مجلة العلوم الاقتصادية والإدارية والقانونية
العدد السابع ــ المجلد الثاني
مايو 2018م
ISSN: 2522-3372

المجلة العربية للعلوم و نشر الأبحاث
Arab Journal of Sciences & Research Publishing
AJSRP

الإطار القانوني لجريمة الإرهاب الإلكتروني

مايا حسن ملا خاطر
كلية القانون || جامعة اليمامة || الرياض || المملكة العربية السعودية

الملخص: لقد تنامت الجرائم الإرهابية اليوم بشكل ملحوظ، وبات الإرهابيون يسخِّرون التكنولوجيا المعاصرة لتنفيذ أفعالهم الجنائية، وتحقيق غاياتهم الإجرامية ومن أبرزها بث الرعب والخوف لدى الأفراد والمؤسسات وحتى حكومات الدول؛ لذا تبرز أهمية هذا البحث في محاولته فضح تلك الأدوات والطرق التي تتبعها التنظيمات الإرهابية في تنفيذ جرائمها الإلكترونية.

وهو مما يستدعي تضافراً دولياً مشتركاً لمنع هذه الجرائم الإرهابية الراهنة، والتي غَدَتْ بمنزلة خطرة تتربص بالعالم كله، نظراً لسهولة ارتكابها، وسرعة وصولها لجميع شرائح المجتمع، وقلة تكلفتها، وارتفاع خطورتها، وصعوبة اكتشاف مرتكبيها، خاصةً إذا ما أخذنا في الحسبان سهولة إنشاء المواقع الإلكترونية واختراقها، وانتشار برامج التجسس وبرامج تدمير المواقع والنظم والمعلومات، والقدرة على بث البيانات والتصريحات والأفلام من خلالها.

الكلمات المفتاحية: القانون الدولي العام، الإرهاب الإلكتروني، مكافحة الإرهاب، الجرائم المعلوماتية.

مقدمة

شهدت الجرائم الإرهابية كغيرها من الجرائم تطوراً ملحوظاً على الصعيدين العالمي والمحلي، إذ بات الإرهابيون يستخدمون التقنيات الرقمية وشبكات الحاسب في ارتكاب أفعالهم الجنائية، للوصول إلى أغراضهم الإجرامية المتمثلة في بث الرعب والخوف لدى الأفراد والمؤسسات وحتى حكومات الدول.

وهو ما يستلزم تعاوناً دولياً سريعاً وفعالاً لمنع هذه الجرائم الإرهابية ذات الطبيعة المستحدثة، والتي أصبحت بمنزلة خطرٍ يهدد العالم بأسره، نظراً لسهولة ارتكابها، وسرعة وصولها لجميع شرائح المجتمع، وقلة تكلفتها، وانخفاض خطورتها، وصعوبة اكتشاف مرتكبها، خاصةً إذا ما أخذنا في الحسبان سهولة إنشاء المواقع الإلكترونية واختراقها، وانتشار برامج التجسس وبرامج تدمير المواقع والنظم والمعلومات، والقدرة على بث البيانات والتصريحات والأفلام ونشرها، وإمكانية ترويج الأفكار والدعوة إلى التجنيد والتعبئة.

وهنا تبرز ضرورة التوعية بالوسائل الحديثة التي تلجأ إليها التنظيمات الإرهابية لمساعدتها في إدارة عملياتها وتنفيذها، من أجل وضع الحلول القانونية والتقنية اللازمة لحل المشكلات المترتبة على سوء استخدام التقنية من قبل هذه الجماعات.

مشكلة البحث:

يمكن إجمال الإشكاليات المطروحة في البحث بما يلي:

- ما هو المقصود بجريمة الإرهاب الإلكتروني؟
- ما هي الأدوات أو الطرق التي تنفذ التنظيمات الإرهابية جرائمها الإلكترونية من خلالها؟
- ما هي الآليات والحلول المناسبة للتعامل مع هذه الظاهرة بفعالية وحزم، والحد من مخاطرها المتزايدة على الأشخاص وعلى أمن المجتمعات واستقرارها واقتصادها؟

أهداف البحث:

يهدف هذا البحث إلى توضيح مدى الاهتمام الدولي والمحلي بظاهرة الإرهاب الإلكتروني، التي باتت تهدد الأمن القومي لجميع دول العالم دون استثناء، خاصةً في ضوء استغلال التقنية الحديثة من قبل الجماعات الإرهابية، في عمليات التخريب وإلحاق الأضرار والأذى المتعمد والحرب النفسية.

أهمية البحث:

تنبع أهمية دراسة الإرهاب الإلكتروني في زيادة استخدام تكنولوجيا المعلومات والاتصالات في حياتنا العملية، في ضوء التطور التقني المتسارع والمواكب للتطورات الاجتماعية والسياسية والاقتصادية، وإن من غير الممكن إغفال أو تجاهل الانعكاسات والآثار المترتبة على استخدام التقنية في الأعمال الإجرامية، فقد ازداد عدد المواقع الإلكترونية التي تديرها المنظمات الإرهابية على الإنترنت زيادة ملحوظة خلال الأعوام القليلة السابقة، وقد كشف مسح أمريكي أجري على شبكة الإنترنت مؤخراً عن مئات المواقع التي تخدم الإرهابيين وأنصارهم، بحيث بات هناك وجود لجميع المنظمات الإرهابية النشطة على الشبكة[1].

منهج البحث:

اعتمد البحث على المنهج الوصفي التحليلي الذي يعبر عن الظاهرة محل البحث، كما توجد في الواقع، والذي لا يقف عند حد الوصف وتوفير المعلومات والبيانات الدقيقة للظاهرة المعنية بالبحث، وإنما يتعدى ذلك إلى تحليلها وتفسيرها، إذ يحدد البحث الأبعاد القانونية، ويسهم في تحليلها، ووصف طبيعتها ومخاطرها، وإبراز الجهود المبذولة لمكافحتها، للوصول إلى استخلاص نتائج عملية تسهم في تحديد الوسائل التي يجب اتباعها لرصدها والتصدي لها، والأساليب الواجب التعامل من خلالها مع هذه الجرائم.

مخطط البحث:

يتناول المطلب الأول من هذه الدراسة ماهية جرائم الإرهاب الإلكتروني، والوسائل المستخدمة من قبل الجماعات الإرهابية في ارتكاب جرائمهم الإلكترونية، بما في ذلك اقتحام المواقع الإلكترونية، والعبث بمحتوياتها وتدميرها، بهدف تعطيلها، للوصول إلى الغاية المنشودة، ألا وهي بث الرعب والخوف في نفوس المستهدفين من هذه العمليات، لتحقيق أغراضهم السياسية.

أما المطلب الثاني، فيبحث في أبرز جهود مكافحة جريمة الإرهاب الإلكتروني على الصعيدين الدولي والمحلي (السعودية نموذجاً)، والتي أسهمت في إنجاح جهود مواجهة هذا النوع من الجرائم، وتضييق الخناق على أصحاب الفكر الضال، الذين يحاولون ارتكاب أعمالهم الإجرامية، وبث أفكارهم المتطرفة وترويجها من خلال الاستعانة بالوسائل الإلكترونية والتقنيات الحديثة.

المطلب الأول

ماهية جريمة الإرهاب الإلكتروني

بات الإرهاب الإلكتروني يشكل هاجساً يقلق جميع الدول، التي أصبحت عرضة للهجمات الإرهابية التخريبية، عبر توظيف الإرهابيين للطبيعة المفتوحة للوسائل الإلكترونية، كشبكة الإنترنت والهواتف المتنقلة

1 Gabriel Weimann, Terror on the Internet, United States Institute of Peace, Washington, April 2006, p.2.

والخدمات الإلكترونية الأخرى، لتنفيذ أنشطتهم الإجرامية، مستفيدين من التقدم الهائل لتكنولوجيا المعلومات والحواسب الآلية وأنظمة الاتصالات.

وفي ما يلي بيان لمفهوم الإرهاب الإلكتروني، ومن ثم أبرز آلياته ووسائله.

أولاً _ مفهوم جريمة الإرهاب الإلكتروني:

لا تزال قضية وضع تعريفٍ محددٍ ومتفقٍ عليه لظاهرة الإرهاب الدولي واحدةً من المشاكل بالغة الصعوبة ومستعصية الحل، ولا يرجع السبب في عدم الاتفاق على تعريفٍ محددٍ للإرهاب إلى غموض المصطلح بحد ذاته، ولا إلى قصور المعاجم اللغوية عن تقديم المفردات لتعريفه، ولكن السبب الحقيقي الكامن وراء الرغبة في عدم الاتفاق على تعريف الإرهاب الدولي، يرجع إلى الاختلاف والتباين الشديدين في وجهات النظر والإرادات السياسية تبعاً لاختلاف الأيديولوجيات والمصالح، فما يراه بعضهم إرهاباً، يراه آخرون عملاً مشروعاً[2].

ورغم من غياب وجود تعريف متفق عليه للإرهاب على الصعيد الدولي، فقد كانت هناك العديد من المحاولات الإقليمية والدولية لتعريفه، وقد تكللت الجهود العربية المبذولة في مجال مكافحة الإرهاب الدولي من خلال إقرار الاتفاقية العربية لمكافحة الإرهاب، التي عرّفت الإرهاب بأنه كل فعلٍ من أفعال العنف أو التهديد به أياً كانت بواعثه أو أغراضه، يقع تنفيذاً لمشروعٍ إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم لإيذائهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بأحد الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر[3].

ومما سبق فإنه يمكن تعريف الإرهاب الإلكتروني بأنه: استخدام الوسائل الإلكترونية والتقنيات الرقمية، الصادر عن الدول أو الجماعات أو الأفراد، ضد أي شخص طبيعي أو اعتباري، بدوافع سياسية، بغرض إخافته أو تهديده والتأثير فيه مادياً أو معنوياً، أو بقصد التأثير في القرارات الحكومية أو الرأي العام.

ومن الممكن القول إن الإرهاب الإلكتروني مرتبط باستخدام أساليب العنف والخوف والرعب، من قبل فرد أو جماعة أو دولة ما، بالاستناد إلى دوافع ذات طبيعة سياسية، بقصد الإخلال بالنظام وزعزعة الأمن والطمأنينة، وتعطيل نظم السيطرة والرقابة الإلكترونية، وهو ما يعرض سلامة المجتمع وأمنه للخطر، ويؤدي إلى تعطيل عمل الأجهزة والمرافق الحكومية والمؤسسات الخاصة، فضلاً عن إلحاق الضرر بالحريات الأساسية، وانتهاكه كرامة الإنسان.

ولهذا تندرج جرائم الإرهاب الإلكتروني ضمن الجرائم الإلكترونية التي تستهدف السيطرة على نظم المعلومات، بغية التخويف ونزع الثقة بنظم التقنية، وذلك باستخدام نظم الكومبيوتر والشبكات الإلكترونية بوصفها وسيلةً لارتكاب جرائمها، إضافةً إلى استخدامها التكنولوجيا بهدف سرقة المعلومات أو نشرها، أو من أجل تمويل العمليات الإرهابية، أو تجنيد الإرهابيين.

ويعتمد بعض مرتكبي جرائم الإرهاب الإلكتروني على وسائل الإقناع وتبادل وجهات النظر، بغية نشر الأفكار الخاصة بالجماعات الإرهابية، والحصول على تأييد الرأي العام، ودعم الموالين والمؤيدين لهم، وتجنيد الأتباع في صفوفهم، وقد يلجأ البعض الآخر منهم إلى استخدام العنف، إما عن طريق القرصنة ونشر الفيروسات واللجوء إلى اختراق أجهزة الكومبيوتر أو البيانات الموجودة بداخلها، بما يؤثر في عملها، ويؤدي إلى تدمير المواقع وتعطيلها وسرقة

---

2 الأشعل، عبد الله (2002) الديمقراطية وحقوق الإنسان في العلاقات الدولية بعد أحداث 11 سبتمبر، مجلة شؤون خليجية، العدد 29، ص 63.

3 المادّة الأولى من الاتفاقية العربية لمكافحة الإرهاب، التي عقدت في إطار جامعة الدول العربية في 22 نيسان عام 1998.

المعلومات، أو من خلال استخدام الأسلحة التقليدية، لمهاجمة البنية التحتية الخاصة بأنظمة لمعلومات كالقيام بقصف كابلات الاتصال ومحطات البث ونقاط الإنترنت الرئيسة[4].

ثانياً _ آليات الإرهاب الإلكتروني:

يشمل الإرهاب الإلكتروني جميع استخدامات التقنية في الأنشطة التي تخدم الأغراض الإرهابية، بما في ذلك عمليات التحريض، وإثارة الأحقاد والخلافات، ونشر الأفكار المتطرفة، مروراً بالتنسيق والتواصل، ومن ثم التمويل والتجنيد، وانتهاءً بتنفيذ الأعمال الإرهابية.

وبناءً على ما سبق فإنه يمكن القول إن الإرهاب الإلكتروني ينفذ بإحدى الأساليب أو الوسائل التالية:

1. التنسيق والاتصال

تستخدم الجماعات الإرهابية البريد الإلكتروني وشبكات التواصل الاجتماعي والمنتديات وغيرها من وسائل الاتصال الحديثة، بوصفها وسيلة للتواصل وتبادل المعلومات والمقترحات فيما بين أعضائها، وللتخطيط لعملياتها، وذلك بهدف تقليل المخاطر الناجمة عن القيام باللقاءات المباشرة بين أعضاء الجماعات الإرهابية على أرض الواقع، أو للتخفيف من استخدام وسائل الاتصال التقليدية التي يسهل من خلالها تتبع الإرهابيين وإلقاء القبض عليهم.

كما يمكنهم استخدامه لنشر أفكارهم والترويج لها، وكسب تعاطف الآخرين معها، وفي هذا الإطار يقوم الإرهابيون كذلك باختراق البريد الإلكتروني للأشخاص، من أجل تتبع مراسلاتهم والاطلاع على بياناتهم الشخصية والسرية، بغية الاستفادة منها في التخطيط لعملياتهم الإرهابية[5].

وعلى سبيل المثال فقد كان "Tom Metzger" من أوائل من وظف الوسائل الإلكترونية في التواصل وبث الأفكار، حيث أسس عام 1985 مجموعة بريد إلكتروني للتواصل مع أتباعه، ويعد "توم" أحد أشهر المتطرفين الأمريكيين، ومؤسس مجموعة المقاومة اليمينية العنصرية المسماة بـ "White Aryan Resistance"[6].

ولا يقتصر الهدف من إنشاء الإرهابيين لمثل هذه المواقع على تقديم التعليم النظري أو الفكري وحسب، بل يتعداه إلى إعطاء التعليمات والإرشادات، وتقديم طرق لتعليم الأعضاء وسائل للتخفي ومسح الأثر عن عيون الأمن، وتدريبهم على كيفية صناعة المتفجرات والقنابل أو طريقة صناعة الأحزمة الناسفة وتركيبها، أو آلية اختراق المواقع الإلكترونية المضادة وتدميرها وتعطيلها، أو الوسائل المستخدمة في نشر الفيروسات، أو طريقة التخطيط والتنسيق للأعمال الإرهابية، وما إلى ذلك من الأساليب المستخدمة لنشر الوعي الإرهابي بين الإرهابيين[7].

2. التجسس على المواقع وتدميرها:

يقوم الإرهابيون المبرمجون الذين يسمون بـ (الهاكرز أو قراصنة الحاسوب) باختراق المواقع أو الحواسب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية

---

4 عبد الصادق، عادل (2009)، الإرهاب الإلكتروني/ القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، الطبعة الثانية، ص 167.

5 أبو رية، وليد محمد (2012)، التعرف على الإرهاب الإلكتروني، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5/ 2011، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، ص 53.

6 حركة المقاومة الأمريكية الأريانية هي حركة عرقية متطرفة، تهدف إلى المحافظة على نقاء العرق الأبيض.

7 القيسي، أيسر محمد عطية (2014)، دور الآليات الحديثة للحد من الجرائم المستحدثة "الإرهاب الإلكتروني وطرق مواجهته"، مؤتمر الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية المقام في عمان، الأردن في الفترة من 2-4/ 9/ 2014، ص 2.

المعلوماتية للمؤسسات الحكومية والخاصة على حدٍ سواء، بما في ذلك البريد الإلكتروني، واشتراكات المستخدمين، والأرقام السرية للبطاقات الائتمانية، وما إلى ذلك.

وبالتالي فإن ارتكاب جرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب الآلي، في إطار جرائم الإرهاب الإلكتروني، يتم باستخدام الفيروسات الإلكترونية، بقصد الحصول على معلومات متعلقة بالأماكن والمنشآت الحيوية لاستهدافها بالعمليات الإرهابية، أو من أجل تدمير أو تعطيل في برامج الحواسيب[8]، ومن الأساليب المستخدمة لتدمير المواقع أيضاً ضخ كميات هائلة من الرسائل الإلكترونية إلى الموقع المستهدف بالتدمير، مما يؤثر على سعته التخزينية، ويؤدي في نهاية المطاف إلى تفجير الموقع وتشتيت بياناته وانتقال معلوماته لجهاز الشخص الذي اخترقه[9].

والأمثلة على مثل هذه الجرائم كثيرة، ومنها على سبيل المثال لا الحصر: قيام الجماعات الإرهابية بمهاجمة نظم التحكم بوسائل المواصلات المختلفة، مما يؤدي إلى تعطيل وإرباك حركة الطيران وإحداث تصادمات فيما بين الطائرات أو القطارات، أو اختراق مواقع المنشآت الحيوية كمؤسسات الكهرباء أو الغاز أو البترول من أجل إلحاق الأذى بها، أو لإضعاف الثقة بالاقتصاد الوطني والمؤسسات الرسمية، أو لتعطيل العمليات المالية التي تقوم بها البنوك، أو العمل على اختراق نظم السلامة الخاصة بالمصانع أو المستشفيات لإحداث أضرار بالناس[10].

3. <u>الترويج الإعلامي:</u>

تسعى العديد من المواقع الإلكترونية التابعة للجهات الإرهابية إلى نشر البيانات والتصريحات والكتب والنشرات، من أجل بث الأفكار المتطرفة التي تتبناها الجماعة الإرهابية التي قامت بالإنشاء.

كما أنها تقوم على نشر الأخبار الكاذبة والمضللة لأجهزة الأمن والرأي العام، أو الآراء التي تسبب التفرقة، أو الإساءة إلى الأديان أو الأعراق أو الأصول، أو تشويه سمعة أشخاص أو جهات معينة والتحريض ضدهم[11].

وفي ذات السياق يمكن أن يكون الهدف من استخدام الإرهابيين للتكنولوجيا نشر ثقافة العنف، والتشجيع على الاستخدام المفرط له، والانخراط في أعمال الإرهاب، من خلال نشر الجهات الإرهابية لنصوص وصور وتسجيلات ومقاطع فيديو وألعاب إلكترونية[12]، تتضمن مشاهد مروّعة تحرض على العنف، وتروج لمثل هذه الأنشطة، وتنشر حالةً من الرعب والخوف في الوقت ذاته[13].

ومع تزايد استخدام المعلوماتية مؤخراً، أصبح الإنترنت وسيلةً مهمةً من الوسائل التي تلجأ إليها المنظمات الإرهابية لتوثيق عملياتها وتمجيد مرتكبيها، من خلال نشرهم أفلام مصورة توضح كيفية ارتكابها، وبيانات منظميها،

---

8 الشهري، حسن بن أحمد والعسيري، محمد بن عبد الله آل فايع (2012)، الإرهاب الإلكتروني وبعضاً من وسائله والطرق الحديثة لمكافحته، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5/ 2011، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، ص 225.

9 السند، عبد الرحمن بن عبد الله (2010)، وسائل الإرهاب الإلكتروني/ حكمها في الإسلام وطرق مكافحتها، دون ناشر، دون مكان نشر، ص 12.

10 Report: Countering the Use of the Internet for Terrorist Purposes –Legal and Technical Aspects, United Nations Counter-Terrorism Implementation Task Force, May 2011, p. 1.

11 Report: The Use of Internet for Terrorist Purposes, United Nations Office on Drugs and Crime, September 2012, p. 4.

12 من ضمن الألعاب الإلكترونية المحرضة على العنف نذكر لعبة (قصف غزة) التي تحاكي العدوان الإسرائيلي على غزة، وتحرض على قتل المدنيين الفلسطينيين.

13 Report: The Use of Internet for Terrorist Purposes, op. cit, p. 4.

ولعل الأمثلة الأبرز في هذا النطاق الأفلام التي نشرتها مواقع إلكترونية تابعة لتنظيم الدولة الإسلامية في العراق وبلاد الشام، والتي أظهرت حادثة إحراق الطيار الأردني معاذ الكساسبة حياً، ومن بعدها فيديو ذبح الرهائن المصريين الأقباط. مع الإشارة أن معظم الأشرطة التي تنشرها مثل هذه التنظيمات المتطرفة تتصف بالاستعانة بمهارات التصوير الفائقة، واستخدام التأثيرات السمعية والبصرية المتطورة، بغية التأثير في الجمهور، سواء بالترغيب من خلال استدرار عواطفهم ومحاولة كسب ودهم وتأييدهم للانضمام إليهم، أم الترهيب من أجل إضعاف معنوياتهم وتثبيط هممهم بتوجيه التهديدات إليهم وإرعابهم.

4. <u>الحرب الدعائية لغايات التمويل والتجنيد</u>

يتم توظيف بعض المواقع الإلكترونية التابعة للمنظمات الإرهابية بغية الترويج للفكر الذي تتبناه الجماعات الإرهابية المتطرفة، وبهدف زيادة أعداد أنصارها، ولتعزيز مواقف أتباعها والمتعاطفين معها، كما يمكن الاستعانة بها بوصفها وسيلة لتجنيد عناصر جديدة وحشدها في صفوف الجماعات المتطرفة[14].

كما تستخدم هذه المواقع الإلكترونية وغيرها من التقنيات الحديثة بوصفها بيئة نموذجية لتسهيل الحصول على مصادر الدعم المالي واللوجستي اللازم لتمويل الإرهابيين وأنشطتهم الإجرامية، ومن الممكن أن يتم ذلك من خلال الاستيلاء على الأموال عبر إجراء تحويلات غير مشروعة، أو من خلال القيام بعمليات تزوير وتزييف باستخدام الوسائل الإلكترونية المتنوعة، أو عن طريق الاستيلاء على حسابات عملاء البنوك، كما تندرج في هذا السياق الأنشطة الإلكترونية التي ترتكب من خلالها المنظمات الإرهابية جرائم غسل الأموال، والاتجار بالمخدرات أو البشر أو الأسلحة وما إلى ذلك، أو ما تقوم به بعض الجمعيات الإرهابية العاملة تحت الغطاء الإنساني أو التطوعي، باستغلال الوسائل التكنولوجية المختلفة في جمع التبرعات، التي يتم تحويلها دون علم المتبرعين بها لتمويل الجماعات الإرهابية.

المطلب الثاني

الجهود السعودية في مكافحة جرائم الإرهاب الإلكتروني:

تتشابه جريمة الإرهاب الإلكتروني مع غيرها من الجرائم الأخرى، كالجرائم الإلكترونية وجرائم الإرهاب والتجسس والاحتيال وقرصنة المعلومات، سواء من حيث النشاط الإجرامي المكون للسلوك الإجرامي أو بالنسبة للجناة أو للنتيجة الإجرامية، وهو ما أحدث إشكاليةً في تحديد التكييف القانوني الواضح لهذه الجرائم المستحدثة.

ونظراً لذلك فإن الدول تتبنى مناهج مختلفة عند تصديها للتحديات الناجمة عن استخدام الإرهابيين للوسائل الإلكترونية، فيتمثل الاتجاه الأول بإعمال القوانين الجنائية التقليدية في مكافحة الإرهاب، والتي لا تكون متعلقة بجرائم الإرهاب الإلكتروني على وجه خاص، أما الاتجاه الثاني، فيشمل ملاحقة هذا النوع من الجرائم بموجب القوانين الخاصة بجرائم الإنترنت أو جرائم التجارة الإلكترونية أو حماية الملكية الفكرية، دون أن تكون هذه

14 الشهري، فايز بن عبد الله (2012)، ثقافة التطرف والإرهاب على شبكة الإنترنت: الملامح والاتجاهات، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5/ 2011، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، ص 16.

الجرائم مرتبطةً بجرائم الإرهاب، وأخيراً تسلك بعض الدول اتجاهاً متمثلاً بتطوير تشريعاتٍ وطنيةٍ مختصةٍ بتجريم وملاحقة ومعاقبة مرتكبي جرائم الإرهاب الإلكتروني بشكلٍ خاصٍ[15].

وبالانتقال إلى جهود المملكة العربية السعودية في مجال مكافحة الإرهاب الإلكتروني، فقد تنبهت المملكة إلى خطورة استخدام الإرهابيين للتقنيات الإلكترونية، واضطلعت بدورٍ مهم في مجابهة هذه الجرائم ومكافحتها، لدرء الأخطار السلبية الناجمة عنها، والتي تهدد أمن الدولة ومصالحها وسلامة مجتمعها وأفرادها. ولهذا فإنه سيتم تناول أبرز الجهود والآليات القانونية المبذولة سواء على المستوى الدولي أم المحلي فيما يلي.

أولاً _ الجهود الخاصة بمكافحة الإرهاب الإلكتروني على الصعيد الدولي:

أولت المملكة العربية السعودية مكافحة الجرائم المعلوماتية اهتماماً كبيراً، إذ قامت بالمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2012، والتي تقضي بتطبيق أحكامها على مجموعة من الجرائم الإلكترونية، ومنها ما هي متعلقة بالإرهاب ومرتكبة بوساطة تقنية المعلومات في ذات الوقت، مثل: نشر أفكار جماعات إرهابية ومبادئها والدعوة إليها، وتمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، ونشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية، ونشر النعرات والفتن والاعتداء على الأديان والمعتقدات[16].

كما صادقت المملكة كذلك على وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات بدول مجلس التعاون الخليجي عام 2012، والتي نصت على ضرورة معاقبة من يقوم بإنشاء مواقع إلكترونية أو ينشر معلومات عن طريق الشبكة الإلكترونية أو إحدى وسائل تقنية المعلومات، من أجل تسهيل الاتصالات بين أعضاء جماعة إرهابية، أو بقصد ترويج أفكارها أو تمويلها، أو نشر كيفية صناعة الأجهزة الحارقة أو المتفجرة، أو أية أدوات أخرى يمكن استخدامها في أعمال إرهابية[17]،

وانضمت المملكة إلى عدد من الاتفاقيات الخاصة بمكافحة الجرائم الإرهابية، ومن أهمها: معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999، والاتفاقية العربية لمكافحة الإرهاب 1998، واتفاقية دول مجلس التعاون لدول الخليج العربية لمكافحة الإرهاب 2004.

وأخيراً فقد وقعت المملكة على مجموعة من الاتفاقيات الثنائية التي تتضمن بنوداً متعلقة بمكافحة الإرهاب وتجفيف منابعه، والتصدي له واجتثاث جذوره.

ثانياً _ الجهود الخاصة بمكافحة الإرهاب الإلكتروني على الصعيد الداخلي:

لم تقتصر جهود المملكة على الصعيدين الدولي والإقليمي، بل امتدت إلى الصعيد الداخلي، حيث أصدر المنظم السعودي جملة من الأنظمة المعنية بمكافحة جرائم الإرهاب، بما في ذلك الإرهاب الإلكتروني، ولكنه لم يفرد قانوناً خاصاً لتجريم هذا الأخير على وجه الخصوص، رغم حرصه على مواكبة الأنظمة للتطورات العلمية والتقنية، ومن ثم فإن التعامل القانوني مع الجرائم الإلكترونية المرتكبة من قبل الجماعات الإرهابية، يكون من خلال مجموعةٍ من الأنظمة واللوائح والقرارات المتوافقة مع التزامات المملكة المتعلقة بمكافحة الإرهاب على الصعيدين الدولي

---

15 Countering the Use of the Internet for Terrorist Purposes –Legal and Technical Aspects, op. cit, P. 5. 6.

16 المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة بتاريخ 21/ 12/ 2010.

17 المادة 29 من وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي، والتي اعتمدت من المجلس الأعلى لدول الخليج العربي في دورته الثالثة والثلاثون التي عقدت في 24 -25 ديسمبر 2012.

والإقليمي، ولعل أهمها: نظام مكافحة الإرهاب وتمويله، ونظام مكافحة الجرائم المعلوماتية، وقرار مجلس الوزراء رقم 163 لعام 1417هـ المتضمن الاشتراطات الخاصة بالمحلات التي تقدم خدمات الاتصال بالإنترنت، وفيما يلي دراسة موجزة لأهم ما ورد في كل منها.

1. نظام مكافحة الإرهاب وتمويله:

يكتسب تطبيق أحكام هذا النظام أهميةً خاصةً فيما يتعلق بحماية الأمن والاستقرار، وردع الإرهاب، وإلحاق الجزاء الرادع بمرتكبي مثل هذا النوع من الجرائم.

وقد عرّف النظام الجريمة الإرهابية بأنها: كل فعل يقوم به الجاني، تنفيذاً لمشروع إجرامي فردي أو جماعي بشكل مباشر أو غير مباشر، بما في ذلك الإخلال بالنظام العام، أو زعزعة أمن المجتمع واستقرار الدولة، أو تعريض وحدتها الوطنية للخطر، أو تعطيل النظام الأساسي للحكم، أو الإساءة إلى سمعة الدولة أو مكانتها، أو إلحاق الضرر بأحد مرافق الدولة أو مواردها الطبيعية، أو محاولة إرغام إحدى سلطاتها على القيام بعمل ما أو الامتناع عنه، أو التهديد بتنفيذ أعمال تؤدي إلى المقاصد المذكورة أو التحريض عليها[18].

ونص النظام على أن تسري أحكامه على كل شخصٍ سعودي أو غير سعودي، ارتكب خارج المملكة جريمة من الجرائم المنصوص عليها في هذا النظام، بما في ذلك التحريض أو الاشتراك أو المساعدة على تغيير نظام الحكم في المملكة، أو تعطيل النظام الأساسي للحكم أو بعض مواده، أو حمل الدولة على القيام بعمل أو الامتناع عن القيام بعمل ما، أو الاعتداء على السعوديين في الخارج، أو الإضرار بالأملاك العامة للدولة في الخارج، أو المساس بمصالح الدولة أو اقتصادها أو أمنها الوطني أو الاجتماعي[19].

ومن الواضح أن أعمال الإرهاب الإلكتروني يمكن أن تندرج تحت هذه الأفعال، فعلى صعيد المثال يمكن النظر إلى الدعوة التي يوجهها الإرهابيون من خلال مواقعهم الإلكترونية لتعطيل الدستور أو قلب نظام الحكم أو الإخلال بالوحدة الوطنية، على أنها بمنزلة التحريض على الإرهاب المعاقب عليه وفق المادة الثالثة من نظام مكافحة الإرهاب وتمويله.

مع العلم أن النظام في المادة السابعة عشرة منه قد منح وزير الداخلية أو من يفوضه السلطة بإصدار أمرٍ مسببٍ، لمراقبة المحادثات والمطبوعات والطرود وغيرها من وسائل الاتصال المختلفة وضبطها وتسجيلها، سواء في جريمة وقعت أم يحتمل وقوعها، إذا كان لذلك فائدة في ظهور الحقيقة، أو منع ارتكاب الجريمة.

أي أن المنظّم السعودي شأنه شأن معظم مشرعي دول العالم، فرض رقابة على سائر وسائل الاتصال، كالبريد الإلكتروني وتطبيقات التواصل الاجتماعي والمدونات والمواقع الالكترونية، وذلك من خلال الصلاحيات الاستثنائية التي منحها وزير الداخلية أو من يفوضه، وذلك بهدف مواجهة خطر الإرهابيين الذي باتوا يستخدمون الفضاء الإلكتروني وسيلةً لارتكاب أفعالهم الإرهابية أو لنشر فكرهم الإرهابي المتطرف.

2. نظام مكافحة جرائم المعلوماتية:

سبقت المملكة العربية السعودية غيرها من الدول العربية في إصدار قانون متعلق بمكافحة الجرائم المعلوماتية، ويهدف هذا النظام إلى الحد من وقوع الجرائم المعلوماتية، بما في ذلك جرائم الإرهاب الإلكتروني،

18 المادّة الأولى من النظام السعودي لمكافحة الإرهاب وتمويله، الصادر بموجب المرسوم الملكي رقم 16 لعام 1435 هـ

19 المادّة الثالثة من النظام السعودي لمكافحة الإرهاب وتمويله.

والمساعدة في تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحواسب الآلية والشبكات المعلوماتية، وحماية المصالح العامة والأخلاق والآداب العامة، وأخيراً حماية الاقتصاد الوطني[20].

أما الأفعال المجرّمة بموجبه، والتي يمكن أن تدخل في نطاق جرائم الإرهاب الإلكتروني فهي: جريمة التنصت على المراسلات الإلكترونية أو التقاطها أو اعتراضها، والدخول غير المشروع لتهديد شخص أو ابتزازه، وجريمة الدخول غير المشروع إلى المواقع الإلكترونية، والقيام بتغيير تصاميمها أو إتلافها أو تعديلها، جريمة التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة.

علماً أن العقوبة المقررة لهذه الجرائم هي السجن مدة لا تزيد عن سنة، والغرامة بما لا يزيد عن خمس مائة ألف ريال، أو إحدى هاتين العقوبتين[21].

فيما يعاقب الجاني بالسجن حسب المادة الرابعة من النظام بالسجن بما لا يزيد عن ثلاث سنوات، والغرامة بما لا يزيد عن مليون ريال، أو إحدى هاتين العقوبتين، إذا قام بالاستيلاء لنفسه أو لغيره على مال منقول أو سند عن طريق الاحتيال، أو إذا حصل على بيانات أو معلومات أو أموال من خلال الوصول بشكل غير قانوني إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية.

ويعاقب الجاني بموجب المادة الخامسة من النظام بالسجن بما لا يزيد عن أربع سنوات، والغرامة بما لا يزيد عن ثلاثة ملايين ريال، أو إحدى هاتين العقوبتين، إذا أقدم الفاعل على الدخول غير المشروع لإلغاء بيانات خاصة أو حذفها أو تدميرها أو تغييرها، أو في حالة إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها، أو إذا حصل إعاقة في الوصول إلى الخدمة أو تشويشها أو تعطيلها.

كما تطرق النظام إلى جريمة إنشاء موقع لمنظمة إرهابية على شبكة الإنترنت، أو على أحد أجهزة الحاسب الآلي، أو القيام بنشر هذا الموقع، لتسهيل الاتصال بقيادات تلك المنظمة أو أحد أعضائها أو بهدف ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو الأدوات التي تستخدم في الأعمال الإرهابية، كما تناول النظام الدخول غير المشروع إلى موقع إلكتروني، أو أي نظام معلوماتي بشكل مباشر أو عن طريق شبكة الإنترنت أو أحد أجهزة الحاسب الآلي، بغرض الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني[22]. أما العقوبة التي حددها النظام لمرتكبي هذه الجرائم فهي السجن مدة لا تزيد عن عشر سنوات، والغرامة بما لا يزيد عن خمسة ملايين ريال، أو إحدى هاتين العقوبتين.

وقد شدد النظام من عقوبة الجاني في حال قام بارتكاب أحد الأفعال المنصوص عليها من خلال عصابةٍ منظّمة، إذ يجب في هذه الحالة أن لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى[23].

ومن الممكن طبعاً تطبيق ما ورد في المادتين الأخيرتين على جرائم الإرهاب الإلكتروني، التي ترتكب من خلال شبكة الإنترنت وغيرها من وسائل التواصل الاجتماعي، بما من شأنه مخالفة القانون، وبث الأفكار الهدامة، والترويج للأفكار المتطرفة، والتشجيع على التطرف والعنف، وإثارة القلاقل وأعمال الشغب، ونشر الفتنة الطائفية، والتحريض على الكراهية.

20 المادة الثانية من النظام السعودي الخاص بمكافحة جرائم المعلوماتية، الصادر بموجب المرسوم الملكي رقم 17 لعام 1428 هـ.

21 المادة الثالثة من النظام السعودي الخاص بمكافحة جرائم المعلوماتية.

22 المادة السابعة من النظام السعودي الخاص بمكافحة جرائم المعلوماتية.

23 المادة الثامنة من النظام السعودي الخاص بمكافحة جرائم المعلوماتية.

3. قرار مجلس الوزراء رقم 163 لعام 1417:

قام مجلس الوزراء بإصدار القرار المتضمن الاشتراطات الخاصة بالمحلات التي تقدم خدمات الاتصال بالإنترنت، وذلك حرصاً على التأكد من عدم إساءة استخدام هذه الخدمات، إذ حظر القرار استخدام شبكة الإنترنت لأغراض غير مشروعة، أو القيام بأية نشاطات تخالف القيم الاجتماعية والثقافية والسياسية والإعلامية والاقتصادية والدينية للمملكة العربية السعودية، كما شمل المنع أيضاً استخدام الشبكة بما يسبب الإزعاج أو التهديد أو نشر الإشاعات لأي شخص أو جهة أياً كانت، وكذلك الدخول إلى حسابات الآخرين أو محاولة استخدامها بدون تصريح، أو تعريض الشبكة الداخلية للخطر بفتح ثغرات أمنية عليها، والاستخدام المكثف للشبكة بما يشغلها دوماً ويمنع الآخرين من الاستفادة من خدماتها[24].

كما تضمن القرار مجموعة إرشاداتٍ لمستخدمي نقاط الاتصال، لضمان حسن استخدامها، من قبل الدول ومؤسسات المجتمع المدني والأفراد على حدٍ سواء، بما يتماشى مع تعاليم الدين الإسلامي الحنيف، والأنظمة الوطنية، والبعد عن كل ما يمس قداسة الإسلام أو يخدش الآداب العامة، أو ينافي أمن الدولة ونظامها، أو يدعو إلى المبادئ الهدامة أو زعزعة الطمأنينة العامة أو بث التفرقة بين المواطنين، وكل ما من شأنه تحبيذ الإجرام أو الدعوة إليه أو حض الاعتداء على الآخرين بأية صورة من الصور، أو يتضمن القدح أو التشهير بالأفراد، فضلاً عن تجريم استخدام البريد الإلكتروني لتبادل أي معلومات تتعارض مع الدين الحنيف والأنظمة الوطنية[25].

ويتضح من هذا القرار وغيره من اللوائح التي سبقته، كلائحة "قواعد ترخيص مقدمي خدمة الإنترنت" عام 1999، ولائحة "جرائم الاختراقات وجزاءاتها التفصيلية"، الحرص الدائم للحكومة السعودية على تنظيم معاملاتها الإلكترونية وضبطها، مما يسهم في وضع حد للجرائم المعلوماتية أو الإلكترونية بشكلٍ عام، وبشكل خاص الجرائم المرتكبة لأغراض إجرامية وإرهابية، من خلال وضع الأطر العامة لضوابط استخدام الإنترنت وأمنه، بما يواكب التطور المتسارع في الأدوات التكنولوجية.

الخاتمة

يتميز الإرهاب الإلكتروني باستغلال التقدم التكنولوجي، بما فيه تكنولوجيا الاتصالات والمعلومات والشبكة العنكبوتية، من قبل الجماعات والمنظمات الإرهابية، بدوافع سياسية، من أجل تخطيط أفعالهم الإرهابية التخريبية وإعدادها وتنظيمها، مع ما يترتب على ذلك من أضرار بالغة في جميع المجالات الاقتصادية والاجتماعية والسياسية، والتي قد تصل إلى حد تقويض سلطة الدولة، وتهديد أمنها القومي، وإلحاق الأذى باقتصادها الوطني واستثماراتها الأجنبية.

وقد خلصت دراسة الأبعاد القانونية لجريمة الإرهاب الإلكتروني إلى مجموعة من النتائج والتوصيات، تستهدف التصدي للخطر المتمثل باستخدام الإرهابيين للجرائم الإلكترونية، سواء على الصعيد المحلي أم الإقليمي أم الدولي، نوردها على النحو التالي:

أولاً – النتائج:

1. إن الإرهاب الإلكتروني يستهدف بالعموم ثلاث فئات مختلفة، الفئة الأولى هي الأنصار أو الأتباع الحاليون والمحتملون، والفئة الثانية هي الرأي العام الدولي، أم الفئة الثالثة فهي جماهير العدو.

---

24 الفقرة الخامسة من قرار مجلس الوزراء السعودي رقم 163 الصادر بتاريخ 24/ 10/ 1417.

25 المرجع نفسه.

2. تتعدد استخدامات الإرهابيين للوسائل التكنولوجية كالإنترنت والأجهزة الذكية وغيرها، لأهداف الترويج لمعتقداتها، وتوجيه رسائل التهديد والوعيد، ومن أجل التجنيد والتعبئة والتخطيط والتنسيق والتمويل وجمع المعلومات واختراق الحسابات، وغير ذلك مما يسهم في تنفيذ أعمالهم الإرهابية الخطيرة.
3. تؤدي المعلوماتية دوراً مهماً في جميع الجرائم الإلكترونية، فهي إما أن تستخدم بوصفها أداة ووسيلة يساء استخدامها، بغية تنفيذ الإرهابيين لجرائمهم، أو تكون المعلومات غايةً وهدفاً بحد ذاتها، أي أن موضوع الجريمة هو سرقة هذه المعلومات والاعتداء عليها أو القيام بتغييرها أو حذفها نهائياً.
4. كانت المملكة العربية السعودية من أوائل الدول العربية التي جرّمت استخدام الإرهابيين لتكنولوجيا المعلومات في ارتكاب جرائمهم الإرهابية.

ثانياً – التوصيات:

1. يجب أن يواجَه استخدام المنظمات الإرهابية للوسائل التكنولوجية الحديثة، بالاعتماد على خبراء التكنولوجيا لملاحقة أعمالهم الإرهابية والحد منها، من خلال توفير البرامج والأنظمة اللازمة لحماية الفضاء الإلكتروني، والكشف المبكر عن الهجمات الإرهابية المحتملة.
2. عدم الإخلال بحقوق الإنسان وحرياته الأساسية، فلا يتم استغلال التخوف من الإرهاب الإلكتروني من أجل انتهاك الخصوصية والحريات الفردية، ولاسيما حرية الرأي والتعبير، من خلال حجب مواقع الإنترنت أو مراقبة البريد الإلكتروني أو التنصت على الاتصالات الإلكترونية، دون وجود أدلة على إمكانية الإخلال بالأمن الوطني.
3. تقوية قدرات الأمن المعلوماتي بكل مكوناته، بما في ذلك رجال القضاء والشرطة، فضلاً عن توفير الأدوات وتنظيم الندوات وتشجيع الأبحاث التي تتناول هذه الظاهرة.
4. توعية أفراد المجتمع من خلال شتى وسائل الإعلام بخطورة جرائم الإرهاب الإلكتروني، مع قيام العلماء والمختصين ورجال الدين والمؤسسات التعليمية والاجتماعية والثقافية بدورها في هذا المجال.

مراجع البحث

المراجع العربية

- أبو رية، وليد محمد (2012)، التعرف على الإرهاب الإلكتروني، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5/ 2011، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض.
- الأشعل، عبد الله (2002) الديمقراطية وحقوق الإنسان في العلاقات الدولية بعد أحداث 11 سبتمبر، مجلة شؤون خليجية، العدد 29.
- السند، عبد الرحمن بن عبد الله (2010)، وسائل الإرهاب الإلكتروني/ حكمها في الإسلام وطرق مكافحتها، دون ناشر، دون مكان نشر.
- الشهري، حسن بن أحمد والعسيري، محمد بن عبد الله آل فايع (2012)، الإرهاب الإلكتروني وبعضاً من وسائله والطرق الحديثة لمكافحته، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5/ 2011، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض.
- الشهري، فايز بن عبد الله (2012)، ثقافة التطرف والإرهاب على شبكة الإنترنت: الملامح والاتجاهات، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5/ 2011، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض.

- عبد الصادق، عادل (2009)، الإرهاب الإلكتروني/ القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، الطبعة الثانية.
- القيسي، أيسر محمد عطية (2014)، دور الآليات الحديثة للحد من الجرائم المستحدثة "الإرهاب الإلكتروني وطرق مواجهته"، مؤتمر الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية المقام في عمان، الأردن في الفترة من 2-4/ 9/ 2014.

المراجع الأجنبية

- Gabriel Weimann, Terror on the Internet, United States Institute of Peace, Washington, April 2006.
- Report: Countering the Use of the Internet for Terrorist Purposes –Legal and Technical Aspects, United Nations Counter-Terrorism Implementation Task Force, May 2011.
- Report: The Use of Internet for Terrorist Purposes, United Nations Office on Drugs and Crime, September 2012.

المواثيق الدولية والأنظمة السعودية:

- الاتفاقية العربية لمكافحة الإرهاب، التي عقدت في إطار جامعة الدول العربية في 22 نيسان عام 1998.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الصادرة بتاريخ 21/ 12/ 2010.
- النظام السعودي لمكافحة الإرهاب وتمويله، الصادر بموجب المرسوم الملكي رقم 16 لعام 1435 هـ.
- قرار مجلس الوزراء السعودي رقم 163 الصادر بتاريخ 24/ 10/ 1417.
- النظام السعودي الخاص بمكافحة جرائم المعلوماتية، الصادر بموجب المرسوم الملكي رقم 17 لعام 1428 هـ.
- وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي، والتي اعتمدت من المجلس الأعلى لدول الخليج العربي في دورته الثالثة والثلاثون التي عقدت في 24 -25 ديسمبر 2012.

The Legal Framework of the Crime of Cyber Terrorism

Abstract: Nowadays the terrorist crimes are increasing significantly, while terrorists are using contemporary technology to carry out criminal actions and to achieve their criminal goals, by spreading terror and fear among individuals, institutions and even governments of the countries.

Therefore this research is showing up the tools and ways in which terrorist organizations are using in their electronic crimes. And also the importance of the international cooperation to prevent the current terrorist crimes, which has become very dangerous for the whole world, according to how easy it is to commit, and because it can reach quickly to all segments of the society, and it has low cost, and it is very difficult to discover its offenders, especially if we take into account the easily of creating websites and the spreading of spyware and the destruction of sites, systems and information, and the ability to broadcast statements ,declarations ,movies ,and dissemination through it.

Keywords: Public International Law, Electronic Terrorism, Combating Terrorism, Cyber Crimes.