حوار الأسبوع

حوار مع الدكتور المصطفى الرزرازي المتخصص في الدراسات الاستراتيجية

على المغرب التصدي للإرهاب المعلوماتي

يشتغل الدكتور الرزرازي في مجال الدراسات الإستراتيجية وإدارة الأزمات، وبوجه خاص دائرة التحديات غير التقليدية كقضايا الإرهاب المعلوماتي، وقضايا بناء الرأي العام وقياس اتجاهاته.

فقد أشرف على تأسيس أول مختبر علمي للدراسات السيبرية (Cyber Studies) باليابان، وأنجز عددا من البحوث والدراسات بالولايات المتحدة الأمريكية واليابان حول نشاط الجماعات الإرهابية داخل الإنترنت.وما يميز بحوث الرزرازي في هذا المجال نظرته الشمولية التي تعتمد على أحدث مناهج البحث في مجال الدراسات الأمنية، علاوة على تمرسه في استعمال تقنيات البحث والتحليل النفساني والاجتماعي.

والدكتور الرزرازي، من مواليد 1964، وبدأ حياته المهنية في جريدة "العلم"، وانتقل لمتابعة دراسته الجامعية في اليابان، حيث يقيم منذ أكثر من عشر سنوات، و تقلد عدة مناصب ومسؤوليات جامعية وإعلامية هناك، إضافة إلى نشاطه المركز كخبير في الشؤون السياسية والإستراتيجية سواء باليابان (جامعة طوكيو، جامعة توهوكو، معهد الإثنولوجيا، وجامعة هاجوروموو الدولية)،أو بالولايات المتحدة الأمريكية (جامعة برنستون)، أو بالعالم العربي (مركز الإمارات للدراسات الإستراتيجية التابع للقيادة العامة للأركان) . علاوة على مساهماته الإعلامية المكتوبة والسمعية البصرية باليابان(قناة الجزيرة، القناة اليابانية الوطنية، قناة أساهي، إذاعة ماينيتشي و جريدة أساهي.)

ونحاوره في هذا العدد لنستعرض معه بعض القضايا المتعلقة . بالإرهاب المعلوماتي وتداعياته على منطقة العالم العربي والمغرب خاصة.

أجز الحوار : **عبد الكامل العيساوي**

■ س : ماهي المساحات المعلوماتية التي تؤطر علميا التفكير في الإرهاب المعلوماتي؟

● ج: إن ظهور الإنترنت كوسيلة لا مركزية للتواصل عبر الحاسوب كان محل ترحيب من قبل العديد من الناس بما انه حافز قوي للتبادل اللامحدود لآراء الشخصية. إذ منذ سنوات تكونها وبغض النظر عن المسافة والحدود السياسية فإن اي شخص على الشبكة اصبح بإمكانه الإتصال باي إنسان آخر على الشبكة وهو طليق من الرقابة المركزية ويتناول مواضيع تحدد بإهتماماته الشخصية وفي أوقات يتم وضعها حسب رغبة كل طرف وما يناسبه. وقد مكنت الشبكة العالمية الشركات والمنظمات السياسية والمجموعات الخاصة وكذلك الافراد من إنشاء هيئات مخصصة تسهر على [illegible] وإسماعها واقناع العديد من الناس من اتباع إهتماماتهم من بين الطبقات الخاصة للشبكة العالمية المتعلقة بعملية الراي العام هو المدى الذي يحتكم فيه للمواقع التي يتم تركيزها من قبل منظمات الاخبار والشركات الخاصة والوكالات الحكومية وحتى الافراد وذلك في وقت الأزمات.

■ س: إذا كان عالم الإنترنت مفتوحا بهذا القدر الذي تصفه، فماهي قدرة القانون على ضبط آليات العمل المعلوماتي؟

● ج: في هذا السياق يمكن ان نلاحظ ان الوكالات الحكومية وجماعات الضغط قد واجهت صعوبات في مراقبة التحرك عبر الإنترنت. بعض هذه الصعوبات تتعلق مباشرة بالتصرف الإقتصادي في الثروة الوطنية مثل الضرائب والمنافسة ومواجهة الدعاية أو صعوبات سياسية محضة لها علاقة بالصراع السياسي بين المؤسسات في المستوى الوطني والإقليمي والعالمي. هنا تتصدر الجرائم السيبرانية والإرهاب السيبرائي إهتمام وكالات الامن وبدات تظهر الأصوات المنادية بالحد من السماح للعموم بالدخول إلى المواقع السيبرانية. ويمكن إعتبار كل ذلك كجزء من ظاهرة العولمة المولودة حديثا. لا انوي إعطاء بسطة واسعة حول "جرائم الحاسوب" كما لا انوي إصدار بيان يدعو إلى تشريع جديد. إن ما يعنيني هو إمكانية القول إن القوانين المعمول بها يمكن الا تكون ملائمة لعالم الفضاءات السيبرانية. ليس بالضرورة ان الفضاءات السيبرانية تتطلب قوانين جديدة وإنما الاكثر من ذلك ان الجرائم في الفضاءات السيبرانية تستلزم شخصا ليصيغ الأعمال الإجرامية في ضوء مختلف لأن "المشاكل" مع الجرائم السيبرانية لا يمكن حلها بمجرد نقل قوانين الإجرام التي سنت لعالمنا المادي إلى الإنترنت والفضاءات السيبرانية. وكذلك لا يمكن ترك الفرصة لرجال الدولة لإستغلال تعلة العمل ضد الإرهاب للحد من الحقوق المكتسبة في الفضاءات المادية والإفتراضية. في وقت قريب كانت ردة فعل العديد من المؤسسات السياسية سلبية حيث أقترحت حق التدخل بما في ذلك الدخول إلى البريد الإلكتروني والخاص بعامة الناس او تعطيل الدخول إلى المعلومة.

■ س: لكن هل يمكن لعلومنا ومناهجنا الاجتماعية التقليدية التعاطي مع العالم المعلوماتي تعاملا سليما؟

● ج: من اهم المظاهر الكارثية لدراسات العولمة هي ان العلماء لديهم الحافز للعمل في مجال الإقتصاد والاخلاق العالمية وفي الهندسة لكن قليل منهم من سار في إتجاه البحث في مجال تاثير العولمة على العلوم الإجتماعية والسياسية وبالتالي ترك هذه العلوم خارج عصرها.

للاسف فإن هذه إمكانية لا يريد العديد من الناس البحث فيها ولا يعتقدون أن مثل هذه الدراسة هي ضرورية. إلا ان هذه الدراسة هي ضرورية لانه في المستقبل القريب سنجد حياتنا تتكيف اكثر فاكثر مع الفضاءات السيبرانية. املي ان يتفهم الآخرون في الأوساط القضائية الاهمية لهذه الواسطة الثورية الجديدة. تماما كما تطلبت الثورة الصناعية العديد من التغييرات في انظمتنا القضائية والإقتصادية وكذلك الإبستيمولوجية.

■ س: دعنا نعود إلى الإرهاب المعلوماتي، وماهو تعريفك له، باعتبارك نشرت أكثر من سبع دراسات متخصصة في الموضوع؟

● ج: يعرف الإرهاب السيبراني على انه الإستعمال الغير قانوني للقوة او العنف ضد الأشخاص والممتلكات لإحراج أو إكراه الحكومة أو المدنيين او اي شريحة اخرى وذلك لخدمة اغراض سياسية او إجتماعية. إذن يمكن تعريف الإرهاب السيبراني بانه إستعمال موارد الحاسوب لتخويف وإكراه الآخرين. لكن المغالطة عندنا هو الخلط الموجود بين الجريمة المعلوماتية والحرب المعلوماتية والإرهاب المعلوماتي، وكمثال على المخالفة المعلوماتية يمكن ان نتحدث عن احتمال التسلل إلى نظام الحاسوب بالمستشفى وتغيير الوصفات الطبية لشخص ما إلى مقادير قاتلة كعمل ثاري. يبدو ذلك مستبعدا إلا ان مثل هذه الأشياء يمكن أن تحدث وقد تحدث بالفعل.

فالإرهاب السيبراني او المعلوماتي هو إلتقاء الإرهاب والفضاء السيبرائي وعموما ما يفهم على انه الهجمات الغير قانونية والتهديدات بالهجوم ضد الحواسيب والشبكات والمعلومات المخزنة فهي تنفذ لتخويف وإكراه الحكومة و مرافقها وذلك لتعزيز الأهداف السياسية والإجتماعية. إلى جانب ذلك يمكن وصف هجوم بانه إرهاب سيبرائي عندما يؤدي إلى العنف ضد أشخاص او ممتلكات او على الاقل ان يتسبب في قدر من الضرر من شانه ان يولد خوفا. كما يمكن إعتبار الهجمات التي تؤدي إلى الموت او الجراح الجسدية او الإنفجارات او تحطم الطائرات او تسمم المياه او خسارة إقتصادية كبيرة أمثلة من هذه الجرائم وكذلك الهجمات الخطيرة ضد البنى التحتية الأساسية يمكن إعتبارها ضمن الأعمال السيبرانية الإرهابية وذلك تبعا لنتائجها. اما الهجمات التي تخل بالمصالح الغير اساسية أو تلك التي تسبب بالأساس إزعاجا مكلفا لا يمكن إعتبارها أعمالا إرهابية. إن الفضاءات السيبرانية هي عرضة للهجمات بصفة مستمرة. يدخل الجواسيس واللصوص والمخربون ومحبو الإثارة إلى نظم الحواسيب لسرقة المعلومات الشخصية وأسرار تجارية وتخريب المواقع وتعطيل المصالح وتخريب المعلومات والنظم ونشر فيروسات الحاسوب والديدان والقيام بعمليات غش ومضايقة الأفرد والشركات. هذه الهجمات اصبحت سهلة بفضل القوة المتزايدة للبرامج الإلكترونية وسهولة إستعمالها والتي هي موجودة مجانا على الآلاف من مواقع الإنترنت فالعديد من الهجمات خطيرة ومكلفة إذ الفيروسات بكل أشكالها على سبيل المثال قد اضر بالملايين من المستعملين وتسبب في اضرار تقدر بمليارات الدولارات. إن وقف الخدمات بسبب الهجمات ضد مواقع للتجارة الإلكترونية قد قدرت خسارته بمليارات الدولارات. كما انه هز ثقة رجال الأعمال والأفراد في التجارة الإلكترونية.

■ س: ماهي درجة وعي المغرب باهمية هذه المخاطر الجديدة؟

● ج: الإرهاب السيبراني هو مشكل متعاظم في المجتمع يجب على كل فرد أن يكون واعيا بما يعنيه وبالأخطار التي يمثلها. وعلى الحكومة ان تؤهل دفاعاتها ضد الإرهابيين السيبرانيين بسبب الخطر المتزايد. كذلك ومع ظهور مستعملي البريد الإلكتروني الجدد واللذين يسعون لمحتويات حية أن تنكشف عندما تفتح الرسائل اصبح من الأسهل على الإرهابيين تدمير حواسيب الآخرين بواسطة الفيروسات. فالإرهاب السيبراني هو خطر حقيقي يجب معالجته لا فقط من قبل مختصين في الحاسوب وإنما من قبل أي شخص يستعمل اي نوع من شبكة الحاسوب. لكن دعني اقولها بصراحة، يجب على المسؤولين بالمغرب التعامل مع الموضوع تعاملا جديا، فالتدابير لا تنفع، ولذا يجب خلق مختبر لدراسة كل ظواهر الإرهاب ، من بينها الإرهاب المعلوماتي، وليكن في إحدى الجامعات او ليكن معهدا مستقلا يتولى مسؤولية البحث والتكوين والتدريب المستمر.

الإرهاب الإلكتروني مشكل متعاظم في المجتمع يجب على كل فرد أن يكون واعيا بما يعنيه وبالأخطار التي يمثلها

لقد قدمت مقترحات في الموضوع لعدد من الزملاء واشتغلنا حول برنامج كامل للبحث والتكوين في الموضوع، لكن يبدو ان هناك حسابات غير حسابات تهيئ الوطن بمناعة حقيقية ضد التهديدات غير التقليدية. شخصيا لا ارى فائدة في تكوين اطرنا لمدة اسبوع أو اسبوعين لنقول اننا نؤهل اطرنا واجهزتنا الأمنية ضد الجريمة المعلوماتية. و السبب بسيط فعالم الإنترنت يتغير بسرعة، ويقتضي تتبعا يوميا، وتحليلا يوميا. و لاعطيك مثالا واحدا. لقد قمت عام 2001بإنشاء مختبر علم الإجتماع المعلوماتي بجامعة هاجوروموو باليابان، وكونت فريقا للبحث لدراسة نشاط بعض التنظيمات الدينية على الإنترنت، فاضطررنا إلى عمل مداومة على مدى 24ساعة في اليوم لمدة سنتين، لاجل فهم اليات العمل داخل بعض المواقع الدينية، وسبل عملها، وطبيعة زبائنها، وغير ذلك من الاسئلة التي اقتضت منا جهدا كبيرا، ووسائل عمل متطورة، وقدرة على استثمار كل مناهج البحث السياسي والاجتماعي. وفي المغرب يمكننا ان نخلق مختبرا مماثلا، قد يتحول إلى مركز خبرة وطني وإقليمي يغطي احتياجات البحث والاستشارة والتكوين عربيا وإفريقيا.

الهجمات الإلكترونية قد تخلف أضرارا بمليارات الدولارات

■ س: يتهمكم بعض البيروقراطيين انتم المختصون في مجال ما يسمى بالتهديدات غير التقليدية بانكم تبالغون في تضخيم مخاطر الإرهاب المعلوماتي، هل لك ان تعطينا امثلة او نماذج لإقناع منتقديكم بالعكس؟

● ج: لقد تم تنفيذ بعض الهجمات بغية تحقيق غايات سياسية وإجتماعية كما تبين الأمثلة التالية:

في سنة 1996إدعى احد لصوص الحاسوب إنتسابه لحركة المتفوقين البيض وعطل بصفة وقتية موقع الحركة (SP)البمستاشوسيتس واضر بجزء من نظام السجلات لهذه الحركة. وحاولت الآي أس بي (SP)ان تمنع هذا اللص من إصدار رسائل عنصرية عبر العالم بإسم ال (SP)كما كان اللص يختم رسائله بالتهديد "سوف ترون الإرهاب الإلكتروني الحقيقي. هذا وعد"

في سنة 1998اغرق المحتجون الإسبان معهد التواصل الكوني (IGC) بالآلاف من الرسائل الإلكترونية المزيفة فعطل البريد الإلكتروني بالنسبة لمستخدمي ال SPكما عطلت أيضا خطوط الدعم من قبل الناس الذين لم يتمكنوا من قراءة بريدهم. كما قطع المحتجون حسابات لسلك ال ISP والاعضاء وعطلوا صفحات الواب بانظمة بطاقات إقتراض مزيفة وهددوا بإتباع نفس الخطط ضد المنظمات التي تستفيد من خدمات المعهد. وطالبوا المعهد بوقف إستضافة مواقع الواب لمجلة "اليوسكال هرية Euskel Herria"وهي نشرة مقرها في نيويورك وهي تدعم إستقلال إقليم الباسك ، وقال المحتجون ان هذا المعهد يدعم الإرهاب لان جزءا من صفحات الواب يحتوي على وثائق حول الجماعة الإرهابية إيتا (ETA)التي اعلنت مسؤوليتها حول إغتيال السياسيين الإسبان وضباط الامن وحول الهجمات على المواقع العسكرية. وفي النهاية لين المعهد من موقفه وسحب الموقع بسبب "إغراق البريد"

وفي سنة 1999اغرقت مدغرة التاميل الإثنية السفارات السريلنكية بثمان مئة رسالة إلكترونية في اليوم على إمتداد فترة اسبوعين. وكانت الرسائل تقول "نحن النمور السود للانترنت ونحن نقوم بهذا العمل للإخلال بإتصالاتكم". ووصفت سلطات المخابرات ذلك بانه اول هجوم معلوم من قبل الإرهابيين ضد نظم الحاسوب التابع للبلد.

خلال الحرب في كوسوفو سنة 1999اتهرضت حواسيب الناتو إلى قنابل بالبريد الإلكتروني وإلى هجمات ضد الخدمات المقدمة من قبل لصوص نشطين كإحتجاج على القصف من قبل الناتو. كما افادت بعض التقارير بان بعض مؤسسات الأعمال والمنظمات العمومية والمؤسسات الجامعية قد تلقت بريدا سياسيا مسيسا جدا وملغوم بالفيروس من قبل العديد من دول اروبا الشرقية كما ان طمس مواقع الواب قد اصبح ظاهرة منتشرة. إذ يعد قصف السفارة الصينية في بلغراد عن طريق الخطإ بعث اللصوص الصينيون النشطون برسائل على غرار "سوف لن نتوقف حتى الهجوم حتى تتوقف الحرب" اي الهجوم على مواقع الواب التابعة للحكومة الأمريكية. في حين ان الأحداث المذكورة اعلاه كانت وراء دوافع سياسية وإجتماعية فإن الحكم عليها بانها ضارة او مرعبة بما فيه الكفاية لتصنيفها ضمن الإرهاب السيبراني يبقى محل جدل. على حد علمي لم يؤد اي من هذه الهجمات إلى العنف أو جرح اشخاص بالرغم من ان بعضها قد ارعب ضحاياه. إذ يرى كل من قراصنة الإنترنت وفرسان الحاسوب الجوديين اعمالهم هذه على انها أشكال من العصيان المدني مثلها مثل إحتجاجات الشارع والإعتصامات وليست اعمال عنف او إرهاب. وهذا تمييز مهم . إن معظم الناشطين سواء المشاركين في مسيرة المليون او في الإعتصامات ليسوا إرهابيين. حسب هذا الراي فإن تهديد الإرهاب السيبراني يبقى بالأساس نظري إلا انه شيء يجب مراقبته واخذ الحيطة المعقولة ضده.

ولكي نفهم التهديد الممكن للإرهاب السيبراني يجب الأخذ في الإعتبار عاملين إثنين: الإعتبار الأول ما إذا كانت الأهداف المعرضة للهجمات قابلة إلى أن تؤدي إلى العنف أو الضرر البالغ وأن العامل الثاني ما إذا كان هناك مهاجمون لديهم القدرة والدافع لتنفيذ هذه الهجمات. بالنظر اولا لمسالة الحساسية فقد بينت بعض الدراسات بان بعض البنى التحتية الهامة هي عرضة للهجمات السبرانية الإرهابية. المرشح لتلقي الهجوم هي تجربة "دون إنذار" تم القيام بها من قبل "وزارة الدفاع سنة 1997 بمساعدة فرق الآن أس أي (NSA)الحمر اظهرت في بيانات القوة والطوارئ أن 11انظام لديها هيئات يمكن إستغلالها من قبل المهاجمين فقط بإستعمال الوسائل المتاحة للعموم على الإنترنت. بالرغم من ان اي من هذه الأنظمة لم يتعرض فعلا لهذه الهجمات فإن بعض الأعضاء الدارسين خلصوا إلى مصالح الخدمات على هذه الأنظمة يمكن أن تتعرض للتخريب. كما اصدرت اللجنة الرئاسية الامريكية حول حماية البنى التحتية الحساسة سنة 1997تقريرا يحذر من ان التعامل المشترك والإرتباط يمكن ان يكون ثغرة تكون من خلالها البنى التحتية الحساسة مهددة بطرق جديدة وان القابلية للتهديد تزداد بإستمرار في حين ان تكاليف الهجمات تنخفض. قبل ست سنوات نقل قسم الشرطة الياباني بالعاصمة ان نظام البرامج الإلكترونية لتلقي اثر 150اعربة شرطة بما في ذلك العربات الغير معلمة قد تم تطويرها من قبل طائفة أم شينريكو وهي نفس المجموعة التي إستعملت غاز السالين في انفاق طوكيو سنة 1995 وتمكنت من قتل 12شخصا وجرح 6000اخرين. وعند إكتشاف المجموعة تبين انها كانت تحصلت على معلومات تقفي ل 15اعربة. كما طورت هذه الطائفة برامج إلكترونية ل 80شركة يابانية و 9اوكالات حكومية على الاقل كم انها تعاقدت من الباطن مع شركات أخرى مما يجعل من المستحيل تقريبا على هذه المنظمات ان تعرف من الذي انتج هذه البرامج. وبصفتها متعاقدة من الباطن تكون هذه الطائفة قد ارست احصنة طروادة لشن وتسهيل هجمات سبرانية إرهابية في اوقات لاحقة و حصل نفس القلق لدى السلطات الامريكية ، فبما ان وزارة الخارجية الامريكية بدورها تخاف حصان طروادة فقد بعثت برسائل عاجلة إلى حوالي 170 سفارة تطالبها بالتخلص من البرامج الإلكترونية التي تبين فيما بعد بانها وضعت من قبل مواطنين من الإتحاد السوفياتي سابقا. لو سلمنا بان البنى التحتية الحساسة هي عرضة لهجمات سبرانية إرهابية يبقى السؤال إذن ما إذا كان هناك إرهابيون لديهم القدرة والدافع لتنفيذ مثل هذه العملية في الوقت الذي يتمتع فيه قراصنة الحاسوب بالمعرفة والآليات لمهاجمة انظمة الحاسوب فإنهم على العموم يفتقدون الدافع إلى إحداث العنف او الضرر الإقتصادي او الإجتماعي البالغ. والعكس صحيح إذ ان الإرهابيين الذين لديهم الحافز لممارسة العنف يبدو انهم تنقصهم القدرة او الرغبة لاحداث ذلك القدر من الضرر في الفضاء السبراني.

■ س: هل تستعمل الجماعات الدينية المتشددة التي غالبا ما توصف بالإرهابية تقنيات المعلوميات لتحقيق أهدافها؟

● ج :يستعمل الإرهابيون الفضاء السبراني لتسهيل الأشكال التقليدية للإرهاب مثل الهجوم بالقنابل. إذ ينشئون مواقع الواب لنشر رسائلهم وجلب مناصرين ويستعملون الإنترنت للإتصال وتنسيق اعمالهم. إلا انه هناك دلائل قليلة تفيد بانهم يتبعون الإرهاب السبراني سواء بصفة منفردة او صحبة اعمال العنف المادي. ففي عام 1998 افاد كلارك ستايتن المدير التنفيذي لمعهد اعمال الطوارئ والبحث في شيكاغو أمام اللجنة الفرعية للتكنولوجيا والإرهاب والمعلومات الحكومية التابعة للجنة القضائية بمجلس الشيوخ افاد بانه يعتقد ان "عناصر من بعض المنظمات الإسلامية الإرهابية هي بصدد تطوير "شبكة للقرصنة" لدعم نشاطاتها عبر الحاسوب بل وحتى الضلوع في هجمات عدوانية في المستقبل في إطار حرب المعلومات". وفي وقت لاحق نقلت وكالة الانباء بدبتروبت أن عضوا من مناضلي جماعة حركة الانصار الهندية الإنفصالية قد حاول شراء برامج عسكرية من قراصنة الحاسوب كانوا قد سرقوها من حواسيب وزارة الدفاع بعد ان إقتحموها. كما أن الجيش الجمهوري الإرلندي المؤقت قد إستخدم مصالح القراصنة المتعاقدين لدخول الحواسيب بغية الحصول على العناوين الشخصية لضباط تطبيق القانون والمخابرات إلا ان المعلومات استعملت لوضع خطط لقتل الضباط خلال "ليلة الساكين الطويلة"الواحدة إن لم تخضع الحكومة البريطانية إلى شروط وقف إطلاق النار الجديد. وكما تبين هذه الحالة فإن الإرهابيين يمكن ان يستعملوا القرصنة كطريقة للحصول على معلومات إستخباراتية لدعم العنف المادي حتى وإن لم يستعملوه ليشفوا غليل غضبهم في الفضاء السبراني.

لقد انجزت في وقت سابق دراسة شملت عدة انواع من الجماعات الإرهابية منها الدينية والجيل الجديد (New Age)وزعماء الحركات الإثنية والقومية والإنفصالية والثورية والمتطرفين من اقصى اليمين. ووقع التسليم بان الجماعات الدينية فقط هي التي يمكن ان تبحث على أعلى درجات القدرة على إلحاق الضرر وذلك تماشيا مع ممارسة العنف انغير مقيد. اما العهد الجديد او الإرهابيون ذوو الإهتمام الأوحد مثل جبهة تحرير الحيوان تمثل التهديد المباشر الأكبر إلا ان مثل هذه الجماعات يمكن ان تقبل بالتعطيل كتعويض للتحطيم. اما الثوريون والإنفصاليون القوميون الإثنيون هم على إستعداد للبحث عن قدرة هيكلية متقدمة.

كما ان للإرهاب السبراني مساوئه. فالنظم معقدة لذلك يمكن القول بالتحكم في الهجوم وتحقيق الدرجة المرجوة من الضرر اكثر صعوبة من إستعمال أسلحة مادية. وطالما ان الناس لم يجرحوا فهناك جنوح اقل نحو الإحساس الدرامي والعاطفي. إلى جانب ذلك فإن الإرهابيين قد لا يبدون رغبة في تحديث اساليبهم طالما انهم لم يروا ان اساليبهم القديمة لم تعد صالحة وخاصة عندما تتطلب منهم الأساليب الحديثة المعرفة والمهارة اللازمتين لتحقيقهما على أحسن وجه. فالإرهابيون عموما يحتفظون بالأساليب الحقيقية المجربة. فالتجديد والتعقيد في الهجوم ربما يكون أقل اهمية من التأكيد على نجاح المهمة الإجرائية. إذن فإن خطر فشل العمل الإجرائي يمكن ان يكون رادعا يثني الإرهابيين. لان القنبلة المنقولة الآن تمثل تهديدا اكبر من القنبلة المنطقية.

إن الجيل القادم من الإرهابيين سوف يعيش في عالم رقمي يكون فيه لديهم اليات قرصنة اكثر قوة واسهل إستعمال بكثير. يمكن لهم ان يتوقعوا قوة للإرهاب السبراني اكثر مما يتوقعها إرهابيو اليوم. وسوف يكون مستوى معرفتهم ومهارتهم المتعلقة بالقرصنة اكبر. فالقراصنة والنافذون يمكن إنتدابهم من قبل الإرهابيين وقد يعرضون انفسهم للإنتداب كإرهابيي السبرانية اي تيموثي مكفايز في الفضاء السبراني. وقد يمر البعض منهم إلى الفعل بسبب مسائل السياسات السبرانية ليجعل بذلك من الفضاء السبراني مصدرا جذابا لتنفيذ هجمات . كما ان الإرهاب السبراني قد يصبح أكثر جاذبية بحكم تقارب العالمين الحقيقي والإفتراضي بفضل عدد اكبر من اللواحق المادية المرتبطة بالإنترنت يمكن التحكم في البعض منها عن بعد. فالإرهابيون على سبيل المثال يمكن ان يستهدفوا الإنسان الآلي المستعمل في الجراحة عن بعد إن لم يقع توفير الامن لهذه الأنظمة بصفة جيدة فإن القيام بعملية من شانها أن تدمر شخصا ما ماديا سوف تكون سهلة بالدرجة التي عليها الآن الدخول إلى موقع واب.

■ س: هل هناك مخاطر جانبية لمكافحة الإرهاب المعلوماتي على المجتمع المدني؟

● ج: إن التصيد العنيف لأهداف سياسية بإستعمال طرق إلكترونية صرفة سوف تحدث على الاقل بعد بضع سنوات في المستقبل. إلا أن الخطر العام للجريمة السبرانية هو جزء واقع في العالم الرقمي اليوم. بالإضافة إلى الهجمات السبرانية ضد المعلومات والأنظمة الرقمية فإن العديد من الناس اليوم يتعرضون للترويع عن طريق الإنترنت مع التهديدات بالعنف المادي.

إذ أن فرض المراقبة المتزايدة على الإنترنت من قبل الحكومة بتعلة توفير الأمن او العمل ضد الإرهاب تواجه الكثير من المعارضة بحجة ان هذه الرقابة تخرق حقوق السرية الذاتية للمدنيين وتكرس الرقابة كعمل مسموح به لتستعمله في تعلات أخرى تتعدى مجالات الامن.

61 13 77 66