الإرهاب الإلكتروني وسبل مكافحته

إعداد طالب الدكتوراه فراس الطحان

إشراف الأستاذ الدكتور أحمد عبد العزيز

المشرف المشارك الأستاذ الدكتور جاسم زكريا

الملخص

تعدُّ جريمة الإرهاب الإلكتروني من أخطر جرائم الإرهاب وأكثرها استحداثاً، في ظل تطور التكنولوجيا وتنامي استخدام شبكة الإنترنت التي ليس لها حدود، وصعوبة اكتشاف الإرهابيين ومعرفتهم كونهم يرتكبون جرائمهم عن بعد، وقدرتهم على تغيير أسلوب عملهم ومقراتهم للحيلولة دون إمكانية تعقبهم، وإخفاء أدلة ارتكاب هذه الجرائم ويستغل الإرهابيون شبكة الإنترنت لإنشاء مواقع إلكترونية أو تدميرها ولنشر أفكارهم ومبادئهم المتطرفة وتجنيد الإرهابيين وجمع المعلومات، فضلاً عن التدريب والتمويل الإلكتروني، الأمر الذي يفترض معالجة الخطر المتنامي للإرهاب الإلكتروني ومكافحته من خلال سن التشريعات وإبرام الاتفاقيات الدولية والمراقبة الإلكترونية والتعاون الدولي، إذْ لا يمكن لأي دولة أن تقضي أو تحدّ من هذه الجريمة بجهودها المنفردة.

الإرهاب الإلكتروني وسبل مكافحته

تعدُّ التكنولوجيا الحديثة من أبرز سمات العصر الحديث إذْ أصبح المجتمع يقاس بمقدار تطور وسائل تبادل المعلومات فيه عبر منظومة الإنترنت التي شاع استعمالها في مجتمعاتنا وأدَّت دوراً في تعزيز التفاهم الإنساني والتواصل الحضاري والثقافي[1]، ومع هذا التطور ظهر في الفضاء المعلوماتي مصطلح جديد هو الجرائم الإلكترونية التي تعدُّ شبكة الإنترنت أداته الرئيسية[2]، ولم تعد هذه الجرائم تقتصر على المساس بالحياة الخاصة للأفراد وإنما قد تنال الأمن القومي والسيادة الوطنية للدول[3] وتعدُّ جريمة الإرهاب الإلكتروني أو الإرهاب عبر شبكة الإنترنت من أخطر هذه الجرائم وأكثرها استحداثاً وقد تؤدي إلى إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصا بين الوحدات والقيادة أو تعطيل أنظمة الدفاع الجوي وإخراج الصواريخ من مسارها أو اختراق النظام المصرفي أو إرباك حركة الطيران أو شل محطات الطاقة الحرارية والنووية الخ.

يتناول هذا البحث جريمة الإرهاب الالكتروني التي تعدُّ إحدى أخطر الجرائم الالكترونية المستحدثة وسأبحث في تحديد ماهية هذه الجريمة وما ميزاتها وخصائصها ووسائل ارتكابها ونقاط الضعف التي يتم استغلالها من قبل الإرهابيين لتنفيذها وذلك بهدف الوقوف على السبل والوسائل الناجعة لمكافحة هذه الظاهرة وطنياً ودولياً.

اتبعت في بحثي المنهج التحليلي الوصفي الذي يقوم على رصد هذه الجريمة ووصفها وتحليلها بدقة للوقوف على جوانبها كلها، معتمداً على بعض الدراسات والبحوث المتعلقة بالموضوع، فضلاً عن المؤتمرات والندوات التي تطرقت لها وقد قسمت بحثي إلى مبحثين وفق الآتي:

- المبحث الأول.. ماهية الإرهاب الالكتروني وميزاته.

- المبحث الثاني.. مظاهر الإرهاب الالكتروني وسبل مكافحته.

وفي نهاية البحث سأشير إلى أبرز التوصيات الكفيلة بالحد من هذه الجريمة.

---

[1] - عالية بايزيد اسماعيل، الإنترنت والجرائم الإلكترونية، بحث بعنوان: تطور القانون والثورة التكنولوجية المعاصرة، مقدم إلى المؤتمر العلمي السنوي الرابع لكلية الحدباء الجامعة، موقع الحوار المتمدن الالكتروني، العدد 1953 2007/6/21.

[2] - د. اياس الهاجري، وحدة خدمات الإنترنت، مدينة الملك عبد العزيز للعلوم والتقنية (ب.س.ط)، ص20.

[3] - د. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، 2008، ص6-7.

المبحث الأول

ماهية الإرهاب الإلكتروني وميزاته

المطلب الأول.. ماهية الإرهاب الإلكتروني

لا بد لتعريف الإرهاب الإلكتروني من تحديد ماهية الجرائم الإلكترونية ومفهوم الإرهاب ليتم بمقتضاه التوصل إلى تعريف محدد للإرهاب الإلكتروني.

أولاً: ماهية الجرائم الإلكترونية

اختلف الفقهاء في تسمية هذه الجرائم فأطلق عليها بعضهم جرائم الكمبيوتر وبعضهم جرائم الإنترنت وأحياناً الجرائم الإلكترونية وفي بعض الأحيان جرائم المعلوماتية كما لم يتم حتى الآن وضع تعريف فقهي شامل وجامع لمفهوم الجريمة المعلوماتية أو الإلكترونية واستند بعض الفقهاء لتعريف الجريمة إلى معيار موضوع الجريمة في حين استند آخرون إلى وسيلة ارتكابه إذْ يعدّ دون باركر أنها: /أي فعل متعمد مرتبط بأي وجه بالحاسبات يتسبب في تكبد أو إمكانية تكبد مجني عليه لخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب/.[1]

ويرى بعضهم بأنها /تلك الجرائم العابرة للحدود التي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها/[2] في حين رأى آخرون أنها /مجموعة الأفعال والأعمال غير القانونية التي تتم عبر شبكة الإنترنت أو تبث عبر محتوياتها/.[3]

وقد عرف بعضهم الجريمة المعلوماتية بأنها: /كل سلوك إجرامي يتم بمساعدة الحاسب الآلي، أو هي كل جريمة تتم في محيط الحاسب الآلي وتتعلق بالبيانات والمعلومات، أو كل سلوك غير مشروع أو

---

[1] - يونس عرب، جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10 - 2002/2/12، ورقة عمل منشورة على الإنترنت.

[2] - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2007، ص30.

[3] - د. عادل عبد الجواد محمد، إجرام الإنترنت، مجلة الأمن والحياة، أكاديمية نايف العربية للعلوم الأمنية، العدد 221، السنة 20، ديسمبر 2000 يناير 2001، ص70.

غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها/[1]، ويتسم هذا التعريف بالعمومية، بينما ذهب آخرون إلى تضييق مفهوم هذه الجريمة فيعرفها بأنها: /كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية لازماً بقدر كبير لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى متى اتصل بالمعلومات أو بنقلها/[2] ويبدو أن هذا التعريف يولي قدراً كبيراً للعلم بتكنولوجيا الحاسبات الآلية ويجعله ركناً أساسياً للجريمة المعلوماتية.

ويعرف خبراء منظمة التعاون الاقتصادي والتنمية، جريمة الكمبيوتر بأنها: /كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و - أو نقلها/ ويتبنى هذا التعريف الفقيه الألماني Ulrich Sieher3، ويبدو أن هذا التعريف يعتمد على معياري وصف السلوك واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

ويبدو أن الجرائم الإلكترونية تختلف عن جرائم المعلوماتية رغم أن كلتيهما مرتبطة بجهاز الكمبيوتر إذْ إنّ الجرائم الإلكترونية تتم من خلال شبكة الإنترنت، وتشمل جرائم متنوعة كالجرائم الجنسية والجرائم الاقتصادية والجرائم الإرهابية..الخ في حين أنَّ جرائم المعلوماتية ترتكب باستخدام الحاسب الآلي أو نظامه بحيث تشمل نسخ أو تغيير أو حذف معلومات، أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر أو تلك التي يتم تحويلها عن طريقه ويمكن إعطاء وصف آخر لها هو جرائم الكمبيوتر.

ثانياً: تعريف الإرهاب

رغم أن الإرهاب أحد مظاهر العنف الذي بدأ يتفشى في المجتمعات بصورة متنامية إلا أنه لم يتم تحديد تعريف متفق عليه لهذا المفهوم[4] بسبب تنوع أشكاله ومظاهره وتعدد أساليبه وأنماطه واختلاف وجهات نظر الفقهاء حوله وسنشير إلى موقف الفقه الغربي والعربي من هذا المفهوم:

---

[1] - د. هشام محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، طبعة عام 1992، ص 21.

[2] - د. نائلة عادل قورة، جرائم الحاسبات الاقتصادية رسالة دكتوراه، جامعة القاهرة 2003 ص 22.

[3] - د. يونس عرب، ورقة عمل بعنوان: صور الجرائم الالكترونية واتجاهات تبويبها، مقدمة إلى ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية المنعقدة في ما بين 2 -4 نيسان 2006 في سلطنة عمان. مسقط، ورقة عمل منشورة على الإنترنت.

[4] - د. وليد هويمل عوجان، بحث مقدم للمؤتمر الدولي: الإرهاب في العصر الرقمي، المنعقد في جامعة الحسين بن طلال ما بين 10 -2008/7/13، بحث منشور على الإنترنت.

1 - الفقه الغربي.

اختلف هذا الفقه وتضاربت آراؤه باختلاف المعايير التي يعتمدها أصحابها لتحديد مفهوم العمل الإرهابي فقد عرف Eric David **الإرهاب بأنه: /عمل عنف إيديولوجي يرتبط بأهداف سياسية/ واعتمد** Soldana **في تحديده لمفهوم الإرهاب على أعمال العنف السياسي إذْ يعرف الجريمة الإرهابية بأنها: /كل جناية أو جنحة سياسية يترتب عنها الخوف العام/[1] وينحاز إلى هذا الاتجاه** Lesrer **الذي عرفه بأنه: /النشاط الإجرامي المتسم بالعنف الذي يهدف إلى التخويف من أجل تحقيق أهداف سياسية/.[2]**

بينما رأى بعضهم الآخر بأن الإرهاب هو: /التطرف في استخدام العنف أو التهديد به بهدف تحقيق أغراض سياسية وتقاس أهميته من الناحية العملية بمدى ما يمكن أن يحدثه العنف من تأثير نفسي في الطرف المستهدف به وإجباره على تغيير سلوكه أو إبدال موقفه تجاه قضية معينة/.[3]

2 - الفقه العربي.

كانت بعض تعريفات الفقه العربي غير موضوعية وتعبر عن وجهة نظر الحكومة الأمريكية وتغفل إرهاب الدولة ونحت بعضها منحنى اجتماعياً فالدكتور متعب مناف يرى أنَّ الإرهاب: /تكتيك تحاول عن طريقه الجماعات المعزولة اجتماعياً البحث عن قوتها والدفاع عن محاولتها التسلط/[4]، وهذا التعريف قاصر ولا يبحث في الإرهاب خارج إطار الجماعات المعزولة كإرهاب الدولة.

ويبدو لنا أنَّ التعريف الذي قدمه الدكتور شريف بسيوني هو أقرب التعريفات إلى الواقع العملي إذْ رأى الدكتور بسيوني أن الإرهاب: /إستراتيجية عنف محرم دولياً تحفزها بواعث عقائدية، وتتوخى

---

[1]- أشار ميرفن في مؤتمر الجمعية الاسترالية النيوزيلندية لمكافحة الجريمة المنعقد من 1 -3 أكتوبر 2003 أن الإرهاب هو: / إشاعة الخوف وتدمير الإحساس بالأمن، وإعادة تشكيل المجتمعات المدنية حسب رأي المجتمعات الدينية المتطرفة ومعتقديها ومجنديها والمتعاونين معهم حول العالم، مما يزيد العبء على الأجهزة المختصة بمكافحة ذلك، وبقية مؤسسات المجتمع الأخرى /.

[2]- عبد السلام بوهوش. عبد المجيد الشفيق، الجريمة الإرهابية في التشريع المغربي، مطبعة الكرامة، الرباط، الطبعة الأولى، 2004، ص28 -45.

[3]- Eris Morris , akd alan hoe terrorism: threat and besponse, (Macmillan press , London and NewYork , 1987 , p.25.

[4]- د. متعب مناف، بحث بعنوان: الإرهاب. والإرهاب في العراق، مجلة المستقبل العراقي، العدد 1، تشرين الأول 2005 ص74.

إحداث عنف مرعب داخل شريحة خاصة من مجتمع معين لتحقيق الوصول إلى السلطة أو القيام بدعاية لمطلب أو مظلمة بغض النظر عما إذا كان مقترفو العنف يعملون من أجل أنفسهم ونيابة عنها أو نيابة عن دولة من الدول/.[1]

ونشير إلى أن وثائق عصبة الأمم تؤكد أنَّ اتفاقاً لمنع الإرهاب والمعاقبة عليه كان قد أُعِدَّ من قبل العصبة منذ عام 1937 [2] إذْ عَدّ الإرهاب: /الأفعال الجنائية الموجهة ضد دولة ما ويكون غرضها أو نتيجتها إشاعة الرعب والذعر لدى شخصيات أو جماعات معينة أو لدى عموم الجمهور). ويبدو أن الدافع لهذا التعريف هو اغتيال ملك الصرب على الأراضي الفرنسية عام 1934 مما دفع فرنسا للعمل على إقرار ميثاق دولي لمكافحة الإرهاب آنذاك.

ويرى مكتب التحقيقات الفيدرالية الأمريكي أن الإرهاب هو: /الاستخدام غير القانوني للقوة والعنف ضد البشر وممتلكاته بغرض إجبار الحكومة أو المجتمع على تحقيق أهداف سياسية أو اجتماعية معينة/[3]، ويبدو أنَّ هذا التعريف قاصر كونه عدّ الإرهاب استخدامًا غير قانوني للقوة، ولم يحدِد المعيار الذي يستند إليه في تحديد قانونية أو عدم قانونية استخدام القوة.

أما وزارة العدل الأمريكية فقد عرفت الإرهاب عام 1984 تعريفاً قاصراً يغفل إرهاب الدولة بالقول إنه: /أسلوب جنائي عنيف يقصد به بوضوح التأثير في حكومة ما عن طريق الاغتيال أو الخطف/.[4]

<u>ويدوري أرى أن الإرهاب هو: /قيام فرد أو مجموعة باستخدام العنف أو التهديد به أياً كانت أهدافهم أو بواعثهم، وسواء تم ذلك من تلقاء أنفسهم أو بتكليف من دولتهم، الأمر الذي يرعب المواطنين ويعرض حياتهم للخطر/.</u>

إن الإرهاب لا يشمل فقط عمليات القتل والعنف بل يشمل أيضاً جميع الأعمال التخريبية التي تزعزع أمن الفرد والمجتمع وتمس بكرامة الأمة بهدف تحقيق أهداف شخصية أو سياسية أو إيديولوجية أو غير ذلك وقد أصبحت الجرائم الإرهابية تعتمد على التقنية الحديثة مما زاد خطورتها.

---

[1]- محمد فتحي عيد، واقع الإرهاب في الوطن العربي، طبعة عام 1999 ص 24.

[2]- نعمة علي حسين، مشكلة الإرهاب الدولي. دراسة قانونية مركز الأبحاث والمعلومات بغداد 1984 ص33.

[3] - انظر: الموقع الالكتروني التابع لمكتب التحقيقات الفيدرالية: www. denver. fbi. gov / interr. htm. p2-3

[4] - د.محمد عزيز شكري، الإرهاب الدولي، دار العلم للملايين، بيروت، الطبعة الأولى، 1991، ص 46.

ثالثاً: تعريف الإرهاب الإلكتروني

أصبح الإرهاب الإلكتروني هاجساً يخيف العالم بأسره وذلك لأنه أكثر جرائم الإنترنت انتشاراً وخطورة وحتى الآن لم يصل الباحثون إلى تعريف مناسب للإرهاب الإلكتروني فبعضهم يرى أنه عبارة عن مهاجمة البنية التحتية للمواقع وآخرون يرون بأنه استخدام التقنيات الرقمية لمهاجمة نظم المعلومات لدوافع سياسية أو دينية أو بهدف تخويف طرف آخر.[1]

إن تعريف الإرهاب الإلكتروني لا بد أن يأخذ بالحسبان الأدوات التي يستخدمها الإرهابيون لتنفيذ جرائمهم وأهدافهم إذْ يرى بعضهم أن الإرهاب الإلكتروني هو: /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 حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد/[2] فالإرهاب الإلكتروني قد يتم من قبل فرد أو دولة ويعتمد على استغلال وسائل الاتصال والإنترنت من أجل تهديد الآخرين والإضرار بهم إلاّ أنّ ما يؤخذ على هذا التعريف أنّه يقصر التهديد على الإنسان فقط ولا يشمل الإرهاب الالكتروني الذي يستهدف جهة حكومية.

وعرفت وكالة التحقيقات الفيدرالية الأمريكية FBI الإرهاب الالكتروني بأنه: /أي هجوم مدبر بدوافع سياسية ضد المعلومات أو أنظمة الكمبيوتر أو برامج الكمبيوتر أو البيانات التي ينتج عنها عنف ضد أي أهداف غير عسكرية بواسطة مجموعات أو عملاء سريين/ في حين عدّه مركز حماية البنية التحتية الأمريكية: /فعل إجرامي يرتب باستخدام إمكانيات الحاسوب والاتصالات وينتج عنه عنف أو تدمير وتعطيل للخدمات لخلق حالة من الخوف تأتي نتيجة الاضطراب والارتباك وسط الجمهور بغرض إكراه الحكومة أو الجمهور للقبول بأجندة سياسية أو اجتماعية أو فكرية /.[3]

ويبدو لنا مما سبق أن الإرهاب الالكتروني هو الاستخدام غير القانوني للوسائل التكنولوجية والتهديد باستخدامها وبدوافع غالباً ما تكون سياسية ويستهدف أنظمة الكمبيوتر وبرامجه وبياناته.. الخ

---

[1] - Gordon , S. Symantec Security Response. Accessed 28-4-2010
http://www.symantec.com / avcenter/reference / cyberterrorism.pdf.

[2]- عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، 2-4 يونيو 2008، بحث منشور على الإنترنت.

3 - د. مضوي مختار المشرف، ورقة عمل حول علاقة جريمة الإرهاب الإلكتروني بغيرها من الجرائم، دورة استخدام الحاسب الآلي في مكافحة الإرهاب، التي نظمتها الإدارة العامة لتنمية الموارد البشرية بالتعاون مع جامعة نايف العربية للعلوم الأمنية، شهر نيسان 2004، منشورة على الموقع الالكتروني للقيادة العامة لشرطة دبي.

ويخلق حالة من الرعب والخوف إلا أنه ينبغي التمييز بين الإرهاب الإلكتروني والجرائم الإلكترونية المرتكبة عبر الإنترنت كاختراق المواقع على الشبكة من قبل بعض الهواة (الهاكرز) أو تدمير البرامج المخزنة على الشبكة والاحتيال المعلوماتي..الخ.

المطلب الثاني.. ميزات الإرهاب الإلكتروني وخصائصه

لا جدال في أن الإرهاب الإلكتروني يحظى بمكانة خاصة عند الجماعات الإرهابية لأن للإنترنت مجالاً واسعاً ومفتوحاً وليس له حدود ويمكن من أي بلد الوصول إلى أي مكان دون أوراق أو قيود ولا يحتاج الإرهابي لتنفيذ جريمته أكثر من حاسب آلي واتصال بشبكة الإنترنت ويمكن القول: إنَّ الإرهاب الإلكتروني يتمتع بميزات لا تتوافر في الجرائم التقليدية تتمثل في:

1 - الحاسب الآلي هو أداة ارتكاب الجريمة:

تعدُّ هذه الخاصية من أهم الخصائص التي تميز هذه الجريمة عن غيرها من الجرائم التقليدية فالحاسب الآلي لا مفر منه في ارتكاب الجريمة وهو النافذة التي تطل بها شبكة الإنترنت على العالم الخارجي ويقصد بالحاسب الآلي مجموعة الأجهزة المتكاملة التي تعمل مع بعضها بعضاً بهدف تشكيل مجموعة من البيانات الداخلة وفقاً لبرنامج موضوع مسبقاً للحصول على نتائج معينة.[1]

2 - الجريمة ترتكب عبر شبكة الإنترنت:

تعدُّ شبكة الإنترنت حلقة الوصل بين الأهداف المحتملة لتلك الجرائم كلها، الأمر الذي دعا للجوء إلى نظم الأمن الإلكترونية للحماية من هذه الجرائم أو الحد منها.[2]

3 - الجريمة تعدّ عابرة للحدود:

تعدّ الجرائم الإلكترونية بشكل عام جرائم عابرة للحدود بسبب قدرة الشبكة على اختصار المسافات وتخطي حدود الدولة التي ارتكبت فيها إذْ يمكن للإرهابيين الموجودين في أكثر من دولة التواصل مثلاً عبر غرف الدردشة لتنفيذ جرائمهم إلا أن هذا لا يعني عدّ هذه الجرائم من قبيل الجرائم الدولية

---

[1] - د. هدى حامد قشقوش، جرائم الحاسب الآلي، دار النهضة العربية، 1992، ص19.

[2] - محمد محمد الألفي، ورقة عمل بعنوان: العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت، مقدمة الى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، 2 -4 يونيو 2008، منشورة على شبكة الانترنت.

التي تنظم في القانون الدولي الجنائي وتم النص على بعضها في إطار اختصاصات المحكمة الجنائية الدولية التي أبرم نظامها الأساسي في روما عام 1998.

فالركن الدولي الذي تكتسبه جرائم الحاسب الآلي ليس الركن ذاته المكون للجرائم الدولية بل ركن آخر يتصل بالجرائم العالمية التي تعدُّ في حقيقتها من الجرائم الداخلية التي يعاقب عليها قانون العقوبات الوطني ويرجع سر تسمية هذه الجرائم بالعالمية إلى مزاولة النشاطات الإجرامية فيها على مستوى عالمي وعبر الحدود نتيجة للتقدم المذهل في وسائل الاتصال.[1]

تعدُّ الجرائم الالكترونية صورة صادقة من صور العولمة فمن إذْ المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة.[2]

إن هذه الميزة تخلق كثيراً من التحديات القانونية في مواجهتها والتصدي لها خاصة فيما يتعلق بمدى إمكانية تطبيق التشريعات الوطنية على هذه الجرائم ومبدأ إقليمية القانون الجنائي[3] وإجراءات الاستدلال والتحقيق والمحاكمة نظراً إلى صعوبة تحديد مكان وقوع الجريمة فالنشاط الإرهابي قد يقع في شرق الكرة الأرضية والنتيجة الضارة تقع في غربها مما يثير التنازع في الاختصاص بشأنها ويتطلب صياغة قواعد قانونية ملائمة لها.

4 - صعوبة إثبات هذه الجريمة:

تعدّ هذه الميزة من أبرز ميزات الجرائم الإلكترونية عموماً ومنها الإرهاب الإلكتروني، والتي تميزها عن جرائم الإرهاب التقليدية وتتمثل صعوبة الإثبات في:

1 - صعوبة اكتشاف الإرهابيين ومعرفتهم كونهم يرتكبون جرائمهم عن بعد باستخدام شبكة الإنترنت ويتم نقل المعلومات وتداولها بصورة غير مرئية ودون أية أدلة ورقية.

2 - يملك الإرهابيون في هذه الجرائم خبرة عالية في تقنية المعلومات وشبكة الإنترنت واستخداماتها بحيث يمكنهم توظيف الشبكة لتنفيذ جرائمهم دون إمكانية تعقبهم.

---

[1]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، بإشراف د. محمد معمر الرازقي، دار الثقافة للنشر والتوزيع، عمان، 2005، ص117 -118

[2] - د. خالد ممدوح ابراهيم، مرجع سابق، ص45.

[3] - د. عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية، جامعة الدول العربية، مصر، 2008، ص13.

3 - قدرة الإرهابيين على تغيير أسلوب عملهم ومقراتهم للحيلولة دون إمكانية تعقبهم وإخفاء مواقعهم على شبكة الإنترنت وإنشاء مواقع جديدة للإفلات من العقاب.

4 - سهولة التواصل بين الإرهابيين عن بعد من خلال الرسائل الإلكترونية والمنتديات وغرف الدردشة وما شابه ذلك من الوسائل، مما يصعب تحديد أماكن وجودهم.[1]

5 - صعوبة الحصول على أدلة ارتكاب هذه الجرائم، إذْ يستطيع الإرهابي بمدة قصيرة أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة على الكمبيوتر.

6 - اختلاف المواقيت بين الدول (البعد الزمني) وإمكانية تنفيذ الجريمة عن بعد (البعد المكاني) والقانون الواجب التطبيق (البعد القانوني) يؤدي دوراً في تشتيت جهود التحري وتعقب المجرمين.

7 - عدم الإبلاغ عن هذه الجرائم في أغلب الأحيان.

8 - غالباً ما يستخدم الجاني اسماً مستعاراً وينفذ جريمته عن طريق مقاهي الإنترنت.

إن هذا الأمر يجعل مأموري الضبط القضائي غير قادرين على تعقب هذه الجرائم والتحري عنها ويصعب تتبع مسار العمليات الإلكترونية العابرة للحدود خاصة إذا كان هؤلاء غير محترفين للتعامل مع هذه الجرائم فقد يتجاهل المحقق الدليل الإلكتروني تماماً ظناً منه أنه غير مهم أو لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو ملحقاته كالطابعة أو الماسح الضوئي[2] علماً أن الخسائر الناجمة عن الإرهاب الإلكتروني تتجاوز أحياناً الخسائر الناجمة عن الإرهاب التقليدي خاصة في الدول التي تعتمد بشكل رئيسي على تقنية المعلومات.

ويبدو لنا بأن هذه الميزات تجعل الإرهاب الإلكتروني متنوعاً ومراوغاً بصورة كبيرة فإذا ما ظهر موقع إرهابي اليوم فسرعان ما يغير نمطه الإلكتروني ثم يختفي ليظهر أيضاً بشكل وعنوان إلكتروني جديد.

---

[1] - أ.د. موسى مسعود ارحومة، ورقة عمل بعنوان: الإرهاب في العصر الرقمي، مقدمة إلى المؤتمر الدولي لجامعة الحسين بن طلال، جامعة قاريوس، بنغازي، منشورة على شبكة الإنترنت.

[2] - د. خالد ممدوح إبراهيم، مرجع سابق، ص46.

المبحث الثاني

مظاهر الإرهاب الإلكتروني وسبل مكافحته

المطلب الأول.. مظاهر الإرهاب الإلكتروني

أصبح الإرهاب الإلكتروني حقيقة واقعة حيث استغل الإرهابيون شبكة الإنترنت لتنفيذ جرائمهم التي تتمثل أبرزها في:

أولاً: إنشاء المواقع الإلكترونية الإرهابية

الموقع الإلكتروني هو عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل html أو / Hyper text mark up browser / ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات الدولية (www Browser) ويقوم بحل رموز html وإصدار التعليمات لإظهار الصفحات المكتوبة.[1]

ويقوم الإرهابيون من خلال الموقع الإلكتروني الذي يقومون بإنشائه بنشر أفكارهم والدعوة إلى مبادئهم والتعبئة الفكرية بهدف تجنيد إرهابيين جدد كما تتضمن المواقع الإلكترونية الإرهابية طرائق صناعة المتفجرات وكيفية اختراق المواقع الإلكترونية وطرائق اختراق الحواسيب الآلية والبريد الإلكتروني والاستيلاء عليه أو إغلاقه والاستيلاء على اشتراكات الآخرين وأرقامهم السرية وطرائق نشر الفيروسات.

ويتبع الإرهابيون أسلوب المراوغة من خلال إنشاء مواقع الكترونية بشكل جديد وتصميم مغاير. وغالباً ما تنشر المواقع الإلكترونية الإرهابية أفلاماً مرعبة للرهائن في أثناء إعدامهم مثل ظهور الرهينة بول جونسون ورأسه مقطوع عبر أحد المواقع الإلكترونية الإرهابية ورغم ذلك يدعي الإرهابيون أنهم أصحاب قضية نبيلة !!

[1] - سايمون كولن، التجارة على الإنترنت، ترجمة يحيى مصلح، بيت الأفكار الدولية، الولايات المتحدة، 1999، ص26.

ولا بد من الإشارة إلى أن المواقع الإلكترونية الإرهابية يستضيفها مزودو خدمات الإنترنت (ISPs) الغربية بصورة مباشرة أو غير مباشرة[1] وأن المواقع الإلكترونية الإرهابية تطورت من 4 مواقع عام 1998 إلى قرابة العشرة عام 2001 وبعد أحداث 11 أيلول 2001 حصل تزايد في هذه المواقع بحيث تم افتتاح 4 آلاف موقع في غضون 4 سنوات وزادت بعد ذلك زيادة أكبر[2] مما يدل على خطورة هذه الجرائم وتناميها.

ثانياً: تدمير المواقع الإلكترونية الإرهابية

تقوم الجماعات الإرهابية بشن هجمات الكترونية من خلال شبكة الإنترنت بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها.

ويقصد بالتدمير الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بشبكة الإنترنت من خلال نظام آلي (Server – Pc) أو مجموعة نظم مترابطة شبكياً بهدف تخريب نقطة الاتصال أو النظام وليس هناك وسيلة تقنية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم فالمتغيرات التقنية وإلمام المخترق بالثغرات في التطبيقات التي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (open Source) سواء كان ذلك في مكونات نقطة الاتصال أو النظم أو الشبكة أو البرمجة جعلت الحيلولة دون الاختراق صعبة جداً[3] وسنشير إلى أبرز الوسائل التي يتم فيها الاختراق من قبل الجماعات الإرهابية:

أ - الاقتحام أو التسلل:

تتم عملية الاقتحام من خلال برامج يتم تصميمها لهذا الغرض ولا يتم كشفها بواسطة برامج مكافحة الفيروسات ويقوم هذا البرنامج بالتجسس على أعمال المستخدم للجهاز المخترق وتسجيل كل تحركاته على الحاسب الآلي وبياناته السرية وحساباته المالية ومحادثاته الخاصة عبر شبكة الإنترنت ورقم بطاقة الائتمان الخاصة به، وحتى كلمات المرور المستخدمة لدخول البريد الإلكتروني خاصة

[1] - صباح جاسم، الإرهاب الإلكتروني. برعاية شركات أمريكية، شبكة النبأ المعلوماتية، الجمعة 3 آب 2007 19 رجب 1428 بحث منشور على الإنترنت.

[2] - د. يوسف رميح، مقالة بعنوان: الإرهاب الإلكتروني طرقه والوقاية منه، صحيفة الجزيرة، 29 ذو القعدة 1429هـ، 2008/11/27م،العدد 13209، انظر الرابط الآتي: http://search.suhuf.net.sa/2008jaz/nov/27/rj6.htm

[3] - عبد الرحمن عبد الله السند، وسائل الإرهاب الإلكتروني. حكمها في الإسلام وطرق مكافحتها، بحث منشور على الإنترنت.

أن مرتكبي هذه الجرائم يملكون كفاءة في استخدام الحاسب الآلي، وليس للبعد الجغرافي أي أهمية في الحد من الاختراقات الإلكترونية.[1]

ومن الممكن تصور قيام إحدى الجماعات الإرهابية بتدمير أحد المواقع الإلكترونية بهدف إغلاق مواقع حيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات ومحطة توليد الطاقة والماء ومواقع الأسواق المالية التي يؤدي توقفها إلى آثار تدميرية.[2]

وقد دمرت منظمة إرهابية استرالية عام 2000 شبكة الصرف الصحي بواسطة عملية الكترونية وفي العام نفسه اخترقت منظمة آدم شيريكو اليابانية الإرهابية البرامج المتحكمة بمسار سيارات الخدمة العامة والتلاعب بأنظمة عدة جهات حكومية وهيمن الذعر في الولايات المتحدة عند اختراق نظام الكمبيوتر بمطار أمريكي وإطفاء مصابيح إضاءة ممرات الهبوط مما هدد بحصول كارثة.[3]

ب - الفيروسات:

يقوم الإرهابيون عند تدمير الأجهزة أو المواقع أو تعطيلها على الأقل لأطول مدة ممكنة باستخدام الفيروسات[4] التي تعدُّ من أخطر آفات الشبكة العنكبوتية، وهي عبارة عن برنامج حاسوبي يلحق ضرراً بنظم المعلومات والبيانات ولها قدرة على التكاثر والانتقال من جهاز إلى آخر وتغيير شكلها وقد تمكن فيروس Blaster عام 2003 من تدمير نصف مليون جهاز كمبيوتر.[5]

ج - الإغراق بالرسائل:

يتم تدمير المواقع الإلكترونية أحياناً من خلال إرسال مئات آلاف الرس/ Hackers/ونية من جهاز الحاسوب الخاص بالإرهابي إلى الموقع الإلكتروني المراد تدميره بحيث لا تتحمل السعة التخزينية له

---

[1] - موزة المزروعي، الاختراقات الإلكترونية خطر كيف نواجهه، مجلة آفاق الاقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000، ص54.

[2] - أكد تقرير صادر عن مكتب المحاسبة العام الأمريكي أنّ نظم البنتاغون هوجمت 250 ألف مرة تقريباً سنة 1995، بمستوى نجاح يصل إلى 160 ألف مرة، وكان الدافع وراء التحقيق في هذا الموضوع نجاح الاختراق الذي قام به شاب بريطاني عمره 16 سنة أطلق على نفسه (راعي بقر تيار المعلومات) يعمل تحت إشراف رجل يستعمل البريد الإلكتروني يدعى كوجي.

[3] - عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مرجع سابق، بحث منشور على الإنترنت.

[4] - محمد محمد الألفي، المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت، المكتب المصري الحديث، 2005، ص33.

5 - حسين سعيد الغافري، بحث بعنوان: الإرهاب الإلكتروني، منشور على الموقع الرسمي لهيئة تقنية المعلومات، سلطنة عمان.

وينفجر وتتشتت بياناته ومعلوماته المخزنة وتنتقل إلى الحاسب الخاص بالإرهابي أو يقوم الأخير بالتحكم بالموقع المدمر ببياناته ومعلوماته كلها.[1]

ولا بد من الإشارة إلى أن محاولة اختراق المواقع الإلكترونية من قبل /Hackers/ لا يعدُّ إرهاباً الكترونياً في كثير من الحالات كون الخطر الناجم عن أعمالهم يبقى محدوداً ويقتصر على إتلاف المحتويات التي يمكن تعويضها باستعادة نسخة مخزنة بشكل آمن.[2]

ثالثاً: تبادل المعلومات الإرهابية ونشرها

يستغل الإرهابيون شبكة الإنترنت لتبادل المعلومات من خلال المواقع الإلكترونية والمنتديات والبريد الإلكتروني بهدف تحقيق الآتي:

أ - نشر المبادئ والأفكار:

يستخدم الإرهابيون الإنترنت لبث الكراهية ونشر المبادئ والأفكار التي يؤمنون بها وثبت أنه عندما كانت الولايات المتحدة تشن حرباً ضد تنظيم القاعدة عقب أحداث 11 أيلول 2001 كان التنظيم يستغل شبكة الإنترنت لنشر أفكاره دون أي رقابة وتستغل الجماعات الإرهابية المنتديات التي ليس لها علاقة بها لنشر أفكارها كما أنها تواكب العصر في وسائلها للتأثير في الشباب[3] وتستفيد من الخدمات المجانية التي تقدمها (yahoo – Google – Msn) لنشر أفكارها.

ب - تجنيد الإرهابيين:

يستغل الإرهابيون شبكة الإنترنت لتجنيد الشباب ممن تتوافر لديهم دوافع الانتماء لهم، وخاصة من خلال غرف الدردشة التي يتم التواصل فيها مع أشخاص في مختلف أنحاء العالم، مما يسهل التأثير في أفكارهم وتجنيدهم.

---

[1]- Ciampa , M.(2005). Security. Guide to NETWORK SECURITY Fundamentals (Second Edition) Accessed 28-4-2010.

[2] - عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مرجع سابق، بحث منشور على الإنترنت.

[3] - في شهر آب 2007 نشرت جماعة إرهابية أغنية راب حملت عنوان: /Dirty Kuffar/ على المواقع الإلكترونية.

- انظر: تقرير لجنة الأمن الداخلي وشؤون إدارة مجلس الشيوخ الأمريكي، تاريخ 2008/6/8 تحت عنوان:

(Vilent Islamist Extremism , the Internet , and the home grown Terrorist threat)

وأكد تقرير لمجلس الشيوخ الأمريكي[1] أن زوار مواقع الإنترنت التابعة لتنظيم القاعدة قد يتعرضون لعملية (Radicalization) عملية يبدي من يمر بها تأييده لتغييرات راديكالية ومن ثم يتصل هؤلاء بالإرهابيين في أنحاء العالم كافة وينضمون للعمليات التنفيذية أو جمع الأموال دون الإفصاح عن هويتهم ويعرض التقرير بصورة مفصلة 4 مراحل تتميز بها هذه العملية وهي:

- مرحلة ما قبل التعرض للإيديولوجية الإسلامية الراديكالية على مواقع الإنترنت، أو ما يسمى Pre-Radicalization.
- مرحلة فقدان الهوية Self – Identification التي يتباعد فيها زوار المواقع من خلالها تدريجياً عن هويتهم السابقة ويتبنون الإيديولوجية الراديكالية.
- مرحلة Indoctrination التي يمر من خلالها الزائر بعملية تذويب أفكاره وتلقي تربية تتعاطف مع الأيديولوجية الراديكالية بصورة لا تقبل الجدال.
- مرحلة Jihadization التي تجعل من الزائر إرهابياً ومتورطاً بعمليات إرهابية.[2]

ج - التدريب الإلكتروني:

تستخدم الجماعات الإرهابية شبكة الإنترنت كأداة لتدريب أفرادها من خلال نشر مواد مسموعة ومرئية تتضمن كتيبات عن الأسلحة وتكتيكات القتال وصناعة المتفجرات، وتقديم دورات الكترونية في صناعة المتفجرات محلياً فضلاً عن إرشادات عن التخطيط والتنفيذ والتخفي..الخ.[3]

إن الإنترنت أصبح شبه بديل لمعسكرات التدريب لهذه الجماعات ووفقاً لتقرير أصدره الجيش الأمريكي في شهر أيار 2007 تم العثور في حواسيب منفذي العملية الإرهابية بمحطات القطار في مدريد على نحو50 كتاباً من تأليف مفكرين راديكاليين تم تنزيلها من شبكة الإنترنت وشكلت للإرهابيين مصدراً استمدوا منه إيحاءهم وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كمٍ

[1]- - انظر: تقرير لجنة الأمن الداخلي وشؤون إدارة مجلس الشيوخ الأمريكي، مرجع سابق.

[2]- نشير إلى أن تنظيم القاعدة أجرى عملية تفاعلية في كانون الأول 2007 بهدف تجنيد إرهابيين حيث طلب أيمن الظواهري عبر تسجيل فيديو نُشرَ عبر الإنترنت إرسال أسئلة من خلال مواقع المنتديات الإسلامية، وبتاريخ 2008/4/2 أجاب الظواهري على جزء منها، مما يعني الاتصال المباشر بين التنظيم وزوار شبكة الإنترنت في أنحاء العالم كافة.

- انظر: تقرير لجنة الأمن الداخلي وشؤون إدارة مجلس الشيوخ الأمريكي، مرجع سابق.

[3]- تقرير لجنة الأمن الداخلي وشؤون إدارة مجلس الشيوخ الأمريكي، مرجع سابق.

هائل من المواقع والمنتديات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة المدمرة.[1]

د - التمويل الإلكتروني:

يقوم الإرهابيون بالاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون إلى شبكة الإنترنت من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية للتعرف إلى أشخاص واستجدائهم بدفع تبرعات لأشخاص اعتبارية أو مؤسسات خيرية تكون واجهة لتنظيمات إرهابية ويتبع الإرهابيون في ذلك رسائل البريد الإلكتروني والمنتديات بصورة لا يشك فيها المتبرع بقيامه بمساعدة أحد التنظيمات الإرهابية.[2]

ويتبع في بعض الحالات غسيل الأموال عبر الإنترنت خاصة أنها عملية سريعة ومغفلة التوقيع ولا توقفها الحدود الجغرافية إذْ يمكن أن يتم غسيل الأموال باستخدام البطاقات الذكية (smart cards) وخاصة تقنية موندكس (Mondex) التي تسمح بتحويل الأموال عبر جهاز مودم أو عبر الإنترنت مع ضمان تشفير العملية وأمنها كما لا يوجد حالياً ما يمنع الإرهابي من استخدام الإنترنت لإنشاء بنك افتراضي أو شركات وهمية في بلدان تغض الطرف عن عمليات غسيل الأموال.[3]

هـ - الاتصال والتخفي:

يستغل الإرهابيون شبكة الإنترنت للاتصال بين أعضاء الخلية الإرهابية بعضهم ببعض والتنسيق فيما بينهم نظراً إلى ما توفره الشبكة من فرصة للاتصال والتخفي باستخدام أساليب متعددة كالبريد الإلكتروني والمواقع والمنتديات وغرف الدردشة كما يمكنهم استعمال رسائل الكترونية مشفرة مما يسهل ترتيب تحركاتهم وتوقيت هجماتهم.[4]

---

[1]- عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مرجع سابق، بحث منشور على الإنترنت.

[2]- عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مرجع سابق، بحث منشور على الإنترنت.

3- د. إبراهيم محمد بركات، بحث بعنوان: أهمية الإفصاح عن مخاطر المعاملات المالية المتعلقة بغسل الأموال في البنوك التجارية، مقدم للمؤتمر العلمي السنوي السابع باسم: (إدارة المخاطر واقتصاد المعرفة)، كلية الاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية عمان، الأردن 16 -18 نيسان 2007، بحث منشور على شبكة الإنترنت.

[4]- عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مرجع سابق، بحث منشور على الإنترنت.

و - جمع المعلومات عبر شبكة الإنترنت:

تعدُّ شبكة الإنترنت مكتبة الكترونية شاملة تحتوي على معلومات حساسة كمواقع المطارات الدولية والمنشآت النووية والمواقع العسكرية وأماكن القيادة والسيطرة، وغالباً ما تكون مدعمة بالصور الضوئية، ويمكن للإرهابيين الاستفادة منها دون أي خرق لقوانين الشبكة وبروتوكولاتها.

رابعاً: التهديد الإلكتروني

تقوم الجماعات الإرهابية بنشر الرعب والخوف في نفوس البشر من خلال التهديد بأن ضرراً سيلحق بهم باستخدام شبكة الإنترنت والبريد الإلكتروني والمنتديات وغرف الدردشة الإلكترونية بهدف الضغط عليهم لتنفيذ أهداف الجماعة الإرهابية ومطالبها من جهة وإبراز قوتها من جهة ثانية وتتعدد أساليب التهديد سواء بالقتل أو بتفجير منشآت أو نشر فيروسات أو تدمير بنى تحتية الخ.[1]

وقد باتت الدول معرضة لما يمكن أن نطلق عليه أسلحة التدمير الشامل باستخدام الأسلحة البيولوجية المعلوماتية المتمثلة في الفيروسات التي تخترق حدود الدول لتدمر البنية المعلوماتية وكلما ارتقت الدول في استخدام شبكات نظام المعلومات زاد تعرضها لمثل هذا النوع من التهديد.

المطلب الثاني.. سبل مكافحة الإرهاب الإلكتروني

ينبغي معالجة الخطر المتنامي للإرهاب الإلكتروني ومكافحته سواء على الصعيد الوطني أم على الصعيد الدولي على النحو الآتي:

أولاً: على الصعيد الوطني

1 - التشريعات الوطنية

انتشر الإرهاب الإلكتروني بصورة ملحوظة في السنوات الأخيرة، بحيث لم تستطع التشريعات الوطنية مواجهته أو الحد منه فلا تزال التشريعات الوطنية في أغلب الدول تنظر إلى الجرائم الإلكترونية على أنها جرائم تقليدية ويبدو أن الفراغ التشريعي الوطني يعدُّ أحد الأسباب الرئيسية في عدم الحد من هذه الجرائم مما يوجب سد هذا الفراغ بعقوبات رادعة والتركيز على الإرهاب الالكتروني حتى لا يستغل الإرهابيون ذلك بتنفيذ جرائمهم في دول لا تجرم هذه الأفعال بصورة واضحة.

[1]- عبد الله عبد العزيز فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مرجع سابق، بحث منشور على الإنترنت.

وتعدُّ السويد أول دولة تسن تشريعات خاصة بجرائم الحاسوب الآلـــي والإنترنـــت إذْ صـــدر قـــانون البيانات السويدي عام 1973 وتبعتها الولايات المتحدة التي شرعت قانوناً خاصـــاً لحمايـــة أنظمـــة الحاسب الآلي (1976 -1985) وتأتي بريطانيا ثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي إذْ أقرت قانون مكافحة التزوير والتزييف عام 1981 كما اهتمت فرنسا واليابان وتـــايوان وهولنـــدا والمجر وكندا بالتنظيم التشريعي لهذه الجرائم لكن يبدو أن هذه التشريعات لم تتضمن -فـــي أغلـــب الأحيان - تجريماً محدداً للإرهاب الإلكتروني.

وفي عام 1997 صدر في ماليزيا نظام للجرائم المعلوماتية صنف جرائم الوصول غير المشروع إلـــى الحاسب الآلي والدخول بنية التخريب وتتراوح العقوبات المحددة بين غرامات تقدر بـــ 150 ألـــف دولار ماليزي إلى السجن مدة عشر سنوات[1]، وفي عام 2001 صدر في إيرلندا نظام للحمايـــة مـــن الجرائم المعلوماتية يتيح معاقبة الاستخدام غير المسموح به لأنظمة الحاسب الآلي.

ورغم صدور عدد من التشريعات العربية بشأن جرائم الإنترنت إلا أن مكافحة هذه الجرائم في عـــدد كبير من الدول العربية لا يزال دون غطاء تشريعي يحددها ويجرم صورها كلها فقد أصدرت المملكة العربية السعودية بعض الأنظمة واللوائح والقـــرارات لمواجهـــة الجـــرائم الإلكترونيـــة والإرهـــاب الإلكتروني فقد صدر قرار مجلس الوزراء السعودي رقم 163 تاريخ 1417/10/24هـــ الذي نـــص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها وتضمن:

- الامتناع عن الوصول أو محاولة الوصول إلى أنظمة الحواسيب الآلية الموصولة بشبكة الإنترنـــت أو أي معلومات خاصة دون الحصول على موافقة المالكين أو من يتمتعون بحقوق الملكية لها.
- الامتناع عن إرسال معلومات مشفرة أو استقبالها إلا بترخيص من إدارة الشبكة المعنية.
- الامتناع عن الدخول إلى حسابات الآخرين أو محاولة استخدامها دون تصريح.
- الامتناع عن إشراك الآخرين في حسابات الاستخدام واطلاعهم على الرقم السري للمستخدم.
- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.
- الامتناع عن تعريض الشبكة الداخلية للخطر عن طريق فتح ثغرات أمنية عليها.

[1] - د.محمد القاسم. د. رشيد الزهراني. د. عبد الرحمن السند. عاطف العمري، دراســـة تجـــارب الـــدول فـــي مجـــال أحكـــام المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، 1423/11/10هـــ، بحث غير منشور.

- الامتناع عن الاستخدام المكثف للشبكة بما يشغلها ويمنع الآخرين من الاستفادة من خدماتها.

- الالتزام بما تصدره وحدة خدمات الإنترنت بمدينة الملك عبد العزيز من ضوابط لاستخدام الشبكة.

- تكوين لجنة برئاسة وزارة الداخلية لمناقشة ما يتعلق بمجال ضبط واستخدام الإنترنت.

كما أصدرت هيئة الاتصالات وتقنية المعلومات [1] نظام مكافحة الجرائم المعلوماتية لعام 1428هـ الذي فرض عقوبات بالسجن أو الغالعام، كليهما معاً على الشخص الذي يرتكب أي من الجرائم المنصوص عليها في النظام ومنها الدخول غير المشروع إلى موقع الكتروني أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه ويعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات المنظمات أو كيفية صنع الأدوات الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية.[2]

وأكد قانون جرائم تقنية المعلومات الإماراتي رقم 2006/2 أن كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالحبس مدة لا تزيد على خمس سنوات.[3]

بينما يجرم قانون جرائم المعلوماتية السوداني لعام 2007 إنشاء المواقع أو نشرها بقصد ترويج الأفكار والبرامج المخالفة للنظام العام دون أن يشير صراحة إلى الإرهاب الإلكتروني.

ولا توجد في سورية قوانين تعاقب على الجرائم الإلكترونية لأن تطبيقات الإنترنت لا تزال محدودة علماً أن مجلس الوزراء السوري أقر في تشرين الثاني 2009 مشروع قانون الاتصالات الذي تتم مناقشته أمام مجلس الشعب لإقراره ويهدف مشروع القانون والوثائق المرفقة به إلى تنظيم قطاع الاتصالات وإقامة نظام للتراخيص في سوق الاتصالات.

---

[1]- انظر الموقع الإلكتروني للهيئة: www.citc.gov.sa

[2]- م7 من نظام مكافحة جرائم المعلوماتية لعام 1428هـ.

[3] - م21 من قانون جرائم تقنية المعلومات رقم 2006/2.

2 - المراقبة الإلكترونية

ينبغي على الدول فرض الرقابة على كل ما يقدم عبر شبكة الإنترنت لمنع الدخول للمواقع التي يتضمن محتواها مواد تتعلق بالإرهاب فضلاً عن مراقبة الاتصالات عبر شبكة الإنترنت والبريد الإلكتروني بهدف ضبط المجرمين وتفتيشهم وجمع الأدلة لإدانتهم وتقديمهم للمحاكمة كما أن مزودات خدمة الإنترنت تتسلم وتنظم كل الطلبات وتستخدم برامج تحسس الرقم الخاص IP مما يعطي بعض البيانات عن المستخدم حتى لو استخدم اسماً وهمياً لدخول الشبكة[1] ويلجأ الإرهابيون أحياناً لوضع أصل المادة المراد نشرها على مواقعهم الأصلية ونقلها إلى منتديات يرتادها الشباب بروابط جديدة غير محجوبة.

ونشير إلى أنه رغم فائدة المراقبة الإلكترونية فإن لها سلبية في عرقلة التتبع الأمني للمطلوبين المراد تعقبهم من خلال الإنترنت فقوات الأمن الباكستانية عثرت على قاتلي دانييل بيرل خلال مدة قصيرة إثر تعرّف IP الخاص بالكمبيوتر الذي أرسلت منه صور عملية القتل[2] ونشير إلى وجود عدة برامج للمراقبة الإلكترونية[3] وبرامج متخصصة بجمع الأدلة والقرائن من رسائل البريد الإلكتروني.

3 - التدريب

إن التدريب ضروري لبناء الخبرة والمهارات[4] خاصة في ظل التقدم المتواصل في تكنولوجيا الحاسب الآلي و الإنترنت الأمر الذي يفرض على جهات إنفاذ القوانين أن تسير في خطوات متناسقة مع هذا التطور حتى يتم التصدي للجرائم الإلكترونية والإرهاب الإلكتروني.

يجب أن يكون رجال القضاء والنيابة العامة على درجة كبيرة من الكفاءة والمعرفة والقدرة على متابعة الجرائم الإلكترونية واستخلاص أدلة الإدانة منها وهذا لا يتم إلا بالتدريب الذي لن يكون بصورة مقبولة إلا بتعاون الدول فيما بينها وأن يشمل جوانب الجرائم الإلكترونية كلها من إذْ تعلم

---

[1]- د. ممدوح عبد الحميد عبد المطلب جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظور أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات في جامعة الإمارات العربية المتحدة، 1-3 مايو 2000، ص42.

[2] - مها فهد الحجيلان، كيف يدعم الإنترنت الإرهاب في السعودية؟، موقع الحوار المتمدن، العدد 888 2004/7/8.

[3] - د. مصطفى محمد موسى، دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، 2005، ص180.

[4] - البند /د/ من القرار الصادر بشأن الجرائم ذات الصلة بالحاسب الآلي، مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة السجناء، هافانا 1990.

كيفية إنشاء المواقع وإدارة الشبكات ونقاط الضعف وأماكن الاختراق لشبكات المعلومات وطرائق الحصول على الأدلة والتعاون الدولي في هذا المجال.

ثانياً: على الصعيد الدولي

1 - الاتفاقيات الدولية

يوجد بعض الاتفاقيات الدولية المتعلقة بجرائم الحاسب الآلي بشكل عام من بينها معاهدة حماية الأفراد المتعلقة بالمعالجة الآلية للبيانات الشخصية المنعقدة في ستراسبورغ لعام 1981 وتعديلاتها لعام 1999 وبروتوكولها الإضافي لعام 2001 وتعدُّ معاهدة جريمة الفضاء التخيلي السيبراني لعام 2001 أو اتفاقية بودابست وبروتوكولها لعام 2003 أبرز اتفاقية تختص بالجرائم الإلكترونية[1] بل إنها فعلياً الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام الكمبيوتر وعبر شبكة الإنترنت ودخلت الاتفاقية حيز النفاذ عام 2004 ووقعت عليها فضلاً عن الدول الأوروبية كندا واليابان وجنوب أفريقية والولايات المتحدة وأكدت الاتفاقية ضرورة التزام الدول الأعضاء بتسليم المجرمين والمساعدة المتبادلة في التحقيق وجمع الأدلة واتخاذ التدابير التشريعية التي تمكنها من الوفاء بهذه الالتزامات.

وأشارت الاتفاقية في مذكرتها التفسيرية أنه من خلال خدمات الاتصالات والمعلومات يستطيع المستخدمون اصطناع فضاء جديد يسمى الفضاء المعلوماتي الذي يستعمل أساساً لأغراض شرعية، لكن يمكن أن يخضع لسوء الاستخدام إذ إن هناك احتمالاً لاستخدام شبكات الحاسب والمعلومات الإلكترونية في ارتكاب أعمال إجرامية ويؤخذ على الاتفاقية أنها تعاقب جزئياً على الجرائم الإلكترونية.[2]

وفي 2006/6/12 صدر إعلان بوخارست حول مكافحة التزوير والقرصنة ويتم حالياً إعداد مشروع اتفاقية عربية لمكافحة جرائم الحاسوب إلا أنه لم تتبلور حتى الآن اتفاقية دولية لمعاقبة مرتكبي

[1]- انظر: بحث بعنوان: برنامج تعزيز حكم القانون في بعض الدول العربية، ندوة إقليمية حول: الجرائم المتصلة بالكمبيوتر، معدة من قبل برنامج الأمم المتحدة الإنمائي، وزارة العدل، المملكة المغربية، الدار البيضاء، من 19 -20 يونيو 2007.

[2] - د. نضال الشاعر، الإطار التشريعي لجرائم المعلوماتية والإنترنت، مداخلة في ورشة عمل حول: (جرائم المعلوماتية والإنترنت. نظرة على دول الشرق الأوسط) فندق موفينبك بيروت، 23 -2006/2/24، تحت رعاية الجمعية المعلوماتية المهنية والمركز التجاري العالمي في بيروت واتحاد جمعيات المعلوماتية العربية.

الجرائم الإلكترونية وخاصة الإرهاب الإلكتروني تتضمن نصوصاً تنظم إجـراءات التفتـيش وأشـكال المساعدة المتبادلة بين الدول مع كفالة حماية حقوق الأفراد والدول.

وبهدف إيجاد آلية عالمية لمكافحة الإرهاب الإلكتروني تدرس كوريا الجنوبية خطة لإنـشاء منظمـة دولية لمكافحة الإرهاب الإلكتروني تتخذ من سيؤول مقراً لها وسيقدَّمُ مقترح بذلك إلى قمة مجموعة (20) المقرر عقدها في سيؤول في شهر تشرين الثاني 2010.

2 - التعاون الدولي

يعدّ التعاون الدولي اللبنة الأولى والأساسية لمواجهة الإرهاب الإلكتروني الذي ينفذ غالباً فـي دولـة وتحصل آثاره في دولة أخرى، ولا يمكن لأي دولة أن تحدّ من هذه الجريمة بجهودها المنفردة.

إن فعالية التحقيق والملاحقة القضائية في الإرهاب الإلكتروني تقتضي تتبع أثر النشاط الإجرامي فـي أكثر من دولة سواء البلد الذي كان منشأ الجريمة أو البلدان التي عبر من خلالها الفعـل الإجرامـي للدولة الهدف الأمر الذي يدفع لضرورة التعاون بين الدول كافةً قضائياً وإجرائيـاً وتحقيـق ذلـك بالسرعة الممكنة نظراً إلى طبيعة هذه الجرائم وتؤكد معاهدة منظمة المـؤتمر الإسـلامي لمكافحـة الإرهاب الدولي لسنة 1999 اختصار الوقت والحد من الإجراءات عن طريق الاتصال المباشـر بـين السلطات المعنية بالتحقيق في الدول [1] لأن بطء الإجراءات يجازف بفقدان الأدلة.

رغم ذلك فإن هناك صعوبات تعترض التعاون الدولي في هذا المجال تتمثل بعدم وجود اتفاقيات دولية تنظم هذا التعاون، وعدم وجود مفهوم عام موحد للنشاط المجرم، وتعقد مشكلات التفتـيش وجمـع الأدلة الخ.

<u>أخيراً لابد من القول:</u> إنه في ظل ثورة الاتصالات واعتماد الدول بشكل رئيسي على تقنية المعلومـات وشبكة الإنترنت تتزايد مخاطر الإرهاب الإلكتروني مما يوجب العمل للحد من هذه الجرائم إن لم يكن القضاء عليها بالاعتماد على آخر ما توصل إليه العلم في مجال المراقبة الإلكترونية وتقنين القواعـد والتشريعات الوطنية الملائمة لها وتنمية الوعي لدى المجتمع خاصة في أوسـاط الـشباب لأنهـم الشريحة الكبرى التي تستخدم شبكة الإنترنت.

[1] - م 30 من معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب لسنة 1999.

إن ما بذلته العديد من الدول من تدابير لمواجهة الإرهاب الإلكتروني لا تزال محدودة وتحتاج إلى بذل المزيد وتفعيل التعاون الدولي والإرهابيون سيستغلون شبكة الإنترنت لتنفيذ جرائمهم ما دامت أجهزة إنفاذ القانون ورجال القضاء والنيابة العامة عاجزين عن ملاحقتهم واستخلاص أدلة إدانتهم وسيبقى الإرهاب الإلكتروني خطراً يهدد العالم بأسره ولاسيمّا الدول المتقدمة التي تدار بنيتها التحتية بالحواسيب الآلية وشبكات الإنترنت.

ولابد لأهمية البحث من تأكيد التوصيات الآتية:

- ضرورة تحديد إستراتيجية واضحة لمواجهة جريمة الإرهاب عبر الوسائل الإعلامية المختلفة تتضمن فهماً عميقاً لجرائم الإرهاب وأسبابه وطرائق التصدي لها ووضع قواعد إرشادية للتقارير الإعلامية بما يحول دون استفادة الإرهابيين منها في الاتصال أو التجنيد[1] ودعوة الجمهور للإرشاد عن الإرهابيين[2] وتوعية الشباب بمخاطر دخول المواقع الإلكترونية الإرهابية.
- تدريب القضاة وأفراد النيابة العامة على كيفية التعامل مع قضايا الإرهاب الإلكتروني بالنظر إلى طبيعتها الخاصة وتطوير أساليب البحث عن الأدلة وتقديمها لتواكب هذه التطورات.
- التدخل التشريعي لمواجهة القصور في التشريعات الحالية وسن تشريعات جديدة تحظر التحريض على الإرهاب عبر الإنترنت وفرض عقوبات شديدة على مرتكبيها ومزودي الخدمة المستضيفة لها.
- السعي لعقد مؤتمر دولي بإشراف الأمم المتحدة لوضع إستراتيجية محددة لمواجهة الإرهاب الإلكتروني الذي يوصف بأنه إرهاب المستقبل وإنشاء مركز دولي لمكافحة الإرهاب لأن أي جهد دولي سيكون قاصراً إذا افتقد العمل الجماعي والمنظور الاستراتيجي الشامل في التعامل معها.
- حث الدول للإسراع بالانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الإرهاب وعقد اتفاقيات دولية متخصصة بمكافحة الجرائم الإلكترونية وتحديداً الإرهاب الإلكتروني.
- عقد اتفاقية عربية على غرار الاتفاقية الأوروبية لمكافحة جرائم الإنترنت لعام 2001.

[1]- موجز التقرير النهائي للمؤتمر الدولي لمكافحة الإرهاب، الرياض 25 -28 ذي الحجة 1425هـ، 5 -8 فبراير 2005.

[2] - د. عبد المحسن بدوي محمد أحمد، ورقة دور برامج الإعلام في تنمية الوعي الأمني ومكافحة الإرهاب، المعوقات والتحديات، جامعة نايف العربية للعلوم الأمنية. الرياض، الخرطوم 2009، بحث منشور على الإنترنت.

- تعزيز التنسيق والتعاون مع المؤسسات الدولية المعنية بمكافحة هذه الجرائم خاصة الأنتربول ونقل البرامج والتقنيات المستخدمة في الدول المتقدمة لمواجهة الإرهاب الإلكتروني إلى الدول التي لا تتوافر فيها لأن خطر هذا الإرهاب لا يقتصر على دولة معينة وإنما يشمل العالم بأسره.
- تكثيف المؤتمرات والندوات العلمية المتعلقة بمكافحة جرائم الإرهاب الإلكتروني، وتعزيز التنسيق والتعاون الدولي قضائياً وإجرائياً لمكافحة هذه الجرائم.
- تقييم عملية المراقبة الإلكترونية وتصميم برامج حاسوبية تدعى شرطة الإنترنت مهمتها تطهير الإنترنت وحجب المواقع الإرهابية وحذف أية رسائل واردة من مصادر معادية وإيقافها.
- صياغة إجراءات قانونية تحد من استضافة مزودي خدمات الإنترنت لمواقع ومنتديات خاصة بالجماعات الإرهابية.
- التوسع في دراسة فكر الجماعات الإرهابية التي تبث عبر شبكة الإنترنت والقيام بنشر التوعية الصحيحة بالأسلوب العلمي، بحيث تكون المواجهة عبر الإنترنت وبالأسلوب نفسه.
- إعادة النظر في مقررات كلية الحقوق في الوطن العربي وأكاديميات الشرطة، بحيث تخصص بعض المواد للتعريف بالإرهاب الإلكتروني ومكافحته وتأهيل الأطر القانونية والأمنية للتعامل معه.

المراجع

الكتب:

1 - د. خالد ممدوح إبراهيم أمن الجريمة الإلكترونية الدار الجامعية الإسكندرية 2008.

2 - سايمون كولن التجارة على الإنترنت ترجمة يحيى مصلح بيت الأفكار الدولية الولايات المتحدة 1999.

3 - د. عمرو حسين عباس أدلة الإثبات الجنائي والجرائم الإلكترونية جامعة الدول العربية مصر 2008.

4 - د.محمد شكري، كري، الإرهاب الدولي، دار العلم للملايين، بيروت، الطبعة الأولى، 1991.

5 - محمد فتحي عيد واقع الإرهاب في الوطن العربي طبعة عام 1999.

6 - محمد محمد الألفي المسؤولية الجنائية عن الجرائم الأخلاقية عبر الإنترنت المكتب المصري الحديث 2005.

7 - محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية إشراف د.محمد معمر الرازقي، دار الثقافة للنشر والتوزيع عمان 2005.

8 - د. مصطفىموسى،موسى دليل التحري عبر شبكة الإنترنت دار الكتب القانونية 2005.

9 - د. نائلة عادل قورة، جرائم الحاسبات الاقتصادية رسالة دكتوراه جامعة القاهرة 2003.

10 - عبد السلام بوهوش. عبد المجيد الشفيق الجريمة الإرهابية في التشريع المغربي مطبعة الكرامة الرباط الطبعة الأولى 2004.

11 - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات دراسة مقارنة دار الفكر الجامعي الإسكندرية الطبعة الأولى 2007.

12 - نعمة علي حسين، مشكلة الإرهاب الدولي. دراسة قانونية، مركز الأبحاث والمعلومات، بغداد، 1984.

13 - د. هدى حامد قشقوش، جرائم الحاسب الآلي دار النهضة العربية 1992.

14 - د. هشافريد، فريد قانون العقوبات ومخاطر تقنية المعلومات طبعة 1992.

المقالات:

1 - صباح جاسم أمريكية، الإلكتروني. برعاية شركات أمريكية شبكة النبأ المعلوماتية الجمعة 3 آب 2007 19 رجب 1428.

2 - د. عادل عبد الجواد محمد إجرام الإنترنت مجلة الأمن والحياة أكاديمية نايف العربية للعلوم الأمنية العدد 221 السنة 20 ديسمبر 2000 يناير 2001.

3 - - مها فهد المتمدن، كيف يدعم الإنترنت الإرهاب في السعودية؟ موقع الحوار المتمدن، العدد 888 2004/7/8.

4 - د.مناف، مناف، بحث بعنوان: الإرهاب. والإرهاب في العراق، مجلة المستقبل العراقي، العدد 1 تشرين الأول 2005.

5 - موزة المزروعي، الاختراقات الإلكترونية خطر كيف نواجهه مجلة آفاق الاقتصادية دولة الإمارات العربية المتحدة العدد التاسع سبتمبر 2000.

6 - د. يوسف رميح، مقالة بعنوان: الإرهاب الإلكتروني، طرقه والوقاية منه صحيفة الجزيرة الخميس 29 ذو القعدة 1429هـ 2008/11/27م العدد 13209.

البحوث والدراسات والمؤتمرات:

1 - د. إبراهيم محمد بركات بحث بعنوان: أهمية الإفصاح عن مخاطر المعاملات المالية المتعلقة بغسل الأموال في البنوك التجارية مقدم للمؤتمر العلمي السنوي السابع باسم: (إدارة المخاطر واقتصاد المعرفة) كلية الاقتصاد والعلوم الإدارية جامعة الزيتونة الأردنية عمان الأردن 16 - 18 نيسان 2007.

2 - د. إياس الهاجري، نشرة تعريفية بعنوان: وحدة خدمات الإنترنت مدينة الملك عبد العزيز للعلوم والتقنية (ب.س.ط).

3 - عالية بايزيد إسماعيلالسند،ترنت والجرائم الإلكترونية جزء من البحث المعنون: تطور القانون والثورة التكنولوجية المعاصرة المقدم إلى المؤتمر العلمي السنوي الرابع لكلية الحدباء الجامعة موقع الحوار المتمدن الالكتروني العدد 1953 2007/6/21.

4 - عبد الرحمن عبد الله السند وسائل الإرهاب الإلكتروني.حكمها في الإسلام وطرق مكافحالعجلان،بد الله عبد العزيز فهد العجلان الإرهاب الإلكتروني في عصر المعلومات المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت القاهرة 2 -4 يونيو 2008.

6 - محمد محمد الألفي، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الإنترنت، المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، 2 -4 يونيو 2008.

7 - د.القاسم.قاسم. د. رشيد الزهراني. د. عبد الرحمن السند. عاطف العمري دراسة تجارب الدول في مجال أحكام المعلوماتية مشروع الخطة الوطنية لتقنية المعلومات 1423/11/10.

8 - د. مضوي مختار المشرف ورقة عمل حول علاقة جريمة الإرهاب الإلكتروني بغيرها من الجرائم دورة استخدام الحاسب الآلي في مكافحة الإرهاب التي نظمتها الإدارة العامة لتنمية الموارد البشرية بالتعاون مع جامعة نايف العربية للعلوم الأمنية شهر نيسان 2004.

9 - د. ممدوح عبد الحميد عبد المطلب جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظور أمني مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية 1 -3 مايو 2000.

10 - أ.د. موسى مسعود ارحومة، ورقة عمل بعنوان: الإرهاب في العصر الرقمي المؤتمر الدولي لجامعة الحسين بن طلال جامعة قاريوس، بنغازي.

11 - د. نضال الشاعر، الإطار التشريعي لجرائم المعلوماتية والإنترنت، ورشة عمل حول (جرائم المعلوماتية والإنترنت. نظرة على دول الشرق الأوسط) فندق موفينبك بيروت 23 - 2006/2/24 تحت رعاية الجمعية المعلوماتية المهنية والمركز التجاري العالمي في بيروت واتحاد جمعيات المعلوماتية العربية.

12 - د. وليد هويمل عوجان، بحث مقدم للمؤتمر الدولي: الإرهاب في العصر الرقمي المنعقد في جامعة الحسين بن طلال ما بين 10 -2008/7/13.

13 - يونس عرب، جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي، 10 -2002/2/12.

14 - د. يونس عرب، ورقة عمل بعنوان: صور الجرائم الالكترونية واتجاهات تبويبها، مقدمة إلـــى ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية المنعقدة ما بين 2 -4 نيسان 2006 في سلطنة عمان. مسقط.

15 - بحث بعنوان: / برنامج تعزيز حكم القانون في بعض الدول العربية في إطـــار نـــدوة إقليميـــة حول: (الجرائم المتصلة بالكمبيوتر) معدة من قبل برنامج الأمم المتحدة الإنمائي وزارة العدل المملكة المغربية الدار البيضاء من 19 -20 يونيو 2007.

المراجع الأجنبية:

- Ciampa , M.(2005). Security. Guide to NETWORK SECURITY Fundamentals (Second Edition). Accessed 28-4-2010

- Eris Morris , akd alan hoe terrorism: threat and besponse, (Macmillan press , London and New York , 1987

- Gordon , S. Symantec Security Response. Accessed 28-4-2010.

تاريخ ورود البحث إلى مجلة جامعة دمشق 2010/7/7.