الفضاء المعلوماتي وإرهاب المستقبل انتقل خطر إرهاب الفضاء المعلوماتي من روايات الخيال العلمي إلى واقع عالمنا المعاصر, كتابا بعنوان (الثلج Dan Verton وأصبحت هناك مخاوف كبيرة من تدمير أنظمتنا المعلوماتية. في عام 2003 أصدر دان فرتون عرض فيه بشكل مثير (Black Ice: The Invisible Threat of Cyber-Terrorism الأسود: التهديد الخفي للإرهاب المعلوماتي لنوع الأخطار التي يمكن أن تهدد العالم في المستقبل القريب, نتيجة احتمال اختراق المنظمات الإرهابية لأنظمة المعلومات المتوافرة لدى الحكومات والمؤسسات المالية والشركات الاقتصادية الكبرى, واستخدامها في تدمير البنية التحتية لأجهزة الكمبيوتر والإنترنت التي تعتمد عليها هذه الحكومات والمؤسسات والشركات في توجيه مختلف أنواع الأنشطة التي تدور حولها الحياة في الدول والمجتمعات المستهدفة. وقد استشهد المؤلف في عرضه لتلك الأخطار بآراء عدد كبير من العسكريين والعلماء ورجال الحكم والسياسة في الولايات المتحدة, كما أورد عددا من الشهادات الحية التي أدلى بها بعض الأفراد الذين اتصلوا بشكل أو بآخر في وقت من الأوقات ببعض الجماعات الإرهابية, وأمكنهم الاطلاع على مدى قدرة هذه الجماعات على الاعتماد على الفضاء المعلوماتي في مهاجمة أنظمة المعلومات في أمريكا بالذات والخسائر الفادحة التي قد تنجم عن هذه الهجمات, كما عرض في الوقت ذاته للأساليب والطرق التي يرى المسئولون عن الأمن القومي أنها كفيلة بالتغلب على هذه الهجمات إن لم يكن التنبؤ بها قبل حدوثها. فضلا عن الجمهور العادي من عامة المثقفين, خاصة, وأن المؤلف كان يعمل في وقت سابق في جهاز المخابرات الأمريكي ويدرك تماما معنى وأبعاد ما يقوله في الكتاب. والواقع أن إمكان استخدام الفضاء المعلوماتي, في شن هجمات إرهابية لتدمير أنظمة المعلومات التي تعتمد عليها الدول المتقدمة في إدارة شئونها السياسية والاقتصادية والاجتماعية, كانت منذ وستيف بيزينيك Tom Clancy الثمانينيات والتسعينيات مصدراً لإثارة خيال عدد من الكتاب والروائيين من أمثال توم كلانسي ولكنها أفلحت في الوقت ذاته في توجيه اهتمام .(Netforce في روايتهما المثيرة المفزعة (قوة الشبكة Steve Pieczennik المسئولين عن الأمن القومي إلى الأبعاد الخطيرة الحقيقية لمثل هذه الهجمات في حالة وقوعها, وهو أمر غير مستبعد. وتدور قصة أحد هذه الأفلام, التي ظهرت منذ أعوام قليلة ـ على سبيل المثال ـ حول استخدام إحدى المنظمات الإرهابية للإنترنت في تدمير أجهزة ونظم التحكم في عدد من محطات توليد القوى النووية, وانصهار أحد المفاعلات النووية, ووقوع كوارث ضخمة وخسائر مادية وبشرية هائلة من جراء هذا الهجوم. وبالرغم من أن القصة كلها من صنع الخيال فقد أخذ المسئولون الأمريكيون المسألة مأخذ الجد ونظروا إلى القصة من زاوية مختلفة تماما وعمدوا إلى دراسة الأخطار المحتملة فيما لو حدث مثل هذا الهجوم بالفعل, وكيف يمكن درء الخطر قبل وقوعه. كذلك ظهرت بعض الكتابات والدراسات الجادة حول إرهاب الفضاء المعلوماتي لعدد من وغيرهما من الكتاب الذين قد لا يكونون John Arquilla وجون أركيلا Winn Schwartau الكتاب من أمثال وين شوارتو معروفين في العالم العربي, ولكن كتاباتهم تلقى كثيرا من الرواج في الخارج على الرغم من أن بعض النقاد يتهمون معظم هذه الكتابات بالمبالغة والمغالاة والبعد عن الواقعية. والرأي الغالب على أية حال يذهب إلى أنه إذا لم يكن مثل هذا الهجوم المدمر قد وقع حتى الآن فإن ذلك لا يمنع من احتمال حدوثه في المستقبل, ولذا ينبغي اتخاذ كل الإجراءات الكفيلة بمنع حدوثه أو التقليل من الخسائر في حالة نجاح إحدى هذه الهجمات.الخطر قائم وقد تكون هناك بالفعل بعض المبالغات من جانب وسائل الإعلام في تركيزها على خطورة إرهاب الفضاء المعلوماتي, وتضخيم حالات نجاح بعض الأفراد في اختراق شبكات المعلومات الخاصة ببعض المؤسسات أو الأفراد الآخرين عن طريق تخليق أنواع من الفيروسات الجديدة التي تسبب كثيرا من الأضرار لأجهزة الكمبيوتر والمعلومات التي يتم تخزينها عليها, واعتبار هذه الاختراقات مقدمة متواضعة لما سوف تكون عليه الهجمات الإرهابية الضارية, التي توجه إلى المؤسسات والأجهزة والإدارات الحيوية في الدول المستهدفة. وثمة من الأمثلة ما قد يستدل منه على إمكان حدوث تلك الهجمات الكبرى التي تسبب خسائر جسيمة يصعب تقديرها بدقة في الوقت الحالي. من ذلك مثلا ما حققته بعض المنظمات الإرهابية في أستراليا عام 2000 من تدمير شبكات الصرف الصحي في إحدى المدن هناك, والأخطار الصحية والاقتصادية الفادحة والخطيرة التي أصابت الأهالي والمؤسسات والأجهزة الحكومية. ومن ذلك أيضا ما حدث في اليابان في مارس عام 2000 حين أعلنت دوائر الشرطة المتروبوليتانية عن أن جماعة آوم شينريكو الإرهابية أفلحت في اختراق نظام البرمجة المتحكم في مسار وأنشطة مائة وخمسين سيارة من سياراتها, بالرغم من أن معظمها لم يكن يحمل أية علامات مميزة, واستطاعت تلك الجماعة أن تتحكم في عمل تلك السيارات وتوجيهها حسب التعليمات التي كانت تصدرها لها, بما يحقق نجاح بعض العمليات الخاصة التي أرادت الجماعة تنفيذها. والمعروف أن هذه المنظمة الإرهابية هي التي ارتكبت عملية إطلاق الغاز السام بمحطة مترو الأنفاق في طوكيو عام 1995, كما أفلحت هذه المنظمة ذاتها في التلاعب بأنظمة الكمبيوتر والإنترنت في أكثر

Summarized by © lakhasly.com

من خمسين شركة من الشركات الكبرى في اليابان, واختراق أنظمة عشر إدارات حكومية وتوجيهها لصالحها الخاص, ولم يتم اكتشاف ذلك الاختراق إلا بعد أن تكبدت الشركات والحكومة خسائر باهظة. وثمة بعض العمليات (الإرهابية) التي لا تخلو من طرافة. مثال ذلك ما حدث عام 1997 لمعهد الاتصال العالمي في سان فرانسيسكو, فقد حدث أن تبنى ذلك المعهد وجهة نظر إقليم الباسك في المطالبة بالانفصال عن أسبانيا, وأصدر بالفعل جريدة على الإنترنت بعنوان (دولة الباسك) يساند فيها تلك الدعوة, وإذا بعشرات الآلاف من الرسائل الإلكترونية تنهمر في وقت واحد ولعدة أيام على المعهد, دون أن يحمل معظمها أي شيء له معنى محدد على الإطلاق, وإنما كان الهدف هو إصابة البريد الإلكتروني للمعهد وبالتالي كل نشاطه بالشلل التام. وأفلحت الخطة بحيث اضطر المعهد إلى التوقف عن إصدار الجريدة وتغيير سياسته إزاء المشكلة. وقد اتهم المعهد الحكومة الأسبانية بأنها وراء ذلك الهجوم (الإرهابي), الذي وصف حينذاك بأنه نوع من (القصف الإلكتروني) تشبيها له بالقصف المدفعي بالقنابل أثناء الحروب.خسائر (أنا أحبك) ويرمي إرهاب الفضاء المعلوماتي إلى تحقيق أهداف سياسية في الأغلب, ولذا فإن عمليات اختراق شبكات الإنترنت التي يقوم بها بعض الأفراد من (الهواة) عن طريق الفيروسات التي يفلحون في تخليقها وإطلاقها دون أن يكون لهم من ورائها أهداف سياسية محددة, لا تدخل في رأي الكثيرين ضمن مفهوم ذلك النوع من الإرهاب على الرغم من كل ما قد تسببه من خسائر فادحة في منظومة المعلومات, وعلى الرغم من إمكان إلحاق الأذى في وقت واحد بعدد كبير جدا من أجهزة الكمبيوتر في مناطق مختلفة ومتباعدة من العالم. فعدد الذين أضيروا من جراء الهجوم على مواقعهم وتخريبها بواسطة الفيروس المعروف باسم I LOVE YOU من بلايين يقدر بأكثر من عشرين مليون مستخدم للإنترنت, كما وصلت الخسائر المادية إلى عدة الدولارات, وهو الأمر الذي قد يصعب تحقيقه على مثل هذا النطاق الواسع من خلال العمليات الإرهابية, التي تتم باستخدام الأسلحة والأساليب التقليدية. وعلى الرغم من فداحة الخسائر فإن الكثيرين لا يعتبرون هذه العملية وأمثالها من أعمال (إرهاب) الفضاء المعلوماتي ويدرجونها بدلا من ذلك تحت ما يطلقون عليه اسم (جرائم) الفضاء المعلوماتي, التي يقوم بها (الهواة) بقصد التسلية في كثير من الأحيان, وحب الاستطلاع والارتياد, حتى وإن نجم عن أفعالهم خسائر مادية وتدمير كثير من المعلومات المهمة أو الحيوية في بعض الأحيان, فضلا عما تسببه من بلبلة وقلق وانزعاج لأناس من الأغراب الذين لا يعرفون عنهم شيئا على الإطلاق. وترتبط فكرة إرهاب الفضاء المعلوماتي بالتطورات التي حدثت في مجتمع المعلومات, وما أثارته خصائص ومقومات هذا المجتمع من جدل ونقاش حول الأخطار المحتمل أن تتعرض لها المجتمعات المعلوماتية الحديثة, والدمار الذي قد يلحقه الهجوم الإرهابي بمنظومة المعلومات التي تتحكم في كل مرافق الحياة في هذه المجتمعات التي تعتمد على الكمبيوتر والإنترنت اعتمادا مطلقا, والخسائر التي قد تنجم عن مثل ذلك الهجوم, فإرهاب الفضاء المعلوماتي يعتمد على القدرة على اختراق شبكات الإنترنت لتحقيق أهداف عدوانية ذات طابع سياسي في الأغلب وإن كان يخلف وراءه آثارا سلبية تنال كثيراً من جوانب الحياة الأخرى. ويتساءل باري كولن Barry Collin من (معهد الأمن والذكاء) بأمريكا عن مستقبل هذا النوع الجديد من الإرهاب. والمعروف أن باري كولن هو المسئول عن وضع اصطلاح إرهاب الفضاء المعلوماتي ـ وهي تسمية ذات دلالة, لأنها تميزه عن الإرهاب العادي أو (التقليدي) الذي يقوم على استخدام (الفضاء الفيزيقي المحسوس) والذي يتمثل هنا في استخدام الأسلحة التقليدية من قنابل ومفرقعات وما إليها, ولا يتردد في أن يعترف بأن هذا الإرهاب المعلوماتي سوف يكون هو إرهاب الغد, نظرا لتعدد وتنوع واتساع مجال الأهداف التي يمكن مهاجمتها مع توفير قدر كبير من السلامة للمهاجمين, وعدم تعرضهم لخطر اكتشاف هوياتهم أو حتى المواقع التي شنوا هجومهم منها, إلا بعد انقضاء كثير من الوقت وبذل كثير من الجهود في البحث الذي قد ينتهي في آخر المطاف إلى لا شيء, وذلك فضلا عن حجم الخسائر الهائلة التي تنجم عن الهجمات المعلوماتية. فتوقف التجارة الإلكترونية مثلا ليوم واحد فقط قد تتسبب عنه خسائر تقدر بستة بلايين ونصف بليون دولار وهكذا. بل وتغيير مواصفات تركيب الأدوية, بكل ما يترتب على ذلك من خسائر في أرواح البشر, بل وقد يمكن لها القضاء تماما على إمكانات أي دولة في توفير الطعام والشراب لسكانها . وغير ذلك كثير. فالكثيرون ينظرون إليها على أنها أمور واردة واحتمالات يمكن تحقيقها بالفعل ودون عناء, وإن كان تنفيذها يحتاج إلى كثير من الدراسة والإعداد والدقة في التخطيط والتنفيذ, مع وجود جهاز كمبيوتر متصل بأي خط إنترنت عن طريق التلفون أو أي وصلة لاسلكية أخرى قد تستخدم تحت اسم مستعار, وقد يميل بعض الكتاب إلى اعتبار إرهاب الفضاء المعلوماتي مجرد (أسطورة), لن تلبث أن تنهار أمام التقدم التكنولوجي, الذي سوف يؤدي بالضرورة إلى ابتكار أساليب ووسائل للحماية من مثل هذه الهجمات. ولكن التقدم في مجال المقاومة والمكافحة, سوف يصاحبه تقدم مماثل في أساليب التغلب على هذه المقاومة والمكافحة وهكذا بشكل مستمر مما يعني أن السباق في التكنولوجيا والتكنولوجيا المضادة ـ إن

Summarized by © lakhasly.com

صحت التسمية ـ سوف يدخل في دائرة مفرغة. والشيء الذي يثير الخوف حقا لدى الكثيرين من المسئولين حول ما قد تصل إليه الأمور في المستقبل, هو أن بعض التقديرات عن الهجمات الإرهابية المعلوماتية على المؤسسات الاقتصادية والمالية الكبرى في العالم وصلت عام 2000 إلى ما يزيد على مائة وثمانين ألف حالة اختراق لأنظمتها المعلوماتية عن طريق الإنترنت, وأن هذه الهجمات والاختراقات تزيد بمعدل 60% سنويا, وأن أحداث التخريب والتدمير تزداد هي أيضا باطراد, مما يضع أعباء مالية ضخمة على الحكومات والمؤسسات لمقاومة هذه الهجمات وإبطال مفعولها. وقد أدى هذا كله إلى ظهور تعبيرات وتسميات جديدة لم يكن لها وجود من قبل, ولكنها تكشف عن مدى خطورة الموقف مثل (حرب المعلومات) أو (حرب الشبكات الدولية) أو وغير ذلك من المصطلحات التي تنم ,(Virtual wars (حرب الكمبيوتر) أو (الإرهاب الرقمي) أو (الحروب المفترضة أو التخييلية عن مدى الفزع, وعن النظرة المتشائمة إلى المستقبل لدرجة أنه سادت في السنوات الأخيرة عبارة (بيرل هاربور الإلكترونية), في إشارة واضحة إلى مدى الدمار والخراب والخسائر التي قد تنجم عن الإرهاب المعلوماتي والهجمات التي يمكن أن تقع في أي لحظة وعلى غير توقع وتأتي من المجهول. والمفارقة الخطيرة والتي تدعو إلى الأسى هنا هي أن الإنترنت التي تؤلف جزءا أساسيا من حياة الإنسان المعاصر وتؤدي من خلال الفضاء المعلوماتي خدمات جليلة لصالح المجتمع, سواء في مجالات التعليم أو الصحة أو السياسة وشئون الحكم أو الاقتصاد والتجارة الإلكترونية, والأهم من هذا كله هو مجال الاتصال والتواصل والتبادل الثقافي والتفاهم بين مختلف الشعوب والثقافات, مما قد يدعم التسامح ويساعد على إقرار السلام. أصبح في الوقت ذاته ومن خلال الفضاء المعلوماتي أيضا أداة خطيرة لتهديد الحياة الإنسانية ونشر الرعب والخراب والدمار, بحيث إن عبارة (إرهاب الفضاء المعلوماتي) لم تعد مجرد مصطلح علمي يتداوله العلماء والأكاديميون والمتخصصون في المعلوماتية وتكنولوجيا الاتصال والمعلومات, وإنما أصبح عبارة متداولة في الصحف اليومية وتتردد بين عامة المثقفين. كما ظهرت حول هذا النوع الجديد من الإرهاب كثير جدا من الكتابات التي تخاطب مختلف المستويات الثقافية في الخارج وكلها تحذر من مخاطر ذلك الإرهاب المدمر الذي (يأتي من المجهول), إذ مع تقدم تكنولوجيا المعلومات وتكنولوجيا الإلكترونيات سوف تزداد الأخطار وتكثر التهديدات, Andrew وتتوالى الأحداث الإرهابية وتتفاقم الخسائر.حرب المستقبل وقد دفع الخوف من إرهاب الفضاء المعلوماتي آندرو راثمل إلى أن يكتب حول هذا الموضوع مقالا بعنوان (إرهاب الفضاء المعلوماتي: شكل صراع المستقبل), نشره في (مجلة Rathmell المعهد الملكي للخدمات المتحدة) ببريطانيا, ذهب فيه إلى أن كل الدلائل المتعلقة بالتطورات التكنولوجية والسوسيو/سياسية تؤكد أن حرب المعلومات ستكون هي حرب المستقبل, وأن ثمة ما يشير إلى إمكان انهيار كل البنى التحتية الخاصة بأنظمة المعلومات في العالم بأسره, وليس فقط في بعض المؤسسات الكبرى أو بعض الدول المستهدفة, وذلك بفعل الهجمات المعلوماتية, التي يتم الإعداد لها بطريقة جيدة والتي تتوخى مهاجمة عدد كبير من الأهداف الحيوية المنتقاة بعناية في مناطق مختلفة من العالم, وبحيث يتم الهجوم عليها كلها في نفس اللحظة. ويرى راثمل أنه إذا كان رجال السياسة والحكم والعسكريون على ثقة من أن حروب المستقبل سوف تعتمد على الفضاء المعلوماتي, ويفخرون بأن هذه الحروب يمكن تحقيق النصر فيها دون إراقة دماء عن طريق الهيمنة المعلوماتية وتدمير المنظومة المعلوماتية لدى الأعداء, وقبل أن ينتبه الطرف المعادي لما يحدث له, فإن من المحتمل ـ من باب أولى ـ أن تلجأ المنظمات الإرهابية إلى هذه الوسيلة التي تضمن لها تحقيق أغراضها المدمرة دون أن يتعرض أعضاؤها للخطر. فالفضاء المعلوماتي سوف يكون في أغلب الظن هو المصدر الأساسي ـ إن لم يكن المصدر الوحيد ـ لانطلاق الحركات ,(الإرهابية في عالم الغد, ولذا فإن ثمة جهودا كثيرة تبذل الآن سواء بشكل علني أو مستتر لتهيئة الأذهان لهذا (الإرهاب الرقمي

Summarized by © lakhasly.com