

الإرهاب الإلكتروني

د / سعيد عبيدي

جامعة سيدي محمد بن عبد الله - فاس - المغرب

ملخص:

في السنوات الأخيرة عرفت المجتمعات البشرية تطورات وأحداث متسارعة، من ذلك ظهور الحواسيب والإنترنت ومواقع التواصل الاجتماعي وغيرها، الأمر الذي سيمهد لاحقا لظهور العمليات الإرهابية في جميع الدول، لذلك تتناول مجموعة من الباحثين على عاتقهم دراسة العلاقة بين الإرهاب والإنترنت التي ظهرت إلى حيز الوجود وشغلت بال الدول والمنظمات المعنية بمكافحة الإرهاب بعد إحداث الحادي عشر من سبتمبر 2001، إذ الإرهاب لم يعد مقتصرًا على المجال المادي الواقعي فقط، بل انتقلت التنظيمات الإرهابية إلى الفضاء الإلكتروني مما أعطى الانطلاقة لما أصبح يعرف بالإرهاب الإلكتروني الذي أصبح عاملاً مساعداً للعمل الإرهابي التقليدي المادي، وذلك بتوفير المعلومات عن الأماكن المستهدفة، أو كوسيط في تنفيذ العمليات الإرهابية بصفة عامة، بالإضافة إلى بأنه أصبح عامل تحريض على الكراهية الدينية وحرب الأفكار، لذلك بدأت هذه المنظمات الإرهابية تسعى إلى الاستفادة من الإنترنت واستثماره في التتقيب عن المعلومات، والحصول على التمويل والتبرعات وتجنيد وحشد الأتباع، وكذلك تحقيق الترابط التنظيمي بين الجماعات وتبادل المعلومات والأفكار والمقترحات حول كيفية إصابة الهدف واختراقه وكيفية صنع المتفجرات. في هذه الدراسة سنحاول التعرف على مفهوم الإرهاب الإلكتروني وأشكاله ونقاط التشابه والاختلاف بينه وبين الإرهاب التقليدي، ومن ثم إلقاء الضوء على الدور الذي يجب أن تضطلع به الدول والجماعات والأفراد للتصدي لهذه الظاهرة والوقاية منها.

الكلمات المفتاحية: الإرهاب، الارهاب إلكتروني، الإنترنت، هجمات، الشبكات المعلوماتية، التقنية.

Abstract :

In the recent years, human societies have known a rapid developments and events, such as, using computers, Internets, social media and others. Consequently, this has paved the way for terrorist actions to take place later in all countries. Thus, many researchers have taken charge of studying the Internet and terrorism relation, which has come to existence and worried many countries and organizations that are in responsible of fighting terrorism after, September 2001, incident. This is so, because terrorism is no longer concerned with tangible and traditional fields only, but it has prevailed to electronic spaces as well. The latter has been a starting point to what is known as the “Electronic Terrorism”, which has become a helping factor to tangible and traditional terrorism by either providing information about the targeted place or as an intermediary to implement the touristic actions. Furthermore, it has become an incitement factor to religion hatred and growing war ideas. By and large, the terroristic organizations have started to strive in order to benefit from the Internet and invest in it in favor of searching for information and getting finance, donation and equipping the followers. In addition to this, realizing the correlation between communities and exchanging information, ideas and suggestions about the manner by which they can point and penetrate the target area and how to make bombs. In the current study, we will try to define the electronic terrorism and its types, besides, spotting the similarities and differences between the electronic terrorism and the traditional one. Last but not least, shedding light to the role, which countries, communities and individuals must undertake so as to confront and prevent this phenomenon.

Key words: Terrorism Electronic terrorism, Traditional terrorism, Technology, Internet, Terroristic organizations.

مقدمة:

لقد أدّى ظهور الإنترنت والحواسيب والآلات الذّكية وغيرها إلى تغيّر شكل الحياة اليومية، فقد أصبح الاعتماد على هذه الوسائل يزداد يوماً بعد يوم، سواء في المؤسسات المالية، أو المرافق العامّة، أو المجال التّعليمي، أو الأمني أو غير ذلك، بيد أنّه وإن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد، فإنّ الوجه الآخر والمتمثل في الاستخدامات السيئة والضّارة لهذه التّقنيات الحديثة أصبح خطراً يهدّد العالم بأسره، فمع هذا التّطور المطرد لهذه التّقنيات تطوّرت أساليب المجرمين وعلى رأسهم الإرهابيين الذين عمدوا في الآونة الأخيرة إلى استخدام التّقنية الرّقمية لتنفيذ عملياتهم الإرهابية، لذلك طغى على السّاحة في عصرنا الزّاهن نوع جديد من الإرهاب هو ما أصبح يعرف "بالإرهاب الإلكتروني" أو "الإرهاب الرّقمي (Electronic or Digital Terrorism)"، إذ بات من السّهل عند هؤلاء تهديد الحياة العامّة عن طريق اقتحام المواقع الإلكترونية وتدميرها وتغيير محتوياتها، أو الدّخول على شبكات الاتّصال بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً...، كما بات عندهم من الصّروري ابتكار آلاف المواقع لنشر أفكارهم ومعتقداتهم والتّخطيط والتّجهيز لعمليات إرهابية، ولتنسيق وتبادل الخبرات الميدانية العملية فيها بينهم، فالإرهاب الإلكتروني هدفه إلحاق الشّلل بأنظمة القيادة والسيطرة والاتّصالات، وكذا تعطيل أنظمة الدّفاع واختراق النظام المصرفي وإرباك حركات الطيران المدني وشلّ مخططات الطاقة الحرارية أو النّووية، فهذا هو الأسلوب الجديد للإرهابيين حالياً في محاولة الوصول إلى أغراضهم بكلّ ارتياح وطمأنينة، لذا من الأهميّة بمكان مدارس مفهوم الإرهاب الإلكتروني، ومعرفة أشكاله، وطرق مكافحته.

مفهوم الإرهاب الإلكتروني:

يعرّف الإرهاب الإلكتروني على أنّه "جريمة العدوان أو التّخويف أو التّهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية، سواء كان صادراً من الدّول أو الجماعات أو الأفراد على الإنسان بشكل عام، وعلى سبيل المثال الأعمال غير المشروعة التي يكون فيها

الكمبيوتر أو الهاتف إمّا وسيلة أو هدفاً أو كليهما، والتي من شأنها أن تؤدي إلى الأنشطة التخريبية أو التهديد بها في عالم الإنترنت، مع نيّة تحقيق المزيد من الأهداف الدينية أو السياسية أو نحوها، أو لتخويف أيّ شخص وبثّ الرعب في نفسه¹.

ويعرّف كذلك على أنّه "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حقّ، باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتّى صنوف العدوان وصوّر الإفساد"².

كما عرّفته الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في بودابست عام 2001 على أنّه "هجمات غير مشروعة، أو تهديدات بهجمات ضدّ الحواسيب أو الشبكات أو المعلومات المخزّنة إلكترونياً، توجّه من أجل الانتقام أو الابتزاز أو الإكراه أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره، لتحقيق أهداف سياسية أو دينية أو اجتماعية معيّنة. وبالتالي لكي ينعّت شخصا ما بأنّه إرهابياً على الإنترنت، وليس فقط مخترقاً، فلا بدّ وأن تؤدي الهجمات التي يشنّها إلى عنف ضدّ الأشخاص أو الممتلكات، أو على الأقلّ تحدث أذى كافياً من أجل نشر الخوف والرعب"³، وهذا يعني أنّ الإرهاب الإلكتروني يهدّد سلامة الأفراد والدول، ويتبنّاه ويقوم به أفراد ودول، الهدف المتوخّى منه هو زعزعة الاستقرار والترويع والتشويش والابتزاز والإساءة، وتدمير كلّ ما هو حيوي من خطوط الطاقة والاتصالات والمعلومات الرقمية.

فالإرهاب الإلكتروني إذن من خلال هذه التعاريف يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف الآخرين، وإلحاق الضرر بهم.

نقاط التشابه والاختلاف بين الإرهاب الإلكتروني والإرهاب التقليدي:

من خلال التعاريف السابقة يتّضح لنا أنّ الإرهاب الإلكتروني لا يختلف كثيراً عن الإرهاب "التقليدي"؛ فالقاعدة الأساسية التي يستند إليها الإرهاب التقليدي هي نفسها التي يستند إليها الإرهاب الإلكتروني؛ وهي التهديد وما يثيره من فزع وخوف وترويع، والذي يؤدي في نهاية المطاف إلى عدم الاستقرار النفسي لدى الضحية، ضف إلى ذلك أنّ كلاهما الغرض منه هو الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر من جهة، وأنّ كلاهما يقوم على خلفية سياسية أو عرقية أو دينية من جهة أخرى.

ورغم اتّفاقيتهما في الهدف فإنّ الإرهاب الإلكتروني يختلف عن الإرهاب التقليدي في عدة نقاط أهمّها الوسيلة المستخدمة؛ فالإرهاب التقليدي يلجأ فيه الإرهابيون إلى استعمال الوسائل التقليدية العادية في تنفيذ عملياتهم الإرهابية كاستخدام السلاح أو القنابل، على عكس الإرهاب الإلكتروني الذي يعتمد على التقنية الرقمية المتطورة من حاسوب وإنترنت وآلات ذكية، كما أنّ الإرهاب الإلكتروني يختلف عن الإرهاب التقليدي من حيث مكان تنفيذ العمليات، فالتقليدي يرتكب في العالم المادي الملموس والمرئي والذي تسهل فيه معاينة الجريمة، بينما الإلكتروني يُرتكب في العالم الافتراضي أي عبر الإنترنت والذي يصعب فيه اكتشاف مدبر ومنفذ الجريمة⁴.

أشكال ومظاهر الإرهاب الإلكتروني:

يتّخذ الإرهاب الإلكتروني مظاهر وأشكال متعدّدة نذكر منها:

1- قيادة الجماعات الإرهابية ونشر الأفكار المتطرّفة: حيث يمكن من خلال شبكة الانترنت بثّ الأفكار المتطرّفة سواء أكانت سياسية أو دينية أو عنصرية، وبالتالي السيطرة على وجدان وعاطفة الأفراد واستغلال معاناتهم لتحقيق أهداف إرهابية، والإساءة إلى المجتمع ككلّ، فالجماعات والمنظمات الإرهابية تستخدم الشبكة المعلوماتية العالمية لنشر ثقافة

الإرهاب والترويج لها، وبتّ الأفكار التي تنادي بها، كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الرّاعبين في تبني أفكارها ومبادئها، فمن خلال الشّبكة المعلوماتية تقوم هذه التّنظيمات بتكوين من لديهم ميول واستعداد للانخراط في الأعمال التّدميرية والتّخريبية، ممّا يوفّر لديها قاعدة ممّن تجمعهم نفس الأفكار والتّوجهات، فيسهل تجنيدهم لتنفيذ هجمات إرهابية في المستقبل⁵.

إنّ استخدام عناصر جديدة داخل التّنظيمات الإرهابية، يحافظ على بقائها واستمرارها؛ لذا فإنّ الإرهابيين يقومون باستغلال تعاطف بعض أفراد المجتمع مع قضاياهم، فيجتذبونهم بأسلوب عاطفي، وعبارات حماسية برّاقة، وذلك من خلال غرف الحوار والمنتديات والمواقع الإلكترونية .

2- القصف الإلكتروني: ويطلق عليه كذلك مصطلح "التّشبع" (Saturation) أو الهجوم المعلوماتي، أو الإغراق بالرسائل، وهو نوع من الاعتداء ضدّ الجهوية أو قابلية عمل النّظام المعلوماتي، ويقضي بملء نظام معلوماتي بكمّ هائل من البيانات إلى حدّ لا يعود بالإمكان معه استعماله بشكل صحيح⁶.

فالقصف الإلكتروني إذن هو أسلوب يستخدمه الإرهابيون للهجوم على شبكات المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى موقع من المواقع ممّا يزيد الضّغط على قدرته على استقبال الرسائل من المتعاملين معه، وهو ما يؤدّي إلى تعطيل هذا الموقع وعدم إمكانية استقباله لأيّة رسائل أخرى، وبالتالي تكبّد خسائر مادية ومعنوية غير محدودة، وهو ما ينتج عنه في نهاية الأمر زعزعة ثقة المتعاملين مع أصحاب هذه المواقع⁷.

وقد ازدادت في الآونة الأخيرة حوادث تعرّض مواقع الشّركات المهمّة على شبكة الإنترنت لهجمات مكثّفة من قبل الإرهابيين، إذ يقوم هؤلاء بإمطار المواقع المستهدفة بفيض لا متناهي من البيانات الموجهة إلى عنوانها الإلكتروني مستخدمين في ذلك عناوين وهمية إلى

درجة لا يعود معها الموقع قادر على استيعاب المزيد من البيانات ممّا يؤدّي إلى توقّفه عن العمل⁸.

وفي ظلّ اعتماد الدّول الكلّي على التّقدم التّكنولوجي أصبح أمر تنفيذ الهجمات المعلوماتية أو القصف الإلكتروني أمراً حتمياً يهدّد بنيتها التّحتية وأهدافها الحيوية وأمنها القومي، وذلك بشنّ هجمات معدّة بطريقة محكمة تدمرها في لحظة واحدة وفي وقت وجيز⁹.

3- تدمير أنظمة المعلومات: قد يستخدم الإنترنت في شنّ هجمات إرهابية بغرض تدمير وإتلاف أنظمة المعلومات التي تعتمد عليها الدّول لاسيّما المتقدّمة في إدارة شؤونها السياسية والاقتصادية والاجتماعية، والمقصود بالتدمير هنا الدّخول غير المشروع إلى "نقطة ارتباط أساسية أو فرعية متّصلة بالشّبكة المعلوماتية من خلال نظام آلي أو مجموعة نظم مترابطة شبكياً، بهدف تخريب نقطة الاتّصال أو النّظام. وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم، فالمتغيّرات التّقنية، وإلّام المخترق بالثغرات في التّطبيقات والتي بنيت في معظمها على أساس التّصميم المفتوح لمعظم الأجزاء سواء كان ذلك في مكوّنات نقطة الاتّصال أو في النّظم أو في الشّبكة أو في البرمجة، جعلت الحيلولة دون الاختراقات صعبة جداً، بالإضافة إلى أنّ هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرّغبة في الاختراق وتدمير المواقع، ومن المعلوم أنّ لدى المؤسّسات من الإمكانيات والقدرات ما ليس لدى الأفراد. ويستطيع قراصنة الحاسب الآلي (Hackers) التّوصّل إلى المعلومات السّرية والشّخصية، واختراق الخصوصية وسريّة المعلومات بسهولة، وذلك راجع إلى أنّ التّطور المذهل في عالم الحاسب الآلي والشّبكات المعلوماتية يصاحبه تقدّم أعظم في الجرائم المعلوماتية وسبل ارتكابها، ولاسيّما وأنّ مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي¹⁰.

فعملية الاختراق الإلكتروني إذن تتمّ عن طريق تسريب "البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتمّ من أيّ مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدّولة التي يتمّ اختراق مواقعها، فالبعد الجغرافي لا أهميّة له في الحدّ من الاختراقات المعلوماتية، ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التّعقيد الذي يتّصف به نظام تشغيل الحاسب الآلي والشّبكات المعلوماتية، فمن الممكن تصوّر هجوم إلكتروني على أحد المواقع الإلكترونية بقصد تدميرها وشلّها عن العمل، حيث يمكن أن يقوم الإرهابيون بشنّ هجوم مدمر لإغلاق المواقع الحيوية على الشّبكات المعلوماتية، وإلحاق الشّلل بأنظمة القيادة والسيطرة والاتّصالات، ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية، بحيث يؤدّي توقّفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه القنابل والمتفجّرات من آثار. كما يمكن تصوّر هجوم إلكتروني على أحد المواقع الإلكترونية بقصد الاستيلاء على محتوياتها، كما لو قامت إحدى التّنظيمات الإرهابية بشنّ هجوم إرهابي على أحد البنوك والمصارف المالية بقصد السرقة والاستيلاء على الأموال"¹¹.

4- التّجسس الإلكتروني: وهو من الأعمال المستهجنة التي تدخل تحت مظلة الإرهاب الإلكتروني، إذ يقوم الإرهابيون بالتّجسس على الأشخاص أو الدّول أو المنظّمات أو الهيئات أو المؤسّسات الدّولية أو الوطنية، ويتميّز هذا التّجسس عن غيره باستعماله لطريقة عصرية تتمثّل في استخدام الموارد المعلوماتية والأنظمة الإلكترونية التي جلبتها الثّورة التّقنية¹²، فالتّجسس الإلكتروني إذن هو "فعل إعطاء أو الحصول أو نشر أو البحث عن أشياء أو مكتوبات أو وثائق أو معلومات سرية عن الوضع العسكري أو الدّبلوماسي أو الاقتصادي والتي تهّم الدّفاع الوطني أو الأمن الخارجي للدّولة بقصد إيصالها إلى شخص ليست له صفة أو إلى عميل دولة أجنبية"¹³.

طرق الوقاية من الإرهاب الإلكتروني:

للوقاية من الإرهاب الإلكتروني اقترح الباحثون وضع استراتيجيات متنوعة قصيرة وطويلة المدى؛ فعلى المدى القصير يجب أن تعتمد إستراتيجية الوقاية من الإرهاب الإلكتروني على ما يلي:¹⁴

1- تخطيط وتنفيذ الصّربات الوقائية الاستباقية ضدّ الخلايا الإرهابية وإحباط مخططاتها وشلّ قدراتها في الزّمان والمكان المناسبين.

2- استهداف وإضعاف القيادات الإرهابية وزعزعتها وتحبيدها وضرب اتّصالاتها وروابطها البيئية وتجفيف مصادرها البشرية والمالية والفكرية.

3- تجنيد وتفعيل وتوظيف العناصر الاستخبارية من بين العاملين بالتّنظيمات والخلايا الإرهابية، والتأكّد من ولائها للأجهزة الأمنية بصورة دائمة ومستمرة.

أمّا على المدى الطويل فإنّ إجراءات مكافحة الإرهاب الإلكتروني يجب أن تتضمّن ما يلي:¹⁵

1- وضع خطط إستراتيجية شاملة ومترابطة مبنية على دراسات وأبحاث ميدانية معمّقة في مجال مكافحة الإرهاب العالمي بكافة أشكاله وصوّره.

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

3- مراجعة التّكنيكات والتّدريبات المعتمدة لمكافحة الإرهاب بشكل دوري، وتعديل ما يلزم لكي تتناسب ومكافحة التّهديدات الإرهابية المستقبلية على السّاحة العالمية.

4- إجراء البحوث والدراسات وعقد المؤتمرات والندوات وأوراش العمل، بهدف متابعة تطوير وتحديث إجراءات مكافحة الإرهاب على المستويات الوطنية والإقليمية والدولية.

هذا ولحدّ من خطورة الإرهاب الإلكتروني يؤكّد أغلب الباحثين في قضاياها على ضرورة "تفعيل التعاون الدولي بين دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المجرمين، وإصدار عدد من القوانين التشريعية الجديدة لتجريم أيّ استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، بالإضافة إلى التعاون والتنسيق الدائم مع الشرطة الدولية في مجال تبادل المعلومات والخبرات الأمنية والفنية في رصد ومتابعة كافة الأنشطة الإجرامية والإرهابية، خاصّة فيما يتعلّق بالنشاط الإرهابي التكنولوجي لزيادة المستمرّ في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية، وذلك لأنّ الفضاء الإلكتروني بات يشكّل بيئة إستراتيجية جديدة لنموّ وبروز أشكال جديدة من الصراع، ولظهور فاعلين جدد على الساحة الدولية"¹⁶.

خاتمة:

لقد أصبح الإرهاب الإلكتروني هاجسا يؤرّق جميع الدّول لما له من أضرار وخيمة، فالمنظمات والجماعات الإرهابية تسعى من ورائه إلى تضخيم صورتها في ذهنية الأفراد، كما تسعى من خلاله إلى البحث والحصول على التّمويل والتّبرعات وعملية التّجنيد والحشد لأتباعها، وكذلك لتحقيق التّرابط التّنظيمي بين الجماعات وداخلها، و تبادل المعلومات والأفكار والمقترحات والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه، وكيفية صنع المتفجّرات والتّخطيط والتنسيق للعمل الإرهابي، وكذلك في تدمير مواقع الإنترنت المضادّة أو اختراق المؤسسات أو تعطيل الخدمات الحكومية وغيرها من المنشآت الحيوية.

الهوامش

- ¹ - محمد بن عبد الله آل فايع العسيري وحسن بن أحمد الشهري، استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين: الإرهاب الإلكتروني وبعض وسائله والطرق الحديثة لمكافحته، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2012، ص: 225.
- ² - مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية: دراسة مقارنة، دار النهضة العربية، القاهرة، الطبعة الأولى، 2001، ص: 152.
- ³ - انظر: حسن مظفر الرزوي، الفضاء المعلوماتي، مركز دراسات الوحدة العربية، بيروت، الطبعة الأولى، 2007، ص: 63.
- ⁴ - محمد الأمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص: 154.
- ⁵ - عصام عبد الفتاح مطر، التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة، الإسكندرية، 2009، ص: 130.
- ⁶ - وليد الزبيدي، القرصنة على الإنترنت والحاسوب: التشريعات القانونية، دار أسامة للنشر والتوزيع، الأردن، الطبعة لأولى، 2003، ص: 47.
- ⁷ - مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية: دراسة مقارنة، دار الكتب والوثائق العربية، القاهرة، الطبعة الأولى، 2003، ص: 203.
- ⁸ - وليد الزبيدي، القرصنة على الإنترنت والحاسوب: التشريعات القانونية، ص: 47.
- ⁹ - هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، القاهرة، الطبعة الأولى، 2000، ص: 100.
- ¹⁰ - أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، ص: 12.
- ¹¹ - أحمد فتحي سرور، المواجهة القانونية للإرهاب، دار النهضة العربية، القاهرة، الطبعة الأولى، 2008، ص: 78.
- ¹² - انظر: رؤوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، القاهرة، الطبعة الأولى، 1985، ص: 18.
- ¹³ - شريف سيد كامل، الجريمة المنظمة في القانون، دار النهضة العربية، القاهرة، الطبعة الأولى، 2001، ص: 102-103.

¹⁴ - عبد الرحيم صدق، الإرهاب السياسي والقانون الجنائي، دار النهضة العربية، القاهرة، 1985، ص: 45.

¹⁵ - نفسه، ص: 47.

¹⁶ - أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته، كلية العلوم الإستراتيجية، عمان، 214، ص: 38.