

ظاهرة الإرهاب في عصر المعلوماتية الرقمية مبررات الحدث وسبل المواجهة

د. عبدالصمد سعدون عبدالله الشمري* د. ليلي عاشور حاجم الخزرجي**

المقدمة والأهمية

يتأثر فعل الإرهاب بالعديد من المتغيرات الكونية والبيئية المتطورة ، إذ يبرز الجانب التقني والرقمي ضمن متغير المعلوماتية الإلكترونية في إطار الموجة الثالثة ضمن أولويات هذا المتغير ، وكوئهما الأكثر تأثيراً في الفعل الإرهابي وحالة التوظيف الآني والإستراتيجي للفعل ورد الفعل ولأي حدث يقع ضمن دائرة الفعل الإرهابي .

المتغير الرقمي أو الإلكتروني Electronic or Digital variable

والذي يُعد أداة من أدوات الإختراق الأمني عبر منظومة المعلومات الإستخباراتية لقياس قدرة العدو وحجم الإمكانيات الدفاعية ومعرفة مواطن الضعف والقوة ومن خلال التعامل مع واقع المعلومة المتاحة وبدقة متناهية على أنها مفتاح حلول للشروع بالعمل الإرهابي وتدمير مكاسب الدولة والمجتمع من قدرات مالية واقتصادية ، فضلاً عن إحداث الترويع والتخويف في نفوس الأبرياء من الشعوب الآمنة ، بهدف تحقيق الغايات التي تكمن في مطالب السلوك الإرهابي وتعدد أغرضها خارج نطاق وحدود القيم والأخلاق والدين .

إن التطور المتسارع في تقنيات المعلومات الدقيقة والإلكترونيات الرقمية ، قد طوعت قوى الطبيعة لمضاعفة قدرة الإنسان وذهنيته خلال مدة زمنية وجيزة تفوق

* أستاذ مدرس في قسم العلاقات الاقتصادية الدولية في كلية العلوم السياسية/ جامعة النهرين

** مدرس في قسم العلاقات الاقتصادية الدولية\ كلية العلوم السياسية \ جامعة النهرين

ملايين المرات قدرته آبان الثورة الصناعية سواء في دقة الأداء أو حسابات التفكير والذاكرة، وهذا بدوره قد أعطى مزايا نوعية لقدرات الإنسان في المبادرة ضمن الفعل أو رد الفعل الإرهابي عبر الاستعانة بالتطبيقات الإلكترونية الرقمية الدقيقة وفي كل المجالات .

وفي هذا الجانب البحثي تتركز أهمية الحقل الإلكتروني كتطور متراكم عن أثر بدايات الحاسبات الإلكترونية حين اعتمدت في السابق الإشارات الكهربائية المبسطة ، وتبدو العملية أسرع بكثير أمام نظم الإلكترونيات الرقمية حين تم معالجة الإشارات الكهربائية عن بعد دون معايير الاهتمام بقياسها ومستوى انتقالها كنظام عددي يتضمن جانبين اقتصاديين أحدهما اختزال الحجم ، وثانيهما انخفاض الكلفة وبشكلٍ مستمر مع كل تطور يحدث في هذا النوع من المعلوماتية المعاصرة. وحين يتم توظيف علم الإلكترونيات الواسع وعلى نطاق غير محدود على الأجل القصير والمتوسط وفيما يتعلق بدينامكية فعل الإرهاب في عصرنا هذا ، فإن الأمر سيكون في غاية التعقيد بالنسبة لأمن الدول ، ولسلطة القانون وحماية المجتمع تحديدا، فضلا عن المحافظة على سمة التطور العلمي والمعرفي، كونه مجالا ساميا من الخصائص الإنسانية والمتراكمات العلمية التي تشكل السلسلة المعرفية لعموم المجتمعات البشرية على أرض البسيطة .

إشكالية الدراسة

إن إشكالية الدراسة تنبع عن تساؤلات تطرحها الظاهرة موضوع البحث والدراسة والتي تترجمها فرضية الدراسة كعلاقة دالية بين نمو فعل الإرهاب الإلكتروني وحالة التطور في المعلوماتية الرقمية والى مستوى عالي من الاختراق والنفوذ الأمني للمؤسسات الاقتصادية والسياسية والاجتماعية مسببة بذلك خطرا كبيرا على سيادات الدول .. إلا أن تطور المعلوماتية وأتساع نطاقها عبر شبكات الإنترنت

وتنوع البرامج وأنظمة الحاسوب ، يساعد هو الآخر على تطور المنظومة الأمنية وبناء قاعدة مضادة لمتغير للإرهاب الإلكتروني وأهدافه في تهديد وترويع المجتمعات ، ذلك أن إستغلال مثل هذا التطور وتوظيفه سلاح ذو حدين ، إذ لا يكون هذا التطور التقني مشروطا في استخدامه أو حصره على جهة معينة سواء رسمية حكومية أم خاصة أو غير رسمية أو جهات (غير مشروعة) وخارجه عن حدود هذا الاستخدام التقني... فالجميع ليسوا يبيعد عن حق التعامل مع التطور الإلكتروني بمختلف أنواعه وصنوفه طالما أن هذه الجهة أو تلك قادرة على دفع الأموال وتقديم العون من أجل استخدام أنظمة الحاسوب والإنترنت .

وهذه هي الإشكالية في ذاتها حين تعترض تساؤلات الفرضية ، ومن خلال رد الفعل المضاد والحث على خلق حالة من الترتيبات الأمنية والاستعدادات الدفاعية غير العادية للحد من مخاطر التقنيات المعلوماتية ، إذا ما تم توظيفها توظيفا مضادا لمصالح الدول والمجتمعات وبما يحقق أهداف الحركات والمنظمات الإجرامية .

فرضية الدراسة

ومن خلال ما تم سرده من مداخل للمقدمة تبدو لنا هذه الفرضية ، على أنها تساؤلات ، تتخللها إشكاليات معقدة ، إذ تتطلب الوقوف وبجذر ودقة في التعامل مع هذا المتغير الذي تلون بلون التطور المعلوماتي واكتسى ثوب التقنية العصرية . إذ تبرز ملامح هذه الفرضية من خلال " أن فعل الإرهاب **Terrorism action** وبكل أشكاله ومظاهره مؤثر وبمستويات مختلفة باختلاف الوسائل والغايات التي تبرر فعله ، وأن الإرهاب الرقمي يُعد مرحلة متطورة لهذا المتغير ، والذي يرتبط بمرحلة ما بعد الحداثة بوسائل التطور التقني والرقمي كمظهر حديث لتحقيق النفوذ والاختراق لمختلف مؤسسات الدولة والمجتمع ، ليبدو بكل المقاييس للعالم على أنه إرهابا عن

بعد وخارج حدود ونطاق السيادات الوطنية والإمكانات الأمنية الوطنية " وهذا سيشكل في المستقبل حالة جدل في أوساط البيئة السياسية والعلاقات الاقتصادية الدولية ، مما يساهم في توسيع قاعدة العنف والعنف المضاد وبث الرعب والتخويف وعدم الاستقرار للسلم والأمن الدوليين ..

منهجية الدراسة

وفي هذا السياق يتم التقصي عن حقائق البحث والدراسة ضمن منهج استقرائي للحدث الناجم عن فعل الإرهاب الرقمي ، كظاهرة باتت مشكلة مألوفة على الدوام في البيئة الدولية ومنذ أن تبلورت سلسلة عناصرها الأساسية في السلوك الإرهابي ومظاهرها وأسبابها لتدور في حلقة مفرغة من الأمن المفقود ، بحثا عن الآليات والحلول في احتواء هذا المتغير الخطير ، على أن وسائل وأساليب البحث تتطلب تحليلا منطقيًا للإجابة الوافية على أسئلة محاور البحث ومن خلال الأسلوب الوصفي تارة والأسلوب النظمي المقارن تارة أخرى لبلوغ نتائج البحث والاستنتاجات والتوصيات التي تخرج منه في المحصلة ضمن الإطار العام من الحلول والمواجهة المطلوبة لإحتواء ووقف تأثير هذا المتغير ..

هيكلية الدراسة ووفق مسارات هذا المنهج المتبع في تحليل محاور الدراسة وفي إطار عناصر الموضوع واتجاهاته الأساسية ، فإن الدراسة ستأخذ ثلاثة محاور فضلا عن مقترحات الحلول والمواجهة والاستنتاج العام والتوصيات كمقومات ضرورية وكمحصلة للنتائج المتحققة من الدراسة إذ يتضمن **المحور الأول** الثورة المعلوماتية ومظاهر الإرهاب الإلكتروني : الخصائص والأسباب **والمحور الثاني** ينصب حول المتاح في كيفية إدارة وسائل الاتصال الرقمي لمواجهة الفعل الإرهابي في حين تناول **المحور الثالث** الإرهاب الإلكتروني الوجه الغاضب والخطر الخارق في توظيف المعلوماتية الرقمية ..

المحور الأول : الثورة المعلوماتية ومظاهر الإرهاب الإلكتروني : الخصائص والأسباب
الأول : الثورة المعلوماتية ومظاهر الإرهاب الإلكتروني

إن نظم المعلومات تشكل إضافة عظيمة في المجالات السياسية ، وبخاصة التخطيط الإستراتيجي للدولة والمجتمع من خلال تشخيص المشاكل والمعوقات والأزمات للبحث عن سبل متطورة لإحتوائها ومعالجتها وهكذا الحال بالنسبة لمتغير الإرهاب الإلكتروني ، الذي يُعد واحد من المتغيرات المهمة في ظل الثورة المعلوماتية الرقمية ، وثورة المعلومات الرقمية يمكن أن تأخذ شكل سلاح ذو حدين ، إما خدمة السلم والأمن العالميين ، وإما تدميرهما اعتماداً على سمة التوظيف لهذه النظم ضمن التخطيط الإستراتيجي .

وكما يرى الباحثان آرثر شربلين Thomas. L. Weelen وديفيد هانكر David Hunger ، من أن نظم المعلومات في التخطيط الاستراتيجي يمكن أن يضع حلولاً لإسئلة كثيرة تدخل في معالجة المشاكل الاستراتيجية وتحت مسمى نظام المعلومات الإستراتيجي الذي يتبنى مسؤولية التخطيط الشامل وضمن مستويات عليا⁽¹⁾.

ويدخل اثر ثورة المعلوماتية الرقمية في تغييرات كبيرة وشاملة وفي توجيه الأنشطة في جميع المجالات الاقتصادية ، فضلا عن الجانبين الأمني والسياسي من خلال انتقال المعلوماتية بشكلٍ عفوي أو بتخطيط واعٍ عبر المسافات البعيدة واختراق نطاقات الحدود السياسية للدول.

(1) Thomas .L. Weelen,David Hunger,Stratigic management and Business policy,5th Edition , (U.S.A ,Addition Wesley Publishing) 1995, p 95.

إن هذا الإنجاز الكبير له تأثيراته الجانبية على ثقافة المتلقي ، لاسيما المجتمع النامي المعتاد على هذا النوع من المستوردات من الصناعات مما يغير من وجهة تفكيرها وتعاملها مع الواقع ، وضمن منظور مختلف تماماً عما يجري في الدول المصنعة ، فضلا عن تغيير جذري في سلوكيات المتلقي ممن لا يدرك تأثير استخدام هذه التقنيات المتقدمة ضمن نمط ضعيف من التلقي والتوظيف ، وهو ما يسيء الى مستوى التعامل مع الواقع⁽²⁾ وهو ما يبعث على القلق وعدم الإطمئنان حول مصير المتلقي من الشباب دون مراعاة نوعية المعلومات التي يمكن أن يحصل عليها بحكم الحاجة الملحة إلى إجراء تغيير في نمط الحياة والسلوك العام ، ومن دون إدراك نوع التوظيف ونوع المعلومات التي يحصل عليها المتلقي ، وهو ما يحدث قطعاً اختراق في أمن المجتمع والدولة .

وقد عُدت هذه الثورة من طليعة التغييرات في الخطط الأمنية وفي آلة الحرب الحديثة بعد أن خرقت مفهوم الأمن القومي ، الأمر الذي يعطي أثرا سلبيا من خلال جعل الأمن وحدود الدول مرهونة بالعلاقات الحميمة والتعاون المشترك نحو تأمين هذه الحدود من الإختراق المتبادل .

وفي هذا الصدد يمكن القول أنه ليس باستطاعة أية دولة بمفردها ولا حتى أقوى دولة في العالم أن تزعم بأنها قادرة أن تحمي مواطنيها في ظل هذا التطور المعلوماتي الرقمي الدقيق ضمن صناعة الآلة العسكرية ومنظومة وسائل الإتصالات الحديثة والمنظومات الإستخباراتية والتجسس ، وأن تستخدم القدرات التدميرية بما فيها أسلحة الدمار الشامل⁽³⁾ . وفي مجال إستخدام المعلوماتية الرقمية للأغراض

⁽²⁾ أنظر: حسن الشريف، البلاد العربية وثورة الإلكترونيات الدقيقة، من كتاب (العرب وثورة المعلومات

(مجموعة باحثين) ط1 (مركز دراسات الوحدة العربية ، بيروت ، 2005) ص ص 87 - 88 .

⁽³⁾ أنظر: كتاب إيفان لوارد ضمن طروحاته للأفكار الموافقة لظاهرة العولمة:

التدميرية والإرهابية عبر اختراق المواقع الإلكترونية، لم يعد أمام الفرد ولا المجتمع تلك القدرة بأن يتطلع في البحث عن أمن متوافر ولا حتى الدول يمكن أن توفر لمواطنيها ولا بالتحالف مع دول أخرى، كون أن المسألة تحتاج إلى أمن داخلي ضمن منظومة مشتركة بين الدولة والمواطن ضمن أمن حقيقي وفاعل يخلق حالة من الحرص الشديد من لدن المواطن تجاه المجتمع وضمن آلية تحقيق ما يُعرف بالأمن الشامل لعموم البشرية .

وعموما يمكن للإرهاب المعلوماتي أن يتمثل في استخدام الموارد المعلوماتية، والمتمثلة في شبكات المعلومات وأجهزة الكمبيوتر وشبكة الانترنت، من اجل أغراض التخويف أو الإرغام لأغراض سياسية. ويرتبط هذا النوع من الإرهاب إلى حد كبير بالمستوى المتقدم جدا لتكنولوجيا المعلومات والذي باتت تلعبه في كافة مجالات الحياة ، إذ يمكن أن يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية وتعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها أو اختراق النظام المصرفي أو إرباك حركة الطيران المدني أو شل محطات الطاقة الكبرى.

وبادئا ذي بدأ لا بد من تعريف اصطلاح الإرهاب من منظور الاتفاقيات الدولية والإقليمية التي بذلت جهودا حثيثة لتحديد ملامح هذا الاصطلاح ، من حيث مظاهره ومخاطره ، فضلا عن دور وجهود أهل العلم ومُشرعي القوانين الجنائية الوطنية التي وضعت بعض من تعاريف هذا المصطلح الذي يصطدم باختلافات وجهات النظر وتباينات الاتجاهات من حيث العقائد والإيديولوجيات

والمصالح التي تبرر أي فعل إرهابي عن غيره من الأفعال بذات التأثير والنتائج ، إذ ما يراه البعض إرهاباً ، قد يراه الآخرون عملاً مشروعاً ومبرراً . ويعرف القانون المصري الإرهاب على أنه " استخدام القوة أو العنف أو التهديد أو الترويع الذي يلجأ إليه الجاني لتنفيذ مشروعه الإجرامي بمفرده أو مع جماعة بهدف الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر، فضلاً عن تعريض البيئة والبنى التحتية (مواصلات، إتصالات، أموال، مباني، أملاك عامة، أملاك خاصة) لخطر التدمير والاستيلاء عليها فضلاً عن الإضرار بدور العبادة ومؤسسات العلم والمعرفة في المجتمع ، ومنع أو عرقلة ممارسة السلطات العامة دورها ومن دون أن تؤدي أعمالها مع تعطيل عمل الدستور والقوانين واللوائح العامة.." (4).

كما عرف مجمع البحوث الإسلامية بالأزهر الإرهاب على أنه "ترويع الآمنين وتدمير مصالحهم ومقومات حياتهم والإعتداء على أموالهم وأعراضهم وحرقاتهم وكراماتهم بغياً وإفساداً في الأرض" (5). وعرف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي، ظاهرة الإرهاب بكل أشكاله على أنه "عدوان وتهديد وتخويف وأضرار مادي ومعنوي صادر عن أفراد، جماعات ودول على حياة الإنسان في دينه ونفسه وعرضه وعقله وماله بغير حق وبشتى صنوف العدوان

(4) للمزيد أرجع إلى : د. عبدالله بن عبدالعزيز بن فهد العجلان ، الإرهاب الإلكتروني في عصر المعلومات (بحث من ضمن بحوث المؤتمر الدولي الأول حول حماية امن المعلومات ، القاهرة ، يونيو 2008) ص2-4 .

(5) أرجع إلى : بيان مجمع البحوث الإسلامية بالأزهر بشأن اصطلاح ظاهرة الإرهاب (القاهرة في الحادي من نوفمبر - 2001) والموافق 15 / 8 / هـ 1422 .

وصور الإفساد في الأرض⁽⁶⁾ . في حين كان تعريف الاتفاقية الدولية لمكافحة الإرهاب المعقودة في جنيف في العام 1973 على أن الإرهاب فعل إجرامي موجه ضد إحدى الدول ، وهدفه إثارة الفرع والرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة⁽⁷⁾ .

وعرفت الاتفاقية العربية لمكافحة الإرهاب في الفقرة الثانية من المادة الأولى الإرهاب بأنه " هو كل فعل من أفعال العنف أو التهديد به أيا كانت بواعثه أو أغراضه ، يقع تنفيذًا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، ويُعرض حياته (حريتهم أو أمنهم) للخطر، فضلا عن إلحاق الضرر بالبيئة أو بإحدى المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعرض أحد الموارد الوطنية للخطر"⁽⁸⁾.

وعرف الإتحاد الأوروبي بعد العام 2002 الإرهاب على أنه " عمل إجرامي هدفه ترويع الناس أو إجبار الحكومات أو الهيئات الدولية على القيام بعمل أو الامتناع عن القيام به أو تدمير الهياكل الأساسية ، سواء السياسية ، الدستورية ، الاقتصادية والاجتماعية للدولة أو الهيئة وزعزعة استقرارها"⁽⁸⁾.

⁽⁶⁾ أرجع إلى بيان مكة المكرمة الصادر عن المجمع الفقه الإسلامي التابع إلى منظمة المؤتمر الإسلامي في دورته السادسة عشر (مكة المكرمة) والموافق في 15/ ينابر من العام 2002 والمصادف 10/26-21 هـ 1422 .

⁽⁷⁾ صحيفة الرياض ، (العدد ، 114335 ، الأحد ، 11 / 9 / هـ 1428) ص 5 .

⁽⁸⁾ محمد محمد الألفي ، العوامل الفاعلة في انتشار جرائم الإرهاب عبر الانترنت ، بحث منشور ضمن أعمال المؤتمر الدولي الأول حول حماية امن المعلومات والخصوصية في قانون الإنترنت ، القاهرة ، 2-4 يونيو 2008 ، ص 3 .

⁽⁸⁾ نقلًا عن : عبدالله بن عبدالعزيز العجلان ، الإرهاب الإلكتروني في عصر المعلومات ، المصدر السابق ، ص ص 11-12 .

ومن مجمل هذه التعاريف والاصطلاحات نلاحظ عدم وجود معنى واضح أو محدد لهذه الظاهرة ، وهو ما جعل هذا الاصطلاح يخضع للإزدواجية والانتقائية في تبرير الحدث بالفعل ورد الفعل ومما فتح باب الاجتهادات في التأويل والتفسير ومما لا شك فيه انعكست وبشكلٍ سلبي على ردود أفعال المنظمات والحركات الإرهابية لإستغلال هذا التضارب بوجهات النظر والمعتقدات والاتجاهات الإيديولوجية ، الأمر الذي سبب نكسات إنسانية إضطهدت على أثرها الشعوب وأزهقت الأرواح وانتهكت الحقوق وخرقت القوانين تحت دعوى أو مسمى وستار مكافحة الإرهاب .

وفي هذا الجانب لم تتوان المجتمعات العربية و الإسلامية في التعبير عن المواقف المضادة من الفعل الإرهابي الإجرامي وذلك من خلال الدعوات الجادة إلى التعاون والتضامن مع المجتمع الدولي لوضع مصطلح محدد لهذا المتغير الخطير .. وكما نص عليه البيان الختامي الصادر عن الدورة التاسعة لوزراء الخارجية للدول العربية والإسلامية المنعقد في الدوحة في العاشر من أكتوبر من العام 2001 وتحت رعاية منظمة المؤتمر الإسلامي⁽⁹⁾.

ومن خلال ما سبق من إصطلاحات في معنى ومضمون الإرهاب فإن الإرهاب الإلكتروني هو معنى مشتق في ظل توظيف الإمكانيات والقدرات المادية وطاقات المعلومات الإلكترونية الواسعة النطاق ودون حدود ، إذ أن الإرهاب الإلكتروني يعتمد الإمكانيات العلمية والفنية من خلال إستغلال الإتصال والشبكات

⁽⁹⁾ وذلك انطلاقاً من مضامين وأهداف منظمة المؤتمر الإسلامي في مكافحة الإرهاب الدولي ، إذ أكد المؤتمر استعداد دولة في المساهمة الفاعلة والجادة وضمن الجهود الدولية وتحت مظلة الأمم المتحدة في وضع مفهوم محدد وشامل لظاهرة الإرهاب وبمختلف أشكاله دون انتقائية وإزدواجية مع معالجة أسبابه وإجتناؤه من جذوره غاية في تحقيق الأمن والاستقرار الدوليين . أنظر عبدالله بن عبد العزيز العجلان ، المصدر السابق ، ص 13 .

المعلوماتية من أجل ترويع وتهديد وتخويف الآخرين وإلحاق الأذى والضرر بهم لتحقيق الغايات غير المشروعة ودون قيم ولا عرف إنساني وأخلاقي ولا وازع دين..

وظاهرة الإرهاب الرقمي (الإلكتروني) ، هو نوع آخر من الإرهاب يرتبط بالتطور المعلوماتي والتقني من خلال استخدام أجهزة الحاسوب الآلي وشبكات الإتصال والإنترنت لإغراض التخريب والتهدم وبث ثقافات العنف والرعب..⁽¹⁰⁾. إن هذا النوع من الإرهاب الحديث يتم فيه نشر الأفكار والمعتقدات ومن ثم التخطيط والتجهيز للعمليات الإرهابية ، ثم التنسيق والتبادل بالمعلومات وكشف مواقع تعليم صناعة المتفجرات والألغام والأسلحة الكيماوية الفتاكة ، فضلا عن طرق وآليات اختراق وتدمير المواقع والبيانات والنظم المعلوماتية ودخول المواقع المحجوبة وأعمال التجسس وطرق نشر الفيروسات مع مواقع تهدف إلى شن حملات نفسية على الدول ولجتمعات بهدف الترويع والتخويف ، كإظهار الأسرى والرهائن وصور بشعة في إعداماتهم...⁽¹¹⁾

الثاني: الإرهاب الإلكتروني : الخصائص والأسباب

يتضمن سلوك الإرهاب الرقمي جملة من الخصائص وجملة من الأسباب الجوهرية والتي تعد من قبيل المبررات للقيام بالأعمال الإرهابية عبر الوسائل التقنية

⁽¹⁰⁾ أرجع إلى بحث د. عبد الرحمن بن عبد الله السندي، وسائل الإرهاب الإلكتروني ، كذلك كتاب "، الطبعة الثانية ، 2003 وعلى الموقع الإلكتروني

Business information systems:

<http://www.identitytheftprotect.us/identity-theftprotection-why.ipg>

⁽¹¹⁾ أنظر : الموقع الإلكتروني السابق .

والمعلوماتية المتطورة في ظل إستخدام الحاسب الآلي وبأعلى درجات السرية في اختراق النظم الأمنية والدفاعية للدول والمؤسسات ..

1- خصائص الإرهاب الإلكتروني أو الرقمي

إن أبرز خصائص هذا المتغير الخطير هي :

أ- إن الإرهاب الرقمي أو الإلكتروني لا يعترف بالحدود الدولية أو النطاقات الإقليمية .

ب- لا يمكن كشف جرائم الإرهاب الرقمي ، كونه متغير يتلون بلون التقنيات المتطورة الخارقة لحدود الأجهزة الأمنية والوقائية ، من حيث طريقة تعقبها أو مراقبتها ..

ج- إن هذا النوع من الإرهاب لا يحتاج اصطدام من خلال القوة والعنف واستعدادات المواجهة العضلية والآلية ، بل يحتاج الجاني إلى حاسوب آلي وشبكات معلوماتية (انترنت وبرامج معدة لهذا الغرض) ..

د- إن المجرم في حقل الإرهاب الرقمي يكون على درجة عالية جداً من المعرفة في مجال الحاسبات والبرمجيات وتفريخ البيانات والدخول على المواقع ورصد المعلومات.

هـ سهولة إتلاف الجاني لأي عمل إرهابي إلكتروني بمجرد تدمير المعلومات بعد الاستفادة منها ومن دون حالة إثبات أو أدلة جنائية .

و- يمكن أن ينفذ الإرهاب الإلكتروني من خلال فرد أو جماعة لتحقيق ذات التأثير في الحدث الإرهابي ..

ز- إن التقنيات والمعلوماتية في حقول العلم والمعرفة لا يمكن أن تكون هدف مشبوه من قبل جهات حكومية وأمنية ، وعلى أنها مصدر من مصادر الإرهاب ،

وهو ما يُعطي لهذه الظاهرة الجو الملائم لتحقيق الأغراض الإجرامية ضد الأهداف المحددة .

2- أسباب ودوافع الإرهاب الإلكتروني

إن أسباب ودوافع الإرهاب الإلكتروني متنوعة بالنسبة للجماعات والمنظمات الإرهابية ، وهذه الأسباب تكون متشابكة ومتداخلة مع الجوانب السلوكية والشخصية والفكرية والسياسية والاقتصادية والاجتماعية ، كون أن ظاهرة الإرهاب وبكل أشكالها وبما فيها الإرهاب الرقمي معقدة ولها مبرراتها ودوافعها ومنها أسباب عامة وأخرى خاصة.

ومن الأسباب العامة للإرهاب الرقمي ، هو اختلاف الاتجاهات الفكرية والظروف الاقتصادية والبيئية التي تحيط بالمجتمعات الدولية والإقليمية ، فضلا عن الجوانب الدينية والاجتماعية والعقائدية والعشائرية وبحسب تكوين هذا المجتمع أو ذاك ونشأته ، فما يدور في حياة مجتمع ما من مقومات وأصول اجتماعية وقيمية هي مختلفة بالتأكيد عما يدور في حياة مجتمعات أخرى ، ولذلك ستتعدد الدوافع وتختلف النوايا ضمن هذا المتغير الخطير . ولعل من أبرز هذه الأسباب هي الدوافع الشخصية كالرغبة في الظهور والشهرة والغنى والانتقام وانعكاس سلوكياته على صفة العمل العدواني كالحسد والحقد الدفين والغيرة القاتلة بالتدمير والتخريب⁽¹²⁾ .

(12) كما أن حالة الإحباط في تحقيق النجاح والشعور دوما بالفشل والنكوص ، هو ما يجعل البعض من ضعفاء النفوس من أن يجنح للعمل الإرهابي ، وذلك باستخدام أخطر الوسائل الممكنة ومنها التقنية الإلكترونية بمواصفاتها المتطورة . أرجع إلى : عبدالله بن عبدالعزيز العجلان ، الإرهاب الإلكتروني في عصر المعلوماتية ، مصدر سبق ذكره ..

ومن دوافع الإرهاب الرقمي ، الفشل المعيشي وحالة الفقر المدقع وعدم تحقيق الفرد في مجتمع ما أي طموحات كان يتمناها دوما ، ويبقى يعيش في دائرة الحرمان والشعور بالنقص إلى درجة البغض والكراهية للآخرين من المتنعمين والمتفوقين والبارزين والناجحين في حياتهم وإلى حدود الانتقام منهم وتدمير حياتهم . كما تبرز دوافع أخرى للإرهاب الرقمي وهي **الدوافع الفكرية** الناجمة عن الفراغ الفكري والجهل بقواعد الدين الحنيف وآدابه وسلوكه والسير على نهج الرسول الكريم (صلى الله عليه وسلم) وآل بيته الطاهرين العظام وجميع المسلمين ممن هم قدوة حسنة للمجتمع الإسلامي . أما في المجتمعات غير الإسلامية سواء على الكتب السماوية أم غيرها فلا يمنعها الخلق القويم واحترام الأعراف القانونية والإنسانية من تحقيق ذات الغرض من الالتزام والاحترام المتبادل ، فالأديان جميعها تشترك بمضامين الحب والعدالة والإنصاف والتعاون وكل ما له صلة بالشعور الإنساني المشترك لا فوارق بين مذهب وآخر أو ملة وأخرى ، فإن أكرم الناس عند الله أتقاهم بالعمل الصالح والتسلح بالأخلاق والقيم النبيلة .. وفضلا عن ذلك يعد الغلو بالفكر إلى درجة التطرف (الراديكالية) والشذوذ عن الحدود المسموح بها غير مقبول شرعا وقانونا .

ولعل الانقسامات والتناحرات الفكرية بين التيارات والأحزاب في مجتمع ما هي الأخرى ستولد مثل هذا الفعل الإجرامي وبشتى الطرق الحديثة والمتاحة ضمن الوسائل الإلكترونية كجهد ووقت مختزلين .

وتأتي **الدوافع السياسية والإقتصادية والإجتماعية** هي الأخرى مؤثرة في تحفيز الفعل الإرهابي ، وذلك من خلال السياسات غير العادلة والظلم والفقر والكبت وتهميش المواطنين وتغييبهم عن المشاركة السياسية ، فضلا عن المساس بحقوق الإنسان وعدم تفعيل دور مؤسسات المجتمع المدني وعدم ظهور الشفافية الكافية

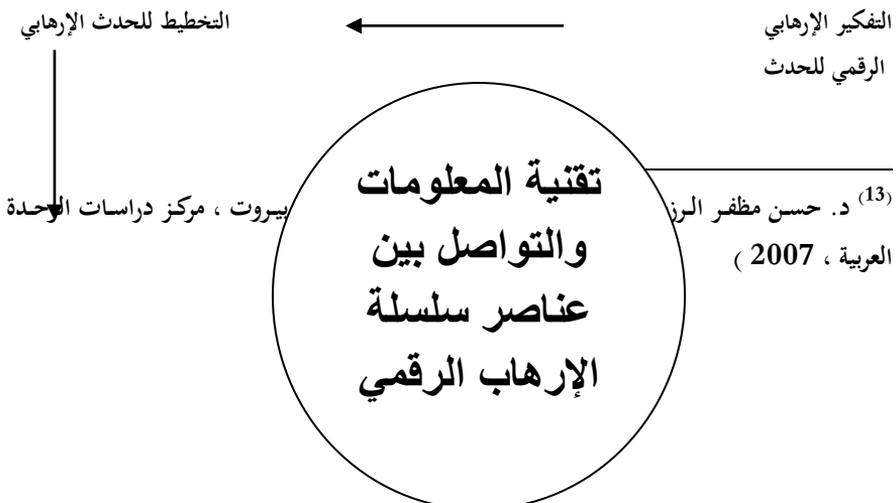
في رفع الحواجز بين الدولة والمجتمع لتبدو السياسة أكثر قبولاً وثقة جماهيرية في جو ديمقراطي عام ، إذ أن غياب الديمقراطية وحرية الرأي في التعبير والمشاركة ، من شأنه أن يولد الحركات والمنظمات السرية وردود الأفعال الغاضبة من أجل التغيير ليكون الفعل الإرهابي أحد أبرز الخيارات لتحقيق هذا الغرض .

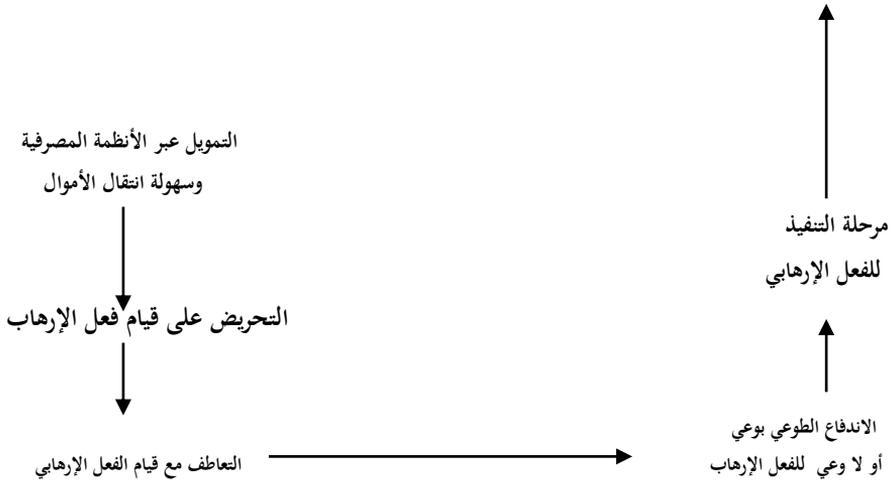
إن غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروة الوطنية وانتشار العاطلين عن العمل وحالة العوز ، فضلاً عن تفاوت مستويات الدخل إلى درجة توليد الطبقة بين فقير وغني وما بين فاسد مستغل وحاسد محبط متمرد ستولد عوامل الانحراف نحو امتهان الجريمة والسرقة والتهديد والخطف للحصول على المال اليسير ، وهذا سيؤهل المجرم في الانحراف ضمن صفوف التنظيمات الإرهابية لتوظيفه بأجر مقابل تحقيق أغراضها المعادية للدولة والمجتمع ومهدده لأمنه واستقراره⁽¹³⁾ .

لقد ساهمت التطورات التقنية والمعلوماتية في توظيف هذه الدوافع المتنوعة بسلوكياتها واتجاهاتها ومن خلال توفير أجواء العمل الإرهابي وعبر سلسلة عناصر الإرهاب المترابطة ما بين التفكير الإرهابي ومستوى التنفيذ للحدث الإرهابي . أنظر المخطط ...

(مخطط يوضح سلسلة الإرهاب الرقمي أو الإلكتروني)

Electronic terrorist series





أما فيما يتعلق بالأسباب والدوافع الخاصة ، فإنها تتضمن:

أ- ضعف الهيكل الخدمي للشبكات المعلوماتية في الدولة والذي يساعد المنظمات الإرهابية بإختراق أي ثغرة وممارسة العمل التخريبي .

ب- إنعدام فاعلية الحدود الجغرافية في ظل تطور المعلومات الرقمية ، وهو ما يؤدي إلى عدم معرفة أو وضوح هوية المستخدم للمعلومات وضمن بيئة مفتوحة ، وهذا يُعد جوا آمنا لمخترق الحاسوب من الإرهابيين من أن يقدر نفسه بالهوية أو الصفة التي يرغب بها ، إذ يتخفى تحت شخصية وهمية ليشن هجومه الإلكتروني بشكل منعزل ومن دون أن يتعرض إلى مخاطر مباشرة⁽¹⁴⁾ .

ج- سهولة الاستخدام مع انخفاض الجهد والكلفة والوقت

د- وجود الفراغات القانونية والأمنية وغياب جهة السيطرة أو الرقابة على الشبكات المعلوماتية . إذ أن الجرائم المعلوماتية تحت مسمى الإرهاب الإلكتروني يمكن أن تنطلق من أي بلد في العالم لا يوجد فيه قانون صارم

⁽¹⁴⁾ أرجع إلى عبدالله بن عبد العزيز العجلان ، المصدر السابق .

ليحقق الغرض بعد أن يشن هجوم إرهابي على بلد آمن فيه قوانين صارمة ، وهو ما يؤدي إلى بروز مشكلة في كيفية تطبيق القانون التجريبي المتكامل لتطويق الجرائم عبر المعلومات الرقمية ، فضلا عن عدم وجود مركزية أمنية موحدة ، يمكن أن تتحكم بالشبكة الإلكترونية وتسيطر على مدخلاتها ومخرجاتها ، الأمر الذي يُعطي حرية واسعة لمجرمي الإرهاب الرقمي في تحقيق الحدث الإرهابي قبل وصول الجهات الأمنية إليهم .

3- الآثار الاقتصادية المحتملة لفعل الإرهاب الإلكتروني

تبرز الآثار الاقتصادية والناجمة عن الفعل الإرهابي عبر منظومة وشبكات الحاسوب والإنترنت ، ولعل من أبرزها خطورة هي :

أ- البطالة :

وتؤدي هذه الآثار إلى توقع المزيد من الانخفاض في الإنفاق الاستهلاكي ، انخفاض في معدلات الإنفاق الاستثماري ، اتجاه الاقتصاد صوب المزيد من التباطؤ في النمو ، مع العديد من المشاكل السياسية والاجتماعية المتداخلة . وقد ارتفعت معدلات البطالة في مختلف بلدان العالم ومنها المتقدمة على وجه الخصوص ، إذ أن هناك ملايين العاطلين عن العمل كنتيجة للكساد وانخفاض الأداء الاقتصادي ، فضلا عن ظاهرة الأزمات المالية والاقتصادية التي تغزو دول الغرب الرأسمالي (أنظر جدول 1)

جدول (1)

النسب المئوية لمعدلات البطالة في دول متقدمة من العالم الرأسمالي

(2001 - 2003)

مايين العام

ت	المناطق الاقتصادية	2001	2002	2003
1	منطقة اليورو	%8.00	%8.3	%8.8

2	الولايات المتحدة الأمريكية	4.8%	5.8%	6.2%
3	اليابان	5.00%	5.4%	5.5%
4	ألمانيا	7.8%	8.2%	8.8%
5	فرنسا	8.6%	8.8%	9.00%
6	المملكة المتحدة	5.1%	5.2%	5.4%
7	كندا	7.2%	7.6%	7.6%

المصادر المعتمدة في الجدول :

1- إحصاءات الصندوق لعام 2001

2- صندوق النقد الدولي ن الآفاق الاقتصادية العالمية ، ابريل \ 2003

أما على المستوى القطاعي ، فقد تم تسريح لآلاف من العمال في قطاع النقل الجوي وحده في الأسبوع الأول بعد أحداث واشنطن ونيويورك \ 2001 . فقد أعلن عن الاستغناء عن ثلاثين ألف موظف يمثلون ثلث العاملين في قطاع تصنيع الطائرات المدنية لشركة الـ Air bas ،⁽¹⁵⁾ . كما توقع حينذاك " جوردون بيتون " رئيس شركة كونتيننتال أن يفقد ما بين 100 - 200 ألف موظف يعملون بشركات الطيران وظائفهم بسبب أحداث سبتمبر وتداعياتها ، فضلا عن توقع عدد من المحللين أن تتجاوز خسائر قطاع النقل في الولايات المتحدة الأمريكية مبلغ سبعة عشر مليار دولار،⁽¹⁶⁾ .

وقد ذكرت وزارة العمل الأمريكية في ذلك الوقت، أن قطاع التصنيع وحده قد فقد 2,6 مليون وظيفة خلال العامين اللذين تليا هجمات الحادي عشر من سبتمبر⁽¹⁷⁾ .

⁽¹⁵⁾ أنظر : أيمن محروس ، الآثار الاقتصادية لهجمات سبتمبر ، على الموقع الإلكتروني لصحيفة

الإسلام اليوم www.islamtoday.net

⁽¹⁶⁾ أرجع إلى: هشام محمد الحرك، بداية النهاية لطغاة العالم ، على شبكة الأنباء المعلوماتية:

www.annabaa.org

⁽¹⁷⁾ ارتفاع معدلات البطالة في الولايات المتحدة ، أرجع إلى موقع هيئة الإذاعة البريطانية ،

ب- حالة الركود أو التضخم

إن الاستقرار السياسي والاقتصادي يزيد من فاعلية الطلب كنتيجة لزيادة الإنفاق الاستهلاكي، وهذا ينتج عنه ارتفاع في المستوى العام للأسعار يكون أحيانا في النطاق المقبول اقتصاديا، وهنا يكون لهذا الارتفاع آثار إيجابية على حفز الاستثمار وزيادة التوظيف، وحين يصبح التضخم عالي نسبيا، فإنه سينتج آثار سلبية في الاقتصاد وعلى المستوى المعيشي العام للمجتمع،⁽¹⁸⁾ ولكن في حالات انعدام الأمن أو زيادة المخاوف فإن الطلب يتضاءل ويترتب على ذلك ركود في الأسواق وكساد في الطلب على المنتجات.. وعلى العموم فإن التضخم تبعا للوضع السياسي الدولي والمستوى الاقتصادي العام للدولة التي يمكن أن تواجه انتشار الإرهاب الرقمي، والذي قد يؤثر بوتيرة نسبية متفاوتة وبحسب درجة تركيز حالة عدم الاستقرار الناجم عن هذا النوع من الإرهاب في حال بث الدعاية المغرضة وفي إمكانية الشروع بالتهديد للمواقع الاقتصادية المهمة في الدولة، فضلا عن ترويج لبعض من مصادر العنف والعنف المضاد وفي مناطق مختلفة من العالم... (انظر جدول 2)

جدول (2) معدلات التضخم مقاسة بأسعار المستهلكين

خلال الفترة (2001-2003 م) (%)

2003	2002	2001	المنطقة الاقتصادية الاتحاد الأوروبي
2.00	2.3	2.5	

www.bbcarabic.com/html3\7\2003

(18) هناك العديد من الآثار الناجمة عن التضخم، لعل من أبرزها: إعادة توزيع الثروة والدخل بين أفراد المجتمع، وسوء توزيع الموارد بين القطاعات المختلفة... أرجع المصدر السابق على الرابط

الإلكتروني: www.bbcarabic.com/html3\7\2003

2.00	2.3	2.6	منطقة اليورو
1.8	1.00	1.9	الاقتصادات الآسيوية الصناعية الجديدة
9.4	11.1	16.3	دول التحول الاقتصادي
5.8	5.4	5.8	الدول النامية

المصدر :

1- إحصاءات الصندوق لعام 2001

2- صندوق النقد الدولي ، الآفاق الاقتصادية العالمية ، ابريل \ 2003

جـ الآثار على الاستثمار

ومما تقدم في هذا المحور يمكن أن نستنتج أن العمليات الإرهابية ومن خلال أجهزة الحاسوب وشبكات المعلوماتية ، تهدف إلى تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية وتعطيلها عن العمل بعد أن تحدث ضرر كبير بالبناء المعلوماتي التحتي ..

فقد انخفضت تدفقات الاستثمار الأجنبي المباشر في العام 2002م بنحو (537) مليار دولار، أي ما نسبته 27% عن مستواها في العام 2001م ، كما شهدت الولايات المتحدة الأمريكية وبريطانيا النسبة الأكبر من هذا الانخفاض إذ أوضحت إحصائية لوزارة التجارة الأمريكية في 26 يونيو/ 2003 من أن الاستثمارات الأجنبية الإجمالية قد تراجعت للعام الثاني علي التوالي* وبنسبة تزيد على النصف، وهو ما يؤكد تراجع إجمالي الاستثمارات العالمية في الولايات المتحدة إلى نحو 64% ، وبقيمة تقدر بنحو (147) مليار دولار أمريكي، كما ذكرت الإحصائية من أن التراجع في الإنفاق الاستثماري يمكن أن يعود إلى عدد من الأسباب المتشابهة منها:

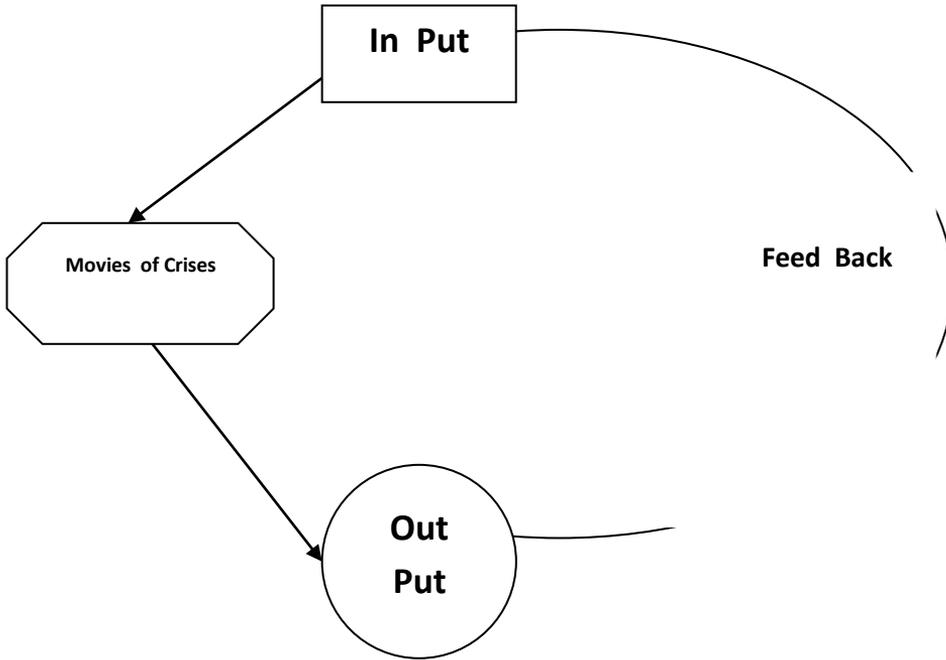
* تقرير صندوق النقد الدولي حول الآفاق الاقتصادية العالمية | أبريل \ 2003

التشاؤم وسيادة حالة عدم اليقين في أوساط المستثمرين الناتجة في المرحلة التي أعقبت أحداث الحادي عشر من سبتمبر وانعكاس ذلك على الكثير من قرارات الاستثمار سلبا .. كذلك تكرر الأزمات الاقتصادية والمالية في الاقتصاد الأمريكي ، يضاف لها ضعف الأداء في أسواق المال من خلال تراجع عمليات الاندماج والشراء في مختلف أسواق العالم ، وتراجع وتباطؤ معدلات النمو الاقتصادي العالمي، ثم انخفاض أسعار الأسهم في معظم أسواق المال العالمية .. إذ يتضح مما سبق أن الحقيقية الاستثمارية في معظم أسواق المال تتعرض إلى فوضى من سلسلة التراجع غير المنتظم في أسعار المتداول من الأسهم للعديد من الشركات التي ربما تعد ساحة أو جزء ممن يتعرض للتهديدات الإرهابية عبر شبكات منظومة الإنترنت بدوافع اقتصادية أو سياسية ، أو صبغة عداوية تدعمها قوى إقليمية أو دولية ذات غايات ومبررات عدة ...

الثالث : المتاح في كيفية إدارة وسائل الاتصال الرقمي لمواجهة الفعل الإرهابي

إن الربط ما بين موضوع إدارة الأزمات باستخدام وسائل الإتصال الرقمي وإدارة الفعل الإرهابي تعد حالة معكوسة ، كون أن الأولى هي رد فعل على الفعل الإرهابي باستخدام ذات الوسائل . ولذلك ترتقي مستويات المعلوماتية في هكذا توظيف إلى أعلى درجات الدقة والحسابات من خلال تخطيط منهجي مبرمج . وفي هذا الجانب يتبين أن النظام الإتصالي من خلال درجة المعلوماتية الرقمية ومستوياتها ، يعطي خطوة متقدمة في منهجية إدارة الأزمة وضمن ما يُعرف بمنهج نظم الأزمة كنظام متكامل يتضمن أربع عناصر تحوي : مدخلات الأزمة - نظام تشغيل الأزمة - مخرجات الأزمة والتغذية العكسية . **أنظر المخطط**

(يوضح توفر آلية نظام التشغيل الاتصالي في إدارة المرشد للحدث الإرهابي)



وفي ضوء المخطط أعلاه يمكن تقسيم إدارة الحدث الإرهابي أو أية أزمة من خلال مراحل ومستويات أربع⁽¹⁹⁾:

⁽¹⁹⁾ أرجع إلى: د. حنان يوسف ، الفضائيات العربية وإدارة الأزمة ، من كتاب (الفضائيات العربية ومتغيرات العصر) (ضمن أعمال المؤتمر العلمي الأول للأكاديمية الدولية لعلوم الإعلام) ، الدار المصرية اللبنانية ، القاهرة ، ط1 ، 2002 ، ص 293 .

- 1- مرحلة ما قبل حدوث الأزمة أو الحدث الإرهابي ، وتعتمد على قدرة القيادة في إستشراف واستكشاف كل الاحتمالات والمتغيرات التي قد ينجم عن الحدث .
 - 2- مرحلة بداية الأزمة ، والتي تتطلب احتواء ومواجهة تعتمد أساساً كفاءة وحجم المعلوماتية المتوفرة والقدرة على تحديد الأولويات ، فضلاً عن الإختيار الدقيق للبدائل الأفضل من جملة البدائل .
 - 3- مرحلة تأزم الحدث أو إنفجار الأزمة ، وعندها لا يستطيع صانع القرار السيطرة عليها ، مما يحدث إرباكاً في بيئة الأزمة دون أن يتيح فرصة لتنمية العلاقات مع العالم الخارجي .
 - 4- مرحلة إنحسار الأزمة Fading of Crises بعد تلاشي مسببات الحدث والعودة نحو مستوى التوازن لما قبل الحدث، ومن خلال شفافية التعامل مع المعلومات المتاحة للنظم الرقمية لمنع حالة الإختراق من جديد ، وعدم إتاحة فرصة التدهور مرة أخرى ، والإبقاء على الوضع الراهن ضمن مستوى يشابه حالة ما قبل حدوث الكارثة .
- وثمة إشكالية تواجه إدارة الأزمة الناجمة عن الحدث الإرهابي ، قد يتبعها تأثيرات أخرى ناجمة عن عمل اتصالي مضاد ، وهو ما يخلق حالة عن عدم توازن ما بين حدوث الكارثة ونتائجها ، وطرق حلها وفقاً لما ترتبت عليه الحالة المتحققة من الفعل الإرهابي .
- فالمسألة لا تتعدى عن كونها مجرد استعداد ووقاية من الحدث وإهمال المراحل الأخرى لاسيما مرحلة استعادة النشاط والوعي المتكامل لأي رد فعل آخر يمكن أن يعزز الحدث الأول وبخاصة أن قنوات التوصيل أو الموقف الإتصالي لدى

الإرهابيين مستمر من خلال المعلومات السمعية والمرئية التي تعطي تفاصيل الحدث بدقة وبحسابات العد التصاعدي لإعلان نقطة الصفر في العملية الإرهابية . وتبقى مرحلة رد الفعل ، هي أن يُخشى ظهور آثار مقصودة وتداعيات غير مطلوبة عبر وسائل علاجية سريعة ضمن منظومة الاتصال الرقمي ، فتؤدي إلى زيادة الشعور بالخطر والإحباط لدى الجمهور، من جراء سؤ الفهم للذعر المتولد عن الأزمة ، وكانعكاس لحالة الصدمة الناجمة عن الكارثة ، وهو ما يضاعف من حدود القلق وعدم الاستقرار كرد فعل نفسي ناجم عن الحالة الذعرية التي تتطلب التعديل والترشيد في السلوك الاتصالي عن منهجية المكون المعرفي Cognitive component لامتناس نتائج الكارثة .

إن الهدف الأساس من الهجمات الإلكترونية تدمير ثلاث اتجاهات وهي ؛ الأهداف الأمنية والسياسية والاقتصادية ، إذ تمثل هذه الأهداف مركز القيادة والتحكم الأمني في المؤسسات الإقتصادية والخدمات كقطاع الكهرباء والماء وتدمير أسواق المال وبالمحصلة تهديد حياة الشعوب وإخضاعهم لإرادة المنظمات الإرهابية . كما أن طرق تدمير المواقع تتم من خلال الدخول غير المشروع على نقطة إرتباط أساسية وثانوية ترتبط بالشبكات المعلوماتية وعبر نظام آلي (Server-pc) أو مجموعة نظم شبكية متصلة (Internet) بهدف تخريب ذلك الاتصال أو النظام⁽²⁰⁾.

كما أن قرصنة الحاسوب الآلي (Hackers) تستطيع من التوصل إلى معلومات سرية وخاصة جدا بسبب الإلمام الكبير والخبرة الواسعة في مجال الحواسيب ، وأن اختراق المواقع يتم من خلال شفرات ورموز خاصة يستخدمها المخترق من أي مكان في العالم دون حاجة إلى وجوده داخل الدولة التي يتم اختراق موقعها . كما ويمكن أن يحدث هجوم إرهاب إلكتروني على مواقع حيوية من خلال شبكات معلوماتية وإلحاق الضرر

(20) د. عبدالله بن عبدالعزيز العجلان ، المصدر السابق .

بما بعد شل حركتها ، كما هو الحال شل حركة أنظمة القيادة والسيطرة والاتصالات ومحطات توليد الطاقة الكهربائية وشبكات المياه ومواقع أسواق المال وبما يعكس سلبا على البناء التحتي للمجتمع مسبا آثار تدميرية تفوق ما تحدته الصواريخ والقنابل المستخدمة بواسطة الطائرات..

المحور الثالث: الإرهاب الإلكتروني الوجه الغاضب والخطر الخارق في توظيف المعلوماتية الرقمية

إن النظام العالمي الجديد يقودنا إلى تفسير منطقي يتناسب مع وقائع الأحداث تحت مظلة ظاهرة العولمة والموجة العلمية والتقنية الثالثة والاندماج القسري للأسواق ونظم النقل والإتصالات وبدرجة متعارف عليها من قبل أو من خلال طريقة التعامل بين الدول كشرركات وأفراد ومصالح بشكل أسرع وأعمق وبمستويات من الكلفة والجهد والوقت أقل بكثير مما كانت عليه الأوضاع في المرحلة التي سبقت أحداث الحادي عشر من سبتمبر / 2001 .

ويرى "توماس فيردمان" في كتابه (العالم في عصر الإرهاب) أن هناك ثلاثة أسس متداخلة ومؤثرة في بعضها البعض يمكن أن تفسر تحولات النظام العالمي الجديد في عصر الإرهاب ، فما بين الأساس الأول الحالة التقليدية للدولة- الأمة في ظل القطب الأوحده ، وهي تفرض على سائر دول العالم سلطتها في أن تتماثل بدرجة أو بأخرى مع سلوكها السياسي والأمني وهو ما نتج عنه خلل في موازين القوة وتضارب المصالح ، يتداخل الأساس الثاني متمثلا بظاهرة العولمة بين كيان الدولة- الأمة والسوق العالمية* من خلال دائرة القطيع الإلكتروني الذي

* لها من التأثير الجبار على كيان الدولة والمجتمع إلى درجة إسقاط الحكومات ، من خلال قدرة المعلوماتية الرقمية وتحكمها في أسواق وبورصات المال . وما حدث في اندونيسيا في العام 1997 وإخراج سوهارتو من دفة الحكم ، جاء كنتيجة لسحب الثقة ما بين الأسواق العملاقة وبين

يحكم مركز كيان الدولة ما بين مراكز الأسواق ومحيطها العالمي كما في ، وول ستريت ، هونغ كونغ ، لندن فرانكفورت وأسواق أخرى عملاقة...فإن الأساس الثالث ، يتعلق بقدرة الأسلحة الإلكترونية وتوسع نطاق الإنترنت وذلك من خلال إزالة الحواجز ما بين الأفراد والجماعات في إطار كيان الدولة ، إذ لم يعد هناك ما يربط الأمن المباشر بين الدولة والمجتمع عبر منظومة المعلومات الرقمية⁽²¹⁾ . وهكذا... يقول "فيردمان" اليوم ليس لدينا قطب عالمي أحادي واقتصادي كوني متداخل ، بل لدينا منظومة أشخاص يتعاملون مع المعلومات الرقمية يسمون (بدوي النفوذ الخارق) بعضهم ذا نفوذ غاضب وسيء (ويقصد بهم الإرهابيون) في توظيف المعلوماتية والبعض الآخر ذوي نوايا حسنة⁽²²⁾ .

فعندما أعلن أسامة بن لادن الحرب على الولايات المتحدة بتفجير سفارتيها في تنزانيا وكينيا ، قام سلاح الجو الأمريكي بقصف صاروخي لأحد معسكراته في أفغانستان ، وبناء على معلومات عالية الدقة ، قد وصلت إلى CIA من إحدى العلماء في مجال المعلوماتية وتدعى "جودي ويليامز" الحائزة على جائزة نوبل للسلام في العام 1997 ، ومن خلال استخدامها البريد الإلكتروني والدخول الخارق على

الحكومة الإندونيسية وتخليها عن دعمها اقتصاديا ، إذ لم يكن الأمر سياسيا بحتاً بقدر ما كان تأثير لسياسات اقتصادية سلبية قد أثرت سلبا على الوضع السياسي العام لإندونيسيا .

⁽²¹⁾ أنظر : توماس فيردمان في كتابه العالم في عصر الإرهاب كمدخل للحدث الأكبر

Thomas.L.Friedmann:: The World In The Age of Terrorism , Longitudes and Attitudes, Copyright© ,Köln–Germany ,2006, pp 12–13

⁽²²⁾ I Bid , p13 .

مواقع الكترونية للحصول على معلومات سرية ، وهو جزء من قدرات بشرية على توظيف هذا النوع من التقنيات لفتح شفرات المواقع على البريد الإلكتروني⁽²³⁾ .

إن أحداث 11/سبتمبر /2001 جاءت كإعكاس لتوظيف قدرات معلوماتية متطورة ، سواء كانت بتخطيط أمريكي مسبق ضمن غايات كامنة أم بفعل تنظيم القاعدة ، وكما أعلن أسامة بن لادن وقتذاك مسؤوليته عن الحدث ، وقد لا يتعدى ذلك عن كونه موقف لهذا التنظيم ، وكرد على الاتهامات الموجهة لهم⁽²⁴⁾ من قبل الإدارة الأمريكية حول ضلوعهم في الأحداث الدامية في واشنطن ونيويورك. وبعد رد الفعل الأمريكي على الحدث في إطار الإدراك الإستراتيجي وخلق مبررات أزمة دولية تحقق من خلالها الولايات المتحدة المكاسب وتعزيز للمصالح في الخارج ، بعد تحشيد جهود المجتمع الدولي في إطار الحدث ، وعلى أن ما تقوم به الولايات المتحدة من منظورها ، هو الدفاع المشروع عن النفس من خلال استخدام مبادئ وشروط الضربة الإستباقية ضمن القانون الدولي، وهو يدخل أيضا ضمن خاصية النفوذ الخارق وكأحد أساليب CIA في رسم صورة مشوهة للعدو وهو الإسلام الراديكالي تحت مسمى الإرهاب ..

فالإستراتيجية الأمريكية في مواجهة الفعل الإرهابي قد أظهرت مفهوما جديدا ليس بالضرورة أن يتفق مع أي مفهوم آخر يمكن تفسيره من قبل أطراف أخرى

(23) I Bid , p14 .

(24) وهو ما يعني أن تغيير موقف أبن لادن، هو كرد على ما وجه ضد تنظيمه من اتهامات بأبأن الحدث، وهو يعد قلب للمقولة (كلمة حق يراد بها باطل) لتصبح (كلمة باطل يراد بها حق) فليس هناك من مخرج إلا بهذا التحدي... أنظر د. عبدالصمد سعدون الشمري، الإرهاب الدولي: المعنى والمضمون في الإستراتيجية الأمريكية، مجلة قضايا سياسية، كلية العلوم السياسية/ جامعة النهدين (العدد11، المجلد3، خريف 2006،ص29.

على أنه إرهاب، ولكي يعطيها حق المشاركة مع رد الفعل الأمريكي تجاه الحدث أو أي حدث إرهابي قادم مستقبلاً (25).

إذ اتضح فيما بعد أن الحدث كان مخططاً ضمن رؤية إستراتيجية في الحرب على الإرهاب وفق عقيدة عسكرية لمحاربة العدو عن بعد وفي عقر داره باستخدام أحدث الوسائل التقنية والمعلوماتية والرقمية عبر منظومة الاتصال السمعي والمرئي كشبكات الانترنت والنقل كأدوات تسخر لخدمة الأغراض الإستخبارية وكمعلومات متدفقة لم تعد سرية بالمعنى التقليدي ، طالما أن مبدأ النفوذ الخارق قد حط على المواقع الإلكترونية بهدف الحصول على المعلومات المطلوبة وفي إطار الحلقة الإلكترونية من التوظيف السريع والقليل الكلفة والجهد .

أولاً: الحلول المقترحة في مواجهه الوجه الغائب للإرهاب الرقمي

إن مشكلة اختراق نظم الحاسوب وإحداث الفعل الإرهابي يتم عبر دخول الجاني لحدار الحماية (فايروول) وخدمات الشبكة ثم التمكن من أنظمة التشغيل لضرب بيانات أية مؤسسة مستهدفة على الموقع بعد أخذ نسخة من ملفاتها السرية وهذا الاختراق ناجم أساساً عن وجود فجوة أمنية في النظام المعلوماتي ، سواء كان حكومي أم خاص، وهذا يأتي عادة بسبب عدم وجود نظام معلوماتي كامل لمراقبة ما يجري على المواقع الإلكترونية (Information security life cycle) وتتم مثل هذه المراقبة عبر أربعة مراحل وهي :

- 1- تقييم الوضع الأمني للتطبيقات كمستوى أول للشبكات الإلكترونية
- 2- مراقبة أنظمة التشغيل وقواعد البيانات وخدمات الشبكات ومن خلال استخدام برامج عالية المستوى وقادرة على اكتشاف نقاط الضعف عند تلك المستويات لتصدر تقارير فورية أحداها للإدارة العليا وأخرى للإدارة الفنية

(25) أيمن السيد عبدالوهاب، تحولات السياسة الأمريكية تجاه القوى الأسيوية بعد أحداث 11 سبتمبر 2001، مجلة السياسة الدولية ن العدد 47، السنة 38 ن كانون الثاني، 2002، ص 81.

يوضح من خلالها الآلية والكيفية الأمنية التي تتم فيها درأ الأخطار وسد الفجوات الأمنية المتوقعة⁽²⁶⁾.

3- إستخدام أفضل التقنيات المتوافرة في العالم كبرامج لمنع الاختراق أو تنشيفات ومضادات الفيروسات - Anti virus and Anti Alter an .

4- تدريب العامل البشري على نمط الخطة الأمنية لضمان التأمين الإداري والفني ، لتكون لديه القدرة على المتابعة وحماية المنشآت والمؤسسات باستخدام منظومة المعلومات الحديثة من أي اختراق في المستقبل .

وهناك طرق وأساليب أخرى لحماية تقنيات المعلومات من الإرهاب الإلكتروني ومنها :⁽²⁷⁾

أ- ضرورة التأكد من أن سياسة الدفاع والأمن الوطني ، تسير على خطى أمنية متكاملة National Security Complimenting of policy .

ب- تعزيز أنظمة المراقبة والتحكم بالأمن المادي من خلال التأكد من الهوية وصفة الدخول والخروج

ج- ضرورة الاعتماد على مركز للطوارئ Emergency center ، كمراكز بديلة لمراكز الحاسوب والمعلوماتية وفي القطاعين العام والخاص ..

د- أن تكون هناك ركائز أساسية لتحقيق أمن المعلومات كالسرية في العمل The Confidentiality of work والجاهزية أو الاستعداد لمواجهة

⁽²⁶⁾ ويتم التركيز في الحلول المقترحة لمواجهة أي اختراق إرهابي رقمي على السياسات ، وليس بالضرورة على التقنيات التي سيأتي الاستعانة بها لاحقا مع ضرورة التركيز على وجوب الترابط بين خطوات التقييم والتصميم والتنفيذ والإدارة من خلال نظم الجودة العالمية . للمزيد حول سبل الحلول المقترحة في مواجهة الإرهاب الرقمي أرجع إلى بحث منشور بهذا الخصوص في صحيفة الشرق الأوسط ، العدد 8372 (الثلاثاء ، 12 / شعبان/هـ 1422- الموافق 30 / أكتوبر / 2001) ص ص 1-2 .

⁽²⁷⁾ أرجع إلى : د. محمد المتولي ن التخطيط الإستراتيجي في مكافحة الإرهاب الإلكتروني ، ط 1 (الكويت ، مطبعة جامعة الكويت ، 2006) ، ص 45 .

الخطر وتكامل المعلومات Integrity of information ، فضلا عن تطبيق برامج مكافحة الفيروسات وأنظمة كشف الإختراقات وأنظمة التشفير وتدقيق المعلومات الداخلة ومراجعتها بصورة مستمرة للتأكد من هويتها ومصدرها..

الثاني: تعزيز منظومة الدفاع والأمن الوطني أمام احتمالات الإرهاب الرقمي
 يمكن استخدام تقنية المعلومات بشكل مضاى لما يستخدمه الإرهابيون على شبكات الإنترنت ، وذلك من خلال التوظيف المعاكس لأجهزة تقنية متطورة ومجربة تقوم بضبط المعلومات الواردة والصادرة عبر مواقع الإنترنت ، على اعتبار أن صفة التجسس عبر الحاسوب الإلكتروني مستمرة ، لذا يمكن رصدها بأجهزة متخصصة لضبط الشفرات والرموز الكودية غير المشفرة (المفتوحة)، أو مفاتيح الإرسال والإستقبال.

كما أن اعتماد وسائل التطور التقني كأنظمة وبرامج التشغيل وقواعد البيانات ووحدات التخزين عبر الحاسب الإلكتروني المتطور مع إمكانية توسيع نطاق شبكات الإنترنت في كل وحدات المؤسسة الأمنية والمدنية، يُعد حالة متطورة في حسابات تعزيز الدفاع والأمن الوطني.

لذلك نرى أن جميع الدول وفي مختلف نطاقات هذا العالم ممن تستخدم الإنترنت بنسبة عالية وترفع معدلات إنفاقها على تطوير التقنيات الإلكترونية من مجمل ناتجها القومي ، يرتفع فيها مؤشرات العمل الدفاعي ومنظومات الأمن الوطني ضد المخاطر التي تتأتى عبر الأنترنت، رغم أن هذا المؤشر قد يقابله ارتفاع في مؤشرات الإرهاب الإلكتروني، إذ أن درجة مخاطره هي الأخرى تتوقف على متغيرات أخرى منها مسألة الديمقراطية، قضايا حقوق الإنسان، إرهاب الدولة، مستوى الفقر والعدالة التوزيعية للموارد الإقتصادية وعوامل أخرى تعد حافزا لهذا السلوك الشاذ والمنحرف.

ونلاحظ في جنوب وشرق آسيا ومجمل دول أوروبا، أن مستويات استخدام التقنية الإلكترونية، هي أعلى نطاقا وأكثر تطورا من أمريكا اللاتينية وأفريقيا، لذا يرتفع لديها الحس الأمني الإلكتروني في مواجهة القرصنة الإلكترونيين Hackers وأي هجوم إرهابي محتمل، إلا أنه ومن جانب آخر قد ينخفض الإرهاب الرقمي لدى أفريقيا مثلا لاعتبارات عدم التطور التقني، وعليه يكون الحس الأمني والدفاعي متناسبا مع إمكانيات التقنية المعلوماتية المتواضعة وهكذا.. أنظر الجدول 3

ولما كانت أهداف المواقع الإرهابية نشر الفكر الضال وجمع الأموال وبث الإصدارات التي تهدف إلى تغيير عقول الشباب وتجنيدهم لخدمة أهدافهم الإجرامية، فلا بد للدولة من اعتماد أحدث التقنيات المتطورة وتوظيفها من أجل نشر الوعي بين المواطنين وتثقيفهم بطريقة استخدام مثل هذه التقنيات استخداما أفضل مع ضرورة الاهتمام بالبنية الأساسية لنظام الشبكات المعلوماتية وتطوير التجارة الإلكترونية وعناصرها الأساسية، وإستحداث الهويات الشخصية من خلال استخدام الرموز السرية كما هو الحال في بيئة المفاتيح PK1 وتفعيل مراكز التصديق الرقمي لسهولة التعامل معها وبشفافية عالية. كما لا بد من تفعيل التشريعات القانونية وخاصة ما يتعلق بأمن المعلومات من الواجهة القانونية للمواطن والأجنبي، فضلا عن إنشاء مركز وطني إرشادي لأمن المعلومات والبيانات العامة والخاصة ومركز أمني آخر للمعلومات متخصص باكتشاف التهديدات والإختراقات على النطاقين الإقليمي والدولي. ففي الولايات المتحدة الأمريكية تم اتخاذ ترتيبات أمنية على أعلى المستويات لمواجهة خطر الإرهاب الإلكتروني، بما فيه أسلوب التنصت على مواقع إلكترونية تعد ضمن خطط السبق الأمني للمعلومات قبل الشروع بالعمل الإرهابي أو حدوثه وقد وضعت إجراءات ترتبط بعمل مباشرة بمكتب مستشار الأمن القومي.

وفي هذا الصدد عين الرئيس الأمريكي "باراك أوباما" مستشارا أمنيا في مجال أمن الفضاء الإلكتروني وهو (هوارد شميت) المستشار السابق في إدارة الرئيس الأسبق "جورج

دبليو بوش " بشؤون مكافحة الإرهاب ، إذ يرتبط هذا المنصب مباشرة بالسلطة التنفيذية للرئيس الأمريكي وبشكل منظم⁽²⁸⁾ كما ويُعد مستشار أمن الفضاء الإلكتروني عضواً في مجلس الأمن القومي، إذ ينسق مع الفريق الإقتصادي حول متطلبات توجيه الجهود الرامية الى تعزيز أمن الفضاء الإلكتروني للمحافظة على الأمن الإقتصادي للبلاد وتحقيق إزدهارها.

ومن جانب آخر وضمن إحتياطات أمريكية من إحتتمالات وقوع أحداث إرهابية عبر المواقع الإلكترونية على أهداف ومصالح أمريكية ، والتي قد تنعكس على أزمات سياسية مستقبلاً قامت الحكومة الأمريكية بإغلاق شبكة " Google " الإلكترونية على الصين في يوم 23 /3 /2010 لإتهامها بالتحسس وضرب مصالح اقتصادية أمريكية داخل الولايات المتحدة..

جدول (3)

النطاق الدولي لمستخدمي الإنترنت ونسبة المستخدم منه عالمياً خلال العام 2007

النطاق الدولي	عدد السكان من مستخدمي الإنترنت في العالم /مليون نسمة	نسبة المستخدم من النطاق إلى المستخدم العالمي
آسيا	409	36%
أوربا	319	28%
أمريكا الشمالية	231	20%
أمريكا اللاتينية	102	9.9%
أفريقيا	33	2.9%
الشرق الأوسط	19	1.6%
أستراليا	19	1.6%

المصدر: جمعت البيانات من المصادر:

(28) وعمل شميث مستشاراً أمنياً لأمن الفضاء الإلكتروني في إدارة جورج بوش ، وهو رئيس لمنظمة " منتدى امن المعلومات " غير الربحية ، إذ يمتلك شميث خبرة أربعة عقود في مجالات الأعمال وتطبيق القانون وواحد من أهم المراجع في أمن الإنترنت . للمزيد أرجع الى الموقع الإلكتروني لصحيفة الإقتصادية الإلكترونية حول مقال " أوباما يعين منسقا أمنياً لأمن الفضاء الإلكتروني.. العدد 5917 ، بتاريخ 23 /12 /2009 ، ص 1 .

- 1- تقرير صندوق النقد الدولي (IMF) لعام 2007 (حول إحصاءات لعدد السكان المستخدم للإنترنت).
- 2- إحصاءات منظمة التجارة العالمية (WTO) لعام 2007 حول مستخدمي الإنترنت على نطاقات مختلفة من العالم.

ويستنتج من كل ما تقدم أنه بإمكان الجيل القادم أن يحدث ثورة في مجال الأعمال والأنشطة المعلوماتية ضمن تشكيلة ابتكارات وإبداعات أكثر اتساعا وقوة وبأقل نشاط ممكن ، مما سيؤدي حتما إلى جعل المؤسسات الكبرى أكثر لا مركزية من السابق أمام تفاقم دور الأفراد والجماعات التي تزداد قوة يوما بعد يوم ، وهو ما سيؤثر بطبيعة الحال على تراتبية السلطة الحكومية من حيث مستوى تعاملها مع المجتمع ودرجة الحذر المتوقع من وقوع الأزمات ، وبخاصة في بيئة مليئة بالعبارات ، كاللص الآلي أو أن هويتي الشخصية اقل تعريفا بي من المعلومات المخزونة عني في الحاسوب أو أن الانترنت يمكن أن يجعلك أذكى ولكن لا يجعلك ذكيا بكل تأكيد، وكل ذلك يعطي دليلا قاطعا على تطور العالم إلى درجة فك الارتباط ما بين أمن السلطة في المجتمع وحماية الحدود السيادية وبين أمن المعلوماتية الرقمية العابرة للحدود والتي لا يمكن لأحد أن يوقفها أو مراقبتها على أنها قد تشكل تهديدا حقيقيا عبر استخدامها من قبل أناس من ذوي النفوذ الخارق لتحقيق أهداف إرهابية وتدميرية واسعة النطاق والى درجة تسبب الإضرار المفاجئ بأمن بالدولة والمجتمع على حد سواء.

التوصيات المقترحة

إن التطور الكبير الذي تحدثه الثورة المعلوماتية الرقمية في العالم ، قد ساهم في إتاحة فرص واسعة وإستغلال غير محدود لأجهزة الحاسوب الإلكتروني عبر منظومة الإنترنت، وظهرت على أثرها المنظمات والحركات الإرهابية التي تستهدف المجتمعات الآمنة والمستقرة ببث الرعب والترويع، فضلا عن تدمير الحياة الإقتصادية والإجتماعية لمختلف شعوب الأرض، فكان لا بد من مواجهة فاعلة لهذا الإرهاب

العصري الخطير من خلال توسيع نطاق شبكات المعلوماتية المضادة للفعل الإرهابي المعلوماتي المدمر، وذلك من خلال تطوير البرامج والنظم المعلوماتية وترسيخ آلية الأمن المعلوماتي.. وأن ذلك يتطلب جملة من التوصيات لتعزيز هذا المسار ، كونه يشكل تعزيز لأرضية صلبة لمواجهة الخطر الذي يتهدد بالمجتمعات وينال من حريتها وأمنها واستقرارها ولعل من هذه التوصيات:

1-دراسة أسباب الإرهاب دراسة مستفيضة وتحليل سلوكه الإجرامي وبخاصة ما يتعلق بالأفكار التكفيرية التي تسيء إلى الدين وتشوه من خلق الإنسان ورسالته في الحياة.

2-القيام بتأهيل الكوادر البشرية المتخصصة في مجال الحاسبات الإلكترونية إلى مستويات عالية ، والاستفادة منها في حقل الأمن المعلوماتي.

3- تزويد المختبرات ومراكز الحاسوب والإنترنت بأدلة إلكترونية لغرض تحليلها والتحقق منها لغرض تعزيز سبل الدفاع والحد من مخاطرها مستقبلا.

4-ضرورة تعزيز التعاون والتنسيق بين جميع الأجهزة الأمنية المختصة لتحقيق الهدف بأقل الخسائر الممكنة المادية منها والبشرية.

5-متابعة الشبكات الإرهابية من خلال تتبعها عن طريق رصد المواقع الإلكترونية باستخدام أفضل التقنيات الحديثة، كما ويمكن من خلال هذا الإجراء التبليغ الفوري عن أي نشاط إرهابي قبل وقوعه..

5-تشجيع حقل البحث العلمي ومراكز الدراسات والبحوث المختصة في مجال تطوير أمن المعلومات وبصورة مستمرة، وذلك من خلال دعم ميزانية البحث العلمي وتقديم الحوافز المادية والمعنوية لجميع الكوادر المتخصصة ضمن مؤسسات التعليم العالي سواء الجامعات أو المعاهد العليا.

6- ضرورة نشر الوعي الديني والأخلاقي والأمني بين المواطنين عبر الحلقات التثقيفية والإرشادية والدورات التدريبية والتأهيلية، فضلا عن تشجيع فرص الاستثمار ضمن حقل التقنيات المعلوماتية، لجعل هذا الحقل رافدا مرتبطا بالاقتصاد المعرفي ومنه تطوير القطاعات الأخرى، ومن خلال التنسيق ما بين العنصر التقني الوطني وبين الاستعانة ببعض الخبرات والاستشارات الأجنبية في مجال التقدم الإلكتروني والمعلوماتي، من أجل بناء قاعدة بيانات رصينة من الأداء والتطور وفي مختلف الحقول والمجالات التنموية..