولية، جامعة الجزائر 3، الجزائر،
djaidja.abdelkader@univ-alger3.dz

زهرة تيغزة
جامعة الجزائر 3، الجزائر، aumlamis1975@yahoo.com

تاريخ الإرسال:30 / 09 / 2020 * تاريخ المراجعة: اليوم / الشهر / السنة* تاريخ القبول: اليوم / الشهر / السنة

ملخص:

يقدم هذا المقال قراءة وصـــفية وتحليلية لظاهرة الإرهاب الإلكتروني، ويهدف إلى التعرف عليها من حيث المفهوم، النشأة والأنماط، الانعكاسات على استقرار المجتمعات، ثم بعض إستراتيجيات المواجهة مع إشارة إلى الســياســة الجزائرية. وقد تم اســتخدام المنهج الوصــفي والتحليلي بالنظر إلى طبيعة البحث. من نتائج البحث أنّ الإرهاب الإلكتروني تهديد خطير، من شــانه زعزعة اســتقرار المجتمعات بالتعدي على خصــوصــية وقيم الفرد الدينية، كما أن خصوصيته تستوجب نوعا خاصا من الإستراتيجيات لمواجهته.

الكلمات المفتاحية:

إرهاب، استقرار مجتمعي، إرهاب إلكتروني، فكر متطرف، إستراتيجيات المواجهة.

Abstract:

This article provides a descriptive and analytical reading of Cyber-Terrorism. It aims to identify its concept, emergence and patterns, its repercussions on the stability of societies, then some strategies to confront it, with an indication of the Algerian policy. The descriptive and analytical approach has been used in view of the nature of this research. Among the research results is that Cyber-terrorism is dangerous, and it can destabilize societies by infringing on the individuals's privacy and religious values. Then, The specificity of Cyber-Terrorism requires a special kind of strategies to confront it.

Keywords:

Terrorism, Societal Stability, Cyber-Terrorism, Extreme Thought, Coping Strategies.

*المؤلف المرسل: عبد القادر جعيجع abdounalger25@hotmail.com

مقدمة:

أفرزت ثورة المعلومات والتكنولوجيا تحولات عميقة في مفهوم الأمن ومضامينه وأبعاده، كما ساهمت في تحول عدد من الظواهر والتهديدات وفي مقدمتها الإرهاب. ويُعد الإرهاب الإلكتروني من أشكال التهديد الجديدة، فقد انتشر بعد أحداث الحادي عشر من سبتمبر 2001 تحت تأثير الثورة التكنولوجية والمعلوماتية التي استفادت منها جماعات إجرامية لتحقيق أهداف معينة، ثم استفحل في خضم موجات الحراك العربي التي أفرزت تحولات جديدة وعميقة أحيانا، حتى بات اعتمادُ التنظيمات المتطرفة في المنطقة العربية على الوسائط الإلكترونية ووسائل التواصل الاجتماعي أسلوبا إستراتيجيا محوريا لتهديد الأنظمة الحاكمة، ترهيب المجتمعات، واستقطاب الأفراد فكريا لتجنيدهم.

وتتعدد أساليب ممارسة الإرهاب الإلكتروني، مما يجعله يشكل تأثيرا سلبيا متناميا على صعيد استقرار المجتمعات. ويتناول هذا المقال ظاهرة الإرهاب الإلكتروني كوجه من وجوه التطور والتحول في الظاهرة الإرهابية بوجه عام، خاصة وأنّ الفضاء "السيبراني" اليوم قد أصبح ساحة للصراعات الأيديولوجية والحروب الجديدة. كما يتناول المقال انعكاسات الإرهاب الإلكتروني على استقرار المجتمعات وخاصة في المنطقة العربية، بالنظر إلى أنه يستهدف خصوصية الفرد من خلال الهجوم على بياناته بالاختراق والتجسس، أو قيمه ودينه عندما نتحدث عن نشر التطرف الديني عبر وسائل التواصل الاجتماعي. كل ذلك يفرض تطويرا في الرؤية والإستراتيجيات الخاصة بمكافحة هذا النوع من التهديدات. بالتالي، تُطرح الإشكالية البحثية الآتية:

كيف انعكس الإرهاب الإلكتروني على استقرار المجتمعات؟ وهل تمكنت الإستراتيجيات المختلفة من التصدي له؟.

وفي إطار الإجابة على الإشكالية المطروحة سيتم الاعتماد على المنهج الوصفي والتحليلي، وهذا بالنظر إلى طبيعة البحث وما يتطلبه من تعريف بالمتغيرات الأساسية في الدراسة، بالإضافة إلى أن المنهج الوصفي يُستخدم في معظم البحوث السياسية والاجتماعية، والتحليل محطة أساسية لاكتشاف تحولات ظاهرة ما أو متطلبات مواجهتها كما هو الحال مع ظاهرة الإرهاب الإلكتروني.

بالنسبة للأهداف المرجوة من هذا البحث، يمكن ذكر أهمها كما يلي:

* التعرف على مفهوم الإرهاب الإلكتروني وأكثر أنماطه انتشارا وخطرا، وهو ما يسمح باكتشاف تداعياته على استقرار الدول والمجتمعات.
* تناوُل جانب من انعكاسات الإرهاب الإلكتروني على استقرار المجتمعات، والتركيز بشكل خاص على خصوصية الفرد وقيمه الدينية بتناول مسألة انتشار والترويج للفكر المتطرف دينيا.
* استعراض بعض الإستراتيجيات الدولية لمواجهة الإرهاب الإلكتروني، مع إشارة إلى الحالة الجزائرية، وتقديم تقييم لهذه الإستراتيجيات في مجال التصدي لهذا النوع الجديد من الإرهاب.

1. ظاهرة الإرهاب الإلكتروني:

تجب الإشارة بداية إلى أن مفهوم "الرقمنة" يشير إلى أسلوب جديد في معالجة المعلومة باستخدام التشفير واللغة الرقمية. والرقمنة كظاهرة بدأت في سنوات الستينيات والسبعينيات مع ابتكار الإعلام الآلي الذي شكّل أكبر قطيعة في القرن العشرين (Musco, 2008, p.p :2-3)، قبل ابتكار الإنترنت نهاية الثمانينيات. وقد تأثرت الظاهرة الإرهابية بهذا التطور لاحقا تزامنا مع تطور تكنولوجيا الإعلام والاتصال، حتى برز نوع جديد

هو الإرهاب الإلكتروني. ويتناول هذا العنصر لمحة حول ظاهرة الإرهاب الإلكتروني، من حيث المفهوم والنشأة وأبرز الأنماط أو الأساليب الشهيرة لممارسة هذا النوع من الإرهاب.

1.1. مفهوم ونشأة الإرهاب الإلكتروني:

يشير مصطلح "إرهاب" من الناحية اللغوية إلى معاني الخوف والفزع الشديدين، أما اصطلاحا فلا يوجد إجماع حول تعريفه، فهو يظل خاضعا لرؤية كل طرف أو دولة بالنظر إلى خلفيات وتوجهات سياسية وإستراتيجية مختلفة (ما أراه إرهابا لا يراه غيري كذلك بالضرورة).

وقد وصفه البعض بأنه "المزهرية التي يضع فيها من يسميها تقييماته الشعورية واللاشعورية، وأن مفهوم الإرهاب صعب التحديد، غامض ولا يتناسب بسهولة مع وصف الوضعيات التاريخية الخاصة، إضافة لكونه مشبعا بالعواطف والانفعالات" (العبيدي، 2018، ص35).

من التعريفات المقدمة في شأنه تعريف موسوعة السياسة: هو "استخدام العنف غير المقنن أو التهديد باستخدامه بمختلف أشكاله وصوره كالاغتيال أو التشويه أو التعذيب أو التخريب أو النسف، وذلك بغية تحقيق هدف سياسي معين، وهو بشكل عام وسيلة من وسائل الحصول على السلطة أو المعلومات أو المال واستخدام الإكراه لإخضاع الآخرين" (عبد الكافي، 2006، ص ص19-20). وعرفه الباحث في قضايا الإرهاب "ألكس شميد" (Alex Shmid) بأنه من أساليب الصراع بحيث "تقع فيه الضحايا الجزافية أو الرمزية كهدف عنف فعال" (عطية، 2015، ص30). ويمكن القول بأن الإرهاب عمل إجرامي تتوفر فيه شروط معينة ومشتركة كغياب شرعية الفعل، استخدام القوة بشكل هجومي، استهداف الأفراد والحكومات بما يعكس الطابع الرمزي للفعل، بالإضافة إلى الهدف السياسي أو الإستراتيجي المرجو من كل ذلك.

أما الإرهاب الإلكتروني Cyber-Terrorism (ويسمى أيضا الإرهاب الرقمي، الشبكي، السيبراني، إلخ) فيشير إلى "كيفية استخدام الحاسب الإلكتروني الرقمي بنُظمه وبرامجه وملحقاته ووسائل الاتصال الرقمية.. سواء كانت تلك التقنية هي محل الجريمة أو كانت وسيلة في ارتكابها" (موسى، 2009، ص270). من التعريفات المقدمة في شأنه ما يلي:

* تعريف وزارة الدفاع الأمريكية: هو عمل إجرامي يتم الإعداد له باستخدام الحواسيب ووسائل الاتصال، وينتُج عنه عنف وتدمير أو بث الخوف لدى من يتلقون الخدمات، لأغراض التأثير على الحكومات وأفراد المجتمع سياسيا، واجتماعيا، وفكريا (عبد الصادق، 2009، ص113).
* تعريف "دنينغ" (Dorothy Denning): هجمات غير قانونية وتهديد بالهجوم على أنظمة الحواسيب والشبكات والمعلومات، بحيث تكون له أهداف سياسية أو اجتماعية ويستهدف التأثير على المجتمع والجكومات (Zahri, Rabiah, 2012, p.02).
* تعريف الأستاذ جميل عبد الباقي: هو ذلك النوع الحديث من الإرهاب الذي يعتمد بصورة كلية على استخدام وسائل علمية وتقنية رقمية، بهدف إلحاق أضرار وبث الخوف والرعب لدى الأفراد ومؤسسات الحكومة (عمير، عبد الله، د.س.ن، ص327).

وإذا كان مفهوم الإرهاب من المفاهيم التقليدية غير أنه يشترك مع الإرهاب السيبراني في نفس الخصائص والعناصر، لكن يبقى الفرق متصلا بمجال ممارسة العمل الإرهابي أي الفضاء الإلكتروني مقابل الفضاء المادي (Zahri, Rabiah, p.01). والفضاء السيبراني أصبح اليوم جزءا أساسيا في "الوسط العام" كما يُسمى في علم الاجتماع، والوسط العام ينقسم إلى ثلاثة أقسام: وسط محتوم متمثل في الأسرة التي ينشأ فيها الفرد، وسط عابر كالمدرسة والجامعة، ووسط مُختار أو مقبول بحيث يكون الاندماج فيه إراديا (موسى، ص34)، وفي هذا الصنف الأخير يمكن إدراجه الفضاء الإلكتروني.

وبالرغم من عدم وجود تعريف دقيق ومتفق عليه للإرهاب الإلكتروني، يظل هذا الأسلوب مرتبطا باعتماده على الفضاء السيبراني والتطور التكنولوجي في بلوغ أهداف سياسية وإستراتيجية لا تتحقق بمعزل عن خلق جو من الهلع والفزع الشديدين لدى الدولة والمجتمع، وهو ما يؤكد حضور "حرب نفسية" شرسة في هذا الفضاء، تختلف خصائصها عن خصائص الحرب العادية التي تحدث في الفضاء المادي، كما تختلف أدواتها وأساليبها.

بالنسبة للنشأة، كان أول استخدام لمفهوم الإرهاب الإلكتروني في الثمانينيات من القرن الماضي، وذلك ضمن دراسة قام بها الباحث "باري كولين" (Barry Collin)، وهو باحث بمعهد الأمن واالاستعلام بكاليفورنيا، خلص من خلالها إلى صعوبة إيجاد تعريف دقيق ومحدد (عبد الصادق، ص111). برزت بعد ذلك مدرستان فكريتان، الأولى يمثلها الباحث "دنينغ" والثانية يمثلها مسؤولون حكوميون وعسكريون يعرفون الإرهاب الإلكتروني بأنه "أي هجوم إلكتروني يهدد أجهزة الحاسوب وشبكة المعلومات" (وهبان، 2015، ص26). أما نشأة الإرهاب الإلكتروني كظاهرة فترتبط بانتشار التطور التكنولوجي والمعلوماتي متمثلا في شبكة الإنترنت، واستغلاله في تحويل مسرح القتال من العالم المادي إلى الفضاء الافتراضي، وقد عرفت فترة الثمانينيات والتسعينيات أيضا حدوث جرائم إلكترونية يمكن تصنيفها كأعمال إرهابية (أعمال القرصنة والسطو عبر الشبكات).

2.1. أنماط الإرهاب الإلكتروني:

بات الإرهاب الإلكتروني أداةً من أدوات الصراع والحرب، بحيث تستطيع الدول الاعتماد عليه في إحداث الضرر بدول أخرى عبر الفضاء السبراني. ومن أنماط الإرهاب الإلكتروني اختراقُ المواقع الإلكترونية والحسابات الشخصية للأفراد، والعمل على تخريب أنظمة البيانات والمعلومات لكُبرى المؤسسات وأجهزة الدولة الحساسة، بما يسمح بالتجسس، الابتزاز وممارسة التهديد، وتسريب معلومات خطيرة.

وقد ظهر العديد من الفيروسات والبرامج الخبيثة لتخريب المواقع والبريد الإلكتروني للمستخدمين مثل: فيروس "برين" سنة 1986، "أحبك" سنة 2001 والذي عمد إلى تدمير الحواسيب عبر خداع المستخدم برسالة غرامية (الزنط، 2010، ص03)، والبرنامج الخبيث "ستوكس نيت" (Stux Net) الذي يهدف إلى تخريب المواقع ومهاجمة المرافق النووية الإيرانية (سينجر، 2018، ص08).

في سنة 1988، أقدمَ تنظيم إرهابي على إغراق سفارات سيري لانكا ب800 بريد في اليوم (Bogdanoski, Petreski, p.61). وفي سنة 2007 وقعت في إستونيا هجمات على مواقع حكومية وإعلامية وبنكية، مما أدى إلى شلّ حركة توزيع الخدمة على مستوى هذه المواقع (بلفرد، 2016، ص145). وفي 2010، فضحت حادثة تسريبات "ويكيليكس" عدة أطراف، فباتت تشكل إرهابا نفسيا لدى دول وشخصيات مرموقة.

كما عمدت الجماعات والتنظيمات الإرهابية إلى الاستفادة قدر الإمكان من التطور التكنولوجي والمعلوماتي، فكان البريد الإلكتروني أول ما تم الاستعانة به في التخابُر وتبادل المعلومات (ملّا خاطر، 2015، ص134). وكان تنظيم "القاعدة" نشطا في مجال ما يعرف بتسمية "الجهاد الإلكتروني"، مما ساهم في استقطاب الأفراد عبر ربوع العالم وكسب مناصرين لقضية التنظيم، وقد عُرفت منابر إعلامية إلكترونية كموقع "النداء" وهو الموقع الرسمي للقاعدة، ومنبر "التوحيد والجهاد". وعلى نفس السياسة سار تنظيم "داعش" الإرهابي.

لقد بات الفضاء الافتراضي وسيطا بين التنظيمات الإرهابية والمنخرطين فيها أو المناصرين في ظل تزايد ملاحقة أجهزة الدولة لنشاط المتطرفين. كما استعانت بعدة أساليب، كالترهيب من خلال نشر محتويات تتضمن تهديدات وأعمالا إرهابية كفيديوهات الحرق والقتل وقطع الرؤوس مثل حادثة ذبح الرهائن المصريين الأقباط، وفي المقابل أسلوب الترغيب في الجهاد دون ضغط أو تهديد بهدف استمالة الأفراد للانخراط في صفوفها.

وينبع اهتمام الجماعات أو التنظيمات المتطرفة والإرهابية بالفضاء السيبراني من عدة أسباب أهمها (شفيق، 2015، ص188):

* انخفاض التكلفة وسهولة امتلاك وحيازة أجهزة الإعلام الآلي.
* ضمان عنصر السرية في العمل.
* ضمان الاستمرارية في نقل المعلومات والأفكار، مما يحقق تنسيقا وانسجاما بين أعضاء التنظيم.
* تمكين التنظيم أو الجماعة من التواصل بسهولة مع المتشبعين بأفكارها عبر وسائط متنوعة كمواقع التواصل الاجتماعي.

بالتالي فإن أنماط ممارسة الإرهاب الإلكتروني تتنوع بين أساليب الهجمات السيبرانية ببرامج خبيثة والقيام بأعمال الاختراق والقرصنة والتخريب والتجسس، واستخدام الشبكة العنكبوتية ومنصات التواصل الاجتماعي لنشر التطرف الديني والتحفيز على تنفيذ أعمال إرهابية.

2. انعكاسات الإرهاب الإلكتروني على استقرار المجتمعات:

يتناول هذا العنصر بعض الانعكاسات لظاهرة الإرهاب الإلكتروني على استقرار المجتمعات، وسيتم التركيز على نوعين هما الأكثر انتشارا، يتعلق الأمر بتهديد الخصوصية الفردية في الفضاء الإلكتروني ونشر والترويج للتطرف الديني.

1.2. مفهوم الاستقرار المجتمعي:

هو من المفاهيم العميقة، المركّبة والواسعة، فالاستقرار في المجتمع تتداخل فيه عوامل وأبعاد متنوعة لتشكّل ترابطا عضويا ضمن نسق اجتماعي عام، يؤدي إلى حالة يمكن وصفها بالاستقرار المجتمعي. هذه العوامل والأبعاد تكون فكرية، اجتماعية، سياسية، اقتصادية وأمنية.

ويوصف الاستقرار في المجتمع بأنه مفهوم نسبي، من أهم مؤشراته: الاستقرار الاجتماعي، السياسي والاقتصادي، ويتم التركيز عادة في دراسته على الاستقرار السياسي في علاقته بقدرة النظام على احتواء الصراعات والانقسامات داخل المجتمع، وما يتضمنه الاستقرار أو عدم الاستقرار المجتمعي من بعد أمني (داود، 2014، ص-ص: 184-187). والاستقرار الاجتماعي مثلا يمكن تعريفه بأنه حالة التوازن والهدوء التي تسود المجتمع، أما السياسي فيشمل غالبا استقرار نظام الحكم ومؤسسات الدولة وطبيعة التفاعل بين الدولة والمجتمع. ومع ذلك لا يوجد تعريف دقيق لمفهوم الاستقرار المجتمعي في أدبيات العلوم الاجتماعية، وربما يعود ذلك إلى أنه مفهوم مركب وتتداخل فيه عناصر عديدة، كما تختلف المعايير التي على أساسها يوصف مجتمع أو بلد بأنه مستقر من حالة إلى أخرى.

2.2. تهديد خصوصية الفرد في الفضاء الإلكتروني:

ساهم التطور التكنولوجي وثورة المعلومات في جعل الحياة بسيطة ومريحة إلى حد بعيد، فهذا التطور قد اختزل المسافات الجغرافية والوقت والجهد وحتى المال، لكنه في الوقت نفسه جعل الخصوصية الفردية في الفضاء الإلكتروني مهدّدة بالاختراق على يد جماعات الهاكرز (Hackers) المختصة، في ظل انتشار التعامل الإلكتروني أيضا مقابل هاجس أمن الفرد في هذا الفضاء.

يعرّف الاختراق بأنه الدخول غير المشروع إلى المواقع، حيث يتم استغلال بعض الثغرات، ومن المعلوم أن تطور التقنية أدى إلى تطور أساليب الجريمة المعلوماتية (الزنط، ص-ص: 4-5). وانطلاقا من ذلك يحدث التعدي على الحياة الخاصة للفرد بالتعرف على محادثاته وما يرسله من محتوى (بيانات، صور ومقاطع فيديو).

هذا يذكرنا بحادثة "كارنيفور" الشهيرة (Carnivore) مطلع الألفية، وهو عبارة عن برنامج أمريكي للتجسس على اتصالات الإنترنت مما يهدد أمن مستخدمي الشبكة (الزنط، ص20).

وقد يصل الأمر إلى حد الابتزاز الذي يحدث إما لدوافع مالية أو جنسية، وهو معروف بكثرة في المجتمعات، لكن الخوف وعدم التبليغ عن هذا النوع من الجرائم ساعد في انتشاره وتهديده لحياة الفرد واستقرارها. ويعتمد الابتزاز على استخدام العنف أو التهديد به، مما يقيد حرية الأشخاص ويؤثر في حياتهم الخاصة، ويجعلهم يستسلمون للمطالب. ومما يشجع على انتشاره أن المؤسسات التي تسهر على حماية المواطنين تظل ضعيفة بالنظر إلى خصوصيات هذه الجريمة، وإحجام الأشخاص عن التبليغ الفوري خاصة بالنسبة للإناث في المجتمعات المحافظة.

3.2. انتشار التطرف الديني:

يشير مفهوم التطرف الديني إلى المغالاة والتشدد في تفسير أمور الدين والالتزام بشكل لا يكون مقبولا في المجتمع، فيهدد استقرارَه وتلاحمَه. ومع اعتماد الجماعات والتنظيمات المتطرفة على الوسائل الإلكترونية والمنصات الاجتماعية (فيسبوك وتويتر) في نشر الفكر المتطرف دينيا وتجنيد أكبر عدد من الأفراد، انتشرت هذه الظاهرة بسرعة فأصبح تأثيرها على صعيد استقرار المجتمعات أكثر خطرا، وهو ما اتضح في المنطقة العربية خلال السنوات الأخيرة.

تعد المدونات، المواقع التفاعلية والمنصات الاجتماعية من أكثر الأدوات التي يعتمد عليها الإرهابيون لاستقطاب الدعم واختراق استقرار المجتمعات (Zahri, Rabiah, p.03). ويُعدُّ انتشار مواقع التواصل الاجتماعي ذا أثر كبير في الانتشار الواسع للأفكار المتطرفة لدى الأفراد والمجتمعات، في ظل ما تقوم به الجماعات والتنظيمات الإرهابية من نشر لمحتوى الكراهية والتطرف واستهداف فئات واسعة من الجماهير بغرض ممارسة تأثير فعال على الرأي العام.

وذكر تقرير لمركز دراسات التطرف بلندن بأن تنظيم "داعش" قد تمكن من استقطاب أكثر من 10 آلاف فرد للانخراط في صفوفه حتى منتصف العام 2014، وذلك من خلال منصات التواصل الاجتماعي (عبد الفتاح، 2014، ص-ص: 35-36). وهو ما يعكس حجم التداعيات السلبية على استقرار المجتمعات وزعزعة قيمة الاعتدال والوسطية في الدين، بحيث يعد أسلوب الدعاية للتطرف والإرهاب من أهداف استخدام الجماعة الإرهابية للإنترنت والوسائط الإلكترونية، مما يؤثر في نفسية الفرد ويساهم في زعزعة جانب القيم الاجتماعية والتربوية ذات الصلة بالدين (تقرير أممي، 2013، ص-ص: 3-5).

كما بات الفضاء الافتراضي وسيطا لتدريب الأفراد على الفعل الإرهابي وتعليم كيفية صنع المتفجرات واستخدام الأسلحة، بالإضافة إلى استغلال الفضاء الإلكتروني في تمويل الأعمال الإرهابية تحت غطاء خيري، بحيث أصبح هذا الفضاء مصدرا لذلك (تقرير أممي، ص-ص: 7-8). ومن الممكن القول بأن التنظيمات الإرهابية في المنطقة العربية استمدت قسطا كبيرا من قوتها من الشبكة العنكبوتية ومواقع التواصل الاجتماعي، نظرا لالتفاف أعداد هائلة من الأفراد حولها واستعداد أعداد كبيرة لاعتناق الأفكار المتطرفة والدفاع عنها باستماتة أحيانا.

لقد أدى انتشار التطرف الديني عبر المنصات الاجتماعية إلى انتشاره وتوسُّع نطاقه الجغرافي. فالترويج للفكر المتطرف عبر الفضاء الرقمي وقابلية أعداد كبيرة من الأفراد عبر العالم لاستهلاكه يظل تهديدا فعليا يواجه الدول والمجتمعات. وقد تمكنت ظاهرة "المقاتلين الأجانب" من خلق هواجس أمنية للدول، فعودة هؤلاء الأفراد مستقبلا إلى بلدانهم الأصلية تعد تهديدا فعليا للاستقرار المجتمعي.

ويمكن تلخيص أهم الانعكاسات والتداعيات التي تفرزها ظاهرة الإرهاب الإلكتروني بالنسبة للاستقرار المجتمعي كما يلي:

* التأثير على نفسية الأفراد بنشر الخوف والقلق نتيجة لإحساسهم بغياب الأمن في الفضاء السيبراني.
* استهداف قيم المجتمع النبيلة واللعب على الجانب الروحي للفرد لجعله يتعاطف ويناصر الجماعات الإرهابية، وذلك بغرس فكرة القضية العادلة المدافَع عنها.
* الترويج للتطرف الديني والكراهية القائمة على أساس الطائفة والمذهب والجنس، مما يساهم في زعزعة أو هدم تلاحم المجتمعات واندماجها.

انطلاقا مما سبق يمكن القول إن انعكاسات الإرهاب الإلكتروني على الاستقرار المجتمعي لا يمكن الاستهانة بها، وهذا بالنظر إلى حجم الضرر النفسي الذي يصيب الأفراد سواء عبر التعدي على خصوصياتهم وحياتهم الشخصية، أو بالعمل على تهديد القيم الخلقية وقيمة الوسطية في الدين وزرع الكراهية والحقد على أساس ديني وطائفي، وهو ما اتضح جليا مع انتشار التطرف الديني خلال السنوات الأخيرة وارتباطه بارتفاع معدل الأعمال الإرهابية في المنطقة العربية بوجه خاص.

كما توجد أشكال أخرى من الانعكاسات لهذه الظاهرة على استقرار المجتمعات، مثل ضرب الاقتصاد الوطني والسياحة وأمن الدولة في العمق، مما يطرح ثغرة واسعة على صعيد أمن الفضاء السيبراني بكافة أبعاده.

3. إستراتيجيات مكافحة الإرهاب الإلكتروني:

في هذا العنصر الأخير من المقال، يتم تقديم لمحة عن الإستراتيجيات الدولية الخاصة بمكافحة الإرهاب الإلكتروني والوقاية منه، وذلك بالإشارة إلى بعض التجارب ومن بينها السياسة الجزائرية في مجال مكافحة الجرائم الإلكترونية بشكل عام.

1.3. مفهوم إستراتيجية مكافحة الإرهاب:

مقهوم إستراتيجية مكافحة الإرهاب "يتضمن مجموعة من النشاطات تتجاوز ذات هذا المفهوم، وتشمل الاستخدام الفعال لمجموعة من الأدوات. إن كل أداة من أدوات مواجهة الإرهاب هي صعبة الاستعمال، ومن الصعب أكثر استخدام هذه الأدوات بشكل جيد، إلا أن استخدام هذه الأدوات في مواجهة الإرهاب يبقى حاسما" (عطية، 2018، ص75). معنى ذلك أن هذه الإستراتيجية يجب أن تكون شاملة وغير محصورة في الجانب الأمني والعسكري الضيق، بحيث تتضمن في المقابل سياسات واقية تردع ممارسات الإرهاب كاستخدام مجموعة من الأساليب والآليات الأمنية والسياسية والقانونية والتنموية والاجتماعية والثقافية. لذلك يمكن القول بأن التصدي للإرهاب يستدعي تضافُر جهود العديد من القطاعات، عديد الفواعل والقنوات. فإذا كان تعريف الإستراتيجية هو حشد الموارد والوسائل لتحقيق الأهداف فإن هذا التعريف ينطبق على كافة المجالات بما فيها مجال مكافحة الإرهاب.

ومع التحول في الظاهرة الإرهابية على صعيد الانتشار الجغرافي والأساليب والوسائل، أصبحت مواجهة أشكال التهديد في الفضاء السيبراني ضرورة، خاصة مع انتشار أسلوب الحكومة الإلكترونية وما يتطلبه من توفير للأمن في هذا الفضاء بالنسبة للمستخدم ومؤسسات الدولة. وتنطلق المواجهة من تحديد طبيعة التهديد وحجمه، فالمجال الافتراضي اليوم ساحة من ساحات الحرب والصراع والسيطرة، وطبيعة ظاهرة الإرهاب الإلكتروني تفرض على الدول مراجعة عقائدها الأمنية في تفعيل آليات المواجهة.

2.3. نماذج دولية لمكافحة الإرهاب الإلكتروني:

أفرز الاستخدام الواسع للفضاء الرقمي نوعا جديدا من الجرائم العابرة للحدود، "الأمر الذي بات يثير بعض التحديات القانونية أمام الأجهزة المعنية بمكافحة الجريمة، فيما يتعلق بإثبات هذه الجرائم" (يحيى، 2013، ص68). لقد أصبح الإرهاب السبراني بديلا عن الإرهاب في صورته التقليدية، وهو في تزايد نتيجة الاستخدام الكبير للإنترنت، فقد ذكرت دراسة لعام 2011 بأن الإمارات العربية المتحدة واجهت 19 جريمة حديثة (رقمية) ولبنان 25 جريمة، وهذا كمثال فقط (UN, 2015, p.05). ويُعد وضع إطار تشريعي يتضمن سياسات وآليات المواجهة محطة أساسية في أيّ إستراتيجية.

عملت منظمة الأمم المتحدة على مواكبة التطور التكنولوجي ودوره في انتشار الجرائم الإلكترونية بما فيها الإرهاب الإلكتروني، ويعد اتحاد الاتصالات الدولية (ITU) واحدا من الوكالات الدولية التي تهتم بمواكبة التطور التكنولوجي في مجال الاتصال، والعمل على بحث سُبل تعزيز الثقة والأمن في الفضاء السيبراني والتصدي للرسائل المقتحمة والتهديدات التي توجه جهاز الحاسوب (الاتحاد الدولي للاتصالات، 2018).

وأصدر مجلس الأمن الدولي قراره رقم 1624 لعام 2005، الخاص بمكافحة الإرهاب والدعاية للنشاط الإرهابي عبر الإنترنت، كما أكد تقرير الأمين العام الأممي في 2006 بعنوان: "الاتحاد في مواجهة الإرهاب: توصيات لإستراتيجية عالمية لمكافحة الإرهاب"، أن تمويل وتدريب وتجنيد الأفراد للنشاط الإرهابي عناصر أساسية في هذا النشاط، وهي تتخذ من شبكة الإنترنت وسيطا لها (UN, p-p :16-17).

ومن الجهود ونماذج مكافحة الإرهاب الإلكتروني يمكن ذكر تجربة منظمة حلف الشمال الأطلسي (الناتو)، ففي قمة براق شهر نوفمبر 2002 عزم الحلف على زيادة قدراته لمواجهة الهجمات السيبرانية، وتم تحضير عدد من الأجهزة المتخصصة مثل: وكالة خدمات أنظمة المعلومات والاتصال (NCSA)، والمركز التقني المكلف بأمن الحواسيب والاتصال. وعلى إثر هجمات إستونيا في عام 2007 برز مفهوم الدفاع السيبراني للناتو في أكتوبر 2008 (Bogdanoski, Petreski, p-p :65-66)، مع الإشارة إلى أن الحلف واجه قبل ذلك هجمات إلكترونية أثناء أزمة كوسوفو سنة 1999، مما جعل بريده يتعطل، لكن التعامل مع ذلك أتى في إطار اعتباره مشكلة تقنية محدودة التأثير (http://www.nato.int/docu/review/2011/11-september/Cyber-Threats/AR/index.htm).

كما تعنى منظمة الأمن والتعاون في أوروبا (OSCE) بتحديات الأمن السيبراني ومن ضمنها الإرهاب الإلكتروني. ففي 2004 أقرّ المجلس الوزاري الأوروبي التصدي لاستخدام الإنترنت من قبل الإرهابيين في أغراض الدعاية والتجنيد، مما يفرضه ذلك من تعاون حثيث على الصعيد الدولي لمراقبة تحركات الجماعات الإرهابية، وتبادل المعلومات بين حكومات منظمة الأمن والتعاون الأوروبية (Bogdanoski, Petreski, p.68).

وفي ماليزيا تم فرض عقوبات في سنة 1997 على الدخول غير المشروع بهدف التخريب أو التعديل، من ضمنها فرض السجن لمدة تصل إلى 10 سنوات (كافي، وآخرون، 2015، ص-ص: 166-167).

وكانت إستونيا من الدول التي أعادت النظر في مفهوم الأمن على إثر الهجمات التي شهدتها في 2007، وذلك من خلال "إعادة تصور جديد في منظومتها الدفاعية للتهديدات الأمنية داخل الفضاء الافتراضي" (بلفرد، ص145). كما تستند الإستراتيجيات الأوروبية إلى الربط بين العمل الأكاديمي والميداني بما يعكس "التدريب المتخصص"، وقد أنشأت جامعة دبلن في إيرلندا على سبيل المثال "مركز الأمن السيبراني والتحقيق في الجرائم السيبرانية" سنة 2006 (UN, p.72).

بالنسبة للدول العربية، كانت مصر من الدول التي اهتمت بالتصدي للإرهاب الإلكتروني عبر الدعوة إلى قرار دولي يفرض حظر جميع المواقع المحفزة على الإرهاب ببث محتويات تدريبية لاستخدام الأسلحة وصنع المتفجرات، وبالتالي توحيد جهود المواجهة (الزنط، ص21). كما تم إنشاء المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) في ديسمبر 2012 من قبل الاتحاد الدولي للاتصالات وسلطنة عمان، الهدف منه نشر الوعي بخصوص أمن الفضاء السيبراني وتعزيز الخبرات والتصدي للحالات الطارئة (https://arcc.com/). وتعد جامعة نايف العربية للعلوم الأمنية من المؤسسات الأكاديمية المرموقة عربيا في مجال تطوير الدراسات الأكاديمية وتنظيم تدريبات دولية للتعريف ومواجهة الجرائم السيبرانية.

ويقوم التحقيق في مجال الجرائم الإلكترونية والإرهاب الإلكتروني على آليات متنوعة من بينها استخدام برمجيات "حصان طروادة" (RATs)، بحيث تُزرع سرا في الحواسيب لجمع البيانات أو التحكم في الجهاز المخترق، كما يتم الاعتماد على أدوات خاصة لمعرفة مصدر ومحتوى الاتصال (UN, p.63).

3.3. مكافحة الإرهاب الإلكتروني في الجزائر:

تندرج مكافحة الإرهاب الإلكتروني في الجزائر ضمن مكافحة الجريمة السيبرانية بكافة أشكالها، مع أنه يوجد غموض وعدم دقة في النصوص القانونية الوطنية في تعريف هذا النمط من الجرائم المستحدثة. لقد تنبّه المشرّع الجزائري إلى ضرورة جعل المنظومة القانونية مواكبة للتطور الحاصل في تكنولوجيا المعلومات والاتصال. في هذا الصدد، صدر القانون رقم 04-15 المتعلق بالمعالجة الآلية للمعطيات (نوفمبر 2004)، ثم القانون رقم 09-04 لسنة 2009، والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ومن التدابير المتخذة من قبَل الحكومة الجزائرية ما يتعلق بالوقاية الإلكترونية التي تشمل، كما حددها القانون 09-04، الوقاية من جرائم الإرهاب والمساس بأمن الدولة، الوقاية من التعدي على أنظمة معلومات يكون هدفه المساس بالدفاع الوطني، ما تقتضيه التحريات والتحقيقات القضائية والمساعدات القضائية الدولية. كما نص القانون على قواعد تفتيش منظومات المعلومات وحجز المعطيات في إطار التحريات (القانون 09-04، 2009، ص، ص: 06، 08).

كما نص قانون العقوبات على عقوبات بالسجن والغرامة المالية، تختلف باختلاف الجريمة المرتكبة، مثال ذلك المادة 394 مكرر، مع مضاعفة العقوبة بالنسبة للجرائم التي تمس أمن الدولة والدفاع الوطني بنص المادة 394 مكرر 3 (قانون العقوبات، 2015، ص-ص: 157-158).

واهتمت وزارة الدفاع الوطني بحفظ الأمن السيبراني، عبر وضع سياسات وبرامج واستحداث آليات لمكافحة الجريمة السيبرانية وحماية البنية التحتية للمعلومات (بارة، 2017، ص264). وتم تعبئة عدد من الأجهزة المتخصصة لحماية أمن الفضاء السيبراني والوقاية من الجريمة مثل: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (القانون 09-04، ص08)، هيئات ذات اختصاص إقليمي تعنى بالجرائم الإلكترونية الواقعة خارج الحدود الوطنية والتي تمس الأمن الوطني، المعهد الوطني للأدلة الجنائية وعلم الإجرام، المديرية العامة للأمن الوطني (عاقلي، 2017، ص-ص: 132-133).

وقد صدر القانون رقم 20-05 (أفريل 2020) المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ليشكّل تكملة لجملة القوانين والنصوص المتعلقة بمكافحة الإجرام والإجرام الإلكتروني ويهدف إلى أخلقة الحياة العامة، مع توصية بإنشاء مرصد وطني للوقاية من التمييز وخطاب الكراهية. ينص القانون على تدابير وعقوبات متنوعة تمس كذاك من يستخدم تكنولوجيا الإعلام والاتصال (وهنا إشارة إلى شبكات التواصل الاجتماعي)

لغرض الدعاية والكراهية ونشر العنف، مع التشديد في جريمة استخدام هذه التكنولوجيا لنشر العنف في المجتمع (القانون 20-05، 2020، ص-ص: 06-08).

وكتقييم لبعض الجهود الدولية في مجال مكافحة الإرهاب الإلكتروني يمكن القول إن استمرار التطور التكنولوجي والاستخدام المتزايد لشبكة الإنترنت من بين أهم التحديات التي تقف في وجه سياسات وإستراتيجيات الدول، إلى جانب عدم وجود تعريف جامع للإرهاب الإلكتروني، والثغرات القانونية بالنسبة لهذا النوع من الجرائم، مثل غياب العنصر المادي أحيانا وصعوبة كشف الجريمة في حينها. يضاف إلى ذلك غياب سياسة تشريعية موحدة في مجال مكافحة الإرهاب الإلكتروني كما هو الحال لدى الدول العربية.

خاتمة:

يُعد الإرهاب الإلكتروني واحدا من التهديدات الأمنية الجديدة، وهو امتداد للتهديد الإرهابي الذي عرف جملة من التحولات في طبيعته وأساليبه خلال السنوات الأخيرة، في ظل الانتشار الكبير والواسع للتقنية وتطور أساليب العمل الإرهابي بالاعتماد عليها للقيام بهجمات تخريبية واعتداءات إلكترونية على مختلف البُنى والنُّظم المعلوماتية، مما يخلف خسائر مادية معتبرة وأضرارا نفسية. وبالنظر إلى خصائص الإرهاب الإلكتروني واستغلاله لبعض الثغرات الموجودة في الفضاء السيبراني، أصبح من بين التهديدات التي لا تقل خطورة ومساسا بالاستقرار المجتمعي. من النتائج التي توصل إليها البحث أنّ الإرهاب الإلكتروني ينعكس سلبا على استقرار المجتمعات والأفراد، فهو يمس خصوصيات الفرد عبر أساليب القرصنة واختراق المواقع والحسابات لغايات التجسس والابتزاز، كما يستهدف في الجانب المقابل نشر التطرف الديني باستغلال منصات التواصل الاجتماعي، وهو ما عرفته المجتمعات العربية في ظل انتشار خطر تنظيم "داعش" الإرهابي خلال السنوات الأخيرة، ولم يتوقف الأمر عند ذلك فقد تم تجنيد آلاف الأفراد للقتال في صفوف التنظيم باستخدام أساليب الترغيب والترهيب. وتماشيا مع طبيعة التهديد وخصوصية الفضاء الافتراضي، تبنّت الدول إستراتيجيات متنوعة لمواجهة الإرهاب الإلكتروني في إطار ما يُعرف بمكافحة الجرائم السيبرانية، ومع ذلك فهي تظل نسبية وفي حاجة إلى تكييف قانوني باستمرار وتحديث لآليات المواجهة. وفي هذا الصدد، يمكن تقديم توصيتين: الأولى بخصوص السعي إلى الاتفاق على مفهوم جامع مانع للإرهاب الإلكتروني، بالإضافة إلى تفعيل التعاون في المجال التشريعي بين الدول (مثلا في المنطقة العربية)، والثانية تخص الحالة الجزائرية بحيث وجَب وضع تعريف دقيق للجريمة الإلكترونية وتحديد واضع لمفهوم الإرهاب الإلكتروني.

قائمة المراجع:

أولا- الوثائق الرسمية

- الجمهورية الجزائرية الديمقراطية الشعبية، الجريمة الرسمية رقم 25، السنة: 57، القانون رقم 20-05، المؤرخ في 29 أفريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.
- الجمهورية الجزائرية الديمقراطية الشعبية، الجريمة الرسمية رقم 47، القانون رقم09–04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- الجمهورية الجزائرية الديمقراطية الشعبية، رئاسة الجمهورية، الأمانة العامة للحكومة، قانون العقوبات، السنة: 2015.

ثانيا –الكتب

- شفيق، حسنين. (2015). الإعلام الجديد والجرائم الإلكترونية: التسريبات، التجسس الإلكتروني، الإرهاب، مصر: دار فكر وفن للطباعة والنشر والتوزيع.
- عبد الصادق، عادل. (2009). الإرهاب الإلكتروني والقوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مصر: مركز الدراسات السياسية والإستراتيجية.
- عبد الكافي، إسماعيل عبد الفتاح. (2006). الإرهاب ومحاربته في العالم المعاصر، مصر: د.د.ن.
- العبيدي، علي. (2018). الإرهاب واستعصاء المفهوم، تونس: دار المنتدى.
- عطية، إدريس. (2018). التهديدات الإرهابية الجديدة في إفريقيا: دراسة في توظيف الظاهرة وتموضعها الجيوبوليتيكي، الأردن: دار الإعصار العلمي.
- مصطفى، محمد موسى. (2009). الإرهاب الإلكتروني: دراسة قانونية، أمنية، نفسية، اجتماعية. مصر: دار الكتب والوثائق القومية المصرية.
- كافي، مصطفى يوسف، وآخرون. (2015). الإعلام والإرهاب الإلكتروني، الأردن: دار الإعصار.
- وهبان، أحمد محمد. (2015). ظاهرة الإرهاب بين صورها التقليدية وأنماطها المستحدثة، المملكة العربية السعودية: سلسلة إصدارات جامعة الملك سعود.
- مجموعة باحثين. (2017). الجريمة الإلكترونية، لبنان: منشورات مركز جيل البحث العلمي.
- مجموعة باحثين. (2014). صعود الراديكالية الدينية في العالم العربي: الأسباب، المؤشرات والإستراتيجيات المضادة، عمّان: مؤسسة فريدريش إيبرت.
- الاتحاد الدولي للاتصالات. (2018). تقرير الأمين العام الأممي: أنشطة الاتحاد الدولي للاتصالات بشأن تعزيز دوره في تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، نيويورك.
- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فرقة العمل التابعة للأمم المتحدة المعنية بتدابير مكافحة الإرهاب. (2013). استخدام الإنترنت في أغراض إرهابية، نيويورك.
- United Nations. (2015). Policy Recommendations on Cybersafety and combating Cybercrime in the Arab region. Newyork.

ثالثا –الدوريات والملتقيات

- بارة، سمير (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني. العدد: 04، الجزائر: جامعة باتنة، الصفحات: 255-280.
- بلفرد، لطفي (2016). الفضاء السيبراني: هندسة وفواعل. المجلة الجزائرية للدراسات السياسية. العدد: 05، الجزائر: المدرسة الوطنية العليا للعلوم السياسية، الصفحات: 145-155.
- حسن ملّا خاطر، مايا (2015). الإطار القانوني لجريمة الإرهاب الإلكتروني. مجلة جامعة ناصر. المجلد: 01، العدد: 05، اليمن: جامعة ناصر.
- داود، أحمد فاضل جاسم (2014). عدم الاستقرار المجتمعي في العراق ما بعد 2003: دراسة تحليلية في التحديات المجتمعية والآفاق المستقبلية. المجلة السياسية والدولية. العدد: 25، العراق، ص-ص: 182-217.
- عطية، إدريس (2015). تهديدات الإرهاب الدولي في منطقة شمال إفريقيا. المجلة الجزائرية للدراسات السياسية. العدد: 04، الجزائر: المدرسة الوطنية العليا للعلوم السياسية، الصفحات: 29-38.
- عمير، حسن تركي، وعبد الله، سلام جاسم (د.س.ن). الإرهاب الإلكتروني ومخاطره في العصر الراهن. مجلة العلوم القانونية والسياسية. عدد خاص. العراق: جامعة ديالى.
- يحيى، ربيع محمد (2013). إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الوسط. مجلة رؤى إستراتيجية، الإمارات العربية المتحدة.
- سينجر، بيتر (2018). الإرهاب الإلكتروني: خرافات وحقائق، وفيروس ستوكسنت، ووسائل الإعلام الاجتماعي، ومسرح المواجهة، سلسلة محاضرات الإمارات. الإمارات العربية المتحدة. أبو ظبي، ب.ت.

- الزنط، سعد عطوة (2010). الإرهاب الإلكتروني وإعادة صياغة إستراتيجيات الأمن القومي، مؤتمر الجرائم المستحدثة: كيفية إثباتها ومواجهتها، مصر، المركز القومي للبحوث الاجتماعية والجنائية، 15-16 ديسمبر.
- Bogdanoski, Mitlko, & Petreski, Drage (). Cyber-Terrorism- Global Security Threat. International Security Defence, Security Peace & Journal. p-p : 59-72.
- Musco, Pierre (2008). La révolution numérique : Techniques et mythologies. La pensé.
- Zahri, Yunos, & Rabiah, Ahmad (2012). A Dynamic Cyber-Terrorism Framework. Internatinal Journal of Computer Science & Information Science. Vol.30, n.30, p02.

رابعا –المواقع الالكترونية

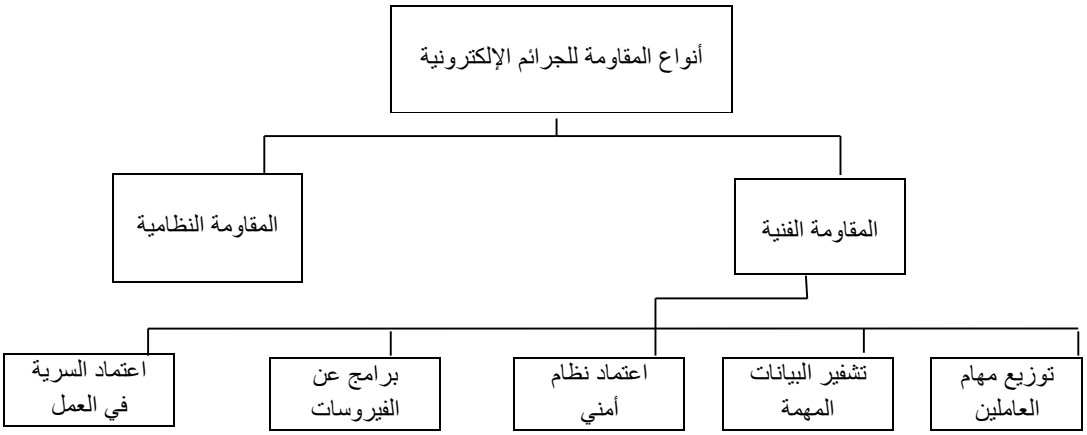
- ناعوس، بن يحيى الطاهر، مكافحة الإرهاب الإلكتروني: ضرورة بشرية وفريضة شرعية، يناير 2015، https://www.alukah.net/library/0/80823، تاريخ التصفح: 2020/09/23.
- الهاشمي، رفد عيادة، الإرهاب الإلكتروني، http//www.mizandz.com/2017/11/pdf.html، تاريخ التصفح: 2020/09/16.
- مجلة الناتو، التهديدات الجديدة: الأبعاد الإلكترونية، 2011/09/11، http://www.nato.int/docu/review/2011/11-september/Cyber-Threats/AR/index.htm، تاريخ التصفح: 2020/09/23.
- المركز العربي الإقليمي للأمن السيبراني، https://arcc.com/، 2020/09/16.

ملاحق:

الشكل (01): أبرز أساليب الإرهاب الإلكتروني.

المصدر: رفد عيادة الهاشمي، http//www.mizandz.com/2017/11/pdf.html، 2020/09/16.

الشكل (02): أنواع مقاومة الجرائم والهجمات الإلكترونية.



المصدر: بن يحيى الطاهر ناعوس، مكافحة الإرهاب الإلكتروني: ضرورة بشرية وفريضة شرعية، يناير 2015، https://www.alukah.net/library/0/80823، تاريخ التصفح: 2020/09/23.