رابطة العالم الإسلامي

الأمانة العامة

الإدارة العامة للمؤتمرات والمنظمات

الإرهاب الإلكتروني الحديث
مظاهره وطرق التصدي له

إعداد

الدكتور/ برهان المرزوقي

الأستاذ في كلية الإمارات للتكنولوجيا – أبو ظبي

مقدم إلى

مؤتمر مكة المكرمة السادس عشر

الشباب المسلم والإعلام الجديد

الذي تنظمه

رابطة العالم الإسلامي

تحت رعاية خادم الحرمين الشريفين

الملك سلمان بن عبد العزيز آل سعود

مكة المكرمة

٣ - ٤ / ذو الحجة / ١٤٣٦ هـ، الموافق ١٦ - ١٧ / سبتمبر / ٢٠١٥ م

رابطة العالم الإسلامي

مكة المكرمة – المملكة العربية السعودية

صندوق البريد (٥٣٧) أو (٥٣٨) مكة المكرمة (٢١٩٥٥)

هاتف: ٠٠٩٦٦١٢٥٦٠٠٩١٩ – الفاكس: ٥٦٠١٣١٩ – ٥٦٠١٢٦٧

برقياً: رابطة – مكة، تلكس: ٥٤٠٠٠٩ و٥٤٠٣٩٠

www.themwl.org

البريد الإلكتروني للإدارة العامة للمؤتمرات والمنظمات

conferences@themwl.org

واتس أب : (٠٠٩٦٦٥٠٣٣٩٦٣٢٠) : whatsApp

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

مقدمة

الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، نبينا محمد وعلى آله وصحبه أجمعين، أما بعد:

فإن الشريعة الإسلامية جاءت كاملة شاملة، صالحة لكل زمان ومكان، محققة لأمن وطمأنينة الشعوب، وقد أكرمنا الله بعقل قادر على التفكير بعمق وعلى تجلية الحقائق وتذليل الصعوبات، ويسعى في عمارة الكون بما يُصلح الخلق والأرض، خلق الله الإنسانَ فأكرمه، قال الله سبحانه: ﴿ ۞ وَلَقَدْ كَرَّمْنَا بَنِيٓ ءَادَمَ وَحَمَلْنَٰهُمْ فِي ٱلْبَرِّ وَٱلْبَحْرِ وَرَزَقْنَٰهُم مِّنَ ٱلطَّيِّبَٰتِ وَفَضَّلْنَٰهُمْ عَلَىٰ كَثِيرٍ مِّمَّنْ خَلَقْنَا تَفْضِيلًا ﴾ [الإسراء: ٧٠]، أي فضَّلْنا ﴿بَنِيٓ ءَادَمَ﴾ بالعلم والنطق واعتدال الخُلق وطهارتهم بعد الموت، ﴿وَحَمَلْنَٰهُمْ فِي ٱلْبَرِّ﴾: على الدواب، ﴿وَٱلْبَحْرِ﴾: على السفن، ﴿وَرَزَقْنَٰهُم مِّنَ ٱلطَّيِّبَٰتِ وَفَضَّلْنَٰهُمْ عَلَىٰ كَثِيرٍ مِّمَّنْ خَلَقْنَا﴾؛ كالبهائم والوحوش، ﴿تَفْضِيلًا﴾، مِن بمعنى ما أو على بابها، وتشمل الملائكة، والمراد تفضيل الجنس، ولا يلزم تفضيل أفراده، إذ هم أفضل من البشر غير الأنبياء[1].

والإرهاب من مظاهر الانحراف عن الفطرة السليمة والتفكير العقلاني وتجاوز أخلاقيات التعايش السلمي بين الأفراد والشعوب، ومن الصور الحديثة للإرهاب: استخدام الوسائل الإلكترونية الحديثة القائمة على ذكاء الأفراد واستحداث طرق مبنية على تكنولوجيا المعلومات، فكان هذا البحث لبيان (الإرهاب الإلكتروني الحديث مظاهره وطرق التصدي له)،

(١) تفسير الجلالين آية ٧٠ من سورة الإسراء.

وقد جعلتُه في المباحث الآتية:

تمهيد:

المطلب الأول: المقصود بالإرهاب الإلكتروني الحديث.

المطلب الثاني: خطر الإرهاب الإلكتروني الحديث.

المبحث الأول: وسائل الإرهاب الإلكتروني الحديث

المطلب الأول: البريد الإلكتروني.

المطلب الثاني: إنشاء مواقع وهمية على الإنترنت.

المطلب الثالث: الشبكات اللاسلكية.

المطلب الرابع: الأنظمة السحابية.

المطلب الخامس: أنظمة الرصد والمتابعة.

المطلب السادس: الأقمار الاصطناعية.

المبحث الثاني: طرق مكافحة الإرهاب الإلكتروني:

المطلب الأول: ترشيح استخدام البريد الالكتروني وطرق الحماية.

المطلب الثاني: مراقبة، حجب وتدمير المواقع الإلكترونية.

المطلب الثالث: مراقبة شبكات الاتصال.

الخاتمة.

تمهيد

المطلب الأول: المقصود بالإرهاب الإلكتروني الحديث

يتألف مصطلح «الإرهاب الإلكتروني» أو(Cyber terrorism) من كلمتين: كلمة مألوفة (Cyber) ومتداولة، وتعني الإنترنت، والكلمة الأخرى (Terrorism) وتعني الإرهاب، وحتى الآن لم تُعرّف تعريفاً محدداً، ولا يختلف الإرهاب الإلكتروني عن الإرهاب العام إلا في نوعية الأداة المستخدمة لتحقيق الغرض الإرهابي، أما لغةً فالإرهاب في اليونانية القديمة: حركة من الجسد تفزع الآخرين[١].

وقال مَجمع اللغة العربية في معجمه الوسيط عن الإرهابيين: وصف يُطلق على الذين يَسلكون سبيل العنف لتحقيق أهدافهم[٢]؛ فكلمة إرهاب تُستخدم للرعب أو الخوف الذي يسببه فردٌ أو جماعةٌ أو تنظيمٌ؛ سواء لأغراض سياسية أو شخصية أو غير ذلك، وقد وضع وزراء العرب للداخلية والعدل في الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م؛ تعريفاً للإرهاب بأنه: كل فعل من أفعال العنف أو التهديد أيًّا كانت بواعثُه وأغراضُه، يقع تنفيذًا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس، أو ترويعِهم بإيذائهم، أو تعريضِ حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو اختلاسها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر[٣]، فالإرهاب: كل عملية نفسية تهدف إلى هدْم معنويات الخَصم وإحداث اضطراب نفسي[٤].

---

(١) الإرهاب السياسي والقانون الجنائي، عبد الرحيم صدق، ص٨١.

(٢) المعجم الوسيط ١/ ٣٧٦.

(٣) الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م.

(٤) الدكتور / زكريا إبراهيم الزميلي، موقف الخطاب الديني من الإرهاب، ص٨.

يسعى الإرهاب إلى ترويع الآمنين، والتهديد والفزع والهلع والذعر والفتنة والاضطراب العنيف، ويرمي إلى إشاعة الخوف من أجل السيطرة أو التسلط، وذلك لتحقيق أغراضٍ دنيئةٍ ما.

ومن أفضل التعاريف الاصطلاحية له من حيث الشمولية وتحديد سلوك الإرهاب: ما توصل إليه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي؛ فقد عرَّفه بأنه: «العدوان الذي يمارسه أفراد أو جماعات أو دول بغيًا على الإنسان دينه، ودمه، وعقله، وماله، وعِرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وما يتصل بصور الحرابة وإخافة السبيل وقطع الطريق، وكل فعل من أفعال العنف أو التهديد، يقع تنفيذًا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم، بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر، ومن صنوفه: إلحاق الضرر بالبيئة أو المرافق العامة والأملاك الخاصة أو الموارد الطبيعية، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها»[(١)(٢)].

إذن فالإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل الإلكترونية الصادرة من الدول أو الجماعات أو الأفراد على الإنسان أو دينه، أو نفسه، أو عِرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض.

والإرهاب الإلكتروني من الموضوعات الحديثة التي فرضت نفسها بقوة على مستوى البحوث المتقدمة التي تشغل بال الأفراد والشعوب، وقد تباينت

(١) انظر: بيان مكة المكرمة الصادر عن المجمع الفقهي لرابطة العالم الإسلامي، الدورة السادسة عشرة، مكة المكرمة، رابطة العالم الإسلامي، ١٤٢٢هـ، ص٨.

(٢) انظر: حسن بن محمد سفر، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، بحث مقدم لمجمع الفقه الإسلامي الدولي، ٢٠٠٩، ص: ٩.

وتعددت مظاهره، فمنها ذو المدلول المادي، ومنها الاجتماعي، ومنها العقائدي، ومنها السياسي، وبرز كأداة لتخريب قواعد البيانات والمواقع الإلكترونية[١] وأنظمة الاتصالات الحديثة، ومن ثم السيطرة على الأفراد والشعوب، وتزداد خطورة هذا الانحراف التكنولوجي عندما يتعلق الأمر بالسيطرة على فكر الإنسان وتحطيم قدراته العقلية، وبالتالي يجسد تهديداً قاتلاً لأمن واستقرار الشعوب.

وقد مثل سرعة تحول الإرهاب الإلكتروني من مدلوله المادي إلى مدلول فكري عقائدي يضر بمكتسبات الأمم وتوازنها الاجتماعي؛ تساؤلاً كبيراً للباحثين والقائمين على دراسته.

ولئن نجحت بعض الدول في الحد من هذه الظاهرة بتطوير استراتيجيات وتقنيات للتصدي والوقاية؛ فإن العديد منها سقط فريسة سهلة لهذا المارد المتصاعد، والتجارب الناجحة في الحد من هذه الظاهرة؛ استندت على نشر الوعي بين مواطنيها والاحتكام لتعاليم ديننا الإسلامي السمحة المعتدلة؛ بعيداً عن كل أشكال الغلو والتطرف، حيث قامت بتركيز استراتيجيات تقنية ذكية، ولكن من جهة مقابلة يُعْرف منفذي الهجمات الإلكترونية أو قراصنة المعلومات (hackers) بذكائهم وسرعة إيجاد الثغرات وتنوع أساليب القرصنة المعتمدة.

استناداً لهذا العرض الأخير؛ يمكنني تعريف الإرهاب الإلكتروني الحديث كفعل إجرامي خطير تكون أدوات تنفيذه تكنولوجية، يمارسه أشخاص أو منظمات أو دول، متخفُّون وراء شبكات اتصال معقدة، باعتماد ذكاء اجتماعي

---

(١) انظر: ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، ٢٠٠٨.

وتقني للتجسس أو للسيطرة أو للإضرار بمحتويات رقمية بهدف السيطرة على مكتسبات غير العقائدية والثقافية والاجتماعية والمادية.

المطلب الثاني: خطر الإرهاب الإلكتروني الحديث

المفهوم السائد للإرهاب الإلكتروني يعبر عن حجم الأضرار التي يمكن أن تصيب الأفراد والمنظمات والدول، ولئن اختلفت حدة تأثيرها حسب منطقٍ ما؛ كالخسارة المادية، وتعطيل سير المعاملات التجارية، وتسرُّب المعلومات الأمنية والعسكرية، أو السيطرة وتوجيه العقول البشرية؛ فإننا اليوم أمام أشكال جديدة من الإرهاب الإلكتروني العابر للقارات.

ويمكننا تصنيف خطر الإرهاب الالكتروني الحديث حسب:

- الهدف المراد استهدافه (أفراد، منظمات، دول).
- الغاية من الاستهداف: (تجسس أو سيطرة أو تخريب).
- حدة التأثير أو حجم الخسائر(محدود أو متوسط أو كبير).
- المدلول (مادي، اجتماعي، ثقافي، عقائدي، سياسي).
- هوية منفذيه (هواة، خبراء مجهولين، تنظيمات معروفة، دول).

وفي السنوات الأخيرة زاد عدد المواقع الإرهابية ومقاطع الفيديو الداعية للتطرف وغسل أدمغة شبابنا، وتجنيدهم للقيام بعمليات تتنافى مع البعد الإنساني والأخلاقي وتعاليم ديننا الحنيف، القائم على الوسطية والمنافي لكل تطرف أيًّا كان مصدرُه.

وأقدم في الجدول التالي تصنيفاً تقنياً حديثاً لخطر الإرهاب الإلكتروني حسب الخصائص المحددة سابقاً:

الوسيلة	الهدف المراد استهدافُه	الغاية من الاستهداف	هوية منفذيه	المدلول	حدة التأثير أو حجم الخسائر
البريد الإلكتروني	الأفراد	الفضول، الابتزاز، التشهير	أصدقاء، زملاء عمل، هواة، مرتزقة	مادي أو اجتماعي	تأثير مادي محدود، وتأثير نفسي كبير
	المنظمات	الابتزاز، التجسس على الموازنات والصفقات، كسب غير مشروع	منظمات ذات الصلة، منظمة منافسة، منظمات إرهابية	مادي، ثقافي، عقائدي	الفوز بالصفقات، السطو ومن ثم الإفلاس، تدمير الخطط ، التأثير على منتسبي هذه المنظمات
	الدول	التجسس، التدمير	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	سياسي، عقائدي	الاطلاع على أسرار الدول وإفشائها، تدمير خادم البريد الإلكتروني وقطع تبادل الرسائل
إنشاء أو تدمير مواقع على الإنترنت	الأفراد	استباحة الحرية الشخصية، قرصنة المدونات وصفحات الويب الشخصية، الدعوات الإرهابية	أصدقاء، زملاء عمل، هواة، مرتزقة	اجتماعي	تأثير نفسي كبير

الوسيلة	الهدف المراد استهدافُه	الغاية من الاستهداف	هوية منفذيه	المدلول	حدة التأثير أو حجم الخسائر
	المنظمات	اختراق مواقع المنظمات ونشر معطيات مزيفة من خلالها، اختلاس البيانات المصرفية، الدعوات الإرهابية	منظمات ذات الصلة، منظمة منافسة، منظمات إرهابية	مادي، ثقافي، عقائدي	خسارة مادية فادحة وعدم القدرة على السيطرة على بنك المعلومات
	الدول	اختراق وقرصنة المواقع الأمنية، إنشاء مواقع للدعوات الإرهابية والتجنيد، إنشاء مواقع لتصنيع المتفجرات، إنشاء مواقع تدعو للعنف والكراهية	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	عسكري، سياسي، عقائدي، اجتماعي، اقتصادي	دمار وخراب المجتمعات، دمار البنية الاقتصادية، انحلال وتطرف فكري
الشبكات اللاسلكية	الأفراد	قرصنة الحواسيب الشخصية	زملاء عمل، مرتزقة	اجتماعي	تأثير مادي ونفسي
	المنظمات	قرصنة الشبكات المحلية للمنظمات	منظمات ذات الصلة، منظمة منافسة، منظمات إرهابية	مادي، ثقافي،	خسارة مادية فادحة، وعدم السيطرة على شبكة الاتصالات

الوسيلة	الهدف المراد استهدافُه	الغاية من الاستهداف	هوية منفذيه	المدلول	حدة التأثير أو حجم الخسائر
	الدول	قرصنة قواعد البيانات وشبكات الاتصال المحلية، تعطيل الخدمات	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	عسكري،سياسي، عقائدي، اجتماعي، اقتصادي	التجسس على الشبكات المحلية، تدمير كامل للمعطيات
الأنظمة السحابية	الأفراد	قرصنة الهواتف الذكية	زملاء عمل، مرتزقة	اجتماعي	تأثير مادي و نفسي
	المنظمات	قرصنة الشبكات السحابية والخوادم الافتراضية	منظمات ذات الصلة، منظمة منافسة، منظمات إرهابية	مادي، ثقافي	تحويل وجهة المعطيات، تدمير الخوادم الافتراضية
	الدول	قرصنة الشبكات السحابية والخوادم الافتراضية، نشر أو تحميل معطيات تدعو للإرهاب (مقاطع فيديو أو مواقع وهمية)، نشر تطبيقات ذكية للقرصنة، إنشاء شبكات لاسلكية مشفرة	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	عسكري، سياسي، عقائدي، اجتماعي، اقتصادي	التجسس على الشبكات المحلية، تدمير كامل للمعطيات المخزنة بالخوادم الافتراضية

الوسيلة	الهدف المراد استهدافُه	الغاية من الاستهداف	هوية منفذيه	المدلول	حدة التأثير أو حجم الخسائر
أنظمة الرصد والمتابعة	الأفراد	رصد تحرك الأفراد بدقة، الترهيب	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	أمني، سياسي،اجتماعي	إمكانية ارتكاب جرائم القتل
	المنظمات	التجسس على المنظمات ومتابعة تنقلات أفرادها	منظمات ذات الصلة، منظمة منافسة، منظمات إرهابية	أمني، سياسي، مادي، ثقافي	إمكانية ارتكاب جرائم القتل
	الدول	رصد كل التحركات داخل منظومة معينة بالدولة، انتهاك الحدود الفكرية والعقائدية و العمل على تفكيك استراتيجية الأمن الإلكتروني	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	عسكري، سياسي، عقائدي، اجتماعي، اقتصادي	اكتشاف الثغرات الأمنية والقدرة على تدمير دفاعاتها، ارتكاب جرائم القتل
الأقمار الاصطناعية	الأفراد	التجسس والسيطرة على الأفراد عن بُعد	خبراء تكنولوجيا معلومات، منظمات إرهابية، دول أخرى	أمني، سياسي،اجتماعي	إمكانية ارتكاب جرائم القتل

الوسيلة	الهدف المراد استهدافُه	الغاية من الاستهداف	هوية منفذيه	المدلول	حدة التأثير أو حجم الخسائر
	المنظمات	التجسس على المنظمات والسيطرة على كل تحركاتها وأنظمتها	منظمات ذات الصلة، منظمة منافسة، منظمات إرهابية	أمني، سياسي، مادي، ثقافي،	إمكانية ارتكاب جرائم القتل
	الدول	رصد كل التحركات داخل الدولة والتجسس على الأنظمة الأمنية والعسكرية	خبراء تكنولوجيا معلومات، خبرات اتصالات لاسلكية وأقمار اصطناعية منظمات إرهابية، دول أخرى	عسكري، سياسي، عقائدي، اجتماعي، اقتصادي	التدمير عن بُعد باستعمال أحدث تكنولوجيا الأقمار الاصطناعية المشوِّشة أو العسكرية

المبحث الأول

وسائل الإرهاب الإلكتروني

المطلب الأول: البريد الإلكتروني

هو خدمة توفر التبادل للرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، وأصبح من أكثر الوسائل استخدامًا في مختلف القطاعات، وخاصة قطاع التجارة الإلكترونية لكونه أكثر سهولةً وسرعةً لإيصال الرسائل؛ وهو أكثر الوسائل المستخدمة في الإرهاب الإلكتروني والتواصل بين الإرهابيين وتبادل المعلومات بينهم، يستغلونه في نشر أفكارهم والترويج لها وتكثير أتباعهم والمتعاطفين معهم عبر المراسلات الإلكترونية.

ومما يقوم به الإرهابيون: اختراق البريد الإلكتروني للآخرين، وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية، وقد نهانا الله عن التجسس، فقال سبحانه: ﴿وَلَا تَجَسَّسُوا﴾ [الحجرات: ١٢]، ونهت الشريعة الإسلامية عن الاطلاع على أسرار الناس وهتك حرماتهم، ففي الحديث أن النبي ﷺ قال: «**إنك إن اتبعتَ عوراتِ المسلمين أفسدْتَهم أو كِدْتَ أن تفسدهم**»[(١)(٢)].

واختراق البريد الإلكتروني تقنياً يتم بعدة طرق نعرضها أكثرها شيوعاً وأكثر تهديداً:

---

(١) أبو داود الأدب (٤٨٨٨).

(٢) رواه أبو داود، حديث رقم (٤٨٨٨)، وقال عنه النووي: إسناده صحيح. انظر: رياض الصالحين باب النهي عن التجسس، ص٥٩٦.

- **الطريقة الأولى**: الروابط الوهمية (Fake Link)

حيث يرسل المخترق رسالةً نصية إلى الضحية؛ بداخلها رابط نحو موقع يكون مفخخًا، من خلاله يتم رصد كلمات العبور.

- **الطريقة الثانية**: الصفحات المزورة (Fake Page)

هي موقع إلكتروني مصمم أو معدل بواسطة المخترِق (الهكر)؛ يأخذ مصدر برمجية (code) الصفحة الأصلية، ويرسل بياناتك للمخترق[1] فتظهر الصفحة الإلكترونية مطابقة للصفحة الرسمية لموقع آخر، وفي حال كانت الصفحة تزويراً لموقع حساس (بنك مثلاً)، فإن المستخدِم المخدوع قد يُدخل بيانات حسابه في الصفحة المزورة، مما يؤدي إلى سرقة هذه المعلومات، تطبق هذه الطريقة مع قرصنة المواقع الاجتماعية.

- الطريقة الثالثة: برمجيات التجسس (Spyware)

بدعوة المستخدم لتفعيل خدمةٍ ما، وبمجرد تفعيلها يتم البرنامج بالانتشار تلقائيًا داخل جهاز الضحية واختراق البريد الإلكتروني، ويقوم برصد والتقاط حركات لوحة الكتابة وكل العمليات وإرسالها تلقائيًا للمخترِق[1]، وتُعد هذه الطريقة من أكثر الطرق ترهيبًا للمستخدمين.

هذه الطرق تعتمد على سذاجة المستخدم أو انعدام الحد الأدنى من المعرفة بتكنولوجيا المعلومات وأساسات الأمن الإلكتروني، فيتم التغرير به من

---

(١) انظر: عبادة أحمد عبادة، التدمير المتعمد لأنظمة المعلومات الإلكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، ٢٠١٠.

خلال عرض روابط مفخخة[١]، ومن ناحية أخرى يتم استدراج المستخدم والتعرف على العديد من المعطيات التي قد تبدو بسيطةً لا تشكل تهديداً كمكان الولادة والوظيفة ونوع الهاتف الجوال واسم نظام التشغيل..إلخ. ويسمى هذا الأسلوب: الهندسة الاجتماعية (Engineering Social).

المطلب الثاني: إنشاء مواقع وهمية على الإنترنت

يقوم الإرهابيون بإنشاء وتصميم مواقع وهمية على شبكة الإنترنت؛ لنشر أفكارهم والدعوة إلى مبادئهم، ومن ثم تجنيدهم عن بُعد وتعليمهم كيفية القيام بالعمليات الإرهابية، فقد أُنشئت مواقع لشرح كيفية صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول للمواقع المحجوبة، وطريقة نشر التهديدات الإرهابية.

والموقع هو: معلومات مخزنة بشكل صفحات داخل خوادم (Servers) عالية الكفاءة والأداء. وإن كان مطوِّرو وخبراء مواقع الويب؛ يعتمدون على لغات برمجة معقدة مثل PHP، AJAX، ASP، JavaScript؛ فإن العديد من المخترقين يستخدمون برمجيات مساعدة تمَكِّنهم من إنشاء مواقعهم في دقائق معدودة دون الحاجة لأن يكونوا خبراء[٢]، كما يحظون بخدمات الاستضافة

(١) انظر: سايمون كولن، التجارة على الإنترنت، نقله إلى العربية: يحيى مصلح، بيت الأفكار الدولية بأمريكا، ١٩٩٩.

(٢) انظر: محمد بن عبد الله القاسم، رشيد الزهراني، عبد الرحمن بن عبد الله السند، عاطف العمري، تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، ٢٠١٢.

المجانية لمواقعهم، وهو ما يعزز قدرتهم على التخفي، وقاموا بإنشاء منتديات الحوار وغرف الدردشة، وأمكنهم أن يجمعوا أتباعًا وأنصارًا عبر إشاعة أفكارهم ومبادئهم الهدامة، وهو ما شكَّل وجهاً من وجوه الإعلام الجديد القائم على مواقعَ تضمن انتشاراً أوسعَ دون أدنى تكلفة[١].

وجد الإرهابيون ضالتهم في تلك الوسائل الإلكترونية الرقمية، فأصبح للمنظمات الإرهابية عدة مواقع على شبكة الإنترنت، فغدت تلك المواقع من أبرز الوسائل المستخدمة في الإرهاب الإلكتروني.

المطلب الثالث: الشبكات اللاسلكية

نظامٌ مَرِنٌ لتوصيل البيانات، وتستخدم كامتدادٍ أو كبديل للشبكة السلكية، حيث تقوم هذه الشبكة ببث المعلومات عن طريق تقنية ترددات أمواج الراديو Frequency Radio عبر الأثير، تتيح أنظمة الشبكات اللاسلكية لمستخدميها إمكانيةَ الدخول علي البيانات فوراً في أي وقت وأي مكان في المؤسسة التي يعملون بها، ويعتمد المخترقون على طرق قرصنة حديثة تمكِّنهم من التقاط حزمات المعطيات (Packets) وتخزينها وتحليلها واستخراج كلمات السر، ويتم ذلك من خلال الكشف عن الشبكات اللاسلكية (scan)، ثم الولوج إليها والتقاط المعطيات المتداوَلة داخلها (Sniffing).

---

(١) انظر: حسن بن محمد سفر، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، مجمع الفقه الإسلامي الدولي، الدورة الرابعة عشرة، الدوحة- قطر، ٢٠٠٣.

وهكذا ينجح المخترقون في تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود المخترق في الدولة التي اختُرقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد منَ الاختراقات الإلكترونية، ولا تزال نسبة كبيرة من الاختراقات لم تُكتشف بعدُ بسبب التعقيد الذي يتَّصف به نظام تشغيل الحاسب الآلي[١]،كما يمكن استغلال ضَعف مستوى الحماية الإلكترونية لتنفيذ هجمات الحرمان من الخدمات أو هجوم حجب الخدمة (Denial of Service Attacks).

المطلب الرابع: الأنظمة السحابية

الأنظمة السحابية (Cloud Computing) من التكنولوجيات الحديثة في مجال هندسة الأنظمة والشبكات وتخزين المعطيات، إذ يمكن من خلالها إنشاءُ عدة خوادم افتراضية على جهاز واحد فقط،كما يَسهل التعامل مع خاصياتها التقنية من حيث اتصالها ببقية الشبكات، وهو ما يوفر فضاءً افتراضياً وبيئةَ عملٍ متكاملةً لقرصنة الشبكات الأخرى دون تكلفة كبيرة، ويقوم الإرهابيون بإخفاء عناوين خوادمهم (IP Address) باستمرار أو باستعمال عنوانين وهمية، مما يُصعب ملاحقتهم واكتشافَ قنوات الاتصال لديهم.

(١) انظر: الاختراقات الإلكترونية: خطر كيف نواجهه، موزة المزروعي، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، ص٥٤، ٢٠٠٠م.

المطلب الخامس: أنظمة الرصد و المتابعة

ترتكز مراقبة تنقُّل الأفراد وتتبُّع تحركاتهم؛ على نظام تحديد المواقع العالمي (Global: GPS Positioning System)[١]؛ إذ يمَكِّن المخربين من تتبُّع ضحاياهم عن بُعد وتحديد مواقعهم بطريقةٍ آنيَّةٍ في أي مكان من العالم، كما يمكنهم رصد تحركات الآليات، وترتكز على تتبُّع الهواتف الذكية والتي يمكن اختراقُها بسهولة، أو من خلال زرع شريحة إلكترونية[٢]، وبالتالي إنشاء خريطة لمواقع التحرك، كما أن توفُّر المواقع التي تَرصد تحرك الطائرات والبوارج والمواقع العسكرية والأمنية؛ أعطى الإرهابيين مصدراً مجّانياً مهماً للمعلومات، في غياب سياسات أمنية تحجب هذه المواقع.

المطلب السادس: الأقمار الاصطناعية

تمثل الأقمار الاصطناعية ذُروة التطور الإلكتروني والتقني الذي تعيشه البشرية[٣]، ومثَّل البعض منها سنداً علمياً وسِلمياً، فمنها ما يقوم برصد التحولات والتقلبات الجوية، ومنها ما يخدم القنوات الفضائية، وما يخدم البحوث العلمية، لكن تبقى الأقمار الاصطناعية العسكرية الموجهة للتجسس على الأفراد أو المنظمات أو الدول؛ من أكبر التهديدات الإرهابية؛ إذ تقوم بمسحٍ كاملٍ وتصويرِ أدق التفاصيل من الفضاء الخارجي[٤].

---

(١) انظر: طارق بن عبد الله الشدي، مقدمة في الحاسب الآلي وتقنيات المعلومات، دار الوطن للنشر، الرياض، الطبعة الثانية، ص ٥٧-٧٣، ٢٠١١.

(٢) انظر: براين كيريز، غزو قراصنة الكومبيوتر، مجلة تَواصل، تَصدر عن هيئة الإعلام والاتصال، ترجمة رضوان كاظم عزيز، العدد٤١،ص٥٤، ٢٠١٤.

(٣) صالح الفريح، مواجهة جرائم التطرف والغلو والتفكير من خلال الإنترنت، ندوة المجتمع والأمن: الجرائم الإلكترونية، الرياض، ٢٠٠٧.

(٤) محمد بن علي البيشي، إنترنت FirFox، الإرهاب الأخضر، مقالات جامعة الملك سعود، مركز التميز لأمن المعلومات، ٢٠١٠.

المبحث الثاني

طرق مكافحة الإرهاب الإلكتروني

نقدم حلولاً تقنية لمواجهة الخطر المتنامي للهجمات الإرهابية الالكترونية، هذه الحلول تمثل أفضل الفرص لمجابهة هذا الظاهرة، وتتطلب تضافر جهود الأفراد والمنظمات والدول على حدٍّ سواء.

وأهم ما يجب توفيره في هذا: توصيات واستراتيجيات للحماية الإلكترونية نستعرضها فيما يلي:

المطلب الأول: ترشيح استخدام البريد الإلكتروني و طرق الحماية

١ – عدم فتح الرسائل الإلكترونية مجهولة المصدر.

٢ – عدم الضغط على روابط دون التأكد من صحتها.

٣ – تغيير مستمر لكلمة السر مع ربط تغييرها ببريد إلكتروني آخر مختلف في كلمة السر، أو ربطها بالهاتف الجوال حيث يتم إشعارك برسالة نصية في حال تغييرها.

٤ – عدم استعمال كلمة سر بسيطة تحتوي على معطيات معروفة، مثل اسمك، أو تاريخ ميلادك، أو اسم أحد أقاربك..إلخ.

٥ – للمنظمات: إنشاء قواعد وأوامر (Policies) وتفعيلها بحيث تضمن مستوى عالياً من أمن كلمات السر، وهذه السياسة الأمنية تمنع فتح البريد الإلكتروني خارج مجال العمل.

٦ – ربط فتح البريد الإلكتروني بمعطَى تعريفي شخصي (Biometric) كالصوت والبصمة.

٧- عند فتح البريد الإلكتروني يتم إشعار المستخدم بذلك آنياً.

٨- ربط البريد الإلكتروني ببريد ثاني يعمل كمَخزن للمعطيات يمكِّن من استرجاع الرسائل في حال حذفها.

٩- تنبيه المستخدم في حال فتح البريد من جهاز غير جهازه الذي يقع ضبطه للاستقبال أو إرسال البريد دون سواه.

١٠- تحديد مجال فتح البريد فلا يتم استعماله إلا في نطاق جغرافي محدود ومبرمج مسبقاً.

١١- الجهات الحكومية عليها استعمال خوادمها الخاصة وبرمجتها وفقاً لقواعد وأوامر صارمة.

١٢- مراقبة حزمة تدفق البريد الإلكتروني بحيث يتم رفض أية حزمة متتالية تحمل عدداً كبيراً من الرسائل (Anti Email Bomb) حتى لو كانت معلومة المصدر.

١٣- قراءة محتوى البريد جيداً وعدم التسرع بالضغط على المرفقات أو الروابط.

١٤- عدم ترك البريد الإلكتروني مفتوحاً على الهواتف الذكية، لأنه في حال ضياع أو سرقة الجهاز؛ يمكن الدخول للمعطيات بسهولة.

١٥- عدم تنزيل برمجيات تدعوك لقرصنة بريد الآخرين، حيث تكون هي من تقوم بقرصنة بريدك الإلكتروني.

١٦- عدم الانجراف وراء الرسائل التي تعلمك بجوائز مالية أو هدايا أو غيرها من عمليات الكسب غير مشروع أو التغرير.

المطلب الثاني: مراقبة، حجب وتدمير المواقع الإلكترونية

١٧- حجب المواقع الضارة والتي تدعو إلى الفساد والشر، ومنها المواقع التي تدعو وتعلم الإرهاب والعدوان والاعتداء على الآخرين بغير وجه حق.

١٨- على مُزودي خدمات الاتصال؛ تطوير تطبيقات ذكية تقوم بتصفية المواقع الداعية للإرهاب وتصنيع المتفجرات والأسلحة من خلال برمجة خوادم النفاذ (Proxy)، حيث يجب منع كل أشكال المعطيات من نصوص وصور وصوت وفيديوهات من المرور، ويتم منع الوصول إليها مستقبلاً.

١٩- مراقبة مواضيع المنتديات وصفحات الدردشة التي تدعو للفتنة والاقتتال.

٢٠- اقتصار استعمال الشبكة العنكبوتية داخل هياكل الدولة على متطلبات العمل.

٢١- اقتصار المؤسسات التعليمية على مواقع التدريس أو مواقع مختارة من طرف وزارات التعليم للدولة دون سواها.

٢٢- تنزيل برامج من طرف الأولياء لمراقبة استعمال الشبكة العنكبوتية بالنسبة لأطفالهم.

٢٣- متابعة محاولات دخول الأفراد بعضَ المواقع الإرهابية والتعرف على الغاية من ذلك.

٢٤- إقامة منظومة لتوقع الهجمات الإلكترونية كما هو الحال بالنسبة لتوقع الجرائم العادية، ومن ثم دراستها والتصدي لها.

٢٥- لتخفيض حصيلة الإرهاب الإلكتروني: يجب القيام بتدمير المواقع الإرهابية إن لزم الأمر، وليس فقط محاولة تفاديها، لأنها ضارة أخلاقيًا أو فكريًا.

٢٦- عدم ربط قواعد البيانات الحساسة بالمواقع الإلكترونية؛ لأنه في صورة نجاح المخترقين في قرصنة المواقع؛ فإن الأضرار تكون محدودة جداً.

٢٧- إقامة نظام إشعار آلي، ففي صورة قرصنة الموقع يتم غلق الخادم آليًا (Shutdown) وبالتالي لن يتم استعماله من قبل المخترِقين، ويمكن تشغيله من جديد بعد إعادة برمجة خصائصه الآمنة.

٢٨- عدم استعمال خوادم مجهولة المصدر لاستضافة موقعك (Hosting) فأغلب هذه الخوادم تكون ملكًا لشركات ربحية، ويكون مستوى الحماية لديها ضعيفًا.

٢٩- عدم ترك المجال لخدمة الإشهار الإلكتروني بالاندماج مع موقعك.

٣٠- تركيز منصة إلكترونية لمراقبة كل المتغيرات (عناوين أجهزة المستخدمين، خصائص أجهزة المستخدمين، تاريخ دخول الموقع، نسبة الدخول لكل صفحة على حدة...إلخ، تهدف أساسًا إلى إيجاد علاقة ذكية بين عشرات المعطيات لتحديد الأخطار المتوقعة من مستخدمي الموقع، فعادةً وقبل استهداف الموقع؛ يحاول الإرهابيون جمْعَ قدرٍ كبير من المعلومات واستكشاف الثغرات، وبهذا يمكننا تمييزُ المستخدِم العادي والمستخدِم الإرهابي؛ فيتم إيقافُ استخدام الإرهابي للموقع.

٣١- إنشاء مواقع «فخ» (Honey Web site) تعمل على استدراج الإرهابيين والكشف عن أجهزتهم ومنْعها من استخدام بقية خدمات الشبكة العنكبوتية.

٣٢-فرْض قانون ربْط المواقع بجهة حكومية واحدة تعمل على تزويد خدمات الشبكة العنكبوتية بكل أمْن، مع ضبط شروط استغلالها والتنسيق مع بقية الدول.

٣٣-ربْط جميع مُزودي الشبكة العنكبوتية بمركزٍ واحدٍ يقوم بتأمين اتصالها وفقًا لقواعد سلامةٍ إلكترونية صارمة.

٣٤-مساعدة الدولة للأفراد أو المنظمات على الاستفادة من خدمات الشبكة الإلكترونية، وترشيد استعمالها وفقًا لمعايير سلامة عالية الجودة وإنشاء خدمة للتدخل السريع لإنقاذهم في حال تعرضهم للقرصنة الإلكترونية.

٣٥-ترشيد مراقبة عمل المبرمِجين تفاديًا لأي خطأ وثغرات لا يمكنه اكتشافُها.

٣٦-المطلب الثالث: مراقبة شبكات الاتصال

٣٧-عدم استخدام شبكات الاتصال المفتوحة لتداول المعلومات الأمنية، مع تطوير وسائل التحكم في الدخول إلى المعلومات والمحافظة على سِريتها.

٣٨-تشفير تداول البيانات المهمة المنقولة عبر الإنترنت أو عبر الأقمار الاصطناعية.

٣٩-فصل قواعد البيانات المهمة عن بقية أنظمة الاتصال (DeMilitarized: DMZ Zone).

٤٠- رسم حدود واضحة لشبكات الاتصال حتى ولو كانت باتصالٍ خارجي مع شبكات عالمية أخرى.

٤١- مراجعة دورية لتركيبة شبكات الاتصال والاعتماد على أخصائيين في الأمن الإلكتروني للقيام بعملياتٍ بيضاءَ للاختراق (Penetration Test).

٤٢- إلزام كل المنظمات والهياكل الحكومية بالحصول على شهادةٍ تثبت تنفيذَها لسياسةٍ أمنيةٍ إلكترونية صارمة تضمن لمستعملي خدماتها أو شبكاتها الحمايةَ التامة.

٤٣- رصد أي تدفق للمعلومات من وإلى شبكة الاتصال بمراقبة حزمة تدفق المعلومات ونوعها بطريقة آلية؛ تفاديًا لهجمات الحرمان من الخدمات أو هجوم حجب الخدمة (Denial of Service Attacks).

٤٤- تشفير قواعد البيانات المهمة المنقولة عبر شبكات الاتصالات كالأقمار الصناعية، أو عبر الألياف البصرية، بحيث يتم تشفيرُها عند الإرسال أو عند الاستقبال.

٤٥- تطوير منظومةِ خِزَنٍ لقواعد البيانات داخل وخارج المبنى ضِمن شبكة اتصال محمية باستخدام تكنولوجيا الشبكات الافتراضية الخاصة والمؤمَّنة (VPN: Virtual Private Network).

٤٦- استخدام منظومات أمنية إلكترونية لدخول الأشخاص المصرَّح لهم فقط إلى مراكز الخوادم؛ كاستخدام أجهزة التعرف على بصمة العين، أو اليد، أو الصوت، بالإضافة إلى تحليل عمليات الدخول المشبوهة والتي لا تتم ضمن الإطار العادي لسير العمل.

٤٧- إنشاء نظام قائمة سيطرة الوصول (Access Control List System) والتي تعزز عملية دخول المستخدمين حسب صلاحيات محدودة.

٤٨- قياس حزمة التدفق العادية المتداولة حسب ساعات وأيام العمل وتحديد مجال تدفقها، ومن ثم ضبط نظام إنذار في حال اكتشاف تدفق كبير للمعلومات وبدون مبرر.

٤٩- منع ربط الهواتف الذكية بقواعد البيانات المهمة إلا من خلال مِنصات مؤمَّنة.

٥٠- وضع قواعد وآليات استخدام الشبكات بحيث يمنع استخدام الأجهزة الشخصية للاتصال بالشبكة داخل فضاء العمل، ولا يُكتفي فقط بأن تكون سياسات مكتوبة، بل يجب على نظام مشغِّل الشبكة منْعُها آليًا.

٥١- وضع القواعد والسياسات الأمنية وتفعيلها آليًا بطريقة إلكترونية لا يمكن تجاهلُها أو تعطيلُها، فتركيز المنظمات أو الدول على وضع لوائح طويلة وقوانين؛ أمر لم يعد يُجدي نفعًا، بل يجب تفعيلُها ومعاقبةُ كل من لا يلتزم بها وعدم ترك مجال لأعطالها.

الخاتمة

لقد أصبح الإرهاب الإلكتروني من أخطر الظواهر على استقرار الأفراد والشعوب، وأشدها فتكًا بمكتسبات الأمم، فيطرق بابَنا منعزلين أو مجتمعين، بالبيت أو خارجه، ومع الازدياد المطرد لاستعمال تكنولوجيا المعلومات الحديثة، طورتُ في هذا البحث تعريفًا جديداً للإرهاب الإلكتروني الحديث، كفعلٍ إجراميٍّ خطيرٍ تكون أدوات تنفيذه تكنولوجية، يمارسه أشخاص أو منظماتٍ أو دول متخفون وراء شبكات اتصال معقدة؛ باعتماد ذكاء اجتماعي وتقني للتجسس أو السيطرة أو الإضرار بمحتويات رقمية بهدف السيطرة على مكتسبات الغير العقائدية والثقافية والاجتماعية والمادية.

ولتعدد أساليب الإرهاب الإلكتروني وأدواته التكنولوجية، فقد اقترحتُ في هذا البحث (٥٠) نقطة للاعتماد عليها للقضاء على الإرهاب الإلكتروني الحديث حسب نوع التهديد، وهي حلول قابلة للتطبيق والتطوير.

حاولت من خلال هذا البحث أن أقدم جملة من التصورات والحلول الواقعية لمجابهة خطر الإرهاب الإلكتروني الحديث، بمنهج يراوح بين الأسلوب الوصفي التحليلي وبين الأسلوب التقني، فتَسهل بذلك القراءة لمختصي الأمن الإلكتروني ولعامة القراء.

النتائج

أبرز ما توصلت إليه في البحث:

أولًا: أن الإرهاب الالكتروني الحديث؛ ظاهرة خطيرة تهدد السلْم الاجتماعي، وأصبح مرتعًا للتطرف الفكري، ووسيلة لارتكاب أبشع أنواع الجرائم.

ثانيًا: تعددت أساليب الإرهاب الإلكتروني، وتطورت أدواته بتطور التكنولوجيا وتنوعت مصادره، ومن أهمها: البريد الإلكتروني، المواقع الإلكترونية، شبكات الاتصال، الأنظمة السحابية، والأقمار الاصطناعية.

ثالثًا: الإرهاب الإلكتروني الحديث يعتمد مع تكنولوجيا المعلومات، على سذاجة مستخدمي التقنيات الحديثة من هواتفَ ذكية وأجهزة حاسب آلي، فتطور أسلوب «الهندسة الاجتماعية» يقضي بجمع العديد من المعطيات الاجتماعية والثقافية والتقنية والشخصية للضحية، ومن ثَم تنفيذ عمليات القرصنة أو غسيل الدماغ.

رابعًا: يجب ألا تَعتمد الحلول لمقاومة الإرهاب الإلكتروني الحديث؛ على مجرد استراتيجيات ولوائح وقوانين وتوقيع اتفاقيات مع أطراف أخرى؛ بل على تعزيزها من خلال برمجتها إلكترونيًا.

خامسًا: يجب المرور من موقع دفاع ضد الهجمات الإلكترونية الحديثة؛ إلى موقع يضمن تدمير القدرات الإلكترونية للإرهابيين، مع مراعاة القوانين والتشريعات التي تُجرِّم انتهاكَ خصوصية الإنسان وممتلكاته الفكرية.

سادسًا: يجب استحداث أجهزة أمنية متخصصة، قادرة على وضع سياسات الأمن الالكتروني وتنفيذ الإجراءات العقابية، وعلى الكشف آليًا عن أي تهديد إلكتروني والقضاء عليه.

مراجع البحث

- محمد بن علي البيشي، إنترنت FirFox، الإرهاب الأخضر، مقالات جامعة الملك سعود، مركز التميز لأمن المعلومات، ٢٠١٠.
- حسن مظفر الرزو، الفضاء المعلوماتي، بيروت، مركز دراسات الوحدة العربية، ص ٢٥٠، ٢٠٠٧.
- براين كيريز، غزو قراصنة الكومبيوتر، مجلة تَواصل، تَصدر عن هيئة الإعلام والاتصال، ترجمة رضوان كاظم عزيز، العدد ٤١، ص٥٤، ٢٠١٤.
- عبد الفتاح بيومي، عالم الجريمة والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠١٣.
- صالح الفريح، مواجهة جرائم التطرف والغلو والتفكير من خلال الإنترنت، ندوة المجتمع والأمن، الجرائم الإلكترونية، الرياض، ٢٠٠٧.
- طارق بن عبد الله الشدي، مقدمة في الحاسب الآلي وتقنيات المعلومات، دار الوطن للنشر، الرياض، الطبعة الثانية، ص ٥٧-٧٣، ٢٠١١.
- حسين محمد أحمد عبد الباسط، التطبيقات والأساليب الناجحة لاستخدام تكنولوجيا الاتصالات والمعلومات في تعليم وتعلم الجغرافيا، مجلة التعليم بالإنترنت، العدد ١٥، ص ٥٦-٦٧، ٢٠١٤.
- عبد الرحيم صدق، الإرهاب السياسي والقانون الجنائي، دار النهضة العربية - القاهرة، ص٨١، ١٩٨٥.
- زكريا إبراهيم الزميلي، موقف الخطاب الديني من الإرهاب، مُنشأة المعارف، ص٨، ٢٠٠٥.

- الإرهاب السياسي والقانون الجنائي، عبد الرحيم صدق، دار النهضة العربية - القاهرة،١٩٨٥.
- حسن بن محمد سفر، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، مجمع الفقه الإسلامي الدولي، الدورة الرابعة عشرة، الدوحة- قَطر ٢٠٠٣.
- محمد بن عبد الله القاسم، رشيد الزهراني، عبد الرحمن بن عبد الله السند، عاطف العمري، تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، ٢٠١٢.
- سايمون كولن، التجارة على الإنترنت، نقله للعربية: يحيى مصلح، بيت الأفكار الدولية بأمريكا ١٩٩٩.
- عبادة أحمد عبادة، التدمير المتعمد لأنظمة المعلومات الإلكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، ٢٠١٠.
- ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، ٢٠٠٨.