الفصل الرابع
الإرهـاب الإلكترونـى

ويشمل:

- الإرهاب الإلكترونى.
- ماهية الإرهاب الإلكترونى.
- خطورة الإرهاب الرقمى.
- الحماية من الإرهاب الإلكترونى فى الدول المتقدمة.
- سيناريوهات حروب المعلومات.
- تصاعد الهجمات الإلكترونية.

الوبـاء الإرهابـي كالمـرض السـرطاني، في خبثـه ومقاومتـه للعـلاج، وفي ضـرورة مواجهته بكافة أنواع العلاجات الأمنية والثقافية والدينية، بهدف قطع دابره واجتثاث جذوره، هكذا حال الإرهاب الخبيث في مراوغته واستعصائه على العلاج، ومن ثم تسلله لاصطياد ضحاياه من الشباب الغر، فبعد أن أحكم المجتمع الدولي الخناق على الإرهاب وتنظيماته ودعاته، عبر الملاحقة الأمنية -دولياً- وإصدار دول عديدة تشريعات تجرِّم دعاة الإرهاب والمحرضين وتبعدهم عن منابر التوجيه والتثقيف والتعليم والإعلام بهدف حماية الشباب من أفكارهم الضالة، استثمروا الفضاء الإلكتروني ومواقع التواصل الاجتماعي، وبخاصة «تويتر»، لنشر أفكارهم المسمومة، لتجنيد الشباب ممن يستهويهم هذا النوع من الفكر المريض، بسبب «القابلية» النفسية والعقلية لديهم، وبسبب ضعف تحصينهم دينياً وثقافياً.

لذلك بدأ المجتمع الدولي في الآونة الأخيرة التحرك لسد هذه الثغرة الإلكترونية الخطيرة في جبهة مكافحة الإرهاب عبر العديد من الإجراءات.

ومن ذلك دعوة «اليونسكو» لعقد مؤتمر في باريس لدراسة السبل الكفيلة بمكافحة التطرف والتشدد لدى الشباب في المجال الإلكتروني، وجاء في بيانها الإعلامي: «أن الإنترنت بات يشكل جزءاً أساسياً من حياة الشباب اليوم، من التنشئة الاجتماعية والترفيه، إلى أداء الواجبات المنزلية، وهي تتيح فرصاً جديدة واسعة النطاق للاتصال والتعليم، وفي الوقت نفسه توفر الشبكة الإلكترونية للمتطرفين والمتشددين أدوات فعالة لنشر الكراهية والعنف واصطياد المجندين المحتملين، وإعدادهم للتحرك، مما يؤدي إلى إنشاء جماعات في الفضاء الإلكتروني من شأنها تشجيع التشدد على الصعيد العالمي».

ويمكن أن تدعم توصيات المؤتمر عمل الدول في هذا المجال، وكذلك منظمات المجتمع الدولي، من خلال فهم أكثر وضوحاً لاستخدام الإنترنت في إذكاء التطرف العنيف واكتشاف أدوات فعالة للتصدي له.

وفي سيدني، تعهد وزراء دول منطقة آسيا والمحيط الهادئ، خلال اجتماعاتهم بمواجهة التشدد العنيف الذي تروج له جماعات مثل تنظيم «داعش»، وكان من النقاط الأساسية التي ناقشها المؤتمرون، الحاجة إلى مواجهة انتشار أيديولوجية «داعش» على الإنترنت، وكيفية تحقيق ذلك.

وكانت الحكومة الأسترالية قد أقرّت عدداً من القوانين لهذا الغرض، مثل إلزام شركات الاتصالات بحفظ بيانات الزبائن الرقمية لمدة عامين.

وفي الولايات المتحدة، اعترف الفتى شكري علي أمين (١٧ عاماً)، أمام المحكمة، بأنه مذنب بتهمة دعم منظمة إرهابية، بعدما نشر أكثر من ٧ آلاف تغريدة دعائية لـ«داعش» ونداءات لتقديم دعم مادي أو إرشادات للراغبين في الانخراط في الجهاد في سوريا.

وكانت دراسة أميركية أخيرة، كشفت أن ما لا يقل عن ٤٦ ألف حساب على تويتر من مؤيدي «داعش»، وأن ثلثاها بالعربية! إن الأخطر في كل ما سبق، ما كشفته دراسة حديثة قام بها فريق بحثي سعودي بيّن أن تزايد استخدام موقع التواصل الاجتماعي (تويتر) في دول المجلس، نتج عنه تزايد ظاهرة التطاول على قيادات دول مجلس التعاون الخليجي، وازدراء الأنظمة الخليجية، كما أنتج ارتفاعاً في استعلاء بعض فئات المجتمع على بعضها الآخر، ونشاطاً كبيراً لإحياء النعرات الإقليمية والانحراف الفكري، متمثلاً في التطرف والتطاول على العلماء، إضافة إلى محاولات الإساءة إلى أمن بلدان الخليج وزعزعته، سواء في التغريدات نفسها أو في إعادتها أو في تفضيلاتها.

الدراسة بعنوان «الأبعاد الأمنية للتغريدات المسيئة في توتر وتأثيراتها في شباب دول مجلس التعاون الخليجي»، وانتهت إلى توصيات مهمة:

١. ضرورة مسارعة دول الخليج إلى إنشاء مركز إعلامي موحد، من مهماته: إبراز الحقائق، وسرعة التفاعل في تفنيد الإشاعات ودحضها على وسائل التواصل الاجتماعي.

٢. أهمية سن تشريعات تواكب تطورات الجريمة التي تقع عبر وسائل التواصل.

٣. أهمية إنشاء مركز حقوقي موحد في دول المجلس، يتولى رفع الدعاوى على المغردين المسيئين إلى هذه الدول بهدف ملاحقتهم قضائياً في الداخل والخارج.

ونبهت الدراسة إلى أن «تويتر» أهم منصة اجتماعية لنشر التغريدات المناوئة لأنظمة الدول وللتطاول على القيادات وتأليب الرأي العام.

ولذا فقد أصبح الفضاء الإلكتروني، بما يبثه ويرسخه من مشاعر الكراهية والتطرف والتعصب في نفوس الشباب، أخطر التحديات التي تواجه الدول في سعيها لتحصين وحماية الشباب من التطرف.

إن خطورة هذه التغريدات المسيئة للأنظمة والمحرضة عليها، كونها تهيئ نفسيات وعقليات قابلة لاعتناق فكر التطرف الذي يحول الشباب إلى «قنابل» بشرية مدمرة.

ماهية الإرهاب الإلكتروني:

الإرهاب الإلكتروني هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين.

أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية .

ولا شك في أن اتجاه وكالات المباحث والاستخبارات المركزية في الولايات المتحدة في أعقاب الحادث إلى الحصول على حريات أكبر في تعقب المعلومات الرقمية، لهو دليل على أهمية الشبكات الرقمية في عالم اليوم، وخطورتها إذا ما استُخدمت بالشكل غير الصحيح.

مفهوم الإرهاب الإلكتروني:

ظاهرة الإرهاب الإلكتروني أو الرقمي Electronic or Digital Tmsirorre هو نوع آخر من الإرهاب نتيجة التطور التكنولوجي والثورة المعلوماتية، بإستغلال شبكة الإنترنت للهدم والتخريب.ويمكن تعريفة بأنه «العدوان أو التخويف أو التهديد ماديًا أو

معنويًا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.»

ويعرف أيضاً «الإرهاب الإلكتروني هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين. أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية»

أشكال الإرهاب الإلكتروني:

استغلال المنابر الإلكترونية للتواصل مع أعوانهم ومموليهم لسهولة الاتصال والتنسيق عبر الشبكة العالمية ووفرة المعلومات وقلة تكاليفها.

والتلقين الإلكتروني بحشد المؤيدين والمتعاطفين معهم، وبث مبادئهم وطرقهم ووسائلهم في محاولة لتجنيد إرهابيين جدد.

حيث وجدت لبعض المنظمات الإرهابية آلاف المواقع لنشر أفكارهم ومعتقداتهم والتخطيط والتجهيز للعمليات الإرهابية وتنسيق وتبادل الخبرات الميدانية العملية فيما بينهم، حيث كشفت مواقع لتعليم صناعة المتفجرات والألغام والأسلحة الكيماوية الفتاكة، وأخرى توضح آلية اختراق وتدمير المواقع والبيانات والنظم المعلوماتية واختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، والتجسس الإلكتروني وطريقة نشر الفيروسات.

ناهيك عن مواقع مخصصة لشن حملات نفسية على الدول والمجتمعات التي تقوم بترويعها، حيث تعرض الرهائن والأسرى وإعدامهم.

وكما أن الإرهاب عبر شبكة الانترنت يمكن أن يتسبب في إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو قطع شبكات الاتصال بين الوحدات والقيادة أو تعطيل أنظمة الدفاع الجوي أو إخراج الصواريخ عن مسارها أو اختراق النظام المصرفي أو إرباك حركة الطيران المدني أو شل محطات الطاقة الحرارية والنووية.

فاختراق موقع البورصة العالمية يهدد الاقتصاد الدولي، أو اختراق موقع مطار دولي والتلاعب ببرامج الاتصالات يهدد سلامة ووصول الطائرات.

ومثال ذلك ما حدث في الولايات المتحدة الأمريكية حين تمكن أحد القراصنة من السيطرة على نظام الكمبيوتر في مطار أمريكي صغير، وأطفأ مصابيح إضاءة ممرات الهبوط، مما هدد بحصول كارثة.

وما حدث في إيطاليا حينما هوجمت عدة وزارات وجهات حكومية ومؤسسات مالية من قبل أحد الإرهابيين.

والإرهاب الإلكتروني يمثل البعد الخامس إلى:

١- الإرهاب التقليدي.

٢- الإرهاب النووي.

٣- الإرهاب البيولوجي.

٤- الإرهاب الكيماوي.

الإرهاب الإلكتروني أخطر معارك حروب الفضاء:

التنظيمات الإرهابية تستخدم أحدث التقنيات التكنولوجية لتنفيذ هجماتها الهجمات تستهدف التدمير العسكري والتخريب الاقتصادي وضرب المنشآت العامة.

الجريمة الإلكترونية هي الأب الشرعي للإرهاب الرقمي، تبدأ بـ «التحرير» وتنتهي بـ «التفجير»

موجة من الإرهاب تضرب غالبية دول العالم بصفة عامة والمنطقة العربية على وجه الخصوص، تمت فيها استخدام تقنيات الفضاء الالكتروني والتطور التكنولوجي لتنفيذ مقاصد الجماعات الإرهابية في تدمير أهدافها، وباتت الأطراف الفاعلة في منظومة الإرهاب على دراية بكل المستجدات والتطورات والتقنيات التكنولوجية

الجديدة بل واستطاعت أن تطور أداءها للهروب من رصد الأجهزة الاستخباراتية والفرار من احتياطات المؤسسات الأمنية بطواقمها وأسلحتها، فباتت كل دول العالم تحت مرمى نيران الإرهاب الالكتروني في ظل وجود فضاء مفتوح لم يستطع أحد السيطرة عليه.

من هو الإرهابي:

وصف الشخص بأنه إرهابيًّا على الإنترنت، يتطلب أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب، وغالباً يبتعد هذا الوصف عن الشخص المخترِق، فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

حروب رقمية:

التعريف الذي تعتمده كليات الحرب الأميركية، وتدعوه بهجمات الشبكات الكمبيوترية، وتصنفه تحت بند الحرب الإلكترونية، يقضي بأنها الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها، وحسب تعريف كلية الحرب فإن العمليات الإلكترونية تتضمن أنشطة مثل أمن العمليات، والعمليات النفسية، والخداع العسكري، والهجمات الفيزيائية، والهجمات على شبكات الكمبيوتر، وهناك الكثير من الطرق التي يمكن من خلالها تنفيذ الهجمات الرقمية، منها الهجمات المباشرة من خلال التدمير المادي لأجهزة الخصم، أو نقاط الاتصالات الهامة ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة.

وهنالك أيضا سرقة المعلومات من أجهزة الخصم، مما يمكن الجهات الصديقة من اتخاذ قرارات أفضل في المعركة، إضافة إلى تخريب قواعد بيانات العدو والتلاعب بها، لجعل العدو يخطئ في اتخاذ القرارات، وبالطبع هناك استخدام الفيروسات

وأساليب رقمية مثل هجمات الحرمان من الخدمات لتركيع مواقع العدو، مما يؤدي إلى التقليل من مقدرة العدو على الاتصال، وإبطاء قدرته على اتخاذ القرار.

الثورة الكبيرة والطفرة الهائلة التي جلبتها حضارة التقنية في عصر المعلومات كانت السبب وراء بروز مصطلح الإرهاب الإلكتروني أو الإرهاب الرقمي، وشيوع استخدامه، وزيادة خطورة الجرائم الإرهابية وتعقيدها، سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها، أو من حيث المساعدة على ابتكار أساليب وطرق إجرامية متقدمة، فأصبح الإرهاب الإلكتروني هاجسًا يخيفُ العالم الذي يتعرض لهجمات الإرهابيين عبر التكنولوجيَا الحديثة، فالإرهاب والإنترنت مرتبطان عن طريق ممارسة الأعمال التخريبية لشبكات الكمبيوتر والإنترنت، بجانب أن الشبكات الالكترونية أصبحت منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف والاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم وبث السموم، وحشد التأييد لأفكارهم وتجنيد من يتبعهم لتنفيذ مخططاتهم الشيطانية عبر الفضاء السيبراني.

جيوش وتنظيمات الكترونية:

وكما هي الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوماً ثلاثة عناصر أساسية من أجل كسب المعركة، وهي العناصر العسكرية، والاقتصادية، والسياسية، نجد في عالم حروب المعلومات تجد العناصر السابقة وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المرافق العامة كمؤسسات المياه والكهرباء والصرف الصحي والمنشآت الطبية وذلك لإخضاع إرادة الشعوب.

ويستهدف الجيش الالكتروني للإرهابيين الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات، ومن السيناريوهات التي تمثل هذا النوع من الهجمات، هو تعطيل مراكز القيادة والسيطرة العسكرية ووسائل الإتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها.

الهجمات ضد نظم المعلومات الاقتصادية يمكن لها أن تكون مؤذية جدا، ومن أمثلتها قيام بعض الإرهابيين بتحويل ملايين الدولارات من بعض الحسابات الشخصية لكبار العملاء بعد إختراق نظام التحويلات المشفر الدولي بين البنوك، وقيام بعض الهاكرز المحترفين بسرقة بيانات كروت الإئتمان من بعض أكبر معاقل التسوق الإلكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقات، وكذلك قيام بعض المنظمات الإرهابية بالعمل على تدمير اقتصاد إحدى دول الشرق الأوسط بشراء سندات دولية لتلك الدولة من داخلها عبر البورصات العالمية وبيعها بالخارج بأسعار أقل من قيمتها مما أدى لإنهيار عملتها ولتوفير تمويل لاعمالها الإرهابية في الدول التي تم بيع السندات فيها.

عمليات إرهابية:

الظروف التي مر بها العالم العربي منذ ما سمي (ثورات الربيع العربي) أي الحريق الغربي لبلداننا وقبلها غزو العراق، وما أعقب ذلك من استخدام التنظيمات الإرهابية المتطرفة مثل داعش للفضاء الإلكتروني في تجنيد عناصر من مواطني دول غربية، وجهت الانتباه إلى أهمية المجال الإلكتروني في حركة العلاقات الدولية والأمن والسلم العالميين، خاصة مع دوره في الحشد والتعبئة والتجنيد واستخدامه في نشر الأفكار المتطرفة، ونجحت عدة منظمات وجماعات إرهابية دولية وعلى رأسها داعش والقاعدة في التخطيط والتنسيق لعملياتها الإرهابية الكبرى في أوروبا، وخاصة في فرنسا وبلجيكا، من خلال شبكات معلومات وتواصل إجتماعي مغلقة لا يمكن رصدها، بل وتمحى بعد قراءتها مباشرة من خلال أجهزة ألعاب الفيديو المتصلة عبر الإنترنت، وأدت هذه العمليات الإرهابية لمقتل نحو مائتي شخص في نوفمبر ٢٠١٥، وفشلت أجهزة المخابرات الأوروبية في رصد العمليات قبل وقوعها لكنها اكتشفت هويات منفذيها من خلال هواتفهم المحمولة ومكالماتهم المتبادلة مع أفراد المنظمة.

الانتشار:

يعزو الخبراء انتشار الإرهاب الإلكتروني إلى ضعف بنية الشبكات المعلوماتية وعدم خصوصيتها وقابليتها للاختراق بسهولة، حيث تحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية يمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية وممارسة العمليات التخريبية والإرهابية، إضافة إلى سهولة الاستخدام التقنى وقلة التكلفة المادية، مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة، 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.

صعوبة اكتشاف وإثبات الجريمة الإرهابية الإلكترونية تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تعطي المجرم أملاً في الإفلات من العقوبة، فضلاً عن الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية بسبب عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخرجاتها.

خطورة الإرهاب الرقمي:

للأسف لقد أصبح اليوم وفي عصر الإرهاب الرقمي الحاسب الآلي المحمول وكاميرا الفيديو بأهمية وخطورة الكلاشينكوف و«الآر بي جي»، وهذا ما أشار إليه أحد قادة الإرهاب عندما ذكر: «أننا نخوض أكثر من نصف معركتنا في الساحة الإلكترونية والإعلامية» وقدم نصيحة لكوادره قائلاً: «عليكم أن تدركوا أن كل لقطة تلتقطونها هي بأهمية صاروخ يطلق على العدو....».

لقد استغل الإرهاب الحاسب والكاميرا إلى أقصى حد ممكن فأصبحت تقدم أدلة عسكرية على شكل كتب وأفلام وسلايدات «باور بوينت» تتضمن معلومات شتى عن الأسلحة والاغتيالات وصنع المتفجرات والسموم، لقد أصبحت شبكة الإنترنت

الواسعة وكأنها معسكر تدريب افتراضي للإرهابيين، ولقد نشرت النيويورك تايمز تقريراً يؤكد أن ٩٠٪ من الهجمات الإرهابية استخدم فيها متفجرات صناعة يدوية من تلك التي توجد وصفاتها بكثرة على الإنترنت. لقد لعب البريد الإلكتروني دوراً مهماً في التواصل بين الإرهابيين وتبادل المعلومات بينهم، للأسف يُوجد على الشبكة الإلكترونية بعض المواد التي تُعتبر بمثابة دروس مجانية للإرهابيين، ابتداء من بيان كيفية صناعة الزجاجة الحارقة، مروراً بكيفية صنع الطرود المفخخة وصولاً إلى كيفية صناعة بعض القنابل، لقد أصبح الإرهاب الحديث أكثر ضراوة لاعتماده على التكنولوجيا المتطورة للإنترنت التي ساعدت المنظمات الإرهابية في التحكم الكامل في اتصالاتهم ببعض، مما زاد من اتساع مسرح عملياتهم الإرهابية، وبالتالي أصبح من الصعوبة اصطياد هذا الوحش الإلكتروني الجديد وتدميره وقتله.

الإرهاب الالكتروني هو إرهاب الغد نظراً لتوسع وتعدد وتنوع مجال الأهداف التي يمكن مهاجمتها مع توفير قدراً كبيراً من السلامة للمهاجمين وعدم تعرضهم لخطر اكتشاف هوياتهم أو حتى المواقع التي شنوا هجومهم منها إلا بعد وقت طويل وجهد في البحث. هذا الإرهاب الإلكتروني له خسائر هائلة فتوقف التجارة الإلكترونية مثلاً ليوم واحد قد يتسبب في خسائر لأكثر من ستة مليارات دولار، وهكذا يمكن لمنظمة إرهابية إلحاق الكثير من الأذى والخلل لأعمال البنوك والبورصات وحركة الطيران، بل وحتى تغيير مواصفات تركيبة الأدوية في مصانع الأدوية مما يترتب عليه خسائر في أرواح البشر.

لقد دمرت منظمة إرهابية في أستراليا عام ٢٠٠٠م شبكة الصرف الصحي بواسطة عملية إلكترونية وفي نفس العام عندما أفلحت منظمة آوم شيريكو الإرهابية اليابانية من اختراق نظام البرمجة المتحكم في مسار أعداد هائلة من سيارات الخدمة العامة بواسطة التلاعب بأنظمة الحاسب، والإنترنت من أعطال أنظمة أكثر من خمسين شركة يابانية كبرى واختراق أنظمة عشر إدارات حكومية وتوجيهها لصالحها، ولم يتم اكتشاف هذه الاختراقات إلا بعد أن تكبدت الشركات والحكومة خسائر باهظة، كذلك

استطاعت إحدى المنظمات الإرهابية مسح جميع البيانات السكانية لليابان بواسطة اختراق أحد المواقع الحكومية، وفي عام ٢٠٠٠م حصلت أكثر من مائة وثمانين ألف حالة اختراق إلكترونية لمؤسسات اقتصادية ومالية كبرى في العالم، وهذه الهجمات والاختراقات تزيد بمعدل ٦٠٪ سنوياً.

لقد أضحى «الإنترنت» الساحة المتاحة لمعتنقي الفكر التكفيري لاجتذاب الشباب من خلال الشات وغرف البالتوك أو بنشر أفكارهم على التويتر والفيس بوك وعلى المنتديات أو من خلال المواقع التي تُعبّر عن الجماعات التي تعتنق هذه الأفكار. ولقد تولدت قناعة لدى بعض المؤمنين بأفكار التنظيمات الإرهابية أن الإنترنت مجال لما أطلقوا عليه الجهاد الإلكتروني ودفعهم ذلك لتدمير المواقع المخالفة لنهجهم ومحاولة نشر فكر التنظيم، وبالتالي أصبحت الشبكة هي البديل لمن لم يتمكن من الإرهاب كسلوك، هذا من جهة ومن جهة أخرى فهو تصوير وإظهار ممارسي الإرهاب الرقمي بمظهر البطولة والقدرة والتي جعلت منهم نجوماً يسعى الكثير من المراهقين لتقليدهم والإفادة من تجاربهم الإرهابية والمتطرفة والتكفيرية، هل يصدق أن إحدى المواقع الإرهابية الكبيرة أسست ما أسمته جامعة الجهاد الإلكترونية تحتضن عدة كليات منها كلية الجهاد الإلكتروني، وكلية جهاد النفس، وكلية تقنية العبوات الناسفة والسيارات المفخخة، وكلية الجهاد الإعلامي، بإمكانيات هائلة في التواصل الصوتي والمرئي والمكتوب بطبيعة سرية وفورية وقليلة التكلفة لتساعد التنظيم الإرهابي على بناء علاقات بين أعضائه في الفضاء الخارجي بعيداً عن المراقبة الأمنية يُستفاد من ذلك في أعداد هائلة من الزوار من مختلف الجنسيات يمكن للتنظيم أن يجند بعضهم أو يكسب تعاطف البعض الآخر.

وكعينة لإرهابيي الإنترنت يونس واسمه في الإنترنت (إرهابي ٧٠٠) وقبض عليه في أكتوبر ٢٠٠٥م. ويونس هذا لم يطلق طلقة واحدة في حياته ولكنه أكثر خطراً من عشرات الإرهابيين حيث لعب هذا الشاب في إعادة تنظيم القاعدة بعد سقوط نظام طالبان، كان يونس يعمل مع اثنين من المتعاملين معه ومع أنه لم يسبق لهم الالتقاء

وجهاً لوجه مطلقاً فإن جميع الاتصالات واللقاءات كانت عبر الشبكة العنكبوتية. لقد كانت هذه الخلية تدير شبكة لبطاقات الاعتماد المزيفة بقيمة بلغت ١,٨ مليون جنيه إسترليني وأنفقت هذه الأموال على شراء معدات لتنظيمات إرهابية وتصميم مواقع تكفيرية متطرفة على الشبكة الإلكترونية. كما تبيَّن أن لهذه الخلية خاصة (إرهابي ٧٠٠) ارتباطاً بالتخطيط لتفجير مواقع عسكرية ومدنية في واشنطن ولندن وله علاقة بالخلية من الأطباء التي حاولت تفجير مطار جلاسكو وعثر بجهاز (إرهابي ٧٠٠) على رسالة تقول «نحن ٤٥ طبيباً مصممون على نقل الحركة إلى داخل أمريكا الفاسدة». كما وجد في حاسبه كذلك على مخطط لضرب قاعدة بحرية أمريكية في فلوريدا. وهذه عينة فقط لإرهابيي الإنترنت ومدى فاعليتهم وخطرهم على المجتمع والأمن ككل.

من المهم معرفة التمويل الإلكتروني، فعددٌ كبير من المواقع الإلكترونية تقدم دعايات وإعلانات وخدمات وتقبض أموالاً طائلة في مقابل ذلك، وقد يكون الموقع عادياً ولكنه واجهة لخلية إرهابية، ودلَّت بعض الدراسات أن بعض هذه المواقع يصل دخلها إلى ملايين الريالات، وهذه المواقع «العادية» تبهر المتصفح بالإعلانات المصممة تصميماً أقرب للخيال العلمي، وهي بذلك تربح الملايين من الأموال من هذه الدعايات والإعلانات والخدمات المقدمة، وللأسف الشديد لا يُعرف أين تذهب هذه الأموال؟

كذلك من الإستراتيجيات الفعَّالة التنسيق مع محركات البحث أمثال جوجل، وياهو، ويوتيوب، ووندوز لايف، ومكتوب، والفيس بوك، وغيرها لمنع دخول الإرهابيين لهذه المواقع وعدم استخدام مواقعهم كوسيلة نشر للفكر الإرهابي. كما أن ضرورة توحيد التشريعات الأمنية على المستوى الدولي؛ بغية تعزيز قاعدة البيانات للمطلوبين أمنياً. ومن الإستراتيجيات كذلك محاولة إنشاء هيئات وطنية تهتم بمكافحة الإرهاب والجرائم المرتبطة بشبكة الإنترنت.

ولذا يعمل العالم جاهداً للحد من جرائم الفضاء الإلكتروني وعلى رأسها الإرهاب المعلوماتي وفي هذا الإطار طرح توقيف مهندس هندي يدير حساباً لتنظيم داعش

على تويتر عدة أسئلة حول مدى إمكانية التنظيم شن هجمات إلكترونية موجعة لمؤسسات غربية خصوصاً مع الاحترافية التي توظف بها عناصر التنظيم مواقع التواصل المختلفة، هل استخدام الإنترنت بكفاءة مؤهلاً لشن هجمات إلكترونية؟ أم أن هناك فروقاً بين الأمرين؟

قوة استراتيجية:

توقف الكثيرون أمام توظيف تنظيم داعش الفضاء الإلكتروني لا سيما مواقع التواصل الاجتماعي التي استخدمها التنظيم بشكل غير مسبوق في أية تنظيمات مشابهة.

ففي الوقت الذي يخوض فيه عناصره معارك لاحتلال هذه المدينة أو تلك، ويقومون بانتهاكات ربما تكون الأبشع بين الجماعات المتطرفة يخوض أفراد تابعون أو متعاطفون مع التنظيم معركة من نوع آخر للاستيلاء لا على بنك أو قطعة آثار بل على عقول وقلوب الرأي العام، ويتم بث مقاطع فيديو على موقع يوتيوب تتسم في مجملها بحرفية واضحة في الإخراج غالباً ما تجد طريقها لدى المشاهد وبصفة خاصة من الأجانب.

كما يقومون بالتفاعل مع موقعي فيسبوك وتويتر وغيرهما بطريقة لا تخلو من احترافية لنشر فكر التنظيم والترغيب في الانضمام له أو حتى التعاطف على أقل تقدير.

يضاف إلى هذا إنشاء مجلات إلكترونية لافتة للنظر نتيجة القالب الاحترافي الذي تخرج به في الشكل والمضمون، ويجمع هذه الوسائل هدف التأثير على المتابع لنشر فكر التنظيم، والرد على ما يثار حوله، وكذلك تثبيط همم الأعداء. ويعتبر تقرير نشره موقع سيكيورتي ويك أن استخدام التنظيم الإعلام الاجتماعي يعتبر قوة استراتيجية لا يستهان بها، كما تعتبر سبباً رئيساً في انضمام عدد كبير من العناصر التي وفدت من دول أجنبية عديدة، لكن هل يرتبط استخدام الفضاء الإلكتروني بطريقة غير مسبوقة بإمكانية شن حرب إلكترونية موازية للحرب على الأرض؟

الخيارات المرعبة مطروحة:

يرى ديفيد ديولت -رئيس شركة FireEye للأمن المعلوماتي- أن التنظيم ربما يسير على خطى الجيش الإلكتروني السوري، وفريق أياكس الأمني الإيراني في الهجوم على أهداف غربية، وأكد أن هناك شواهد على أن المنظمات الإرهابية تنوي الدخول بقوة في عالم الجريمة الإلكترونية لا سيما مع ازدهار الأسواق السرية التي تتعامل مع السوفت وير المشبوه، ولا يستبعد أن تكون الجماعات الإرهابية زبوناً لدى تلك الأسواق الرائجة إلى حد كبير فيما يسمى الشبكة السوداء حسبما ذكره لصحيفة فايننشيال تايمز. وأكد أن هناك مواقع تسوق عادية مثل eBay أحياناً تعرض تلك الأدوات الضارة في الفضاء الإلكتروني بتكلفة ضئيلة نسبياً، ولا تحتاج تلك الأدوات إلى خبرة كثيرة للتعامل معها، وشدد على أن تلك «الأسلحة» الإلكترونية لن تقل أهمية عن الأسلحة التقليدية لدى جماعات الإرهاب المختلفة.

أما عن احتمالية شن هجمات محدودة، لكن مؤثرة من قبل التنظيم يرى جون كوهين -منسق مكافحة الإرهاب في الأمن الداخلي بواشنطن- أن داعش تبحث دوماً عن الأحداث التي تلفت الأنظار إلى وجودها وأهدافها.

لذا ليس من المستبعد أن تضع بين أهدافها القيام بأعمال إلكترونية تخريبية ضد الأهداف الأمريكية، إلا أنه يرى أن التنظيم لن يكتفي بمجرد المضايقة ولإثبات الوجود بقدر ما يتوقع أن يعمد إلى إحداث أزمة حقيقية، ويضرب أمثلة بضرب مفاعلات الطاقة على الأراضي الأمريكية.

كما أن المؤسسات المالية قد تكون هدفاً للتنظيم بحيث يساعد اختراقها إلكترونياً على تأمين تمويل للتنظيم الذي يعتبر الأضخم تمويلاً بين الجماعات المتطرفة.

وقد دفع الجدال حول الإرهاب المعلوماتي جيمس كومي -مدير المباحث الفيدرالية FBI- للخروج في أول ظهور تليفزيوني له لمناقشة المسألة محذراً من خطر تلك التهديدات، وأنه لا يجب التهاون في التعامل معها.

أما مايكل روجرز -مدير وكالة الأمن القومي الأمريكية- فقد طالب باتخاذ أقصى التدابير الأمنية تحسباً لوقوع هجمات إلكترونية من جماعات متطرفة، ودعا للعمل مع دول أخرى للتنسيق للعمل معاً ضد هذه التهديدات.

وفي ذات السياق عقد حلف شمال الأطلسي تدريبات للأمن المعلوماتي استمرت ثلاثة أيام على مقربة من السواحل الروسية، وقد ركزت هذه التدريبات -التي تعد الأكبر في تاريخ الناتو- على السيناريوهات المفترضة للقيام بهجمات إلكترونية إرهابية.

هجمات هوليودية (سينمائية)

وعلى الجانب الآخر ترى سيلينا ريليو -رئيسة برنامج مكافحة تمويل الإرهاب بالخارجية الأمريكية سابقاً- أنه يجب التفرقة بين استخدام التنظيم الفضاء الإلكتروني كأداة إعلامية، والقدرة على توظيفه للقيام بعمليات إرهابية تستهدف المواقع الإلكترونية الحساسة.

ولا تعتقد أن الوقت الراهن سيشهد قيام الجماعات المتطرفة بهجمات كارثية على مواقع تخص دول غربية، لكنها تدعو للتحسب لحدوث تغيير في المستقبل فيما يخص هذا النوع من العمليات، وإذا كان الأمر اليوم بمثابة تهويل لقدرات التنظيم، فإن الغد يختلف.

من جانبه يرى ستيفن بونر -خبير الأمن الإلكتروني- أن ما يتردد عن حدوث ضربات إرهابية من خلال الإنترنت ذات تأثير ضخم يعتبر ضرباً من الخيال، ويقول: إنه لم ير انهيار شركات كبرى بسبب اختراق حواسيبها إلا في أفلام هوليوود، إلا أنه يوصي بتفعيل أنظمة دفاع إلكتروني قوية.

ولا تختلف هذه التوصية عن تلك التي أطلقها توم كين ولي هاملتون -معدا تقرير لجنة ١١ سبتمبر- مشيرين إلى أن الدرس المستفاد من هجمات سبتمبر أن الولايات المتحدة لم تنتبه لتهديدات الإرهاب ال الإلكتروني إلا في وقت متأخر جداً، وطالبا بعدم تكرار العالم هذا الخطأ بأن تتخذ إجراءات الأمن المعلوماتي تحسباً لأي اختراق

من جماعات إرهابية، لأن التغيرات المتسارعة في الظروف الجيوسياسية العالمية تدعو لليقظة من تنامي تلك المخاطر.

ويقول كريغ جليانو -خبير التأمين المعلوماتي والمسؤول السابق في البنتاغون- إنه لا يوجد إثبات واحد لفرضية قيام الجماعات الإرهابية بشن هجمات إلكترونية على البنية التحتية لأية دولة تستهدفها. وشدد على أن تلك الجماعات -ومنها داعش- لا تمتلك الكوادر البشرية المؤهلة لقيادة مثل هذا الهجوم، كما لا تمتلك المصادر التي تمكنها من ذلك. وقال: إن فرضية حدوث مثل تلك الهجمات ربما تكون واردة في المستقبل، لكن ليس في الوقت الراهن.

ويوضح أن المقارنة تظهر البون الشاسع بين تنظيم داعش وعمليات القرصنة الإلكترونية التي تمارسها كيانات مدعومة من دول مثل هجمات القراصنة الصينيون على أهداف أمريكية، وثمة إفادات بأن المهاجمين يتلقون دعماً واسعاً من السلطات الصينية، كما أن عدداً منهم يعمل بالجيش الصيني.

ويؤكد هذا الرأي جيم لويس -الخبير بمركز الدراسات الاستراتيجية والدولية، مشيراً إلى أن التنظيم لا تتوافر لديه الإمكانيات التقنية والبشرية التي تتيح القيام بهجمات تدميرية مؤثرة على المواقع المعادية.

ويوضح أن هدف الهاكرز الصيني المدعوم حكومياً اقتصادي في المقام الأول، حيث يقومون باختراق حواسيب الشركات الكبرى للوقوف على الأسرار التجارية لتلك الشركات، والملكية الفكرية للمنتجات.

أما في حالة داعش فالهدف الأول حالياً هو بسط النفوذ على أكبر مساحات ممكنة من الأراضي لإقامة دولة الخلافة، وليس من أهدافها شن هجمات إلكترونية على المواقع الغربية.

وأشار تقرير لتاي كورين وغابي سيبوني أن الهدف الأول من استخدام التنظيم الإنترنت ذو أبعاد نفسية في المقام الأول لتصوير قوة وهمية، حيث تنشر الفيديوهات

الصادمة الرعب لدى مشاهديها، فيما تعزز مشاهد الفتوحات والغنائم الصورة المطلوب تعميمها.

إلا أن هناك مؤشرات إلى أن التنظيم يمتلك الأدوات المتقدمة التي تمكنه من القيام بهجمات إلكترونية حسب التقرير المنشور بدورية معهد دراسات الأمن القومي .

ومن هذه المؤشرات أن قيادة التنظيم تضم مجموعة من القادة في مرحلة الشباب على قدر كبير من المعرفة التقنية، فضلاً عن ثراء التنظيم الذي يسمح له بتوفير الإمكانيات، يضاف إلى هذا ما نشر في عام ٢٠١٢ عن تسرب معلومات تقنية بالغة الحساسية من إيران وكوريا الشمالية لمجموعات إرهابية.

تجدر الإشارة إلى أن هناك عدداً من عناصر داعش ذات صلة بهجمات أو جرائم إلكترونية ومنهم أبو حسين البريطاني الذي سبق سجنه في عام ٢١٠٢ لمحاولات اختراق حساب البريد الالكتروني لرئيس الوزراء البريطاني السابق توني بلير، كما خصص حسابه على تويتر للدعوة لتجنيد المزيد من الشباب.

وهناك مجموعة تطلق على نفسها Lizard Sguad التي أعلنت مسؤليتها عن تعطيل مواقع الإنترنت الخاصة بالفاتيكان وشركة سوني وغيرهما، وتعلن هذه المجموعة -على حسابها بتويتر- أنها وضعت علم التنظيم على الصفحات التي أغلقتها. ومع ذلك هناك من يطرح تساؤلات حول إمكانية البعض اللعب بورقة الإرهاب والتطرف للنيل من المؤسسات الأمريكية والغربية لدفع العالم أجمع للوقوف في وجه العالم الإسلامي، على اعتبار أن الهجمات الإلكترونية المتوقعة ستسجل باسم تنظيم داعش.

الحماية من الإرهاب الإلكتروني في الدول المتقدمة:

في فجر الثورة الرقمية، في منتصف العقد الماضي، انتبه الغرب إلى قضية الإرهاب الإلكتروني ومخاطره، حيث قام الرئيس الأمريكي بيل كلينتون في العام ١٩٩٦ بتشكيل لجنة حماية منشآت البنية التحتية الحساسة WWW.Nipc.govv . وكان أول استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات

الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة.

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 ألفا من خبراء أمن المعلومات، وقوة ضاربة على مدى ٢٤ ساعة لمواجهة الإرهاب الإلكتروني. وقامت القوات الجوية الأمريكية باتخاذ خطوات مماثلة، ومثلها المباحث الفدرالية. كما تقوم قوات الأمن في أوروبا، وخصوصا الدول التابعة لحلف الأطلسي، باتخاذ إجراءات مماثلة.

الحرب الرقمية من المنظور الأمريكي:

نقتبس فيما يلي التعريف الذي تعتمده كليات الحرب الأمريكية، وتدعوه بهجمات الشبكات الكمبيوترية، وتصنفه تحت بند «حرب إلكترونية». ويقول التعريف بأن الحرب الرقمية هي «الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها.» وحسب تعريف كلية الحرب فإن العمليات الإلكترونية تتضمن أنشطة مثل أمن العمليات، والعمليات النفسية، والخداع العسكري، الهجمات الفيزيائية، والهجمات على شبكات الكمبيوتر. وهناك الكثير من الطرق التي يمكن من خلالها تنفيذ الهجمات الرقمية، منها الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات الهامة ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة. وهنالك أيضا سرقة المعلومات من أجهزة الخصم، مما يمكن الجهات الصديقة من اتخاذ قرارات أفضل في المعركة، إضافة إلى تخريب قواعد بيانات الخصم والتلاعب بها، لجعل الخصم يخطئ في اتخاذ القرارات. وبالطبع هناك استخدام الفيروسات وأساليب رقمية مثل هجمات الحرمان من الخدمات لتركيع مواقع الخصم، مما يؤدي إلى التقليل من مقدرة الخصم على الاتصال، وإبطاء قدرته على اتخاذ القرار.

سيناريوهات حروب المعلومات:

وكما هي الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة؛ وهي العناصر العسكرية، والاقتصادية، والسياسية أو بكلمات أخرى إرادة الشعب. وفي عالم حروب المعلومات تجد العناصر الثلاث نفسها وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إرادة الشعوب.

الهجمات على الأهداف العسكرية:

تستهدف هذه النوعية من الهجمات عادة، الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات. وهذا النوع من الهجمات نادر الحدوث عادة لعدة أسباب أولها هو أنه يتطلب معرفة عميقة بطبيعة الهدف، وطبيعة المعلومات التي يجب النفاذ إليها، وهي معرفة لا تمتلكها إلا الحكومات، إضافة إلى أن الحكومات تقوم عادة بعزل المعلومات العسكرية الحساسة عن العالم، ولا تقوم بوصل الأجهزة التي تحملها بالعالم الخارجي بأي شكل من الأشكال. ولكن يبقى الحذر واجباً من عمليات التخريب الداخلية، ومن هنا تأتي ضرورة وضع نظم موثوقة للتحقق من شخصيات المستخدمين، والتحديد الدقيق لطبيعة المعلومات التي يُسمح بالنفاذ إليها. ومن السيناريوهات التي تمثل هذا النوع من الهجمات، هو النفاذ إلى النظم العسكرية واستخدامها لتوجيه جنود العدو إلى نقطة غير آمنة قبل قصفها بالصواريخ مثلا.

الهجمات على الأهداف الاقتصادية:

أصبح الاعتماد على شبكات الكمبيوتر شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات، نظراً لطبيعتها المترابطة، وانفتاحها على العالم، هدفا مغريا للعابثين والهكرة. ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل كبير بالانطباعات السائدة والتوقعات، والتشكيك في صحة هذه المعلومات، أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة

في النظام الاقتصادي. ولذلك فإن الهجمات ضد نظم المعلومات الاقتصادية يمكن لها أن تكون مؤذية جداً. ومن الأمثلة على الهجمات الاقتصادية هي العملية التي قامت بها مجموعة من الهكرة، تُعرف باسم نادي الفوضى، في عام ١٩٩٧، حيث قام هؤلاء بإنشاء بريمج تحكم بلغة آكتف إكس مصمم للعمل عبر إنترنت ويمكنه خداع برنامج كويكن Quicken المحاسبي بحيث يقوم بتحويل الأموال من الحساب المصرفي للمستخدمين. وباستخدام هذا البريمج أصبح بإمكان هؤلاء الهكرة سرقة الأموال من أرصدة مستخدمي برنامج كويكن في جميع أنحاء العالم. وهذه الحالة هي مثال واحد فقط على الطرق التي يمكن بها مهاجمة شبكات المعلومات الاقتصادية واستغلالها، وهي طرق يمكن أن يكون لها آثار مدمرة على المجتمعات.

الهجمات على شبكات الطاقة الكهربية:

أصبح الاعتماد على شبكات المعلومات، وخصوصا في الدول المتقدمة، من الوسائل المهمة لإدارة نظم الطاقة الكهربية. ويمكن لهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطرة وحقيقية، وخصوصا في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية. ومن الإحصائيات البشعة التي يمكن لها أن تدلنا على فعالية مثل هذا النوع من الهجمات هي تلك المتعلقة بالهجمات على العراق خلال حرب الخليج الثانية، حيث تشير مصادر كلية الحرب الأمريكية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين ٧٠ إلى ٩٠ ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية. ولذلك، فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الإلكتروني.

ولا يتوقف الأمر عند هذا الحد، حيث أن هنالك الكثير من الأهداف الأخرى، التي يمكن بواسطتها للهكرة المتمكنين أن يشيعوا الفوضى في الحياة المدنية. فهنالك مثلا شبكات المعلومات الطبية، والتي يمكن مهاجمتها، واختراقها، ومن ثم التلاعب بها أن يؤدي إلى خسائر في أرواح المرضى من المدنيين. وهنالك حالات في العالم

الغربي حيث قام الهكرة بالنفاذ إلى سجلات المستشفيات والتلاعب بسجلات المرضى بشكل أدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم. وحتى لو افترضنا أن الشبكات المعلوماتية الخاصة بالمؤسسات الطبية منيعة، فإن رسالة واحدة تُنشر مثلا بالبريد الإلكتروني، مفادها أن هنالك دماء ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثارا مدمرة على الصعيد الاجتماعي.

سبل الحماية:

يمكننا أن ندخل هنا في موضوعات شتى حول سبل حماية نظم المعلومات الهامة، ولكن تبقى الخلاصة هي أنه لا يمكن تقديم حماية مطلقة وتامة لنظم المعلومات المرتبطة بشبكات الاتصالات. والسبيل الوحيد لتأمين المعلومات الحساسة هو عزل الأجهزة التي تحتوي هذه المعلومات عن العالم. ولكن مثل هذه الإجراءات يمكن لها أن تؤدي إلى نتائج أكثر إيذاء على المدى الطويل تتمثل في حرمان المجتمع من وسائل زيادة الإنتاجية والفعالية. ومع ذلك، فإن استخدام مجموعة من الإجراءات الأمنية الأساسية يمكن لها أن تقلل بشكل كبير من مخاطر الاختراقات والإرهاب الإلكتروني. وتشمل الإجراءات الأمنية التي يجب مراعاتها ثلاث نواح هامة يجب تغطيتها جميعاً وبشكل متكافئ، وإلا فإن السياسة الأمنية ستعتبر فاشلة.

تأمين خطوط الدفاع الأمامية باستخدام تطبيقات الجدران النارية:

وتقوم هذه الفئة من التطبيقات بتأمين المنافذ Ports التي تحصل من خلالها التطبيقات على خدمات إنترنت. 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 للهكرة للنفاذ إلى النظم. وتعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالاعتماد على مجموعة من السياسات Policies التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات التي يُسمح للعاملين بالمؤسسة النفاذ إليها. وضمن فئة الجدران

النارية يوجد نوع هو الجدران النارية المؤسسية، والتي تقوم بحماية تطبيقات المؤسسات على مستوى الأجهزة المزودة، وبالتالي 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 مؤخرا 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 استخدام طبقات أخرى من الأمن تتجاوز الخطوط الأمامية.

تأمين حسابات المستخدمين ونظم التحقق من الهوية:

رغم 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 شيوعا للتحقق من الهوية، رغم أن هذه الأساليب بدأت تصبح أضعف وأضعف بتطور التقنيات التي يستخدمها الهكرة لكشفها وخرقها. ومع ذلك، فهنالك الكثير من الوسائل التي يمكن استخدامها للحد من قدرة الهكرة على اختراق واكتشاف هذه الرموز. وتعتمد هذه الوسائل أساسا على تحديد حقوق نفاذ المستخدمين إلى الشبكات، وحصرها بما يحتاجه كل مستخدم. ولكن هذه التقنيات، ورغم قوتها، ليست حلولا سحرية، إذ أنها تتطلب الكثير من المهارة والتخطيط الواعي قبل تطبيقها كي تحقق النجاح.

تصاعد الهجمات الإلكترونية:

أصبحت وتيرة الهجمات الإلكترونية تتزايد وتتكرر بصورة تصاعدية، وهذا بدون شك يشير إلى أن الإرهاب يتلون ويأخذ صوراً وأشكالا متعددة كلها تصب في خانات متعددة تشمل التخريب والاستغلال والاستحواذ والهيمنة والابتزاز، وهذه الأمور كالعادة تبدأ بمبادرات فردية عبثية ومع استفحالها وتطورها يبدأ تبنيها من قبل منظمات وشركات

ومراكز استخبارات، الهدف منها تحطيم الخصم، والفوز بقصب السبق حتى إذا أتت أكلها استساغتها دوائر أكبر وأشمل ضمن دوائر الصراع والتنافس، وأصبح هناك نوع من التحدي الإلكتروني بين الأطراف المتصارعة مما حدا بالدول ذات الوعي التقني إلى إنشاء جيش إلكتروني يسمى جيش السيبر يكون ملحقا بالجيوش النظامية أو مستقلاً، له أهداف متعددة منها ما هو شرعي، ومنها ما هو غير شرعي، ويشمل ذلك العمل على صد الهجمات الإلكترونية أو تنفيذ هجمات إلكترونية أو العمل على شل القدرات العسكرية الدفاعية والهجومية بالإضافة إلى شل حركة المؤسسات الأمنية والمدنية. ولعل ما نشاهده من هجمات إلكترونية متكررة بمسميات مختلفة مثل «شارون – والفدية» وغيرها لا تعدو كونها بروفات وتجارب ميدانية لبعض الفيروسات الإلكترونية لدراسة مدى تأثيرها وانعكاساتها وبالتالي العمل على تطويرها، وهذا يعني أن عصر الإرهاب الإلكتروني قد بدأ بنشر ظلاله على كافة المستويات، وهذا نذير بتحوله من مجرد إرهاب إلى حرب ضروس تعجز الدول والشعوب التي لم تستعد لها عن الوقاية منها و يجعلها تقع ضحية لذلك المارد الذي بدا يفقس من البيضة ويتحول إلى وحش كاسر لا يرده سوى العلم والمعرفة اللذان يستطيعان بناء أسوار وعوائق إلكترونية على قدر عال من الكفاءة والندية بل المتفوقة، وهذا يدعونا إلى المناداة بإنشاء جيش سيبر دون تأخير، خصوصاً أن مختلف الدول والمؤسسات تسعى جاهدة إلى امتلاك الأدوات والوسائل الخاصة بها للحماية من ذلك المارد الذي انطلق من عقاله وأصبح وسيلة من لا وسيلة له للإضرار بالآخرين.

وقد بدأ عصر الإرهاب الإلكتروني بنشر ظلاله على كافة المستويات، وهذا نذير بتحوله من مجرد إرهاب إلى حرب ضروس تعجز الدول والشعوب عن الوقاية منها.

إن الإرهاب وبالتالي الحروب الإلكترونية فيها معتدٍ وفيها ضحية وهذا ما خلق اليوم سباق التسلح بالعلم والمعرفة الإلكترونية على مستوى المؤسسات والشركات خصوصاً المالية مثل البنوك المركزية والبنوك التجارية ومراكز الاستثمار والمؤسسات الخدمية والإعلامية وقبل ذلك وبعده المؤسسات العسكرية والأمنية.

نعم إن العصر الحاضر أصبح عصر تقنية المعلومات، وأصبحت جميع الفعاليات الحالية تعتمد على استخدام الحاسوب في كافة القطاعات مما ينذر باندثار المعاملات الورقية وحتى الصحف وإخواتها بصورة تدريجية، ولن يتوقف الأمر على ذلك بل سوف يتعداه إلى النقود التي تتحول بصورة متسارعة إلى عملات إلكترونية مما جعل تلك القطاعات مجتمعة أو منفردة هدفاً استراتيجياً سهلاً يعمل الأرهابيون على اختراقه والتجسس عليه أو تعطيله أو تدميره، والحقيقة المرة أن مثل تلك الهجمات تمهد لما بعدها خصوصاً في مجال الاستحواذ على الأموال من خلال سحبها وتحويلها إلى حسابات آخرى، ومن ثم الاستيلاء عليها من خلال القرصنة الإلكترونية المتقدمة.

وهذا ما يدعو جميع المؤسسات وخصوصاً المالية منها إلى عدم التخلي عن النظام الورقي بل ابقائه كاحتياط يتم اللجوء إليه في حالة الضرورة القصوى ناهيك عن العمل على تبني أنظمة الكترونية احتياطية داخلية متقدمة تكون بمعزل عن تلك الهجمات يركن إليها وقت الضرورة للمواجهة والحد من تأثير ما هو قادم من هجمات أشد وأنكأ.

إن التحسب للأسوأ جزء من الحذر الذي يجب أن نتحلى به ونضعه قاعدة للعمل.

إن الإرهاب الإلكتروني لم يعد يقتصر على ما نشاهده من هجمات إلكترونية، ومن إساءة استخدام لوسائل التواصل الاجتماعي مثل فيسبوك وتويتر ومدونات ووتس اب وغيرها، بل سوف يستحدث ما هو أشد وأنكأ ضرراً منها. وهذا يدعونا إلى إنشاء جيش سيبر على مستوى كل من الدولة والمؤسسات للوقاية والهجوم المضاد للدفاع وصد ذلك الإرهاب والحرب التي تتطور بصورة متسارعة إلى ما هو أكبر ضرراً وأبلغ أثراً وأشد تأثيراً.

الخلاصـــة:

بشكل عام فإن الحرب الإلكترونية، من أجل خرق السيادة الوطنية لأية دولة، والحصول على معلومات استخباراتية، وتجنيد العملاء وغيرها من الأنواع المستخدمة، محرّمة.

حيث أن الفقرة الرابعة من المادة الثانية لميثاق الأمم المتحدة تنص على أنه: «يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة».

كما أن الفقرة ٧ من المادة نفسها تقول: «ليس في هذا الميثاق ما يسوغ للأمم المتحدة أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما، وليس فيه ما يقتضي الأعضاء أن يعرضوا مثل هذه المسائل لأن تحل بحكم هذا الميثاق، على أن هذا المبدأ لا يخل بتطبيق تدابير الردع الواردة في الفصل السابع».

ومن الضروري لمواجهة الإرهاب الإلكتروني تفعيل التعاون الدولي في العديد من دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المُجرمين، وإصدار عدد من القوانين التشريعية الجديدة لتجريم أى استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، بالإضافة إلى التعاون والتنسيق الدائم مع الإنتربول الدولي في مجال تبادُل المعلومات والخبرات الأمنية والفنية في رصد ومُتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايده المُستمر من خلال عناصرهِ الإجرامية المُحترفة والمُنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية.

●●●