Cyber Terrorism and ways to face it

الإرهاب الالكتروني وسبل مواجهته

أ.م.د. سامر مؤيد عبد اللطيف
جامعة كربلاء /مركز الدراسات القانونية والدستورية

مستخلص البحث

يمثل الإرهاب بجميع أشكاله تهديدا خطرا للأمن الوطني والدولي على حدٍ سواء ، نظراً لما له من آثار وخيمة على أمن المواطنين واستقرارهم، وعلى الإمكانات الإقتصادية والهيبة السياسية للدولة في محيطيها الإقليمي والدولي. ومما زاد في مخاطر النشاط الإرهابي ، التطور الهائل في وسائل الاتصالات وثورة الانترنيت التي حولت العالم الى قرية صغيرة ، وجعلت المعلومات في متناول إرهابيين يستخدمونها في تنفيذ انشطتهم الإرهابية ، لينشأ بذلك نمط جديد من الإرهاب يدعى الإرهاب الالكتروني .

يهدف هذا البحث الى تبيان ماهية الإرهاب الالكتروني ، وتحري أسبابه وصوره ، ومن ثم تبيان سبل التصدي له .

وقد توصل البحث الى نتيجة مفادها ان الإرهاب الإلكتروني يمثل نشاطا غير مشروع بإستخدام تطبيقات الشبكة الدولية للمعلومات ، صادر من الدول أو الجماعات أو الأفراد لالحاق الضرر بالبنى المادية والمعنوية لمجتمع ما أو مؤسساته لتحقيق اهداف سياسية . فتكون المعلومة هي سلاح هذا النوع من الإرهاب ، والذي يزداد خطورةً وفتكاً كلما زاد التقدم في المجال المعلوماتي لاسيما في الدول الاكثر تقدما في المجال التقني . وفي مواجهة ذلك وجب اتخاذ ما يمكن من وسائل للمواجهة هذا التهديد الالكتروني عبر سلسلة من الاجراءات على صعيد الدولة والمجتمع الدولي ، وعلى صعيد التشريعات القانونية الاستعدادات التقنية . والله الموفق .

Abstract

All forms of terrorism represent a threat to national and international security , because of its devastating effects on the citizens' security and stability, and the economic capabilities and political prestige of the State in the regional and international environment . Adding to the risk of terrorist activity, the tremendous development in mass communications and the Internet revolution that has transformed the world into a small village, and made the information available to terrorists to use in the implementation of their terrorist activities, to be created this new type of terrorism called cyber terrorism.

This research aims to identify the nature of the cyber terrorism, and investigate the causes and manifestations, and then identify ways to face it.

The research has come to the conclusion that cyber terrorism is an illegal activity using the International Network of Information applications, issued by states, groups or individuals to harm the physical and moral structures of a society or its institutions to achieve political goals. This make information as a weapon of this type of terrorism, which is getting more dangerous and deadly greater progress in the informational field, especially in the most advanced countries in the technical field. On the face of it, the states must take what could be a means to counter this electronic threat through a series of actions at the states level and the international community, and in terms of legislation, technical and legal preparations. God bless.

المقدمة

يمثل الإرهاب بجميع أشكاله تهديدا خطراً للأمن الوطني والدولي على حدٍ سواء ، نظراً لما له من آثار وخيمة على أمن المواطنين وإستقرارهم، وعلى الإمكانات الإقتصادية والهيبة السياسية للدولة في محيطيها الإقليمي والدولي. ومما زاد في مخاطر النشاط الإرهابي ، التطور الهائل في وسائل الاتصالات وثورة الانترنيت التي حولت العالم الى قرية صغيرة ، وجعلت المعلومات في متناول إرهابيين يستخدمونها سواء في تسهيل الاتصال بينهم أو تنسيق عملياتهم ، أو حتى بتوظيفها في تنفيذ أنشطة إرهابية من قبيل التجسس وتدمير الفعاليات الالكترونية للدول والمؤسسات وإبتكار أساليب وطرق إجرامية متقدمة ، لينشأ بذلك نمط جديد من الإرهاب يدعى الإرهاب الالكتروني .

أولاً: أهمية البحث

يستمد هذا البحث أهميته من خطورة موضوعه (الارهاب) وما يفرضه من تهديدات على الامن الوطني للعديد من دول العالم . مثلما يستمد أهميته كذلك من المكانة التي باتت تشغلها الشبكة الدولية للمعلومات في المنظور الاستراتيجي لهذه الدول بالنظر لإعتمادها المتزايد عليها في العديد من أنشطتها ، بصورة تجعل أي عمل ارهابي يطال هذه الشبكة ، يمكن أن يخلف دماراً كبيراً لاقتصاديات تلك الدول وأمنها الوطني وسيادتها الاقليمية . ومع ندرة الكتابات السياسية التي تصدت لهذا النوع الجديد من الإرهاب ، وما يمكن إتخاذه من إجراءات لمواجهة هذه التهديدات الارهابية لاسيما في بلد يعاني من خطر الإرهاب بأبشع صوره منذ وقت ليس بالقليل مثل العراق ، تظهر الحاجة العلمية لمعالجة هذا الموضوع وتحليل أبعاده .

ثانياً : مشكلة البحث وهدفه

بالنظر لما تشكله الشبكة الدولية للمعلومات من بيئة خصبة ومفتوحة لاستقطاب كل اشكال التفاعلات على الصعيد المعلوماتي السلمية وغير السلمية ، المشروعة وغير المشروعة ، مثلت هذه الشبكة بالمقابل ، بيئة مناسبة أيضاً لممارسة ونشر العمليات الإرهابية على اختلاف صوره والياته بصورة متسارعة ومتزايدة بالإفادة من التطور المتسارع في تقنيات المعلومات وفضاءاتها المفتوحة . ومن هنا تحددت إشكالية البحث في الكشف عن الطبيعة المتميزة لهذا الوجه الجديد من الارهاب الدولي ، وما يستخدمه من أساليب تقنية رقمية لتهديد أمن البلدان ومصالحها ، وما يمكن أن تتسلح به هذه البلدان من اجراءات وإستعدادات في مواجهة هذا التهديد الارهابي .

ثالثاً : منهجية البحث

يعتمد هذا البحث في تحليل معطياته وبلوغ اهدافه على إفتراضات منهج التحليل الوصفي في إستجلاء ملامح هذه الظاهرة وكشف مخاطرها على الامن الوطني ؛ مع الاستعانة الضمنية بالمنهج التأريخي في تقصي جذور وتطور هذه الظاهرة .

رابعاً : خطة البحث

ينقسم هذا البحث ، على ثلاثة مباحث ، ينصرف الأول منها الى التعريف بظاهرة الإرهاب الالكتروني وتحديد خصائصها وجذورها وأسبابها ، أما المبحث الثاني فيعالج أنواع هذا الإرهاب الالكتروني المباشرة وغير المباشرة ، وسبل مواجهة الإرهاب على الصعيدين التنظيمي والفني . ثم ينتهي البحث الى خاتمة تتضمن اهم ما توصل اليه الباحث من نتائج وتوصيات .. والله ولي التوفيق .

المبحث الأول : مفهوم الإرهاب الالكتروني

إن موضوع الإرهاب من اكثر الموضوعات إثارةً للجدل وتعدد وجهات النظر ، إذ احاط الخلاف بهذا الموضوع بشكل حاد حتى أننا لانكاد نسجل إتفاقاً حول أي جانب من جوانبه النظرية المتعلقة بتعريفه أو خصائصه لاسيما مع حداثة نشأته وتداخل أسبابه ضمن نطاق الحلقة الاوسع للإرهاب بوجه عام ، وهذا ما يستدعي معالجة هذا الموضوع عبر مطلبين ، يخصص الأول للتعريف بالإرهاب الالكتروني وبيان خصائصه ، ويتصدى المطلب الثاني جذور الإرهاب الالكتروني وأسبابه .

المطلب الأول : مفهوم الإرهاب الالكتروني وبيان خصائصه

سيتم في هذا المطلب التعريف اولاً بماهية الارهاب الالكتروني ، ثم التصدي في الفرع الثاني لبيان خصائصه .

الفرع الأول : مفهوم الارهاب الالكتروني

تجمع قواميس اللغة العربية على أن كلمة إرهاب تعني الفزع والخوف والرعب . وكلمة إرهاب مشتقة من الفعل المزيد (أرهب)؛ويقال أرهب فلانا: أي خوَّفه وفزَّعه، وهو نفس المعنى الذي يدل عليه الفعل المضعف (رَهّبَ). أما الفعل المجرد من نفس المادة وهو (رَهِبَ)، يَرْهبُ رَهْبَةً ورَهْبًا ورَهَبًا فيعني (خاف) مع تحرز واضطراب. فيقال رَهِبَ الشيء رهبا ورهبة أي خافه، وكذلك يستعمل الفعل ترهب بمعنى توعد إذا كان متعديا فيقال ترهب فلانا: أي توعده.[1] وأرهبه وإسترهبه أي اخافه وافزعه .[2]

واما بالنسبة للشق الثاني من العبارة ، ونقصد به (الكتروني) الْمَنْسُوبُ إِلَى الإِلِكْتُرُونِ وهي مفردة دخيلة على اللغة العربية ولاوجود لها في قواميس هذه اللغة ومعاجمها ، جرى تعريبها لمواكبة التطورات التقنية التي عاشها العالم في ظل عصر المعلومات ، بعد إنتشار إستخدام العَقْلُ الإِلِكْتُرُونِيُّ لتعني كُهَيْرِبِيّ [3]، بوصفها أَحَدُى مُكَوِّنَاتِ فِي ذَرَّاتِ الْمَادَّةِ .

ومع دخول الإرهاب على الفضاء الرقمي وشبكة المعلومات الدولية وتسخيره في خدمتها وتطوير فعالياتها نشأ مصطلح (الإرهاب الالكتروني) بعد أن جرى تداوله بصورة مكثفة في هذه الادبيات ليعكس تطوراً متنامياً في رصد ومتابعة هذا النوع الناشئ من الإرهاب في الفضاء الالكتروني . [4]

واما النظير الانكليزي لعبارة (الإرهاب الالكتروني) فهو (Cyber terrorism) ، كلمة مألوفة (Cyber) ومتداولة وتعني الفضاء الرقمي ، والكلمة الأخرى (Terrorism) وتعني الإرهاب .

وحول هذا المصطلح الجديد (الارهاب الالكتروني) تعددت التعاريف واختلفت ، وتباينت في شأنه الاجتهادات ، وأضحى هذا المفهوم يستعمل بمعانٍ ملتبسة ومضامين مختلفة . ويرجع ذلك إلى تنوع أشكاله ومظاهره ، وتعدد أساليبه وأنماطه، وإختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والأيديولوجيات التي تعتنقها الدول تجاهه، فما يراه البعض إرهاباً يراه الآخر عملاً مشروعاً. [5]

وكانت فاتحة هذا الاهتمام مع توقيع اتفاقية منع الإرهاب التي نظمت أيام عصبة الأمم المتحدة عام(1937)، إذ عرفت الإرهاب الدولي بأنه " أفعال إجرامية موجهة ضد دولة من الدول، ويقصد بها أو يراد منها خلق حالة من الرهبة في إذهان أشخاص معينين، أو مجموعة من الأشخاص أو الجمهور العام " [6] فتم في هذا التعريف تحديد الغاية دون توضيح السبب والوسيلة .

وقد عرفت الاتفاقية العربية لمكافحة الإرهاب ، في الفقرة الثانية من المادة الأولى منها ، الإرهاب بأنه : " كل فعل من أفعال العنف أو التهديد به، أيا كانت بواعثه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي يهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر" . [7]

الى جانب تلك المحاولات على المستويين الدولي والإقليمي بغية الوصول إلى تعريف موحد للإرهاب، ظهرت محاولات رجال القانون لتوصيف معالم الإرهاب وتعريفه ، ومنها تعريف الدكتور محمد عبد المنعم عبد الخالق للإرهاب بأنه " تلك الجريمة التي ترتكب ضد الاشخاص أو الاموال سواء داخل الدولة أو خارجها بإستخدام القنابل أو وسائل المفرقعات أو غيرها من الاسلحة أو المواد الناسفة بغية إثارة الرعب أو الفزع في نفوس المواطنين الامنين " [8]

فكان الخلط وضاحاً في هذا التعريف مع الجريمة بعد أن غاب البعد السياسي عن التعريف ، وهو الامر الذي تجاوزه الدكتور رجب عبد المنعم متولي في تعريفه الإرهاب على أنه (فعل من أفعال القوة أو العنف قصد به الإرهاب أو التخويف أو ممارسة الضغط على السلطة أو جهة معينة بقصد فرض فكر معين عليها وأياً كان الهدف الذي تصيبه مدنياً كان أم عسكرياً وبطريقة عشوائية)[9].

وبالإنتقال الى مصطلح" الإرهاب الإلكتروني" الذي ظهر حديثاً في مجال الاهتمام الدولي عقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات وإستخدامات الحواسب الآلية ، والإنترنت تحديداً ، في إدارة معظم الأنشطة الحياتية، وكان ذلك في دراسة قدمها (كولين باري) - الباحث في معهد الأمن والاستخبارات في ولاية كاليفورنيا - في عام 1997 ، أشار فيها الى " ان ديناميكية الاعمال الإرهابية ستفضي في مراحل لاحقة الى تصاعد وتيرتها بل وحتى انتقالها من العالم المادي إلى العالم الافتراضي ، ليكون الإرهاب الالكتروني هو نقطة التقاء العالمين"[10] ، وقد عرف هذا النوع من الإرهاب على أنه ((عمل إجرامي يرتكب عن طريق إستخدام أجهزة الكمبيوتر ويؤدي إلى تدمير أو انقطاع الخدمات الإلكترونية ليخلق الخوف ضمن مجموعة سكانية معينة بهدف التأثير على الحكومة أو السكان لتنفيذ اجندة سياسية أو إجتماعية))[11] .

وجاء الاعتراف والتعريف الرسمي بالإرهاب الالكتروني من قبل منظمة الامم المتحدة في تشرين الأول/ أكتوبر 2012 حينما عرفته على أنه "إستخدام الانترنت لنشر أعمال إرهابية". فجاء هذا التعريف هلامياً بابعاده غامضاً بمقصده ، فلا يكشف عن طبيعة هذه الاعمال الارهابية ولا عن مغزاها ولا حتى المستهدفين بها . وضمن نفس السياق جاء تعريف الموسوعة الالكترونية للإرهاب الالكتروني بأنه " إستخدام التقنيات الرقمية لإخافة وإخضاع الآخرين. أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية". فتحرى هذا التعريف عن الدوافع لكنه توسع في المدى الذي تشمله هذه الهجمات ؛ كون التقنيات الرقمية تشمل الحاسوب وغيره مثلما هي نظم المعلومات دون ان تكون الدولة طرفاً ضمن هذا المحتوى التوصيفي للارهاب.

ووفقاً لمكتب التحقيقات الفيدرالي، فان الإرهاب الإلكتروني هو " هجمات ذات دوافع سياسية مبيتة ضد المعلومات، وأنظمة الكمبيوتر وبرامجه وبياناته ،لإحداث أضرار ضد أهداف غير قتالية من قبل جماعات شبه قومية أو عملاء سريون".[12] وكان وصف الهجمات مدخلاً مفتوح المضامين ، اذ يشمل الارهاب والحرب الالكترونية على حد سواء .

وضمن السياق ذاته ، صاغ مركز الدراسات الاستراتيجية والدولية (CSIS) تعريفاً للإرهاب الالكتروني بأنه "إستخدام أدوات شبكة الكمبيوتر لإغلاق البنى التحتية الوطنية الهامة (على سبيل المثال، والطاقة، والنقل، والعمليات الحكومية) أو لإكراه أو ترهيب حكومة أو المدنيين السكان."[13] والملاحظ على هذا التعريف ولوجه غير المتوازن في التفاصيل مع إغفاله للدافع السياسي واقصاءه لصور اخرى من الارهاب الرقمي مجالها التجسس والتدمير لنظم المعلومات .

وكان التعريف الأكثر إنتشاراً للإرهاب الالكتروني ذلك الذي تقدم به البروفيسور دوروثي اي. دينينغ - مدير معهد جورج تاون لأمن المعلومات في الولايات المتحدة -الذي وجد فيه الإرهاب الالكتروني :" الهجمات والتهديدات للهجوم غير المشروعة ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها بقصد تخويف أو إجبار حكومة ما أو شعبها تحقيقاً لأهداف سياسية أو إجتماعية".[14]

وبالإنتقال الى الضفة الاكاديمية العربية ، نجد أن د.هشام بشير- المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الإنترنت- قد عرف مفهوم "الإرهاب الإلكتروني" بأنه 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، بإستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان" [15] والمستخلص من هذا التعريف مزجه بين الارهاب والعدوان على الرغم من مجال الافتراق الواضح بين لمفهومين ، ناهيك عن استبعاد التعريف لجانب الشروع والقيام الفعلي بالنشاط الارهابي ضد الاهداف المقصودة منه بسبب اكتفاءه بجانب التهديد .

كما عرف الدكتور حسين بن سعيد الغافري هذا النوع من الإرهاب على أنه "هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو إجتماعية معينة". ومن ثم فلكي ينعت شخصا ما بأنه إرهابياً على الإنترنت، وليس فقط مخترقاً، فلا بد وأن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب". فالإرهاب الإلكتروني يعتمد على إستخدام الإمكانيات العلمية والتقنية، وإستغلال وسائل الإتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم"[16].

والإرهاب الالكتروني كما يراه الدكتور مصطفى محمد موسى هو قيام شخص أو مجموعة اشخاص منضمين لتنظيم أو غير منظمين بإستخدام التقنية الالكترونية الرقمية وشبكاتها بصورة مخالفة للقانون لتحقيق اغراض مختلفة " [17]

ومما تقدم يمكن الخروج بتعريف للإرهاب الالكتروني بأنه "هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو إبتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو إجتماعية معينة ".

الفرع الثاني : خصائص الإرهاب الإلكتروني

مما لا شك فيه أن الإرهاب الإلكتروني ينفرد بعدد من الخصائص التي يختص بها دون سواه، ويتميز بها عن العديد من الظواهر الإجرامية الأخرى، وتحول دون اختلاطه بالإرهاب العادي، ومن الممكن إيجاز أهم تلك الخصائص والسمات فيما يأتي :

1. إرهاب تقني معلوماتي لا يتسم بالعنف ولا يلجأ الى القوة ، بل يتحقق عبر الوسائل الناعمة للتأثير والتدمير، فهو إذن لا يحتاج الى القوة الجسمانية لمرتكبه بل يحتاج الى القوة المعرفية له. وتبعا لذلك فهو إرهاب اكثر عرضة للتطور والتنوع في وسائله واثاره ، لاعتماده المطلق على المعلومات والتقنيات الرقمية التي تمثل لغة العصر ومجال التغيير الاساس فيه [18].
2. ان هذا النوع من الإرهاب وخلافا لسائر انواع الإرهاب يمكن أن يشن من قبل فرد واحد ودون معونة من غيره ، شريطة أن يكون هذا الفرد من ذوي الاختصاص والمعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.
3. لا بد ان يؤدي الى ايقاع الرعب لدى الناس ولو على سبيل الاحتمال ويكون هدفه تعريض امن المجتمع للخطر أو الاخلال بالنظام العام .[19]
4. يتسم بقدرته على تجاوز الزمان والمكان ، إذ يعد جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود ، كما لا يمكن تحديد زمن الشروع فيها ، أو حتى حصر إمتدادات تأثيراتها المستقبلية . [20]
5. إن الإرهاب الإلكتروني لا يترك أيّ دليل مادي بعد إرتكاب جرائمه وهذا ما يصعب عملية التعقب وإكتشاف الجريمة أساساً ؛ فهو محاط بهالة من الغموض والتضليل من جانب مرتكبيه ؛ فلا يترك أثراً خلفه ، أو حتى تحديد حجم الضرر ، نظراً لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره ، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم. [21]

المطلب الثاني : جذور الإرهاب الالكتروني وأسبابه

تمتد جذور الاهاب بكل صوره عميقاً في تأريخ الحضارات والشعوب ، فهو مرتبط بالإنسان ونزعاته غير المشروعة . وعلى امتداد هذه الرحلة التأريخية الطويلة للإرهاب ، لم يكن الإرهاب الالكتروني إلا صورة حديثة النشأة من صور ذلك الإرهاب التقليدي ، فكان هذا الشكل الجديد للإرهاب، تتويجاً واستكمالاً لتلك السلسلة من الظروف والاسباب والخبرات التاريخية التي مر بها واكتسبها ذلك النوع المخضرم من الارهاب ، ليكتسب بتفاعله وأفادته من التطورات التقنية زخماً ودماراً مضاعفاً. وعلى أساس ما تقدم سيتم تقسيم هذا المطلب على فرعين ، يتتبع الاول الجذور التاريخية للإرهاب الالكتروني ، ويتفحص الثاني أسباب هذه الظاهرة بشكليها التقليدي والمعاصر .

الفرع الأول : جذور الإرهاب الالكتروني

مع تطور إستخدام الحاسبة الالكترونية وظهور الشبكة الدولية للمعلومات ، إزدادت قدرة الإرهاب على التأثير والتدمير عما كانت عليه في الماضي، إذ وجد الإرهابيون فيه مرتعاً خصباً لتحقيق أغراضهم بوسائل متطورة ومتنوعة وبعيداً عن الرقابة والملاحقة .

ومنذ أن شهدت الشبكة الدولية للمعلومات في عام 1989 ، أول الاختراقات الالكترونية على شكل مغامرة فردية ، أقدم عليها بعض الاشخاص لدوافع غير سياسية وتحت مضلة ما ظهر حديثاً وسمي آنذاك بـ(القرصنة) [22] بتطويرهم برنامج قائم بذاته قادر على نشر نسخ الوظيفة نفسها أو شرائح لأنظمة الكمبيوتر الخاصة بهم والتي انتشرت في العديد من أجهزة الكمبيوتر للمستخدمين على الشبكة [23] .

وكانت البداية المؤشرة كنقطة شروع للتنظيمات الإرهابية في الفضاء الرقمي في بريطانيا منتصف التسعينيات من القرن السابق ، إذ كشفت تقارير بريطانية عن تطوير الجيش الجمهوري الايرلندي لنظام معلوماتي معقد تمكن من الوصول إلى ملفات عملاء شركة الهاتف البريطانية والسجلات الصحية لعملاء أحد أكبر المؤسسات الصحية الخاصة في بريطانيا إضافة إلى ملفات عملاء شركة توماس كوك.

وقد سجل العام1996 البداية الحقيقية والشرسة للهجمات الإرهابية الالكترونية المنظمة على الشبكة الدولية للمعلومات ، حينما نفذت حركة البيض العنصرية المتطرفة في الولايات المتحدة هجوما الكترونيا لتعطيل وإتلاف جزءٍ من نظام حفظ السجلات (ISP) الخاص بولاية ماساتشوستس ، وبعد إنتهاء الهجوم ترك المهاجمون الرسالة الأولى التي ورد فيها إصطلاح الإرهاب الالكتروني في تأريخ الشبكة الدولية للمعلومات مؤكدين فيها : " إذا كنت لا تعرف الإرهاب الالكتروني الحقيقي ، فوعد منا بأن نجعلك تراه ".[24]

ومنذ ديسمبر 1997 دخلت الشبكة الدولية للمعلومات بقوة على خط المواجهة الشعبية مع الحكومات ، لتسجل منعرجا تأريخياً مهماً في سياق تطور الإرهاب الالكتروني ، وذلك حينما عمد الاف المحتجين الأمريكيين بتنفيذ اعتصام الكتروني ضد المواقع المؤيدة لحركة زاباتيستا في تشياباس المتمردة في المكسيك ، وذلك بالدخول بتوقيت واحد وبإستخدام برنامج خاص لتوجيه سيل

من طلبات التحميل السريع والمتكرر على تلك المواقع ، الأمر الذي تسبب بتعطيلها عن الخدمة . وتكررت هذه الالية في الهجوم الالكتروني من قبل جماعات حقوق الحيوان إحتجاجاً على الاساءة للحيوانات .

وقد إمتد نطاق هذه الاحتجاجات والهجومات الالكترونية على الشبكة الدولية للمعلومات من النطاق الوطني والمحلي الى نطاق دولي عابر للدول، حينما نفذت مجموعة من ناشطي الشبكة عملية اعتصام الكتروني بطريقة القصف الالكتروني ضد منظمة التجارة العالمية اثناء مؤتمرها المنعقد في سياتل أواخر عام 1999 ؛ وبذلك اكتسبت امثال تلك الهجومات الالكترونية بعدا عالميا بعد ان تجاوزت حدودها المحلية ، مؤشرة بذلك تقدما اخر في مسار الإرهاب الالكتروني عبر التوسع والامتداد في النطاق المكاني لها.[25]

ومثلما لم تتقيد العمليات الإرهابية الالكترونية بنطاقها المكاني والزماني ، فإنها قد تنوعت كذلك بوسائلها وأساليب هجماتها الالكترونية ، معبرة بذلك عن التطور الذي تمر به تقنية المعلومات وميدانه الامثل (الشبكة الدولية للمعلومات) ، ففي مارس 2000، ذكرت إدارة شرطة العاصمة اليابانية أن برنامجا استخدمته طائفة أوم Shinryko الإرهابية [26] لتتبع 150 سياراتها في العاصمة طوكيو. علاوة على ذلك، قامت هذه الطائفة بتجنيد وكلاء سريين لاختراق برامج ما لا يقل عن 80 شركات يابانية و 10 وكالات حكومية. بغية تدميرها أو التجسس عليها .[27]

في مواجهة التنامي الملحوظ في الأنشطة الإرهابية بإستخدام الشبكة الدولية للمعلومات ، تنبه الغرب الى خطورة هذه الظاهرة وتحدياتها المتفاقمة ، فبادرت الولايات المتحدة في أثناء مدة حكم الرئيس الأمريكي بيل كلينتون في العام 1996 بتشكيل لجنة حماية منشآت البنية التحتية الحساسة من خطر العمليات الإرهابية الالكترونية.

وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة بإنشاء هيئاتها ومراكزها الخاصة للتعامل مع احتمالات الإرهاب الإلكتروني، فقامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفاً من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني.[28]

ولم يكن أمر الهجمات الالكترونية الإرهابية والاحتجاجية حكراً على عالم الشمال، بل إمتد نطاقه مع إمتداد نطاق خدمات الشبكة الدولية للمعلومات الى عالم الجنوب ، عندما وقع الهجوم الإرهابي الالكتروني على السفارات السريلانكية عام 1998، وإستند الهجوم على محاكاة الإسلوب ذاته في إرسال الاف الرسائل الالكترونية الى الموقع الالكتروني لهذه السفارات بهدف إيقافه الذي إستمر لمدة أسبوعين وكان فحوى الرسالة هو "نحن اسود ونمور الإنترنت، ونحن نفعل ذلك لقطع الاتصالات الخاصة بك" [29]

وقد ظهر أوضح إرتباط بين الشبكة الدولية للمعلومات والإرهاب ، بعد أحداث الحادي عشر من سبتمبر 2001 الإرهابية في نيويورك ، إذ إجاد تنظيم القاعدة في توظيف تطبيقات الشبكة الدولية للمعلومات في تهيئة أسباب الدعم والتحضير لإنجاح هذه العملية ، بعد أن اتخذها مقراً عاماً افتراضياً للقيام بـ (الإعلام وبث الدعايات المثيرة والأخبار والأفلام عن العمليات الإرهابية التي تقع على أرض الواقع والتثقيف) [30] بتوفير المعلومات الهادفة الى تلقين المرشحين للتدريب على القتال في المدن وإستخدام الاسلحة المختلفة فيها .[31] وهكذا إتسع نطاق المواجهة ضد الإرهاب والإرهابيين ليشمل الى جانب المواجهة المادية المباشرة في الميادين ، المواجهة الإلكترونية في خضم حروب رقمية ؛ فأصبح الإنترنت من أشد ساحات المواجهة سخونة بين الطرفين بعد ان انتهت العمليات الحربية في افغانستان والعراق بعد عام 2003 ، وتنوعت الأسلحة الإلكترونية والمواجهات مع كل تطور تشهده ثورة المعلومات حتى يومنا هذا.

وإتفق الخبراء أن عام 2004 كان العام الأكثر إغراقا للشبكة الدولية للمعلومات بالفيروسات المختلقة والبرامج المفجرة، وفيه أيضاً زادت الرسائل الإلكترونية المزعجة بنسبة 40 في المائة ، هذا الى جانب إستخدام التسهيلات التي تقدمها الشبكة الدولية في تنفيذ العمليات الإرهابية العنيفة في الواقع مثل ما حصل في الهجمات الإرهابية في مومباي (الهند)، عام 2008 ،إذ إستخدمت الهواتف التي تعمل بالأقمار الصناعية وشبكة الانترنت لتحديد المواقع المستهدفة والتثبت من إنجاز الأهداف وإيصال المعلومات الى الفاعلين[32].

الفرع الثاني : أسباب الإرهاب الالكتروني

لا ينكر ان ثمة تنوعاً في أسباب ظاهرة الإرهاب ، مرده تباين الظروف السياسية والإقتصادية والإجتماعية لكل مجتمع تنشأ فيه هذه الظاهرة ، وتباين المواقف منها ؛ فضلاً عن التطورات التي لحقت بهذه الظاهرة من جراء توظيفها للفضاء الالكتروني ، حتى ظهر طيف اخر من الأسباب الخاصة بالشكل الجديد من الإرهاب الالكتروني .

وعلى اساس ما تقدم ، تم تقسيم البحث في أسباب الإرهاب الالكتروني على فرعين ، يتناول الفرع الأول الأسباب العامة لظاهرة الإرهاب ، وفي الفرع الثاني تم تناول الأسباب ذات الطبيعة الفنية الخاصة بظاهرة الإرهاب الالكتروني .

أولاً : الأسباب العامة للإرهاب الالكتروني

1- الأسباب السياسية :

يعد الدافع السياسي من أهم الدوافع المحفزة للإرهاب ، إذ تلجأ الجماعات والأفراد الى العنف لتحقيق اهداف سياسية معينة منها :

أ- التطلع الى السلطة والتنافس للإستحواذ عليها عبر إستغلال العمليات الإرهابية لتهديد وجود القائمين عليها وزعزعة إستقرار وأمن البلاد في سبيل إنهاء التأييد الشعبي وتفتيت الأساس الشرعي لبقاء النظام الحاكم .

ب- محاولة فرض مذهب أو رؤية سياسية أو عقائدية معينة أو إقامة كيان سياسي .

ت- السياسات الاستبدادية التي تنتهجها بعض الدول ضد مواطنيها، المؤدية الى حالة من الاستياء والنقمة الشعبية التي تترجم الى عمليات وتنظيمات إرهابية تستخدم العنف خارج نطاق الشرعية كرد فعل على ممارسات النظام القمعي ووسيلة للضغط عليه بهدف اجباره على الاستجابة لها.[33]

ث- الاضطهاد الديني والطائفي والقومي من قبل مكون ضد آخر داخل الدولة .

ج- دلت الوقائع على أن النزاعات القائمة بين دولتين غالباً ما تؤدي الى تبادل العمليات الإرهابية ودعم التنظيمات الإرهابية بينهما بشكل سري أو مكشوف.

ح- سياسات الهيمنة وإستخدام القوة والتدخل السافر التي تنتهجها بعض الدول الكبرى على صعيد علاقاتها مع الدول الاخرى .[34]

2- الأسباب الإقتصادية

بالنظر لدور الإقتصاد المحوري في الحياة الدولية كونه القوة الأساسية في تحديد أنماط التفاعلات ، وتوزيع مراكز القوة والتأثير على الخارطة الدولية ، فانه لا يمكن تجأوز ما لهذا الاخير من دور آخر في تقديم تفسيرات موازية لظاهرة الإرهاب على تخوم الظلم الذي يخلقه التفأوت في توزيع الموارد والقدرات الإقتصادية بين الدول والتي يمكن إيجازها بالآتي: [35]

أ- معاناة الأفراد من المشكلات الإقتصادية المتعلقة بالفقر وغلاء المعيشة والتضخم في أسعار المواد الغذائية والخدمات الأساسية ، كل ذلك من العوامل المؤثرة في إنشاء روح التذمر في الأمة، وربما دفعت بعض الشباب إلى التطرف والإرهاب كنوع من التمرد على الواقع أو محاولة إسترداد الحقوق الإقتصادية المسلوبة بإستخدام الوسائل الإرهابية

ب- انتشار البطالة في المجتمع وزيادة العاطلين عن العمل وعدم توفر فرص العمل، من أقوى العوامل المساهمة في إمتهان الجريمة والاعتداء والسرقة وتفشي ظاهرة الإرهاب.[36]

ت- التطور اللاّمتكافئ بين الدول المتقدمة والدول التي تسعى إلى النمو، ما ادى إلى تنامي حالة النقمة والاستياء المعبر عنه بسياسات واعمال إرهابية تعبر عن حالة الرفض لهذا النظام الإقتصادي الدولي ومخلفاته في التبعية واتساع البون الإقتصادي بين تلك الدول وبين الدول المتقدمة .[37]

3- الأسباب الإجتماعية والنفسية

أ- تؤدي التركيبة الذاتية للفرد دوراً كبيراً في إتجاهه نحو العمل الإرهابي فمن يملك غريزة عدوانية يكون أقرب الى ممارسة العمل الإرهابي لاسيما إذا كان ذلك الفرد محاطاً بظروف حياتية معقدة فمن الممكن أن يتم الاستفادة منهم لخدمة المجتمع بدلاً من الاضرار به عبر سلوكيات مرفوضة إجتماعياً .[38]

ب- التفكك الأسري والإجتماعي، مما يؤدي إلى إنتشار الأمراض النفسية والإنحراف والإجرام والإرهاب.

ت- فقدان الهوية المجتمعية والفشل العميق في منظومة واليات التربية والتعليم بكل مستوياته في المجتمع ؛ وشيوع حالة التشدد والغلو في الفكر، وغياب لغة الحوار بين أفراده وأطيافه تعد أسبابا اخرى لتفشي ظاهرة الإرهاب.[39]

ث- هناك نوع من الصلة بين إرتفاع الكثافة السكانية وتفشي ظواهر العنف والجريمة والفوضى الداخلية ، مثلما يساعد على ارتفاع معدلات العنف والجريمة الإرهابية تفاقم النزاعات الاهلية وغياب الاستقرار الإجتماعي .[40]

ج- الإحباط وافتقاد الشخص لأهمية دوره في الأسرة والمجتمع، وفشله في الحياة الأسرية: يمارس دورا اساسيا في مرحلتي المراهقة والرشد في ابراز السلوك الإرهابي الى العلن.[41]

ثانياً : الأسباب الخاصة :

ويمكن تشخيص هذه الأسباب بالاتي : -

1- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق:

إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها؛42 رغبة في التوسع وتسهيل دخول المستخدمين، وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية، يمكن للمنظمات الإرهابية استغلالها في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية ، أو التجسس على المعلومات السرية التي تمس امن الدول والهيئات المختلفة .

2- غياب الحدود الجغرافية وتدني مستوى المخاطرة:

إن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعدُّ فرصة مناسبة للإرهابيين، إذ يستطيع محترف الحاسوب أن يقدِّم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية، ومن ثم يشن هجومه الإلكتروني وهو مسترخٍ في منزله من دون جهدٍ أو عناء ، وبعيداً عن أعين الناظرين .[43].

3- سهولة الإستخدام وقلة التكلفة:

إن السمة العولمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الإستخدام، طيعة الإنقياد، قليلة الكلفة، لا تستغرق وقتاً ولا جهداً كبيراً، مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة بأقصى سرعة وأعمق أثراً ، ومن دون الحاجة إلى مصادر تمويل ضخمة ؛ فالقيام بشن هجومٍ إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة. [44] .

4- الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية :
إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والإرهاب الإلكتروني يعد من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني، وحتى لو وجدت قوانين تجريمية متكاملة فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق .

المبحث الثاني : صور الإرهاب الإلكتروني وسبل مواجهته

من الصعوبة بمكان حصر وتحديد جميع أشكال الإرهاب؛ نظراً لتنوع مصادره وتطور وسائله وإنفتاح حدوده عبر الشبكة الالكترونية وصعوبة اخضاعه للمراقبة ، والاصعب من ذلك محاولة التصدي الفاعل له . وإعتماداً على هذا المدخل سيتم تقسيم هذا المبحث بين مطلبين ، يكون الاول لتصنيف صور الارهاب ، وأما الثاني فمجاله البحث عن وسائل مواجهته .

الفرع الأول : صور الإرهاب الالكتروني :

يمكن تقسيمها بحسب الوسائل المستخدمة على نوعين احدهما مباشر والاخر غير مباشر .

اولاً: الإستخدام المباشر لشبكة المعلومات في الأنشطة الإرهابية

1- التهديد الإلكتروني

يقصد بالتهديد ، الوعيد بشر، وزرع الخوف في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أن ضرراً ما سيلحقه أو سيلحق أشخاصاً أو أشياء له بها صلة .

وفي هذا المجال تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات، وعبر الشبكة العالمية للمعلومات (Internet) . ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني ، إرسال الرسائل الإلكترونية المتضمنة التهديد (E-mails)، وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية.

ومن أمثلة التهديد الإلكتروني "ما قام به شاب أمريكي يدعى "جاهابر جويل" ، حين هدد كل من مدير شركة "مايكروسوفت"(ج) والمدير التنفيذي لشركة M.P.I بنسف شركتيهما إذا لم يتم دفع خمسة ملايين دولار، وقد قامت الشركة بتفتيش منزل المذكور بعد القبض عليه وعثروا في حاسبه الآلي على عدة ملفات رقمية تحتوي على معلومات عن تصنيع القنابل تم إنزالها عبر الإنترنت.

2- القصف الإلكتروني

هو إسلوب تلجأ له المنظمات الإرهابية للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات مما يزيد الضغط على قدرتها على إستقبال رسائل من المتعاملين معها والذي يؤدي إلى وقف عمل الشركة أو الحرمان من الخدمات التي تقدمها بإستخدام الانترنت [45].

وكمثال على المواقع التي تعرضت للقصف الإلكتروني موقع " شركة أمازون" لبيع الكتب على الإنترنت وأيضا شركة "سي ان ان " للأخبار على الإنترنت ، ما أدى إلى بطء تدفق المعلومات لمدة ساعتين.[46]

3- تدمير أنظمة المعلومات

يقصد بهذا المفهوم محاولة اختراق تقوم بها التنظيمات الإرهابية عبر شبكة المعلومات الخاصة بالأفراد أو المؤسسات العامة العسكرية منها أو المدنية فضلاً عن الشركات الخاصة بهدف تخريب نقطة الاتصال أو النظام عن طريق تخليق أنواع من الفيروسات الجديدة التي تسبب ضررا كبيرا لأجهزة الكمبيوتر والمعلومات التي تم تخزينها على هذه الأجهزة.

وتعدُّ (الفيروسات أو الديدان)[47] من أخطر الاسلحة التي تستخدمها المجاميع الإرهابية في شن هجوماتها الالكترونية على تلك المواقع ونظم معلوماتها الى جانب انواع اخرى من الانظمة الفيروسية من امثال (حصان طروادة ، والقنابل المنطقية) [48]؛ حتى اضحت هذه الفيروسات من أخطر آفات شبكات المعلومات بالنظر الى ما تمتلكه من خصائص ذاتية وقدرات تدميرية لأنظمة المعلومات ؛ إذ تشير بعض الدراسات العلمية الى وجود اكثر من (000 60) فيروس في العالم الرقمي ، وعدد منها لها القدرة على التكيف والتحول من شكل الى آخر والانتشار [49].

وقد تسارع معدل خلق الفيروسات في السنوات القليلة الماضية، بمعدل وصل الى ما يقرب من 250 فيروس جديد شهريا ؛ [50] الأمر الذي يتسبب بخسائر مادية تصل قيمتها لنحو(6.5) مليار دولار يوميا.[51]ويكفي للتدليل على كلفة ومقدار هذا الدمار الإرهابي عبر شبكة المعلومات ، حساب ما خلفته ثلاث فيروسات فقط من أضرار إقتصادية وصلت الى (5) مليار دولار أمريكي ، بمعدل خسائر يومي يصل الى ما قيمته 6.5 مليار دولارعلى صعيد المعاملات التي تجري بإستخدام الشبكة الدولية للمعلومات [52].

إن مثل هذا الاحتمال يظل قائماً إذا ما دخلت على خط المواجهة والإرهاب الالكتروني دول ومنظمات إرهابية بإمكانيات واسعة أو شهدت مثل هذه البرامجيات تطورات نوعية تحقق تلك الأغراض الإرهابية في هذا الميدان بالمستوى الذي تخشاه الدول المتقدمة على أمنها الوطني ، والمثل على هذا الإحتمال ينهض من الفيروسات (ستكسنت ولهب) التي طورتها الولايات المتحدة واسرائيل للنيل من البرنامج النووي الايراني وتعطيله عن طريق تعديل سيطرتهم الإشرافية وأنظمة الحصول على البيانات (SCADA)، دون أن يكتشف ذلك الأمر لوقت طويل نسبي بهدف تأخير البرنامج النووي الإيراني لعدة أسابيع. وهو الأمر الذي ينطبق على وصف إرهاب الدولة طالما كان هذا العمل غير مشروع ولتحقيق اغراض سياسية دون ان تعلن حالة الحرب بين هذه الدول [53].

ثانياً: الإستخدام غير المباشر لشبكة المعلومات في الأنشطة الإرهابية

إذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً بالنسبة للإرهابيين، فإن إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات (Internet) ، لخدمة أهدافهم وترويج أفكارهم وكسب المؤيدين والانصار لهم ، أصبح أمراً سهلاً وممكناً. لذا حرصت معظم التنظيمات الإرهابية على تأسيس المواقع الالكترونية الخاصة بها ، لتكون بمثابة المقر الافتراضي لها الذي تباشر عبره كل عملياتها وأنشطتها بإستخدام الامكانات والتسهيلات التي تتيحها الشبكة الدولية للمعلومات في تأمين الإسناد اللوجستي والدعم المعنوي حتى من دون الحاجة الى إستخدام هذه الأخيرة في إختراق أو شن هجمات الكترونية على المواقع الالكترونية للجهات المستهدفة.[54] ومن أهم العناصر المستخدمة لتحقيق هذا الغرض ما يأتي :-

1- الاتصالات واعطاء التعليمات

تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الإتصال ببعضها البعض والتنسيق فيما بينها، وذلك نظراً لسرعة وقلة تكاليف الاتصال بإستخدام الانترنت، مقارنةً بالوسائل الأخرى، ناهيك عن درجة السرية والامان التي توفرها هذه الوسيلة لمستخدمها بالإبقاء على سرية هويته الشخصية ، من أمثلتها إستخدام الرموز أو الكلام المشفر كما فعل أعضاء تنظيم القاعدة في مراسلاتهم الالكترونية عند التحضير لشن هجماتهم على أبراج التجارة والبنتاغون عام 2001 بإستخدام كلمات وعبارات تتعلق بحوار بين طالب واستاذ لأمر يخص الدراسة والعلم [55].

وقد يقوم الإرهابيون بالاتصال ببعضهم عبر منتديات الالعاب الالكترونية ، وبعض الأحيان يستخدمون الدردشة على الهواء في مواقع الالعاب الالكترونية اليابانية التي لايتنصت عليها الا المراهقون .[56]

2- الدعاية وتجنيد إرهابيين جدد

إن إستقدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها وإستمرارها في سعيها لتحقيق أهدافها ؛ فكانت الشبكة الدولية للمعلومات ضمن هذا المسار من الوسائل الحديثة الأكثر فاعلية في بلوغ الاهداف الأيديولوجية بإعتماد وسائل الدعاية الالكترونية التي يوفرها الانترنيت عبر تطبيقاته المختلفة ، ليس فقط في الترويج والتبرير لتصوراتهم وانشطتهم الإرهابية ، أو في ترويض الإذهان لتقبلها وتنمية نوازع التطرف لدى من لديه الاستعداد لذلك من الانصار وغيرهم، مما يسمح بخلق بيئة افتراضية معزولة وآمنة لخلق ما يسمى بظاهرة الذئاب المنفردة في كل انحاء العالم عبر ما يبث من صور وفعاليات على الشبكة ، فتكون الشبكة الالكترونية الوسيلة الاكثر خطورةً وسهولة لكسب التأييد والتجنيد للأنصار دون حتى الاقتراب المادي منهم ، عبر كتيبات التعليمات وأشرطة الفيديو والمجلات والمنتديات التفاعلية والخطب المتطرفة والرسائل والخطب العاطفية والحماسية المؤثرة والموجهة للألاف الاشخاص من المهتمين بالانضمام إلى تلك التنظيمات [57].

وهذا ما كشفت عنه وأكدته محاضر إستجواب المحتجزين في خليج غوانتانامو الذين وقعوا ضحية لعملية غسيل دماغ شامل بفضل تلك المواقع الالكترونية وما تروجه من أفكار ودعايات [58].

3- الحصول على التمويل

تقدم الشبكة الدولية للمعلومات فرصاً غير محدودة للتنظيمات الإرهابية في الحصول على التمويل اللازم لإدامة أنشطتها الإرهابية عبر منافذ وطرق متنوعة وتحت عناوين وهمية ، ومن أمثلتها القيام بإحصاءات سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة عبر الاستفسارات والإستطلاعات الموجودة على المواقع الإلكترونية، في التعرف على الأشخاص ذوي القلوب الرحيمة ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين، يمثلون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة البريد الالكتروني بطريقة ماكرة لا يشك فيها المتبرع بأنه يساعد إحدى المنظمات الإرهابية. [59] . هذا الى جانب عمليات الاختراق والسطو الالكتروني الذي تنفذه هذه التنظيمات على المواقع الالكترونية لبعض الشركات والمصارف للاستيلاء على المزيد من الاموال . وبذلك تحقق هذه التنظيمات عدة مقاصد في وقت واحد أولها الحصول على التمويل اللازم لعملياتها ، وثانيها اضعاف تلك القوى واستنزافها إقتصاديا في سياق مخططاتها الإرهابية ، وآخرها توجيه رسالة تتضمن معاني القدرة الالكترونية المتاحة لتلك التنظيمات لردع وإرهاب خصومها ودحرهم معنوياً [60].

المطلب الثاني: مواجهة الإرهاب الالكتروني

ليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماما دون حصول هذه الاختراقات الإرهابية لشبكة المعلومات الدولية ، فالمتغيرات التقنية، وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open source)، سواء كان ذلك في مكونات نقطة الاتصال أو في النظم أو في الشبكة أو في البرمجة، جعلت الحيلولة دون الإختراقات صعبة جداً، بالإضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها إحداث الاختراق وتدمير المواقع . [61].

وما دمنا سلمنا بالتطور المستمر بأدوات الإرهاب الالكتروني وإتساع نطاقه ، بالشكل الذي يؤكد وجود حالة من حرب المعلومات المستمرة بين الإرهابيين، وأجهزة الدولة المختلفة وبخاصة الاجهزة الامنية فيها ، فمن المهم إذن مجابهة المعرفة بمزيد من المعرفة والتنسيق المسبق بين الاجهزة المعنية بتوفير الامن .[62]

وقبل الشروع بالمواجهة المنشودة ، تنبع الحاجة الماسة لإشاعة الوعي بخطورة هذه الظاهرة وتداعياتها ، والسبل الممكنة والمتوافرة لمواجهتها على الصعيدين الرسمي والشعبي ، مقترنة بمسعى جاد لإشاعة المعرفة الالكترونية بين أفراد الشعب في

سبيل التصدي لهذا الشكل من الإرهاب . فإذا كان أمن المعلومات يمثل صناعة متطورة ، وجب تدريب الأفراد وتوعيتهم بمستلزماته بإستخدام مجموعة متنوعة من المناهج العلمية المتطورة لمواكبة هذا التطور وتحقيق التوازن معه [63].

صفوة القول ، فان وسائل المكافحة ينبغي ان تتنوع ويتفاوت تأثيرها بدرجات تتوقف على نوع الهيئة الإجتماعية التي تمارس الضبط وكذا نوع الوسيلة المستعملة ونوع الإرهاب المطلوب مجابهته ؛ على ان تبدأ هذه العملية بالاستعداد الجيد سواء من حيث إعداد الكفاءات البشريّة المؤهلة، وإنشاء الوحدات المتخصصة للتحقيق في جرائم الحاسب، والإنترنت، ويترافق مع هذا ضرورة توفير الموارد الماليّة اللازمة لهذه الوحدات التي ترصد، وتضبط الظواهر الإجرامية التي تتسم بالتغيّر، والسرعة . ومن هذه المنطلقات يمكن تحديد اهم الوسائل الممكن اتباعها في مكافحة الإرهاب الالكتروني :

الفرع الأول : التدابير السياسية والتنظيمية لمواجهة الإرهاب الالكتروني

تتطلب المواجهة مع الإرهاب بوجه عام والإرهاب الالكتروني بوجه خاص حزمة من التدابير القانونية والتنظيمية ، يمكن تشخيصها وفق السياق الاتي : -

اولاً: التنضيد السياسي للإرهاب الالكتروني

إذا كان ما يميز الإرهاب بشكل عام عن غيره من صور الجريمة المنظمة ، يقع في دائرة السعي لتحقيق أغراض سياسية – بقطع النظر عن مشروعيتها - فان الخطوة الأولى على طرق المواجهة الشاملة مع الإرهاب بكل صوره تتمثل بتجفيف منابع الإرهاب الالكتروني على المستوى السياسي ، بعد إنعقاد الإرادة السياسية في البلدان وتوافر عنصر الجدية فيها على المضي قدماً في هذا السبيل وصولاً الى غايته النهائية ، والمدخل العملي الى إمكانية تحقق هذا الإجماع تمر بالضرورة على مفازة الإدراك الجماعي والإتفاق على حجم هذا التهديد وتداعياته المستقبلية على الأمن والأهداف الوطنية الكبرى ، سبيلاً للانتقال الى المحطة الثانية في تحقيق الإتفاق المبدئي بين القوى الوطنية على الإطار العام قبل التفاصيل لهذه المواجهة .

إن مثل هذا الاطار المشترك هو الذي سيخلق البيئة المناسبة لبناء مخطط المواجهة بكل تفاصيله . وعند هذا المفصل تزداد وعورة الطريق السياسي للمواجهة بتقاطع الرؤى والاهداف ، التي ينبغي أن لا تنصرف على الأعم الأغلب عن إدراك هدف مؤداه تصفية دوافع الإرهاب وإستئصال مسبباته من المجتمع ومفتاح الحل لهذه المعضلة يكمن في تحقيق الإصلاح وإتمام بناءاته المجتمعية إنطلاقاً من الإيمان بالإرتباط بين الحاجة للإصلاح السياسي الشامل والمواجهة الشاملة للإرهاب بعد التسليم بحتمية الإرتباط بين الإرهاب الالكتروني وسائر أصناف الإرهاب [64]، بعد تفريغ كل شحنات الإحتقانات المجتمعية من ترسباتها وتداعياتها السلبية والمتعارضة مع توجه النخبة الحاكمة للمجتمع . وطريق الإصلاح السياسي يبدأ من تبني الخيارات الديمقراطية الحقيقية القائمة على توسيع مساحة المشاركة السياسية أمام المواطنين والإنطلاق بالحريات الى فضاءاتها الرحبة ، وإشاعة روح التسامح والإنفتاح بين مكونات الشعب وقواه السياسية ، وإسقاط منطق الإقصاء والإنغلاق من مفترضات العمل السياسي سبيلاً لتكريس الهوية الوطنية المشتركة مع تنوع النسيج الإجتماعي ، مروراً ، بإحكام إغلاق دائرة حكم القانون ومؤسساته وتأمين مبدأ سمو الدستور وتوابعه من ضمانات قانونية لشرعية السلطة [65].

ثانياً : تدعيم التعاون الإقليمي والدولي في مجال تحقيق الأمن الالكتروني

إن المشكلات والظواهر الأمنية التي يواجهها العالم في الوقت الحاضر وسوف يواجهها في المستقبل المنظور هي بالأساس مشكلات ذات طابع عالمي أو شبه عالمي ، بمعنى أن أبعادها وتأثيراتها تطال أغلب دول العالم بصورة مباشرة أو غير مباشرة ، وتتعدى قدرتها منفردة على مواجهة تلك التهديدات . وهو ما يحتم التعاون الاقليمي والدولي في مختلف المجالات الأمنية عبر تكثيف الإهتمام بإقامة المؤتمرات وتوقيع الاتفاقيات الدولية الجماعية والثنائية للتعاون والتنسيق وتبادل المعلومات والخبرات بين الدول في مجال مكافحة الإرهاب الالكتروني ؛ ومما يذكر في هذا المجال الاتفاقية الدولية لمكافحة الإرهاب والجريمة الالكترونية التي وقعتها عام 1999 اكثر من(26) دولة ؛ تبعها إتفاق الدول الصناعية الثماني الكبرى في مؤتمرهم السنوي بالمانيا عام 2007 على خطة لمواجهة الإرهاب الالكتروني على مستوى العالم . هذا الى جانب إصدار الاعلانات الدولية وسن القوانين الوطنية أو تعديلها لتجريـــم ما تفعله المنظمات الإرهابية بجميع أعمالها التخريبية والتجسسية والحربية وتشديد العقوبات على من فعلها ، بما يساير ويلائم تطور النمط الإرهابي الالكتروني من جهة والقيم الإجتماعية الالكترونية من جهة اخرى .

ثالثاً : التدابير الامنية لمواجهة الإرهاب الالكتروني

مهما تعددت صور الإرهاب واثاره بضمنها الإرهاب الالكتروني – محل البحث – فهي لاتعدو أن تكون صوراً للجريمة المنظمة الذي تقع مهمة ملاحقته وإستئصاله على عاتق الاجهزة الأمنية والإستخبارية مهما تعددت تسمياتها وتنوعت أساليبها .

وهذا الأمر بحد ذاته يستلزم تبني سلسلة طويلة ومعقدة من الإجراءات والفعاليات ليس على صعيد الخطط والامور الفنية فحسب ، بل ووضع الاسس التشريعية ذات الأبعاد التجريمية أو تطويرها لملاحقة ومعاقبة من ينخرط في هذه الأنشطة الإرهابية وسد الفراغات التشريعية العديدة في هذا المضمار قياساً للتطورات التقنية التي وفرت منافذ سهلة ومتنوعة للإفلات من العقاب على مثل هذه الجرائم الالكترونية . ويتساوق مع هذا التوجه الذي يقع على عاتق المشرعين في كل البلدان ، توجه لإنشاء جهاز قضائي متخصص بإسلوب يفوت على الإرهابي فرصة الافلات من العدالة ، ويوفر الحصانة اللازمة للأفراد من الوقوع بمكائده والانخداع بدعواته المغرضة [66].ويتم إغلاق الحلقة الاخيرة في هذه السلسلة القانونية عبر إنشاء جهاز شرطة متخصص لمكافحة الإرهاب الالكتروني وتزويده بالإمكانات المادية من نظم ومعلومات وإمكانات بشرية قادرة على إستخدام هذه التقنية . وكمثال على ذلك (إستحداث قسم محاربة جرائم الكومبيوتر والإرهاب الالكتروني في مكتب التحقيقات الفدرالي في الولايات المتحدة في عام 1998

. وبكل الاحوال لايمكن – في خضم هذه المواجهة الالكترونية – تجاوز الدور الحيوي للنشاط الاستخباراتي الإستباقي المتقدم ، متذكرين في هذا السياق ما قدمته أجهزة الإستخبارات الدولية المتقدمة من رافد نوعي فاعل جداً في تتبع مسار الارهاب الالكتروني والتصدي المسبق له بتنفيذ عمليات تشويش وتدمير للمواقع الالكترونية الإرهابية [67] ؛ مع تفعيل اليات التعاون والتواصل بين أفراد الشعب والجمعيات الاهلية وبين المسؤولين الرسميين للتصدي لمثل هذه الأنشطة الإرهابية وتسهيل مهمة الاجهزة الامنية في مجال مكافحتها .عبر قيام مزودي خدمة الإنترنت بالإبلاغ عن النشاط الإرهابي الملموس إن شعر بأنه يتضمن تهديداً بالموت أو الإصابة الجسدية الخطيرة لأي شخص.[68]

الفرع الثاني : التدابير التقنية لمواجهة الإرهاب الالكتروني

من حيث المبدأ ، لا يمكن القول بوجود طرق مضمونة تماماً لحماية نظام المعلومات من الإختراق والتعرض الإرهابي الالكتروني حتى يومنا هذا . وعلى الرغم من ذلك عمدت أغلب الدول والمؤسسات الى إعتماد جملة من التدابير والاجراءات الالكترونية التي إتخذت شكل مجموعة من الأجهزة والأنظمة والبرامج المتكاملة مع بعضها وفقاً لبرنامج موضوع مسبقاً للتصدي ومعالجة أي اختراق أو إختلال في نظم معلوماتها بقصد حمايتها تقنياً من الهجمات الإرهابية الالكترونية . أما أهم هذه التدابير فيمكن إيجازها بالآتي :-

أولاً : انشاء مواقع على الانترنت لملاحقة الإرهابيين واعادة تأهيلهم

1. مثال ذلك ما قامت به الشرطة اليابانية من انشاء موقع مثبت فيه صور واسماء (25) من أخطر المجرمين والإرهابيين الملاحقين .
2. إنشاء مواقع الكترونية لإعادة التوازن المعنوي للإرهابيين عبر إعادة تصحيح مفاهيمهم عن الدين وفتح مجال الحوار معهم ومثال ذلك موقع حملة السكينة الذي نفذته السلطات السعودية لإقناع المتطرفين بالعدول عن أفكارهم وقد نجح بالفعل في إقناع أكثر من 690 متطرفاً .[69]

ثانياً: تطوير برامج حماية المعلومات وتطبيقاتها

1- تأمين خطوط الدفاع الأمامية بإستخدام تطبيقات الجدران النارية

تقوم هذه الفئة من التطبيقات بتأمين المنافذ (ports) التي تحصل عبرها التطبيقات على خدمات شبكة المعلومات . وهذه المنافذ تُحدد برمجياً ضمن نظم التشغيل أو التطبيقات المستخدمة. وفي كثير من الأحيان لا يستعمل المستخدم كافة هذه المنافذ مما يجعله يسهو عن تأمينها وحمايتها، مما يشكل فرصة مثالية للقرصنة على نظامه. وتعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالإعتماد على مجموعة من السياسات (policies) التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات التي يُسمح للعاملين بالمؤسسة الولوج إليها. أي أنها تعمل على تحديد الخدمات والإتصال المأمون بها لكل مستخدم، بالتعرف على البروتوكول المخصص له ضمن الشبكة [70].

وضمن فئة الجدران النارية يوجد صنفان، الأول هو الجدران النارية المؤسسية، والتي تقوم بحماية تطبيقات المؤسسات على مستوى الأجهزة المزودة، ومن ثم الأجهزة المرتبطة بهذه النظم المزودة، طالما بقيت مرتبطة بالشبكة. ولكن في عصر المستخدم النقال، والعمل من المنزل، حيث لا يوجد جدران نارية وأجهزة مزودة، تكتسب الجدران النارية الشخصية، أهمية خاصة.

وقد بدأ مدراء المعلوماتية في الغرب مؤخراً يقومون بتثبيت الجدران النارية الشخصية على الأجهزة المحمولة التي يستخدمها العاملون في المؤسسات. ويجب أن نذكر هنا أن الجدران النارية ليست الحل السحري الذي يوفر الأمن الشامل، وأنه يجب إستخدام طبقات أخرى من الأمن تتجاوز الخطوط الأمامية.

2- تأمين حسابات المستخدمين ونظم التحقق من الهوية

على الرغم من وجود العديد من تقنيات التحقق من الهوية وخصوصا أساليب التحقق البيولوجي من الهوية (بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص)، تبقى كلمات السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعاً للتحقق من الهوية ، رغم أن هذه الأساليب بدأت تصبح أضعف وأضعف بتطور التقنيات التي يستخدمها القراصنة لكشفها وخرقها. ومع ذلك، فهنالك العديد من الوسائل التي يمكن إستخدامها للحد من قدرة القراصنة على اختراق واكتشاف هذه الرموز. وتعتمد هذه الوسائل أساساً على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم. ولكن هذه التقنيات، ورغم قوتها، ليست حلولاً سحرية، إذ أنها تتطلب العديد من المهارة والتخطيط الواعي قبل تطبيقها كي تحقق النجاح. وتتكون نظم التحقق من الهوية من ثلاث تقنيات مهمة هي (خدمات الأدلة Directory Services، وهيكلية المفاتيح العامة Public Key Infrastructure، والشبكات الافتراضية الخاصة Virtual Private Networks.) وتشكل هذه التقنيات الثلاث هيكلية شاملة للتحقق من هوية المستخدمين، وضمان تحديد حقوق النفاذ. [71]

أ- خدمات الأدلة (تشفير البيانات)

يعد هذا الإسلوب ، الأكثر شيوعا في حماية نظم المعلومات وهو عبارة عن قواعد بيانات خاصة، ذات مستوى عالٍ من الأمان عادة، ومصممة لجمع، وإدارة المعلومات المتعلقة بمستخدمي الشبكات. ولا يقتصر دور هذه البرمجيات على جمع كلمات السر وأسماء المستخدمين، بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين. ويتم إستخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بجميع مكوناتها كالتطبيقات، والأجهزة الخادمة، والمجلدات، وحتى شكل الشاشة التي يستعملها المستخدم.

وتُدار هذه كلها بشكل مركزي من مكتب مدير الشبكة دون الحاجة للقيام بأية زيارات إلى الأجهزة أو المستخدمين. وتعتبر شركة نوفيل Novell الشركة الرائدة في هذا المجال بمجموعتها الكبيرة من التطبيقات الموجهة لهذا الغرض. [72]

ب-تقنية المفتاح العام

تعتمد هذه التقنية على تقنيات تشفير البيانات، أو بعثْرَتِها scrambling اعتمادا على علاقات رياضية خاصة تجمع ما بين مفتاحين (أو بالأحرى كلمتين سريتين) أحدهما عام والآخر خاص. فعند إرسال رسالة message (كلمة رسالة هنا تشمل أي نوع من المعلومات المُتناقلة بين النظم الإلكترونية بما في ذلك الأوامر التي تتناقلها التطبيقات بين بعضها البعض) يقوم التطبيق الموجود على الجهاز بتشفيرها، أو بعثرة بياناتها، بإستخدام كلمة سر غير معروفة لأحد بإستثناء المستخدم نفسه، ثم تشفيرها ثانية بالمفتاح العام للمستقبل. والسبيل الوحيد الذي يمكن به للمستقبل أن يتعامل مع هذه الرسالة يتمثل في فك تشفيرها، أو إعادة ترتيب بياناتها، بإستخدام مفتاحه الخاص (أو كلمته السرية) أولا، ومن ثم إستخدام المفتاح العام لفك الشفرة الخاصة بهذا المستخدم. وتقوم هيئات عالمية وشركات خاصة بإصدار شهادات رقمية للمصادقة على صحة هذه المفاتيح ومنها شركات مثل RSA أو Verisign (فيري ساين).

ت-الشبكات الافتراضية الخاصة

لا توجد طريقة أكثر أمنا من الشبكات الافتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى الشبكة الدولية. وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ عبرها إلا من يقوم بتحديده مدير الشبكة. وفي هذه الحالة يمكن للمستخدمين المعينين النفاذ إلى الشبكة عبر إنترنت وإسقاط الحزم الواردة من أية جهات أخرى غير هؤلاء المستخدمين.[73] وتعتمد هذه التقنيات على بروتوكولات إتصالات آمنة وخاصة أهمها بروتوكول IPSec والذي يعتمد شفرات بطول 128 بت .[74]

3- تقنية إستمرارية الأعمال

إستمرارية الأعمال هي عنصر حيوي آخر في الاستعدادات لمواجهة خطر الإرهاب الالكتروني يضمن أن العمليات التنظيمية الخاصة بالمستخدم سوف تستمر في التشغيل المريح حتى في حال وقوع هجوم الكتروني على جهاز الحاسوب خاصته ، وذلك عبر التعويض بالنسخ الاحتياطية للبيانات المخزونة على الجهاز بصورة منتظمة حتى تتم المعالجة التدريجية والتامة من الاصابة الفايروسية [75] .

الخـــاتمـــة

أولاً: النتـائـــج

1- على الرغم من عدم توصل المجتمع الدولي الى تعريف متفق عليه للإرهاب بشكل عام والإرهاب الالكتروني بوجه خاص ، فانه يمكن تعريف الأخير بكونه : "شكل من اشكال العدوان الصادر من الدول أو الجماعات أو الأفراد على الإنسان، ماديا أو معنويا بإستخدام الوسائل الإلكترونية أو التهديد به بصورة تلحق الاضرار بالبنى المادية والمعنوية للمجتمع" .

2- يرتبط الإرهاب الإلكتروني بالتطورات التي تحدث في مجتمع المعلومات، فهو يزداد خطورةً وفتكاً كلما زاد التقدم في المجال المعلوماتي، فالاكتشاف والتطور والبناء الذي يجعل من المعلومة مادته الاساسية حتماً ، يقابله الهدم والدمار الذي يمارسه الإرهاب بإستخدام سلاح المعلومة ذاته، فتكون الاخيرة مادةً وسلاحاً في البناء والهدم على حدٍ سواء بفارق الغرض .

3- مهما تعددت دوافع وأسباب الإرهاب الالكتروني ، فإنها لن تخرج عن تلك الأسباب المتعلقة بظاهرة الإرهاب بشكل عام ، الا بفارق العامل التقني المعلوماتي الذي وفر بفضاءاته المفتوحة وإمكاناته الواسعة فرصاً وتسهيلات أكثر تنوعاً وجاذبية للتنظيمات الإرهابية ؛ طالما شكل الإرهاب الالكتروني ، الوجه والإمتداد التقني المتطور للإرهاب بشكله العام .

4- لقد أفضى الإرهاب الالكتروني بشكل مباشر وغير مباشر الى نزيف حاد في الحقوق والحريات ولاسيما تلك المتعلقة بالحق بالخصوصية بسبب من طبيعة الإرهاب الالكتروني المتسللة عبر غطاء من الغموض والمخاتلة ، وليس أدل على ذلك من سلة التشريعات التي صاحبت المواجهة الشاملة للإرهاب الالكتروني في الدول المتقدمة ولاسيما بعد الهجمات الإرهابية في الولايات المتحدة عام 2001.

5- مع تنامي حجم الاعتمادية الدولية على شبكة المعلومات الدولية ووسائل الاتصالات المتطورة ، تنوعت مظاهر ووسائل الإرهاب الالكتروني بين ما يستهدف المعلومة وانظمتها مباشرة عبر الاختراق والتجسس والتدمير وبين من يسخر هذه المعلومة لتحقيق مارب اخرى أكثر ملامسة للواقع ، لتزداد بذلك قدرة تلك التنظيمات الإرهابية على التدمير بإستخدام هذا الشكل المتطور من التقنية وتتراجع امامها قدرات الدول على المواجهة والاستئصال لخطر هذا الإرهاب .

6- من العسير التحقيق في ظل الإرهاب الالكتروني ، تحديد حجم الدمار الذي يمكن أن تسببه الهجمات الالكترونية .

7- إن خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهل المنال، فهناك إذن علاقة طردية بين درجة تطور البلدان ودرجة تعرضها للإرهاب الالكتروني التي تزداد مع تطور هذه البلدان .

8- إذا كانت المعلومات هي ادوات القوة الناعمة ، جاز القول بأن الإرهاب الالكتروني هو سلاح الدمار لهذه القوة الناعمة والخطر المستقبلي المتربص بمعطيات الحضارة الانسانية ؛ نظراً للتطور المتسارع في مجال الإنترنت وتكنولوجيا المعلومات من جانب ، وتنوع وسائل الإرهاب الالكتروني وإتساع مجال الأهداف التي يمكن عبر وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيداً عن الإزعاج والفوضى، مع توفير قدر كبير من السلامة والأمان للإرهابيين.

ثانياً: التوصيات

1. ضرورة السعي إلى عقد مؤتمر دولي بإشراف هيئة الأمم المتحدة يتم عبره تحديد طبيعة الإرهاب الالكتروني وصوره ، مع تحديد خطة عملية دولية لمكافحته واستئصاله تودع باتفاقية دولية جماعية تضمن اكبر مشاركة واقصى درجات التعاون والتنسيق بين الدول والمنظمات الدولية لتحقيق هدفها المحوري في مكافحة الإرهاب .
2. يتوازى مع الخط الاممي الأول ، توجه اقليمي آخر لإبرام اتفاقيات وإنشاء منظمات إقليمية مختصة بتعضيد التعاون والتنسيق الأمني في مجال مكافحة الإرهاب الالكتروني وأهمية هذا التوجه تبرز على مستوى أكثر الحاحاً بالنسبة لمنطقة الشرق الأوسط بسبب أوضاعها الأمنية المتدهورة .
3. حث كافة دول العالم على مراجعة نظمها القانونية ، بإصدار قوانين جديدة تحرم وجود المنظمات والأنشطة الإرهابية على إختلاف أنواعها وصورها ،وتعاقب من يثبت قيامه بأي من هذه الأنشطة أو يشارك فيها بأقصى العقوبات ، لمواكبة ومواجهة ما يستجد من صور الإرهاب ووسائله وبخاصة تلك المتعلقة بأنظمة الحاسوب والاتصالات .
4. إنشاء مركز دراسات – وطني أو اقليمي- يضم أفضل النخب من الفنيين والباحثين المتخصصين بأمور الامن المعلوماتي والبرمجيات بهدف تطوير إستراتيجيات فاعلة لمكافحة الإرهاب الإلكتروني وتطوير وسائل مقاومته، عبر وضع سيناريوهات المخاطر المحتملة وأساليب المكافحة، ودعم بحوث أمن المعلومات ومكافحة الإرهاب الإلكتروني وتشجيع تصنيع برامج وطنية ، للحماية، وجدران النار، ومحاولة الإستغناء، عن استيراد برامج الحماية، وبرامج التشفير .
5. تأمين شبكات المعلومات وأنظمة الاتصالات ومصادر الطاقة ، مادياً (متانة المباني، إجراءات الأمن، الحراسات) ، وفنياً (التدريب، برامج الحماية). مع محاولة انشاء شبكة معلومات وطنية خاصة مفصولة عن الشبكة الدولية أو حتى تحديد مسارات الاتصال وعقده مع الشبكة الدولية ، لتحجيم فرص اختراق الشبكات الوطنية .
6. الاحتفاظ بنسخ احتياطية من قواعد البيانات الوطنية (الأمنية، المالية، العسكريّة..الخ).
7. العمل على إعادة النظر الجذرية في المناهج الدراسية في كل المراحل بدءاً من رياض الاطفال وحتى الجامعات ، لتطوير وعي الطلبة بما يحث ويساعد الإستخدام الآمن للحاسبات والفضاء الرقمي والحذر من مخاطره .

الهوامش

(1)ابو الفضل محمد بن مكرم بن منظور ، لسان العرب ، المجلد الثالث ، دار لسان العرب ، بيروت ، 1968 ، ص 903 .

(2)محمد بن يعقوب الفيروزبادي ، القاموس المحيط ، ط2، مؤسسة الرسالة ، بيروت ، 1987 ، ص118.

(3)http://www.almaany.com/ar/dict/ar-en/electronic/

(4)http://www.almaany.com/ar/dict/ar-ar/

(5)http://www.ibtesama.com/vb/showthread-t_10265.html

(6)د. خليل إسماعيل الحديثي، الإرهاب الدولي .... مدان قانونا أم سياسة ؟ ، مجلة العلوم السياسية، جامعة بغداد ، العدد 26 ، 2002، ص151

(7) الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998م.

(8)د.محمد عبد المنعم عبد الخالق ، الجرائم الدولية دراسة تأصيلية للجرائم ضد الانسانية وجرائم الحرب ، دار النهضة المصرية ، القاهرة ، 1989 ، ص 104 .

(9)د.رجب عبد المنعم متولي ، حرب الارهاب الدولي والشرعية الدولية ، ط2، دار النهضة العربية ، القاهرة ، 2006 ، ص 385.

(10)Major J P I A G CHARVAT, Cyber Terrorism: A New Dimension in Battlespace, Course Director in Centre of Excellence Defense Against Terrorism,p.2

(11)Cyber Terrorism A Global Menace Criminology Essay , http://www.ukessays.com/essays/criminology/cyber-terrorism-a-global-menace-criminology-essay.php

(12)Ph.D. Serge Krasavin, What is Cyber-terrorism?, http://www.crime-research.org/library/Cyber-terrorism.htm

(13) Ph.D.William L. Tafoya, Cyber Terror, the law enforcement bulletin, FBI Academy, Volume 80, Number 11,November 2011,p2

(14)Zahri Yunos and Syahrul Hafidz, Cyber Terrorism And Terrorist Use Of ICT And Cyberspace, Ministry of Foreign Affairs Malaysia, Southeast Asia Regional Center for Counter Terrorism, no. 6184,2013

(15) شريهان نشأت المنيري ، ندوة" مخاطر جرائم الإنترنت على استقرار النظام الدولي ،ا لمركز الدولي للدراسات المُستقبلية والاستراتيجية ، مجلة السياسة الدولية ، العدد 199 ، 2012 ، ص 112.

(16) د. حسين بن سعيد بن سيف الغافري ، الإرهاب الإلكتروني ، على الرابط:
5&LID=9&PID=1http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=
(17) د.مصطفى محمد موسى ، الارهاب الالكتروني : دراسة قانونية –امنية- نفسية-إجتماعية ، مطابع الشرطة ، القاهرة ، 2009، ص173.
(18)محمود الرشيدي ، العنف في جرائم الانترنت : اهم القضايا : الحماية والتامين ، الدار المصرية اللبنانية ، القاهرة ، 2011، ص 37.
(19)جلال محمد الزعبي واسامة احمد المناعسة ، جرائم التقنية نظم المعلومات الالكترونية : دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان ، 2010 ، ص277.
(20)Rajeev C. Puran, Beyond Conventional Terrorism...The Cyber Assault,SANS GIAC Security Essentials Certification (GSEC) v1,pp.7-8
(21)م. مهران زهير المصري ، الإرهاب الإلكتروني ، مجلة المعلوماتية ، الجمعية العلمية السورية ، دمشق ، العدد (69) ، تشرين الثاني 2011 ، ص 36 .
(22) القرصنة يشير إلى جميع أشكال ووسائل الوصول -غير المصرح بها وغير المشروعة- إلى نظام الكمبيوتر أو الشبكة الدولية للمعلومات . انظر : د. حسام الفوزان ، برمجيات التجسس : القليل من المعرفة شيء رائع ، مجلة الثقافة المعلوماتية ، العدد الثالث والعشرون ، ايلول 2007 ، ص ص 17-18.
(23)Cyber Terrorism A Global Menace Criminology Essay, op.cit
(24)Dr. Edward J. Maggio, Cyber Terrorism, Center for Security and Disaster Response, Institute of Technology, New York,
http://www.survivalinsights.com/modules.php?name=News&file=article&sid=39
(25)عبد الصبور عبد القوي ، الجريمة الالكترونية ، دار العلوم للنشر والتوزيع ، بلا سنة نشر ، ص ص 88-89.
(26) وهي نفس المجموعة التي شنت هجمات بالغاز في مترو طوكيو عام 1995 ما أسفر عن مقتل 12 شخصا و إصابة أكثر 6000 .
(27) lbid
(28)الارهاب الالكتروني في القانون الدولي ، نشرت بواسطة: موقع السكينة 4 نوفمبر، 2013، على الرابط : html31803/1www.assakina.com/news/news

(30) ويكفي للتدليل على ذلك ان الكتاب الذي الفه ايمن الظواهري (فرسان تحت راية النبي) قد انتشر بسرعة رهيبة بفضل المواقع الاسلامية على الانترنيت .
(31)د. مصطفى محمد موسى ، مصدر سابق ، ص ص 226-228 .
(32)Cyber-Terrorism: The Emerging Threat , http://www.emrisk.com/knowledge-center/newsletters/cyber-terrorism-emerging-threat
(33)د. مسعد عبد الرحمن زيدان ، الارهاب في ضوء احكام القانون الدولي العام ، دار الكتب القانونية ، القاهرة ، 2007 ، ص 122.
(34) حسين العزاوي ، مصدر سابق ، ص 52 .
(35)د. تميم العودات وأ. حسين الطروانة " تأريخ الإرهاب " ورقة عمل مقدمة إلى مؤتمر الإرهاب في العصر الرقمي جامعة الحسين بن طلال / الأردن ،http://www.ahu.edu.jo/tda/papers%5C99.doc.
(36) المصدر السابق ، ص 135.
(37) حسين العزاوي ، مصدر سابق ، ص 52 .
(38)المصدر السابق ، ص 54 .
(39) لقد حذر الإسلام من الغلو حتى ولو كان بلباس الدين يقول النبي عليه الصلاة والسلام :(إياكم والغلو)
(40)المصدر السابق ، ص 53 .
(41) د.حسنين المحمدي بوادي ، العالم بين الارهاب والديمقراطية ، دار الفكر الجامعي ، الاسكندرية ، 2007 ، ص 97
(42)د. عبد الملك الدناني ، البث الفضائي العربي وتحديات العولمة الاعلامية ، المكتب الجامعي الحديث ، 2007 ، ص 245.
(43) Cyber Terrorism,op.cit
(44)lbid
(45) محمد امين الشوابكة ، جرائم الحاسوب والانترنت : الجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، 2009 ، ص 170.
(46) د.مصطفى محمد موسى ، مصدر سابق ، ص ص 238- 242.
(47) فيروس الكمبيوتر هو برنامج حاسوبي يلحق الضرر بنظام المعلومات والبيانات، ويقدر على التضاعف والانتشار تلقائيا ، والانتقال من جهاز إلى آخر عند نقل البرامج والملفات المصابة ؛ وهو بهذه الخصائص يتشابه مع الفيروس الطبيعي من نواح عدة، فهو يغير خصائص البرامج كما يقوم الفيروس الطبيعي بتغيير خصائص الخلايا المصابة، و يتكاثر وينتشر ويغير من شكله

تماماً كالفيروس الطبيعي. جدير بالذكر ان فيروسات الحاسبة – شأنها شأن الفيروسات الطبيعية – تكون على انواع عدة ،و متدرجة من حيث الأضرار التي تلحقها بالأجهزة بدءً من الأضرار اليسيرة إلى تدمير النظام بأكمله . ويمكن للإرهابي إستخدام الفيروسات لنشر الدمار عبر الشبكات المعلوماتية والأنظمة الإلكترونية، كما يمكنه إستخدامها في الاختراق والتجسس أيضاً. انظر : محمد امين الرومي ، جرائم الكمبيوتر والانترنت ، دار المطبوعات الجامعية ، الاسكندرية ، 2003 ، ص 26.

48) للمزيد من التفاصيل حول هذه البرامجيات المدمرة يمكن الرجوع الى : سراب ثامر احمد ، الهجمات على شبكات الحاسوب في القانون الدولي الانساني ، اطروحة دكتوراه مقدمة الى كلية الحقوق في جامع النهرين ، 2014 ، ص ص 85-89.

49) محمود احمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة للنشر والتوزيع ، 2005 ، ص ص 100-101.

50 Dr. Edward J. Maggio, Terrorism: Cyber Terrorism, Criminal Justice Center for Security and Disaster Response, New York, www.survivalinsights.com/modules.php?...News .

51 Jake Koss, Cyber Terrorism, Melrose-Mindoro High School: Wisconsin High School, Committee: 4,p3

52 Cyber Terrorism A Global Menace Criminology Essay, http://www.ukessays.com/essays/criminology/cyber-terrorism-a-global-menace-criminology-essay.php

53 Cyber Insurance and the Terrorism Exclusion, http://www.cyberriskinsuranceforum.com/content/cyber-insurance-and-terrorism-exclusion

(54) من الأمثلة على بعض المواقع الإلكترونية العربية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية ما يأتي:

1. موقع النداء :وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001م، ومن خلاله تصدر البيانات الإعلامية للقاعدة.
2. ذروة السنام :وهي صحيفة إليكترونية دورية للقسم الإعلامي لتنظيم القاعدة.
3. صوت الجهاد :وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وهي تصدر بصيغتي : (word) , (pdf)وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.

55 J P I A G CHARVAT,op.cit, pp.4-5.

(56)د.مصطفى محمد موسى ، الارهاب الالكتروني ، مصدر سابق ، ص ص 236 -237 .

(57)عبدالله بن عبدالعزيز بن فهد العجلان ، الإرهـاب الإلكتـرونـي في عصر المعلومات ، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008م، ص 63.

58 S. Keene, “Terrorism and the internet: A double edged sword.” Journal of Money Laundering Control, 14/4 ,(2011).. pp.359-370.

(59)د. محمد بن حمود الهدلاء ، كثرة المواقع الإلكترونية للشبكات الإرهابية تدق ناقوس الخطر! ، مقال منشور في صحيفة الجزيرة ، العدد 14640 الأحد 12 ذو الحجة 1433.

60 James A. Lewis,Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:Center for Strategic and International Studies,Washington.D.C, December 2002,P.8

61 Kevin Coleman, Cyber Terrorism, Directions Magazine, Friday, October 10th 2003

(62)د.مصطفى محمد موسى ، مصدر سابق ، ص ص 266- 267 .

63 Jimmy Sproles and Will Byars, Cyber-terrorism, A Student paper for Computer Ethics at ETSU 1998 http://csciwww.etsu.edu/gotterbarn/stdntppr/

64 Rajeev C. Puran,op.cit , p.5

65 Valarie Findlay, Cyber-Terrorism and Canada’s Cyber-Security Strategy , Centre for Security Governance, Apr 9, 2014, http://www.ssrresourcecentre.org/2014/04/09/cyber-terrorism-and-canadas-cyber-security-strategy/

66 lbid

67 What is cyber terrorism?, http://readanddigest.com/contact-us/

(68)م. مهران زهير المصري ، الإرهاب الإلكتروني ، مصدر سابق ، ص 58.

(69) د.مصطفى محمد موسى ، مصدر سابق ، ص ص 280 -281 .

70 Jimmy Sproles and Will Byars,op.cit

71 محمود الرشيدي ، مصدر سابق ، ص 143.

72 Rajeev C. Puran,op.cit ,p.11

73 د.خالد بن سليمان الغثبر ود.محمد بن عبد الله القحطاني ، امن المعلومات بلغة ميسرة ، مكتبة الملك فهد الوطنية ، الرياض ، 2009 ، ص 25.

(74)الارهاب الالكتروني ، الموسوعة الالكترونية الحرة (ويكيبيديا) ، الرابط :

75 Cyber-Terrorism: The Emerging Threat, op.cit

المصادر

أولا : الكتب

- **القران الكريم**

1. ابو الفضل محمد بن مكرم بن منظور ، لسان العرب ، المجلد الثالث ، دار لسان العرب ، بيروت ، 1968.
2. د. احمد ابو الحسن زرد ، قوانين مكافحة الارهاب تطبيق لالتزام دولي ، الهيئة العامة للاستعلامات ، وزارة الاعلام – جمهورية مصر العربية ، بلا سنة طبع.
3. جلال محمد الزعبي واسامة احمد المناعسة ، جرائم التقنية نظم المعلومات الالكترونية : دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، 2010 ، عمان ، 2010.
4. د. حسنين المحمدي بوادي ، العالم بين الارهاب والديمقراطية ، دار الفكر الجامعي ، الاسكندرية ، 2007 .
5. د. خالد بن سليمان الغثبر ود.محمد بن عبد الله القحطاني ، امن المعلومات بلغة ميسرة ، مكتبة الملك فهد الوطنية ، الرياض ، 2009 .
6. د.رجب عبد المنعم متولي ، حرب الارهاب الدولي والشرعية الدولية ، ط2، دار النهضة العربية ، القاهرة ، 2006.
7. عبد الصبور عبد القوي ، الجريمة الالكترونية ، دار العلوم للنشر والتوزيع ، بلا سنة نشر .
8. د. عبد الملك الدناني ، البث الفضائي العربي وتحديات العولمة الاعلامية ، المكتب الجامعي الحديث ، 2007.
9. محمد امين الرومي ، جرائم الكمبيوتر والانترنت ، دار المطبوعات الجامعية ، لاسكندرية ، 2003 .
10. محمد امين الشوابكة ، جرائم الحاسوب والانترنت : الجريمة المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، 2009.
11. محمد بن يعقوب الفيروزبادي ، القاموس المحيط ، ط2، مؤسسة الرسالة ، بيروت ، 1987.
12. د. محمد عبد المنعم عبد الخالق ، الجرائم الدولية دراسة تأصيلية للجرائم ضد الانسانية وجرائم الحرب ، دار النهضة المصرية ، القاهرة ، 1989.
13. محمود احمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة للنشر والتوزيع ، 2005.
14. محمود الرشيدي ، العنف في جرائم الانترنت : اهم القضايا : الحماية والتامين ، الدار المصرية اللبنانية ، القاهرة ، 2011.
15. د. مسعد عبد الرحمن زيدان ، الارهاب في ضوء احكام القانون الدولي العام ، دار الكتب القانونية ، القاهرة ، 2007
16. د. مصطفى محمد موسى ، الارهاب الالكتروني : دراسة قانونية –امنية- نفسية-إجتماعية ، مطابع الشرطة ، القاهرة ، 2009.

ثانيا : البحوث والدوريات

1. د. حسام الفوزان ، برمجيات التجسس : القليل من المعرفة شيء رائع ، مجلة الثقافة المعلوماتية ، العدد الثالث والعشرون ، ايلول 2007 .
2. د. خليل إسماعيل الحديثي، الإرهاب الدولي .... مدان قانونا أم سياسة ؟ ، مجلة العلوم السياسية، جامعة بغداد ، العدد 26 ، 2002 .
3. عبدالله بن عبدالعزيز بن فهد العجلان ، الإرهـاب الإلكتـرونـي في عصر المعلومات ، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008م.
4. د. محمد بن حمود الهدلاء ، كثرة المواقع الإلكترونية للشبكات الإرهابية تدق ناقوس الخطر! ، مقال منشور في صحيفة الجزيرة ، العدد 14640 ، الأحد 12 ذو الحجة 1433.
5. م. مهران زهير المصري ، الإرهاب الإلكتروني ، مجلة المعلوماتية ، الجمعية العلمية السورية ، دمشق ، العدد (69) ، تشرين الثاني 2011.
6. ندوة" مخاطر جرائم الإنترنت على استقرار النظام الدولي ،المركز الدولي للدراسات المُستقبلية والاستراتيجية ، مجلة السياسة الدولية ، العدد 199 ، 2012.

ثالثاً : الأطاريح الجامعية

- سراب ثامر احمد ، الهجمات على شبكات الحاسوب في القانون الدولي الانساني ، اطروحة دكتوراه مقدمة الى كلية الحقوق في جامع النهرين ، 2014 .

ثالثا : النصوص القانونية

- الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998م.

رابعا : مصادر الشبكة الدولية للمعلومات

د.حسين بن سعيد بن سيف الغافري ، الإرهاب الإلكتروني ، على الرابط
5&LID=9&PID=1http://www.ita.gov.om/ITAPortal_AR/Pages/Page.aspx?NID=
الارهاب الالكتروني في القانون الدولي ، نشرت بواسطة: موقع السكينة 4 نوفمبر، 2013، على الرابط :
.html31803/1www.assakina.com/news/news
الارهاب الالكتروني ، الموسوعة الالكترونية الحرة (ويكيبيديا)
د. تميم العودات / أ. حسين الطروانة " تأريخ الإرهاب " ورقة عمل مقدمة إلى مؤتمر الإرهاب في العصر الرقمي جامعة الحسين بن طلال / الأردن ،http://www.ahu.edu.jo/tda/papers%5C99.doc.

The English References

First- Articles

1. Ph.Dr.William L. Tafoya, Cyber Terror, the law enforcement bulletin, FBI Academy, Volume 80, Number 11,November 2011.
2. Zahri Yunos and Syahrul Hafidz, Cyber Terrorism And Terrorist Use Of ICT And Cyberspace, Ministry of Foreign Affairs Malaysia, Southeast Asia Regional Center for Counter Terrorism, no. 6184,2013
3. Rajeev C. Puran, Beyond Conventional Terrorism...The Cyber Assault,SANS GIAC Security Essentials Certification (GSEC) v1,
4. Jake Koss, Cyber Terrorism, Melrose-Mindoro High School: Wisconsin High School, Committee.
5. James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:Center for Strategic and International Studies,Washington.D.C, December 2002 .
6. Kevin Coleman, Cyber Terrorism, Directions Magazine, Friday, October 10th 2003
7. S. Keene, "Terrorism and the internet: A double edged sword." Journal of Money Laundering Control, no14 ,(2011).
8. Major J P I A G CHARVAT, Cyber Terrorism: A New Dimension in Battlespace, Course Director in Centre of Excellence Defense Against Terrorism.

Second -INTERNET

1. Cyber Terrorism A Global Menace Criminology Essay ,
2. http://www.ukessays.com/essays/criminology/cyber-terrorism-a-global-menace-criminology-essay.php
3. Cyber Terrorism A Global Menace Criminology Essay,
4. http://www.ukessays.com/essays/criminology/cyber-terrorism-a-global-menace-criminology-essay.php
5. Cyber-Terrorism: The Emerging Threat ,
6. http://www.emrisk.com/knowledge-center/newsletters/cyber-terrorism-emerging-threat
7. Cyber Insurance and the Terrorism Exclusion,
8. http://www.cyberriskinsuranceforum.com/content/cyber-insurance-and-terrorism-exclusion
9. Dr. Edward J. Maggio, Cyber Terrorism, Center for Security and Disaster Response, Institute of Technology, New York,
10. http://www.survivalinsights.com/modules.php?name=News&file=article&sid=39
11. Jimmy Sproles and Will Byars, Cyber-terrorism, A Student paper for Computer Ethics at ETSU 1998 http://csciwww.etsu.edu/gotterbarn/stdntppr/
12. Ph.D. Serge Krasavin, What is Cyber-terrorism?, http://www.crime-research.org/library/Cyber-terrorism.htm
13. Valarie Findlay, Cyber-Terrorism and Canada's Cyber-Security Strategy , Centre for Security Governance, Apr 9, 2014, http://www.ssrresourcecentre.org/2014/04/09/cyber-terrorism-and-canadas-cyber-security-strategy/
14. http://www.almaany.com/ar/dict/ar-en/electronic/
15. http://www.almaany.com/ar/dict/ar-ar/
16. http://www.ibtesama.com/vb/showthread-t_10265.html
17. What is cyber terrorism?, http://readanddigest.com/contact-us/