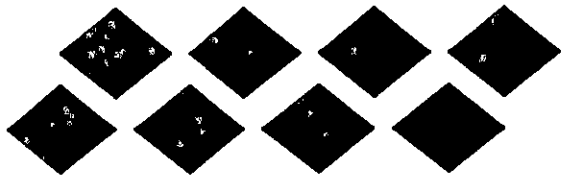
مجلة كلية الآداب بقنا (دورية أكاديمية علمية محكمة)



الإرهاب والجريمة الالكترونية بالمجتمع السعودي رؤية سوسيولوجية

د/ يوسف بن أحمد الرميح
رئيس قسم الاجتماع والخدمة الاجتماعية
جامعة القصيم

أبحاث

الإرهاب والجريمة الالكترونية بالمجتمع السعودي رؤية سوسيولوجية

د/ يوسف بن أحمد الرميح
رئيس قسم الاجتماع والخدمة الاجتماعية
جامعة القصيم

مقدمة

لقد أدى ظهور الحاسبات الآلية إلى تغيير شكل الحياة في العالم، وأصبح الاعتماد على وسائل تقنية المعلومات الحديثة يزداد يوماً بعد يوم، سواء في المؤسسات المالية، أو المرافق العامة، أو المجال التعليمي، أو الأمني أو غير ذلك، إلا أنه وإن كان للوسائل الإلكترونية الحديثة ما يصعب حصره من فوائد، فإن الوجه الآخر والمتمثل في الاستخدامات السيئة والضارة لهذه التقنيات الحديثة ومنها الإرهاب الإلكتروني الذي أصبح خطراً يهدد العالم بأسره، إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى في غرفته في أحد الفنادق.

ولعل ما يدفع إلى الاهتمام بهذا النوع من الإرهاب تلك الأخطار وأشكال الدمار الذي يسببه سواء للأفراد أو الجماعات أو الدول وهذا يقودنا إلى إلقاء الضوء حول مفهوم الإرهاب ولعل أفضل الرؤى من وجهة نظر الباحث لهذا المفهوم ما توصل إليه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي فقد عرف الإرهاب بأنه: العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً على الإنسان ودينه، ودمه، وعقله، وماله، وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الحرابة، وإخافة السبيل، وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو المرافق العامة والأملاك الخاصة أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها. (المجمع الفقهي، ١٤٢٢، ص٨)

لذا فالإرهاب الإلكتروني يعد أحد الأشكال وصور الإرهاب فلقد أصبح الإرهاب الإلكتروني هاجساً يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضراراً جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن

هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

وتحاول هذه الأطروحة أن تقدم تحليلاً نظرياً للإرهاب الإلكتروني والذي يتناول في ثناياه مجموعة من القضايا التي ترتبط بالمفهوم والأبعاد والوسائل وبعض الاتجاهات النظرية مختتما العرض بصور التعامل مع الإرهاب الإلكتروني ومواجهته وأخيراً تحديات المواجهة في إطار العولمة الثقافية.

أولاً: الإرهاب والجريمة الإلكترونية رؤية للمفهوم:

إن الجريمة بمعناها التقليدي تعنى كل أو أي خروج عن السلوك أو المعايير الاجتماعية والثقافية والاقتصادية، والتي يحكمها القانون الوضعي لأي مجتمع.

وبالتالي فإن التعدي على الفرد وحقوقه وكذلك المجتمع يعرض دائماً مرتكبي هذا السلوك للمسائلة القانونية والجنائية.

لذلك فإن الجريمة التقليدية تعنى كل عمل إنساني يخالف القانون، يقوم به المجرم لتحقيق أهداف إجرامية محددة.

أما الإرهاب هو ذلك السلوك الإجرامي الذي يسبب قدراً كبيراً من الدمار والخسائر البشرية وينفذه جماعات متخصصة من ذوي الخبرات العالية التي تمتلك معرفة تكنولوجية في مجالات متعددة ولها قدرة عالية على التخطيط. (هاشم الزهراني، ٢٠٠٧، ٣٧٩)

في حين أن مفهوم الجريمة الإرهابية التقنية يمكن تحديدها بأنها "أي نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطرية مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإرهابي المقصود. (عبد الفتاح بيومي، ٢٠٠٩، ١٧)

ويعرفها آخرون "سلوك غير مشروع يعاقب عليه قانوناً صادر عن إرادة جريمة – مذنبه – ومحله معطيات الحاسب الآلي"

ولذلك وفي جريمة مستترة تتسم بالسرعة والتطور في أساليب ارتكابها، أقل عنفاً في التنفيذ، وعابرة للحدود ويصعب إثباتها لصعوبة وجود أدلة مادية عليها، ويسهل إتلاف الأدلة الخاصة بها. (عبد الفتاح بيومي، ٢٠٠٩، ١٩)

وينظر إليها البعض على أنها "نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد وإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع. (حسنين بوادي، ٢٠٠٦، ٥٤)

وأخيراً يمكن النظر إليها على أنها "استخدام الحاسوب الرقمي بنظمه وبرامجه وملحقاته ووسائل الاتصال في ارتكاب الجرائم الإرهابية سواء كانت تلك التقنية هي

محل الجريمة أم كانت وسيلة في ارتكابها وسواء كانت عبر شبكة الإنترنت أو بدونها. (مصطفى موسى، ٢٠٠٥، ٧٤)

من العرض السابق نتوصل إلى أن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر عن الدول أو الجماعات أو الأفراد على الإنسان، دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.

ومن ثم قام الباحث بتقسيم الإرهاب الإلكتروني إلى ثلاثة مجموعات هي:

١. المجموعة الأولى: الجرائم التي تستهدف النظم والمعلومات كهدف.
٢. المجموعة الثانية: الجرائم التي تستخدم وسائل تكنولوجيا المعلومات كوسائل لارتكاب الجرائم.
٣. المجموعة الثالثة: الجرائم التي ترتبط بمحتوي مواقع المعلومات وبياناتها.

(عبد العزيز الشبل، ٢٠٠٧، ٧٥٠)

ويعتبر هذا التصنيف كمثابة تحديد إجرائي للتعرف على الجرائم الإرهابية الإلكترونية.

ثانياً: أبعاد وسمات الجريمة الإلكترونية ومرتكبيها:

ويمكن عرض أهم أبعاد وسمات الجريمة الإلكترونية في المجتمعات العربية على النحو التالي: (أديب حضور، ٢٠٠٧، ١)

١. الطابع التديني: تنطلق التنظيمات الإرهابية في البلدان العربية من منطلقات تدينيه، وترفع شعارات دينية، وتزعم أنها تعمل تحت مظلة دينية.
٢. تدعى جميع التنظيمات الإرهابية في البلدان العربية أنها تخدم قضية وأنها تعمل في خدمة المصلحة العامة (الدينية والاجتماعية والوطنية)
٣. تحاول التنظيمات الإرهابية العربية استغلال ارتباط الكثير من الأنظمة العربية وتعثر خطواتها في إنجاز مهامها الوطنية والاجتماعية والثقافية لصالحها، وتسعى لتجبير هذا الارتباط (وربما الفشل أحياناً)، والشعور بالإحباط الناجم عنه لصالحها، وتظهر بمظهر القوة التي تتبنى نضال الشعوب لإنجاز المهام الوطنية والاقتصادية والثقافية والدينية.
٤. من المؤكد أن التنظيمات الإرهابية في المجتمعات العربية لم توجد في فراغ، وإنما ظهرت في سياق ظروف سياسية واجتماعية واقتصادية ودينية معينة، أنتجتها وربما ما زالت تعيد إنتاجها.
٥. تعتمد التنظيمات الإرهابية في المجتمعات العربية أساساً على فئة الشباب المحبط بسبب معطيات الواقع العربي ومفرداته.

٦. تتميز التنظيمات الإرهابية في المجتمعات الدينية بطابعها غير القطري، وبأنها عابرة للحدود القطرية، وذلك نتيجة للقضية العامة، التي تزعم أنها تعمل من أجلها.

٧. تحرص التنظيمات الإرهابية العربية على تحقيق التواصل الدائم مع الجماهير الواسعة من خلال استخدامها لوسائل الإعلام العامة، والإلكترونية (الإنترنت الخاصة)، وإقامة صلات خاصة مع بعض الوسائل الإعلامية العربية (وخاصة الفضائيات التلفزيونية الواسعة الانتشار) واعتمادها على بعض الأوساط المتدينة المتعاطفة معها.

وتتسم الجرائم الإرهابية التقنية بعدد من الخصائص التي تميزها عن الجرائم التقليدية ومن أهم تلك الخصائص (هاشم الزهراني، ٢٠٠٧، ٣٩٨ : ٣٩٩):

١. استخدام التقنية الحديثة أو الأساليب المبتكرة في كل عملية من مراحل الجريمة والأمر البارز أن عملية الاستحداث ذاتها متطورة ومتجددة مع كل تطور تقني.

٢. تدويل الجريمة وإخراجها من الحدود الوطنية والإقليمية سواء في مرحلة الإعداد أو التنفيذ أو الآثار المترتبة عليها سواء العاجلة منها أو الآجلة.

٣. تعدد جنسيات الأشخاص والمنظمات المرتبطين بها بل وتتزايد عدد الأشخاص المشتركين في الجريمة والمضارين منها بشكل كبير كلما توفرت وسائل التقنية الحديثة.

٤. تعقدت الظروف المهيأة لاكتشاف تلك الجرائم.

٥. ارتفاع تكلفتها وتعاظم آثارها على البنية الاجتماعية وذلك من حيث حجم الضحايا والمصابين مادياً ونفسياً وكذلك الدمار الذي يصيب الممتلكات من مباني وآليات وخلافه.

وتعمل التنظيمات الإرهابية بشكل مستمر على مثالية استخدام وسائل المعلومات الإلكترونية المتطورة وما يشجعها على ذلك ما تحصل عليه من فوائد يمكن تلخيصها فيما يلي:

١. ضمان عنصر السرية: حيث تتسم الجرائم الإرهابية التي تعتمد على التقنية على نظام سري محكم وكفاءة التنظيم تعتمد على عنصر السرية الذي يكفل عدم اختراقه.

٢. استمرار المعلومات والأفكار: باعتبار أن أنظمة المعلومات الإلكترونية المتطورة تضمن نقل المعلومات والأفكار وتبادلها من خلال شبكات التنظيم الإرهابي مما يؤدي إلى عمومية تلك الأفكار وبناء علاقات حميمة مع أعضاء التنظيم مع بعضهم البعض.

٣. الانخفاض الكبير في أسعارها وصغر حجمها وسهولة الحصول عليها.

٤. زيادة الإمكانات المتوفرة في وسائل وأنظمة المعلومات الآلية ومثل تلك الإمكانات تعزز قوة التنظيم الإرهابي وتظهر أكبر من حجمه الطبيعي وهذا ينسجم مع أهدافه.

٥. تمكين التنظيم: الاتصال بالجماهير بسهولة من خلال مواقع الإنترنت وعن طريق البريد الإلكتروني. (هاشم الزهراني، ٢٠٠٧، ٤٠١، ٤٠٢)

أما فيما يتعلق بمرتكبي هذا النوع من الجرائم يمكن النظر إليهم كما يلي:

فالمجرم الإلكتروني التقني هو الشخص الذي يخالف القانون ولديه معرفة إلكترونية لاستخدام الحاسب الآلي وشبكة الإنترنت وأجهزة الاتصال جنباً إلى جنب، أما التقنية الحديثة فهي الوسيلة (الجديد منها وما يستجد في المستقل) في حين أن الجريمة الإلكترونية الحديثة هي أيضاً كل فعل لا اجتماعي تعني بفرض تحقيق غرض إجرامي إرهابي محدد فيه اعتداء على المصلحة العامة أو النفس أو المال. (عبد الرحيم صدقي، ١٩٨٩، ١٤٣)

ومن هنا نجد أن المجرم في ظل نظام العولمة الثقافية، يطلق عليه المجرم الإلكتروني الرقمي وهو اصطلاح له عدة مدلولات قانونية، الكترونية، وأيضاً لغوية.

فمن حيث الاصطلاح القانوني، فإن المجرم الإلكتروني التقني يطلق عليه علماء وفقهاء القانون الجنائي اصطلاح "المجرم المعلوماتي" وهو يعني الشخص الذي لديه مهارات تقنية أو دراية تكتيكية باستخدام الحاسب الآلي والقادر أيضاً على اختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسب نفسه. (هدى حامد، ٢٠٠٠، ٢٧)

أما من ناحية الأصطلاح الإلكترونية، فيطلق خبراء أمن المعلومات الإلكترونية مصطلح "هاكرز" Hackers، وهي جمع لكلمة "هاكر" وتعنى الإنسان الذي يقوم بعمليات الاختراق والتخريب عبر شبكة الإنترنت، كما يطلقون مصطلح "كراكرز" Crackers على المتخصصين بفك شفرات البرامج وليس تخريب الشبكات، فهم نوع من "الهاكرز" المتخصص.(مصطفى موسى،٢٠٠٣، ١٥_ ١٦)

أما من ناحية المعنى اللغوي لكلمة "الهاكرز" فنظر لعدم وجود ترجمة دقيقة وواضحة للكلمة حتى الآن، فإن مصطل الهاكرز يستخدم كما هو، وإن كان مصطلح "مخترقوا أمن الشبكات" هو الأقرب تفسيراً للمعنى حتى الآن، ويطلق "مصطفى موسى" اصطلاح "المجرم الإلكترونية الرقمي" على كل مخترق لشبكة الإنترنت، ويقصد بالرقمي Digital تخزين البيانات في ذاكرة الحاسب الآلي الرقمي في شكل أرقام، وحين تطلب تخرج على شاشة الحاسب أو الطابعة في الشكل المقروء حسب اللغة التي خزنت بها، وليس كما هي مسجلة في ذاكرته، وعلى ذلك فالمجرد الإلكتروني الرقمي هو الذي لديه قدرته على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسب الإلكتروني الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء

فعل محدد، مما يحدث اضطرابات في المجتمع المحلي أو الدولي نتيجة لمخالفة قواعد الضبط الاجتماعي محلياً ودولياً. (مصطفى موسى، ٢٠٠٣، ١٦ ـ ١٧)

وإذا نظرنا إلى هذه الجرائم وأساليب ارتكابها وسلوك مرتكبيها، نجد أن الفرصة متاحة لهؤلاء المجرمين ـ أفراداً ومنظمات ـ أن يضعفوا المجتمع ويقوموا بهدم أي مجتمع دون الحاجة إلى إطلاق رصاصة أو صاروخ واحد، ولكي ندرك هذه الحقيقة يجب أن نتصور عدد القطاعات الرئيسية في أي مجتمع حديث، وبخاصة تلك التي تعتمد على التقنية الحديثة، والتي بفقدانها ربما تحل كارثة كبيرة في هذا المجتمع أو ذاك ومن هذه القطاعات على سبيل المثال لا الحصر القطاع الصحي، البنوك، القطاع الصناعي، النقل والمواصلات، والأهم والأكثر خطورة القطاع الأمني والعسكري، وكذا بقية القطاعات الحكومية الأخرى.

ثالثاً: أساليب الجرائم الإرهابية التقنية:

لقد زادت في الآونة الأخيرة الجريمة، بشكل يصعب معه تحديد مرتكبيها ومعاقبتهم، وذلك نظراً لاستخدام أساليب التقنية رقمية، جعلت من الصعوبة بمكان الوصول إلى المجرم في ظل هذا النظام التقني والفضائي الحديث.

وهذه مشكلة كبيرة يعاني منها كل من الدول المتقدمة تكنولوجياً، والدول النامية التي تأخذ ببعض البرامج التكنولوجية الحديثة. وذلك بسبب تعدد الأساليب المتعلقة بالجريمة التقنية من ناحية، ونوعية المجرم التقني الذي يستخدم هذه الأساليب التقنية الرقمية من ناحية أخرى. لذلك لابد لنا أن نتعرف على الأساليب الإلكترونية الرقمية، ونوعية المجرم التقني الرقمي، وكذلك أنواع تلك الأساليب التقنية المستخدمة في هذه النوعية من الجرائم.

فإذا ما تم لنا معرفة ذلك، أمكن لنا أن نشكل الأساليب المضادة للحد من الجريمة وضبطها، وبذلك تسهم هذه المعرفة في تمكن رجال البحث الجنائي الإلكتروني من ضبطها، حتى تكون معرفتهم لهذه الجرائم التقنية الرقمية سابقة على المجرم الإلكتروني الرقمي في الوقت الراهن.

وقد تعددت، بل واختلفت طرق وأساليب جرائم الحاسبات الآلية والإنترنت، فهناك أساليب شائعة ومعروفة في ارتكاب جريمة الحاسب الآلي، والتي يمكن أن توظيف في مجالات الإرهاب المتنوعة والمتعددة، نذكر منها على سبيل المثال لا الحصر ما يلي (مصطفى موسى، ٢٠٠٥، ١٤٤ ـ ٢٢٠):

أولاً: الأساليب الإجرامية الإلكترونية في الاعتداء على المال، ويتضمن المزادات الإجرامية عبر الإنترنت، التسول عبر الإنترنت، الاستيلاء على بطاقات الائتمان، أساليب التحويل الإجرامية بالتقنية الرقمية.

ثانياً الأساليب الإجرامية الإلكترونية الرقمية في الاعتداء على العرض والنفس والتي تتضمن الدردشة المثيرة للغريزة، وإنشاء مواقع إباحية، وإرسال رسائل

الكترونية إباحية، وإنشاء مواقع لممارسة الجنس عبر الإنترنت ويمكن أن تستخدم تلك الأساليب عبر الإرهابيين للابتزاز والحصول على مال أو معلومات يمكن أن توظيف في أي عمل إرهابي.

ثالثاً: الأساليب الإجرامية الإلكترونية الرقمية المضرة بأمن المجتمع ومنها أساليب منع الوصول إلى المواقع عبر الإنترنت من خلال إغراق المواقع المستهدفة بمجموعة من البيانات تفوق الجيجا بايت في الثانية الواحدة وتلك البيانات عبارة عن طلبات غير حقيقية.

كذلك التهديد عبر الإنترنت، نشر العنصرية وإذكاء التمييز العنصري، التزوير الإلكتروني الرقمي للأوراق المالية.

وقد أخذت كثير من الدول والمجتمعات حالياً بنظام الإدانة الإلكترونية أو الحكومة الإلكترونية في كثير من تعاملاتها ونظمها ومن المفيد في هذا الصدد (عبد الفتاح بيومي، ٢٠٠٨، ٣١٥ ـ ٣٣٠):

أولاً: تزوير البيانات والمعلومات أو المخرجات الكومبيوترية الخاصة بالحكومة الإلكترونية:

ثانياً: جرائم الأموال: مثل سرقة المعلومات المالية والأموال، واختراق الحسابات المصرفية وتحويل مبالغ مالية من حسابات العملاء إلى حسابات المخترقين وجريمة الإتلاف المعلوماتي.

ثالثاً: جرائم الاعتداء على بيانات الحكومة الإلكترونية: والركن المادي لهذه الجريمة له صور متعددة منها الدخول غير المشروع لمواقع الحكومة الإلكترونية والتعدي على البيانات الشخصية، وانتهاك سرية وخصوصية البيانات، والاعتداء على التوقيع الإلكتروني والاعتداء على البيانات المشفرة.

لذلك، فإن الأسلوب الإجرامي، هو ذلك الذي يتعلق بكيفية قيام المجرم باستخدام طريقة تتصل بالفعل أو الأداء المتمثل في القيام بفعل أو الامتناع عنه مما يحدث اضطراباً في المجتمع نتيجة مخالفة قواعد الضبط الاجتماعي.

وهذا الفعل أو الامتناع، يطلق عليه اسم "الجريمة" وعلى من أرتكبه اسم "المجرم" والفعل الذي يرتكبه المجرم بواسطة وسائل تقنية الكترونية رقمية سواء شبكة الإنترنت أم بدونها، يمكن أن يطلق عليه اسم "الجريمة الإلكترونية" ويطلق على من يرتكبها اسم "المجرم الإلكتروني الرقمي" وعندما نقول أساليب الجريمة الإلكترونية، فإننا نقصد هنا بالأساليب الإجرامية الرقمية، كيفية استخدام الحاسب الآلي بنظمه، وبرامجه، ووسائل الاتصال الرقمي، في ارتكاب الجرائم، سواء كانت هذه التقنية الرقمية هي محل الجريمة أم كانت وسيلة من وسائل ارتكابها، وسواء كانت عبر شبكة الإنترنت أو بأي أسلوب تقني أخرى، يستخدم وسائل الكترونية رقمية حديثة.

ويستخدم "الإنترنت كوسيلة لارتكاب الجرائم والتي تنقسم إلى قسمين:

الأول: وهو القسم الذي يحمل طابعا جنائياً بحتاً.

والثاني: وهو يحمل طابع سياسي.

وسواء كانت الجرائم التي ترتكب تحمل طابعاً جنائياً بحتاً، أو طابعاً سياسياً خالصاً، وهي جرائم تبدو تقليدية تماماً، فإن الوسائل التي تستخدم في ارتكابها اليوم، تعد وسائل تقنية والكترونية رقمية، وخاصة أن الوسيلة التي تستخدم في ارتكابها هي "الإنترنت" مما يجعلها تصبح جريمة الكترونية رقمية ذات طابع تقني في أسلوبها وفي طريقة القيام بها.

رابعاً: دور المجتمع تجاه تلك الجرائم:

اتجهت المملكة بموجب القرار ١٦٣ بتاريخ ١٤١٧/١٠ بتشكيل اللجنة الأمنية الدائمة للإنترنت تحت رئاسة وزارة الداخلية وعضوية عدة وزارات وتلك اللجنة هي المعنية باتخاذ القرارات فيما يخص المواد المرشحة في خدمة الإنترنت داخل المملكة، وبعدها تم تحويل مدينة الملك عبد العزيز للعلوم والتقنية ومن بعدها هيئة الاتصالات وتقنية المعلومات بحجبها مباشرة دون الرجوع إلى اللجنة وذلك بسبب الكثرة الهائلة للمواقع الإباحية التي كان يطلب حجبها. ثم صدر قرار رئيس مجلس الوزراء رقم ٢٢٩ بتاريخ ١٤٢٥/٨/١٣ القاضي بإعادة تنظيم هذه الخدمة في المملكة ونقل الإشراف عليها من مدينة الملك عبد العزيز إلى هيئة الاتصالات وفي هذا الصدد تشير إلى قيام أربعة جامعات أجنبية نظام الترشيح السعودي وهي (هارفرد، كامبرج، تورنتو، إكسفورد) وجاءت نتائجها كما يلي:

- كفاءة ترشيح المواقع الإباحية ٩٨%.
- كفاءة ترشيح مواقع المخدرات ٨٦%.
- كفاءة ترشيح مواقع الميسر ٩٣%.
- كفاءة ترشيح المواقع السياسية ٣%.
- كفاءة ترشيح المواقع الخاصة بالكيان الصهيوني ٢%.
- كفاءة ترشيح المواقع الدينية ١%

ووفق نتائج استبانة عامة طبقتها هيئة الاتصالات في ٢٠٠٥/٥م اتضح أن نسبة ٦٥% من المستخدمين يؤيدون استمرار أو تقوية نظام الترشيح، ٢٨% يؤيدون تخفيف أو إلغاء الترشيح، ٧% إمتنعوا عن التصويت (مشعل القدهي، ٢٠٠٧، ٥٩٩ ـ ٦٠٠)

أما الدور غير الرسمي في مواجهة الانحراف التقني تجاه الأحداث تقتضي العمل في ثلاثة اتجاهات هي (عبد الفتاح بيومي، ٢٠٠٩، ٢٧٩ ـ ٢٨٠):

١- تكريس دور الأسرة معلوماتياً، بمعنى مسارعة الأب والأم إلى الإلمام بتقنية الإنترنت والتعامل معها على نحو يمكن كلاهما من مراقبة الطفل أو الحدث حالة تجواله على الشبكة.

٢- اهتمام المدرسة -في كافة المراحل التعليمية - بتسخير تقنية الإنترنت لأغراض تعليمية، وغرس وتدريس ثقافتها للطفل على نحو يعي معها أخطارها قبل المزايا المستمدة منها.

٣- السيطرة على جماعات الأقران التي قد تدفع الحدث إلى الانحراف التقني سواء من خلال اللقاء على مقاهي النت أو في غرف الورشة أو في الاستراحات وتسريب الخبرات الضارة فيما بينهما عن تلك السلوكيات غير المشروعة المستمدة من تلك التقنيات.

أما من المنظور الأمني الاجتماعي فإن إستراتيجية تنمية المعرفة الإلكترونية إحدى الإستراتيجيات الهامة المقترح تطبيقها من أحد الباحثين في هذا الصدد وتتلخص أبرز ملامحها في (يحيى أبو مغايضي، ٢٠٠٧، ٤٣٦ : ٤٣٨):

أ. التحفيز التلقائي: حيث أن الشروع في عملية التعلم الإلكتروني سيدفع وبشكل تلقائي إلى رفع مستوى المعرفة الرقمية لدى الجهة القائمة على التدريب وكذلك الجهات المستفيدة.

ب. التوافق بين الأسلوب والمضمون: حيث أن تقديم المعرفة الإلكترونية يتطلب أسلوباً يساعد على استيعابها والإقبال عليها بعيداً عن الأسلوب التقليدي بغرض كسر الحاجز النفسي لدى الباحثين عن المعرفة الرقمية.

ج. التفوق على العنصر الزماني والمكاني: حيث أن العملية التدريبية يمكن أن تتم في أي زمان وأي مكان وذلك من خلال استخدام التقنيات الإلكترونية المتعددة.

د. التطوير الذاتي: حيث جعلت عمليات التعلم الإلكتروني من المتدرب ذاته محوراً للعملية التعليمية مما يساعده على اكتشاف قدراته وتنميتها وتطويرها بنفسه.

ه. استثمار الطاقات الإبداعية: حيث تساهم الأساليب الإلكترونية في اكتشاف الطاقات الإبداعية والمواهب الفذة بشكل ملموس حيث يحرر المستخدم من كل القيود ويجعله في حرية تامة مع العملية المعرفية.

و. المعرفة للجميع: حيث توفر الأساليب الالكترونية لنقل وتنمية المعرفة فرصاً أكبر لمن يريد الحصول عليها من منسوبي المنظمات الأمنية بطرق وأساليب مختلفة.

وقد أضاف أحد المهتمين بالسياسات الأمنية باعتبارها مجموعة من التوجهات المتبعة من طرف المنظمة في مجال تأمين وحماية النظم المعلوماتية أن تلك السياسة الأمنية يجب أن تكون مبنية على (محمد لطفي، ٢٠٠٧، ٧٢٢):

١- إشعار وتحسيس المستخدمين بالقواعد والإجراءات التي يجب الالتزام بها بشكل دوري.

٢- نظام أمني مادي ومنطقي يتلاءم مع احتياجات المنظمة والمستخدمين.

٣- إجراءات خاصة بإرادة عمليات تحديث التطبيقات والبرمجيات.

٤- إستراتيجية واضحة بعملية حفظ وتخزين المعلومات.

٥- خطة لاسترداد النظام في حالة حدوث مشاكل.

٦- نظام مكتبي وتوثيقي يتم تحديثه باستمرار.

والمواجهة من خلال المنظور الشرعي يمكن أن يتضح جليا من خلال تجربة حملة السكينة التي يمكن عرض ملخص لها كما يلي (صالح الفريح، ٢٠٠٧، ٧٣٩ : ٧٤٢) هي حملة شعبية في انطلاقتها الأولى بدأ بها عشرون شاباً، بينتها الأساسية "الإنترنت" ثبتها فيما بعد وزارة الشئون الإسلامية – الأوقاف والدعوة إلى الإرشاد بالمملكة – اعتمدت على حسن التنظيم وتوزيع المهام وفق الأقسام التالية:

أولاً: قسم المتابعة والرصد: ويتولى أفراده دخول المنتديات والمواقع وغرف الدردشة والبالتوك لمتابعة ورصد ما يبث فيها من أفكار.

ثانياً: القسم العلمي: ويتولى أفراده مناقشة تلك الأفكار المرصودة وتقديم جرعات فقهية وعلمية في جوانب أخرى ذات ارتباط.

ثالثاً: قسم النشر: حيث يتولى نشر إنتاج القسم العلمي في المواقع والمنتديات وغيرها المزدحمة بالعيون والآذان.

رابعاً: قسم الدراسات: ويهتم هذا القسم بالعائدين إلى الحق ممن تمت محاورتهم حيث تدرس حالاتهم لمعرفة كيف تحولوا إلى أفكارهم السابقة ثم توظيف ذلك في مهام الحملة.

وتتبع الحملة منهجية الأسلوب العلمي المنطقي وجذب المترددين على المواقع لهم من خلال طرحهم إحدى الموضوعات الهامة حيث يتبين لهم بعدها المتبنين لأفكار خاطئة ثم يبدأ والحوار معهم ويعملون أمام المستخدمين بشكل مزري لا على أنهم فريق عمل جماعي.

أما المواجهة القانونية: فإنها تستدعي ما يلي:

أ. تعديل قانون الاتصالات الدولية ليشمل التعامل على الظواهر المعلوماتية المستحدثة.

ب. التعامل مع شبكة الإنترنت عن طريق البطاقة الإلكترونية التي تحوي اسم المشترك وعنوانه وموطنه وتاريخ ميلاده ونوعية الخدمة المطلوبة.

ج. حماية البنوك وجميع المصارف من كل وسائل التزوير والسرقة المالية بتغيير الشفرة السرية كل فترات زمنية قصيرة مما يضمن حقوق العملاء كما يجب تغيير مواقع المسئولين والموظفين في إطار النظام المعمول به في البنوك والمصارف الوطنية.

خامساً: بعض النماذج التطبيقية لأساليب الجريمة الإلكترونية:

هناك العديد من النماذج التطبيقية لأساليب الجريمة الإلكترونية الرقمية، فكما سبق أن أشرنا، فهناك جرائم ذات طابع جنائي، وأخرى ذات طابع سياسي، وسوف نتعرض لبعض هذه النماذج، باعتبارها وسائل مستخدمة لارتكاب الجرائم الإلكترونية، وبخاصة تلك الجرائم التي تستخدم "الإنترنت" باعتباره أحد أهم هذه الوسائل المستخدمة لارتكاب مثل هذه الجرائم، وبعض هذه النماذج التطبيقية نذكرها على النحو التالي:

١- قيادة الجماعات الإرهابية عن بعد: بحيث يمكن من خلال شبكة الإنترنت بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية، والتي تسيطر على وجدان الأفراد وتفسد عقائدهم، وتستغل معاناتهم في تحقيق مآرب خاصة تتعارض مع مصلحة الأفراد والمجتمع. (جميل الصغير، ٢٠٠٢م، ٣٢)

فقد قامت فتاة تدعى "أنجيلا ناركان" من ألمانيا، وهي تنتمي إلى إحدى الجماعات المتطرفة، قامت بوضع معلومات مفصلة على موقعها الخاص في الإنترنت عن كيفية القيام بأعمال تخريبية، منها كيفية العبث بأسلاك صناديق الإشارة الكهربائية في السكك الحديدية لتعطيل حركة القطارات، بالإضافة إلى حالات أخرى لنشر مواد إباحية تتعلق باستخدام الأطفال في الجنس، أو أساليب العنف الجنسي، وهو ما يتعارض مع قوانين الآداب العامة وقوانين حماية الطفل.

٢- تنسيق جهود عصابات الجريمة المنظمة: حيث كشف باحثة بريطانية عن استغلال شبكة الإنترنت في تجارة "الرقيق الأبيض" من خلال عقد صفقات لبيع الفتيات من أربعة دولة نامية ومن أوربا الشرقية لمواطنين في جول الغرب من أجل المتعة والجنس. حيث يتم إرسال كتالوجات تتضمن مواصفات دقيقة عن فتيات مراهقات من أوربا الشرقية والفلبين وكوستاريكا وغيرها، والثمن المحدد للشراء، وكيفية الاتصال بالوسيط، مع تنظيم لقاءات للراغبين في الشراء، ومقابلة الفتيات، اللاتي يحصلن على وعود بالزواج والثراء التي لا أساس لها من الصحة، وتربح العصابات من ورائها ملايين الدولارات. (جميل الصغير، ٢٠٠٢م، ٢٣ ـ ٢٤)

٣- جرائم تهديد الأمن القومي والعسكري: في الآونة الأخيرة وقعت عدة حوادث تبين تعرض بعض المراكز العسكرية لجرائم قرصنة معلوماتية بهدف الوصول والحصول على معلومات مخزنة في ذاكرة الحاسبات الآلية المستعملة فيها، وأكبر مثال على ذلك، سرقة معلومات عسكرية تتعلق بالسفن الحربية الخاصة

بالدول الأعضاء في حلف شمال الأطلنطي NATO وذلك من خلال أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية في صيف ١٩٩٤م.

وقد حدث، أيضاً، أن تمكن قرصان أمريكي يبلغ من العمر ثمانية عشر عاماً، من اختراق واحداً من أكثر النظم التقنية العسكرية أماناً، وهو الخاص بوزارة الدفاع الأمريكية "البنتاجون" وتسلل عبر ما يسمى "الجدران النارية" Fire Wals التي وضعت لحماية هذه الشبكة وكان بإمكانه أن يعرض البشرية كلها لخطر الإبادة لو تمكن من مواصلة عمله للنفاذ المخزون النووي الاستراتيجي ومعرفة شفرته، وضبطها نحو اتجاه معين لإطلاق آلاف القنابل النووية. (جميل الصغير، ٢٠٠٢م، ٢٤)

وفي إسرائيل، ألقى البوليس القبض على كاتب إسرائيلي بتهمة الاعتداء على أمن الدولة، حيث قام بنشر معلومات محورة على الإنترنت تتعلق باختفاء الغواصة Sous – Marin في البحر المتوسط عام ١٩٦٨م.

وأثناء عملية غزو العراق للكويت، تمكن أحد اللصوص الهولنديين من سرقة أسرار عسكرية أمريكية بالغة الأهمية، من بينها تحركات القوات الأمريكية ومواقعها وأسلحتها وتحركات الطائرات المقاتلة، وقد أرسل هذه المعلومات على العراق قبل اندلاع الحرب، إلا أن العراقيين رفضوا هذه الهدية خشية أن يكون في الأمر خدعة. (خالد حنفي، ٢٠٠٥، ١٦)

وقد أدى انتشار استخدام الحاسبات الآلية، ووسائل التقنية الإلكترونية الرقمية، إلى قلة أو ندرة الجواسيس الدوليين، الذين يتبادلون حقائب الملفات في أماكن سرية، أو نقل معلومات مهمة في ميكروفيلم يخفي في أماكن معينة من جسم الإنسان، فالمواد المحظورة مثل المنشورات الإرهابية أو الخطط الإرهابية التخريبية، أو المواد الخطرة، يمكن بل يسهل نقلها الآن من خلال ضغطه واحدة خفيفة على زر موجود بلوحة مفاتيح جهاز الكمبيوتر. (جميل الصغير، ٢٠٠٢م، ٣٤)

وهناك العديد من النماذج التطبيقية لأساليب الجريمة الإلكترونية الرقمية، يصعب حصر أنماطها، نظراً للتطور السريع في أساليب التقنية الحديثة لأنماط جرائم الحاسبات الآلية، فهناك جرائم إلكترونية رقمية تشمل العديد من أوجه الحياة الاجتماعية والاقتصادية والثقافية، وكذلك تشمل الأمن الاجتماعي والقومي والاستراتيجي والعسكري. فعلى سبيل المثال لا الحصر، هناك جرائم للسطو على البنوك، وجرائم تمثل الاحتيال باستخدام بطاقات الدفع الإلكتروني، والجرائم المخلة بالآداب العامة للمجتمع واستثارة الغرائز الجنسية، وجرائم الأحداث وبيع الأطفال عبر الشبكة العملاقة "الإنترنت".

ومن الأمثلة التطبيقية لمثل هذه الجرائم نذكر منها بعضاً من النماذج التي استخدمت تلك التقنية الحديثة في غير الغرض المخصص لها، وهي جريمة لصبي يبلغ من العمر ستة عشرة سنة من أصل استرالي، قام بالدخول إلى أحد المواقع البولندية على شبكة الإنترنت، وقام بتحميل البرامج التي تستخدمها بالبنوك. لكي يتوصل إلى

الترتيب العشوائي لترقيم بطاقات الائتمان. وبعد أن توصل إلى الأرقام الصحيحة لهذه البطاقات، استخدمها في شراء أجهزة كمبيوتر بلغت قيمتها ٣٧ ألف دولار استرالي (حوالي ٢٤ ألف دولار أمريكي) وتبرع لأحد الجمعيات الخيرية بمبلغ ٥,٧٠٠ دولار.

ومن أمثلة النماذج التطبيقية لأساليب الجريمة الإلكترونية، والتي تمس الأمن الاجتماعي لأي مجتمع، تلك الجريمة التي قام بها طالب مصري يدرس بمعهد الطيران المدني ويدعى (أ – أ – ش) حيث روج هذا الطالب "عبر موقع أنشأه على الإنترنت باللغة الإنجليزية" لشائعة وجود سفاح طليق بمنطقة مصر الجديدة ومدينة نصر، يقوم باستدراج الفتيات وقتلهن، مما ترتب عليه إنتشار الذعر والخوف بين الفتيات والنساء بهذه المناطق، مما أدى إلى زعزعة الأمن والاستقرار الاجتماعي بهذه المناطق لفترة من الزمن.

وقد حكمت محكمة أمن الدولة بحبس الطالب شهرين وغرامة ٢٠٠ جنيه مصري، في أول قضية من نوعها ينظرها القضاء المصري، وبخاصة في مجال استخدام الحاسب الآلي، مستنداً في ذلك على المادة ١٠٢ مكرر من قانون العقوبات والخاصة "بكل من أذاع عمداً شائعات كاذبة من شأنها زعزعت الأمن العام، وإلقاء الرعب في قلوب الناس وإلحاق الضرر بالمصلحة العامة".

ومن الأمثلة التطبيقية على أنواع الجرائم التي تمس الأمن الاستراتيجي والعسكري، تلك الجريمة التي قام بها "ريتشارد برايس"، والذي يبلغ من العمر ١٦ عاماً وهو بريطاني الجنسية حيث استخدم شبكة الإنترنت لاختراق محطة الأبحاث النووية لكوريا الشمالية، وشبكة القوات الجوية الأمريكية، مما كان سيعرض هذه المجتمعات إلى كارثة نووية وعسكرية خطيرة، ليس فقط على كوريا الشمالية والولايات المتحدة، بل كارثة تشمل العالم كله، مما يهدد الأمن والاستقرار العالمي. وهذه جرائم في غاية الخطورة على الأمن والسلام العالميين. (مصطفى موسى، ٢٠٠٣م، ٧٠ – ٧١)

وعموماً، فإن كل هذه النماذج التطبيقية السابقة للجرائم الإلكترونية الرقمية، وغيرها الكثير، ليست هي الغرض الأساس الذي ظهرت من أجله أجهزة الحاسبات الآلية، ليست هي الغرض الأساسي الذي ظهرت من أجله أجهزة الحاسبات الآلية، أو الشبكة العملاقة "الإنترنت" وإنما كان الهدف الأول من إنشائها هو زيادة حجم المعلومات وانتشارها عبر القارات بشكل سريع، وكذلك الاستفادة من الثورة العلمية الحديثة، والاستفادة من الدراسات على مستوى العالم ..... إلى غير ذلك من الأهداف المفيدة علمياً وتكنولوجيا وتكون أيضاً ذات أهداف نبيلة تحمل قيماً إنسانية.

سادساً : تحديات مكافحة الجريمة في ظل نظام العولمة الثقافية:

تواجه الجريمة الإرهابية التقنية في ظل العولمة الثقافية، تحديات كبيرة في مواجهتها ومكافحتها، نظراً لأساليب التقنية التي تستخدمها من ناحية، وتنوع أشكالها وتعددها من ناحية أخرى. فتلك الجرائم كثيرة ومتنوعة وسريعة، وتشمل كافة نواحي

الحياة الاجتماعية والاقتصادية والثقافية وأيضاً الأمنية، مما يجعل هذه الجرائم تمثل تهديداً خطيراً لأمن الفرد والمجتمع والثقافة.

ومن هنا نجد أنه لا يوجد حل جذري ينصح به للوقاية من جرائم الحاسب الآلي بأشكالها المختلفة، فكما سبق أن رأينا، فإن جرائم الحاسب الآلي والإنترنت تتنوع أشكالها وتتعدد أساليب إرتكابها وتظهر في كل يوم أساليب جديدة بحسب التطور التقني الذي يحدث بسرعة رهيبة، في كافة الوسائل والأساليب الاتصالات الحديثة، إلا أنه يجب وضع إستراتيجية أمنية شاملة لنظم المعلومات تحدد عناصرها ومسئوليات الدخول إلى نظم المعلومات، كما يجب وضع خطة طوارئ دقيقة واختبارها ومراجعتها بصفة دورية. (صالح المسند، ٢٠٠٠م، ١٩٠)

أما عن تحديات مواجهة الجريمة الإرهابية التقنية في ظل نظام العولمة، فقد قدم "مارتن نايجمان" M. Nabgman تقريراً حول "أوربا ومجتمع المعلومات العالمي" أو ما يسمي بمجتمع الإعلام الكوكبي، وقد نشر التقرير في يوليو ١٩٩٤م، وقد تضمن التقرير خطة عمل ضمن أربعة محاور رئيسية، وقد كانت أهم نقطة في التقرير هي "ضرورة سرية البيانات وحماية حقوق الملكية الفكرية". (محمد الرومي، ٢٠٠٣، ١١٢ ـ ١١٣)

وقد ناقش وزراء خارجية دول الاتحاد الأوربي مشروع يسمح بحماية أسس البيانات، هذا بالإضافة إلى قرارات مؤتمر قمة الدول الصناعية السبعة في فبراير من عام ١٩٩٥م.

ولمكافحة الجريمة التقنية، وحماية البيانات والمعلومات الإلكترونية، فقد قدم كل من وزير العدل الكندي والنائب العام في نهاية ١٩٩٥م، قدما مشروع قانون يقترحان فيه ما يقرب من مائة وخمسون تعديلاً في قانون العقوبات والقوانين الأخرى المرتبطة به، والخاصة بالجرائم التكنولوجية، وتزوير كروت الاعتماد والاحتيال، والحصول على خدمات بوسائل تدليسية، وذلك من أجل مكافحة ومواجهة الجرائم الالكترونية، وتشديد العقوبات الخاصة بهذه الجرائم، نظراً لخطورتها على المجتمع والأمن القومي لكافة المجتمعات.(السيد عتيق، ٢٠٠٢م، ٤٢)

ولما كان لجرائم الإنترنت هذه الخطورة على أمن الفرد والمجتمع، وبخاصة ما يتعلق بحرية البيانات والمعلومات الخاصة بكل فرد أو مؤسسة، وخاصة أن تلك الجرائم تمثل اعتداءاً على النفس والعرض والمال وغيرها. وكذلك ما تمثله هذه الجرائم من تهديد للأمن القومي للمجتمعات على مستوى العالم، ما يتبع ذلك من آثار اجتماعية وثقافية واقتصادية سلبية، وبخاصة أن هناك بعض من هذه الجرائم تمثل اعتداءاً على حياة وأمن واستقرار الأسرة والمجتمع، لأن من بين الجرائم التي ترتكب في هذا الشأن ما يعرض تلك الأسر أو المجتمعات لمشكلات اجتماعية بالغة الخطورة، خصوصاً أنها تمس أعراض هذه الأسر، أو التشهير ببعض أفرادها. وكذلك بث الصور والموضوعات التي قد تتسبب في التفكك الأسري، والخلافات العائلية، والتي غالباً ما تؤدي إلى الانفصال أو الطلاق في كثير من الأحيان.

ولما كان لهذه الجرائم هذا القدر من الخطورة، فإنه كان لزاما على الجهات الأمنية والتشريعية والقضائية أن تطور أساليبها ووسائلها حتى يمكنها التعامل مع جرائم ثورة المعلومات الحديثة، ومواجهة تلك الجرائم الإلكترونية بأسلوب علمي متطور وغير تقليدي، حتى يمكنها أن تقف أمام تحديات عصر العولمة الثقافية وتكنولوجيا الاتصالات والمعلومات، وذلك في ظل التقدم التقني الذي فتح آفاقاً جديدة، وجلب معه مشكلات ومخاطر جديدة لم تكن نسمع عنها من قبل، لذلك فإن لم نستطع أن نواجهه هذه المخاطر والتهديدات والمشكلات الناجمة عن هذه الثورة المعلوماتية، ونتعامل معها بكفاءة عالية واقتدار، وأن نطور مؤسساتنا وأنظمتنا، فإن أمننا الاجتماعي والقومي سيكون مهدداً وتصبح بذلك حياتنا الاجتماعية والثقافية والاقتصادية، بل والإستراتيجية في خطر كبير، لذلك يجب وضع البرامج والأساليب والطرق الحديثة الفعالة للتعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد والمجتمعات على مستوى العالم كله. (صالح المسند،عبد الرحمن المهيني ٢٠٠٠م، ١٩٤)

ورغم أن "الإنترنت" يمكن أن يستفاد منه في فتح آفاق جديدة للمعرفة والتقدم التقني لكافة المؤسسات التعليمية والصحية والاقتصادية، والاستفادة كذلك منه في التسويق والإعلان والخدمات العديدة الأخرى، وهذا هو الغرض الأساسي الذي أنشئ من أجلها، لخدمة البشرية وتيسير الاتصالات الدولية ونقل البيانات والمعلومات التي تعود بالفائدة على الفرد والمجتمع، إلا أنه قد فتح أبواباً خلفية للمتسللين واللصوص لارتكاب العديد من المخالفات والجرائم. وبخاصة تلك النوعية التي تهدد أمن الفرد والمجتمع، أو تلك الجرائم التي تؤثر سلباً على الأمن الاجتماعي والقومي لكافة مجتمعات العالم، وهذه النوعية من الجرائم الإلكترونية تمثل خطراً – ليس كلياً بل دولياً – كبيراً يجب التصدي له ومواجهته تتضافر فيه جهود الفرد والمجتمع المحلي وكذلك الدولي نظراً لما تحمله من تهديدات على الصعيدين الفردي والمجتمعي.

مراجع البحث

١. المجمع الفقهي (١٤٢٢) بيان مكة المكرمة لرابطة العالم الإسلامي ، مكة المكرمة ، الدورة السادسة عشرة .
٢. هاشم الزهراني (٢٠٠٧) الإرهاب المعلوماتي : المواجهة، كلية الملك فهد الأمنية. مركز البحوث، ندوة المجتمع والأمن الجرائم الإلكترونية، الرياض .
٣. عبد الفتاح بيومي (٢٠٠٩) الأحداث والإنترنت : أثر الإنترنت في انحراف الأحداث، دار الفكر العربي ، الإسكندرية .
٤. حنين بوادي (٢٠٠٦) الإرهاب ، مكتبة العبيكان ، الرياض .
٥. مصطفى موسى (٢٠٠٥) أساليب إجرامية بالتقنية الرقمية ماهيتها .. مكافحتها دار الكتب القانونية، المحلة الكبرى .

٦. عبدالعزيز الشبل (٢٠٠٧) الجرائم الإلكترونية نسخ البرامج أنموذجاً، ندوة الأمن والمجتمع ، الجرائم الالكترونية ، الرياض .
٧. أديب حضور (٢٠٠٧) بين رسوخ الظاهرة ولحظة الحدث : المواجهة بين الإعلام العربي والإرهاب ، مركز اسبار للدراسات والبحوث والأعلام ، الرياض .
٨. عبدالرحيم صدقي (١٩٨٩) الظاهرة الإجرامية، دار الثقافة العربية ، القاهرة .
٩. هدى حامد (٢٠٠٠) الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون جامعة الإمارات .
١٠. مصطفى موسى (٢٠٠٣) أساليب إجرامية بالتقنية الرقمية : ماهيتها ـ مكافحتها ، دار الكتب والوثائق المصرية، القاهرة .
١١. عبدالفتاح بيومي (٢٠٠٨) عالم الجريمة والمجرم المعلوماتي ، منشأة المعارف، الإسكندرية .
١٢. يحيى أبو مقايضي (٢٠٠٧) استراتيجيات تقنية لمواجهة الجريمة الالكترونية، نموذج شمولي ، ندوة المجتمع والأمن الجرائم الإلكترونية الرياض .
١٣. محمد لطفي (٢٠٠٧) الجرائم المعلوماتية: التحديات والحلول ندوة المجتمع والأمن الجرائم الالكترونية ، الرياض .
١٤. صالح الفريح (٢٠٠٧) مواجهة جرائم التطرف والغلو والتفكير من خلال الانترنت، ندوة المجتمع، والأمن ، الجرائم الإلكترونية ، الرياض
١٥. جميل الصغير (٢٠٠٢) الانترنت والقانون الجنائي، دار النهضة العربية ، القاهرة.
١٦. خالد حنفي محمد (٢٠٠٥) الإنترنت وتصدير الإرهاب، السياسة الدولية، مركز الأهرام للدراسات الإستراتيجية، القاهرة .
١٧. محمد امين الرومي(٢٠٠٣)جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية .
١٨. السيد عتيق (٢٠٠٢) جرائم الإنترنت، دار النهضة العربية، القاهرة .
١٩. صالح المسند، عبدالرحمن الجهني(٢٠٠٠) جرائم الحاسب الآلي: الخطر الحقيقي في عهد المعلومات، أكاديمية نايف للعلوم الأمنية، مجلدة ١٥ عدد ٢٩ الرياض .
٢٠. مشعل بن عبدالله القدهي (٢٠٠٧) مسح وتحليل ظاهرة تقنية الإنترنت حول العالم مع تحليل الأساليب المتبعة في ذلك ، ندوة الأمن والمجتمع الجرائم الالكترونية ، الرياض
٢١. المجمع الفقهي (١٤٢٢) بيان مكة المكرمة لرابطة العالم الإسلامي ، مكة المكرمة ، الدورة السادسة عشرة .
٢٢. هاشم الزهراني (٢٠٠٧) الإرهاب المعلوماتي : المواجهة، كلية الملك فهد الأمنية، مركز البحوث، ندوة المجتمع والأمن الجرائم الإلكترونية، الرياض .
٢٣. عبد الفتاح بيومي (٢٠٠٩) الأحداث والإنترنت : أثر الإنترنت في انحراف الأحداث، دار الفكر العربي ، الإسكندرية .
٢٤. حنين بوادي (٢٠٠٦) الإرهاب ، مكتبة العبيكان ، الرياض .
٢٥. مصطفى موسى (٢٠٠٥) أساليب إجرامية بالتقنية الرقمية ماهيتها .. مكافحتها دار الكتب القانونية، المحلة الكبرى .

٢٦.عبدالعزيز الشبل (٢٠٠٧) الجرائم الإلكترونية نسخ البرامج أنموذجاً، ندوة الأمن والمجتمع ، الجرائم الالكترونية ، الرياض .
٢٧.أديب حضور (٢٠٠٧) بين رسوخ الظاهرة ولحظة الحدث : المواجهة بين الإعلام العربي والإرهاب ، مركز اسبار للدراسات والبحوث والأعلام ، الرياض .
٢٨.عبدالرحيم صدقي (١٩٨٩) الظاهرة الإجرامية، دار الثقافة العربية ، القاهرة .
٢٩.هدى حامد (٢٠٠٠) الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون جامعة الإمارات .
٣٠.مصطفى موسى (٢٠٠٣) أساليب إجرامية بالتقنية الرقمية : ماهيتها – مكافحتها ، دار الكتب والوثائق المصرية، القاهرة .
٣١.عبدالفتاح بيومي (٢٠٠٨) عالم الجريمة والمجرم المعلوماتي ، منشأة المعارف، الإسكندرية .
٣٢.يحيى أبو مقايضي (٢٠٠٧) استراتيجيات تقنية لمواجهة الجريمة الالكترونية. نموذج شمولي ، ندوة المجتمع والأمن الجرائم الالكترونية الرياض .
٣٣.محمد لطفي (٢٠٠٧) الجرائم المعلوماتية: التحديات والحلول ندوة المجتمع والأمن الجرائم الالكترونية ، الرياض .
٣٤.صالح الفريح (٢٠٠٧) مواجهة جرائم التطرف والغلو والتفكير من خلال الانترنت. ندوة المجتمع، والأمن ، الجرائم الإلكترونية ، الرياض
٣٥.جميل الصغير (٢٠٠٢) الانترنت والقانون الجنائي، دار النهضة العربية ، القاهرة.
٣٦.خالد حنفي محمد (٢٠٠٥) الإنترنت وتصدير الإرهاب، السياسة الدولية، مركز الأهرام للدراسات الإستراتيجية، القاهرة .
٣٧.محمد امين الرومي(٢٠٠٣)جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية. الإسكندرية .
٣٨.السيد عتيق (٢٠٠٢) جرائم الإنترنت، دار النهضة العربية، القاهرة .
٣٩.صالح المسند، عبدالرحمن الجهني(٢٠٠٠) جرائم الحاسب الآلي: الخطر الحقيقي في عهد المعلومات، أكاديمية نايف للعلوم الأمنية، مجلدة ١٥ عدد ٢٩ الرياض .
٤٠.مشعل بن عبدالله القدهي (٢٠٠٧) مسح وتحليل ظاهرة تقنية الإنترنت حول العالم مع تحليل الأساليب المتبعة في ذلك ، ندوة الأمن والمجتمع الجرائم الالكترونية ، الرياض .