السياسة الجنائية

في مواجهة الإرهاب الإلكتروني

« دراسة مقارنة »

دكتـــــور

سليم محمد سليم حسين

مدرس القانون الجنائي

بالأكاديمية الحديثة

لعلوم الكمبيوتروتكنولوجيا الإدارة

بالمعادي

الملخص

لقد غزت المنظمات الإرهابية في السنوات الأخيرة الفضاء الإلكتروني وجعلته ساحة للقتال. فلم تعتد هذه المنظمات تعتمد على القوة العسكرية مثل الأسلحة والدروع والقنابل فقط، بل أصبحت أكثر ذكاء واستراتيجيتها وتكتيكاتها أصبحت ذات توجه تكنولوجي. بالإضافة إلى ذلك لم تعد أنشطة الإرهابيين قاصرة على تنفيذ الهجمات المادية، وإنما سعوا إلى مهاجمة ضحاياهم من خلال تخريب البنية التحتية للدول من أي مكان بالعالم وبطريقة تخفي هويتهم الفعلية عبر تقنيات الشبكة المظلمة.

ويهدف هذا البحث إلى دراسة وتحليل لثلاثة جوانب رئيسة يثيرها موضوع السياسة الجنائية في مواجهة الإرهاب الإلكتروني:

الجانب الأول: يتعلق بمفهوم الإرهاب الإلكتروني والتمييز بينه وبين بعض المفاهيم التي قد تختلط به، وما الأسباب التي أدت إلى ظهوره ؟ وما الأدوات المستخدمة في تنفيذ هجمات الإرهاب الإلكتروني ؟ وما العوامل التي تدفع الإرهابيين على شن هذه الهجمات ؟ وما وجهاته ؟ وما مظاهر وأشكال الإرهاب الإلكتروني ؟

الجانب الثاني: يتمثل في التساؤل حول الطبيعة القانونية لجريمة الإرهاب الإلكتروني، وما صور الجريمة الإرهابية الإلكترونية ؟ وكيف تعامل المشرع معها في التشريعات المقارنة ؟

الجانب الثالث: يتعلق بمكافحة الإرهاب الإلكتروني والاستراتيجية المثلى في مواجهته والتصدي له، وما هي الإجراءات الوقائية التي يتعين اتخاذها من قبل المنظمات والحكومات والشركات لتجنب الهجمات الإلكترونية ؟ وكيف يمكن إدارة حوادث الإرهاب الإلكتروني والتخفيف من حدتها والحد من أضرارها ؟ وكيف يتم إدارة عواقب حوادث الإرهاب الإلكتروني ؟

Abstract

In recent years, terrorist organizations have invaded cyberspace and made it an arena for fighting. Not only are these organizations relying on military force, such as weapons, armor and bombs, but they have become smarter, their strategy and tactics have become technologically oriented. In addition, terrorist activities are no longer limited to carrying out physical attacks, but they seek to attack their victims by sabotaging the infrastructure of states from anywhere in the world and in a manner that conceals their actual identity through dark network techniques.

This research aims to study and analyze three main aspects raised by the subject of criminal policy in the face of cyber terrorism:

The first aspect: relates to the concept of cyber terrorism and the distinction between it and some of the concepts that may be mixed with it, and what are the reasons that led to its emergence? What tools are used to carry out cyber attacks? What are the factors that drive terrorists to launch such attacks? What are his destinations? What are the manifestations and forms of cyber terrorism?

The second aspect: is the question of the legal nature of the crime of cyber terrorism, and what are forms of the crime of cyber terrorism? How did the legislator deal with them in comparative legislation?

The third aspect: the combat against cyber terrorism and the best strategy in facing and confronting it, and what preventive measures should be taken by organizations, governments and companies to avoid cyber attacks? How can incidents of cyber terrorism be managed, mitigated and reduced in harm's way? and how are the consequences of cyber terrorism being managed?

المقدمة

بالأمس شهد العالم ثورة صناعية غيرت مجري التاريخ، واليوم يشهد ثورة ولكنها من نوع جديد، ألا وهى الثورة التكنولوجية في مجال الأنظمة المعلوماتية وعلوم الحاسب والإنترنت، تلك الثورة لم يتم استخدامها فى الأعمال السلمية فقط، ولكن تم استخدامها بشكل سلبى بعد أن تم التزاوج بين تكنولوجيا الاتصال والمعلومات والإرهاب وظهور مصطلح الإرهاب الالكترونى الذي أصبح أكثر ضراوة من الإرهاب التقليدي، نظرًا لاستغلاله للموارد المعلوماتية المتاحة لتحقيق الأهداف الخاصة بالإرهابيين.

وقد ظهر الارتباط بين الإنترنت والإرهاب بشكل واضح بعد أحداث الحادي عشر من سبتمبر ٢٠٠١، وانتقال المواجهة ضد الإرهاب والإرهابيين من المواجهة المادية المباشرة إلى المواجهة الإلكترونية، وتحولت الحروب الواقعية إلى حروب رقمية، وأصبح الإنترنت من أشد الأسلحة فتكا وهدما إذا ما استُخدم لأغراض سياسية و تحقيق نوايا إرهابية. فالدمار الذي قد يلحقه الهجوم الإرهابي بأنظمة المعلومات التي أصبحت تتحكم في كل مرافق الحياة في المجتمعات التي تعتمد على الكمبيوتر والإنترنت اعتمادا مطلقا قد يعطل حياة هذه المجتمعات بأكملها. فالإرهاب والإنترنت مرتبطان بطريقتين: الأولى ممارسة الأعمال التخريبية لشبكات الكمبيوتر والإنترنت. والثانية أن الإنترنت أصبحت منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف وللاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم، وحشد التأييد لأفكارهم وتجنيد من يتبعهم لتنفيذ مخططاتهم الإجرامية عبر الفضاء الإلكتروني.

أهمية الموضوع:

يكتسب موضوع السياسة الجنائية في مواجهة الإرهاب الإلكتروني أهمية خاصة من كونه يناقش أحد الموضوعات التي تحتل حيزًا مهمًا في النقاشات المُثارة

على الساحة الدولية خلال الفترة الأخيرة، ألا وهو الإرهاب الإلكتروني وذلك ليس لكونه أمرًا غير اعتيادي في طبيعته، بل لأسباب وحجم التهديدات التي يفرضها على المستويات المختلفة (الدول، الشركات، الأفراد). كما أن التهديدات التي يقوم بها إرهابيو الإنترنت تمثل تحديًا مضاعفًا لأنها تتطلب، عند تحليلها، الأخذ في الاعتبار عدة عوامل أهمها: دوافع الإرهابيين، قدراتهم على إحداث الضرر، نقاط الضعف في النظم المعلوماتية، ومدى قدرة الحكومات والمؤسسات والأفراد في الدفاع عن أنفسهم في مواجهة مثل تلك التهديدات.

وتأتي أهمية الموضوع في وقتنا الحالى نظرًا لشيوع ظاهرة الاعتماد على النظم المعلوماتية في القطاعات الاقتصادية وأسواق رأس المال والمؤسسات المالية، فجميع النشاطات العامة في أغلب الدول في الوقت الحالى أصبحت محوسبة، كما أن العديد من الدول أصبحت تعتمد في إدارتها لمرافقها على نظام الحكومة الإلكترونية[1]، وبالتالى تتفاقم الخطورة في المجتمعات التي تدار بنيتها التحتية

---

(1) يقصد بالحكومة الإلكترونية استخدام تكنولوجيا المعلومات في تحسين الخدمات الحكومية التي تقدم للمواطنين والموظفين والشركات عن طريق الخدمات الإلكترونية، مما ينعكس إيجابًا على تسهيل الإجراءات وعلى الصناعة والاستثمار، ويشجع المواطنين على المشاركة في اتخاذ القرار من خلال استطلاعات الرأي التي تتم عن طريق المواقع الإلكترونية الحكومية، وقد تم تبني خدمات الحكومة الإلكترونية في جميع دول العالم مع الاختلاف في مستوي ونوعية الخدمات الإلكترونية المتاحة، ويمر تطبيق الحكومة الإلكترونية بمراحل متدرجة، تبدأ أولها بالظهور على الويب وعرض معلومات بسيطة عن جهة أو جهات حكومية ، تلي هذه المرحلة مرحلة النشر الإلكتروني ، وفي هذه المرحلة يتم زيادة الخدمات الإلكترونية والجهات الحكومية التي تقدم هذه الخدمات، وتتطور هذه المرحلة إلى مرحلة ثالثة تسمي مرحلة الوجود التفاعلي، فينشيئ علاقة تفاعلية بين الجمهور والدوائر الحكومية الموفرة للخدمة؛ بحيث تتوافر أدوات بحث قوية وقواعد بيانات، ويمكن إجراء بعض المعاملات عن طريق الإنترنت بشكل آمن كدفع الضرائب، وقيمة المخالفات، والفواتير، وتتمثل المرحلة الأخيرة من مراحل الحكومة الإلكترونية في الوصول للحكومة الإلكترونية الكاملة، ونصل لهذه المرحلة عندما تقدم الحكومة

بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهل المنال: فبدلا من استخدام المتفجرات، تستطيع الجماعات الإرهابية، من خلال الضغط على لوحة مفاتيح، تدمير البنية التحتية المعلوماتية لهذه المجتمعات وإغلاق المواقع الحيوية وشل أنظمة القيادة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو اختراق النظام المصرفي.

والأخطر أن الإرهاب الإلكترونى لم يعد يقتصر خطره على ممارسة الأعمال التخريبية ضد شبكات الحاسوب والإنترنت، بل امتد ليشمل أنشطة أكثر خطورة تمثلت في الاستخدام اليومي للإنترنت من قبل المنظمات الإرهابية لتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم. فالجماعات الإرهابية أصبح لها حضور وانتشار كبير على الانترنت عبر الصفحات والمواقع الإلكترونية تستخدمه فى الترويج والدعاية الخاصة بهدف استقطاب الشباب من مختلف دول العالم.

ونظرًا لزيادة المواقع الإلكترونية[1] التي تحرض على الإرهاب أو تسهل التخطيط للعمليات الإرهابية وتنفيذها، واحتوائها على معلومات حساسة حول كيفية

جميع خدماتها عبر موقع واحد على الويب؛ بحيث تدمج العديد من الخدمات الحكومية حسب الحاجات والوظائف وليس حسب الوزارات والمؤسسات، مع ضمان الحكومة توفير الشعور لدي الجمهور بوجود أمن معلوماتي والمحافظة على سرية بياناتهم.

See. William Ouko & Yanal Yzing, E-Government Implementation, A dissertation Submitted to The Faculty of Graduate school of the University og Minnesota, 2010. pp. 32-34.

[1] فتنظيم القاعدة على سبيل المثال له العديد من المواقع الإلكترونية والصحف الإكترونية والتى تصدر بلغات مختلفة، كما ظهر مؤخرًا تنظيم " داعش" والذى يستخدم الفضاء الإلكترونى بشكل واسع، وله العديد من المواقع الالكترونية والصحف والتى تصدر بلغات مختلفة ويستخدمها للترويج له، حيث يقوم بنشر الأعمال الإرهابية التى يرتكبها والمصورة بتقنية عالية الجودة تشبه أفلام هوليود، كذلك الترويج لنمط حياة الأفراد فى المناطق التى يسيطر عليها التنظيم، وترويج وتضخيم لقوتهم لتشكيل صورة ذهنية عنهم بأنهم الأقوى والأخطر عالميًا.

إعداد المتفجرات والمواد السامة وصناعة الصواعق بتفاصيل دقيقة ومكونات يمكن الحصول على الكثير منها من أي مكان دون إثارة الريبة، ولا تقتصر خطورة توفر هذه المعلومات على الفئات الضالة، بل يمكن أن تمهد الطريق لارتكاب الجرائم الفردية في ظل اعتماد الجماعات الإرهابية على طرق بسيطة تتيح للجميع الدخول المباشر إلى مواقع محجوبة عبر التصفح العادي أو عبر البرامج التبادلية.

كما تعتبر وسائل التواصل الاجتماعي التي توفرها شبكة الإنترنت من أهم الوسائل التي تتيح للإرهابيين حرية التواصل فيما بينهم وتبادل المعلومات والتنسيق الشامل لشن هجمات إرهابية بعيدًا عن رقابة ومتابعة الأجهزة الأمنية. فضلا عن المزايا الأخرى التي توفرها الوسائل الرقمية للتواصل من سرعة الاتصال وقلة تكلفته وإمكانية المناورة والتخفي عن ملاحقة الأجهزة الأمنية مقارنة بالوسائل الأخرى. بالإضافة إلى ذلك فقد أسهمت هذه التقنية في تدفق الدعم والمساعدات للجماعات الإرهابية، إذ تتيح بواسطة الإنترنت الوصول إلى جمهور ضخم من المانحين وتسمح للأعضاء بالتنسيق سريعًا مع أكبر عدد من الأتباع لضمان سريان سريع ومستمر للتعليمات يضمن أقصى درجات التنظيم لنشاطات المجموعات الإرهابية، كما توفر منبرا للدعاية والتحريض ضد مؤسسات الدولة[١].

---

[١] ففي الأيام الأخيرة نجح قطاع الاتصالات وتكنولوجيا المعلومات بوزارة الداخلية المصرية في ضبط ٥٣ قضية تحريض على العنف عبر شبكة الإنترنت، وذلك من خلال متابعة أنشطة العناصر الإرهابية المحرضة على العنف ضد المؤسسات والمواطنيين عبر صفحات فيسبوك. كما أغلقت أجهزة الأمن بوزارة الداخلية ٥ صفحات حرضت على مهاجمة رجال الشرطة والجيش والقضاء والإعلام، من خلال المنشورات التي تدعو إلى قتل رجال المنظومة العسكرية ومهاجمة مؤسسات الدولة في إطار مخطط يسعي لنشر الفوضي والانفلات الأمني. وقد قدرت الصفحات المحرضة على الإرهاب، التي أعلنت وزارة الداخلية إغلاقها نحو ٣٠٠٠ صفحة، فيما ألقي القبض على ٦٤٣ متهما، في سبيل الجهود المبذولة لمنع حدوث الجريمة الإلكترونية، والحفاظ على أمن واستقرار البلاد. وبالرغم من كل الحملات الأمنية لأجهزة المعلومات بوزارة الداخلية لضبط القائمين على تلك الصفحات المحرضة على الإرهاب، إلا أنه

وأمام هذه الظواهر وتلك التحديات خالجت نفسي العديد من التساؤلات:

أولها: هل هناك علاقة بين الإرهاب المادي والإرهاب الإلكتروني ؟ وما العلاقة بين الجريمة الإلكترونية وجريمة الإرهاب الإلكتروني ؟ وهل يمكن أن يصبح الإرهاب الإلكتروني إرهاب المستقبل ؟!

ثانيهما: ما مظاهر الإرهاب الإلكتروني ؟ وما وجهاته ؟ وما أبرز الجهات المستهدفة ؟ وما خطورته على الأفراد قبل الدول والحكومات ؟ وكيف تنفذ الهجمات السيبرانية ضد البني التحتية للنظم المعلوماتية والشبكات ؟ وهل تكفي القوانين الجنائية التقليدية في مواجهة هذه النوعية من الجرائم الإرهابية ؟

ثالثهما: هل ستدفع خطورة هجمات الإرهاب الإلكتروني مطوري تكنولوجيا المعلومات للقيام بأنشطة حماية وسد الثغرات لحماية الفضاء الإلكتروني لكي لا يصير ساحة للإرهاب ؟ وهل تكفي الإجراءات الوقائية التي تتخذها الشركات أو المنظمات أو الحكومات عبر استخدام الحلول التكنولوجية فقط في تجنب هجمات الإرهاب الإلكتروني؟ أم ينبغي التعامل مع الإرهاب الإلكتروني من خلال استراتيجية شاملة لمكافحته والتصدي له ؟

ولقد حاولت الإجابة على هذه التساؤلات من خلال اختيار موضوع الدراسة « السياسة الجنائية في مواجهة الإرهاب الإلكتروني» إلاَّ أَنه يتعين علينا في سبيل الإجابة على هذه التساؤلات المحورية أن نتصدى بالتحليل والدراسة لثلاثة جوانب رئيسة يثيرها الموضوع.

مازالت هناك صفحات تعلن عن مسئوليتها بكل فخر وتباهي عن جرائمهم الإرهابية التي يرتكبونها ضد مؤسسات الدولة.

تهامي محمد، رغم إغلاق مئات صفحات التحريض .. تنظيمات الإرهاب مازالت تتحدي الداخلية عبر فيسبوك، جريدة التحرير، في ٢٠١٧/٨/٣٠، على الرابط الإلكتروني للجريدة:
https://www.tahrirnews.com/

أولهما يتعلق بمفهوم الإرهاب الإلكتروني والتمييز بينه وبين غيره من المفاهيم التي قد تختلط به، وما الأسباب الخاصة لظهوره ؟ وما أدواته ووسائله ؟ وما دوافع هجمات الإرهاب الإلكتروني ؟ وما وهي وجهاته ؟ وما مظاهره وأشكاله ؟

وثانيهما يتمثل في التساؤل حول الطبيعة القانونية لجريمة الإرهاب الإلكتروني، وما صور الجريمة الإرهابية الإلكترونية ؟ وكيف تعامل المشرع معها في التشريعات المقارنة ؟

ويتعلق الجانب الأخير بمكافحة الإرهاب الإلكتروني والاستراتيجية المثلي في مواجهته والتصدي له، وما الإجراءات الوقائية التي يتعين اتخاذها لمنع شن هجمات الإرهاب الإلكتروني ؟ وكيف يمكن إدارة حوادث الإرهاب الإلكتروني والتخفيف من حدة الهجمات السيبرانية والحد من أضرارها ؟ وكيف يتم إدارة عواقب حوادث الإرهاب الإلكتروني ؟

لذلك رأيت تناول موضوع البحث من خلال بيان مفهوم الإرهاب الإلكتروني وأبعاده وملامحه، ثم تسليط الضوء على جرائم الإرهاب الإلكتروني في التشريعات المقارنة، والأسلوب الأمثل في مكافحتها والتصدي لها.

منهج البحث:

لقد حاولت في هذا البحث اتباع منهج الدراسة التحليلية التأصيلية المقارنة التي تعتمد على تحليل نصوص قوانين العقوبات، وقوانين مكافحة جرائم تقنية المعلومات في التشريعات المقارنة المتعلقة بالموضوع، بالإضافة إلى الاطلاع على الاستراتيجيات المختلفة لمكافحة الإرهاب الإلكتروني وحماية البني التحتية الحيوية في الدول التي تعتمد بشكل أساسي في إدارة مرافقها على تكنولوجيا المعلومات والإنترنت هذا المنهج الذي يركز على دراسة الواقع الفعلي لظاهرة الإرهاب الإلكتروني وتقصي أسبابها وعرض سبل مواجهتها والتصدي لها.

خطة البحث:

سنتناول دراسة موضوع السياسة الجنائية في مواجهة الإرهاب الإلكتروني من خلال أربعة فصول: نخصص الأول للوقوف على مفهوم الإرهاب الإلكتروني، والثاني لبيان أبعاد وملامح الإرهاب الإلكتروني، والثالث للتعرف على جرائم الإرهاب الإلكتروني في التشريعات المقارنة، والرابع، نتناول فيه استراتيجية مكافحة الإرهاب الإلكتروني وذلك على النحو التالى:

الفصل الأول: مفهوم الإرهاب الإلكتروني.

الفصل الثاني: أبعاد وملامح الإرهاب الإلكتروني.

الفصل الثالث: جرائم الإرهاب الإلكتروني في التشريعات المقارنة.

الفصل الرابع: مكافحة الإرهاب الإلكتروني.

بينما أخصص الخاتمة للوقوف على النتائج التي أسفر عنها البحث وما تفرع عنها من توصيات.

الفصل الأول
مضمون الإرهاب الإلكتروني

بات الإرهاب الإلكتروني يشكل هاجسًا يقلق جميع دول العالم من تعرضها للهجمات الإرهابية التخريبية، عبر توظيف الطبيعة المفتوحة للوسائل الإلكترونية، كشبكة الإنترنت والهواتف المتنقلة والخدمات الإلكترونية الأخري، والاستفادة من التقدم الهائل لتكنولوجيا المعلومات والحاسبات الآلية وانظمة الاتصالات في الأنشطة الإجرامية[١].

إلا أن الإرهاب الإلكتروني يوجه مشكلة أساسية تكمن في عدم وجود اتفاق حول ماهيته، خصوصًا أن مفهوم الإرهاب تطور على مدار السنوات الأخيرة، وتداخلت معه العديد من العوامل، بما صعَّب من إمكانية تعريف أحد تجلياته المتمثلة في "الإرهاب الإلكتروني"، الأمر الذي يتطلب إعادة قراءته من جديد لمحاولة فهمه وتحديد ماهيته، والأسباب الخاصة لظهوره، والأدواته المستخدمة في تنفيذ هجماته[٢].

ترتيبًا على ما تقدم سوف نتناول مضمون الإرهاب الإلكتروني في ثلاثة مباحث على النحو التالى:

المبحث الأول: ماهية الإرهاب الإلكتروني.

المبحث الثاني: أسباب ظهور الإرهاب الإلكتروني.

المبحث الثاني: أدوات الإرهاب الإلكتروني.

---

(١) د/ مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة الناصر، العدد الخامس ، المجلد الأول، يناير – يونيو ٢٠١٥، ص ١٣٢.

(2) **Thomas M. Chen, Lee Jarvis & Stuart Macdonald**, "Cyberterrorism: Understanding, Assessment, and Response". New York, Springer 2014, pp vii-viii.

المبحث الأول
ماهية الإرهاب الإلكتروني

ينبغي لتحديد ماهية الإرهاب الإلكتروني أن نتعرض لتعريفه، ثم التمييز بينه وبين غيره من المفاهيم التي قد تختلط به مثل استخدام الإرهابيين للإنترنت، الجرائم الإلكترونية، الجهاد الإلكتروني، والاحتجاج الإلكتروني. ومن ثم سوف نقسم الموضوع إلى مطلبين على النحو التالى:

المطلب الأول: تعريف الإرهاب الإلكتروني.

المطلب الثاني: الإرهاب الإلكتروني والمفاهيم الأخري.

المطلب الأول
تعريف الإرهاب الإلكتروني

على الرغم من ظهور مصطلح الإرهاب الإلكتروني بشكل متزايد في السنوات الأخيرة، إلا أن معناه أضحي متنازعًا عليه، خصوصًا أن التعامل مع الأنشطة الإلكترونية – أيًا كان نوعها – تم إدراجها في إطار المعني الواسع للإرهاب، وهو ما يعتبر أمرًا غير مرغوب فيه، وغير مفيد فيما يتعلق بهذا المفهوم.

لذا سوف يقتضي تعريف الإرهاب الإلكتروني بداية أن نعرف الإرهاب عند أهل اللغة، ثم بعد ذلك في الإصطلاح قبل أن نتطرق للإرهاب الإلكتروني. ومن ثم سنتناول تعريف الإرهاب الإلكتروني في فرعين على النحو التالى:

الفرع الأول: التعريف اللغوي للإرهاب.

الفرع الثاني: التعريف الاصطلاحي للإرهاب.

الفرع الأول
التعريف اللغوي للإرهاب

كلمة الإرهاب مشتقة من رهِب: بالكسر، يرهب، رهبة. ورهبًا – بالضم، ورهبًا بالتحريك بمعنى أخاف. وترهّب غيره: إذا توعّده، وأرهبه ورهّبه: أخافه وفزعه. ورهب الشيء رهبًا ورهبًا، ورهبه: خافه. والاسم: الرّهب، والرهبي، ورهبوت، والرهبوتي[١].

وكلمة "إرهاب" تشتق من الفعل المزيد أرهب؛ ويقال أرهب فلانا: أي خوَّفه وفزَّعه، وهو المعنى نفسه الذي يدل عليه الفعل المضعف رَهّبَ، أما الفعل المجرد من المادة نفسها وهو رَهِبَ، يَرْهبُ رَهْبَةً ورَهْبًا ورَهَبًا فيعني خاف، فيقال: رَهِبَ الشيء رهبًا ورهبة أي خافه. والرهبة: الخوف والفزع[٢].

وفي المعجم الوسيط، الإرهابيون: وصف يطلق على الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم السياسية[٣].

وفي المنجد كلمة الإرهابي تدل على كل من يلجأ إلى الإرهاب لإقامة سلطة[١]، والحكم الإرهابي هو نوع من الحكم يقوم على الإرهاب والعنف تعمد إليه حكومات أو جماعات ثورية[٢].

---

(١) انظر: الصحاح، إسماعيل حماد الجوهري، تحقيق أحمد عبدالغفور عطار، دار العلم للملايين، بيروت، ط ٢، ١٩٧٥م، مادة: رهب.

(٢) انظر: القاموس المحيط، مجد الدين محمد يعقوب الفيروز آبادي، مؤسسة الرسالة، بيروت، ط ٢، ١٤٠٧ هـ /١٩٨٧م، باب الباء فصل الراء، ص ١١٨.

(٣) المعجم الوسيط، معجم اللغة العربية، ط ٢، القاهرة ١٩٧٢، ص ٢٨٢.

و"الإرهاب" في الرائد هو رعب تحدثه أعمال عنف كالقتل وإلقاء المتفجرات أو التخريب، و"الإرهابي" هو مَنْ يلجأ إلى الإرهاب بالقتل أو إلقاء المتفجرات أو التخريب لإقامة سلطة أو تقويض أخرى، و"الحكم الإرهابي" هو نوع من الحكم الاستبدادي يقوم على سياسة الشعب بالشدة والعنف بغية القضاء على النزعات والحركات التحررية والاستقلالية[٣].

وبناءً على ما تقدم يتبين لنا أن الإرهاب في اللغة يدل على الإخافة والترويع والتفزيع والرعب والاضطراب هو المراد للدلالة على الإرهاب.

الفرع الثاني
التعريف الاصطلاحي للإرهاب

قبل التطرق إلى تعريف الإرهاب الإلكتروني لابد أن نشير أولا إلى تعريف الإرهاب المادي أو التقليدي. وذلك على التفصيل الآتي:

أولًا: الإرهاب التقليدي:

اختلف الباحثون في تعريف الإرهاب وتاريخ ظهوره، ومنهم من أهمل مسالة التعريف تلافيا لصعوبته مكتفيا ببحث ظاهرة الإرهاب وسرد خصائصها وصورها[٤]،

---

[١] المنجد في اللغة، دار المشرق، بيروت، ط ٢٩، ١٩٨٦م، ص٢٨٠.

[٢] المرجع السابق، ص ٢٨٢.

[٣] الرائد معجم لغوي عصري، مسعود (جبران)، دار العلم للملايين، بيروت، ط ١، ١٩٦٧م، ص ٨٨.

[٤] ويري أنصار هذا الاتجاه أنه ليس من المناسب وضع تعريف للإرهاب نظرًا لصعوبة التعريفات البريئة أو المقنعة أو المشتركة، فالقيام بتعريف الإرهاب نوع من أنواع المغامرة، وأنّ نقد التعريفات أسهل من استخدامها كأدوات للتمييز بين الإرهاب وغيره من الصور التي تختلط به. لذلك اتجه المجتمع الدولي إلى تحديد أفعال بعينها كي تعتبر إرهابا واستبعد الأفعال الأخري العدوانية من نطاقه، وقد ترتب على ذلك إرجاء الجهود الدولية لوضع اتفاقية عالمية لمكافحة الإرهاب.

بينما سعى البعض الى وضع تعريف محدد وجامع، فكان إن برزت العديد من التعاريف التي تحوي على بعض عناصر الإرهاب والتي من الممكن أن تكون أساسا في تحديد مفهوم هذه الظاهرة.

وتنصب الآراء التي أدلي بها الفقه بصدد تعريف الإرهاب في اتجاهين رئيسيين يدور كل منهما حول محورٍ معينٍ ويرتكزٍ على أساسٍ محددٍ: الأول : مادي يعتمد أنصاره على تعداد العناصر المكونة للإرهاب. والثاني : معنوي يركز

في عرض هذا الاتجاه، انظر: د/ إمام حسنين عطا الله، جرائم الإرهاب الدولي في التشريعات المقارنة – دراسة تحليلية للتشريعات الجنائية العربية والأجنبية والتشريعات الإسلامية، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٠، ص ١٣ وما بعدها؛ د/عصام عبد الفتاح عبد السميع مطر، الجريمة الإرهابية، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٥، ص ٩٦ وما بعدها؛ د/ أحمد عبد العظيم مصطفى المصري، المواجهة التشريعية لجرائم الإرهاب في التشريع المصري والقانون المقارن، رسالة دكتوراه –حقوق القاهرة، ٢٠٠٣، ص ٤٠. انظر ايضا:

Freedman Laweence, et al., Terrorism and International Order, The Royal Institute of International Affairs, Routbedge, 1988. p. 11.

Sliwouski George, Legal Aspects of Terrorism in International World Security, Halsted Press Book, New York, Toronto, 1974. p. 76.

ويسوق أنصار هذا الاتجاه ما يعضد سلامة موقفهم بالقول بان العديد من قمم الدول الكبري لم تتعرض لماهية الإرهاب مفضلة تركيز جهودها على إدانة الإرهاب كقمة الدول الثماني الصناعية الكبري بطوكيو ١٩٨٦ وما تلاها من قمم أخري من عدم الوقوف على تعريف للإرهاب، بل إدانته دون بيان ماهيته، كما ظهر ذلك أيضا في مناقشات الجمعية العامة للأمم المتحدة ١٩٨٥ وضربت صورًا وأمثالًا للإرهاب مثل خطف الطائرات وأخذ الرهائن، والتفتت عن إيراد تعريف له، كما ظهر ذلك في مؤتمر منع الجريمة ومعاملة المسجونين الذي عقد في هافانا ١٩٩٠ والذي اهتم ببيان الإجراءات الفعالة لمكافحة الإرهاب دون بيان ماهيته، كما سلك المؤتمر الدولي لمنع الجريمة ومعاملة المذنبين الذي عقد في القاهرة ١٩٩٥ نفس المسلك، إذ ركز الأخير على جهود مكافحة الإرهاب وتحديد الأسباب الجذرية له والقضاء عليه دون التعرض لتعريفه. انظر:

وثائق مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المذنبين، المنعقد بالقاهرة في الفترة من ٢٩– ٨ مايو ١٩٩٥، الوثيقة رقم (CA/CONF. 169/5) ، ص ٢٠.

أنصاره على الغاية أو الهدف الذي يسعي إليه الإرهابي من خلاله. وذلك على التفصيل التالى:

الاتجاه الأول:

يركز أنصار الاتجاه المادي على السلوك المكون للجريمة أو الأفعال المكونة لها في تعريف الإرهاب دون البحث في الغرض أو الهدف من العمل الإرهابي[١]، وبناء عليه عرف أنصار هذا الاتجاه الإرهاب بأنه عمل أو مجموعة من الأفعال المعينة التي يقصد بها أساسًا إحداث الرعب والخوف[٢]. فالإرهاب يستخدم من منظور الفعل العنيف، والإرهابي هو من يرتكب الفعل سواء تحرك من خلال أيديولوجية سياسية أو دينية أو خليط بينهما.

إلا أن أصحاب هذا الاتجاه اختلفوا فيما بينهم في الطريقة التي تناولوا بها العمل بالتحديد والتعيين، إذ اكتفي البعض بتعداد الأعمال أو الأفعال التي تعد إرهابية بطبيعتها كالقتل، الاغتيال، الاختطاف، احتجاز الرهائن، أعمال القرصنة[٣].

ولا يخفى ما يكتنف هذا التحديد من قصور تمثل في تجاوزه عن أهم عنصر من عناصر الجريمة الإرهابية وهو الغرض أو الهدف السياسي[٤]، كما إن التحديد الحصري لجرائم معينة على إنها إرهابية يؤدي الى خروج الكثير من الجرائم من دائرة

---

(1) **V. De La Cuesta (J-L)**, Traitement Juridique du Terrorisme en Espagne, Rev. Sc. crim, 1997. p. 37 **et voir aussi. Rivero (J)**, Responsabilite de L'ètat et Droits des Victimes d'actes Terrorisme, AJDA, 1993. p. 59.

(٢) د/ أحمد جلال عز الدين، الإرهاب والعنف السياسي: كتاب الحرية، دار الحرية للصحافة والطباعة والنشر، ١٩٨٦، ص ٢٦.

دار الحرية للصحافة والطباعة والنشر

(٣) د/ محمد مؤنس محب الدين، الإرهاب في القانون الجنائي، دراسة قانونية مقارنة على المستويين الوطني والدولي، مكتبة الأنجلو المصرية، ١٩٧٣، ص ٢٠٧-٢٠٨.

(٤) د/ إمام حسانين خليل، نحو اتفاق دولي لتعريف الإرهاب – الجرائم الإرهابية في التشريعات المقارنة، مركز الخليج للدراسات الاستراتيجية، الطبعة الأولي ٢٠٠٨، ص ١٠.

الإرهاب لاالشيء سوى أنها لم تذكر ضمن هذا النوع من الجرائم متجاوزين عما قد يجلبه التطور العلمي والتقني من صور جديدة للجرائم الإرهابية.

إزاء ذلك اتجه غالبية أنصار الاتجاه المادي إلى تحديد صفات معينة للجرائم الإرهابية لتمييزها عن غيرها وعدم الاكتفاء بالتعداد الحصري، ومن تلك الصفات على سبيل المثال لا الحصر:

١- إن الأعمال الإرهابية تتصف بأعمال العنف، أو التهديد، وبذلك لا يقتصر على الإرهاب العنف المادي بل يشمل المعنوي ايضا[١]، لكن تقدير جسامته محل اختلاف الفقهاء. فمنهم من لا يشترط درجة معينة من الجسامة في هذا العنف، في حين استلزم البعض أن يكون عنفًا غير مشروع وقوي[٢]. أو عنف متطرف أو غير اعتيادي[٣].
٢- أن يكون من شان هذا العنف إحداث الرعب أو التخويف أو إحداث قدر من الرهبة في نفوس المجتمع أو طائفة معينة منه بقصد السيطرة عليهم أو توجيههم بما يحقق أغراض الإرهاب النهائية[٤].
٣- أن يتصف العنف بالتنظيم والاتصال فلا يكون عارضًا أو عشوائيًا بل عملًا منسقًا، ومنضمًا، ومستمرًا، على ذلك فعمل الاغتيال الذي لا يكون جزء من نشاط منظم لا يعد إرهابيًا. بالإضافة إلى السرية والمباغتة في تنفيذ العمل الإرهابي.

---

[١] د/ محمد السيد سليم، الإرهاب وسبل معالجته، ندوة مركز الخليج للدراسات الإستراتيجية، ص ٣٨.

[٢] د/ نور الدين هنداوي، السياسة الجنائية للمشرع المصري في مواجهة جرائم الإرهاب، دار النهضة العربية، ١٩٩٣، ص ١٠.

[٣] د/ أحمد محمد رفعت، الإرهاب الدولي في ضوء أحكام القانون الدولي والاتفاقيات الدولية، دار النهضة العربية، ١٩٨٨، ص ١٩٣-١٩٦.

[٤] د/ طارق عبد العزيز حمدي، التقنين الدولي لجريمة إرهاب الدولة، دار الكتب القانونية، ٢٠٠٩، ص ١٦-١٧.

الاتجاه الثاني:

يركز أنصار الاتجاه المعنوي في تعريف الإرهاب على أساس الغاية أو الهدف الذي يسعى إليه الإرهابي من خلال عمله. غير أن أنصار هذا الاتجاه يختلفون في طبيعة هذه الأهداف فهناك أهداف سياسية وأخرى دينية وثالثة فكرية، وهكذا فهل يتعلق الإرهاب بهدف من هذه الأهداف بالتحديد باعتباره الركن المعنوي للجريمة الإرهابية ؟

استقر الرأي الغالب على القول بأن الركن المعنوي في الجريمة الإرهابية يتجلى في غاية الإرهاب ذاته وهو توظيف الرعب والفزع الشديد لتحقيق مآرب سياسية أيًا كان نوعها[١]. وفي ذلك يعرف البعض الإرهاب بشكل عام باعتباره استخدام غير شرعي للقوة أو العنف أو التهديد باستخدامها بقصد تحقيق أهداف سياسية[٢]. أو أن الهدف في الجريمة الإرهابية يتجلى في غاية الإرهاب ذاته وهو توظيف الرعب والفزع الشديد لتحقيق مآرب سياسية أيًا كان نوعها[٣]. فالإرهابيون يستخدمون العمل الإرهابي كحملة سياسية ضد الحكومة أو ضد سياسة معينة لا يوافقون عليها[٤].

غير أن هذا التعريف يشكل نوع من التطابق بين الجريمة السياسية والأعمال الإرهابية وهو أمر غير مقبول لما يقود إليه ذلك من تخفيف للعقوبة وعدم إمكان

---

(1) **V. Bouloc (B)**, Le Terrorisme Problèmes Actuels de Science Criminelle, 11ème Presses Universitaires d'Aix Marseille 1989. p. 65; **Joas Marcello de Arago Junior**, L'extractions dans la Constitution Brésilienne de 1988. Rev. Dr. Pén. Int. 1991, p. 982.

انظر ايضا: د/ أحمد شوقي أبوخطوة، تعويض المجني عليهم عن الأضرار الناشئة عن جرائم الإرهاب، دار النهضة العربية، ١٩٩٩، ص ٤٥.

(٢) د/ هيثم المناع، الإرهاب وحقوق الإنسان، دراسة مقدمة إلى مجلة التضامن العربية، ١٩٩٠، ص ٥٢.

(٣) د/ فكري عطا الله، الإرهاب الدولي– المتفجرات، دار الكتب الحديثة، ٢٠٠٠، ص ١٣.

(٤) د/ أحمد جلال عز الدين، المرجع السابق، ص ٤٦.

تسليم المجرمين[١]، فإذا كان الغرض السياسي عنصرًا مهمًا في الجريمة الإرهابية فهو ليس المعيار الوحيد في تميزها.

إزاء ذلك ذهب البعض[٢] إلى التركيز على عناصر أخرى في التعريف منها استخدام الوسائل القادرة على إحداث حالة من الرعب والفزع بقصد تحقيق الهدف أيًا كانت صورته سياسيًا أو دينيًا أو عقائديًا أو عنصريًا، وفي هذا إخراج للجريمة السياسية والتي يمكن أن تحصل دون اللجوء إلى العنف. كما أنّ الإرهاب له أسباب متعددة عقائدية وفكرية ودينية وعنصرية، ومن ثمّ يكون الهدف السياسي ليس هو المميز الوحيد للعمل الإرهابي ولكن يعد أحد جوانبه[٣].

ومن هذا المنطلق نشايع الرأي[٤] الذي ذهب إلى أن الإرهاب هو طريقة أو أسلوب، فهو سلوك خاص وليس طريقة للتفكير أو وسيله للوصول إلى هدف معين. ويؤيد ذلك أن المقطع الأخير من كلمة Terrorisme بالفرنسية Isme والتي تعني النظام أو الأسلوب – فالإرهاب على ذلك هو الأسلوب أو الطريقة المستخدمة والتي من طبيعتها إثارة الرعب والفزع بقصد الوصول إلى الهدف النهائي.

ونرى أن هذا التعريف مقبول إلى حد كبير فهو يتضمن العناصر الواجب مراعاتها في تحديد مضمون الأعمال الإرهابية وتمييزها عما قد يختلط بها من أفعال أخرى. على أنه من المهم التأكيد على أن تكون أعمال العنف تلك، أعمالا"غير

---

[١] د/ علي حسين الخلف، المبادئ العامة في القانون، بدون دار نشر، ١٩٨٢، ص٢٩٨.

[٢] د/ ديش موسي، النظام القانوني لتعويض ضحايا الجرائم الإرهابية – دراسة مقارنة، رسالة لنيل درجة الدكتوراه، كلية الحقوق جامعة ابي بكر بلقيد– تلمسان، الجزائر ٢٠١٦، ص ٢٨–٢٩.

[٣] د/ مصطفى مصباح دبارة، الإرهاب مفهومه وأهم جرائمه في القانون الدولي الجنائي، منشورات جامعة قاريونس، ليبيا ١٩٩١، ص ١٢٩.

[٤] وهو رأي الدكتور/ إمام حسانين عطا الله. مشار إليه لدي د/ محمد مونس محب الدين، الإرهاب والعنف السياسي، مجلة الأمن العام، عدد ٩٤، سنة ٢٤ يوليو ١٩٨١، ص٢٧٤.

مشروعة لتميز الفعل الإرهابي عن أعمال العنف المشروعة كأعمال المقاومة والكفاح المسلح. ومن ثم يمكن تحديد عناصر تعريف الجريمة الإرهابية فيما يلي:

١- العنف غير المشروع[١].
٢- التنظيم والتنسيق.
٣- أن يؤدي العنف لخلق حالة الرعب والفزع.
٤- أن يهدف العمل إلى تحقيق أهداف سياسية أو دينية أو عقائدية أو عنصرية بعيدة عن الغايات الفردية.

وقد عرف القانون الأمريكي الصادر لسنة ٢٠٠١ لمكافحة الإرهاب والمعروف بـ Patriot Act[٢]، الإرهاب بأنه القيام بالأنشطة التي تتضمن أعمال العنف أو أعمالًا تمثل خطورة على حياة الإنسان، ويكون الغرض منها تخويف السكان المدنيين، أو التأثير على سياسة وأداء الحكومة عن طريق التخويف أو الترهيب بالدمار الشامل أو الاغتيال أو الخطف، وتعد هذه الأعمال إذا ارتكبت داخل الولايات المتحدة، أو أية دولة أخري انتهاكًا للقوانين الجنائية للولايات المتحدة أو غيرها من الدول.

---

(١) د/ أحمد جلال عز الدين، المرجع السابق، ص٢٦.

(2) Public Law 107-56- act, 26, 2001, (USA Patriot act), Act of 2001.

وقد عرف المنظمة الإرهابية بأنها: مجموعة مكونة من فردين أو أكثر علي صلة أو متورطة في أنشطة إجرامية سواء تعلقت بالإرهاب أم لا، وتشمل هذه الأنشطة تقديم الدعم المادي للإرهابيين أو جمع الأموال للمنظمات الإرهابية.

وفي المملكة المتحدة ورد تعريف الإرهاب[١] في المادة الأولي من قانون الإرهاب الصادر لسنة ٢٠٠٠ (Terrorism Act: TA 2000) [٢]، بأنه يقصد بالإرهاب الفعل أو التهديد بالفعل بحيث يشمل:

١- كل فعل يتضمن عنفا خطيرا ضد شخص أو خطر جدي أو يضر بحياة شخص أو ينشئ خطرًا جديًا على الصحة العامة أو على طائفة من الناس أو لكي يعطل نظاما إلكترونيًا.

٢- استعمال العنف أو التهديد به للتأثير على الحكومة أو لترهيب الناس أو طائفة منهم.

٣- استعمال العنف أو التهديد به بغرض إبراز قضية سياسية، دينية، عقائدية.

أما بالنسبة للقانون الفرنسي، فلم يرد به تعريف للإرهاب ولا الجريمة الإرهابية[٣]. بيد أنه نص على عدد من الجرائم التي يمكن تصنيفها إلى مجموعات

---

(١) وقد عرفت المادة ٢٠ من قانون منع الإرهاب الصادر لعام ١٩٨٩ بأنه : « استخدام العنف لتحقيق أهداف سياسية، بما في ذلك أي استخدام للعنف بغرض إشاعة الخوف بين أفراد الشعب، أو بين قطاع منهم».

Prevention of Terrorism (Tempotaty Ptovisions) Act 1989.

(٢) انظر التشريع البريطاني للإرهاب علي الربط التالى:

http//:www.hmso.GOV.UK/ACCT2000/00011-B.HTM, p. 1.

(٣) وقد اتبع المشرع الأسباني نهج المشرع الفرنسي بمعني أنه أخذ بالأسلوب الغائي بنصه علي جرائم بعينها، وإخضاعها لمعاملة عقابية خاصة إذا ارتكبها أشخاص يعتبرون أعضاء في تنظيمات إرهابية أو التمرد باستخدام أسلحة نارية أو قنابل أو متفجرات أو موارد حارقة.

ولمزيد من التفاصيل حول تعريف الإرهاب في التشريعات الأجنبية، انظر:

د/ صباح عبد الرحمن حسن الغيص، السياسة الجنائية لمواجهة الجرائم الإرهابية، رسالة دكتوراه – حقوق عين شمس، ٢٠٠٩، ص ٦٣ وما بعدها؛ د/ علي محمد عامر العجمي، الإرهاب في القانون الجنائي، رسالة دكتوراه– حقوق طنطا، ٢٠٠٩، ص ٦٠ وما بعدها؛ د/ محمد أبو الفتوح غنام، تعريف الإرهاب، مجلة الأمن العام، العدد ١٤٣ س ٣٥، أكتوبر ١٩٩٣، ص ٩ وما بعدها.

ثلاث: **أولها**، تضم بعض جرائم العنف ضد الأشخاص. **وثانيها**، تشمل جرائم الاعتداء التي من شأنها إيجاد خطر عام. **وثالثها**، تضم الجرائم التي تدخل في إطار الخطر العام. وقد اعتبر المشرع هذه الجرائم إرهابية إذا اتصلت بمشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام بصورة جسيمة عن طريق التخويف والترويع[١].

وقد عرف قانون العقوبات المصري المعدل بالقانون رقم ٩٧ لسنة ١٩٩٢ الإرهاب في المادة ٨٦ لهذا القانون بأنه: كل استخدام للقوة أو العنف أو التهديد أو الترويع، يلجأ إليه الجاني تنفيذًا لمشروع إجرامي فردي أو جماعي. بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر. إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بالمواصلات أو بالأموال أو بالمباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها، أو تعطيل تطبيق الدستور أو القوانين أو اللوائح[٢].

---

(1) **Galmard (M.H)**, Vers une nouvelle approche du phénomène terroriste ? Apports de la loi no 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives aux contrôles transfrontaliers, Revue pénitentiaire, Mars 2007. p. 5.

(٢) راجع المادة ٨٦ من قانون العقوبات المضافة بالقانون رقم ٩٧ لسنة ١٩٩٢ بشأن تعديل بعض أحكام قانون العقوبات المصري.

والجدير بالذكر أن المشرع المصري قد عرف العمل الإرهابي في المادة الثانية من القانون رقم ٩٤ لسنة ٢٠١٥ الخاص بمكافحة الإرهاب بأنه: « كل استخدام للقوة أو العنف أو التهديد أو الترويع في الداخل أو الخارج، بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع أو مصالحه أو أمنه للخطر، أو إيذاء الأفراد أو إلقاء الرعب بينهم، أو تعريض حياتهم أو حرياتهم أو حقوقهم العامة أو الخاصة أو أمنهم للخطر، أو غيرها من الحريات والحقوق التي كفلها الدستور والقانون، أو الإضرار بالوحدة الوطنية أو السلام الاجتماعي، أو الأمن القومي، أو

ثانيًا: الإرهاب الإلكتروني:

كما اختلفت الأراء في تعريف الإرهاب، اختلفت أيضا فيما يخص الإرهاب الإلكتروني[١]. فهناك من يري أنه ظاهرة جديدة [١]، أو نوع من الجرائم الإلكترونية

إلحاق الضرر بالبيئة، أو بالموارد الطبيعية أو بالآثار أو بالآموال أو بالمباني أو بالأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو منع أو عرقلة السلطات العامة أو الجهات أو الهيئات القضائية أو مصالح الحكومة أو الوحدات المحلية أو دور العبادة أو المستشفيات أو مؤسسات ومعاهد العلم، أو البعثات الدبلوماسية والقنصلية، أو المنظمات والهيئات الإقليمية والدولية في مصر، من القيام بعملها أو ممارستها لكل أو بعض أوجه نشاطها، أو مقاومتها أو تعطيل تطبيق أي من أحكام الدستور أو القوانين أو اللوائح.

كذلك كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبينة في الفقرة الأولي من هذه المادة، أو الإعداد لها أو التحريض عليها، إذا كان من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية أو بالنظم المالية أو البنكية، أو بالاقتصاد الوطني أو بمخزون الطاقة أو بالمخزون الأمني من السلع والمواد الغذائية والمياه، أو بسلامتها أو بالخدمات الطبية من الكوارث والأزمات».

[١] وتجدر الإشارة إلى أن مصطلح الإرهاب الإلكتروني Cyberterrorism قد بدأ في الظهور في أوائل الثمانينيات من القرن الماضي بواسطة Barry Collin وهو باحث رفيع المستوي في معهد الأمن والاستخبارات بولاية كاليفورنيا الأمريكية، فهو مصطلح مزدوج بين مفهوم العلم الإلكتروني والتحكم الآلي وبين مفهوم الإرهاب. راجع:

Barry Collin, 'The Future of Cyberterrorism, Crime and Justice International'. Vol. 13, Issue. 2, March 1997. pp. 15-18; See also **Barry C. Collin**, "The Future of CyberTerrorism: Where the Physical and virtual Worlds Converge", 11th Annual International Symposium on Criminal Justice Issues, 1997. pp. 15-18.

وقد تم تعريف الإرهاب الإلكتروني بشكل مختلف من قبل الباحثين في أوائل الثمانينات من القرن الماضي حيث ينظر إليه علي أنه مزيج من التهديدات المادية العالمية والإلكترونية والتي تنطوي علي هجمات علي الحاسبات والشبكات عبر الإنترنت ، انظر:

Kuboye Oluwafemi Samuel. et al., Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Scienceand Mobile Computing, Vol.3 Issue.5, May 2014. p. 1082.

التي لها أهداف وخصائص معينة [٢]، وآخرون يرون أنه مجرد تكتيك جديد للإرهاب[٣]، حيث يشير مصطلح الإرهاب الإلكتروني في سياقه النظري والعملي إلى ارتباط الاعتداءات الواقعة ضد الحاسبات والشبكات والمعلومات بأهداف سياسية وأخري اجتماعية تؤدي في النهاية إلى حدوث إصابات أو إراقة دماء أو إحداث اضرار جسيمة بالنظر إلى الطبيعة السريعة والمتطورة للهجمات الإلكترونية والتي تحول في الوقت نفسه دون إيجاد حلول سهلة لمواجهة هذه الظاهرة [٤].

وبالرغم من تعدد الآراء التي تناولت الإرهاب الالكتروني واختلافها في التفاصيل إلا أن النتيجة التي انتهت إليها واحدة وهي أن الإرهاب الإلكتروني يتعلق بالإعتداء على البنية التحتية للنظم المعلوماتية[٥]. إذ يذهب البعض إلى أن الإرهاب الإلكتروني هو اعتداء غير مشروع أو التهديد بالاعتداء على أجهزة الكمبيوتر والشبكات المعلوماتية المخزنة فيها بهدف إرهاب الحكومة أو المواطنين لتحقيق

---

(1) **Kinner, W.F. & Fream, A.M**, "A social learning theory analysis of computer crime among college students", The Journal of Research in Crime and Delinquency,Vol. 34, No. 4, 1997. pp. 495-518.
FOLTZ, C. Bryan, "Cyberterrorism, computer crime, and reality", Information Management & Computer Security, Vol. 12 Issue. 2, 2004. pp.154-166.

(2) **Ahmed H. Anjariny et al.,** "Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies", International Journal of Cyber Warfare and Terrorism (IJCWT) Vol 6, Issue I, 2016. p. 1.

(3) **Peter Fleming & Michael Stohl**, Myths and realities of cyber terrorism, reserachgate, January, 2001. p. 4.

(4) **Alan E. Brill,** From Hit and Run to Invade and Stay: How Cyberterrorists Could Be Living Inside Your Systems, Defence Against Terrorism Review. Vol.3, No.2, Fall 2010, pp. 23-36.

(5) **V. Alix DESFORGES**, "Cyberterrorisme: quel périmètre?", Fiche de l'Irsem n° 11, décembre 2011. p. 3. disponible sur: https://www.defense.gouv.fr/content/download/153102/1551441/file/Fiche_n11_perimetre_cyberterrorisme.pdf

Ben Saul & Kathleen Heath, Cyber terrorism, Sydney law of school, Legal studies Research paper, No. 14/11, January 2014. Available at: http://ssrn.com/abstract=2387206.

Ali Jahanger, cyber space, cyber terrorism and information warfare: A perfect recipe for confusion world wide selected speakers, Note 20. 2009.

أهداف سياسية أو اجتماعية أو أيديولوجية، وينبغي أن يكون الهجوم مدمرًا وتخريبيًا لتوليد الخوف والرعب ويكون مشابه للأفعال المادية للإرهاب [١].

وذهب رأي آخر إلى أن الإرهاب الإلكتروني هو كل نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الأفكار المتطرفة، سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد، وإفساد عقائدهم، وإذكاء تمردهم، واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع [٢].

بينما ذهب رأي آخر أن الإرهاب الإلكتروني هو نشاط إجرمي مخطط ومنظم مخالف للقانون يقوم به التنظيم الإرهابي بواسطة التقنية الإلكترونية الرقمية لتحقيق غرض معين تحت تغطية [٣]. وذهب رأيٌ آخر القول بأن المناط في تحقق الإرهاب الإلكتروني يكمن في استخدام الإنترنت في تنفيذ هجمات إلكترونية ضد البنية التحتية للنظم المعلوماتية بالدولة [٤].

في حين ذهب رأي خامس إلى أن الإرهاب الإلكتروني هو العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد

---

(1) **Dorothy E. Denning**, Activism, Hacktivism and cyber terrorism, the internet as a tool for influencing, Foreign policy. In: Arquilla & D. Ronfold (eds.), Networks and net wars, the future of terror crime and miletences, National Defense Research Institute, 2001. pp. 239-288.

(٢) د/ حسين المحمدي بوادي، الرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦، ص ٥٤.

(٣) د/ مصطفي محمد موسي، الإرهاب الإلكتروني، بدون دار نشر، الطبعة الأولي ٢٠٠٩، ص ١٧٣.

(4) **Maura Conway**, Terrorism and new media: the cyber-battl espace. In: Forest, James F., (eds.), Countering terrorism and insurgency in the 21st century. Greenwood Publishing Group, Inc., Westport, CT, 2007. pp. 363-384.

على الإنسان في دينه أو نفسه أو عرضه، أو عقله، أو ماله، أو بشتي صور العدوان والإفساد، وذلك باستخدام الموارد المعلوماتية والوسائل الإلكترونية[١].

بينما ذهب رأي سادس إلى أن الإرهاب الإلكتروني هو الفعل الإجرامي الذي يرتكب بإستخدام الحواسيب وتكنولوجيا الاتصالات السلكية واللاسلكية ويؤدي إلى العنف من خلال التسبب في الارتباك بهدف التأثير على الحكومة أو المواطنيين لترويعهم؛ تحقيقًا لأهداف سياسية أو اجتماعية أو أيديولوجية[٢].

ولعل أفضل تعريف – من وجهة نظري– للإرهاب الإلكتروني هو الأفعال أو الأنشطة التي يقوم بها أفراد أو جماعات باستخدام تكنولوجيا المعلومات وشبكة الإنترنت، بقصد إحداث دمار للبنى التحتية المرتبطة والمدارة بواسطة هذه التكنولوجيا، كشبكات توزيع المياه والكهرباء، أنظمة الخدمات المصرفية، السجلات الصحية، الأنظمة العسكرية، وغيرها من البنى التحتية التي من شأن تدميرها أن يحدث أضرارًا مباشرة وغير مباشرة بالمواطنين والدول[٣].

---

(١) انظر: د/ عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الإنترنت والمنعقد بالقاهرة في الفترة ٢– ٤ يونيو ٢٠٠٨. متاح على الرابط التالى:
http://www.shaimaaatalla.com
انظر ايضا: د/ محمد عبدالله آل فايع العسيري ود/ حسن أحمد الشهري، الإرهاب الإلكتروني وبعض وسائله والطرق الحديثة لمكافحته، بحث مقدم إلى الندوة العلمية «استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين» والتي نظمتها جامعة نايف العربية للعلوم الأمنية بالرياض في الفترة ٩–١١ مايو ٢٠١١، مجموعة أعمال الندوة، ص ٢٢٥.

(2) **Peter J. Phillip**, The hunt for cyber terrorism, University of Southern Queenland, Faculty of business, 15 April 2013. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2253632

(٣) د/ رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، الدورة التدريبية حول توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب المنعقدة في الفترة من ٢٣–٢٧ فبراير

ويأتي هذا التعريف من منطلق قناعتي بأن الإرهاب الإلكتروني يقوم على استخدام الإرهابيين للتقنيات الرقمية في تنفيذ هجمات منتظمة ومدروسة بعناية فائقة ضد البنية التحتية لنظم المعلومات والشبكات مخلفًا آثار تخريبية مدمرة غايتها نشر الخوف والرعب وإخضاع الآخرين سواء كانوا دولًا أو أفرادًا، ومن ثم لا يضطلع به شخص بمفرده وإنما يقوم عليه في الغالب مجموعات من الأفراد ذوي الخبرات التقنية العالية على خلفية دوافع سياسية أو اجتماعية أو أيديولوجية، وغالبا ما يتضمن برامج يتم إنشاؤها خصيصًا لهذا الغرض[١]، الأمر الذي يستدعي أن يساير هذا التقدم التقني تقدم آخر قانوني يواكبه ويحافظ عليه ويكفل حمايته، ويضع حلولا لما يطرأ من مشكلات تترتب على سوء استخدام تكنولوجيا المعلومات[٢].

المطلب الثاني
الإرهاب الإلكتروني والمفاهيم الأخري

يعتبر الإرهاب الإلكتروني من أخطر أنواع الجرائم التي تقع في بيئة الإنترنت ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة، والقائمة على دوافع سياسية[٣]، أما إذا استخدم الإنترنت ليس لمهاجمة البيانات، أو البنية التحتية المعلوماتية، أو الأصول العسكرية المباشرة وإنما للاتصالات والتمويل وتجنيد

٢٠١٣، كلية التدريب قسم البرامج التدريبية بجامعة نايف للعلوم الأمنية، الرياض ٢٠١٣، ص ٨.

(1) **See. Devost M.G.,** National security in the information age, Unpublished Master thesis, University of Vermont, Burlington, May 2007.

(٢) انظر: د/ أيمن سيد العسقلاني، الإرهاب الإلكتروني في إطار القانون الدولي، بحث مقدم لمؤتمر القانون والتكنولوجيا المنعقد في الفترة ٩-١١ ديسمبر ٢٠١٧، مجموعة أعمال المؤتمر، الجزء الثاني ديسمبر ٢٠١٧، ص ١٩١٥.

(3) **Patrick Galley**, Terrorism Informatique: Quels sont Les Risques?. 1996. p. 14. disponible sur: http://strategique.free.fr/analyses/terrinfo.pdf

الإرهابيين والدعاية والتغطية الإعلامية والتلاعب بالرأي العام فيسمي استخدام الإنترنت لأغراض إرهابية[١]، أما إذا استعملت في تنفيذ أفعال القرصنة والسرقة والنصب والقذف والسب وسرقة المعلومات وانتهاك حقوق الملكية الفكرية والاحتيال المعلوماتي ... إلخ، فتسمي بالجرائم الإلكترونية. أما إذا استخدمت كوسيلة للتعبير عن المعتقدات السياسية أو الأيدلوجية ولم تنطو على عنف مادي فتسمي بالجهاد الإلكتروني[٢]، أما إذا استخدمت للضغط على الجهات الرسمية بالدولة لتحقيق مطالب معينة فتسمي بالاحتجاج الإلكتروني.

ولذلك كان ضروريًا أن نميز بين الإرهاب الإلكتروني والمفاهيم الأخرى، كاستخدام الإرهابيين للإنترنت أو استخدام الإنترنت في الأغراض الإرهابية، الجرائم الإلكترونية، الجهاد الإلكتروني، والاحتجاج الإلكتروني؛ لكي لا تختلط المفاهيم، وذلك أربعة أفرع على النحو الأتي:

الفرع الأول: الإرهاب الإلكتروني واستخدام الإرهابيين للإنترنت.

الفرع الثاني: الإرهاب الإلكتروني والجريمة الإلكترونية.

الفرع الثالث: الإرهاب الإلكتروني والجهاد الإلكتروني.

الفرع الرابع: الإرهاب الإلكتروني والاحتجاج الإلكتروني.

الفرع الأول
الإرهاب الإلكتروني واستخدام الإرهابيين للإنترنت

(1) **Irving Lachow**, Cyber Terrorism: Menace or Myth? In: Larry K. Wentz, Stuart H. Starr & Franklin D. Kramer (eds.), Cyberpower and National Security. National Security Center for Technology and National Security Policy, National Defense University and Potomac Books, Inc., 2009. p. 451.

(2) **Molly Sauter**, The Coming Swarm, DDoS Actions, Hacktivism, and Civil Disobedience on the Internet, Bloomsbury Academic, 2014. p. 27.

ثمة حاجة للتفرقة بين مفهوم الإرهاب الإلكتروني أو المصطلحات الرديفة كالإرهاب الافتراضي أو المعلوماتي أو الرقمي أو السيبراني وبين مفهوم استخدام الإرهابيين للإنترنت أو استخدام الإنترنت لأغراض إرهابية[١].

فالإرهاب الإلكتروني يشير إلى سير أوجه السلوك الإجرامي المقصود والمستند إلى دوافع سياسية ضد المعطيات بأنواعها ونظم وبرامج الكمبيوتر والاتصالات السلكية واللاسلكية تحقيقا لأغراض إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم وإثارة الفوضى وإشاعة الخوف وتعطيل الأداء الطبيعي لنظم السيطرة والرقابة الإلكترونية وتعطيل عمل الأجهزة والهيئات الحكومية والمرافق الاستراتيجية في الدولة[٢].

ويدور الارهاب الالكتروني في فلك محورين من الاعتداءات الموجهة ضد سلطات الدولة والحكومات. **أولهما**، الاعتداء على البيانات بإنواعها كسرقة البيانات أو تدميرها بما يؤدي إلى تخريب الخدمة وهو الشكل الأكثر شيوعًا للإرهاب الإلكتروني. **وثانيهما**، الهجمات على أنظمة التحكم الإلكتروني لتعطيل البنية التحتية الحيوية بالدولة أو التلاعب بها[٣]. على سبيل المثال استهداف شبكات إمداد الطاقة

---

(1) **Elizabeth Renieris**, "Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and the United Kingdom and the Need for an International Solution," Vanderbilt Journal of Entertainment and Technology Law, Vol. 11, Issue 3, 2009. pp. 687–688.

(٢) د/ محمد يونس عرب، الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، بحث مقدم إلى الندوة العلمية «استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين» والتي نظمتها جامعة نايف العربية للعلوم الأمنية بالرياض في الفترة ٩-١١ مايو ٢٠١١، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولي ٢٠١٢، ص ١٥٨.

(3) **Mitko BOGDANOSKI & Drage PETRESKI**, Cyber Terrorism–Global Security Threat. Contemporary Macedonian Defense - International Scientific Defense, Security and Peace Journal, 2013. p. 61. Available at: http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf.

عن بعد، والسكك الحديدية وإمدادات المياه، ويتم ذلك عن طريق إرسال البيانات عبر الإنترنت، أو عن طريق اختراق أنظمة الأمن(١).

ولكي يكون الاعتداء مؤشرا على الإرهاب الإلكتروني، يجب أن يؤدي إلى العنف ضد الأشخاص أو الممتلكات، أو على الأقل يسبب ضررا كافيا لتوليد الخوف لدي المواطنيين، على سبيل المثال الهجمات التي تؤدي إلى الوفاة أو الإصابة الجسدية، أو الانفجارات، أو حوادث الطيران، أو تلوث المياه، أو الخسائر الاقتصادية الشديدة. كما يمكن أن تكون الهجمات الخطيرة ضد البنى التحتية هي أعمال الإرهاب الإلكتروني، تبعا لتأثيرها. أما الهجمات التي لا ينتج عنها سوي تعطيل الخدمات غير الضرورية أو التي تشكل إزعاجا مكلفا للدولة فلا تدخل في نطاق الإرهاب الإلكتروني(٢).

ولذلك يشكل حماية البنية التحتية الحيوية جزءًا هامًا من الأمن السيبراني في الدول الغربية وكفالة تأمين البنية التحتية بالشكل السابق بيانه يعد واحد من أهم المسائل الوطنية المتعلقة باستيراتجيات الأمن السيبراني على الصعيد الوطني لهذه الدول. انظر:

Minister for the Cabinet Office and Paymaster General. The UK cyber security strategy: protecting and promoting the UK in a digital world. Cited 12 February 2012. Retrieved from: http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_Cyber_Security_Strategy.pdf; 2011.

(١) وقد استخدمت نقاط الضعف في نظام الأمن الإلكتروني لمشروع معالجة مياه الصرف الصحي بإستراليا حيث قام Vitek Boden المستشار في ذلك المشروع في مارس عام ٢٠٠٠ على خلفية رفض عمله بدوام كامل full-tim باستخدام الإنترنت وراديو لاسلكى وبرنامج مراقبة لاطلاق ما يصل إلى مليون لتر من مياه الصرف الصحي غير المعالج في نهر Maroochydore، وقد حكم عليه في نوفمبر ٢٠٠١ بالسجن لمدة عامين.

Robert Lemos, Cyberterrorism: The real risk, 2002. Available at: http://www.crime-research.org/library/Robert1.htm

(2) **Dorothy E. Denning**, "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Washington, D.C., 23 May 2000, p. 1. Available at: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf.

فالإرهاب الإلكتروني يكمن في استخدام الإنترنت بهدف تدمير المجتمع أو إصابة أنظمة الكمبيوتر ونظم المعلومات لأغراض سياسية. ومن المحتمل أن يستهدف الإرهاب الإلكتروني نظام إدارة زوار الموقع الجوي في البلاد، أو البنية التحتية للاتصالات السلكية واللاسلكية؛ لذا يتطلب في القائمين عليه أن يكونوا متمتعين بخبرات تقنية عالية في هذا المجال، أضف إلي الوفرة في الأعداد التي يتطلبها تنفيذ الإرهاب الإلكتروني والتي قد تصل إلي الآلف وعدد من سنوات التخطيط لتنفيذ ذلك[١].

أما استخدام الإرهابيين للإنترنت أو استخدام الإنترنت لإغراض إرهابية فهو مفهوم أوسع من ذلك بكثير[٢]، فهو يشير الى طائفة معتبرة من أنشطة الإرهاب المتقدم خاصة عندما يستخدم الإنترنت كوسيلة لارتكاب الجرائم الإرهابية، ولكنه يشمل بشكل رئيسي وضمن مفهوم منضبط ونطاق محدد سائر الأنشطة التي يستخدم فيها الانترنت كبيئة للجريمة الإرهابية[٣] والتي لا يستغرق تنفيذها وقت يذكر، ولا تحتاج لهذا الكم من الأشخاص ذوي الخبرات التقنية العالية، مثل نشر الأفكار الضالة والتدميرية، التواصل مع الممولين والمساندين والمؤيدين للجماعات الإرهابية، التجنيد، والتخطيط، والتنسيق وتبادل الخبرات في مجال العمليات الإرهابية[٤]، إضافة إلي نشر المواد المتعلقة بصناعة الأسلحة والمتفجرات والألغام

---

[١] د/ هشام بشير، ندوة نظمها المركز الدولي للدراسات المستقبلية والاستيراتيجية في ١١ ابريل ٢٠١٢ تحت عنوان مستقبل الإرهاب الإلكتروني، متاح على الموقع الإلكتروني لمجلة السياسية الدولية، على الرابط التالى:

http://www.siyassa.org.eg/Newscontent/6/51/2450

[2] **See. E. Noor,** "The Problem with Cyber Terrorism," Proceeding of Southeast Asia Regional Center for Counter Terrorism's (SEARCCT) Selection of Articles, Ministry of Foreign Affairs Malaysia, Vol 2/2, 2011. pp. 51-64.

[٣] د/ محمد يونس عرب، المرجع السابق، ص ١٥٨.

[٤] د/ حسن أحمد الشهري، الإرهاب الإلكتروني- حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد ٤ العدد ٨، يناير ٢٠١٥، ص ١.

وطرق إعداد العمليات الانتحارية وتنفيذها، وتوفير الدعم أثناء اعداد هذه العمليات وخلال مراحل تنفيذها[١]، والترويج لها والدفاع عن مرتكبيها وتصويرهم كما لو كانوا مناضلين أو متشددين ...إلخ، وليسوا إرهابيين وقتلة.

الفرع الثاني
الإرهاب الإلكتروني والجريمة الإلكترونية

يتداخل الإرهاب الإلكتروني بشكل كبير مع الجريمة الإلكترونية بحيث يصعب التمييز بينهما[٢]؛ حيث استخدم المصطلحان بالتبادل أو كمترادفين بعض الأحيان، وفي كثير منها استخدما بشكل مغاير للآخر[٣]، وهو ما يثير الارتباك لدي

---

(1) **Matteo Cavallini**, Terrorist use of the Internet: an analysis of the current threat and its potential evolution, Technical Report, Information Security Group Royal Holloway, University of London Egham, Surrey TW20 0EX, United Kingdom, September 2014. p. 9. Available at: https://www.ma.rhul.ac.uk/static/techrep/2014/RHUL-MA-2014-11.pdf

(٢) وفي هذا الصدد يعترف Brett Pladna أحد خبراء أمن المعلومات بصعوبة التمييز بين الإرهاب الإلكتروني والجريمة الإلكترونية قائلا : أنه في كثير من الأحيان ليست مهمة سهلة التمييز بين الهجمات على شبكة الكمبيوتر التي يقوم بها الإرهابيون والجرائم الإلكترونية التي قام بها المتسللين؛ لأن المهاجم، أيا كان، يحاول دائما استغلال نقاط الضعف في النظام بغض النظر عن جوهر الدوافع الحقيقية. ومع ذلك، هناك بعض الاتجاهات التي يمكن أن تساعد في إحداث فرق واضح بين كلا الفعلين. فعلى سبيل المثال، تركزت أعمال الإرهابيين في معظم حالات الهجمات الإرهابية على شبكات الحاسوب على تشويه مواقع الويب وتفجير البريد الإلكتروني. انظر:

Brett Pladna, Cyber terrorism and information security, East Carolina University, 2008, p.5. available at: http://www.infosecwriters.com/text_resources/pdf/BPladna_Cyber_Terrorism.pdf

(3) **INFOSEC INSTITUTE**, Cyberterrorism Defined (as distinct from "Cybercrime"), posted in General Security on 21 December 2012. Available at: http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/#gref

غير الملمين بتفاصيل هذه المسألة[١]؛ لذا يعد التمييز الصحيح بين المصطحات هو جُلّ اهتمام هذه الدراسة خاصة مع تردد مصطلحات أخري مماثلة تغذي هذا الارتباك وتزيده كالحرب الإلكترونية Cyberwar[٢].

ولعل الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية بين الدول هو الذي أدي إلي عدم الاتفاق على مصطلح موحد للدلالة عليها[٣]، والذي أسهم بدوره في عدم وضع تعريف موحد لهذه الظاهرة[٤]؛ خشية حصرها في مجال ضيق[١].

---

(1) War on Terrorism, Testimony Before the Select Committee on Intelligence of the United States Senate (2003) (testimony of Robert S. Mueller, III, Director, FBI). available at: https://archives.fbi.gov/archives/news/testimony/war-on-terrorism

(٢) يقصد بمصطلح الحرب الإلكترونية: « الأعمال تقوم بها الدولة والتي تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها».

Richard A. Clarke & Robert knake, Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins Publishers, 2010. p.6.

(٣) ومن هذه المصطلحات نذكر: جرائم الكمبيوتر والإنترنت، جرائم التكنولوجيا الحديثة، جرائم إساءة استخدام الحاسب، جرائم الفضاء الكوني، جرائم المعالجة الآلية للبيانات، جرائم تقنية المعلومات، الجرائم المرتبطة بشبكة المعلومات، جرائم التقنية العالية، الجرائم المعلوماتية ....الخ. وللمزيد من التفاصيل حول هذه المصطلحات، راجع:

«Computer crime» from Wikipedia, the free encyclopedia. Available at: http://en.wikipeida-org/wiki/Computer-crime

(٤) ويمكن تصنيف التعريفات المختلفة للجريمة الإلكترونية إلى أربع طوائف: **أولها**، تعتمد على وسيلة ارتكاب الجريمة، وبالتالى عرفتها بأنها كل أنواع السلوك غير المشروع الذي يرتكب عن طريق الحاسب الآلي أو بمساعدته أو أن يكون أداة رئيسية في ارتكابه. **وثانيها**، تدور حول موضوع أو محل الجريمة، وبالتالى عرفتها بأنه كل سلوك غير مشروع موجه إلى المعالجة الآلية للبيانات أو نقلها. **وثالثها**، حاولت الجمع بين وسيلة ارتكاب الجريمة وموضوعها، وبالتالى عرفتها بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية او المعنوية يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية. **ورابعها**، ركز على

وتعرف الجريمة الإلكترونية لدي جانب كبير من الفقه المصري بأنها: « كل فعل أو امتناع يؤديه شخص طبيعي أو معنوي عن طريق ممثليه، باستعمال نظام إلكتروني معين يتمثل في الحاسبات أو ما يقوم مقامها من نظم مطورة، وشبكات الاتصال، إضرارا بمصلحة أو حق يحميه القانون من خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحمية تمثل نماذج معلوماتية مستحدثة، أو كانت تدخل في نطاق المصالح أو الحقوق التي يحميها مسبقًا قانون العقوبات بالطرق التقليدية وسواء كان الاعتداء واقعا داخل حدود الدولة أو كان يمس أقاليم عدة دول»[٢].

وباستعراض تعريف الجريمة الإلكترونية والإرهاب الإلكتروني نجد أنهما يتشابهان في جوانب ثلاثة: أولها، أن كل منها جرائم. **وثانيها،** أن محل ارتكاب الجريمة في كلاهما واحد وهو البيئة الإلكترونية؛ لذا يغلب عليهما الطابع الدولي بخلاف الجريمة التقليدية[٣]. **ثالثها،** أن كليهما قد يوجه ضد فرد أو منظمة أو

شخص الجاني وما يتمتع به من دراسة لتقنية نظم المعلومات، وبالتالى عرفها بأنها أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لدي مرتكبه. لمزيد من التفاصيل حول التعريفات المختلفة للجريمة الإلكترونية، **راجع:**

د/ حاتم عبد الرحمن منصور، الإجرام المعلوماتي، دار النهضة العربية، الطبعة الأولي ٢٠٠٣، ص ٢١ وما بعدها؛ د/ محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، الطبعة الأولي ٢٠١٦، ص ٦٠ وما بعدها.

(١) د/ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية ٢٠٠٤، ص ٤٣.

(٢) د/ هلالي عبد اللاه أحمد، المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني في ضوء إتفاقية بودابست، دار النهضة العربية، الطبعة الثانية ٢٠١٣، ص ١١٣؛ د/ عمر أبو الفتوح الحمّامي، الحماية الجنائية للمعلومات المسجلة إلكترونيًا، دار النهضة العربية، ٢٠١٠، ص ٥٩.

(3) **Enver BUÇAJ**, The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law, JURIDICA, Acta Universitatis Danubius. Juridica, vol. 13, no. 1/2017, p. 148. Available at: *http://journals.univ-danubius.ro/index.php/juridica/article/download/3882/3949*

دولة[١]. بالمقابل تنضوي جرائم الإرهاب الإلكتروني بوجه عام في خانة الجرائم الإلكترونية التي تستهدف المعطيات والنظم كهدف أو محل للجريمة أو تستخدم نظم الكمبيوتر والشبكات كوسيلة لارتكاب الجرائم التقليدية ضد الاشخاص أو الأموال[٢]. لذا قيل – وبحق – أن جميع الأعمال الإرهابية هي جرائم إلكترونية ولكن ليست جميع الجرائم الإلكترونية تدخل ضمن الأعمال الإرهابية[٣].

وتختلف الجريمة الإلكترونية عن الإرهاب الإلكتروني في الدافع[٤]، ففي الأولي يكون الدافع إلى حد كبير تحقيق الكسب المادي. أما الثانية فالدافع فيها يكون سياسي أو اجتماعي أو أيدلوجي بهدف زعزعة استقرار الدول وتدمير البنية التحتية المستهدفة [٥]، ولتوضيح ذلك نسوق المثال التالى: أنه قد يتطابق الإجراء الذي يتخذه كل من الإرهابي الإلكتروني والمجرم الإلكتروني لاختراق حساب ما بهدف سرقة المعلومات. لكن الاختلاف يكمن في السبب في فعل الاختراق، فعادة إذا ما كانت وراءه جماعة إرهابية فإنها لا تكتفي بأن تبلغ عبر شخص مجهول بأن هجوم سوف يحدث وإنما تعتمد على أن يعلم الجميع عقب التنفيذ أنهم قد نفذوا الهجوم. أما في الجريمة الإلكترونية فالجاني لا يريد أحد أن يعرف أنه فعل ذلك؛ لذا

---

(١) د/ حسن أحمد الشهري، الإرهاب الإلكتروني...، المقالة السابقة، ص ٧.

(٢) د/ يونس محمد عرب، المقالة السابقة، ص ١٥٨.

(3) **Ashish Pandey**, Cyber Crime Prevention and Detection, 1st Ed, 2006. p. 93.

(4) **Namosha Veerasamy**, Motivation for Cyberterrorism, Defence, Peace, Safety and Security (9 th Annual Security of South Africa (ISSA), Johannesburg, 2-4 August 2010). http//icsa.cs.up.ac.za/issa/2010/Proceedings/Research/02_paper.pdf. [accessed 1 August 2015].

(5) **Nazli Zeynep BOZDEMİR,** "Re-Conceptualizing Cyberterrorism: Towards a New Definitional Framework", Master of Arts, Hacettepe University Graduate School Of Social Sciences Department of International Relations International Relations MA, Ankara, 2016. pp. 54-55; **Clay Wilson**, Cyber Threats to Critical Information Infrastructure. In: Thomas M. Chen, Lee Jarvis & Stuart Macdonald (eds.), Cyberterrorism: Understanding, Assessment and Response. Springer, New York, 2014. p. 132.

يحرص على ألا يُكتشف ارتكابه لفعل الاختراق، وعليه يعد الدافع هو المفتاح للتمييز بين الإرهاب الإلكتروني والجريمة الإلكترونية[١].

كذلك يختلفان في النتيجة، فالإرهاب الإلكتروني ينطوي على نتائج جد خطيرة، فقد تؤدي إلى الوفاة أو الإضرار المادي بالأشخاص، أو الممتلكات، أو تترك أثارً مدمرة تُشيع قدر كبير من الرهبة في نفوس المجتمع، وهو في ذلك يشابه الطابع المادي للإرهاب وإن كان ذلك ليس غالبا[٢]. بخلاف الجريمة الإلكترونية التي لا يُخلَف ارتكابها مثل هذه النتائج؛ لأنها جرائم يغلب عليها الاعتداء على الجانب المالى أو المعنوي للأشخاص كسرقة الهوية أو الاحتيال المعلوماتي والمواد الإباحية المتعلقة بالأطفال والتشهير والسب والقذف والاعتداء على حقوق الملكية الفكرية ... إلخ، والتي هي جرائم في حد ذاتها لكنها تكتسي بهذا الوصف – أي الجرائم الإلكترونية– نظرًا لارتكابها من خلال شبكات الاتصالات السلكية واللاسلكية، فهي مجرد وصف لسلوك غير مشروع يتم في الفضاء الإلكتروني[٣].

الفرع الثالث

الإرهاب الإلكتروني والجهاد الإلكتروني

الجهاد الإلكتروني Hacktivism هو مزيج من الخبرة في الاختراق وممارسة بعض النشاطات السياسية والدينية وتوظيف الاختراق بالأساس للدفاع عن قضية[٤]،

---

(1) **A. M Sharp Parker**, "Cyberterrorism: The Emerging Worldwide Threat", in The Faces of Terrorism: Multidisciplinary Perspectives (ed D. Canter). 1st ed. Oxford, UK: Wiley- Blackwell Press, 2009. p. 250.

(2) **Ashish Pandey**, Op.cit., p. 94.

(3) **Idem**.

(٤) وقد ظهر هذا المصطلح في سنة ١٩٩٤ من قبل أحد أعضاء إحدى منظمات القرصنة يعرف باسم "أوميجا" من أمثلته ما حصل خلال احتجاجات الانتخابات الإيرانية ٢٠٠٩–٢٠١٠ حيث لعبت مجموعة أنونيموس دورا في نشر المعلومات من وإلى إيران عن طريق إنشاء موقع "أنونيموس إيران"، وقاموا أيضا بإصدار مقاطع فيديو مانيفستو للحكومة الإيرانية. كما يشتبه بمشاركتهم في هجوم داين الإلكتروني Dyn cyberattack الذي حدث في ٢١ أكتوبر

وقد كبر هذا النوع من القرصنة وسطع من كونه مجرد اختراقات أو هجمات إلكترونية عشوائية إلى دفاع عن قضية[١]. وفي جوهره هي الطريقة التي يستخدم بها القراصنة التكنولوجيا كوسيلة للتعبير عن معتقداتهم السياسية وأيديولوجياتهم، وغالبا ما أرتبطت أهداف الجهاد الإلكتروني بحرية التعبير، أو حقوق الإنسان، أو حرية المعلومات. لذا يطلق عليه البعض وصف القرصنة لقضية سياسية[٢].

ويعرف مصطلح Hacktivism تقنيًا بأنه: هجمات قرصنة منظمة ومدروسة من قبل خبراء الاختراق والقرصنة ضد جهة معينة قد تكون دولة، أو عدة دول، أو جهات أخرى مثل الشركات أو المنظمات، للدفاع عن قضية معينة[٣].

٢٠١٦ والمتمثل في عدة هجمات لحجب والحرمان من الخدمة، واستهدفت نظام أسماء النطاقات (DNS) الخاص بالشبكات التي تديرها شركة داين، مما جعل العديد من المواقع والخدمات الموجودة على الإنترنت غير متاحة لعدد كبير من سكان أوروبا وأمريكا الشمالية. راجع:

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

[١] وقد كان الغرض في بداية الأمر من تنفيذ هجمات القرصنة هو لفت الأنظار ووسائل الإعلام للقضية المراد الدفاع عنها وتسليط الضوء نحوها ولكن مع تطور أساليب القرصنة وبدء القراصنة في تكوين تنظيمات سرية اصبح الامر اكثر خطورة وأكثر تنظيمًا من مجرد لفت انتباه، إذ يمكن لهجمة قرصنة إنهاء دولة بالكامل في الوقت الحالى.

[2] The Difference Between Hacktivism and Cyber Terrorism, Info Barrel Technology, Dec 18, 2009. Available at:
http://www.infobarrel.com/The_Difference_Between_Hacktivism_and_Cyberterrorism

إذ ينظر البعض إليه على أنه نوع من أنواع حرية التعبير وإبداء الرأي المفتوح. ولكن الأمر أكثر من ذلك فقد يتسبب الجهاد الالكتروني بخسائر مالية فادحة بسبب مهاجمة مواقع البورصة والمواقع الحكومية وأنظمة البنية التحتية للبلد وتجميد كل شيء تقريبا. راجع:

علي الوشلي، ما هو النضال الإلكتروني(Hacktivism) ونشاته ؟ منشور بتاريخ ٢٣ يونيو ٢٠١٤ على الربط التالى:

https://www.isecur1ty.org

[٣] الإشارة السابقة.

ويطلق على الأشخاص الذين يقومون بأعمال الجهاد الإلكتروني Hacktivists القراصنة ذوي الدوافع السياسية [١].

وتشمل الأشكال النموذجية للهجوم من قبل هؤلاء القراصنة Hacktivists الاعتصامات الإلكترونية، الحصار، والقصف الآلي بالبريد الإلكتروني، والفيروسات والديدان، والتشهير[٢]، تغيير المظهر المرئي للمواقع وتشويهها، وإعادة توجيهها أو خداعها، ترك البيانات السياسية، الحرمان من الخدمة، وفي بعض الأحيان اقتحام نظم الكمبيوتر، وسرقة المعلومات[٣].

ويتشابه الجهاد الإلكتروني مع الإرهاب الإلكتروني من زاويتين : أولها، أن كليهما يستخدم نفس التقنيات والأدوات في تحقيق أهدافه[٤]. وثانيها، أن الدافع وراء ارتكابهما سياسي.

وبالرغم من أن الجهاد الإلكتروني له دوافع سياسية إلا أنه لا يرقي إلى مرتبة الإرهاب؛ لأن القراصنة ذوي الدوافع السياسية لا يريدون من جراء أفعالهم القتل، أو أصابة الأشخاص، أو بث الرعب في النفوس، وإنما مجرد توجيه الانتباه لقضية سياسية، أو اجتماعية بالطرق السلمية من خلال الاعتراض وتعطيل الخدمات

(1) **Margaret Rouse**, Definition Hactivism. Available at: http://searchsecurity.techtarget.com/definition/hacktivism

(2) **Alexandra Whitney Samuel**, Hacktivism and the Future of Political Participation, A thesis Doctor of Philosophy in the subject of Political Science Harvard University Cambridge, Massachusetts September 2004. p. 7.

(3) Threat Assessment: The cyber threat against Denmark, **by. Centre for Cyber Security (F.E)**, January 2016. Available at: https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf

(4) **Dorothy Denning,** Hacktivism is the marriage of hacking and activism. In Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija (eds.), Hacktivism, Cyber Terrorism and Cyberwar the Activities of the uncivil, 2003, p. 24.

الإلكترونية[١]. بخلاف الإرهابين الإلكترونين الذين يستولون على انتباه الجمهور بالطرق العدوانية وتحديدًا غرس الخوف في قلوب عامة الناس[٢].

لكن في بعض الأحيان يتعذر التمييز وتصعب التفرقة بين الإرهاب الإلكتروني والجهاد الإلكتروني خاصة إذا كانت الجماعات الإرهابية لديها القدرة على تجنيد، أو توظيف القراصنة ذوي الدوافع السياسية، أو إذا قرر هؤلاء تصعيد أفعالهم من خلال مهاجمة الأنظمة الإلكترونية المدار من خلالها البنية التحتية الوطنية كالهجوم على شبكات الطاقة والمياه أو خدمات الطوارئ[٣].

الفرع الرابع
الإرهاب الإلكتروني والاحتجاج الإلكتروني

يعد الاحتجاج شكلا من أشكال الضغط غير العنيف على المؤسسات الحكومية أو الرسمية؛ وذلك لتحقيق مطالب معينة. ويأتي هذا الضغط في شكل

---

(١) إذ شنت مجموعة "أنونيموس" هجوما في إبريل ٢٠١٣ على مواقع إسرائيلية دعما للأسرى والقضية الفلسطينية، وشملت القائمة مواقع البورصة الإسرائيلية، ورئيس الوزراء، ووزارة الدفاع، وموقع جهاز الأمن الداخلي (الشاباك)، والصناعات العسكرية الإسرائيلية، إضافة إلى موقع مكتب الإحصاء الرسمي، وموقع وزارة التربية والتعليم، وعشرات المواقع الأخرى وآلاف الحسابات الإسرائيلية على موقعي فيسبوك وتويتر. متاح على الرابط التالى:
https://www.elwatannews.com/news/details/2095075
كما شن قراصنة تابعين لمجموعة "أنونيموس" هجوم الحرمان من الخدمة DDos في ٢٧ نوفمبر ٢٠١٥ ضد مواقع الحكومة الإيسلندية مثل وزارة الداخلية ووزارة الشئون الخارجية ومكتب رئيس الوزراء كجزء من حملة مكافحة صيد الحيتان، مما أدى إلى توقف هذه المواقع لمدة ١٣ ساعة كاملة عن تقديم خدماتها للمواطنيين .
http://icelandmonitor.mbl.is/news/politics_and_society/2015/11/30/iceland_hit_by_whalin//g_cyber_attack

(2) **Gabriel Weimann**, Cyberterrorism. How Real Is the Threat, United States Institute of Peace, Washington, May 2004. p. 4. Available at: https://www.usip.org/sites/default/files/sr119.pdf

(3) **Ibid.** p. 5.

إضراب عن العمل أو وقفات احتجاجية أو أي مظاهر احتجاج يتم الاتفاق عليها. وقد حدث تزاوج ما بين الاحتجاج باعتباره أداة للتعبير عن الرأي وشبكة الإنترنت بوصفها وسيلة وأداة لاستخدام الفضاء الإلكتروني في التنظيم والحشد والتعبئة والتجنيد والتنسيق وشن حملات دعائية. ويأتي هذا في صورة تقديم المساعدة في الشكل التنظيمي والدعائي للاحتجاج التقليدي، أو في وجود احتجاج يأخذ طابعًا إلكترونيًا بحتًا أو وجود احتجاج يجمع كلا النمطين[١].

وتتمثل أهم أشكال الاحتجاج الإلكتروني في جمع التوقيعات الإلكترونية للمطالبة بتغيير سياسات أو قرارات أو إزالة صور تعد مسيئة أخلاقيًا أو دينيًا. ولعل أشهر المواقع في هذا الصدد هو موقع Petition Online بوصفه المنصة الرئيسيةٌ لإطلاق صواريخ الاحتجاجات وحملات جمع التوقيعات ضد أي شيء وكل شيء . إذ وفر الموقع وسيلة للتعبير عن الرأي في بيئة إلكترونية جعلت من السهولة بمكان الحصول على ملايين الأصوات؛ نظرًا لسهولة التواصل عبر الإنترنت .. والدخول إلى غرف الدردشة والمنتديات للقيام بحوارات وتكوين رأي مناصر أو مناهض لقضية من القضايا .. وتكوين التحالفات السياسية في الإنترنت[٢].

---

[١] د/ عادل عبد الصادق، الإرهاب الإكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، الطبعة الثانية، ٢٠١٣، ص ١٣٤.

[٢] ويتم نشر أفكار الإضرابات أو الاعتصام بين أكبر عدد من مستخدمي الإنترنت عن طريق: المجموعات البريدية، رسائل المحمول مهاجمة المواقع الحكومية الإلكترونية أو مواقع الخصوم، القرصنة، سرقة المعلومات، نشر الفيروسات .. الخ، وارسال كم كبير من الرسائل الاحتجاجية لجميع الأطراف المعنية بصورة ضاغطة ومزعجة عن طريق البريد الإلكتروني، إنشاء مواقع إنترنت لنشر الأفكار والرؤي الخاصة بالموقف الاحتجاجي للحصول على تأيد الرأي العام وتجنيد الموالين والداعمين لفكرة الاحتجاج من جماعات المصالح المختلفة.

ويختلف الاحتجاج الالكتروني عن الإرهاب في كونه مجرد أداة سياسية للضغط لتنفيذ مطالب معينة في شكل نوع من العصيان المدني، ويكمن خلف اللجوء إليه عدد من الأبعاد أهمها:

البعد الموسسئ، ويتمثل في ضعف دور الأحزاب السياسية والمجتمع المدني وممثلي السلطة التشريعية باعتبارها جميعًا مؤسسات وسيطة بين الحاكم والمحكومين، وعدم التوافق بين التغييرات في الرأي العام وعملية وضع السياسات.

البعد التكنولوجي، يتعلق بالارتباط المتزايد بتكنولوجيا الاتصال والمعلومات وتوفير فرص أما لاعبين جدد، وخاصة مع وجود وسيلة سهلة ورخيصة وسريعة الانتشار واندماج الخدمات مع بعضها؛ حيث يتيح الإنترنت خدمة الاتصال، والموبايل يتيح خدمة الإنترنت، وامكانية التراسل المجاني بينهما، فضلا عن الحرية المتاحة وارتفاع سقفها عن وسائل الإعلام التقليدية.

البعد التنموي، حيث إن المجتمعات التي تكون في طور التحول يكون لديها حالة متصاعدة من الحراك السياسي بين المهتمين بالشأن العام، بالإضافة إلى أن الانفتاح على الخارج يجعل لديه طموحات وتطلعات أكبر قد تمثل ضغطًا على صانعي القرار، وقد لا تتوافق مع الواقع الاجتماعي والاقتصادي[١].

وفي النهاية ولكي لا تختلط المفاهيم يجب ألا ندخل في نطاق الإرهاب الإلكتروني ما ليس ذلك، إذ يجب النظر إلى الإرهاب الإلكتروني نظرة منفصلة وبعيدة كل البعد عن استخدام الإرهابيين لشبكة الإنترنت والتي تشمل عدة جوانب مثل الاتصالات، التجنيد، التمويل، الدعاية، المواد التعليمية الخاصة بالاعمال الإرهابية، والتحريض على الإرهاب... إلخ. وبين الجرائم الإلكترونية والتي تعتبر

---

[١] د/ عادل عبد الصادق، الاحتجاج الإلكتروني والفاعلون الجدد في الحياة السياسية، ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١٦٢، يونيه ٢٠٠٨.

شبكة الإنترنت والفضاء الإلكتروني أداتها وساحتها وهدفها ويدخل تحت هذه **الخانة** طيف واسع من الجرائم الإلكترونية كالقرصنة[١]، التجسس، النصب، سرقة المعلومات، ... إلى آخر هذه الأفعال الإجرامية[٢].

وتسهيلًا لهذه التفرقة وضع الفقهاء حدودًا فاصلة بين المصطلحات المختلفة حتي لا تتداخل فيما بينها، ومن ثم تستقيم المفاهيم. إذ قسموا المتخصصين والخبراء في أمن المعلومات الناشطين عبر الانترنت على أربع مجموعات، مع إقامة الفارق بينهم[٣]: **أولهما**، الناشطون Activists وهم الذين يستخدمون الإنترنت فقط للترويج لقضية سياسية معينة أو يدافعون عن أيديولوجية معينة من خلال ممارسة الضغط المباشر على صانع القرار[٤]. **وثانيهما**، القراصنة لأغراض سياسية Hactivists وهم الذين يهاجمون مواقع الإنترنت تعزيزًا لأجندة سياسية أو دفاعًا عن أيديولوجية معينة من خلال تخريب مواقع الإنترنت أو شبكات الكمبيوتر .... إلخ لغرض نقل رسالة سياسية[٥]. **وثالثهما**، القراصنة Hakers وهم الذين يهاجمون مواقع الانترنت

---

(١) ويشير مصطلح القرصنة إلى الهجمات الإلكترونية المنتظمة والمدروسة القائم عليها خبراء الاختراق والقرصنة ضد جهة معينة قد تكون دول أو جهات أخري مثل الشركات أو المنظمات المعنية بالدفاع عن قضايا معينة أو لفت انظار وسائل الاعلام لقضية معينة.

(2) **See. Varvara Mitliaga**, Cyber terrorism, A call for governmental action British and trish law education & technology association, 2001; Anna – Maria, Cyber Terrorism in Theory or in Practice, Defense Against Terrorism Review, Vol. 2. Fall 2010.

عكس ذلك، انظر:

Victoria Baranetsky, what is Cyber Terrorism? Even Experts can't Agree, Harvard Law Record, Vol. 129, No. 4, 5 November 2009. Available at: http://hlrecord.org/2009/11/what-is-cyberterrorism-even-experts-cant-agree/

(3) **See**. **John Arquilla & David Ronfeldt,** The Advent of Netwar (Revisited), In: Arquilla & D. Ronfold (eds.), Networks and net wars, the future of terror crime and miletences, National Defense Research Institute, 2001. pp.19-20.

انظر ايضا: د/ رائد العدوان، المرجع السابق، ص ٨.

(4) **Dorothy E. Denning**, Activism, Hacktivism and cyber terrorism, Op. cit, p. 240.

(5) The cyber threat against Denmark, Threat Assessment Branche under Centre of Cyber Security, January 20 16, p. 7. Available at:

لتعطيلها دون نية أو القدرة على إحداث دمار كبير فيها ويدخل أفعالهم ضمن طائفة الجرائم الإلكترونية.

وتتمثل المجموعة الأخيرة في الإرهابيين Cyber-terrorist وهم أشخاص يحركهم دافع سياسي، يهاجمون المواقع الإلكترونية والبنية التحتية لنظم المعلومات بالدولة المرتبطة بالانترنت بغية إحداث دمار كبير بشري أو مادي ويدخل أفعالهم ضمن طائفة الإرهاب الإلكتروني. ويدخل ضمن أنشطتهم الوصول إلى الإشارات التي تتحكم في التكنولوجيا العسكرية وتعطيلها أو تعديلها، استهداف أنظمة البنية التحتية الحيوية للدولة. على سبيل المثال، تعطيل خط أنابيب الغاز، أو مصفاة تكرير النفط أو حتي مواقع الطاقة النووية بما يؤدي إلى انقطاع التيار الكهربائي في منطقة ما أو تعطيل محطة معالجة المياه، وهذا النوع من الهجمات الإلكترونية يمكن أن يعطل المدن الكبرى، ويسبب أزمة صحية عامة، ويعرض السلامة العامة لملايين الناس للخطر، ويسبب الذعر والوفاة[١].

كذلك يدخل في عداد الإرهاب الإلكتروني الاعتداءات الموجهة ضد الأجهزة وشبكات الكمبيوتر العامة والشبكات الحكومية أو الشبكات الخاصة بالقطاعات الاقتصادية وأسواق رأس المال والمؤسسات المالية واستهداف مواقع الاتصالات[٢]، كما يدخل ضمن هذه الأنشطة الأفعال الأتية: التسلل إلى نُظم التحكُّم الوطني في الطيران لإحداث تصادم بين الطائرات، اختراق نُظم التحكُّم الوطني في قطارات السككِ الحديديَّة لإحداث تصادم بين القطارات، تعديلُ ضغط الغاز عن بُعد في أنابيب الغاز لتفجيرها، تعديل نُظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، الدخولُ عن بُعد لنظامِ التحكُّم في علاج المرضى في المستشفيات بهدفِ

---

https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf

(1) **Margaret Rouse**, cyberterrorism: Publish in December 2017. Available at: http://searchsecurity.techtarget.com/definition/cyberterrorism

(٢) د/ حسن أحمد الشهري، الإرهاب الإلكتروني...، المقالة السابقة، ص ٧.

قتل المرضي، والدخولُ عن بُعد لنظامِ التحكُّم في مصانع غذاء الأطفال لتغيير مُستويات نسب المواد الغذائيَّة بهدف قتل الأطفال، وتحقيق أكبر قدر من الضحايا(١).

وتشمل هذه الأنشطة أيضا التهديد والترويع الإلكتروني(٢) والأفعال العمدية التي من شأنها تعطيل واسع النطاق لشبكات الكمبيوتر وخاصة أجهزة الكمبيوتر الشخصية المتصلة بالإنترنت، عن طريق أدوات مثل الفيروسات، حصان طروادة، والديدان أو تشويه مواقع الويب، أو تعطيل المواقع الرئيسية، أو وقف حركة المرور إلى المواقع المختلفة ... إلخ(٣). والتجسس الإلكتروني Cyber Espionage على المؤسسات الرسمية أو الدول أو المنظمات لأغراض سياسية أو عسكرية (٤).

ونلفت الانتباه إلى أن التجسس الإلكتروني على قادة الدول المتنافسة من أجل التعرف على مواقع القوات أو اكتساب ميزة تكتيكية خلال الحرب والذي يقوم به

---

(1) **Dorothy E. Denning**, Activism, Hacktivism and cyber terrorism, Op. cit., p. 282.

انظر أيضا: د/ هشام بشير، ندوة نظمها المركز الدولي للدراسات المستقبلية والاستيراتيجية في ١١ ابريل ٢٠١٢ تحت عنوان مستقبل الإرهاب الإلكتروني، متاح علي الموقع الإلكتروني لمجلة السياسية الدولية، علي الرابط التالى:
http://www.siyassa.org.eg/Newscontent/6/51/2450

(٢) كتهديد الشخصيات السياسية أو الدينية أو العامة بالقتل أو التهديد بتفجيرات في الأماكن والمتنزهات العامة والمراكز السياسية والرياضية أو إتلاف أنظمة المعلومات.

(3) **Jonathan Matusitz,** Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age? American Foreign Policy Interests, Vol. 27, Issue. 2, 2005, pp. 137-147; **Soumen Ganguly**, Impact of Cyberterrorism in digital world, International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 1, No. 1, October 2011, pp 35-36.

(4) **Clay Wilson**, Cyber Crim. In: Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz (eds.), Within the Cyberpower and National Security, National Defense University Press, WASHINGTON, D.C. 1st ed. 2009. p. 422.

القراصنة لحساب الحكومات لا يعتبر بالضرورة إرهابا إلكترونيًا ما لم يتم بقصد تنفيذ هجوم إرهابي إلكتروني[١].

المبحث الثاني
أسباب ظهور الإرهاب الإلكتروني

بسبب طبيعة شبكة الإنترنت وانفتاحها غير المحكوم أخلاقيًا وسياسيًا وثقافيًا وقانونيًا وتجاريًا وعدم ارتباطها بدولة معينة أو حدود جغرافية أو سياسية وبسبب صعوبة الرقابة أو المحاسبة على ما ينشر فيها؛ لكل هذه الأسباب أصبح الفضاء الإلكتروني الساحة التي تنفذ من خلالها أو داخلها أعمال متصلة بالإرهاب، والمحل المختار لهذا النوع الجديد من الإرهاب.

ونظرًا لافتقار شبكة الإنترنت لعناصر الرقابة، أصبح الفضاء الإلكتروني الميدان الجديد للتنظيمات الإرهابية تستخدمه في الاتصال والتخفي وتجميع المعلومات والتخطيط والتنسيق والحصول على التمويل والدعاية ونشر الأفكار المتطرفة التي تسيطر بها على وجدان الأفراد لتفسد عقائدهم وتستغل من خلاله معاناتهم في تحقيق مآربها خاصة التي تتعارض ومصلحة المجتمع، كما تستخدمه أيضًا في القيام بالأعمال التخريبية حيث لا تظهر فيها الهوية المباشرة للإرهابيين بشكل أبسط مما يقومون به في العالم المادي.

ونظرًا لتعدد العوامل والدوافع التي جعلت الإرهاب الإلكتروني سلاحًا سهلًا للجماعات والمنظمات الإرهابية مقارنة بالإرهاب المادي الذي يحتاج إلى أسلحة وتحركات سرية جدًا قد تصيب أو تخفق، ناهيك عن التكاليف المادية الضخمة لإنجاح عملياته، لذا نجد لزاما علينا أن نوضح الأسباب هيأت إلى ظهور الإرهاب الإلكتروني في العقد الأخير من القرن الماضي، وذلك على التفصيل الأتي:

---

(1) **Margaret Rouse**, cyberterrorism: Publish in December 2017. Available at: http://searchsecurity.techtarget.com/definition/cyberterrorism

المطلب الأول: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق.

المطلب الثاني: سهولة الاستخدام التقني وقلة التكلفة المادية

المطلب الثالث: عدم وضوح الهوية الرقمية للمستخدم.

المطلب الرابع: صعوبة اكتشاف وإثبات الجريمة الإرهابية الإلكترونية.

المطلب الخامس: تنوع وكثرة الوجهات التي يستهدفها الإرهاب الإلكتروني

المطلب السادس: غياب السيطرة والرقابة على الشبكة المعلوماتية.

المطلب الأول
ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق

لعل السبب الرئيسي في ظهور الإرهاب الإلكتروني يكمن في ضعف بنية الشبكات المعلوماتية وعدم خصوصيتها وقابليتها للاختراق؛ لأنّ شبكاتِ المعلومات مصممة في الأصل بشكلٍ مفتُوحٍ دون قيود أو حواجز أمنية عليها؛ رغبة في التوسع وتسهيل دخول المستخدمين، وللإسف لاتخلو الأنظمة الإلكترونية والشبكات من ثغرات معلوماتية، يمكن للمنظمات الإرهابية استغلالها في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية[1].

حتي أن الأنظمة الإلكترونية للطائرات لم تسلم بدورها من الاختراقات، إذ أعرب جيف كولر نائب رئيس شركة بوينج الرائدة في مجال تصنيع الطائرات المدنية عن قلقه بشأن التهديدات التي تتعرض لها برامج ونظم الطيران، قائلا: « أن الطائرات باتت في أمس الحاجة إلى الحماية الإلكترونية». مضيفًا « أن الطائرات أصبحت معرضة للخطر بسبب تعدد النظم الإلكترونية ....، ... فبعد أن يدخل – الإرهابيون– إلى المطار يبدأون في تبادل المعلومات حول مواطن الضعف والقصور في هذه الانظمة». حتي إن طائرات البوينج في السنوات القليلة الماضية كانت

---

[1] انظر: د/ عبد الله عبد العزيز العجلان، المقالة السابقة.

محور اهتمام الأمن السيبراني، وذلك عندما ادعي أحد المحللين أن طائرة الركاب ٧٨٧ دريملاينر تعاني من ضعف خطير في شبكات الكمبيوتر الموجود على متن هذه الطائرة والتي تسمح للركاب بالسيطرة عليها(١).

المطلب الثاني
سهولة الاستخدام التقني وقلة التكلفة المادية

لقد أصبحت شبكة الإنترنت وجميع وسائل التواصل الالكترونى زهيدة التكلفة ومتوفرة في جميع دول العالم، بخلاف فترة الثمانينيات من القرن الماضى، فالسمة العولمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستخدام، لا تستغرق وقتًا ولا جهدًا كبيرًا، ومصدرًا منخفض التكلفة لجمع المعلومات الاستخباراتية، مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة، ومن دون الحاجة إلى مصادر تمويل ضخمة. فعلى سبيل المثال، أتاحت تقنية Google Earth لجماعة لشكر طيبة الباكستانية الإرهابية من التخطيط لهجمات موباي عام ٢٠٠٨(٢).

فمقارنة بالإرهاب المادي الذي يتطلب أسلحة أو مدرعات أو قنابل أو مفرقعات وتحركات سرية جدًا قد تصيب أو تخفق، ناهيك عن التكاليف المادية

---

(1) **Nick Collins**, "Cyber terrorism is biggest threat to aircraft" The Telegraph, Dec 27, 2013, Available at: https://www.telegraph.co.uk/finance/newsbysector/transport/10526620/Cyber-terrorism-is-biggest-threat-to-aircraft.html

(٢) كذلك في عام ٢٠٠٧ عندما قام مجموعة من الجنود الأمريكين بالتقاط صور تذكارية في قاعدة عسكرية في العراق، وكانت خلفهم مجموعة من طائرات الهيلكوبتر، ثم قاموا بتحميلها علي الإنترنت، ولم تكن الصور توضح نوعية الطائرات أو أي معلومات مفيدة للجماعات الإرهابية، ولكن استطاعت بعض الجماعات الإرهابية استغلال العلامات الجغرافية Geotags التي حوتها الصور، لتتمكن من تحديد موقع القاعدة العسكرية، ومن ثم تدمير أربعة من طائرات الهيلكوبتر في هجوم بقذائف الهاون. راجع:

أحمد عبد الناصر أبو السعود، الإرهاب الإلكتروني – الموسوعة السياسية. علي الرابط التالى: http://political-encyclopedia.org/

لإنجاح عملياته، يحتاج الإرهاب الإلكتروني إلى بعض المعلومات وجهاز حاسوب متصل بشبكة الإنترنت لتنفيذ هجمات إلكترونية قد تسبب أضرارًا مادية واسعة النطاق، كما قد تفوق خسائرها ما قد تسببه هجمات الإرهاب المادي[١].

المطلب الثالث

عدم وضوح الهوية الرقمية للمستخدم

إذا كانت السمة العامة للجرائم الإلكترونية هي عدم وضوح هوية الجناة، فمن الضروري أن نذكر بأن عنوان برتوكول الإنترنت IP هو الوسيلة الوحيدة التي تمكن السلطات العامة من تعقب ومعرفة الجاني، إلا أن هناك طرق للتمويه واخفاء الهوية تجعل من الصعب تعقب الجناة وتقديمهم للعدالة. فعلى سبيل المثال إذا استخدم الجاني أحد مقاهي الإنترنت لتنفيذ الهجوم الإرهابي الإلكتروني ولم يكن مالك المقهي ملزما بتسجيل الزائرين أو لم يكترث بتسجيل المستخدمين سينتهي الأمر دون تحديد هوية الجاني. ونفس المشكلة تتكرر مع الشبكات اللاسلكية WLAN إن لم تكن محية بشكل خاص من قبل المالك، إذ يمكن الوصول لشبكة الإنترنت من قبل أي شخص يقع في نطاق التقاط الشبكة[٢].

بالإضافة إلى ذلك يمكن استخدام طرق أكثر تقنية لإخفاء الهوية على الإنترنت، على سبيل المثال استخدام خوادم بروكسي، أو شبكات إخفاء الهوية، أو توجيه حركة المرور الخاصة بالجناة على أجهزة الكمبيوتر المخترقة للمستخدمين

---

(1) **Gabriel Weiman**, Cyberterrorism. How Real Is the Threat, United States Institute of Peace, Washington, May 2004. p. 6. Available at: https://www.usip.org/sites/default/files/sr119.pdf

(2) **Phillip W. Brunst,** "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet". In: Marianne Wade & Almir Maljevic (eds.), A War on Terror? The European Stance on a Changing Laws and Human Rights Implications, New York: Springer, 2010. p. 54.

الأبرياء. في أي من هذه الحالات، لا يمكن تتبع جهاز الكمبيوتر الذي استخدمه الجاني[١].

لذا يعطي عدم وضوح الهوية الرقمية للمستخدم الفرصة للإرهابين في شن الهجمات الإلكترونية بعيد عن السلطات العامة، حيث يستطيع محترف الحاسوب استخدام تقنيات إخفاء الهوية، أو يتخفي تحت شخصية وهمية، أو يسجل الدخول على موقع إلكتروني على أنه "مستخدم ضيف غير محدد"، مما يجعل من الصعب جدا على الأجهزة الأمنية وقوات الشرطة تعقب الهوية الحقيقية للإرهابيين. ففي الفضاء السيبراني لا توجد حواجز مادية مثل نقاط التفتيش، أو حدود للعبور، أو مفتشي جمارك [٢].

المطلب الرابع
صعوبة اكتشاف وإثبات الجريمة الإرهابية الإلكترونية

نظرًا لما تتسم به الجريمة المعلوماتية من تباعد جغرافي وإقليمي بين الجاني والمجني عليه، وما يستخدمه الأول من وسائل فنية تقنية معقدة في كثير من الأحيان، وبراعته في انجاز العمل، فقد لا يستغرق ارتكاب الجريمة أكثر من بضع ثوانٍ بالإضافة إلى سهولة محو الدليل المتحصل عنها والتلاعب فيها[٣].

في كثير من أنواع الجرائم المعلوماتيّة لا يعلم بوقوع الجريمة أصلًا وخاصة في مجال جرائم الاختراق، وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع

---

(1) **Ibid. p. 55.**

(2) **Gabriel Weiman**, Cyberterrorism. How Real Is the Threat, United States Institute of Peace, Washington, May 2004. p. 6. Available at: https://www.usip.org/sites/default/files/sr119.pdf

[٣] د/ محمد عزت عبد العظيم، المرجع السابق، ص٦٥.

المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تعطي المجرم أملًا في الإفلات من العقوبة[١].

وبمقارنة الجريمة الإرهابية التقليدية والجريمة الإرهابية الإلكترونية، نجد الجاني في الأولي يبدأ التحضير والإعداد للجريمة مثل زيارة الموقع وتفقده في سبيل معرفة مداخله ومخارجه وتحديد الهدف ووقت تحركاته ذهابا وإيابا، أو انتقاء محل وضع القنبلة ... إلخ، أما في الجريمة الإرهابية الإلكترونية فالجاني لايحضر جسديًا في مكان الجريمة، بل يكفي أن يكون متصلا بالإنترنت من أي مكان على وجه الأرض، سواء كان هذا الاتصال ثابتا، في المنزل أو في مقهي للإنترنت، أو اتصالا محمولا عبر الهاتف الجوال. وهي ميزة كبيرة عن الهجمات الإرهابية التقليدية حيث التعرض لمخاطر الاشتباه والتعرض لمرتكبيها والقبض عليهم[٢].

المطلب الخامس
تنوع وكثرة الوجهات التي يستهدفها الإرهاب الإلكتروني

يستهدف فعل الإرهاب الإلكتروني مجموعة متنوعة من الإهداف تحقيقا لغرض محدد[٣]، حيث يساهم نظم الكمبيوتر والسكان المدنيين في تفرد الإرهاب الإلكتروني، ويتضح ذلك وبشكل جليا من خلال إمكانية تعطيل الهجمات الإلكترونية لشبكة الاتصالات السلكية واللاسلكية بأكملها، ومهاجمة المجتمع المدني حيث يتوافر

---

(١) د/ علي عدنان الفيل، الإرهاب الإلكتروني، مجلة الجامعة الخليجية، المجلد الثاني – العدد الثاني، ٢٠١٠، ص ٢٣. منشور على الموقع التالى:
https://platform.almanhal.com/Files/2/7983

(2) **Phillip W. Brunst,** Terrorism and the Internet: …, Op. cit., p. 53.

(3) **Ackerman. G., et al.,** "Assessing Terrorist Motivations for Attacking Critical Infrastructure," Center for Nonproliferation Studies, Monterey Institute of International Studies, California, Jul. 2007.

للإرهابيين مجموعة متنوعة من الأهداف الجذابة يتوقف الانتقاء منها على ما سيخلفه الهجوم من أضرار ودمار وما يحظي به الهدف من أهمية في المجتمع(١).

فالافتراض القائل بأن الهجمات ضد أنظمة الكمبيوتر لا تشكل خطرًا بالنظر إلى أنها توقع مجرد خسائر اقتصادية دون الوصول لإزهاق الأرواح. قولًا يفتقد للدقة؛ وذلك لأن التطور التكنولوجي بات يعتمد على خدمات الحوسبة والتي تطورت بهدوء لتدخل منشآت التغذية والإنتاج، والمنتجات الصيدلانية، ونظم إدارة حركة المرور وبخاصة القطارات والطائرات، والعديد من المؤسسات العسكرية والمدنية ... إلخ، عبر ما يعرف بأنظمة التحكم وحيازة البيانات (SCADA)، وهي تستخدم لقياس ومراقبة النظم الأخري، وفي كثير من الأحيان تكون هذه الأنظمة إما متصلة مباشرة بالإنترنت، أو متصلة بالشبكات الداخلية المرتبطة نفسها بالإنترنت، وبالتالى يمكن التحكم فيها عن بعد(٢).

---

(1) **Lewis T.G., et al.,** "Critical Infrastructure as Complex Emergent Systems," International Journal of Cyber Warfare & Terrorism, Vol. 1, No.1, 2011. pp.1-12.

(2) **Phillip W. Brunst,** Terrorism and the Internet: …, Op. cit., p. 65.

ووفقا لمصادر غير رسمية فإن ١٧% من أعطال أنظمة SCADA يرجع السبب فيها إلى إمكانية الوصول المباشر إلى هذا النظام، وذلك بسبب الرغبة في أن تكون هذه الأنظمة في كل مكان وفي متناول الجميع بحيث يمكن التحكم في البيانات والأنظمة عن بعد، مما ترتب عليه أن أصبحت العديد من خطوط الاتصال التي تحمل بيانات حساسة موجودة على الأرض أو حرة في الهواء أو تحت المياه بما يجعلها هدفا للعمليات الإرهابية، بالإضافة إلى ذلك يمكن لأي هجوم ناجح ضد أي موقع أن يمكن منفذيه من الوصول والتلاعب في العديد من المواقع المختلفة نظرًا لأنها – أي أنظمة التحكم عن بعد – تعتمد على أنظمة ويندوز، ويونكس في تشغيلها. راجع:

Sieber Ulrich, & Phillip W. Brunst, Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In: Council of Europe (eds.), Cyberterrorism – The Use of the Internet for Terrorist Purposes. Strasbourg: Council of Europe Publishing, 2007. pp. 9-105.

وتجدر الإشارة إلى أن تأثير اختراق أنظمة SCADA المتصلة بالإنترنت ظهر على السكان المدنيين بالولايات المتحدة الأمريكية عام ٢٠٠٣ عندما تم إسقاط ٢١ محطة للطاقة وغيرها من

ويناقش P.W. Brunst [1] **ثلاثة سيناريوهات يجب على واضعي سياسات الأمن السيبراني أخذها في الاعتبار: أولها**، الهجمات على السدود الكهرومائية. **وثانيها**، التلاعب بالسكك الحديدية وأنظمة التحكم في حركة المرور الجوي. **وثالثها**، السيطرة على محطات توليد الطاقة حيث يقدم في استعراضه الأدبي أمثلة ممتازة للهجمات الإرهابية على أنظمة التحكم هذه والتي كان من شأنها توليد الرعب في نفوس السكان المدنيين. ولا شك أن الهجمات السيبرانية الناجحة على أنظمة التحكم هذه لها تأثيرات طويلة الأمد، لما تزرعه من خوف وتشكل في الوقت نفسه خطرًا مباشرًا على حياة البشر.

إلى جانب التركيز على البنية التحتية لتكنولوجيا المعلومات والاتصالات، يستهدف الإرهاب السيبراني السكان المدنيين أيضًا[٢]. فالهجمات ضد البنية التحتية الحيوية التي تنشر الخوف وتسبب الأذى للأشخاص الأبرياء داخل المجتمع يجب

المؤسسات الهامة مثل قاعدة أندروز الجوية التي بها مركز اختبار القاذفات B-1، B-2 والذي تسبب في هبوط كبير في الطاقة في الولايات المتحدة وشرق كندا.

Phillip W. Brunst, Terrorism and the Internet…, Op. cit., pp. 65-66.

لذا تعد واحدة من المهام الكبري في الولايات المتحدة تحديد أجزاء البنية التحتية "الحيوية" وتأمينها بما يحول دون نجاح الهجوم عليها وتعريض حياة الأمة للخطر. ومنذ منتصف تسعينيات القرن الماضي حددت لجنة حماية البنية التحتية الحيوية التي شكلها الرئيس الأمريكي ثمانية مجالات من البنية التحتية واعتبرتها أهداف مستهدفة وأخري محتملة للهجمات.

See. Ayn Embar-Seddon, "Cyberterrorism: Are We Under Siege?," American Behavioral Scientist, Vol. 45, No. 6, Feb. 2002, pp. 1033-1043. Available at: http://abs.sagepub.com/content/45/6/1033.full.pdf+html [Accessed 06.09.2013].

(1) **See. Phillip W. Brunst,** Terrorism and the Internet: …, Op.cit., pp. 66-68.

(2) **R. Heickero**, "Terrorism Online and the Change of Modus Operandi," Swedish Defence Research Agency, Stockholm, Sweden, 2007, pp. 1-13.

ولمزيد من التفاصيل حول هذا الموضوع، راجع:

Michael Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Game?," Crime, Law and Social Change, Vol. 46, No. 4-5, 2006. pp.223–238; **G. Ackerman et al.,** "Assessing Terrorist Motivations for Attacking Critical Infrastructure," Center for Nonproliferation Studies, Monterey Institute of International Studies, California, Jul. 2007.

أن تصنف كإرهاب إلكتروني[١]. من منظور التأثير؛ نظرًا لأن عواقب تأثيرها على السكان المدنيين أشد من نظيرتها الموجهة ضد البنية التحتية للمعلومات والاتصالات، وبالتالى فإنها سوف تجذب انتباه الإعلام المرئي، ومن ثم يتم نشرها على نطاق أوسع.

المطلب السادس
الفراغ التنظيمي والقانوني وغياب السيطرة والرقابة على الشبكة المعلوماتية

إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والإرهاب الإلكتروني يعتبر من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني، وكذلك لو وجدت قوانين تجريمية متكاملة فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق.

كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخرجاتها يعدُّ سببًا مهمًا في تفشي ظاهرة الإرهاب الإلكتروني، حيث يمكن لأي شخص الدخول ووضع ما يريد على الشبكة، وكل ما تملكه وحدات إنفاذ القانون ووكالات مكافحة الإرهاب اختراق هذه المواقع أو إغلاقها أو وتدميرها، أو البحث عن مجهولي الهوية ومراقبتهم وتعقبهم في محاولة لإيجادهم، وهو أمر أصبح بعيد المنال في ظل هجرة الإرهابيين من شبكة الويب السطحية إلى الشبكة الويب المظلمة[٢].

---

(1) **Gabriel Weimann**, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace (USIP), Special Report 116, March 2004, pp. 1-11. Available at: https://www.usip.org/sites/default/files/sr116.pdf

(2) **Gabriel Weimann**, Terrorist Migration to the Dark Web, Perspectives on Terrorism, Vol. 10, No. 3, June 2016, p. 41. Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/viewFile/513/1013

المبحث الثالث

أدوات الإرهاب الإلكتروني

يستخدم الفضاء الالكترونى فى الارهاب بصورة غير مباشرة عن طريق تسهيل تنفيذ العمل الارهابى من خلال التواصل بين الإرهابين والتنسيق وتوفير المعلومات والحصول على التمويل ... إلخ، أو يستخدم لنشر الخوف والفزع والرعب وبث الكراهية عبر أدوات ذات طابع الكترونى فى الصراع – كالقرصنة، الفيروسات، البريد الإلكتروني، الحرمان من الخدمة، والتشفير – يكون الفضاء الالكترونى مسرح لها، وهذه الأدوات يصعب الفصل فيما بينها بمعنى أنه قد يتم استخدام واحدة أو أكثر من هذه الأدوات في الصراع. لذا قد يصعب الفصل بين الأدوات المستخدمة في الإرهاب الإلكتروني.

وعليه سوف نتناول الأدوات المستخدمة الإرهاب الإلكتروني في ستة مطالب وذلك على النحو التالى.

المطلب الأول: القرصنة:

المطلب الثاني: الفيروسات.

المطلب الثالث: البريد الإلكتروني.

المطلب الرابع: الحرمان من الخدمة.

المطلب الخامس: تشويه مواقع الويب.

المطلب السادس: التشفير.

المطلب الأول
القرصنة

تعد القرصنة Hacking من أكثر الطرق التي يستخدمها الإرهابيون[١]، وهي مصطلح عام يشير إلى جميع أشكال الوصول غير المصرح به إلى أجهزة الكمبيوتر والشبكات، والبيانات، وإلحاق الإضرار بها، وقد تظهر القرصنة في العديد من أشكال السلوك الإجرامي بما في ذلك الجرائم الإلكترونية[٢].

وتعتبر القرصنة أحد أدوات الإرهاب الإلكتروني إذا كان القصد منها تعطيل أو إصابة نظم المعلومات، أو البنية التحتية الحيوية المدارة عبر الشبكات، أو قتل الأشخاص، أو إصابتهم لغرض سياسي أو أيدلوجي. وعليه يعد من قبيل الإرهاب الإلكتروني ما قام به القراصنة في مستشفي ليفربول بإنجلترا عام ١٩٩٤ من تلاعب في النظام العلاجي للمرضي بالمستشفي عبر شبكة المعلومات، ليقدم لهم خليط شديد السمية، وقد نجا واحد منهم يبلغ تسع سنوات؛ لأن الممرضة قررت التحقق من نوع العلاج الذي وقع عليه الطبيب، إلا أن الآخرين لم يكن لهم ذلك الحظ[٣].

كذلك توفي أحد رجال المافيا ويدعي don لا لتبادل إطلاق النار الذي دخل على آثره المستشفي للعلاج، وإنما لاقتحام القراصنة لأجهزة الكمبيوتر بالمستشفي التي يعالج بها وتغييرهم نوع العلاج حتي يتسني إعطائه الحقنة القاتلة

---

(1) **See**. **Saheli Naik**, A Biggest Threat to India – Cyber Terrorism and Crime, Journal of Research in Humanities and Social Science, Quest Journals, Vol. 5, Issue. 4, 2017. pp. 27-30; **Maura Conway**, Cyberterrorism: Hype and reality. In: Leigh Armistead (eds.), Information Warfare: Separating Hype from Reality, Potomac Books, Inc. Washington, D.C. 2007. p. 83.

(2) **Rohas Nagpal**, Cyber terrorism in the context of globalization. Paper presented at II World Congress on Informatics and Law. Madrid, Spain. September 2002. p. 4. available at: http://www.asianlaws.org/aboutus/spain.pdf

(3) **Shubham Chaudhary**, Cyber Terrorism: World Wide Weaponisation!, International Journal of Law and Legal Jurisprudence Studies, Vol. 3, Issue. 2, April 2016, p. 279.

(١). ثم قاموا بتغيير الوصفات الطبية التي تمت مراجعتها بحيث يتم إلقاء اللوم على الممرضة في الحادث (٢).

وخلال الفترة من إبريل ١٩٩٠ إلى مايو ١٩٩١ نجحت مجموعة من القراصنة الهولنديين في الوصول إلى أسرار عسكرية أمريكية بالغة الحساسية عن تحركات القوات الأمريكية – إبان حرب الخليج – ومواقعها وإسلحتها، وتحركات الطائرات المقاتلة، وسعوا إلي بيع هذه المعلومات إلى السلطات العراقية إلا أن الشرطة الهولندية قبضت عليهم(٣).

وهناك العديد من الوسائل التكنولوجية التي تسهل عمليات القرصنة وأهمها ما يجري عبر التقاط حزم البيانات المارة بالشبكات packet sniffing، وهجوم العاصفة tempest attack، وكسر كلمة السر password cracking، وتجاوز المخزون الموقت buffer overflow(٤).

لمطلب الثاني
فيروسات الكمبيوتر

أولًا: تعريف الفيروسات:

الفيروسات عبارة عن برمجيات مشفرة للحاسب الآلي مثل أي برمجيات أخري يتم تصميمها بهدف محدد وهو إحداث أكبر ضرر ممكن بأنظمة الكمبيوتر،

---

(1) **See. Mohamed Chawki & Mohamed S. Abdel Wahab**, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, vol.11, No. 1, Spring 2006, p. 14. Available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf

(2) **Soumen Ganguly**, Op. cit., p. 36.

(3) **See Jack L. Brock**, Computer Security: Hackers Penetrate DOD Computer Systems. (Washington DC: General Accounting Office, 1991). Full text available online at: http://www.globalsecurity.org/security/library/report/gao/145327.pdf (accessed May25, 2006).

(٤) حول هذه التقنيات وأليات عملها، راجع:

Rohas Nagpal, Cyber terrorism ..., Op.cit., p. 4.

وتتميز بقدرتها على ربط نفسها بالبرامج الأخري وإعادة إنشاء نفسها حتي تبدو وكأنها تتكاثر وتتوالد ذاتيا، بالإضافة إلى قدرتها على الانتشار من نظام إلى أخر عبر شبكة الاتصالات بحيث يمكنها أن تنتقل عبر الحدود من أي مكان إلى أخر في العالم حتي أن انتشارها يكون أسرع من توقفها[١]، كما أن أقل الفيروسات ضررا يمكن أن يكون مميتا. على سبيل المثال، الفيروس الذي من شانه أن يوقف أجهزة الكمبيوتر التي تدعم الحياة في المستشفيات، هذا الفيروس قاتل[٢].

ولقد عانت شبكات الكمبيوتر على مر السنين من الإرهاب الإلكتروني وذلك من خلال المحاولات الدائمة والمتعمدة لزرع الفيروسات، مما تسبب في تدمير

---

[١] د/ حسين سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، دار النهضة العربية، ٢٠٠٩، ص ٤٠٦.

[2] **Rohas Nagpal**, Cyber terrorism ..., Op.cit., p. 6.

معلومات مستخدمي الكمبيوتر[١]، وأشدها شهرة هي ميليسا[٢]، إكسلوري زيب[٣]، تشيرنوبيل[٤]، الباكستاني برين[٥]، ومايكل أنجلو[١]، وسلامر[٢].

---

[١] د/ عمر أبو الفتوح الحمّامي، المرجع السابق، ص ٢٥٤.

[٢] يعد فيروس Melissa من أسرع الفيروسات التي انتشرت في العالم، وقد ظهرت تحديدا في ٢٦ مارس ١٩٩٩، وهي من نوع ماكرو فيروس متخصص في إصابة البريد الإلكتروني وهي تقوم بالإنتشار عن طريق الإلتصاق في برامج النصوص كملحق في رسالة البريد الإلكتروني وما إن يقوم المستخدم بفتح الملف الملحق بالرسالة إلا و يبدأ الفيروس بالعمل حيث يستطيع الوصول إلى قائمة المراسلة الخاصة بالمستخدم ليقوم بإرسال نفس الرسالة إلى أول خمسين عنوان دون علم المستخدم و يستمر على نفس المنوال. وقد سبب من الخسائر ما يقارب ٨٠ مليون دولار من إنتاجية ضائعة وعمليات تنظيف.

[٣] فيروس ExploreZip مشابه لميليسا وقد اكتشف لأول مرة في يونيه ١٩٩٩، إلا أنه لم يكن فيروسا وإنما تروجان وهذا يعني أنه غير قادر علي تكرار نفسه كفيروس ميلسيا ولكنه مدمر أكثر حيث يصيب الأجهزة المزودة بنظام مكرسوفت ويندوز، كذلك يختار بعض الملفات ويجعل حجمها صفر وذلك بخفض البيانات إلى لاشيء، بالإضافة إلى عدم إمكانية استرجاع هذه الملفات.

[٤] فيروس تشيرنوبيل أو PE CIH واحد من أشد الفيروسات تدميرا، يصيب الحواسيب التى تعمل بنظام ويندوز ، وينشط كل عام في يوم ٢٦ أبريل وهو الذكري السنوية لكارثة محطة تشيرنوبيل للطاقة النووية في أوكرانيا التي وقعت عام ١٩٨٦، ويقوم فيرس تشيرنوبيل بمسح الماستر بوت ريكورد للقرص الصلب فيصبح الجهاز غير قادر على الإقلاع.في نفس الوقت يقوم بمحاولة مسح البيوس حيث يكون هذا الأخير في غالب الأحيان محمي من الكتابة، لكن إن حدت مسح فسيصبح الأمر مستعصيا إذ لا بد من إعادة تنصيب البيوس و هو أمر صعب على المبتدئين، لذلك فإن الناس الذين أصيبوا بهذا الفيروس قاموا بتغيير أجهزتهم أو بالأحرى يغيرون اللوحة الأم للحاسوب.

[٥] فيرس Brain هو أول فيرس حقيقى – بالمعنى المتعارف عليه اليوم– قام بتصميمه الأخوان الباكستانيان باسط و أمجد فاروق ألفي ، حيث تضايقا الأخوان من سرقة البرامج التى صمموها ، لذا فكر الأخوان فى تصميم برنامج يشبه "مضاد النسخ المسروقة" كحماية للملكية الفكرية للبرامج التي قاما بكتابتها ، لكن بسبب وجود عيب فى البرمجة استطاع البرنامج

وقد أصاب فيروس الكمبيوتر I love you [٣] حوالى ٥٤ مليون جهاز كمبيوتر على مستوي العالم والتي تكلف إصلاحه ٧ مليار دولار ساعات إنتاجية تقريبًا[٤]، كما إتلف معلومات قدرت قيمتها بنحو يبدأ من ٥ مليار دولار حتي ١٠

استنساخ نفسه. ويقوم فيرس Brain على تغيير قطاع الإقلاع (Boot Sector) القرص المرن فإذا تم وضع القرص المرن فى جهاز الكمبيوتر ، يقوم الفيرس بنسخ نفسه فى ذاكرة الجهاز ، ومن هنا يصيب المزيد من الأقراص بمجرد وضعها فى جهاز الكمبيوتر.

(١) يعتبر فيروس مايكل أنجلو أسوأ فيروس يصيب نظام MS.DOS على الإطلاق، حيث يهاجم قطاع التشغيل في المشغل الصلب في الجهاز وأي قرص فلوبي يدخل الكمبيوتر، مما يسبب انتشار الفيروس بسرعة كبيرة. وقد تم اكتشافه لأول مرة فى إبريل ١٩٩١ فى نيوزلندا وظل ساكنا –غير محدثًا لأية أضرار حتي يوم ٦ مارس ذكرى ميلاد الفنان مايكل أنجلو – حيث أحدث أكبر قدر ممكن من التدمير في البيانات وعشرات الآلاف من الأجهزة.

(٢) ظهر هذا النوع من الفيروسات في أواخر يناير عام ٢٠٠٣ ويستهدف الخوادم وينتشر عبر الانترنت، وقد وكان العديد الشبكات غير مستعدة لمثل هذا الهجوم فنتج عن ذلك انهيار الكثير من أنظمة الخوادم المهمة مثل نظام البنك الأمريكي لخدمات ATM، ورحلات طيران شركات كونتينتال حيث قامت الأخيرة بإلغاء الكثير من الرحلات وتعطل الحجز الإلكتروني للتذاكر. وقد اصاب الفيروس حوالي ٧٥٠٠٠ نظام في ١٠ دقائق فقط وتسبب في هذا اليوم بخسائر تقدر بمليار دولار، وقد احتاج هذا الفيروس إلى ١٥ دقيقة فقط لكي يُصيب نصف عدد الخوادم الداعمة للإنترنت.

(٣) عرف هذا الفيروس بكونه واحدا من أول الفيروسات التي تخدع المستخدمين لفتح ملف ما، حيث يأتي على شكل رسالة غرامية ويرسل أعدادا هائلة منها بعنوان"I Love You"، وللأسف وصل عدد الأجهزة التي تأثرت به إلي ١٠% علي مستوي العالم، الأمر الذى اسلتزم خروج الرئيس الأمريكي فى تلك الفترة ليطمئن الشعب الأمريكي على سلامة أجهزة البنتاغون.

(4) **Jovi Tanada Yam**, Cybercrime Treaty Under Way, BUSINESSWORLD, May 3, 2001. p. 9. available at LEXIS, News Group File.

مشار إليه لدي:

Amalie M. Weber, The Council of Europe 's Convention on Cybercrime, Berkeley Technology Law Journal, Vol. 18, Issue. 1, January 2003. p. 426 note (5).

بلايين دولار أمريكي، وذلك في مايو عام ٢٠٠٠[١]. ولسنا ببعيدين عما أحدثه فيروس بلاستر الذي ألحق الدمار بنصف مليون جهاز من أجهزة الحاسوب، وذلك عام ٢٠٠٣ [٢]. بل وفيروس نيمادا nimada الذي تسبب في تدمير أكثر من ٨.٥ مليون جهاز كمبيوتر بلغت خسارتها مليار دولار تقريبا ومازال ينتشر إلى الآن[٣].

وقد قدّر مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت كلفة إصلاح الأضرار التي تسببها فيروسات المعلوماتية بنحو ١٢ مليار دولار أمريكي سنويًا[٤].

وتجدر الإشارة إلى أن كلمة الفيروس Virus في مجال المعلوماتية تستخدم للدلالة على كل البرامج الخبيثة التي تسبب إتلافا للحاسبات أو نظم المعلومات والشبكات، إلا أن الفيروس في حقيقة الأمر هو أحد أنواع هذه البرامج، والتي تشمل إلى جانبه، البكتريا Bacterium، الديدان Worms، حصان طروادة Trojan Horses، والقنابل المعلوماتية Logic Bombs، وتسبب هذه البرامج جميعا في إتلاف مكونات الحاسب الآلي[٥]. مما يتعين معه أن نلقي الضوء على أهم هذه الفيروسات، وذلك كالأتي:

ثانيًا: أنواع الفيروسات:

---

(1) **Ibid.** p. 425.

(٢) د/ عدنان جمعان محمد الزهراني، أحكام التجارة الإلكترونية في الفقه الاسلامي، دار القلم، لبنان، الطبعة الأولي ٢٠٠٩، ص ٢٨.

(٣) د/ وليد الزيدي، القرصنة علي الإنترنت والحاسوب، دار أسامة للنشر والتوزيع، عمان ٢٠٠٣، ص ٢٩.

(٤) د/ محمود الرشيدي، العنف في جرائم الإنترنت: الحماية والتأمين، الدار المصرية اللبنانية، القاهرة، ٢٠١١ ، ص ٨٥-٨٧.

(٥) د/ أحمد محمود مصطفي، جرائم الحاسبات الآلية في التشريع المصري دراسة مقارنة، دار النهضة العربية، الطبعة الأولي ٢٠١٠، ص ٢٣٤.

أ- حصان طروادة:

هي عبارة عن برامج فيروسية لديها القدرة على الاختفاء داخل برامج أخري أصلية للمستخدم بحيث عندما تعمل البرامج الأصلية ينشط الفيروس وينتشر ليبدأ أعماله التخريبية، وهو يختلف عن الفيروس في أنه لا يتكاثر ولا يلتصق بالملفات وإنما هو برنامج مستقل بذاته يحمل في طياته توقيت وأسلوب استيقاظه[١]، وهو يؤدي إلى تعديل هذه البرامج وتزوير المعلومات ومحو بعضها، وقد يصل الأمر إلى تدمير النظام كله[٢].

وتعد هذه البرمجيات من الناحية التقنية برمجيات اختراق وتجسس تهدف إلى جمع المعلومات والبيانات الخاصة بالمستخدمين وكلمات السر الخاصة بهم وغيرها ومن ثم إرسالها إلى صاحب البرنامج أو مصممه[٣]، والأسوأ من ذلك أنه يسمح للقراصنة بتصفح الجهاز المصاب أو التحكم بالملفات الموجودة به بشكل كامل أثناء اتصال الجهاز بالشبكة[٤]. وتكمن الخطورة فيما إذا ما توصل الإرهابيون إلى زراعة هذه البرمجيات في الحاسبات التي تدير مرافق البنية التحتية الحيوية ومن ثم التحكم في المرافق الاستراتيجية بالدولة المستهدفة، ولا يخفي ما قد يخلفه هذا النوع من الهجمات من خسائر فادحة.

والجدير بالذكر أن القراصنة الروس قد نجحوا عام ٢٠١١ في زراعة برامج ضارة "حصان طروادة" في البرنامج الذي يدير الكثير من البنية التحتية الحيوية

---

(1) **Michael Erbschloe**, Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code, Oxford, Elsevier Butterworth-Heinemann, 2005, p. 21.

(٢) د/ هدي حامد قشقوش، جرائم الحاسب الآلكتروني في التشريع المقارن، دار النهضة العربية، ١٩٩٢، ص ١٠٣.

(3) **George W. Reynolds**, Information Technology for Managers, Congage Learning, Boston, USA, second Edition, 2015, p. 314-315.

(٤) د/ محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية ٢٠١٠، ص ٥٢٧.

الأمريكية بما في ذلك أنابيب النفط والغاز وشبكات نقل الطاقة الكهربائية وتوزيع المياه وأنظمة الترشيح، وحتى محطات توليد الطاقة النووية، بما يسمح لهم بالسيطرة أو إيقاف المكونات الرئيسية للبنية التحتية في الولايات المتحدة مما شكل تهديدًا لمئات الآلاف من الأمريكيين، إلى أن تم اكتشافة عام ٢٠١٤[١].

ب- دودة الكمبيوتر:

دودة الكمبيوتر Computer Worms هي عبارة عن برامج تقوم باستغلال أية ثغرة في أنظمة التشغيل لكي تنتقل من حاسب لآخر، أو من شبكة لأخري عبر الوصلات التي ترتبط بها وذلك دون حاجة إلى تدخل إنساني لتنشيطها، بخلاف حصان طروادة الذي يعتمد على التدخل الإنساني لمباشرة نشاطه، كذلك هي لا تلتصق بأنظمة التشغيل في أجهزة الحاسب الآلي التي تصيبها مثل الفيروسات[٢]. وتمتاز بسرعة الانتشار ويصعب التخلص منها نظرًا لقدرتها الفائقة على التكاثر والتلون والمراوغة[٣]، وتعمل على تقليل كفاءة الشبكة، أو التخريب الفعلي للملفات والبرامج ونظم التشغيل[٤].

---

(1) **George W. Reynolds**, Ethics in Information Technology, Congage Learning, Boston, USA, Sixth Edition, 2018, p. 91.

ولمزيد من التفاصيل حول هذا الموضوع، راجع:

Jack Cloherty & Pierre Thomas, 'Trojan Horse' Bug Lurking in Vital US Computers Since 2011, ABC News, November 6, 2014, Available at: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476

(٢) د/ عمر محمد أبو بكر، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، ٢٠٠٤، ص ٣٦٧.

(٣) د/ محمد عبيد الكعبي، السياسة الجنائية في مواجهة جرائم الإنترنت «دراسة مقارنة»، دار النهضة العربية ٢٠٠٩، ص ٢١٧.

(٤) د/ محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان ٢٠٠٤، ص ٢٤٠.

ولقد ظهرت هذه النوعية من البرامج الضارة أول مرة في عام ١٩٨٨على يد الطالب الأمريكيRopert Morris وهي ماعرفت بدودة موريس[١]، التي تسببت في تدمير الآلاف من شبكات الحاسب الآلي المنتشرة في الولايات المتحدة، أضف إلى ذلك إعاقة أكثر من ستة آلاف حاسوب عن العمل من بينها الحاسبات الخاصة بوكالة الفضاء الأمريكية ناسا[٢]، بالإضافة إلى إعاقة طريق ومسلك الشبكات ناهيك عن الخسائر المادية التي ترتبت على انتشار هذا البرنامج والتي قدرت بحوالى ١٢ مليون دولار [٣].

ومن أشهر أشكال برامج الدودة عبر الإنترنت تلك المعروفة باسم دودة الحب Love Bug والتي ظهرت في الرابع من مايو عام ٢٠٠٠ وتسببت في خسائر بملايين الدولارات في العديد من المؤسسات مثل NASA، وإدارة الأمن القومي الأمريكية SAC والعديد من الشركات. ومن الأشكال الأخري للدودة فيروس جونر GONER الذي ظهر أواخر عام ٢٠٠١ وبلغت خسائرها خمسة مليارات دولار، وهناك دودة PLEXUS.B التي ظهرت وانتشرت في منتصف ٢٠٠٤ عبر البريد الإلكتروني من خلال وسائل تبادل الملفات المعروفة بـ P2P [٤].

---

[١] ودودة موريس عبارة عن برمجية تم تصميمها خصيصا لكي تعمل من خلال شبكات الحاسب الآلي عبر البريد الإلكتروني، وهي مصممة لكل حاسوب فيما إذا كان قد أصيب بها من عدمه فإذا كانت الإجابة بنعم فإنها تنتقل إلى غيره في حين إذا كانت الإجابة بالنفي فإنها تطبع نفسها فيه ثم تنتقل إلى آخر عبر الشبكة وهكذا، وتسبب حركة الدودة تعطيل جهاز الحاسب بتجميد لوحة المفاتيح والشاشة وتعبئة الذاكرة وتبطئة الجهاز. راجع: د/ عمر محمد أبو بكر ، المرجع السابق، ص ٣٦٨.

[٢] د/ حسين سعيد الغافري، المرجع السابق، ص ٤١١.

[٣] د/ أحمد محمود مصطفي، المرجع السابق، ص ٢٣٥.

[٤] راجع: د/ حسين سعيد الغافري، المرجع السابق، ص ٤١١ وما بعدها.

وهناك دودة **Santy** التي استخدمت محركات البحث Google، Yahoo، Aol، للوصول إلى المواقع المستهدفة التي تعمل ببرنامج المنتديات phpBB، بحيث تطلب من محرك البحث إنشاء قائمة بأسماء المواقع الموجودة بها الثغرة التي تنفذ من خلالها، لتدمر جميع محتويات الموقع، تاركة رسالة تفيد بأن الموقع قد تم تشويهه بواسطتها، وما إن أطلقت في ٢٠ ديسمبر ٢٠٠٤ حتي دمرت أكثر من ٤٠ ألف موقع في أقل من ٢٤ ساعة. كذلك دودة كونفيكر **Conficker** التي تصيب شبكات الشركات أو المؤسسات حيث تفتح رابطًا يمكنها من خلاله سحب معلومات من أجهزة الحاسوب الموجودة على الشبكة، وقد انطلقت في أكتوبر ٢٠٠٨ مستهدفة نظام التشغيل مايكروسوفت مستغلة ضعفا في إحدى خدمات ويندوز لتنتشر بعد ذلك عبر أجهزة الحاسوب والشبكات لدرجة أنها اصابت نحو ١٥ مليون خادم من خوادم مايكروسوفت[١].

كما لم تكتف دودة **Stuxne** بمهاجمة أجهزة المستخدمين العاديين، بل قامت بأعمال تجسس على الأنظمة الصناعية التي تعمل على نظام ويندوز وإعادة برمجتها، وخاصة نظام SCADA الذي يستخدم فى مجالات تنظيم حركة السير، وخطوط الأنابيب وإدارة المفاعلات النوويّة، وقد ضربت دودة Stuxne عدة منشآت صناعية هامة كمفاعل بوشهر النووى بإيران فضلا عن ١٥ مؤسسة صناعية أخرى، وذلك عام ٢٠١٠. وتجدر الإشارة إلى أن إيران كان لها النصيب الأفر من خسائر هذا الفيروس حيث قدرت خسائرها وحدها بحوالى ٦٠% من إجمالى الخسائر التي سببتها دودة Stuxne الأمر الذي يتبين معه أن الهدف من إطلاقها كان سياسيًا بامتياز وتقف وراءه قوى دولية[٢].

---

(١) راجع: محمد فارس، أخطر ١٠ فيروسات في التاريخ، وادي التقنية ٢٠١١/٨/١٨ على الرابط التالى: https://itwadi.com/node/1928

(2) **Yibin Xiang**, Intrusive Viruses Depth Analysis and Teaching Research, 6 th International Conference on Information Technology for Manufacturing Systems (ITMS 2016). p. 124.

ج- القنبلة المعلوماتية:

القنبلة المعلوماتية هي نوع من البرامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير مشروعة وخفية مع برامج أخري. فشكليا هي ليست ملفا كاملا متكاملا وإنما شفرة تنضم إلى مجموعة ملفات البرامج وذلك بتقسيمها إلى أجزاء متفرقة هنا وهناك حتي لا يمكن التعرف عليها بحيث تتجمع فيما بينها بحسب الأمر المعطي لها في زمن معين أو حدوث واقعة معينة، فهي مصممة بحيث تبقي ساكنة وغير فعالة إلا في الزمن المحدد أو الواقعة المحددة لذا يتعذر اكتشافها لمدة قد تصل لأشهر وأعوام[١]، ويؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل البرنامج عبر جهاز الحاسب الآلي، كما تستخدم لإتلاف المعلومات والبيانات وتغيير برامج ومعلومات النظام[٢].

د- الباب الخفي:

نشأت هذه البرامج في الأصل كآلية يستخدمها المبرمجون لتضمن لهم مدخلا خاصا للأنظمة التي يقومون ببرمجتها، خاصة عندما يتسبب خطأ برمجي في التوقف التام للنظام، وفي بعض الأحيان يقومون بذلك لأسباب خبيثة أو على الأقل مشبوهة. ومع الوقت أصبحت تستخدم من قبل القراصنة في ولوج الأنظمة المعلوماتية، واختراقها.

وأنواع شفرة الباب الخفي كثيرة ومتعددة، ولكنها تجتمع في كونها تعطي ولوجا خاصا يتجاوز الإجراءات الروتينية، ورغم أن البعض يخلط بينها وبين حصان طرواده إلا أنه يمكن التفريق بينهما من حيث أن الأخير يوحي للمستخدم بأنه برنامج ذو منفعة، في حين أن برامج الباب الخفي تقوم بعملها في الخفاء[٣].

---

[١] د/ جميل عبد الباقي الصغير، مذكرات في الحاسب الآلي، محاضرات لطلبة كلية الحقوق الفرقة الثالثة – جامعة عين شمس، مكتبة الجامعة ١٩٩٨، ص ٣٣.

[٢] د/ عمر محمد أبو بكر، المرجع السابق، ص ٣٧١.

[٣] د/ حسين سعيد الغافري، المرجع السابق، ص ٤١٧.

المطلب الثالث

البريد الإلكتروني

برز البريد الإلكتروني كشكل من أشكال الاتصالات الحديثة الأكثر تفضيلا في العالم، إلا أن سهولة استخدامه وسرعته في إيصال الرسائل فضلا عن عدم الكشف عن الهوية النسبية لمستخدميه جعلت منه أداة قوية في يد الإرهابيين والخارجين على القانون(١). إذ يعد البريد الإلكتروني من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني حيث يتم من خلاله التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، واستغلاله في نشر أفكارهم ومعتقداتهم والترويج لها والسعي لتجنيد الآخرين وضم المتعاطفين معهم عبر الرسائل الإلكترونية. كما يقوم الإرهابيون أيضا باختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليهم لمعرفة مراسلاتهم والاستفادة منها في عملياتهم الإرهابية(٢).

المطلب الرابع

الحرمان من الخدمة

الحرمان من الخدمة عبارة عن هجمات تتم عن طريق إغراق المواقع بسيل من الطلبات والبيانات حتي تصل إلى حجم أكبر من طاقتها فتنهار أو تخرج من الخدمة، وبذلك يتحقق هدف الإرهابين من إيقاف الموقع عن العمل أو حرمان من يستخدم هذا الموقع من الاستفادة منه(٣).

---

(1) **Rohas Nagpal**, Cyber terrorism ..., Op.cit., p. 8.

(٢) د/ محمد عبد الله الفايع العسيري، د/ حسن أحمد الشهري، المرجع السابق، ص ٥.

(3) **Shamsuddin Abdul Jalil**, Countering Cyber Terrorism Effectively: Are We Ready to Rumble? . US, System Administration, Networking, and Security Institute (SANS), 2003. p. 8. Available at: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154

ويدعي هذا النوع من الهجمات في بعض الأوساط "بإيدز الإنترنت"؛ وذلك لأنه ليس له علاج حتى الآن، فمهما بلغت مواصفات الهدف وسرعته وقدرته على معالجة واستقبال الطلبات يبقى له سقف معين لا يستطيع تجاوزه وإلا توقف وخرج من الخدمة. ويتم هذا الهجوم بدون كسر ملفات كلمات السر أو سرقة البيانات السرية، فهجمات حجب الخدمة تتم ببساطه بأن يقوم المهاجم بإطلاق أحد البرامج التي تزحم المرور للموقع المستهدف وبالتالى تمنع أي مستخدم آخر من الوصول إليه[١].

لذا تظل هذه الهجمات من أكثر الهجمات خطورة على شبكة الإنترنت؛ نظرًا لأنها تهدد الدول والحكومات وكل الشبكات هي عرضة لهجوم الحرمان من الخدمة وانهيار شبكاتها وأجهرتها.

هذه الهجمات تصنف الى قسمين: **أولهما**، هجمات الحرمان من الخدمة Denial of Service Attacks (DoS)، وتتم عن طريق جهاز كمبيوتر واحد وخط إنترنت واحد. وهذا النوع من الهجمات أجبر شركة كلاود ناين مزود لخدمات الإنترنت في المملكة المتحدة، إلى إغلاق الموقع بعد أن أدى الهجوم الذي استمر

ولا يزال هجوم الحرمان من الخدمة DoS أحد أكثر الأنواع شيوعًا حيث لا تتطلب هذه الهجمات من الجاني معرفة تقنية متقدمة. على سبيل المثال الهجوم الذي تعرض له ١٩٠٠٠ موقع فرنسي على شبكة الإنترنت في سياق الهجوم على مقر مجلة شارلي أبدو الساخرة في ٧ يناير ٢٠١٥، والهجمات على مواقع شبكات X-Box، PlayStation ، والهجوم الذي تعرضت له شركة دينا هوستين والذي يعد الأكبر من نوعه حيث تلقي الموقع سيل من الطلبات قدره ٤٠٠ جيجا بايت، مستغلين ضعف بروتوكول الإنترنت في تلك اللحظة. راجع:

David Cantón, Classification of DoS Attacks, Instituto Nacional de Ciberseguridad de Espana S.A. [ES]. Available at: https://www.certsi.es/en/blog/classification-dos-attacks

[١] علي الوشلي، هجمات الحرمان من الخدمة. منشور بتاريخ ٣١ أكتوبر ٢٠١٣ على الرابط التالى: https://www.isecur1ty.org

أسبوعا إلى التوقف التام عن خدمتها، وذلك في يناير ٢٠٠٢[١]. **وثانيهما**، هجمات الحرمان من الخدمة الموزعة Distributed Denial-of-Service Attacks (DDoS) وتتم عن طريق أكثر من جهاز كمبيوتر وأكثر من خط إنترنت من جميع أنحاء العالم[٢].

وهذا النوع من الهجمات، هو الذي استخدم في الهجوم على كبرى مواقع الإنترنت، مثل: ZDNet،Yahoo!، eBay، Amazon، CNN، وغيرها، وذلك في فبراير عام ٢٠٠٠[٣]، وقد بلغت الخسائر أكثر من مليار دولار [٤]. ويعد الهجوم على مصنع الصلب الألماني عام ٢٠١٤ مثال صارخ لما يمكن أن يسببه هذا النوع من أضرار مادية حيث يعتبر هذا الهجوم أحد أول هجمات الحرمان من الخدمة الموزعة ذات النوع المدمر، والذي كان له تأثير ضار على العناصر المادية في نظام التحكم الصناعي بالمصنع. فقد استخدم المهاجمون أولا تقنية التصيد الإلكتروني للوصول إلى شبكة الشركة، ثم تسللوا إلى نظام التحكم الصناعي للتأثير

---

(1) **Shamsuddin Abdul Jalil**, Op. cit., p. 8.

ولا يزال هجوم الحرمان من الخدمة DoS أحد أكثر الأنواع شيوعًا حيث لا تتطلب هذه الهجمات من الجاني معرفة تقنية متقدمة. على سبيل المثال الهجوم الذي تعرض له ١٩٠٠٠ موقع فرنسي علي شبكة الإنترنت في سياق الهجوم على مقر مجلة شارلي أبدو الساخرة في ٧ يناير ٢٠١٥، والهجمات على مواقع شبكات X-Box، PlayStation ، والهجوم الذي تعرضت له شركة دينا هوستين والذي يعد الأكبر من نوعه حيث تلقي الموقع سيل من الطلبات قدره ٤٠٠ جيجا بايت، مستغلين ضعف بروتوكول الإنترنت في تلك اللحظة. راجع:

David Cantón, Classification of DoS Attacks, Instituto Nacional de Ciberseguridad de Espana S.A. [ES]. Available at: https://www.certsi.es/en/blog/classification-dos-attacks [accessed feb 26 2015]

(2) **Shubham Chaudhary**, Op. cit., p. 281.

(3) **Ethan Zuckerman et al.,** Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites, The Berkman Center for Internet & Society at Harvard University, December 2010, p. 12. Available at: http://www.refworld.org/pdfid/4d3025492.pdf

(4) **Dorothy E. Denning**, Cyberterrorism: …, Op. cit., p. 1.

في عدد من أنظمة الأمان مما جعل من المستحيل التحكم في اغلاق أفران الإنفجار، الأمر الذي تسبب في خسائر مادية جسيمة للشركة(١).

وقد تعرضت إستونيا لأضخم هجوم لحجب الخدمة الموزعة DDos في التاريخ، حيث تعرضت الحكومة الإستونية لسلسلة هجمات حجب الخدمة عن المواقع الحكومية والقطاع الخاص بما في ذلك المؤسسات المصرفية والمواقع الاخبارية بدء من يوم ٢٧ إبريل ٢٠٠٧ لتبلغ ذروتها في ٩ مايو من ذات العام – يوم النصر – وذلك بالتزامن مع الاحتجاجات الشعبية باستوانيا وذلك على أثر الخلاف مع روسيا حول ازالة النصب التذكاري للحرب في عهد الاتحاد السوفيتي(٢). وقد تم توزيع معظم الهجمات DDoS باستخدام أساليب مختلفة مثل فيضان بينغ ping floods واستخدام شبكات Botnet التي تستخدم عادة لتوزيع البريد المزعج، أضف إلى ذلك أنه تم عرض رسائل غير مرغوب وتعليقات ساخرة على بوابات الأخبار بما في ذلك موقع الحزب الإصلاحي الإستوني(٣).

وقد أدي الهجوم إلى احداث شلل تام فى كل أوجه الحياة فى استونيا حيث أدت الهجمات الى وقف حركة قطارات السكك الحديدية؛ نظرًا لأن انظمة التحكم الخاصة بها كانت أنظمة تعمل بالكمبيوتر وكذلك توقفت ماكينات الصراف

---

(١) راجع:

David Cantón, Classification of DoS Attacks, Instituto Nacional de Ciberseguridad de Espana S.A. [ES]. Available at: https://www.certsi.es/en/blog/classification-dos-attacks

(2) **Jose Nazario**, Politically Motivated Denial of Service Attacks. In Christian Czosseck and Kenneth Geers (eds.), The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press BV, 2009. p. 165.

ولمزيد من التفصيلات، راجع:

Mitko BOGDANOSKI & Drage PETRESKI, Op. cit., p. 62; **Ian Traynor**, Russia accused of unleashing cyberwar to disable Estonia, The Guardian 17 May 2007. Available at: https://www.theguardian.com/world/2007/may/17/topstories3.russia

(3) Estonia fines man for 'cyber war'". BBC. 25 January 2008. Retrieved 23 February 2008. http://news.bbc.co.uk/2/hi/technology/7208511.stm

الالى عن العمل، كما تضمن التقارير الإخبارية معلومات عن تباطؤ في المعاملات المالية بالمصارف، كما شهدت حركة المرور اختناقات شديدة نتيجة الخلل بمنظومات التحكم فى التدفق المرورى، وتوقفت كافة أشكال الخدمات الحكومية الإلكترونية كنتيجة لهجمات الحرمان من الخدمة(١).

وتعتمد هذه الهجمات على تجنيد أجهزة كمبيوتر متصلة بالإنترنت، بدون علم مالكيها، وتوجيهها إلى بث الرزم الشبكية إلى مزود معين، بهدف إيقافه عن العمل، نتيجة ضغط البيانات المستقبلة. ويعتمد هذا النوع من الهجمات على وضع برنامج خبيث خاص، من نوع حصان طروادة في كل حاسوب متصل بالشبكة يمكن الوصول إليه، عن طريق إرسال البرنامج بواسطة البريد الإلكتروني، مثلًا، وتفعيله على هذه الأجهزة، لتعمل كأجهزة بث للرزم الشبكية، عند تلقيها الأمر بذلك من برنامج محدد يقبع على جهاز أحد المخترقين(٢).

وتستهدف هجمات الحرمان من الخدمة ثلاثة فئات هي الشبكات والنظم والتطبيقات، وعادة ما تجتمع الشبكات والأنظمة معا؛ لأن الأنظمة تتألف من الشبكات والأهداف المقصودة عادة ما تكون جزء لا يتجزأ من واحد أو آخر، بخلاف التطبيقات فيتم التعامل معها بشكل مختلف، حيث يتم الاحتفاظ بواحدة أو أكثر من الطلبات غير المرغوب فيها، وتصبح في النهاية غير قادرة على الاستجابة للطلبات المشروعة للخدمة. على سبيل المثال إذا جلست على جهاز الكمبيوتر الخاص بك وكان المتصفح مشبع بهجمات (DoS) أو (DDoS)، سيجعله عديم الفائدة وغير

---

(1) **See**. **Jose Nazario**, Op.cit., p. 166.

انظر ايضا: عادل عبد المنعم، الحروب السيبرانية .. بين المليشيات الإلكترونية والجيوش النظامية، مجلة الأهرام للكمبيوتر والإنترنت والإتصالات "لغة العصر " بتاريخ ٢٠١٧/٩/٥ ، متاح على الربط التالى:

http://aitmag.ahram.org.eg/News/83568.aspx

(2) **Rohas Nagpal**, Cyber terrorism ..., Op.cit., p. 8.

قادر على الاتصال بالإنترنت[١]. ويعمل المهاجمون في هجمات الحرمان من الخدمة بنوعيها وفي كل الفئات المستهدفة السابق الإشارة إليها على التلاعب بالشبكات المستهدفة أو خوادم الهدف مباشرة ويرجع ذلك نقص البروتوكولات أو المعايير التي قد تؤدي إلى فشل الموقع وإغلاقه، أو عن طريق استنزاف عرض النطاق الترددي أو الذاكرة أو قدرات الموقع على المعالجة[٢].

المطلب الخامس
تشويه مواقع الويب

يستهدف هذا النوع من الهجمات تشويه مواقع الويب الخاصة بضحايا الإرهاب الإلكتروني، إذ يمكن للإرهابيين تغيير محتوي هذه المواقع تماما أو جعلها تعرض دعاية للإرهابيين أو إيقافها أو إعادة توجيهه مستخدميها آليا إلى مواقع ويب أخري تحمل ذات الرسائل أو الدعاية السابقة[٣].

---

(1) **Kent Beckert**, What is a Denial of Service (DoS) Attack? - Definition, Types & Examples, Available at: https://study.com/academy/lesson/what-is-a-denial-of-service-dos-attack-definition-types-examples.html

(2) **Ibid; Georg Disterer**, Ame Alles and Axel Hervatin, Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation. In Lech J. Janczewski & Andrew M. Colarik (eds.), Cyber Warfare and Cyber Terrorism, Information Science Reference (an imprint of IGI Global), Hershey - New York, 2007. p. 263.

(3) **Michal Choras. et al.**, Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In: Akhgar, Babak & Brewster, Benjamin (eds.), Combatting Cybercrime and Cyberterrorism. Springer 2016. pp. 295-321; **Shamsuddin Abdul Jalil**, Op.cit., p. 8.

ولمزيد من التفاصيل حول هذا الموضوع، راجع:

Alexandra Whitney Samuel, Op.cit., pp. 8-9; **Noah C.N. Hampson**, Hacktivism: A New Breed of Protest in a Networked World, Boston College International & Comparative Law Review, Vol. 35. 2012. pp. 519-520; **Dorothy**

ويقصد بتشويه مواقع الويب Defacement of web sites تغيير الصفحة الرئيسية للموقع، بصفحة أخري يعلن فيها القراصنة انتصارهم على نظام مزود الويب، والإجراءات الأمنية للشبكة، الأمر الذي يتطلب معرفة معمقة لطريقة عمل الإنترنت، وبرتوكولات التشبيك، وأنظمة التشغيل التي تعمل عليها مزودات الويب. وتقتصر الأضرار التي تتسببها عمليات التشويه على الإضرار بسمعة الجهة المالكة للموقع، حيث يتم تغيير الصفحة الرئيسة فقط من الموقع، بصفحة html من تصميم الجناة، الذين يقتصر هدفهم على إيصال رسالة إلى العالم عبر الموقع، حيث يمكن في أغلب المواقع التي تتعرض لعمليات التشويه، الوصول إلى جميع الصفحات المكونة للموقع، إذا كان المستخدم يعلم عنوان الصفحة كاملًا. ومن الأمثلة على تشويه المواقع قيام مجموعة من القراصنة في أكتوبر عام ٢٠٠٠ باقتحام موقع حزب الله وحذف محتوياته ووضع نجمة داود وعلم إسرائيل عليه، وما قام به جهاز الموساد الإسرائيلي عام ٢٠٠١ من اقتحام موقع حركة حماس ونشر صور إباحية عليه[١].

كذلك ما قامت به مجموعة من الهاكرز في ٢١ يناير ٢٠٠١ من هجمات على مواقع حكومية في كل من الولايات المتحدة الأمريكية والمملكة المتحدة وأستراليا حيث استبدلت الصفحات الخاصة بتلك المواقع الحكومية بشعار المجموعة مع رسالة تفيد بأن هذا الهجوم يعتبر أكبر تشويه لمواقع حكومية وعسكرية في تاريخ البشرية، وكان من بين تلك المواقع، موقع الهيئة التشريعية لولايات كاليفورنيا وموقع وزارة الداخلية للأسكا

E. Denning, Hacktivism is the marriage of hacking and activism, Op.cit., pp. 27-28.

[١] د/ حسين سعيد الغافري، المرجع السابق، ص ٢٦٢.

وبعض مواقع السلطات المحلية بالمملكة المتحدة[١]. وخلال الفترة من ٢٨ إبريل إلى ٨ مايو ٢٠٠١ قام القراصنة الصينيون بتشويه ما يقرب من ١٠٠٠ موقع ويب أمريكي[٢].

والواقع أن مثل هذا النوع من الهجمات قد تقلص في السنوات القليلة الماضية بفعل زيادة الوعي بهذه المسألة، إلا أن ذلك لا يمنع من ظهوره مجددًا، مما يستدعي اتخاذ التدابير التقنية الاحترازية لتفادي تكرار مثل هذه الحالات الكارثية[٣].

المطلب السادس

التشفير

وثمة اتجاه يبعث على الانزعاج في الوقت الراهن ألا وهو تزايد استخدام الإرهابيين وأعضاء عصابات الجريمة المنظمة للتشفير Cryptography ذوو التردد العالى سواء كان متعلق بالصوت أو البيانات، كذلك أسلوب الإخفاء...إلخ[٤]. ومن الأمثلة البارزة على استخدام الإرهابيين للتشفير في أعمال الإرهاب أسامة بن لادن[٥]، ورمزي يوسف[١]، وليري[٢]، وكارتيل كالي[٣]، والعصابات الهولندية[٤]، والمافيا الإيطالية.

---

(١) هشام سليمان، حملة على مواقع الإنترنت الحكومية بالعالم، مقال منشور على موقع إسلام أون لاين على شبكة الإنترنت بتاريخ ٢٠٠١/١/٢٣. مشار إليه لدي: د/ حسين سعيد الغافري، المرجع السابق، ص ٢٦٣ هامش (١).

(2) **Robin A Gandhi, et al.,**, Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, IEEE Technology and Society Magazine, Spring 2011. p. 30.

(3) **Shamsuddin Abdul Jalil**, Op.cit., p. 9.

(4) **Rohas Nagpal**, Cyber terrorism ..., Op.cit., p. 10; **Shubham Chaudhary**, Op cit., p. 281.

(٥) يعتقد انه العقل المدبر وراء هجوم ١١ سبتمبر على مركز التجارة العالمى فى الولايات المتحدة، وقد استخدم أسلوب إخفاء المعلومات Steganography والتشفير ٥١٢ بت للحفاظ على قنوات اتصالية آمنة.

كذلك استخدمت تقنيات التشفير في بعض القضايا الجنائية الشهيرة، مثل: قضية أوم شيري كيو[٥]، وقضية الإرهابيين البوليفيين[٦]، وقضية جيمس دالتون بيل[١]، وقضية كيفين بولوسون[٢].

---

(١) المعقل الدبر لتفجير مركز التجارة العالمي في الولايات المتحدة الأمريكية عام ١٩٩٣ بواسطة طائرة مدنية تابعة لشركة مانيلا للخطوط الجوية عام ١٩٩٥.

(٢) وقد حكم عليه بالسجن لمدة ٩٤ عاما لادانته بتفجير مترو أنفاق نيويورك بالولايات المتحدة بواسطة قنابل حارقة عام ١٩٩٥، حيث وجدت السلطات جرثومية متطورة خاصة بتشفير الملفات الموجودة على جهاز الكمبيوتر الخاص بالجاني.

(٣) وقد اشتهر Cali cartel بأنه يستخدم تشفيرا متقدما للغاية بغرض إخفاء اتصالاته الهاتفية، وذلك عبر أجهزة اللاسلكي والراديو التي تشوه الأصوات، والهواتف التي توفر التوثيق البصري لهوية المتصل، وأدوات معرفة المتراسل من اجهزة الكمبيوتر وأجهزة المودم.

(٤) تستخدم عصابات الجريمة المنظمة الهولندية مثل PGP و PGPfone التشفير، لتشفير اتصالاتهما. كما أنهما يستخدمان الحواسيب الشخصية المحمل عليها جهاز آمن Secure Device، وهو أحد منتجات البرمجيات الهولندية لتشفير البيانات، والتي تسمح للحواسيب المحمل عليها هذا البرنامج بالاستفادة من قواعد بيانات مركبات الشرطة والاستخبارات.

(٥) ففي ٢٠ مارس ١٩٩٥ القت السلطات اليابانية القبض على طائفة (الحقيقة العليا) بعد أن القت حقائب من غاز السارين للأعصاب في مترو أنفاق طوكيو، إذ طورت هذه الطائفة العديد من الأسلحة الكيميائية والبيولوجية بما في ذلك غاز السارين، غاز الخردل، السيانيد، الجمرة الخبيثة، ويعتقد أيضا أن الاستعدادات جارية لتطوير قدرات نووية، كذلك شعاع الموت Death Ray القادر على تدمير أي وجه للحياة. وقد تم تخزين سجلات الطائفة في شكل مشفر (باستخدام التشفير غير المتناظر) على أجهزة الكمبيوتر التي عثرت عليها السلطات، وتمكنت من فك تشفيرها عقب العثور على المفتاح الخاص بأحد الإسطوانات المدمجة التي عثر عليها في مبني الطائفة، وقد كانت المعلومات المشفرة تحتوي خطط لو نفذت لتسببت بوفيات جماعية في كل من اليابان والولايات المتحدة الأمريكية.

(٦) وفي عام ١٩٩٧ اغتالت منظمة إرهابية بوليفية أربعة أفراد من الجيش الأمريكي، ونتيجة لذلك قامت القوات بغارات على مخابئ الإرهابيين حيث تمخض عن أحد الغارات العثور على معلومات مشفرة (باستخدام التشفير المتناظر)، وقد أسفر فك تشفير هذه المعلومات في وقت

ويعرف التشفير بأنه تحويل المعلومات إلى شفيرات غير مفهومة تبدو غير ذات معني[٣]، ويهدف التشفير إلى الحفاظ على سرية المعلومات الثابتة والمتحركة باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء؛ لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة[٤].

لاحق في القضاء علي الإرهابيين والقبض على واحدة من أكبر شبكات تهريب المخدرات في تاريخ بوليفيا.

(١) أطلق جيمس بيل الثار ضد دائرة الإيرادات الداخلية Internal Revenue Service (IRS) في الولايات المتحدة الأمريكية، حيث شملت دائرة نشاطه تخويف مسئولي مصلحة الضرائب الأمريكية، ومكافأة أولئك الذين قتلوا موظفي الحكومة، وتلويث منطقة خارج مباني مصلحة الضرائب في العديد من الولايات في الولايات المتحدة الأمريكية بواسطة رائحة الغاز الكريهة، وبعد القبض عليه تمكن المحققون من فك تشفير الرسائل المشفرة باستخدام التشفير المتناظر Pretty Good Privacy (PGP) التي تلقاها الجاني فقط لاكتشافهم المفتاح الخاص بكلمة المرور.

(٢) كان كيفن بولسون من القراصنة المهرة الذين قاموا بالأفعال الأتية: تزوير مسابقات إذاعية، سطو على مكاتب تبديل الهواتف، اختراق شبكات الهاتف من أجل تحديد الهواتف التي كان يجري التصنت عليها ومن ثم استغلالها وابتزازها. وقد شفر بولس كل شيء عن التنصت على الهواتف حيث اكتشف السلطات جميع الملفات التي قام بتجميعها عن ضحاياه، وقد شفر هذه الملفات أكثر من مرة. وقد استغرقت وزارة الطاقة الأمريكية العملاقة عدة أشهر لفك تشفيرها حيث تم العثور على ما يقارب من عشرة آلاف صفحة من الأدلة عقب العثور على المفتاح الخاص بالتشفير.

(٣) د/ محمد عبد الله الفايع العسيري، د/ حسن أحمد الشهري، المرجع السابق، ص ٩.
وقد عرفت المادة ٢/٥ من قانون التوقيع الإلكتروني التونسي التشفير بأنه: استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها.

(٤) هلال محمد البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، ٢٠٠٩، ص ١٧٥.

ويتم التشفير باستخدام أدوات أو وسائل لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها استخدامًا غير مشروع، بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها، وبحيث يتأكد المرسل أيضًا أن المعلومات لم يتسلمها شخص سوي المرسل إليه الذي يستطيع باستخدام الوسائل الفنية الاطلاع على محتوي المعلومات[١]، كما يتم الاطلاع على المعلومات المشفرة باستخدام ما يسمي بالمفتاح العام وهو نظام معلن للشفرة ومفتاح خاص وهو تشفير سري، ويتعين استعمال المفتاحين للتأكد من شخصية المرسل ومن قيامه بالتعبير عن إرادته[٢].

وتعتمد قوة التشفير على عدد الخانات المكونة لكل رقم وتقاس بـ (البت) فمثلا إذا كان الرقم مكون من ٤٠ خانة فإن قوة التشفير ستكون ٤٠ بت، وإذا كان الرقم عبارة عن ٥٦ خانة فإن القوة ستكون ٥٦ بت، وهكذا. علما بإن التقنية المتوفرة في هذا المجال يمكن أن توفر قوة تشفير تصل إلى أكثر من ٣٠٠٠ بت ولكن لم تسمح الحكومة الأمريكية حتي الأن بتداول قوة تشفير أكثر من ١٢٨ بت؛ لأنه كاف حدًا لحماية التجارة الإلكترونية[٣].

---

(١) د/ محمد عبيد الكعبي، الحماية الجنائية للتجارة الإلكترونية، المرجع السابق، ص ٢٩٤.

(2) **Kevin Curran**, Cryptography. In: Lech J. Janczewski & Andrew M. Colarik, (eds.), Cyber Warfare and Cyber Terrorism, Information Science Reference (an imprint of IGI Global), Hershey - New York, 2007. p. 61.

(٣) تجدر الإشارة إلى أن الوقت اللازم ليتمكن أحد قراصنة الإنترنت لفك شفرة بقوة ٥٦ بت هو ٢٢ ساعة تقريبا، أما الوقت اللازم لفك شفرة بقوة ١٢٨ بت باستخدام التقنية الحالية لفك الشفرات فهو ترليون سنة !! لأن القرصان في حالة ٥٦ بت بحاجة لتجربة ٧٢ كوادر ليون من الاحتمالات (يعني رقم وأمامه ١٥ صفر)، أما في قوة ١٢٨ فإن الاحتمالات المطلوبة للتجربة تصل إلى عدد فلكي وهو ٣٤٠ انديسليون (يعني رقم وأمامه ٣٦ صفر)؛ لذا لم نسمع أبدا بأن معلومة تم تشفيرها بهذه القوة قد تم فكها. راجع: هلال محمد البوسعيدي، المرجع السابق، ص ١٧٩.

وقد شهدت أسواق هذه البرامج انتعاشا مذهلا بعد أن سمحت السلطات الأمريكية للشركات التجارية المتخصصة ببيع هذه التقنية للجمهور وعامة الناس بعدما كانت محصورة للاستخدامات العسكرية والحكومية لسنوات طويلة، ولقد اتخذت الحكومة الأمريكية هذا القرار في سبيل تدعيم الجانب الأمني للتجارة الإلكترونية، علما بأنها وحتي وقت قريب لم تسمح بتصدير هذه التقنية إلى خارج الولايات المتحدة، وخاصة التي تزيد قوة تشفيرها عن ٥٦ بت[١]. وقد اعترف المشرع الفرنسي بالتشفير بمقتضي القانون الصادر عام ١٩٩٠ والذي سمح للمشروعات الخاصة باستخدام التشفير بعدما كان قاصرًا على المجالات العسكرية والدبلوماسية والحكومية[٢]، وخفف القانون الصادر في ٢٦ يوليو ١٩٩٠ من بعض القيود المتعلقة بالتشفير، ثم وضع القرار رقم ٩٨-١٠١ الصادر في ٢٤ فبراير ١٩٩٨ الضوابط المتعلقة باستخدام التشفير[٣].

---

[١] المرجع السابق، ص ١٧٥.

[٢] د/ مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، ٢٠٠١، ص ٣٢.

[٣] د/ فهد سيف راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، رسالة دكتوراة – أكاديمية الشرطة، مصر ٢٠٠٧، ص ٩١.

الفصل الثاني
أبعاد وملامح الإرهاب الإلكتروني

يمثل الإرهاب الإلكتروني تقاربًا بين العالم الافتراضي للفضاء السيبراني الذي تعمل فيه الأنظمة الإلكترونية وتنتقل فيه البيانات، والعالم المادي الذي يظهر فيه آثار الإرهاب المتمثل أحداث الخوف والتهديد[١]. ويلاحظ في وقتنا الحالى امتداد الإرهاب إلى العالم الافتراضي من الفضاء السيبراني وانتشاره وهو الأمر بات يهدد جميع الدول دون استثناء خاصة في ضوء استغلال هذا الفضاء من قبل الجماعات الإرهابية في عمليات التخريب وإلحاق الأذي المتعمد والحرب النفسية.

(1) **See**. **Rabiah Ahmad & Zahri Yunos**, A Dynamic Cyber Terrorism Framework, International Journal of Computer Science and Information Security, Vol. 10, No. 2, 2012. p. 156.

وكما استخدم الإرهابيون تكنولوجيا المعلومات والاتصالات كأداة للاتصال والتنسيق فيما بينهم واستخدامها في التخطيط والتدريب للعمليات الإرهابية والتجنيد وتلقي التمويل[١]، ثم توظيفها أيضًا في نشر الفكر الإرهابي عبر المواقع الإلكترونية ومن خلال وسائل التواصل الاجتماعي، والاستفادة مما توفره هذه التقنية من إخفاء للهوية وتشفير الرسائل الإلكترونية[٢]. حتي صارت شبكة الإنترنت البيئة الحاضنة للإرهاب، وبنيتها التحتية – كنظم المعلومات وأنظمة الكمبيوتر – محلا لهجماته، بالإضافة إلى استهداف البنية التحتية الحيوية من قبل جماعات الإرهاب والجريمة المنظمة، وهو الأمر الأكثر خطورة، لما قد تسببه هذه الهجمات من أضرار واسعة النطاق[٣].

لذا بات ضروريا أن نقف على الدوافع الخلفية للإرهاب الإلكتروني قبل التعرف على الجهات التي يستهدفها. وما هي مظاهر الإرهاب الإلكتروني وأشكاله ؟. وسوف نتناول ذلك في ثلاثة مباحث على النحو التالى:

المبحث الأول: دوافع الإرهاب الإلكتروني.

المبحث الثاني: وجهات الإرهاب الإلكتروني.

المبحث الثالث: مظاهر الإرهاب الإلكتروني .

المبحث الأول

دوافع الإرهاب الإلكتروني

(1) **Elizabeth Minei & Jonathan Matusitz,** Cyberspace as a new arena for terroristic propaganda: an updated examination. [Published online 2012 Aug 9.]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3510409/

(2) **See. Namosha Veerasamy & Marthie Grobler**, Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure, https://www.researchgate.net/publication/266173850 Published online January 2011.

(3) **Namosha Veerasamy**, Motivation for Cyberterrorism …, Op. cit., p. 1.

ولما كان الإرهاب الإلكتروني يشير إلى الهجمات ضد المعلومات وأنظمة الكمبيوتر والشبكات المعلوماتية المخزنة فيها بهدف إرهاب الحكومة أو المواطنين؛ تحقيقًا لأهداف سياسية أو اجتماعية باعتباره أحد جوانب الإرهاب. كما قد تستهدف الجماعات الإرهابية المواطنيين الأبرياء داخل المجتمع أو تستهدف النظم المعلوماتية احتجاجا على قضية أو الترويج لها. وعليه قد يأتي الإرهاب الإلكتروني تعبيرًا عن الدوافع السياسية أو الاجتماعية أو الأيديولوجية أو الاقتصادية التي تقود إلى استغلال تكنولوجيا المعلومات والاتصالات بهدف إلحاق الضرر بها، أو خلق حالة من الخوف والفزع في نفوس المواطنين[١].

لذا نجد لزامًا علينا أن نلقي الضوء على دوافع الهجمات السيبرانية التي تقف خلفها جماعات الإرهاب التقليدي أو الجريمة المنظمة ... إلخ، وذلك من خلال مناقشة عدد من الهجمات تغذيها دوافع سياسية، أو اجتماعية، أو أيديولوجية ، أو حتي اقتصادية. وذلك في أربع مطالب على النحو التالى:

المطلب الأول: الدوافع السياسية.

المطلب الثاني: الدوافع الإجتماعية.

المطلب الثالث: الدوافع الأيديولوجية.

المطلب الرابع: الدوافع الاقتصادية.

المطلب الأول
الدوافع السياسية

(1) **Christopher Beggs**, Cyber-Terrorism in Australia. In: Marian Quigley (eds.), Encyclopedia of Information Ethics and Security. Hershey: IGI Global, 2007. pp. 108-113. Available at: http://dx.doi.org/10.4018/978-1-59140-987-8.ch017

أتاحت التكنولوجيا الرقمية للجماعات والمنظمات الإرهابية فرصًا واسعة نحو تعزيز أعمال العنف والتخويف لمجرد احترافها هذه التقنية، ومن ثم تحقيق أهدافها السياسية[١]، حيث تصبوا هذه الجماعات إلى تقويض الثقة في المؤسسات السياسية عبر خلق مجموعة من العراقيل تحول دون استفادة المواطنيين بهذه التقنية أو النفاذ إليها، أو جعلها غير متاحة، كذلك يمكنها عبر هذه التقنيات إلحاق الأذي والضرر بالأفراد، ومن ثم إشاعة الخوف والترويع لمجموعات منهم تنفيذًا لاجندتها السياسية[٢]. وما حدث لموقع المعهد العالمي للاتصالات IGC بمدينة سان فرانسيسكو عام ١٩٨٨ خير دليل على ذلك.

فقد تلقي موقع المعهد سالف الذكر وهو المزود الرئيسي لخدمات الإنترنت IPS والذي يستضيف مواقع لمجلات إلكترونية داعمة لنشاطات منظمة الباسك الإسبانية الانفصالية ETA خلال دقائق معدودة ملايين الرسائل الإلكترونية على شكل هجمات بريد الإلكتروني واسعة النطاق، استطاعت في النهاية إيقاف الموقع عن العمل. بل وصل الأمر بمصدر هذه الرسائل الجرأة إلى التهديد بتدمير المواقع المساندة لهذا المعهد، واستهداف المؤسسات التي تستخدم خدمات IGC أيا كانت ما لم يستجيبوا لطلبهم بإيقاف موقع المجلة الإلكترونية Euskal Herria على شبكة الإنترنت[٣]، وعلى أثر ذلك أجبر المعهد إلى الإذعان لطلباتهم وتم إغلاق الموقع الإلكتروني لهذه المجلة [٤].

---

(1) **Michael Stohl**, Op cit., p. 225.

(2) **S. Berner**, "Cyber-Terrorism: Reality or Paranoia?," South African Journal of Information Management , vol. 5, No. 1, 2003, pp. 1- 4.

(٣) وتعد جريدة Euskal Herria بمثابة منشور يدعم استقلال إقليم الباسك الإسباني، ومقرها مدينة نيويورك بالولايات المتحدة الأمريكية، ورأى المهاجمون أن المعهد العالمي للاتصالات دعم المجموعة الإرهابية مثل "الأباند" و "ليبراسيون" أو "إيتا" ، التي يُعتقد أنها مسئولة عن اغتيال المسئولين الإسبان السياسيين منهم والأمنيين.

(4) **Namosha Veerasamy**, Motivation for Cyberterrorism …, Op. cit., pp. 1-2.

وفي عام ١٩٩٨ قصفت ميلشيات التاميل العرقية المحظورة حسابات البريد الإلكتروني لسفارات سريلانكا بـ ٨٠٠ رسالة يومية ولمدة أسبوعين، هذه الرسائل كانت تتضمن على سبيل المثال " نحن نمور التاميل السوداء ونقوم بهذه الهجمات لتعطيل الاتصالات". ولم يكن بوسع الحكومة السيرلانكية مراقبة نشاط منظمة نمور التاميل إيلام الانفصالية على شبكة الإنترنت بالرغم من حظرها؛ لأن موقعها الإلكتروني مقره لندن(١). كما هاجم القراصنة البرتغاليون في سبتمبر من ذات العام مواقع الحكومة الإندونسية احتجاجا على انتهاكات حقوق الإنسان في تيمور الشرقية وعرض شعار "تيمور الشرقية حرة" بالحروف الكبيرة السوداء على ذات المواقع التي هاجموها(٢).

واثناء حرب كوسوفو ١٩٩٩ هاجم قراصنة صربيون المواقع الإلكترونية للولايات المتحدة وحلف شمال الأطلنطي معترضين على تدخل الأخير في الحرب اليوغوسلافية مستخدمين هجوم Fraggle وهو عبارة عن إرسال عدد كبير من حزم البيانات لشل النظام، وقد أدي الهجوم إلى تعطيل الخدمات على العديد من أجهزة الكمبيوتر ومواقع الانترنت الحكومية(٣)، كما قام القراصنة باطلاع الجمهور الدولي بآثار تدخل الحلف في الحرب اليوغسلافية عن طريق إرسال الرسائل النصية والصور ومقاطع الفيديو عبر الفضاء الالكتروني.

وفي ديسمبر ٢٠٠٨ تعرض الموقع الإلكتروني للسفارة الفرنسية بمدينة بكين بالصين لهجوم من قبل القراصنة الصينيين كرد فعل لاجتماع الرئيس الفرنسي نيكولا ساركوزي مع الزعيم الروحي للتبت الدالاي لاما(٤).

---

(1) **Ipid.** p. 2.
(2) **Dorothy E. Denning**, Activism, Hacktivism, and Cyberterrorism …, Op. cit., p. 262.
(3) **Robin A Gandhi, et al.,** Op. cit., p. 29.
(4) **M. Handelman**, "French embassy in Beijing under cyber-attack," infosecurity.us, Dec. 12, 2008; http://infosecurity.us/?p=4408

المطلب الثاني
الدوافع الإجتماعية

لاشك أن الفضاء الإلكتروني يعد الساحة المثلي للتعبير عن مختلف الأراء واثارة القضايا الشائكة، حيث أصبح الفضاء السيبراني وبشكل متزايد وسيلة لإجراء الاحتجاجات والاعتصامات الإلكترونية التي تعبر عن الغضب من سياسات معينة، كما أصبح في الوقت نفسه محلًا للانتقام وممارسة العنف والإضرار. فقد تأتي الهجمات الإلكترونية احتجاجًا على أحداث معينة مثيرة للجدل، أو كرد فعل للاعتداء على حقوق الإنسان، أو اعتراضًا على سياسات اجتماعية معينة أو سياسات من شأنها الإضرار بالبيئة، أو أحداث تذكارية لا تحظي بشعبية. ويمكن ربط العديد من الهجمات السيبرانية بالأحداث الحالية أو التاريخية في المجال الاجتماعي[١].

فعلى سبيل المثال قامت مجموعة مناهضة للإجهاض anti-abortionist في الولايات المتحدة الأمريكية بإنشاء موقعًا إلكترونيًا لتهديد الأطباء الذين يمارسون هذا النوع من العمليات، حيث طالب الموقع من الجمهور المساهمة في الحملة عبر تقديم عناوين منازل هؤلاء الأطباء، وأرقام لوحات تراخيص سياراتهم وأسماء أبنائهم. وبناء عليه تم الاعتداء على غالبيتهم، وتعرض بعض منهم إلى القتل. ونتيجة لذلك قضي الأطباء المنشورة أسماؤهم على هذا الموقع فترة من عمرهم في حالة من الخوف والرعب حتي أن كثيرا منهم لجأ إلى التنكر، واستخدم البعض منهم واقيات من الرصاص، وقام البعض الأخر باستئجار حراسات خاصة. وقد أحيلت القضية إلى المحكمة في نهاية المطاف حيث قضي بأن نشر أسماء الأطباء الذين يقومون بعمليات الإجهاض عبر الموقع الالكتروني بمثابة عقوبة الإعدام لهؤلاء، وأمر

(1) **Anup Sharma, et al.**, A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference, International Journal of Information and Computer Security, Vol. 5, Issue. 4, Dec 2013. pp. 301-333. Available at: https://digitalcommons.unomaha.edu/compscifacpub/24/

القاضي بإزالة الموقع بالإضافة إلى التعويض بمبلغ ١٠٠ مليون دولار عن الأضرار التي لحقت بالأطراف المتضررة[١].

وفي ٢١ ديسمبر ١٩٩٥ شنت مجموعة تطلق على نفسها أسم شبكة سترانو Strano Network هجومًا إلكترونيًا ضد مواقع الويب الخاصة بالحكومة الفرنسية احتجاجا على السياسات الاجتماعية للحكومة الفرنسية، إذ أطلق المهاجمون حملة تسمي Net strike لمدة ساعة ضد المواقع الفرنسية وحث المحتجين من جميع أنحاء العالم على توجيه متصفحاتهم إلى مواقع الويب الفرنسية في ذات الساعة، ومن ثم اغراقها بسيل من الطلبات تفوق قدرتها على المعالجة[٢]. ووفقا للتقارير المعلوماتية خرجت غالبية هذه المواقع من الخدمة خلال تلك الفترة.

وفي عام ١٩٩٦ تمكن القراصنة من إغلاق شبكات الوصول العامة في نيويورك باستخدام هجوم hack attack والذي كان بمثابة ربوت إلغاء Cancelbot يمنع النفاذ آليًا لشبكة الإنترنت، والذي تسبب في تدمير أكثر من ٢٥٠٠٠ شبكة لمجموعة النقاش Usenet بعدما أصدر الكونجرس قانون آداب الاتصالات (CDA)، كما اخترقوا الموقع الإلكتروني لوزارة العدل الأمريكية وحذفوا محتويات القانون المذكور، كما حذفوا أيضًا ملفات الوزارة من على شبكة الإنترنت واستبدالها بصفحاتهم الخاصة احتجاجا على ما تم تمريره في قانون آداب الاتصالات[٣].

وفي مارس ٢٠٠١ هاجم قراصنة كوريون جنوبيون موقع وزارة التعليم اليابانية احتجاجًا على نشر كتاب التاريخ الياباني المثيرة للجدل[٤]، والتي شعروا بأنه

---

(1) **See**. **Namosha Veerasamy**, Motivation for Cyberterrorism …, Op. cit., p. 2.

(2) **See. Robin A Gandhi, et al.,** Op.cit., p. 30; **Dorothy E. Denning**, "Activism, Hacktivism, and Cyberterrorism ..., Op. cit., p. 264.

(3) **See. Michael Cross & Debra Littlejohn Shinder**, Scene of the Cybercrime, 2nd Revised Edition., Syngress, 2008. p. 52.

(٤) في إشارة إلى المسودة النهائية للكتاب المقرر على طلبة المدارس والذي يتناول حروب شرق آسيا الكبرى والذي جري تحديثه وخضع لفحص وزارة التعليم اليابانية حيث تغاضت الوزارة عن تفاصيل مهمة في هذه الحرب مثل احتلال اليابان لشبه الجزيرة الكورية والذي دام خمسة

لا يعالج العدوان العسكري الياباني على دول شرق أسيا واحتلال هذه الدول إبان الحرب العالمية الثانية بشكل عادل[١].

المطلب الثالث

الدوافع الأيديولوجية

كما استخدمت الهجمات الإلكترونية لتحقيق الأغراض السياسية والاجتماعية، استخدمت كذلك لتعزيز الدوافع الأيديولوجية لجماعات الإرهاب التقليدي والجريمة المنظمة. على سبيل المثال، قام قراصنة الكمبيوتر المتصلين بجماعة متعصبة للجنس الأبيض عام ١٩٩٦ بإسقاط المزود الرئيسي لخدمات الإنترنت IPS لولاية ماساتشوستس الأمريكية، كما أتلفوا جزءًا من نظام حفظ السجلات الخاص بنظام IPS، وقد حاول القائمون على مزود الخدمات إيقاف القراصنة عن إرسال رسائلهم العنصرية للمستخدمين والتي ارسلوها باسم مزود الخدمة، فكان رد الفعل انتقاميا إذا هدد القراصنة المستخدمين ومزود الخدمة برسائل مفادها " أنكم لم تروا بعد إرهابًا إلكترونيا". وقد استخدم في هذا الهجوم أسلوب تشويه صفحات الويب وإفساد البيانات والحرمان من الخدمة DoS تعزيزًا لعنصرية الجماعات المتعصبة للعرق الأبيض [٢].

المطلب الرابع

الدوافع الاقتصادية

وثلاثون عامًا والتي منع فيها الكوريون من استخدام لغتهم واسمائهم الخاصة، فضلا عن اجبارهم على حلف قسم الولاء لامبراطور اليابان، بالإضافة إلي تمييز انتصارات اليابان على القوي الغربية، والذهاب إلى القول بأنها – أى اليابان– قد ساعدت الدول المستعمرة في أسيا في الحصول على الاستقلال.

(1) CNN, " Japanese textbook dispute sparks cyber attack" CNN.com, Mar. 31, 2001. Available at: http://edition.cnn.com/2001/WORLD/asiapcf/east/03/31/japan.korea.website/index.html

(2) **Namosha Veerasamy**, Motivation for Cyberterrorism …. Op. cit., p. 1.

قد يتسبب الجشع الشخصي لمحترفي تكنولوجيا المعلومات، أو وقوعهم وفي ضائقة مالية، للعمل كمرتزقة لمن يدفع الثمن، ومن ثم تستقطبهم وتستغلهم جماعات الجريمة المنظمة، أو التنظيمات الإرهابية في تنفيذ أعمالهم الإجرامية في الفضاء الإلكتروني وهذا الأمر محل قلق الكثيرين. ولقد حدث ذلك بالفعل في مجال الجريمة السيبرانية، إذ تحول محترفو تكنولوجيا المعلومات – وبخاصة الصينيون – صوب هذا الميدان على أثر الركود الاقتصادي الذي ضرب الاقتصاد العالمي في الفترة من ٢٠٠٨ إلى ٢٠٠٩ وتباطؤ الاقتصاد في العديد من البلدان وفقدهم مبالغ مالية كبيرة في سوق الأوراق المالية[١].

فعلى سبيل المثال تمكن أحد محترفي تكنولوجيا المعلومات الأوكرانيون عام ٢٠٠٩ من إعادة توجيه متصفحي الويب إلى الصفحة التي قيد فيها برامج تجسس ومكافحة فيروسات مزورة ليجني من بيع هذا البرامج عبر البطاقات الائتمانية مبلغ ١٧٢٠٠٠ دولار أمريكي خلال ١٦ يوما[٢]، كما تم استغلال نقاط الضعف في الموقع الإلكتروني لوزارة الصحة للمهن الطبية في ولاية فرجينيا في مايو ٢٠٠٩ من قبل القراصنة حيث قاموا بتشفير أكثر من ٨ ملايين سجل للمرضى، وحوالي ٣٥ مليون روشتة طبية في قاعدة البيانات، ثم حذفوا البيانات الأصلية من على الموقع ثم طلب فدية بقيمة عشرة ملايين دولار نظير كلمة المرور التي تفك تشفير البيانات،

(1) **See. Robert McMillan**, "China becoming the world's malware factory," Network World, MAR 24, 2009, Available at: https://www.networkworld.com/article/2265827/data-center/china-becoming-the-world-s-malware-factory.html

(2) **Ellen Messmer,** " Ukrainian cybercriminals raked in $10K/day, Finjan reports" Network World, MAR 23, 2009 , Available at: https://www.networkworld.com/article/2265257/lan-wan/ukrainian-cybercriminals-raked-in--10k-day--finjan-reports.html

والتحذير من التأخر أو المماطلة والتسويف في دفع الفدية، والتهديد بزيادة قيمتها أو ببيع البيانات والتي تشمل أسماء وعناوين وأرقام الضمان الاجتماعي ... إلخ، [١].

المبحث الثاني
وجهات الإرهاب الإلكتروني

يستهدف الإرهاب الإلكتروني في عصرنا الحالى مواقع القوات المسلحة والجهات الأمنية، أنظمة التحكم الإلكتروني الخاصة بالبنية التحتية الحكومية، البنية التحتية الحيوية، عمل المؤسسات القومية والوطنية، والكيانات الصناعية والشركات الكبري المدارة من خلال شبكة الإنترنت.

وعليه سوف نتناول وجهات الإرهاب الإلكتروني في خمسة مطالب على النحو التالى:

المطلب الأول: الإرهاب الإلكتروني ضد القوات المسلحة.

المطلب الثاني: الإرهاب الإلكتروني ضد البنية التحتية الحكومية.

المطلب الثالث: الإرهاب الإلكتروني ضد البنية التحتية الحيوية.

المطلب الرابع: الإرهاب الإلكتروني ضد الهوية الوطنية والاجتماعية.

المطلب الخامس: الإرهاب الإلكتروني ضد الجهات الصناعية الخاصة.

---

(1) **Homeland Security News Wire**, "Virginia medical records hijacking;" May 8, 2009, Available at: http://www.homelandsecuritynewswire.com/virginia-medical-records-hijacking-update

المطلب الأول

الإرهاب الإلكتروني ضد القوات المسلحة

تستهدف هذه النوعية من الهجمات عادة، الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات. ويعد هذا النوع من أخطر السناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، وتبدأ المرحلة الأولي من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي، والصواريخ النووية، فقد تتوافر للارهابيون فرصة فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة، فيحدث ما لا يحمد عقباه على المستوي العالمي[١].

وقد يتخذ هذا النوع من الهجمات الإرهابية أشكالا مختلفة، منها رفض الخدمة Dos، التجسس، كذلك الهجمات التي تستهدف طائفة واسعة من البنى التحتية العسكرية، والوظائف، والعمليات، والخدمات، والنظم، وسائر القدرات العسكرية الأخري. وقد تم استخدام الإنترنت من قبل الجماعات الإرهابية للقيام بهجمات الإرهاب السيبراني ضد الولايات المتحدة الأمريكية بجعلها – أي شبكة

---

[١] وقد تمكن قرصان أمريكي لم يبلغ الثامنة عشرة من عمره من اختراق واحد من أكثر النظم أمانا وهو الخاص بوزارة الدفاع الأمريكية (البنتاجون) وتسلل عبر الجدرن النارية Fire Walls والتي وضعت لحماية الشبكة، وكان بإمكانه أن يعرض البشرية كلها لخطر الإبادة لو تمكن من مواصلة عمله بالنفاذ للمخزون النووي الاستراتيجي ومعرفة شفرته، وضبطها بالتالى صوب اتجاه معين لإطلاق آلاف القنابل النووية. راجع:
د/ عادل محمد علي مصطفي، جرائم الإرهاب عبر الإنترنت، مجموعة أعمال مؤتمر القانون والتكنولوجيا والذي نظمته كلية الحقوق – جامعة عين شمس في الفترة من ٩-١١ ديسمبر ٢٠١٧، الجزء الأول، ديسمبر ٢٠١٧، ص ٦٧.

الإنترنت– ساحة لمعركة افتراضية بين الأطراف العسكرية المتصارعة في وقت سابق[١].

وفي أوائل التسعينيات من القرن الماضي، تم الهجوم على مركز روما لتطوير الهواء المعروف باسم مختبرات روما وتم نسخ البيانات من أجهزة الكمبيوتر التي تحتوي على بيانات البحث والتطوير الحساسة المتعلقة بالقوات الجوية الأمريكية [٢]. كما تم سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها الجيوش التابعة للدول الأعضاء في حلف شمال الأطلنطي NATO من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية خلال عام ١٩٩٤، الأمر الذي أثار حفيظة قيادة الأركان بالحلف وحمل السلطات العسكرية الفرنسية على تصميم برامج جديدة لحماية حاسباتها الآلية[٣].

وفي عام ٢٠٠٣، شُن هجوم باستخدام دودة الإنترنت المعروفة باسم سلامر Slammer، لاختراق شبكة المعلوماتية لمحطة الطاقة النووية دافيس– بيس التي تقع في ولاية أوهايو، مما تسبب في تعطيل أنظمة الكمبيوتر الخاصة بها[٤].

وفي عام ٢٠٠٨، واجه البنتاغون الأمريكي مشكلة بسبب الهجمات السيبرانية التي أجريت باستخدام الفيروسات، مما دفع وزارة الدفاع لاتخاذ خطوة غير مسبوقة من حظر استخدام الأجهزة الخارجية[١].

---

(1) **Timothy L. Thomas**, Al Qaeda and the Internet: The Danger of "Cyberplanning", Parameters, Vol. 23, Issue. 1, 2003. pp. 112-123.

(2) **Susan W. Brenner**, "At Light Speed: Attribution and Response to Cybercrime/ Terrorism/ Warfare". Journal of Criminal Law and Criminology, Vol. 97, Winter, 2007. pp. 379-476.

(٣) د/ جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي– الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠٢، ص ٣٣.

(4) **Clay Wilson**, Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress. 2003. Available at: https://fas.org/irp/crs/RL32114.pdf

وفي عام ٢٠١٠، تم استخدام برمجيات ستاكسنيت الخبيثة Stuxnet Malware أو دودة الكمبيوتر لإجراء شكل آخر من أشكال هجوم الإرهاب الإلكتروني المعروف باسم التخريب عن طريق إرسال قراءات خاطئة لموظفي مراقبة المنشآت من أجل تخريب أجهزة الطرد المركزي النووية في محطة ناتانز النووية Natanz nuclear plantفي إيران(٢).

وفي عام ٢٠١١، تم تشويه العديد من المواقع الحكومية في الولايات المتحدة بما في ذلك موقع البيت الأبيض وبيئة الحوسبة الجوية في الولايات المتحدة من قبل المجموعة الباكستانية التي تعرف باسم نادي القراصنة Hackerz Club، والتي نفذت أيضا عمليات اقتحام غير مصرح بها وهجمات لخدمة أسماء الدومين DNS تستهدف الهياكل الأساسية العسكرية مثل الموردين العسكريين، ونظم المعلومات، ومجموعات أنظمة الأسلحة، والقوات الجوية [٣].

---

(1) **Bogdanoski, M. & Petreski, D.,** Cyber Terrorism– Global Security Threat Contemporary Macedonian Defense - International Scientific Defense, Security and Peace Journal, Vol. 13, 2013. pp. 59-73.

(2) **Jarvis, L., Macdonald, S. & Chen, T.,** A Multidisciplinary Conference on Cyberterrorism: Final Report, Cyberterrorism Project Research Report (No. 2), Swansea University, UK, July 2013. p. 10. Available at: http://www.cyberterrorism-project.org/wp-content/uploads/2013/07/CTP-Conference-Report.pdf

(3) **Jim D. Ramsay, et al**., Development of an Outcomes-based, Undergraduate Curriculum in Homeland Security. Homeland Security Affairs Journal, Vol. 6, Issue. 2, 2010. pp. 1-20; Available at: https://www.hsaj.org/articles/679
Rajeev. C. Puran, Beyond Conventional Terrorism… The Cyber Assault. SANS Institute, 2003. Available at: https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-9314

كما نفذ تنظيم داعش في مارس ٢٠١٥ عمليات اختراق لمواقع امريكية من بينها اختراق القاعدة الخاصة ببيانات الجيش الأمريكي وقام بالاستيلاء علي بيانات حساسة من خوادم وقواعد بيانات الجيش وهي خاصة بالعمليات التي تقوم بها الولايات المتحدة ضد تنظيم داعش، وطالما سرب موقع « سايبر الخلافة » تفاصيل شخصية لحسابات تم اختراقها، بما في ذلك أرقام الهواتف النقالة، لرؤساء وكالة المخابرات المركزية الأمريكية ومكتب التحقيقات الاتحادي ووكالة الأمن القومي الأمريكي. راجع:

المطلب الثاني
الإرهاب الإلكتروني ضد البنية التحتية الحكومية

ويستهدف هذا النوع من هجمات الإرهاب الإلكتروني البنى التحتية والمرافق الإلكترونية السيبرانية أو المادية. وقد أدى هجوم من هذا النوع ضد مرافق الحكومة الإستونية والجورجية إلى جعل البنية التحتية الحكومية في كليهما غير مجدية [١].

ففي عام ١٩٩٧، هاجم قراصنة ماساتشوستس خدمات الاتصالات الخاصة برج المراقبة التابع لإدارة الطيران الفيدرالية، مما أدى إلى توقف جميع الاتصالات بالمطار لمدة ست ساعات تقريبا[٢].

وفي عام ١٩٩٨، تم تشويه الصفحة الرئيسية لمركز بحوث Bhabha الذرية بالهند من قبل مخربي الإنترنت الذين سرقوا حساب البريد الإلكتروني الخاص بالمركز كاحتجاج على التجارب النووية الهندية[٣]. وفي ذات العام أيضا غمرت

جاسم محمد، الهجمات السيبرانية والإرهاب الإلكتروني.. من يقف وراءها؟ مقال منشور على موقع روسيا الأن بتاريخ ١٣ فبراير ٢٠١٧، على الرابط التالى: http://russia-now.com/ar

(1) **Maurice Dawson, et al.,** Understanding the Methods behind Cyber Terrorism. In: Mehdi Khosrow-Pour (eds.), Encyclopedia of Information Science and Technology, 3rd ed., 2015. pp. 1539–1549. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-5888-2.ch147

(2) **Susan W. Brenner**, At Light Speed …, Op.cit., p. 389; **Susan W. Brenner,** Cyber- Crime, Cyber-Terrorism and Cyber- Warfare, Revue Internationale de Droit Pénal, Vol. 77, No. 3, 2006. p. 458.

(3) **Kevin Curran, et al.,** Cyber terrorism: attacks cyber warfare and cyber terrorism. In Lech J. Janczewski & COLARIK, A. M. (Eds.) Cyber Warfare and Cyber Terrorism. Hershey- New York. 2008, p. 3.

خدمة البريد الإلكتروني لسفارات سري لانكا ٨٠٠ رسالة يوميا لمدة أسبوعين من قبل منظمة نمور التاميل السوداء لقطع أنظمة الاتصالات والحاسوب الحكومية[١].

في عام ٢٠٠١، استخدم رجل أسترالي الإنترنت للوصول إلى نظام إدارة الصرف الصحي بهدف الإفراج عن كمية هائلة من مياه الصرف الصحي الخام في الحدائق العامة، وقد أثر ذلك تأثيرا خطيرا على الحيوانات والحياة البحرية والصحة العامة[٢].

ففي أكتوبر عام ٢٠٠٢، أطلقت كيانات غير معروفة هجوم الحرمان من الخدمة خدمة DDoS ذلك الهجوم المعروف باسم DNS الذي تركز على خوادم الجذر الثلاثة عشر التي تحكم عناوين الإنترنت بالولايات المتحدة مما تسبب في تعطل ثمانية منها، ومن ثم إيقاف الملقمات لفترة من الزمن [٣]. على النقيض من هجوم DNS واجه الآلاف من عملاء الإنترنت في غرب الولايات المتحدة تأخيرات خطيرة عندما عاني مزود الخدمة مشاكل في التوجيه بسبب أخطاء البرمجة، مما أدي إلى تعطيل الخدمة، لكنه لم يكن له أي تأثير على الأمن القومي[٤].

وفي عام ٢٠٠٦، تلقى مكتب الصناعة والأمن (BIS) في وزارة التجارة الأمريكية[٥] هجوما على أنظمته الحاسوبية، مما أجبر بنك التسويات الدولية على فصل حواسيبه عن الإنترنت، مما أثر على أداء الموظفين[٦].

---

(1) **Dorothy E. Denning**, Cyberterrorism: …, Op. cit., p. 2.

(2) **Dan Verton**, Black Ice: The Invisible Threat of Cyber-Terrorism, New York, McGraw-Hill/ Osborne, 2003. p. 130.

(3) **James A. Lewis.,** Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: Center for Strategic and International Studies, Washington, DC, December 2002, p. 6.

(4) **Idem**.

(٥) مكتب الصناعة والأمن Bureau of Industry and Security في الولايات المتحدة الأمريكية هو المسؤول عن السيطرة على صادرات الولايات المتحدة من السلع والبرمجيات والتكنولوجيا والاستخدامات سواء التجارية أو العسكرية.

(6) **Susan W. Brenner**, At Light Speed …, Op. cit., pp. 389-390.

وفي عام ٢٠١٠، استهدفت وزارة العمل بدولة الإمارات العربية المتحدة هجمات انتحال الهوية من خلال نسخة مكررة من موقعها على شبكة الإنترنت تهدف إلى تضليل الأشخاص الذين يبحثون عن وظائف في الإمارات العربية المتحدة لملء بياناتهم الحساسة(١).

المطلب الثالث

الإرهاب الإلكتروني ضد البنية التحتية الحيوية

بعد أن بات الاعتماد على شبكات المعلومات وبخاصة في الدول المتقدمة من الوسائل المهمة لإدارة نظم البنية التحتية الحيوية بالدولة، ومن ثم يمكن للهجمات الإلكترونية على الشبكات التي تدار من خلالها البنية التحتية والمرافق الاستراتيجية أن تؤدي إلى نتائج خطيرة وإلحاق أوسع الضرر بالبلدان المستهدفة(٢)، في ظل اعتماد الدول المتقدمة تكنولوجيا على أجهزة الكمبيوتر ونظم البرمجيات وشبكات الاتصالات في إدارة البنية التحتية الحيوية بها، حيث ينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة، وسيادة الفوضي في الدولة(٣).

وتعرف البنية التحتية الحيوية في الولايات المتحدة بأنها: « النظم، والشبكات، سواء المادية أو الافتراضية، والتي يترتب على عجزها أو تدميرها تأثير مدمر على الأمن القومي والاقتصاد الوطني والصحة والأمن العام»(٤). أو هي تلك

---

(1) **Fadi A. Aloul**, The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, Vol. 3, No. 3, August 2012, p. 177.

(2) **See. Martin Rudner**, Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge, International Journal of Intelligence and CounterIntelligence, Vol. 26, No. 3, 2013, pp 453-454.

(3) **DCSINT**, Critical Infrastructure Threats and Terrorism: Handbook Kansas, Deputy Chief of Staff for Intelligence. 2006, pp I1-11. Available at: https://fas.org/irp/threat/terrorism/sup2.pdf

(4) Department of Homeland Security. Critical infrastructure. Washington, DC: Department of Homeland Security. Cited 23 November 2012. Retrieved from: http://www.dhs.gov/files/ programs/gc_1189168948944.shtm; 2011.

المرافق التي من شأنها توصيل الكهرباء، والمياه، والسيطرة على حركة الملاحة الجوية، وتدعيم القطاعات المالية في الدولة، والتي يعتبر انتظامها وعدم انقطاعها بمثابة البقاء على قيد الحياة، حيث يعتمد وجود هذه المرافق وضمان استمرارها في أداء وظائفها بشكل مباشر على الاتصالات والبنية الأساسية للشبكات بمختلف أنواعها(١).

وفي هذا الصدد تشير مصادر الاستخبارات البريطانية إلى أن المملكة المتحدة تتعرض لقصف الآلاف من الهجمات السيبرانية يوميا، التي يرتكبها القراصنة لحساب بعض المنظمات والتي تستهدف الحكومة والأعمال التجارية من أجل سرقة أسرار أو تعطيل النظم المحوسبة المتصلة بالشبكة(٢).

وقد تستهدف الهجمات الإرهابية الإلكترونية مجموعة واسعة من البنى التحتية الوطنية الهامة مثل المنظمات المالية، والسدود ، وأنظمة معالجة المياه، وأنظمة الاتصالات، ومرافق البريد، والمؤسسات التعليمية، وأنظمة النقل، ومقدمي الرعاية الصحية، والخدمات الدولية، وخدمات الطوارئ، ومرافق الطاقة(٣).

وتشير التقديرات إلى أن هجمات الإرهاب السيبراني على نظم المعلومات في أحد المصارف بالولايات المتحدة الأمريكية تسببت في خسائر قدرت بمليارات

---

(1) The Whitehouse. International strategy for cyberspace: prosperity, security, and openness in a networked world. Cited 12 February 2012. Retrieved from: http://www. whitehouse.gov/sites/default/files/rss viewer/international strategy for cyberspace.pdf; 2011.

(2) **Martin Rudner**, Op. cit., p. 453.

(3) **See. Dogrul Murat, et al.**, Developing an International Cooperation and Deterrence against Cyber Terrorism. Paper Presentet a the 3r International Conference on Cyber Conflict, Tallinn, 2011. Pp. 29-43. Available at: http://www.ccdcoe.org/publications/2011proceedings/DevelopingAnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf
See also. Federal Bureau of Investigation, FBI Information Sharing and Safeguarding Report 2012 (Washington, DC, 2012, available at: http://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1/fbi-information-sharing-and-safeguarding-report-2012 (accessed May 26, 2014).

الدولارات[١]. في عام ٢٠٠٤ على سبيل المثال، اعتقل مكتب التحقيقات الفيدرالي FBI إرهابيا عبر الإنترنت قام بهجوم على خدمات الطوارئ في الشرطة، مما أدى إلى استخدام بعض مستخدمي خدمة WebTV لإجراء مكالمات طوارئ مزيفة للشرطة لزيارة المواقع المزورة [٢]. في المملكة المتحدة، قام قراصنة بريطانيون بشن هجوم ضد السجلات الطبية في مستشفى ليفربول وغيروا الوصفات الطبية التي قدمتها الممرضات للمرضى بخليط شديد السمومة[٣].

في عام ٢٠٠٧، شنت هجمات DDoS الحرمان من الخدمة باستخدام حصان طروادة على البنى التحتية المالية والإعلامية والذي تسبب في تشويه هذه المواقع وإغلاقها[٤]. كما تم الكشف عن هجوم إرهابي آخر باستخدام برمجيات أورورا الخبيثة Aurora Malware للتجسس السيبراني على مقاتلات الشبح الصينية من طراز F35 وطائرات أخرى. كما أطلقت برامج فلامر الخبيثة لتصيب أجهزة الكمبيوتر في عدد من البلدان مثل إيران، لكي تنشط عن بعد الميكروفونات وكاميرات الفيديو، وتسجيل اللمسات الواقعة على لوحات المفاتيح واتخاذ لقطات لشاشات الكمبيوتر غير القانونية [٥].

في عام ٢٠٠٠، قام الكندي المعروف باسم "Mafiaboy" بعدة هجمات ضد المواقع الأتية: CNN، Yahoo، Amazon، eBay، مما تسبب في إغلاق مواقعها الإلكترونية لفترة من الزمن[٦].

---

(1) **Bhavani Thuraisingham**, Data mining for counter-terrorism. In: KARGUPTA, H., JOSHI, A., SIVAKUMAR, K. & YESHA, Y. (eds.), Data Mining: Next Generation Challenges and Future Directions. Maryland, MIT/AAAI Press.2004. pp. 157–183.

(2) **DCSINT**, Critical Infrastructure Threats and Terrorism: Handbook Kansas, Deputy Chief of Staff for Intelligence. 2006, p. VIII -2.

(3) **Rohas Nagpal**, Cyber terrorism ..., Op. cit., p. 4.

(4) **Jarvis, L., Macdonald, S. & Chen, T.,** Op. cit., p. 7.

(5) **Ibid**. p. 10.

(6) **Susan W. Brenner**, At Light Speed …, Op. cit., p. 384.

وفي عام ٢٠٠٨ نفذت هجمات ضد البنية التحتية العامة في بعض الدول العربية مثل هجمات الاحتيال المعلوماتي ضد شركة الاتصالات البحرينية، وبنك الكويت الوطني[١]. وفي يناير ٢٠١٠ كانت العديد من المواقع الإلكترونية في دولة الإمارات العربية المتحدة هدفا لهجمات الاحتيال المعلوماتي كما أفاد موقع ITP [٢]. وفي إبريل ٢٠١٠ فقد العديد من المستخدمين مدخراتهم المصرفية في الإمارات العربية المتحدة من خلال هجمات الاحتيال عبر الإنترنت[٣]. وفي إبريل ٢٠١٠ أصاب فيروس الكمبيوتر وزارة التعليم في دولة الإمارات العربية المتحدة[٤]. في يونيو ٢٠١٠ تم اختراق موقع بنك الرياض السعودي[٥]. وفي يونيو ٢٠١٠ أوقف القراصنة أيضا بث قناة الجزيرة الرياضية العالمية[٦].

المطلب الرابع

الإرهاب الإلكتروني ضد الهوية الوطنية والاجتماعية

تعمل بعض الدول والمنظمات بفاعلية في المجتمع الدولي وهي تحظي في هذا الشأن باحترام وتقدير كبير بين الأمم والمنظمات المختلفة نظرًا لمواقفها الثابتة المنحازة دائما للحق والقانون الدولي، وبالتالى إذا شوهه هذا العنصر الحيوي فقد يؤثر ذلك في الكيان المستهدف سواء كان دولة أو منظمة أو تحالف دولي. ومن

---

(1) **Fadi A. Aloul**, Op. cit., p. 176.

(2) **Vineetha Menon**, "UAE bank targeted in major phishing attacks", ITP, 2010. Available at: http://www.itp.net/579059-uae-banktargeted-inmajor-phishing-attack [Accessed January 23, 2010]

(3) "Phishing raid empties bank accounts", The National, 2010. Available at: http://www.thenational.ae/apps/pbcs.dll/article?AID=/20100405/NATIONAL/704049912&SearchID=73398739698056.

(4) Internet virus infects Ministry of Education", UAE Today, 2010. Available at: http://www.emaratalyoum. com/local-section/accidents/2010-04-12-1.106891.

(5) Riyad bank website hacked", AMEinfo, 2010. Available at: http://www.ameinfo.com/235378.html.

(6) Al Jazeera blames hackers for World Cup interruption, The National, 2010. Available at: http://www.thenational.ae/apps/pbcs.dll/article?AID=/20100613/NATIONAL/706129867&SearchID=73402848695382.

أكثر الطرق شيوعا لتدمير سمعة الهدف تشويهه عبر مواقع الويب، أو نشر الشائعات الكاذبة من خلال الوسائل الإلكترونية والشبكات الإجتماعية ... إلخ، وهي أمثلة على هجمات الإرهاب الإلكتروني [١].

ولكي يحقق الإرهابيون غايتهم المنشودة، ومن ثم يصبحون كيانًا بارزًا في عالم الإرهاب الإفتراضي يجب أن تترك هجماتهم السيرانية أثارًا مادية أو نفسية كبيرة على الكيان المستهدف. فعلى سبيل المثال أصاب فيروس الكمبيوتر عام ٢٠٠٠ حوالي ألف جهاز كمبيوتر بشركة فورد الأمريكية للسيارات حيث تلقت الشركة ١٤٠ ألف رسالة بريد إلكتروني ملوثة خلال ثلاث ساعات، مما تسبب في تعطيل خدمة البريد الإلكتروني بالشركة مدة أسبوع [٢].

وقد يحمل الإرهاب الإلكتروني وجهًا آخرًا من التهديدات التي تستهدف الأخلاق والقيم المجتمعية المعروف باسم الذعر الاخلاقي Moral Panics[٣] وهذا النوع من الهجوم الإلكتروني يستهدف الشباب عوما والفتيات بالأخص عبر الابتزاز

---

(1) **Shamsuddin Abdul Jalil**, Op.cit., p. 6.

(2) **James A. Lewis,** Assessing the Risks of Cyber Terrorism, …, Op. cit. p. 7.

(٣) ويستخدم مصطلح الذعر الاخلاقي Moral Panics للإشارة إلى مجموعة من السلوكيات المعادية للمجتمع التي ترتكبها وسائل الاعلام، وتتميز بسمات خمسة: أولها، تحويل حدثا عاديًا إلى غير عادي بوصفه سايبر بيرل هاربور أو ١١ سبتمبر الرقمي أو أنه واحد من أكبر تهديدات الإرهاب الإلكتروني. وثانيها، تضخيم انحراف بعض رجال الدين ووصفهم بأنهم السبب في التدهور الأخلاقي والاجتماعي بالمجتمع. ثالثها، وضع الأطر الأخلاقية للمجتمع وتشويه الجماعات الخارجة على هذه الأطر. رابعها، يحدث الذعر الأخلاقي أيضا خلال فترات التغيير الاجتماعي السريع والمضرب في المجتمعات. وأخيرا، يميل الذعر الأخلاقي لاستهداف الشباب وسلوكهم والذي يعتبر مقياسًا للصحة المجتمعية، وهو ما كان له صدي حقيقي في خطابات الإرهاب الإلكتروني. راجع:
Jarvis, L., Macdonald, S. & Chen, T., Op. cit., p. 9.

الجنسي Sextortion، والتنمر الإلكتروني Cyberbullying[١]، والإغواء الإلكتروني Cyber-grooming المسبب لكثير من المشكلات الاجتماعية[٢]. وقد أظهرت الدراسات أن تحميل صورة محرجة للضحية السيبرانية قد يؤدي إلى إهانة واسعة النطاق [٣]. وأظهرت دراسات أخرى أن ضحية التنمر الإلكتروني قد تتجه إلى

---

(١) التنمّر الإلكتروني Cyberbullying وسيلة يستعملها بعض المراهقين للإساءة إلى بعضهم، والتنمر له وجهان: **أولهما**، مباشر وفيه يتوجه المعتدي بعمله مباشره للضحية بعد أن يكون قد امتلك معلومات عنها مثل:

١- ارسال رسائل عبر الجوال أو الايميل فيها تهديد بالقتل أو التشهير أو تهديد بنشر الإشاعات.

٢- سرقة أرقام الحسابات السرية للضحية والاستيلاء على البريد الالكتروني الخاص به أو أحد حساباته في المواقع الاجتماعية.

٣- تشهير المتنمر بزملائه أو من كان يرتبط بهم بعلاقة عاطفية أو صداقة أو قرابة وذلك بكتابة مقالات تشويه للسمعة أو نشر صور أو فيديوهات للضحية لتصل لأكبر عدد من المشاهدين عبر شبكات التواصل الاجتماعي.

٤- ارسال مقاطع فيديو وصور جنسية للضحية بهدف استثارته أو مضايقته وتحصل غالبا حين يقوم شاب بمضايقة فتاة مراهقه بهذا العمل.

٥- انتحال شخصية الضحية عبر الانترنت في أحد المواقع الاجتماعية بهدف الاستهزاء ونشر الإشاعات ونشر صور خاصه به.

والوجه الثاني للتنمر يكون غير مباشر ويحدث عندما يتم الاستعانة بوسيط بين المعتدي والضحية. مثل الاستعانة بأحد المختصين بالكمبيوتر والبرامج واختراق أجهزة الضحايا بهدف الحصول على معلومات عنهم لتهديدهم بها .

https://en.wikipedia.org/wiki/Cyberbullying

ولمزيد من التفاصيل حول التنمر الإلكتروني، راجع:

Ian Rivers, Homophobic Bullying. Research and Theoretical Perspectives, New York : Oxford University Press, 2011; **Smith, P. K., et al.**, "Cyberbullying: Its Nature and Impact in Secondary School Pupils", Journal of Child Psychology & Psychiatry, Vol. 49, 2008. pp. 376-385; **Valerie E. Besag**, Understanding Girls' Friendships, Fights and Feuds. A Practical Approach to Girls' Bullying, Maidenhead, UK, Open University Press. 2006.

(2) **Jarvis, L., Macdonald, S. & Chen, T.,** Op. cit., p. 9.

(3) **Colette Langos**, Cyberbullying: The Challenge to Define, Cyberpsychology, Behavior and Social Networking, Vol. 15, No. 6, June 2012. pp 285-289.

الافراط في تناول الكحول أو الانخراط في تعاطي المخدرات كرد فعل سلبي على ما تتعرض له من تنمر، أو انخفاض مستوي الأداء الأكاديمي، كما قد تحفز لديها أفكار الانتحار، أو تنزلق إلى طريق الانحراف وممارسة السلوكيات العدوانية... الخ [١].

المطلب الخامس

الإرهاب الإلكتروني ضد الجهات الصناعية الخاصة

قد يكلف الإرهاب الإلكتروني منظمات الأعمال مليارات الدولارات إذا ما هاجم الإرهابيون نظم المعلومات المصرفية وأجهزوا على حسابات الأموال فيفقد البنك ملايين الدولارات وربما المليارات إذا ما تم شل نظام الكمبيوتر [٢]. وقد تمكن البعض من اختراق مجموعة سيتي جروب الأمريكية واستطاعوا سرقة عشرات

وقد أجريت دراسات في المملكة المتحدة والسويد وكل من إسبانيا وإيطاليا وألمانيا بخصوص التنمر الإلكتروني حيث أشارت الدراسات إلي أن الوسائط البصرية هي الأكثر ضررًا للضحية . وقد أخذت الدراسة الأحدث التي وقعت على ١٠٩٢ مراهق إيطالى تقييم مدي شدة تأثير الأنماط المختلفة للتنمر على الضحية، حيث أشارت النتائج إلى أن أكثر طرق التنمر الإلكتروني إلحاقًا بالضرر للذكور والأناث هي الأوضاع المرئية سواء كانت صورًا أو تسجيلات فيديو . حول هذه الدراسات راجع:

Slonje, R., & Smith, P. K., 'Cyberbullying: Another Main Type of Bullying?' Scandinavian Journal of Psychology, Vol. 49, No. 2, 2008. pp. 147-154; **Annalaura Nocentini et al.**, 'Cyberbullying: Labels, Behaviours and Definition in Three European Countries' Australian Journal of Guidance & Counselling, Vol. 20, No. 2. 2010. pp. 129-142; **Ersilia Menesini, et al**., The Measurement of Cyberbullying: Dimensional Structure and Relative Item Severity and Discrimination', Australian Journal of Guidance & Counselling Vol. 14, No. 5, 2011. pp. 267-274.

(1) **Hinduja, S. & Patchin, J.W., Bullying**, Cyberbullying, and suicide. Archives of Suicide Research, Vo. 14, No. 3, 2010. pp. 206-221; **Colette Langos**, "Regulating Cyberbullying: A South Australian Perspective", Flinders Law Journal, Vol. 16, No. 1, 2014. pp. 73-109.

(2) **Bhavani Thuraisingham,** Developing and Securing the Cloud, CRS Press, 2013. p. 361.

الملايين من الدولارات، مما أصاب الاقتصاد الأمريكي بخسائر فادحة[١]. وقد استخدم الإرهاب الإلكتروني من قبل في تدمير قطاعات صناعية محددة[٢].

وقد يكون التجسس الإلكتروني وسيلة للتحضير للإرهاب الإلكتروني حيث استخدم برنامج Titan Rain Malware لسرقة البيانات من أجهزة الكمبيوتر والشبكات التي تنتمي إلى منظمات خاصة[٣]، وخير دليل على ذلك ما حدث مع طائرات الشبح الصينة المقاتلة من طراز F35 والطائرات الأخري ، حيث تم استخدام برمجيات أورورا الخبيثة للتجسس الصناعي على هذه المقاتلات[٤].

كذلك تم استخدام برنامج Stuxnet Malware أو دودة الكمبيوتر والتي قامت بتخريب أجهزة الطرد المركزي في محطة ناناتز النووية في إيران والتي كان من شأنها إرسال قراءات خاطئة لموظفي مراقبة هذه المحطة[٥].

المبحث الثالث

أشكال الإرهاب الإلكتروني

من الصعب تحديد أشكال الإرهاب؛ فطبيعة الإرهاب الإلكتروني تتطلب اللامحدودية في التصنيف نظرًا لأنها تستخدم تكنولوجيا تتطور يومًا بعد الآخر، ولكن هناك أشكال أشار إليها أغلب الكتاب يمكن أن تصنف على أنها أشكال وأنواع الإرهاب الإلكتروني استنادا لتعريف الإرهاب الإلكتروني الذي تم ذكره ودوافعه. وتتجلي أهم أشكال الإرهاب الإلكتروني في إنشاء المواقع الإلكترونية الإرهابية،

---

(١) د/ عادل محمد علي مصطفي، المرجع السابق، ص ٦٨.

وفي ابسط الأحوال قد يسبب انقطاع التيار الكهربائي بفعل الهجمات الإلكترونية فقدان عدد من ساعات الانتاج، وبالتالى يكون سببًا في خسائر كبيرة لقطاعات المال والصناعة. انظر:

P. Santhosh Raj, et al., Role of Data Mining in Cyber Security, International Journal of Engineering Science and Computing, Vol 7. Issue No.7, July 2017.

(2) **Shamsuddin Abdul Jalil**, Op. cit., p. 7.

(3) **Ahmed H. Anjariny, et al.,** Op. cit., p. 4.

(4) **Jarvis, L., Macdonald, S. & Chen, T.,** Op. cit., p. 10.

(5) **Idem.**

تدمير المواقع الإلكترونية والنظم المعلوماتية، التهديد والترويع الإلكتروني، والتجسس الإلكتروني. وسوف نتناولها في أربع مطالب على النحو التالى:

المطلب الأول: إنشاء المواقع الإلكترونية الإرهابية.

المطلب الثاني: تدمير المواقع الإلكترونية والنظم المعلوماتية.

المطلب الثالث: التهديد والترويع الإلكتروني.

المطلب الرابع: التجسس الإلكتروني.

المطلب الأول
إنشاء المواقع الإلكترونية الإرهابية

إذا كان الحصول على المنصات الإعلامية كالقنوات التلفزيونية والإذاعية صعبًا بالنسبة للإرهابيين، فإن إنشاء مواقع خاصة بهم على شبكة الإنترنت لتخدم أهدافهم وتروج لأفكارهم الضالة أصبح سهلا وممكنا؛ لذا تحرص معظم التنظيمات الإرهابية على ان يكون لها مواقع إلكترونية وهي تعد بمثابة المقر الافتراضي لها في الفضاء السيبراني والبوق الإعلامي لهذه التنظيمات[١]. حيث استغل مجرمي الإرهاب الإلكتروني غياب السيطرة والرقابة على الشبكة المعلوماتية في إنشاء وتصميم المواقع الإلكترونية وذلك لإبراز قوتهم التنظيمة واستخدامها في الوقت نفسه للتعبئة الفكرية وتجنيد إرهابيين جدد وجمع المال وتلقين أفراد المنظمة التدريب والتعليم والوسائل المتعددة للهجمات الإرهابية [٢]. بالإضافة إلى ذلك استخدمت هذه المواقع في بيان كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية، ولشرح طرق اختراق

---

[١] د/ عبد الله عبد العزيز العجلان، المقالة السابقة.

[٢] د/ حسن أحمد الشهري، الإرهاب الإلكتروني ...، المقالة السابقة، ص ١٦.

البريد الإلكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات ... الخ[١].

وقد قام Weimann برصد الآلاف من المواقع الإلكترونية التي تديرها المنظمات الإرهابية على شبكة الإنترنت خلال الفترة من ١٩٩٧ إلى ٢٠٠٧ [٢]. حيث لاحظ اضطراد متنامي في إعداد تلك المواقع، فعند بدء الدراسة لم يكن هناك سوي ١٢ موقعًا إرهابيا، وبحلول عام ٢٠٠٠ كانت جميع الجماعات الإرهابية قد أقامت مواقع لها على شبكة الإنترنت، وفي عام ٢٠٠٣ أصبح هناك أكثر من ٢٦٠٠ موقعًا إرهابيا[٣]، بحلول نوفمبر ٢٠٠٧ ارتفع هذا العدد بشكل لافت للنظر حيث سجلت آليات الرصد ما يزيد عن ٥٨٠٠ موقع تخدم الإرهابيين ومؤيديهم[٤]. وهو ما اعتبر مؤشرا على الوجود المكثف والمتنامي للإرهاب على صفحات شبكة الإنترنت، ويستطرد قائلا: « إن الوجود الإرهابي النشط على شبكة الإنترنت هو وجود متفرق ومتنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم، فسرعان ما يغير نمطه الإلكتروني غدا، ثم يختفي ليظهر مرة أخري بعده بفترة قصيرة بشكل جديد وعنوان إلكتروني جديد ».

ويؤكد على استخدام المنظمات الإرهابية لأساليب المراوغة قائلا: « إن الجهود الحثيثة لمنع منظمة القاعدة من استخدام شبكة الإنترنت باءت بالفشل، فعند

---

[١] د/ عبد الرحمن أحمد السند، وسائل الإرهاب الإلكتروني حكمها في الإسلام ... وطرق مكافحتها، مجلة الأمن والحياة، العدد ٣٢٥ – جمادي الآخرة ١٤٣٠هـ ، ص ٣٦.

[2] **Gabriel Weimann,** Terror on the Internet: The New Arena, the New Challenges, United States Institute of Peace Press, Washington, D. C. 2006.

[3] **Gabriel Weimann**, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace (USIP), Special Report 116, March 2004.

[٤] وتتضمن آلية رصد المواقع الإرهابية على شبكة الإنترنت: تتبع المواقع الإرهابية وتحميل محتوياتها، وترجمة الرسائل سواء كانت نصوصًا أو رسومات وأرشفتها وفقًا لنظام ترميز مسبق الأعداد بما يسمح بتحليل محتويات المواقع المختلفة.

اختراق أحد مواقعهم أو استئصاله من الشبكة، تظهر عدة مواقع جديدة بملقمات جديدة URL؛ لذا تجد لبعض المنظمات الإرهابية آلاف المواقع، وذلك ليضمنوا انتشارًا أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت بعضها للتدمير تبقى المواقع الأخرى ويمكن الوصول إليها»[١].

وقد عرض Weimann نبذة عن العدد الضخم للمنظمات الإرهابية من مختلف أنحاء العالم، التي تحتل شبكة الإنترنت، والمواقع الإلكترونية لتلك المنظمات حيث لاحظ أن هذه المواقع لا تخاطب أعوانها ومموليها فحسب، بل توجه رسالاتها أيضًا للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وفيها يدعي الإرهابيون أنهم أصحاب قضايا نبيلة، ويشتكون من سوء المعاملة من قبل الآخرين.

ولقد حذر مرصد الفتاوي التكفيرية والآراء المتشددة التابع لدار الإفتاء المصرية من تنامي ظاهر الإرهاب الإلكتروني، التي كانت سببا رئيسيا في انتشار العنف والتطرف، موضحا أن المنتديات الإلكترونية ومواقع التواصل الاجتماعي أضحت الأداة الأهم في يد الجماعات الإرهابية لنشر أفكارها ووضع خططها وتجنيد أعضائها. مؤكدا في تقريره الخامس والعشرين الذي جاء تحت عنوان " دور المنتديات الإلكترونية ومواقع التواصل الاجتماعي في تجنيد الإرهابيين- الخطورة وسبل القضاء عليها" أن ٨٠ % من الذين انتسبوا إلى تنظيم داعش تم تجنيدهم عبر وسائل التواصل الاجتماعي[٢].

ولقد كشفت دراسة حديثة لمركز « سمت» للدراسات عن حجم التغلغل الكبير للتنظيمات الإرهابية والجماعات المتطرفة عبر المنصات الإعلامية ومواقع

---

[١] د/ حسن أحمد الشهري، الإرهاب الإلكتروني ....، المقالة السابقة، ص ١٦.

[٢] د/ غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ٢٠١٧، ص ٩١.

التواصل الاجتماعي، إذ قفز عدد المواقع المحسوبة على هذه الجماعات إلى ١٥٠ ألف موقع حتي نهاية عام ٢٠١٤ [١].

وقد تنبهت الحكومات الغربية إلى خطورة انتشار الفكر المتطرف على المواقع الإلكترونية وما أسفر عنه من تجنيد تنظيم داعش لمقاتلين ينتمون لهذه

---

[١] وقد أشارت الدراسة إلى : « اعتماد التنظيمات الإرهابية، عمومًا، وتنظيم داعش خصوصًا، على وسائل التواصل الاجتماعي، إذ ينشر تنظيم داعش ٣٨ رسالة جديدة يوميًا ما بين مقاطع مصورة مدتها ٢٠ دقيقة، وأفلام وثائقية طويلة، ومقالات مصورة، ومقاطع صوتية بلغات عدة. حيث جذب التنظيم من خلال شعاره الإرهابي المعروف «باقية وتتمدد» نحو ٣٠ ألف مقاتل من جميع أنحاء العالم ». وقد رصدت الدراسة تحليلًا لعينة من حسابات المتطرفين، كشفت فيها عن أن بعض المغردين يحدِّث حسابه كل خمس دقائق، ويصل مجموع التغريدات إلى ٢٦١٢ تغريدة في الساعة، فيما تشكل التغريدات النصية فقط ٩٣ % من مجموع التغريدات، وهو ما ساعد «داعش»، على سبيل المثال، في تجنيد حوالى ١٦ ألف مقاتل من ٩٠ دولة، حتى نهاية عام ٢٠١٤، وهو العام نفسه الذي وصل فيه عدد حسابات التنظيم في «تويتر» إلى ٤٦٠٠٠ حساب، كما يقضي أنصار هذه الجماعات المتطرفة نحو ٧٠ في المئة من وقتهم على الموقع نفسه.

وقد ألقت الدراسة الضوء على اهتمام التنظيمات المتطرفة على موقع «يوتيوب»، بوجود أكثر من ٩ ملايين مقطع للتنظيمات الإرهابية باللغة الإنكليزية، وأكثر من ٤٧ ألفًا باللغة الفرنسية، وأكثر من ٢٠ ألفًا بالروسية، وأكثر من ١٢ ألفًا بالعربية، وجميعها تشرح كيفية إعداد وتحضير المتفجرات، وهو ما يبرر أن ٩٠ % من الهجمات الإرهابيّة التي نفذتها جماعات إرهابيّة متطرفة استخدم فيها متفجرات يدوية الصنع. وعرّجت الدراسة على الحجم التقريبي لعدد المواقع المتطرفة التي تمتلك صفحات في الإنترنت، والتي بلغت ٢٧٠ ألف موقع، ومدى تأثيرها مقارنة بالمواقع التي تمتلكها المؤسسات الرسمية الدينية التي باتت، وفق الدراسة، صفحات «شبه ميتة» وبعدد متابعين لا يُضاهي صفحات الجماعات المتطرفة. وكذلك رصدت الدراسة أشهر المواقع والنوافذ التي تطلُّ من خلالها التنظيمات الإرهابية على العالم، وأشهرها ١٦ شبكة إعلام بلغات عدة، من بينها مؤسسة السحاب ومؤسسة الملاحم، ومؤسسة الأندلس، ومؤسسة المنارة البيضاء، ووكالة أعماق الإخبارية، ومؤسسة الفرقان، ومؤسسة الحياة، ومؤسسة أجناد.

الدول، وتوجيه هؤلاء لاشخاص أخرين داخل دولهم لارتكاب أعمال إرهابية عبر ما عرف بظاهرة الإرهاب الموجه عن بعد Terror Plots from Afar [١]، وذلك عقب سلسلة الهجمات التي تعرضت لها العاصمة الفرنسية باريس في نوفمبر ٢٠١٥ والتي أدت إلى مقتل ١٣٥ شخص، حيث قررت عدد من هذه الحكومات إزالة المحتوي المتطرف من على شبكة الإنترنت، مما أجبر الإرهابيين على البحث عن ملاذات آمنة جديدة على الإنترنت[٢].

---

[١] وقد استخدم تنظيم داعش هذا النمط من العمليات الإرهابية بدءًا من أوائل عام ٢٠١٤ ، فمن بين حوالى ٣٨ عملية إرهابية قام بها داعش في الولايات المتحدة خلال الفترة الممتدة بين ١ مارس ٢٠١٤ إلى ١ مارس ٢٠١٧، وجد أنه على الأقل ثماني هجمات منها (أي ٢١ % من مجموع هذه الهجمات) تضمنت وجود نوع من التواصل عبر الفضاء السيبراني بين منفذ العملية وأحد العناصر المرتبطة بداعش.

Alexander Meleagrou-Hitchens & Seamus Hughes, The Threat to the United States from the Islamic State's Virtual Entrepreneurs, CTC sentinel, Vol. 10, Issue 3, March 2017, p. 1.

وبالمثل، فإن الظاهرة نفسها يمكن رصدها في عدد من الدول الأوربية والأسيوية، إذ كشف تحليل حديث لحوالى ٣٨ عملية إرهابية تبناها داعش، وقعت في الفترة بين عام ٢٠١٤ إلى أكتوبر ٢٠١٦، أن حوالى ١٩ عملية منها (أى حوالى ٥٠ % من إجمالى العمليات)، تضمنت توجيهات من داعش عبر الفضاء السيبراني، وقد كان أحد أبرز الأمثلة في هذا السياق العملية التي تمت في ربيع عام ٢٠١٥ عندما قام طالب تكنولوجيا المعلومات يدعي "سيد أحمد علام" بإطلاق النار على كنيسة في باريس بعد أن تلقي توجيهات من قبل عناصر داعش عبر الإنترنت.

Ipid. p. 6; **Rukmini Callimachi**, Not "lone Wolves" after all: How ISIS guides world's terror plots from afar, The New York Times, February 4, 2017, Available at: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html [Accessed Feb 4, 2017]

وفيما يتعلق بالدول الآسيوية، فيلاحظ تكرار النمط الإرهابي نفسه هناك. ففي ماليزيا، وجد أن سبعة من ثلاث عشرة عملية إرهابية ل"داعش" تم إحباطها ما بين ٢٠١٣ وسبتمبر ٢٠١٦، يعتقد أنها تمت بتوجيه من أحد عناصر" داعش" في سوريا، والمنتمي إلى الجنسية الماليزية، وبالمثل، سعى "داعش" لتنفيذ سبع عمليات إرهابية في إندونيسيا باتباع الأسلوب نفسه.

Andrew Zammit, The Role of Virtual Planners in the 2015 Anzac Day Terror Plot, Security Challenges, Vol. 13, no. 1, 2017, p. 45.

[2] **Gabriel Weimann**, Terrorist Migration to the Dark Web …, Op. cit., p. 40.

وقد كشف ويمان في تقريره السابق عن بعض المؤشرات المبكرة على تزايد اهتمام الإرهابيين بمنصات الإنترنت المظلمة، وفي غضون عدة أشهر أكدت مراقبة الإرهاب على شبكة الإنترنت على وجود مؤشرات ونتائج جديدة لوجود الإرهابيين على شبكة الويب المظلمة.

ونتيجة للرقابة الإلكترونية الأمنية على شبكة الإنترنت السطحية Surface Web توجهت الجماعات والتنظيمات المتطرفة مثل داعش والقاعدة ... إلخ نحو استخدام شبكة الويب المظلمة[١]؛ للتواصل فيما بينها، والقيام بنشر أفكارها، وتجنيد الشباب من خلال غرف الدردشة المنتشرة في هذه الشبكة، إضافة إلى إنشاء مواقع

Gabriel Weiman, "Going Dark: Terrorism on the Dark Web", Studies in Conflict & Terrorism, Vol.39. Issue 3, 2016, pp. 195-206. URL: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546

[١] يشير مصطلح (Dark Web) إلى المحتوى الموجود على شبكة الويب العالمية غير المفهرس بواسطة محركات البحث القياسية، والذي لا يمكن الوصول إليها إلا عبر المتصفحات المتخصصة. وهي عبارة عن أنظمة شبكية تهدف إلى إخفاء هوية كل من يدخل إليها وجعله مجهولا تمامًا، وبالتالى لن تحتوي أجهزة المستخدم على أرقام بروتوكلات مفهومة حتى يمكن التعرف على جهاز المستخدم وموقعه وأي معلومات عنه، وتسمح هذه الشبكة بالعديد من الممارسات غير القانونية وهو الهدف الرئيسي لها.

Ryan Ehney and Jack D. Shorter, Deep Web, Dark Web, Invisible Web and The Post Isis World, Issues in Information Systems, Volume 17, Issue IV, 2016, pp. 36-41. Accessible at: http:// www.iacis.org/iis/2016/4_iis_2016_36-41.pdf

وقد توصلت دراسة حديثة حول شبكة الويب المظلمة إلى أن ٥٧٪ من هذه الشبكة مشغولة بمحتوى غير قانوني مثل: المواد الإباحية، والتمويل غير المشروع، ومحطات المخدرات، وتهريب الأسلحة، والعملة المزيفة، والغرف الحمراء وتتعلق بتعذيب وأكل لحوم البشر، والاتصالات الإرهابية... إلخ. ولعل أكثر هذه الأنشطة يمكن مطالعتها على أكثر المواقع شهرة "Silk Road" وهو موقع إلكتروني وسوق سوداء وأحدث سوق ممنوعات وقد اشتهر الموقع كمنصة لبيع المخدرات، وقد حقق هذا الموقع أرباح تتجاوز ١.٢ مليار دولار قبل أن تغلقه السلطات الأمريكية في أكتوبر ٢٠١٣ وتقبض على مالكه روس ويليام أولبريتشت (٣٢ عاما) بمدينة سان فرانسيسكو بولاية كاليفورنيا. وقد ارتبطت شبكة الويب المظلمة بشركة ويكيليكس سيئة السمعة، بالإضافة إلى البيتكوين، التي يُقال إنها عملة الويب المظلم، وبالطبع تستخدم الجماعات السياسية المنشقة ونشطاء الحقوق المدنية والصحفيين الاستقصائيين في البلدان القمعية شبكة الويب المظلمة للاتصال والتنظيم السري.

Daniel Moore & Thomas Rid, "Cryptopolitik and the Darknet", Survival, vol. 58. no. 1, February–March 2016, pp. 7–38. Available at: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true

وتطبيقات داخل الشبكة المظلمة لجمع التبرعات المالية غير المشروعة لتمويل هذه التنظيمات، ومن الأمثلة على ذلك استخدام تطبيق المحفظة المظلمة Dark Wallet وهو تطبيق يقوم بإخفاء المعاملات المالية الخاصة القائمة باستخدام عملة البيتكوين، وإن كانت لا تزال المنتديات وغرف الدردشة باللغتيين الإنجليزية والفرنسية تتوافر على نطاق واسع على شبكة الويب السطحية. لكن الجزء الأكبر من الخطاب المتشدد يحدث داخل الشبكة المظلمة[١]، وتأتي هذه الخطوة بعد أن تمت إزالة مئات من المواقع المرتبطة بـ ISIS كجزء من حملة عملية باريس (OpParis) [٢].

وقد ذهب تنظيم «داعش» إلى ما هو أبعد من مجرد استخدام مواقع الشبكة المظلمة، إذ عمل التنظيم على تطوير قدراته التقنية في الشبكة المظلمة، حيث أطلق في منتصف يناير ٢٠١٥ تطبيقًا مشفرًا يدعى الراوي «Alrawi» بهدف ترويج دعايته الإعلامية والأخبار ومقاطع الفيديو، وتصعب ملاحقته ومراقبة محتواه من قبل الحكومات والجهات الأمنية والوصول إليه بسبب درجات الأمان وتعقيدات الشبكة المظلمة. وهذا التطبيق غير متوافر للتحميل سوى من خلال الشبكة المظلمة وعبر روابط سرية يتداولها أفراد التنظيم من خلال تطبيق التليغرام المشفر والذي يعمل على أجهزة الأندرويد، IOS، والويندوز، وطرق أخرى أيضًا مشفرة[٣].

وقد نشر المركز الإعلامي لداعش – مركز الحياة للإعلام – رابطًا وتوضيحات حول كيفية الوصول إلى موقع الويب الجديد على الشبكة المظلمة على منتدى مرتبط بـ ISIS، كما تم توزيع الإعلان عن تطبيق الراوي المشفر الذي تستخدمه مجموعة داعش على التليجرام، وترتبط الرسائل المشتركة لمجموعة داعش بخدمة Tor مع عنوان "onion" على شبكة الويب المظلمة. ويحتوي موقع داعش على الشبكة المظلمة أرشيفًا لمواد داعش، بما في ذلك فيلمه الوثائقي لهيب الحرب

---

(١) انظر: الشبكة المظلمة، مقال متاح على الرابط التالى:
https://www.assakina.com/awareness-net/rebounds/98256.html

(2) **Gabriel Weimann**, Terrorist Migration to the Dark Web, Op.cit., p. 41.

(3) **Idem.**

The flame of war، كما يتضمن الموقع أيضا رابطًا إلي بوابة الرسائل لمجموعة داعش على التليجرام[١].

المطلب الثاني
تدمير المواقع الإلكترونية والنظم المعلوماتية

تقوم التنظيمات الإرهابية بشن هجمات إلكترونية من خلال شبكة الإنترنت، بقصد تدمير المواقع الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتشمل ثلاثة أهداف، العسكرية، والسياسية، والاقتصادية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية، فمن الممكن تصور هجوم إلكتروني إرهابي مدمر على المواقع الحيوية على الشبكة المعلوماتية وإلحاق الضرر بأنظمة القيادة والسيطرة والاتصالات ومحطات الطاقة وأسواق المال وإطفاء مصابيح ممرات هبوط الطائرات ... إلخ، بحيث يؤدي توقفها أو العبث بأنظمتها إلي حدوث آثار تدميرية تفوق ما تحدثه القنابل والمتفجرات[٢]، كما قد يحدث هجوم إلكتروني على المواقع الإلكترونية بقصد الإستيلاء على محتوياتها، كشن هجوم على المصارف المالية للاستيلاء على ما بها من أموال من أجل تمويل التنظيم[٣].

ويتم تدمير المواقع الإلكترونية أو نظم المعلومات عن طريق الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي Server-PC، أو مجموعة نظم مترابطة شبكيًا بهدف تخريب نقطة الاتصال أو النظام[٤].

---

(1) **Idem.**

(2) **See. Susan W. Brenner**, At Light Speed …, Op. cit., pp. 379-476.

(٣) د/ أيمن سيد العسقلاني، المرجع السابق، ص ١٩٢٤.

(٤) د/ عادل محمد علي مصطفي، المرجع السابق، ص ٦٤.

ولمزيد من التفاصيل حول طرق تدمير واتلاف المواقع الإلكترونية، راجع:

وتجدر الإشارة إلي أنه ليس هناك وسيلة تقنية أو تنظيمية تحول تماما دون تدمير المواقع أو اختراقها بشكل دائم؛ وذلك لأن المتغيرات التقنية، وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء سواء كان ذلك في مكونات نقطة الاتصال أو في النظم أو في الشبكة أو في البرمجة، جعلت الحيلولة دون الاختراقات صعبة جدًا، بالإضافة إلى أن هناك منظمات إرهابية يدخل ضمن أهدافها اختراق وتدمير المواقع الإلكترونية والنظم المعلوماتية.

وتتم عملية الاختراق الإلكتروني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، ويمكن أن تتم هذه العملية من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية، ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسب الآلي والشبكات المعلوماتية[1].

ومن الوسائل المستخدمة حاليًا لتدمير المواقع الإلكترونية إغراقها بمئات الألاف من الرسائل الإلكترونية من جهاز الحاسوب الخاص بالمدمر عبر ما يعرف بهجوم الحرمان من الخدمة Dos حتي تصل إلي حجم أكبر من طاقتها التخزينية، مما يشكل ضغطا يؤدي في النهاية إلي تفجير الموقع على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية

محمد سليمان الخوالدة، جريمة الدخول غير المشروع على المواقع الإلكترونية أو نظام المعلومات وفق التشريع الإردني، رسالة ماجستير، كلية الدراسات العليا، الجامعة الاردنية ٢٠١٢، ص ٦٦ وما بعدها.

[1] د/ عادل محمد علي مصطفي، المرجع السابق، ص ٦٤.

التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه[١].

المطلب الثالث

التهديد والترويع الإلكتروني

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات، ومن خلال الشبكة الدولية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرقه، وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب في محاولة للضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية تارة، ومن أجل الحصول على التمويل المالي تارة أخري [٢]. ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة التهديد، أو التهديد عن عبر المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية[٣].

وتتعدد الأساليب الإرهابية في التهديد والترويع الإلكتروني للمواطنيين، فتارة يكون التهديد بنشر فيروسات لإلحاق الضرر والدمار بأجهزة الكمبيوتر والشبكات المعلوماتية والأنظمة الإلكترونية، وتارة يكون التهديد بمهاجمة الأنظمة الصناعية الحرجة للمجتمعات الحديثة التي تعتمد على أنظمة التحكم الصناعي المدارة عبر الشبكات، والتي تجعلها عرضة للتهديدات من الخارج للبنية التحتية عبر البرامج الضارة، أو شبكات بوت، أو رفض الخدمة. وتارة ثالثة يكون التهديد بمهاجمة البنية التحتية الحيوية الحرجة لهذه المجتمعات[٤]، مثل إمدادات المياه والكهرباء والرعاية

---

[١] راجع: د/ عبد الله عبد العزيز العجلان، المقالة السابقة.

[٢] د/ أيمن سيد العسقلاني، المرجع السابق، ص ١٩٢٤.

[٣] انظر: عبد الله عبد العزيز العجلان، المقالة السابقة.

[٤] وفي هذا الصدد ارجع كريبينفيتش رئيس المركز الاستراتيجي للميزانية والتقيمات التابع للبنتاجون التزايد التدريجي للهجمات السيبرانية على البنية التحتية الحيوية نظرًا لاعتماد الأخيرة في تشغيل وظائفها على أنظمة المعلومات بشكل عام والوصول إلى الإنترنت بشكل خاص.

الصحية والاتصالات ومعالجة المياه وتكرير النفط والغاز وإنتاج المواد الكيميائية ومعالجة وإدارة خطوط الأنابيب وكهرباء السكك الحديدية لتدميرها أو على الأقل تعطيلها لفترة، بما لاتستقيم معه الحياة اليومية العادية للمواطنين، الأمر الذي من شأنه أن تقويض ثقة المواطنين في الحكومة، ويشكك في قدرتها على المحافظة على البنية التحتية الحيوية الحرجة للدولة[١].

المطلب الرابع

التجسس الإلكتروني

بالرغم من أن التجسس الإلكتروني ظاهرة جديدة نسبيًا[٢]، فان التجسس ليس بالتأكيد كذلك، إذ تم ممارسته منذ فجر التاريخ. ويصف التجسس في مفهومه

ويزيد Weimann على ذلك مستطردًا القول: أنه " في الغالب ما تكون أنظمة البنية التحتية الحيوية معقدة للغاية وبالتالى سيكون بها ضعف طفيف يمكن استغلاله، حتي أن الأنظمة التي تبدو أكثر أمانًا أما التلاعب الخارجي يمكن النفاذ إليها من قبل المطلعين الذين قد يعملوا بمفردهم أو بالتنسيق مع الإرهابيين، لأحداث ضرر كبير".

See. Andrew F. Krepinevich, Cyberwarfare: A "Nuclear Option"? Washington, D.C.: Center for Strategic and Budgetary Assessments, 2012, p. 3. Available at: http://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf

See also. **Gabriel Weimann,** "Cyberterrorism: The Sum of All Fears?" Studies in Conflict & Terrorism, Vol. 28, No. 2 , 2005. p. 144. Available at: http://dx.doi.org/10.1080/10576100590905110.

(1) ***Nina Olesen***, European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism. In: Babak Akhgar and Ben Brewster (eds.), Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities, Springer International Publishing, 2016. pp. 266-267.

(2) **Eliza Watt**, Cyberspace, Surveillance, Law and Privacy, A Thesis submitted in partial fulfilment of the requirements of the University of Westminster for the degree of Doctor of Philosophy, September 2017. p. 14. Available at: http://westminsterresearch.wmin.ac.uk/20610/1/Watt_Eliza_thesis.pdf

لكنه – أي التجسس الإلكتروني– ظاهرة آخذة في التوسع، حتي أن بعض المعلقين يجادلون بان التجسس الإلكتروني يتمتع في الوقت الحالى بعصر ذهبي؛ وذلك لعدة أسباب: أولها، أن التجسس الإلكتروني من شأنه تقليل المخاطر على وكالات الاستخبارات. وثانيها، يسمح التجسس

التقليدي الممارسة التي يتم بموجبها إرسال الدولة وكيلا عنها إلي أراضي دولة أخري من أجل الوصول إلي المعلومات السرية والحصول عليها. ومع ذلك، فقد استغلت الدول التطورات التي حدثت في مجال التكنولوجيا من أجل ابتكار طرق أكثر فعالية يمكن من خلالها إجراء التجسس. ومع اكتشاف السفن والطائرات والأجرام السماوية، بدت البحار والسماء والفضاء الخارجي كنطاقات يمكن استغلالها كمنصات للتجسس عن بعد. ولذلك، فإنه ليس من المستغرب تسخير الفضاء الإلكتروني أيضا كوسيلة يمكن من خلالها ارتكاب التجسس(١).

والتجسس هو الأسلوب السائد في جمع المعلومات الاستخبارية، ويعرف بأنه « جمع بوعي لمعلومات محددة، ووفقًا لإسلوب مخادع، أمرت به حكومة أو منظمة معادية أو مشبوهة، وتم إنجازه من قبل أشخاص غير مصرح لهم من قبل الهدف، في القيام بهذا التجميع »(٢).

أما التجسس الإلكتروني فيكمن في الحصول على المعلومات السرية دون إذن من أصحابها سواء كانوا أشخاص، أو شركات، أو حكومات، تحقيقًا لميزة اقتصادية، أو سياسية، أو عسكرية بإستخدام وسائل غير مشروعة عبر الإنترنت، أو

الإلكتروني بتوسيع نطاق مصادر أنشطة جمع المعلومات الاستخبارية. ثالثها، توفيره إمكانيات لم يسمع بها من قبل عن سهولة وسرعة وتكلفة جمع المعلومات الاستخبارية. رابعها، يعمل التجسس على جلب كميات لا حصر لها من المعلومات.

Katharina Ziolkowski, "Peacetime cyber espionage- new tendenceies public international law" In: Katharina Ziolkowski (eds.), Peacetime Regime for state activities in Cyber-space: International law, International Relations Diplomacy, (NATO CCDCOE Publications, Tallinn 2013). p. 425.

(1) **See. Ruseell Buchan**, "Cyber espionage and international law". In: Nicholas Tsagourias and Russell Buchan and Russell Buchan (eds.), Research. Handbook on International Law and Cyberspace, (Edward Elgar Publishing 2015). p. 170.

(2) **Geoffrey B. Demarest**, Espionage in International law, Journal of International Law and Policy. Vol. 24, 1996. pp. 321-326.

الشبكات، أو أجهزة الكمبيوتر. كما يمكن أن يتم من خلال القرصنة أو البرمجيات الخبيثة مثل أحصنة طروادة وبرامج التجسس(١).

ووفقًا لتوجيهات السياسة الرئاسية الأمريكية المعنونة " سياسة الولايات المتحدة للعمليات الإلكترونية" تم تعريف التجسس الإلكتروني على أنه العمليات أو البرامج أو الأنشطة ذات الصلة التي أجريت في الفضاء الإلكتروني، أو من خلاله، لغرض أساسي هو جمع المعلومات الاستخبارية من أجهزة الكمبيوتر، أو نظم المعلومات، أو الاتصالات، أو الشبكات والتي تهدف إلي البقاء والاستمرار دون أن يتم أكتشافها(٢).

وقد ذهب رأي إلي أن التجسس الإلكتروني: « هو استخدام القدرات السيبرانية لإجراء عمليات رصد، أو مراقبة، أو التقاط، أو تسريب الاتصالات الإلكترونية، أو المخزنة، أو البيانات المخزنة، أو معلومات أخري»(٣). في حين ذهب رأي ثانٍ إلي أنه: « الاستخدام المقصود لأجهزة الكمبيوتر، أو أنشطة الاتصالات الرقمية وصولًا إلى معلومات حساسة عن الخصم أو المنافس؛ بغرض الحصول على ميزة أو بيع هذه المعلومات نظير الحصول على مكافأة مالية»(٤).

---

(1) **Fahad Ullah Khan**, States rather than criminals pose a greater threat to global cyber security: a critical analysis, the Institute of Strategic Studies Islamabad (ISSI). Volume XXXI, no 3. Autumm 2011. p. 93. Available at: http://issi.org.pk/wp-content/uploads/2014/06/1328592265_43276030.pdf

(2) U S Presidential Policy Directive, " U.S. Cyber Operation Policy" (October 2012) URl: http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf. Accessed 7 october 2014. **similarly**, Lin defines cyber espionage as " the use of action and opperation - perhaps over an extended period of time - to obtain information that would otherwise be kept confidential and is risident on or transmitting through an adversary's computers systems or networks; **Herbert S. Lin**, Offensive Cyber. Operations and the Use of Force, Journal of National Security Law & Policy, Vol. 4, 2010. p. 63

(3) **Michael N. Schmitt & Liis Vihul**, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017. note 13, Rule 32, p. 168.

(4) **David Weissbrodt**, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minnesota Journal of International Law, Vol. 22, Issue. 2, Summer 2013. p. 370.

نستخلص مما سبق أن التجسس الالكتروني يمكن أن يكون شكلًا من أشكال الإرهاب الإلكتروني، إذا اعتمد على استخدام التكنولوجيا بشكل سلبي من أجل إحداث آثارًا مدمرة وأضرارًا بالغة وكبيرة لمحطات التحكم وأجهزة الكمبيوتر وشبكات الاتصال(١). فمن الممكن استخدام التجسس السيبراني للاستطلاع واستكشاف النقاط شديدة الضعف في البنية التحتية لأنظمة الكمبيوتر، ومن ثم تصميم برامج تستغل هذه الثغرات؛ لتنفيذ هجمات الإرهاب السيبراني في المستقبل(٢).

فالتجسس الإلكتروني ينطوي على الوصول إلى أنظمة الكمبيوتر المستهدفة سرًا من أجل جمع المعلومات الحساسة عنها، وهو ما يتم عادة عبر تقنية التخفي Stealth Technology ، كما يمكن أيضا أن يتم من خلال اشخاص داخل المؤسسة يقومون خلسة بتثبيت كود التجسس الإلكتروني داخل نظم الكمبيوتر المحمية(٣). من ثم يتم جمع المعلومات الضرورية لمساعدة المجموعة الإرهابية على

---

(1) Near this concerned. ***Irving Lachow***, Cyber Terrorism: Menace or Myth? …, Op. cit. p. 439.

(2) ***See. Clay Wilson***, Cyber Threats …, Op. cit., p. 129.

وفي ذات المعني يقول CHUIPKA أن: « التجسس الإلكتروني لا يشكل تهديدًا ماديا بشكل مباشر، إلا أن المعلومات التي يتم جمعها من خلال الفضاء السيبراني قد يكون من نتائجها تنفيذ عمليات مستقبلية قد تكون عنيفة». انظر:

Adam Chuipka, The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorist? Major Research Paper: Graduate School of Public International Affairs University of Ottawa, Ottawa, Ontario, November 2016, p. 10. Available at:
https://ruor.uottawa.ca/bitstream/10393/35695/1/CHUIPKA%2c%20Adam%2020169.pdf

(٣) كما يمكن للقراصنة أيضا الوصول عبر استخدام طرق الهندسة الاجتماعية social engineering methods مثل التصيد الإلكتروني– أي استهداف مستخدم معين يتمتع بإمتيازات الوصول داخل مؤسسة معينة – وتحميل برنامج ضار معين يتم إدخاله في نظام الكمبيوتر المستهدف، وهو أمر ممكن بسبب وجود ثغرة أمنية. (وهو ما يذكرنا بحادث الهجوم على مصنع الصلب الألماني ٢٠١٤، والذي استخدم فيه تقنية التصيد الإلكتروني للوصول إلى شبكة المصنع، ثم التسلل لشبكة التحكم الصناعي والتحكم في أفران الغاز).

تحديد نقاط الضعف داخل النظام المستهدف[١]. وبالتالي قد تبين المعلومات التي تم جمعها من خلال شفرة التجسس تكوين شبكة البنية التحتية للمعلومات الحرجة Critical information infrastructure [٢]، أو تحديد طرازات المعدات الضرورية لمرافق البنية التحتية الحرجة الهامة في العملية، أو نسخ محتويات ملف يحتوي على كلمات مرور صالحة لمستخدم[٣].

وعليه قد يستخدم الإرهابيون المعلومات التي تم جمعها لزيادة فعالية هجوم مستقبلي. فبمجرد التثبيت، قد يرسل الرمز الخبيث معلومات حساسة إلي نقطة تجميع مركزية عن بعد. في وقت لاحق، قد يتم إرسال أمر لإصدار تعليمات برمجية

FBI, Spear Phishing – Angling to Steal Your Financial Info (Apr 1, 2009), At: https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109.

ولمزيد من التفاصيل حول تقنيات التجسس الإلكتروني، راجع:

Ido Kilovaty, World Wide Web of Exploitations – The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach, Columbia Science and Technology Law Review, Vol. 18, 2016. pp. 50-51.

(1) ***Clay Wilson***, Cyber Threats …, Op. cit., p. 129.

(٢) يشير مصطلح البنية التحتية للمعلومات الحرجة إلى الأصول التي تدعم الوظائف العادية للمجتمع الحديث والاقتصاد،وتشمل هذه الخدمات الأساسية، والمرافق الأساسية مثل: شبكة الطاقة الكهربائية، والاتصالات السلكية واللاسلكية، والنقل، والنظم المالية وغيرها من الخدمات الأساسية. كما تشمل أيضًا أنظمة التحكم المحوسبة التي تساعد على تشغيل وتنظيم هذه الخدمات، والتي لها أسماء شائعة ومختلفة، منها: أنظمة التحكم الموزعة، وأجهزة التحكم المنطقية القابلة للبرمجة ، وواجهات الآلة البشرية . ولعل الأكثر استخدامًا لمعدات منشأة البنية التحتية للمعلومات الحرجة هي أنظمة التحكم الصناعية (ICS)، وأنظمة المراقبة الإشرافية وحيازة البيانات (SCADA). تعمل أدوات التحكم في الكمبيوتر هذه على إجراء تعديلات مستمرة ودقيقة على تشغيل العمليات الصناعية، وعادةً ما يتم بناء آلات ومعدات الماكينة بقوة بما يكفي للسنوات طويلة قبل الحاجة إلى الصيانة أو الاستبدال.

Ibid. p. 124.

ولمزيد من التفاصيل حول أجهزة التحكم الموجودة في منشأت البنية التحتية الحرجة، راجع:

Panayotis A. Yannakogeorgos, Rethinking the threat of cyberterrorism. In: Thomas M. Chen, Lee Jarvis and Stuart Macdonald (eds.), Cyberterrorism: Understanding, Assessment, and Response. Springer, New York, 2014. pp. 43-62.

(3) **Clay Wilson**, Cyber Threats …, op.cit., p. 129.

ضارة لبدء الهجوم الإرهابي على الإنترنت. وقد تعطي التفاصيل التي تم جمعها بواسطة الشفرة الخبيثة القدرة على إغلاق صمامات التحكم المحددة في مرفق أساسي من مرافق البنية التحتية، أو يكون من نتائجها إصدار تعليمات غير صحيحة قد تؤدي في النهاية إلي تدمير معدات محددة في موقع حساس[١]، مثل الذي أحدثته شفرة ستاكسينت الخبيثة **Stuxent malware** في محطة ناتانز الإيرانية النووية[٢].

---

(1) **Ibid.** p. 129.

(2) ***Tom Simonite***, Stuxnet tricks copied by computer criminals. MIT Technology Review, 2012. https://www.technologyreview.com/s/429173/stuxnet-tricks-copied-by-computer-criminals/. [Accessed 19 Sep 2012].

وقد كان نطاق عمل دودة ستاكسينت مقصور على مرفق ناتانز للطاقة النووية بإيران حيث كانت تتم هناك عملية تخصيب اليورانيوم في مخابئ تحت الأرض، وقد ذهبت دودة ستاكسينت إلى أبعد من ايقاف وتعطيل عمليات التخصيب وذلك بعد اصابة انظمة التحكم الصناعية الخاصة بأجهزة الطرد المركزي التي صنعتها شركة سيمنز، حيث أرسلت تعليمات من شأنها إلحاق الضرر بهذه الأجهزة والتي تعمل على فصل اليورانيوم المخصب عن اليورانيوم الطبيعي، كما عرضت الدودة أيضًا معلومات عادية على شاشات الكمبيوتر حتي لا يلاحظ الأشخاص المشغلون للمحطة الهجمات.

David Talbot, Intelligent Machines: New Malware Brings Cyberwar One Step Closer. MIT Technology Review, 2011. https://www.technologyreview.com/s/425832/new-malware-brings-cyberwar-one-step-closer/. [Accessed 20 October 2011].

وتعتبر دودة ستاكسنت أكثر البرمجيات الخبيثة على الاطلاق والتي جاءت نتيجة لجهد أمريكي إسرائيلي مشترك، حيث تم اختبار فعاليتها داخل مفاعل ديمونة النووي بإسرائيل قبل اطلاقها بغرض تقويض جهود أيران في صنع القنبلة النووية، حيث قضت هذه الدودة علي نحو خُمس أجهزة الطرد المركزي بمحطة ناناتز وساعدت في تأخير قدرة إيران على صنع أول أسلحة نووية، وإن لم يكن تدميرها.

The New York Times, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, by. William J. Broad, John Markoff and David E. Sanger. Available at: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. [Accessed 15 Jan 2011].

الفصل الثالث

جرائم الإرهاب الإلكتروني في التشريعات المقارنة

تتعامل السياسة الجنائية مع جرائم الإرهاب الإلكتروني بوصفها أحد الجرائم الإلكترونية وذلك بكافة التدابير والإجراءات المستخدمة في مواجهة الظواهر الإجرامية الأخرى بما في ذلك الوقاية والمنع والتجريم والعقاب، واستجابة لمتطلبات التجريم والعقاب دأبت النصوص الجنائية في مختلف البلدان على تكييف الإرهاب الإلكتروني[١]، جرائم معاقب عليها بعقوبات تراعي تحقيق هدفي السياسة الجنائية المتمثلة في الردع والإصلاح.

وسوف نتناول جرائم الإرهاب الإلكتروني من خلال بيان التكييف القانوني للجريمة الإرهابية الإلكترونية، وصورها المختلفة وتحديدًا في التشريع المصري وعقوبتها، وموقف التشريعي المقارنة منها. وذلك في ثلاثة مباحث على النحو التالي:

المبحث الأول: الطبيعة القانونية لجريمة الإرهاب الإلكتروني.

المبحث الثاني: صور جريمة الإرهابية الإلكترونية.

المبحث الثالث: الموقف التشريعي من جريمة الإرهاب الإلكتروني.

المبحث الأول

الطبيعة القانونية لجريمة الإرهاب الإلكتروني

---

[١] تارة بأنه جريمة وطنية، وتارة أخري بأنه جريمة دولية.

يتنازع الفقه الجنائي والدولي بخصوص التكييف القانوني لجريمة الإرهاب الإلكتروني ثلاثة أوصاف قانونية: الأول، يعبر عن وجهة نظر المشرع الوطني إذ يري الإرهاب جريمة جنائية قائمة بذاتها. والثاني، يعبر عن وجهة نظر المجتمع الدولي والذي يعتبر الإرهاب الإلكتروني جريمة دولية. والثالث، يعبر عن قرار سياسي داخل المجتمع الدولي يعتبر الإرهاب الإلكتروني نزاعا مسلحا يتعين مواجهته بالردع. ويخضع الوصف الأول للإرهاب الإلكتروني للشرعية الدستورية التي تحكم القانون الوطني بخلاف الوصفين الثاني والثالث فيخضعان للشرعية الدولية المتمثلة في أحكام القانون الدولي[١].

وعليه سوف نستعرض الأوصاف القانونية للإرهاب الإلكتروني في مطلبين على النحو التالي

المطلب الأول: الإرهاب الإكتروني جريمة وطنية.

المطلب الثاني: الإرهاب الإلكتروني جريمة دولية.

المطلب الأول
الإرهاب الإلكتروني جريمة وطنية

ينظر المشرع الوطني إلي الإرهاب الإلكتروني كجريمة جنائية تتوافر فيها أبعاد مختلفة من جرائم عادية مثل القتل والسرقة والإتلاف والتدمير والتزوير[٢]، بالإضافة إلي بعد خاص يميزها عن الجرائم العادية وهي أنها تقع في بيئة الإنترنت ضد أجهزة الكمبيوتر والشبكات المعلوماتية المخزنة فيها بهدف إرهاب الحكومة أو

---

[١] انظر: أسراء طارق جواد كاظم، جريمة الإرهاب الإلكتروني– دراسة مقارنة، رسالة ماجستير، كلية الحقوق – جامعة النهرين، العراق، ٢٠١٢، ص ٦٢.

[٢] د/ أحمد فتحي سرور، المواجهة القانونية للإرهاب، مركز الأهرام للترجمة والنشر– مؤسسة الأهرام، الطبعة الثانية، ٢٠٠٨، رقم ٣٩ ص ٧٧.

لتحقيق أهداف سياسية أو اجتماعية. وعلى هذا الأساس تتميز جريمة الإرهاب الإلكتروني عن الجريمة العادية في استغلالها الموارد المعلوماتية لإحداث أضرارًا بالبني التحتية لنظم المعلومات والشبكات لأغراض التخويف أو الإرغام لأهداف سياسية[١].

ويتطلب التكييف القانوني لجريمة الإرهاب الإلكتروني تعريفا قانونيا للجريمة يحدد أركانها، يتبناه المشرع وفقا لمبدأ شرعية الجرائم والعقوبات مع الالتزام بمبادئ الضرورة والتناسب عند التجريم والعقاب للأفعال التي يتضمنها هذا التعريف، وهو ما فعله المشرع المصري في القرار بقانون رقم ٩٤ لسنة ٢٠١٥ الخاص بمكافحة الإرهاب الذي عرف الإرهاب محددًا الأفعال التي تعد من قبيل الإرهاب الإلكتروني.

وتتميز جريمة الإرهاب الإلكتروني بذاتية خاصة من الناحية القانونية نظرًا لخطورتها، وهو ما ينعكس بوجه خاص في تجريم مجرد الأعمال التي ينبعث منها خطر معين ولو لم يترتب عليها ضرر فعلى. مثال ذلك إنشاء المواقع الإلكترونية أو استخدامها في الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب الأعمال الإرهابية حتي ولو لم تجد قبولا عند متلقيها أو رفضًا (المادة ١/٢٩).

وقد اعتبرت الفقرة الثانية من المادة ٢٩ من القانون سالف الذكر الدخول بغير حق أو بطريقة غير مشروعة موقعًا إلكترونيًا حكوميًا بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغير محتواها أو إتلافها أو تزوير محتواها الموجود بها ظرفًا مشددًا طالما كان ذلك بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولي من هذه المادة أو الإعداد لها.

---

[١] انظر: د/ محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، ٢٠١٢، ص ١٣؛ د/ عادل محمد علي مصطفي، المرجع السابق، ص ٧٤.

وإزاء خطورة الإرهاب الإلكتروني ثار التساؤل الآتي: **هل يعد الإرهاب الإلكتروني جريمة جنائية في حد ذاته أم مجرد ظرف مشدد بالنظر إلي أدواته أو أهدافه أو ضحاياه؟**

لا شك أن العامل الإرهابي يتجاوز مجرد كونه ظرفًا مشددا في جريمة عادية إذ يندمج في جريمة الإرهاب الإلكتروني حتي يصبح مكونًا طبيعيًا في الجريمة كاشفا لخطورتها وخطورة مرتكبيها. وأمام خطورة هذه الجريمة يخضع الإرهاب الإلكتروني لنظام إجرائي متميز يراعي فيه مدي جسامة هذه الجريمة ومختلف أبعادها، ومنها البعد الدولي إذا ما تجاوزت حدود دولة معينة، وليست الإقليمية حاسما في تحديد الاختصاص القضائي بل ينظر عند تجاوز أعمال الإرهاب لإقليم الدولة إلي جنسية كل من الجناة والضحايا وإلي عبور أدواته ووسائله للأوطان وإلي تنظيماته التي قد تصل إلي حد تكوين الخلايا المنظمة في بعض الدول[١].

المطلب الثاني
الإرهاب الإلكتروني جريمة دولية

يعد الإرهاب الإلكتروني من الجرائم الدولية إذا كانت مخالفة للقواعد الدولية التي تترتب عليها المسئولية الجنائية الشخصية، سواء تلك التي نصت عليها الاتفاقيات الدولية، أو تضمنتها القواعد الدولية العرفية Customary rules[٢].

ولكي يصنف الإرهاب الإلكتروني ضمن طائفة الجرائم الدولية يجب توافر عدة عناصر: أولها، ألا يقتصر على حدود دولة معينة وإنما يتجاوز حدود الدولة الوطنية، سواء فيما يتعلق بالمتهمين أو بالوسائل المستخدمة أو بنوع العنف المستخدم[٣]. وثانيها، أن تتعلق الجريمة بالمجتمع الدولي بأسره ومصالحه وذلك على

---

[١] أسراء طارق جواد كاظم، المرجع السابق، ص ٦٣.

[٢] د/ أحمد فتحي سرور، المرجع السابق، رقم ٤٣ ص ٨٤.

[٣] انظر: أسراء طارق جواد كاظم ، المرجع السابق، ص ٦٤.

نحو يمكن عده تهديدًا لأمن هذا المجتمع[١]. وثالثها، يتعلق بحدود أعمال الإرهاب إذ يشترط أن تبلغ حدًا كبيرًا من الجسامة يصاحبه فقد كثير من الأرواح أو وقوع أضرار بالبني التحتية الكونية للمعلومات التي تستحق الحماية الدولية[٢].

وإذا كان استيفاء هذه العناصر لازما لعد الإرهاب تهديدًا للأمن الدولي فقد استتبع ذلك- في الوقت نفسه- اعتباره جريمة دولية بوصفه ماسا بالمصالح التي تهم المجتمع الدولي. ويتنازع الإرهاب – بصفته جريمة دولية- ثلاثة أنواع من الأوصاف القانونية وفقا للقانون الدولي: الأول، بصفته مجرد جريمة دولية. والثاني، بصفته مجرد جريمة المصالح الدولية. والثالث، بوصفه جريمة حرب[٣].

والوصف الأول لا يتوافر إلا إذا وقعت الجريمة في وقت السلم وتوافرت فيها عناصر الجريمة الدولية كما بينا آنفا. والأصل أن الدول من خلال من يشغلون وظائف المسئولية فيها هم الذين يرتكبون الجرائم الدولية إلا أن ذلك لا يستبعد ارتكاب الجرائم ضد الإنسانية أو المصالح الدولية بواسطة جماعات من الأفراد لا تعد من أجهزة الدولة وهو ما يثير وقوع إمكان وقوع الأعمال الإرهابية بواسطة هذه الجماعات[٤].

---

[١] لذا وصفه البعض بأنه أصبح عدو الدولة الوطنية والمجتمع الدولي معًا، بل هو عدوً أكثر ضراوة؛ لأنه لا يقبل أي حل تفاوضي ولا يبغي سوي النصر مهما كان الثمن غاليًا في الدمار الذي يحققه.

Uves Jeanclos, Terrorisme et securité international: collection Études stratégiques internationales, Bruylant, 2004, pp. 13-45.

[٢] د/ أحمد فتحي سرور، المرجع السابق، رقم ٤٣ ص ٨٣.

[٣] د/ عبد العزيز مخيمر عبد الهادي، الإرهاب الدولي مع دراسة في الاتفاقيات الدولية والقرارات الصادرة عن المنظمات الدولية، دار النهضة العربية، ١٩٨٦، ص ٢٣،٤٥.

[٤] د/ ثامر إبراهيم، مفهوم الإرهاب في القانون الدولي، دار حوران للطباعة، دمشق، ١٩٩٨، ص ٥٥.

أما الإرهاب بوصفه جريمة حرب فإنه يقع أثناء النزاع المسلح متي استخدمت الوسائل الإرهابية لنشر الرعب بين السكان المدنيين وفي هذه الحالة يعد الإرهاب جريمة حرب لمخالفة القانون الدولي الإنساني فإذا بلغت الأعمال الإرهابية حدًا كبيرًا من الجسامة تعد أيضا جريمة ضد الإنسانية[١].

المبحث الثاني
صور الجريمة الإرهابية الإلكترونية

تمثل كل من جريمة إنشاء المواقع الإلكترونية أو استخدامها من أجل الترويج الإرهابي، وجريمة الدخول بغير حق لموقع إلكتروني تابع لأي جهة حكومية للحصول على البيانات أو المعلومات الموجودة عليها بغرض الترويج الإرهابي أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية والمنتمين إليها في الداخل والخارج أبرز جرائم الإرهاب الإلكتروني في القانون المصري. وسوف نتناولهما في مطلبين على النحو التالي:

المطلب الأول: إنشاء المواقع الإلكترونية أو استخدامها للترويج الإرهابي.

المطلب الثاني: الدخول بغير حق لموقع إلكتروني حكومي.

المطلب الأول
جريمة إنشاء المواقع الإلكترونية أو استخدامها للترويج الإرهابي

أولًا: النص القانوني:

نصت المادة ٢٩ من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥ على أنه : « يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين كل من أنشأ أو استخدم موقعًا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما

---

[١] د/ أحمد فتحي سرور، المرجع السابق، رقم ٤٧ ص ٩٣.

يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة فى شأن أى جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية فى الداخل والخارج.

ثانيًا: أركان الجريمة:

يجب لقيام جريمة إنشاء المواقع الإلكترونية أو استخدامها للترويج الإرهابي توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

يتكون الركن المادي بصفة عامة من ثلاثة عناصر: الأول، السلوك الإجرامي والذي يعد بمثابة نشاط إنساني إرادي في المحيط الخارجي يتم التعبير عنه بحركة من الجسم أو مجرد السكون. والثاني، يعرف بالنتيجة الإجرامية ويقصد بها الأثر المادي الخارجي الناجم عن السلوك الإجرامي والذي يعتد به المشرع في التكوين القانوني للجريمة[١]. والثالث، علاقة السببية والتي يعني بها ذلك الرباط الذي يربط سلوك الجاني بالنتيجة الإجرامية التي يسأل عنها. وهذا العنصر لا وجود له في الجرائم التي لا تشكل النتيجة فيها أحد عناصر الركن المادي، بينما تعد عنصرًا ضروريًا من عناصر الركن المادي بالنسبة للجرائم ذات النتيجة[٢].

---

[١] د/ محمود نجيب حسني، علاقة السببية في قانون العقوبات، دار النهضة العربية، ١٩٨٣، ص ٤٨.

ومن المتصور توافر الركن المادي للجريمة دون توافر النتيجة الإجرامية؛ لأن النتيجة الإجرامية ليست عنصرًا ضروريًا في الركن المادي كما هو الحال في جرائم الخطر والجرائم السلبية وجرائم الشروع.

[٢] د/ محمد محيي الدين عوض، مبادي القانون الجنائي، القسم العام، ١٩٨١، ص ١٧٦.

والسلوك الإجرامي في الجريمة التي نصت عليها المادة ٢٩ من قانون مكافحة الإرهاب يتوافر من عنصرين: أولهما، إنشاء موقع أو استخدامه على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها. وثانيهما، يتعين أن يكون إنشاء الموقع الإلكتروني أو استخدامه من أجل تحقيق أحد ثلاثة أغراض[١]:

(الأول) الترويج للأفكار أو المعتقدات الداعية إلي ارتكاب أعمال إرهابية[٢]، ولم يشترط المشرع شكلا معينًا يتم فيه الترويج، فمن الممكن أن يكون بالكتابة أو برسم صورة تعبيرية أو أيًا من صور التواصل التي تخترق الحظر الذي فرضه المشرع لمواجهة هذه الطائفة من الجرائم والتي تدعو إلي ارتكاب أعمال إرهابية[٣]. وبالنسبة لهذا الغرض فإنه قد يتعدي مجرد الترويج المذكور إلي التحريض العام على إرتكاب جريمة إرهابية إذا كان من شأنه بث فكرة الجريمة العمدية.

(الثاني) بث ما يهدف إلي تضليل السلطات الأمنية أو التأثير على سير العدالة في شأن جريمة إرهابية. على سبيل المثال دس معلومات كاذبة موجهة تستهدف عمل السلطات الأمنية من أجل تشتيتها وإرباكها لعدم الوصول إلي هوية الجناة الأمر الذي من شأنه أن يحدث تأثير على سير العدالة [٤].

---

[١] د/ أحمد فتحي سرور، الوسيط في قانون العقوبات القسم الخاص "الكتاب الأول"، نادي القضاة ٢٠١٦، رقم ١٥١ ص ٢٠٢.

[٢] حتي لو لم يترتب على هذا الترويج وقوع أعمال إرهابية؛ وذلك لأن مناط التجريم هو الترويج للأفكار أو المعتقدات الإرهابية.

[٣] د/ عادل محمد علي مصطفي، المرجع السابق، ص ٧٧.

[٤] د/ كمال أحمد، الوسيط في شرح قانون مكافحة الإرهاب، دار النهضة العربية، ٢٠١٧، ص ٥١٣.

(الثالث) تبادل الرسائل وإصدار التكليفات بين الجماعة الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل أو الخارج.

ويتعين أن ينطوي السلوك الإجرامي في حد ذاته على التعبير عن أحد الأغراض الثلاثة.

وتتمثل النتيجة الإجرامية فيما يترتب على هذا السلوك الإرجرامي من خطر يهدد المصلحة المحمية من وراء تجريم العمل الإرهابي[١].

ب- الركن المعنوي:

هذه الجريمة عمدية، يقتضي المشرع لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، هذا بالاضافة إلي توافر القصد الخاص الذي يعبر عنه الفقة[٢] بالنية الإرهابية، مادام غرض الجناية قد اتصف بالطابع الإرهابي ألا وهو الترويج للأفكار والمعتقدات الداعية إلي ارتكاب أعمال إرهابية أو تضليل السلطات الأمنية أو التأثير في سير العدالة في جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية والمنتمين لها في الداخل والخارج.

ثالثًا: العقوبة:

جعل المشرع المصري عقوبة السجن مدة لا تقل عن خمس سنوات، جزاءً لكل من أنشأ أو استخدم موقع على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، وذلك متي كان غرض الجاني من فعله تحقيق الأغراض الإرهابية المنصوص عليها في المادة (١/٢٩).

---

[١] د/ أحمد فتحي سرور، المرجع السابق، رقم ١٥١ ص ٢٠٣.

[٢] المرجع السابق، رقم ١٥٢ ص ٢٠٣.

المطلب الثاني

الدخول بغير حق لموقع إلكتروني حكومي

أولًا: النص القانوني:

نصت الفقرة الثانية من المادة ٢٩ من قانون مكافحة الإرهاب المصري رقم ٩٤ لسنة ٢٠١٥ على أنه : « يعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من دخل بغير حق أو بطريقة غير مشروعة موقعًا الكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولي من هذه المادة أو الاعداد لها».

ثانيًا: أركان الجريمة:

يجب لقيام جريمة الدخول بغير حق لموقع إلكتروني حكومي توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

يتوافر السلوك الإجرامي في الجريمة التي نصت عليها المادة ٢/٢٩ من قانون مكافحة الإرهاب من عنصرين:

أولهما، الدخول بغير حق[١] أو بطريقة غير مشروعة[١] إلي موقع إلكتروني تابع لأية جهة حكومية، وهو فعل غير مشروع في حد ذاته.

---

[١] يقصد به دخول شخص ليس لديه صلاحية للدخول هذه المواقع حتي ولو كان هذا الشخص موظفا في نفس الجهة التي يتبع لها الموقع الإلكتروني، وذلك بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها.

وثانيهما، أن يكون هذا الدخول بقصد الحصول على البيانات أو المعلومات الموجودة بالموقع، من أجل ارتكاب جريمة الترويج الإرهابي، أو تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن جريمة إرهابية، أو تبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل أو الخارج، أو الاعداد لها.

وتتمثل النتيجة الإجرامية في هذه الجريمة في الخطر المترتب على هذا السلوك الإجرامي، والذي يهدد المصلحة المحمية من وراء تجريم العمل الإرهابي.

الركن المعنوي:

هذه الجريمة عمدية، يقتضي المشرع لقيامها توافر القصد الجنائي العام بعنصريه العلم والإرادة، وبالتالي إذا حدث الدخول بطريق الخطأ لا تقوم الجريمة. هذا بالاضافة إلي توافر القصد الخاص من جريمة الدخول غير المشروع وهو الحصول على البيانات أو المعلومات الموجودة على الموقع أو الاطلاع عليها أو

ووفقا لنظام تقسيم الصلاحيات على مستخدمي المواقع الإلكترونية فإنه لا يجوز لأي موظف تجاوز الصلاحيات الممنوحة له، ففي بعض الجهات الحكومية يكون لكل موظف صلاحيات محدودة في الدخول والعمل في هذه المواقع وفقا لتخصصه ودرجته الوظيفية، فيمنح المديرين صلاحيات واسعة تتمثل في الإضافة والتعديل والحذف وهي أعلي الصلاحيات في سلم النظام الأمني لاستخدام المواقع الإلكترونية، ويأتي في أدني هذا السلم صلاحية إدخال البيانات فقط دون السماح بالتمتع بصلاحية التغيير أو الحذف، وبالتالى فان دخول الموظف في هذه الحالة يكون دخول بغير حق.

(١) يقصد به النفاذ المتعمد وغير المشروع لأجهزة وأنظمة الحاسب أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح.

تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها وذلك من أجل ارتكاب الجريمة الإرهابية[١].

ثالثًا: العقوبة:

شدد المشرع المصري عقوبة الدخول بغير حق أو بطريقة غير مشروعة موقعًا الكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها طالما كان ذلك بغرض ارتكاب جريمة من الجرائم التي تناولتها (المادة ١/٢٩) أو الإعداد لها حيث جعل العقوبة السجن المشدد مدة لا تقل عن عشر سنوات.

المبحث الثالث

الموقف التشريعي من الجريمة الإرهابية الإلكترونية

ونظرًا لحيوية الدور الذي تضطلع به التكنولوجيا المعلوماتية في المجتمعات الحديثة، الاعتماد عليها في إدارة البنية التحتية الحيوية والمرافق الاستراتيجية لهذه المجتمعات، أصبحت هذه التكنولوجيا محلًا للهجمات الإرهابية ولاسيما الجرائم الواقعة ضد الأنظمة المعلوماتية والشبكات والحاسبات الآلية[٢]. إلا أن التشريعات المقارنة في الدول المختلفة لم تتفق علي آلية التعامل مع هذا النوع من الجرائم، فبعض هذه التشريعات تعاملت معها بالقوانين الجنائية التقليدية، وهناك دول أخري

---

[١] وهي الترويج الإرهابي، أو تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن جريمة إرهابية، أو تبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل أو الخارج، أو الاعداد لها.

[2] **Enver Bucaj,** The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law, Acta Universitatis Danubius. Juridica, Vol. 13, No. 1, 2017.

تلاحقها بقوانين مكافحة جرائم التقنية، والبعض الأخر تعامل معها بموجب القوانين الجنائية المتعلقة بمكافحة الإرهاب.

وعليه سوف نتناول موقف التشريعات الأجنبية والعربية من جريمة الإرهاب الإلكتروني في مطلبين علي النحو التالي:

المطلب الأول: الموقف التشريعي للدول الغربية من جريمة الإرهاب الإلكتروني.

المطلب الثاني: الموقف التشريعي للدول العربية من جريمة الإرهاب الإلكتروني.

المطلب الأول
الموقف التشريعي للدول الأجنبية من جريمة الإرهاب الإلكتروني

لم تصدر الدول الأجنبية قوانين خاصة بمكافحة الإرهاب الإلكتروني، وإنما تعاملت معها باعتبارها واحدة من الجرائم الإلكترونية، عن طريق إصدار قوانين مستقلة لمكافحة جرائم الحاسب الآلي والإنترنت[١]، ومن بينها جرائم الاختراق غير المشروع للنظام المعلوماتي أو إتلاف النظم المعلوماتية، ومثال ذلك قوانين إساءة استخدام الحاسب الآلي في كل من بريطانيا، والولايات المتحدة الأمريكية. وأما عن طريق تجريم هذه الأفعال غير المشروعة في قوانينها التقليدية عبر تحديث هذه القوانين بحيث تستوعب هذا النوع من الجرائم المستحدثة. ومن هذه الدول فرنسا[٢].

---

[١] ويمثل هذا الإتجاه كل من الولايات المتحدة الأمريكية، المملكة المتحدة، السويد، البرتغال، فنزويلا، هولندا، المجر، بولندا، جمهورية كسوفو، كندا، وإستراليا.

[٢] ويمثل هذا الإتجاه كل من مالطا، اليونان، إيطاليا، بلجيكا، ألمانيا، الدنمارك، النرويج، نيوزلندا، سويسرا، والبوسنة والهرسك.

وعليه سوف نتناول الموقف التشريعي لكل من فرنسا، والمملكة المتحدة، والولايات المتحدة الأمريكية في التعامل الإرهاب الإلكتروني في ثلاثة أفرع علي النحو التالي:

الفرع الأول
التشريع الفرنسي

أسبغ المشرع الفرنسي حمايته للمواقع الإلكترونية والأنظمة المعلوماتية ومحتوياتها، وذلك بمواجهة الاعتداءات علي مواقع شبكة الإنترنت وصفحاتها من خلال تجريم الدخول والبقاء غير المشروع للمواقع الإلكترونية أو تدميرها[١]. إذ حظرت المادة ٣٢٣-١ من قانون العقوبات الفرنسي المعدلة بالقانون ٩١٢-٢٠١٥ الصادر في ٢٤ يوليه ٢٠١٥ الدخول والبقاء غير المشروع علي المواقع والنظم الإلكترونية بقولها: يعاقب علي الدخول أو البقاء – بطريق الغش- داخل كل أو جزء من نظام المعالجة الآلية للبيانات بالحبس لمدة سنتين وغرامة قدرها ٦٠ ألف يورو. وإذا نجم عن هذا الدخول محو أو تعديل في البيانات المختزنة في النظام او إتلاف تشغيل هذا النظام، تكون العقوبة الحبس لمدة ثلاثة سنوات وغرامة قدرها ١٠٠ ألف يورو.

وفي الحالات التي ترتكب فيها الجرائم المنصوص عليها في الفقرتين السابقتين ضد نظام المعالجة الآلية للبيانات الشخصية التي تنفذها الدولة، تزاد العقوبة إلى الحبس لمده خمس سنوات وغرامه قدرها ١٥٠ ألف يورو[٢].

---

(١) انظر: د/ راشد محمد المري، الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية، ٢٠١٨، ص ٧٥ وما بعدها.

(2) **Art. 323-1 Modifié par LOI n° 2015-912 du 24 juillet 2015- art. 4:** « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

أما بالنسبة لجريمة إتلاف المواقع الإلكترونية فقد عاقبت المادة ٣٢٣-٢ عقوبات فرنسي كل من قام بإعاقة أو إفساد نظام المعالجة الآلية للبيانات بالحبس خمس سنوات وغرامة قدرها ١٥٠ ألف يورو. وعندما ترتكب هذه الجريمة ضد نظام للمعالجة الآلية للبيانات الشخصية التي تنفذها الدولة، تزاد العقوبة إلى الحبس لمدة سبع سنوات وغرامه قدرها ٣٠٠ ألف يورو[١].

في حين عاقبت المادة ٣٢٣-٣ عقوبات فرنسي علي إدخال البيانات بطريق الغش في نظام المعالجة الآلية، أو استخراجها أو إحتوائها أو نسخها أو محوها أو تعديلها بالاحتيال أو إفساد نظام المعالجة الآلية للبيانات بالحبس خمس سنوات وغرامة قدرها ١٥٠ ألف يورو. وعندما ترتكب هذه الجريمة ضد نظام للمعالجة الآلية للبيانات الشخصية التي تنفذها الدولة، تزاد العقوبة إلى السجن لمدة سبع سنوات وغرامة قدرها ٣٠٠ ألف يورو[٢].

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

ولمزيد من التفاصل حول دور القانون الجنائي في مواجهة الإرهاب الإلكتروني بفرنسا، راجع:

Romain BOOS, La lutte contre la cybercriminalité au regard de l'action des États. Thèse, Université de Lorraine, 2016. p. 106 et s.

(1) **Art. 323-2 Modifié par LOI n° 2015-912 du 24 juillet 2015- art. 4:** « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

(2) **Art. 323-3 Modifié par LOI n° 2015-912 du 24 juillet 2015- art. 4:** « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

وهكذا جرم المشرع الفرنسي فعل الدخول غير المشروع إلي أنظمة المعالجة الآلية للمعلومات باعتباره بوابة المرور لارتكاب سائر الجرائم الإلكترونية ومنها جرائم الإرهاب الإلكتروني، كما شدد العقوبة علي الجاني إذا ما نشأ عن هذا الدخول محو أو تعديل في البيانات المخزنة في النظام، أو إتلاف تشغيل هذا النظام. كما نص علي ظرفي تشديد بتوافره ترتفع العقوبة عن سابقيها وذلك في حالة الدخول غير المشروع علي نظام المعالجة الآلية للبيانات الشخصية تنفذه الدولة. ويلاحظ أن المشرع الفرنسي لم يقصر التجريم علي الدخول غير المشروع وإنما امتد ليشمل البقاء غير المشروع أيضًا، ليعالج الحالة التي يكون الدخول فيها إلي النظام تم بمحض الصدفة وانتفي القصد الجنائي لدي الجاني ومع ذلك يبقي في النظام وتنصرف إرادته إلي ذلك[١].

كما عاقب علي تعطيل أو إفساد نظام المعالجة الألية للبيانات أو إدخال البيانات أو إلغائها أو تعديلها بطريقة غير مشروعة مشددا العقوبة إذا ما ارتكبت هذه الجريمة ضد نظام للمعالجة الآلية للبيانات الشخصية تنفذها الدولة.

الفرع الثالث
التشريع الأمريكي

أصدر المشرع الأمريكي قانون الاحتيال وإساءة استخدام الحاسبات الآلية (The Computer Fraud and Abuse Act of 1986)، وقد جرمت المادة ١٠٣٠ (أ) (٢،١) من القانون المذكور الدخول المتعمد غير المشروع إلي الحاسبات الآلية التابعة للحكومة الفيدرالية الأمريكية ولم يشترط، هذا القانون حدوث

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.

[١] د/ حسين سعيد الغافري، المرجع السابق، ص ٣٦٥ هامش (١).

ضرر[١]. ويشتمل هذا القانون بحمايته أيضًا الحاسبات الآلية غير العائدة للحكومة الفيدرالية الأمريكية إذا كانت تلك الحاسبات الآلية من ضمن الحاسبات المحمية Protected Computers ويعرف هذا القانون الحاسب الآلي المحمي بأنه: « كل حاسب آلي مخصص لاستعمال مؤسسة مالية، أو حكومة الولايات المتحدة الأمريكية مما يشكل جريمة تؤثر علي استخدام أو حكومة الولايات المتحدة الأمريكية أو أن هذا الحاسب مخصص للاستخدام في التجارة البينية بين الولايات المتحدة الأمريكية أو التجارة أو الاتصالات الدولية»[٢].

وبما أن شبكة الإنترنت يغلب استخدامها لتسهيل التجارة الدولية والتجارة البينية في الولايات المتحدة فإنه يغلب أن يكون أي حاسب آلي سواء كان عامًا أم خاصًا حاسبًا محميًا مادام أنه مرتبط بشبكة الإنترنت وفقا لنصوص هذا القانون[٣].

---

(١) وقد جرمت المادة ١٠٣٠ (a) (١) من القانون ذاته الدخول غير المشروع المتعمد لحاسب آلي غير عام بدون الحصول على تصريح إذا كان استخدام هذا الحاسب محصور بالحكومة الأمريكية أو إذا أثر الدخول غير المصرح به على أي أستخدام حكومي. أنظر:

18 U.S.C ff 1030 (e) (2) (A) –(B).

See Also. Mary M Calkins, They Shoot Trojan Horses, Don't They? An EconomicAnalysis of Anti-Hacking Regulatory Model, Georgetown Law Journal, November, 2000. At 3-5.

في حين جرمت المادة ١٠٣٠- (a) -3 من ذات القانون تعاقب على الدخول المجرد إلى الحاسبات الآلية التي تعمل فقط داخل الحكومة الفيدرالية، أو الحاسبات التي وإن كانت لا تعمل داخل الحكومة الفيدرالية إلا أن الدخول إليها من شأنه التأثير على مصالح الحكومة التي ترتبط بشكل أو بأخر بهذه الحاسبات.

http://www.usdoj.gov/criminal/cybercrime/lyttlePlea.htm

(2) 18 U.S.C ff 1030 (e) (2) (A) –(B).

(3) **See also Michael Lee, et al**., Comments, Electronic Commerce, Hackers, and The. Search for Legitimacy; A Regulator Proposal, 14 Berkley Tech. L.J., 839, 844 (1998).

ولم يشترط، هذا القانون حدوث ضرر لتحقق المسئولية الجنائية، فحتي لو لم يتحقق الضرر بتحقق الجريمة بالدخول غير المشروع إلي الحاسب الآلي إذا تمكن المخترق من الحصول علي معلومات مالية أو ذات علاقة بالديون أو معلومات ذات علاقة بالحكومة الأمريكية أو أي معلومات تحصل عليها من حاسب آلي محمي شريطة أن يتضمن هذا السلوك الاتصالات بين الولايات المتحدة أو الاتصالات الأجنبية(١).

كما جرم هذا القانون الأفعال الأتية للحصول علي معلومات وهي: الدخول المتعمد غير المشروع إلي الحاسب الآلي أو تجاوز القدر المصرح به للدخول للحصول علي التالي:

أ- المعلومات المخزنة في السجلات المالية لمؤسسة مالية.

ب- المعلومات العائدة لإحدي الوزارات أو المصالح الحكومية للولايات المتحدة الأمريكية.

ج- المعلومات المخزنة في حاسب آلي محمي إذا تضمن هذا السلوك اتصالات بينية عبر الولايات أو اتصالات أجنبية(٢).

وقد عاقب هذا القانون علي الشروع في الدخول غير المشروع إلي الحاسب الآلي بذات العقوبة المقررة للجريمة التامة(٣). إلا أنه لم يشترط، حدوث ضرر ناتج

---

(1) I. d. 1030 (a) (2).

(2) I. d. 1030 (a) (2).

(3) ***L. Gainer***, Federal Criminal Code Reform: A Past and Future, 2 Buuff. Crim L. Rev 45, 65 (1998).

وقد نصت بعض التشريعات صراحة على تجريم الشروع في جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، كما هو الحال في البرتغال، وقانون العقوبات الفرنسي (المادة ٣٢٣-٧).

عن الإهمال وهو شيء يصعب تحققه في حالة الشروع في ارتكاب جريمة الاختراق. كما أن جرائم الدخول غير المشروع إلي الحاسب الآلي هي صعبة الاكتشاف عمومًا وتكون في الشروع أكثر صعوبة فيما يتعلق باكتشافها(١).

أما علي مستوي الولايات فنجد أن معظم الولايات تتوافر لديها تشريعات تعتبر الدخول إلي أنظمة الكمبيوتر أو الشبكات بدون ترخيص جريمة وهي ما تعرف بتشريعات القرصنة Hacking(٢)، كذلك فان معظم الولايات تقرر عقوبات مشددة

بالمقابل لم يرد في قانون العقوبات الألماني والنرويجي والبلجيكي أي حكم بشأن الشروع في جريمة الدخول غير المصرح به، في حين نص القسم ٨/٧٤٤ من قانون الجرائم الإلكترونية الأسترالى رقم ١٦١ لسنة ٢٠٠١ على عدم العقاب على الشروع في جريمة الدخول غير المصرح به.

(1) ***See. Steven D. Mitchell & Elizabeth A. Banker***, Private Intrusion Response, II Harv. J.L and Tech 699, 704 – 709 (1998).

كما يتضمن قانون إساءة استخدام الحاسبات الآلية لسنة ١٩٨٦ نصًا يعقد المسئولية المدنية بحق المخترق مما يشكل رادعًا إضافيا إلى جانب العقوبات الجنائية التي يتضمنها هذا القانون في حالة الدخول غير المشروع بطريقة الإهمال. مما يفسح المجال في طلب التعويض من المخترق عن أي ضرر ينتج من جراء هذا الدخول غير المشروع.

(2) See e.g., IND. CODE ANN. § 35-43-2-3. See also A LA. CODE § 13 A-8-102 (1994); ALSKA STAT. § 11. 46. 484; ARK. CODE ANN. § 5-41; CAL. PEAL CODE § 502; COLO. REV. STAT. § 185. 5102; CONN. GEN. STAT. ANN. § 53a-251; DEL. CODE ANN. tit. 11, § 932; FAL. STAT. ch. § 815. 06; GA. CODE ANN. § 16-9-93; IDAHO CODE § 18-2202; 720 ILL. COMP. STAT. 5/16D3, 5/15D7; IOWA CODE § 716A. 2; KAN. STAT. ANN. 21-3755; KY. REV. STAT. ANN. §§ 434.845, 434.850; ME. REV. STAT. tit. 17-A, § 432 ; MD. CODE ANN., CRIMES & PUNISHMENTS § 146 ; MASS. ANN. LAWS ch. 266, § 120F ; MICH. COMP. LAWS ANN. § 752.795 ; MINN. STAT. ANN. § 609.891 ; MO. ANN. STAT. § 569.099; MONT. CODE ANN. § 456311 ; NEB. REV. STAT. §§ 28-1343.01, -1347 ; NEV. REV. STAT. § 205.4765 ; N.H. REV. STAT. ANN. 638.17 ; N.J. STAT. ANN. § 2C. 20-32 ; N.M. STAT. ANN. § 30-45-5 ; N.Y. PENAL LAW §§ 156.05, 06, .10 ; N.C. GEN. STAT. § 14-454 ; OHIO REV. CODE ANN. § 2913.04 ; OKLA. STAT. tit. 21, § 1953; OR. REV. STAT. § 164. 377; 18 PA. CONS. STAT. ANN. § 3933; R.I. GEN. LAWS § 11-52-3; TENN. CODE ANN. § 39-14-602; TEX. PENAL CODE ANN. § 33.02.

علي الدخول غير المشروع بقصد إلحاق الضرر أو تعطيل عمل النظام أو الإضرار بأية صورة بالنظام أو المعطيات[١]، وتعتبر ولاية نيويورك اختراق الكمبيوتر بنية ارتكاب أو محاولة ارتكاب أي جريمة بمثابة جريمة معاقب عليها[٢].

أما بالنسبة لجريمة إتلاف المواقع الإلكترونية فلم يحتوي التشريع الأمريكي علي ما من شأنه تجريم إتلاف البيانات والمعلومات والبرامج بصورة عامة، وإنما اقتصر التجريم علي الإتلاف الذي يترتب عليه إعاقة أنظمة الحاسبات الآلية عن العمل، حيث جاءت الفقرة الثانية من المادة ١٠٣٠ (a) لتنص علي تجريم إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية. كما جرمت الفقرة الخامسة من ذات المادة الإتلاف العمدي غير المصرح به

مشار إليها لدى د/ محمد يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية، ورقة بحثية مقدمة لورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية المنعقدة في مسقط بسلطنة عمان في الفترة ٢-٤ إبريل ٢٠٠٦، ص ٩.

(1) ***See e.g.***, ARK. CODE ANN. § 5-41 – 104. ***See also*** ALA. CODE § 13A-8-102; ARIZ. REV. STAT. § 13-2316; CAL. PENAL CODE § 502; COL. REV. STAT. § 18-55-102; CONN. GEN. STAT. ANN. § 53a-251; DEL. CODE ANN. Tit. 11, §§ 934,935; FAL. STAT. ch. 815.05; GA. CODE ANN. § 16-9-93; HAW. REV. STAT. § 708-892; IOWA CODE § 716A.3 ; IDAHO CODE § 18-2202; 720 ILL. COMP. STAT. 5/16D3, 5/16D4 ; KAN. STAT. ANN. § 21-3755 ; LA. REV. STAT. ANN. § 14:73.2 ; ME. REV. STAT. ANN. Tit. 17-A, § 433; MD. CODE ANN., CRIMES & PUNISHMENTS § 146 ; MICH. COMP. LAWS ANN. §§ 752.795, 797 ; MINN. STAT. ANN. § 609.891 ; MISS. CODE ANN. § 97-45-9 ; NEB. REV. STAT. § 28-1343.01, -1345 ; NEV. REV. STAT. 205.4765 ; N.H. REV. STAT. ANN. § 638:17 ; N.J. STAT. ANN. § 2C: 20-25 ; N.M. STAT. ANN. §§ 30-45-4, 5 ; N.Y. PENAL LAW §§ 156.05, .20, .25, .26, .27 ; N.C. GEN. STAT. §§ 14-454, 455 ; N.D. CENT. CODE § 12.1-06.1-08; OKLA. STAT. tit. 21, §§ 1953, 1958 (1983 & Supp. 2000); OR. REV. STAT. § 164. 377; 18 PA. CONS. STAT ANN. § 3933; R.I. GEN. LAW § 11-52-3; S.C. CODE ANN. § 16-16-20; TENN. CODE ANN. § 39-14-602; UTAH. CODE ANN. § 76-6-703; AV. CODE ANN. § 18.2-152.4; VT. STAT. ANN. Tit. 13. § 4103; WIS. STAT. § 943. 70; WYO. STAT. ANN. § 6-3-502.

مشار إليها لدى د/ محمد يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية ...، المرجع السابق، ص ٩.

(2) See N. Y. PENAL LAW § 156.10.

لمعلومات يحتويها حاسب آلي تابع لحكومة الولايات المتحدة وإداراتها، أو حاسب آلي غير تابع للحكومة إلا أنه يستخدم من قبلها أو لصالحها، أو إعاقة هذا الحاسب عن إدارة المهام المختلفة التي تباشرها الحكومة بواسطته[١].

وفي عام ١٩٩٦ صدر قانون حماية بنية المعلومات القومية The NII Protection Act وبصدوره عدلت المادة السابقة حيث تم التوسيع من نطاق حماية أنظمة الكمبيوتر، حيث لم تعد الحماية قاصرة علي الحاسبات التابعة للحكومة وإداراتها، وإنما اتسعت الحماية لتشمل جميع الحاسبات التي تستخدمها المؤسسات الاقتصادية التابعة لحكومة الولايات المتحدة الأمريكية، كذلك تلك التي تستخدم في التجارة والاتصالات بين الولايات الأمريكية فيما بينها أو بين الولايات الأمريكية والدول الأخري، كما امتد النص ليشمل أعمال الإتلاف التي تقع من أشخاص مصرح لهم بالدخول إلي النظام متي تم ذلك عمدًا[٢].

الفرع الثالث

التشريع الإنجليزي

أصدر المشرع الإنجليزي قانون إساءة استخدام الحاسب الآلي لسنة ١٩٩٠ (Computer Misuse Act of 1990)، ويهدف هذا القانون إلي تجريم الدخول غير المشروع علي النظم المعلوماتية.

وقد نص هذا القانون علي أن الشخص يعتبر مذنبًا بجريمة الدخول غير المشروع إلي النظام المعلوماتي إذا انطبق عليه ما يلي:

١- تسبب بجعل حاسب آلي يؤدي وظيفة معينة بنية الدخول إلي برنامج أو بيانات مخزنة في أي حاسب آلي.

---

[١] د/ حسين سعيد الغافري، المرجع السابق، ص ٤٢٥.

[2] ***Heymann Stephen***, Legislating Computer Crime, H.J.L, 1997, Vol. 34.

٢- وكان الدخول قد تم بشكل غير مشروع.
٣- ويعلم عند قيامه بجعل الحاسب الآلي يقوم بهذه الوظيفة أنه يقوم بذلك بشكل غير مشروع.

ولم يشترط المشرع الإنجليزي وجود نية إحداث هذا الدخول بخصوص برنامج معين أو بيانات معينة أو بيانات أو برامج مخزنة في حاسب آلي معين.

ويعاقب علي جريمة الدخول غير المشروع إلي النظام المعلوماتي في القانون الإنجليزي بالسجن لمدة لا تتجاوز ستة أشهر أو بغرامة لا تتجاوز ٥٠٠٠ إسترليني، أو بالعقوبتين معًا. وفي أحد القضايا في بريطانيا حكم علي أندرو هارفي بالسجن لمدة ستة أشهر وعلي جوردان برادلي بالسجن لمدة ثلاثة أشهر لإدانتهما بصنع واستخدام دودة إلكترونية أطلق عليها اسم T-Kworm وقد استخدمت هذه الدودة عبر قنوات المحادثة Chat Chanells لإصابة الحاسبات الآلية الأخري، وقد أدي ذلك إلي سيطرة هذين المخترقين علي الحاسبات الآلية المصابة بالفيروس. وقد استمعت محكمة Newcastle Crown Court إلي كيفية إصابة إحدي الحاسبات الآلية التابعة للشرطة بهذا الفيروس وتسبب بدوره في الانتقال إلي أكثر من ١٩ ألف حاسب آلي في مدة لا تتجاوز أسبوعين، وقد أقر المحكومان بالاشتراك في الدخول غير المشروع إلي حاسبات آلية مع توافر النية للقيام بهذا الفعل. كما أقرا بأنهما قاما بهذا الفعل بسبب رغبتهما في التحكم بالحاسبات الآلية المملوكة للغير والشعور بالسيطرة الذي يمنحه لهما دون هدف آخر مادي أو غيره[١].

---

[١] وقد تم القبض على هذه المتهمين عام ٢٠٠٣ على أثر التحقيق المشترك بين وحدات مكافحة جرائم الحاسب الآلي في كل من بريطانيا والولايات المتحدة الأمريكية، وقد كان هذين المخترقين عضوين في مجموعة تعرف باسم Threat Krew. وقد أثرت الدودة التي تم استخدامها من قبل الجانيين في الحاسبات الآلية التي تستخدم أنظمة تشغيل ميكروسوفت.
See. BBC News, Hackers Jailed over virus. Available at:
http://newsvote.bbc.co.uk/mapps.bbc.u.knews.

المطلب الثاني
الموقف التشريعي للدول العربية من جريمة
الإرهاب الإلكتروني

تعاملت بعض الدول العربية مع هذا النوع من الجرائم بالقوانين الجنائية المتعلقة بمكافحة الإرهاب كالقانون المصري ولعل ذلك يرجع إلى عدم إصدار قانون مكافحة جرائم تقنية المعلومات حتي كتابة هذه السطور، إلا أن الغالبية العظمي منها قامت بإصدار تشريعات مستقلة تجرم جرائم الحاسب الآلي ومنها جرائم الإرهاب الإلكتروني[١].

وعليه سوف نتناول موقف التشريعي في كل من جمهورية مصر العربية، والمملكة الأردنية الهاشمية، والإمارات العربية المتحدة، والمملكة العربية السعودية كأمثلة للدول العربية في التعامل مع جرائم الإرهاب الإلكتروني في أربعة أفرع علي النحو التالى:

الفرع الأول: التشريع المصري.

الفرع الثاني: التشريع الأردني.

الفرع الثالث: التشريعي الإماراتي.

الفرع الرابع: التشريع السعودي.

الفرع الأول
التشريع المصري

[١] ويمثل هذا الاتجاه كل من : المملكة العربية السعودية، الأمارات العربية المتحدة، الكويت، سلطنة عمان، البحرين، قطر، السودان.

أسبغ المشرع المصري حماية خاصة للمواقع الإلكترونية لما لها من أهمية متعددة الأطراف حيث ضمن تجريم استخدام الإنترنت في الترويج للأعمال الإرهابية أو تبادل الرسائل أو نقل التكليفات بين المنتسبين للجماعات الإرهابية ضمن قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥. إذ نصت المادة ٢٩ من القانون المشار إليه إلى أنه: « يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين كل من أنشأ أو استخدم موقعًا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة فى شأن أى جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية فى الداخل والخارج.

فيما يعاقب الجاني بالسجن المشدد مدة لا تقل عن عشر سنين، إذا أقدم الفاعل علي الدخول بغير حق أو بطريقة غير مشروعة موقعًا الكترونيا تابعًا لجهة حكومية، بقصد الحصول علي البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولي من هذه المادة أو الإعداد لها (المادة ٢/٢٩) [١].

---

[١] وتجدر الإشارة إلى أن مشروع قانون مكافحة جرائم تقنية المعلومات قد جرم كافة الاعتداءات على سلامة الشبكات وأنظمة تقنية المعلومات في الباب الثالث منه مقررًا عقوبة مغلظة على مرتكب هذا النوع من الجرائم، وقد تمت موافقة البرلمان على جميع بنود المشروع المقدم من الحكومة بجلسة الأثنين ١٤ مايو ٢٠١٨ المنعقدة بمجلس النواب. وتعالج المواد ١٥، ١٩، ٢٠، ٢١ جرائم الدخول غير المشروع، وإتلاف أو تشويه المواقع أو تغيير تصاميمها، والاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، والاعتداء على سلامة الشبكة المعلوماتية على التفصيل التالى:

المادة ١٥: تعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ٥٠ ألفا ولا تتجاوز ١٠٠ ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل عمدا أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه.

فإذا أنتج عن ذلك إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن ١٠٠ ألف جنيه ولا تتجاوز ٢٠٠ ألف أو بإحدي هاتين العقوبتين.

المادة ١٩: تعاقب بالحبس مدة لا تقل عن ٣ أشهر، وبغرامة لا تقل عن ٢٠ ألف جنيه ولا تتجاوز ١٠٠ ألف جنيه أو بإحدى العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوه أو أخفي، أو غير تصاميم موقعًا خاصًا بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.

المادة ٢٠: تعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن ٥٠ ألف جنيه ولا تتجاوز ٢٠٠ ألف جنيه، أو بإحدي هاتين العقوبتين، كل من دخل عمدا أو بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية تكون العقوبة السجن والغرامة التى لا تقل عن ١٠٠ ألف جنيه ولا تتجاوز ٥٠٠ ألف جنيه.

وفى جميع الأحوال، إذا ترتب على أى من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كليا أو جزئيا بأى وسيلة كانت، تكون العقوبة السجن والغرامة التى لا تقل عن مليون جنيه ولا تتجاوز ٥ ملايين جنيه.

المادة ٢١: تعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لاتقل عن مائة ألف جنيه ولا تتجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها، أو الحد من كفاءة عملها، أو التشويش عليها، أو إعاقتها، أو اعتراض عملها، أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها.

ويعاقب كل من تسبب بخطأه في ذلك، بالحبس مدة لا تقل عن ثلاثة شهور، وبغرامة لاتقل عن خمسين ألف جنيه ولا تتجاوز مائتى ألف جنيه أو بإحدى العقوبتين.فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة، أو تدار بمعرفتها او تملتكها، تكون العقوبة السجن المشدد وبغرامة لاتقل عن خمسمائة ألف جنيه ولاتتجاوز مليون جنيه.

الفرع الثاني
التشريع الأردني

لم ينص المشرع الإردني على تجريم الإرهاب الإلكتروني في ظل قانون العقوبات رقم ١٦ لسنة ١٩٦٠ وقانون منع الإرهاب رقم ٥٥ لسنة ٢٠٠٦ (قبل التعديل الأخير)، وإنما ركن إلى النصوص التقليدية في تجريم الإرهاب بصورته التقليدية حيث إن النصوص التقليدية تسمح بإدراج كافة صور الإرهاب الإلكتروني، إضافة إلى النصوص المنظمة لجرائم أمن الدولة التي تتسم بالمرونة بشكل يستوعب الإرهاب الإلكتروني.

لكنه أجري تعديلا على قانون منع الإرهاب وعدل القانون القديم بقانون رقم ١٨ لسنة ٢٠١٤ وأضاف إليه نصا صريحا اعتبر فيه الإرهاب الإلكتروني في حكم الأعمال الإرهابية المحظورة حيث أورد المادة ٣ فقرة هـ "استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بإعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم".

كما أصدر المشرع الأردني قانون الجرائم الالكترونية رقم ٧ لسنة ٢٠١٥ الذي دخل حيز النفاذ بتاريخ الأول من يونيه لعام ٢٠١٥ وقد حل محل قانون جرائم أنظمة المعلومات المؤقت لسنة ٢٠١٠، بموجب المادة ٩٤ من الدستور الأردني.

وقد عاقب الجاني بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد علي سنة وبغرامة لا تقل عن مائتي دينار ولا تزيد علي ألف دينار، إذا أقدم الفاعل علي

ونلفت الانتباه إلى أن العقوبات المقررة بمشروع القانون لا تخل بأية عقوبة أشد منصوص عليها فى قانون العقوبات أو أى قانون آخر – كقانون مكافحة الإرهاب–، على أن يراعي في ذلك أحكام قانون الطفل رقم ١٢ لسنة ١٩٩٦ والمعدل بالقانون ١٢٦ لسنة ٢٠٠٨.

الدخول غير المشروع إلى موقع إلكتروني لتغييره أوإلغائه أو إتلافه أو تعديل محتواه أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه[١]. أو إذا أدخل أو نشر أو استخدم قصدًا برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع علي بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو اشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح[٢].

وقد عاقب الجاني بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن خمسمائة دينار ولا تزيد عن خمسة آلالف دينار، إذا أقدم الفاعل عمدًا دون تصريح أو بما يخالف أو يجاوز التصريح للدخول إلى الشبكة المعلوماتية أو نظام المعلومات بهدف الاطلاع علي بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني (المادة ١٢/أ). فيما شدد العقوبة إلى الأشغال الشاقة المؤقتة والغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار إذا كان الدخول المشار إليه في الفقرة السابقة بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تغييرها أو نقلها أو نسخها أو إفشائها (المادة ١٢/ب).

كما عاقب كل من دخل قصدًا إلى موقع إلكتروني للاطلاع علي بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لاتقل عن أربعة أشهر والغرامة التي لا تقل عن خمسمائة دينار(المادة ١٢/ج).. فيما شدد العقوبة إلى الأشغال

---

[١] المادة رقم ٣/ج من قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥.

[٢] المادة رقم ٤ من قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥.

الشاقة المؤقتة والغرامة لا تقل عن ألف دينار ولا تزيد عن خمسة آلاف دينار إذا كان الدخول المشار إليه في الفقرة ج بقصد الغاء تلك البيانات أو المعلومات أو إتلافها أو تغييرها أو نقلها أو نسخها أو إفشائها (المادة ١٢/د).

الفرع الثالث
التشريع الإماراتي

أصدرت دولة الإمارات العربية المتحدة القانون الاتحادي رقم ٥ لسنة ٢٠١٢ بشان مكافحة جرائم تقنية المعلومات والذي تضمن تعديلات لما ورد في القانون الاتحادي رقم ٢ لسنة ٢٠٠٦ في شأن مكافحة جرائم تقنية المعلومات والذي ألغي بصدور هذا القانون. ويرجع ذلك إلى رغبة المشرع الإماراتي في مواكبة المتغيرات والمستجدات المتعلقة بأنماط الجرائم المستجدة علي الساحة المحلية أو الاقليمية أو الدولية في هذا المجال[١].

وقد نصت المادة ٤ من المرسوم سالف الذكر علي عقوبة السجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم و لا تجاوز مليون وخمسمائة ألف درهم لكل من دخل بدون تصريح إلى موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات، سواء كان الدخول بقصد

---

[١] ولمزيد من التفاصيل حول سياسية المشرع الإماراتي تجاه أنماط الجرائم المستجدة والأنشطة التجارية والمالية المختلفة والأمن المعلوماتي. راجع:

د/ عبيد صالح حسن، سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، المجلد الرابع والعشرين، العدد ٩٥ – أكتوبر ٢٠١٥، ص ٤٤–٤٧.

الحصول علي بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية.

أما إذا تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر، فتكون العقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم و لا تتجاوز مليونين درهم (المادة ٢/٤).

وقد عاقب الجاني بالحبس والغرامة التي لا تقل عن مائة ألف درهم و لا تتجاوز ثلاثمائة ألف درهم أو بإحدي هاتين العقوبتين، إذا أقدم الفاعل علي الدخول بغير تصريح لموقع إلكتروني بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه[١].

فيما جرمت المادة ٢٦ من ذات المرسوم كل من أنشأ أو أدار موقعًا إلكترونيًا أو أشرف عليه أو نشر معلومات علي الشبكة المعلوماتية أو وسيلة تقنية معلومات، وذلك لجماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة بقصد تسهيل الاتصال بقياداتها أو أعضائها، أو لاستقطاب عضوية لها، أو ترويج أو تحبيذ أفكارها، أو تمويل أنشطتها، أو توفير المساعدة الفعلية لها، أو بقصد نشر أساليب تصنيع الأجهزة الحارقة أو المتفجرات، أو أي أدوات أخري تستخدم في الأعمال الإرهابية وحددت عقوبة السجن مدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن مليون درهم ولا تتجاوز مليوني درهم.

الفرع الرابع
التشريع السعودي

---

[١] المادة ٥ من مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الاتحادي.

أصدرت المملكة العربية السعودية نظام مكافحة الجرائم المعلوماتية[١]، ويهدف هذا النظام إلى الحد من وقوع الجرائم المعلوماتية، بما في ذلك جرائم الإرهاب الإلكتروني، والمساعدة في تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة علي الاستخدام غير المشروع للحواسب الآلية والشبكات المعلوماتية، وحماية المصالح العامة والأخلاق والآداب العامة، وأخيرا حماية الاقتصاد الوطني[٢].

وقد نص نظام مكافحة الجرائم المعلوماتية في مادته الثالثة علي عقوبة السجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين لكل شخص يقوم بالدخول غير المشروع إلى المواقع الإلكترونية، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه.

وقد عاقب الجاني بالسجن مدة لا تزيد على أربع سنوات وبغرامة لاتزيد على ثلاثة ملايين ريال، أو بإحدي هاتين العقوبتين، إذا أقدم الفاعل على الدخول غير المشروع لإلغاء بيانات خاصة أو تدميرها أو تسربها أو إتلافها أو تغييرها أو إعادة نشرها، أو في حالة إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها، أو إذا حصل إعاقة في الوصول إلى الخدمة أو تشويشها أو تعطيلها[٣].

كما تطرق النظام إلى جريمة إنشاء موقع لمنظمة إرهابية على شبكة الإنترنت، أو أحد أجهزة الحاسب الآلي، أو القيام بنشر هذا الموقع، لتسهيل الاتصال بقيادات تلك المنظمة أو أحد أعضائها أو بهدف ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو الأدوات التي تستخدم في الأعمال

---

[١] الصادر بقرار مجلس الوزراء رقم ٧٩ وتاريخ ١٤٢٨/٣/٧هـ، المصدق عليه بموجب المرسوم الملكي رقم م/١٧ وتاريخ ١٤٢٨/٣/٨هـ.

[٢] المادة الثانية من النظام السعودي الخاص بمكافحة الجرائم المعلوماتية.

[٣] المادة الخامسة من النظام السعودي الخاص بمكافحة الجرائم المعلوماتية.

الإرهابية. كما تناول النظام الدخول غير المشروع إلى موقع إلكتروني، أو أي نظام معلوماتي بشكل مباشر أو عن طريق شبكة الإنترنت أو أحد أجهزة الحاسب الآلي، بغرض الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني. أما العقوبة التي حددها النظام لهذه الجرائم فهي السجن مدة لا تزيد على عشر سنوات، والغرامة بما لايزيد على خمسة ملايين ريال، أو أحد هاتين العقوبيين[١].

وقد شدد النظام من عقوبة الجاني الذي قام بارتكاب أحد الأفعال المنصوص عليها من خلال عصابة منظمة، إذ يجب في هذه الحالة أن لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلي[٢].

الفصل الرابع
مكافحة الإرهاب الإلكتروني

تمهيد:

لا شك أنه ليس باستطاعة أي بلد في عصرنا الحالى أن يعيش معزولا عن التطورات التقنية المتسارعة، والآثار الاقتصادية والاجتماعية والأمنية الناجمة عنها في ظل الترابط الوثيق بين اجزاء العالم وعبر تقنيات المعلومات والاتصالات والتطبيقات التي سمحت بانسياب الأموال والسلع والخدمات والأفكار والمعلومات بين مستخدمي تلك التقنيات، ومن ثم بات ضروريًا لكل بلد حماية أفراده ومؤسساته ومقدراته من آثار هذا الانفتاح.

لذا يبدو من الحكمة أن نتوقع انطلاق هجمات الإرهاب الإلكتروني عاجلًا أو آجلًا. ومن ثم لنا أن نتساءل كيف سيتم التعامل مع الإرهابيين في الفضاء الإلكتروني قبل أن تنطلق هذه الهجمات وعقب انطلاقها ؟

---

[١] المادة السابعة من النظام السعودي الخاص بمكافحة الجرائم المعلوماتية.

[٢] المادة الثامنة من النظام السعودي الخاص بمكافحة الجرائم المعلوماتية.

للإجابة على هذا التساؤل المحوري الذي يدور في فلكه هذا الفصل من دراستنا يتعين التمييز بين شكلين من أشكال الدفاع: الدفاع السلبي والدفاع النشط(١).

الدفاع السلبي يهدف بالأساس إلى حماية الهدف وتحصينه عبر استخدام التقنيات المختلفة على سبيل المثال، الجدران النارية، التشفير، كشف التسلل، وإجراءات السلامة القياسية، مثل تلك التي تنظم عمليات الاستعادة وإعادة التشكيل للمؤسسات التي تعرضت لهجمات الإرهاب الإلكتروني بهدف حماية أصول تكنولوجيا المعلومات التي يملكها أو يشغلها فردًا كان أو منظمة(٢).

وقد تكون بعض أشكال الدفاع السلبي ديناميكية، مثل ايقاف هجوم مستمر. لكن وفقا تعريف الدفاع السلبي، لا يترتب على الدفاع السلبي خطرًا جسيمًا أو عقوبة على الطرف المعتدي(٣).

أما الدفاع النشط، فهو الدفاع الذي يفرض خطرًا أو عقوبة خطيرة على المعتدي بحكم التعريف. والخطر أو العقوبة قد تشمل نوعين من الإجراءات: **أولهما**، التعرض والتحقيق والملاحقة القضائية وذلك يحدث عقب تحديد الهوية، **وثانيهما**، شن الهجمات المضادة أو الهجمات الاستباقية لردع الطرف المعتدي(٤).

---

(1) ***See. Seymour E. Goodman,*** "Toward a treaty-based international regime on cyber crime and terrorism," Cyber Security: Turning National Solutions into International Cooperation, Center for Strategic and International Studies Press, Washington, D.C., 2003. pp. 65-78. Available at: http://csis.org/pubs/2003_cyber.html

(2) **Dhiraj Kukreja**, Securing Cyberspace, Liberal Studies Journal, Vol. 2, Issue 2, July-December 2017, pp.195-204. Available at: http://sls.pdpu.ac.in/downloads/Dhiraj%20Kukreja.pdf

(3) **Ibid**. p. 200.

(4) **Seymour E. Goodman**, Cyberterrorism and Security Measures. In: Roddam Narasimha, Arvind Kumar, Stephen P. Cohen & Rita Guenther (eds.), Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop, International Strategic and Security Studies Programme of the National Institute of Advanced Studies, National Academy of Sciences, National Academies Press, Washington, D.C. 2007. pp.43-69.

ولكن يؤخذ على التدابير السلبية أنها تتيح للمهاجمين الحرية في مواصلة الهجوم دون الخشية من رد فعل الطرف المدافع، وبالتالى سوف نكون أمام فرضين لا ثالث لهما وهما أما أن ينجح المهاجمين، أو يشعروا بالإحباط ويبحثوا عن مكان آخر. وبالنظر إلى نقاط الضعف التي لا تخلوا منها معظم الأنظمة الإلكترونية، والتكلفة المنخفضة لمعظم الهجمات، وقدرتهم على إصابة نظم الأمان، بالإضافة إلى المهارة والعزم لدي المهاجمين، سيكون الاحتمال الأقرب للتحقق هو النجاح [١].

أما الاعمال الدفاعية، على سبيل المثال وقف هجوم حدث في التقدم فقد يتم عبر استخدام الوسائل السلبية والنشطة على حد سواء. بشكل سلبي، حال قيام المدافع بسد ثغره الضعف في الوقت الحقيقي. وبشكل نشط، حال قيام المدافع بتحديد الموقع والعودة للتعامل مع مصدر الهجوم[٢].

ولعدة أسباب قانونية وأخري غير قانونية، تقع معظم اشكال الدفاع النشط بالضرورة على عاتق الحكومات[٣]؛ وذلك لأن معظم أشكال الدفاع النشط مجرد شكل إيجابي زائف أو افتراض نظري بحت يصعب تطبيقه، نظرًا إلى الصعوبات التي تحول دون تحديد الهوية، أضف إلى أنه من المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالى. فبعض الحالات قد تتطلب أشهرا لرصدها وهو ما يلغي مفعول الردع بالانتقام، وكثير من الحالات لا يمكن تتبع مصدرها بالمقابل، وحتي إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير

(1) **Ibid**. p. 45.

(2) **Dhiraj Kukreja**, Securing Cyberspace, Op.cit., p. 200.

(3) **See**. **Stephen J. Lukasik et al.** Protecting Critical Infrastructures Against Cyber-Attack, Adelphi Paper 359, International Institute for Strategic Studies, London, U.K. 2003. Available at: http://www3.oup.co.uk/adelph/hdb/Volume_359/Issue_01/

حكوميين، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتي يتم الرد عليها[١].

والحديث عن مكافحة الإرهاب الإلكتروني يستدعي أن نناقش الأشكال الأكثر وضوحا للدفاع، وكيفية مواجهة الأنشطة الإرهابية في الفضاء الإلكتروني ؟ والتي تتم على ثلاث مراحل: أولها، الوقاية والمنع ويطرح هذا الشكل من أشكال الدفاع السؤالين الأتيين: كيف يمكن منع شن الهجمات الإلكترونية؟ وكيف يمكن إفشال الهجوم قبل الوصول إلى الهدف ؟

وثانيها، إدارة الحوادث والتخفيف من الهجوم، والحد من الأضرار وذلك الشكل من أشكال الدفاع يبدأ مع انطلاق الهجوم ووصوله إلى الهدف. وفي هذه المرحلة من الدفاع تثور ثلاثة أسئلة: الأول، كيف نستعد لقيادة الدفاع أثناء الهجوم ؟ والثاني، كيف نتغلب على الهجوم دون خسارة ؟ والثالث، كيف يمكننا تحديد الضرر والتخفيف من أثاره ؟

وثالثها، تتعلق بإدارة عواقب الهجوم الإرهابي الإلكتروني، وفيها يطرح التساؤلين الآتيين: ماذا نفعل بعد أن حقق الهجوم الإلكتروني الهدف منه ؟ وما هي الإجراءات الواجب اتخاذها نحو استعادة الكيان المصاب لما كان عليه قبل الهجوم ؟

وبناء عليه سوف نتناول الأشكال الرئيسية للدفاع من خلال استعراض المراحل الثلاثة لمكافحة الإرهاب الإلكتروني، وذلك في ثلاثة مباحث على النحو التالى:

المبحث الأول: الوقاية والمنع.

المبحث الثاني: إدارة الحوادث والتخفيف من حدتها.

---

[١] د/ عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية دراسة في النظرية والتطبيق، المكتبة الأكاديمية، ٢٠١٦، ص ٣٠٨.

المبحث الثالث: إدارة عواقب حوادث الإرهاب الإلكتروني.

المبحث الأول
الوقاية والمنع

لكي نكون بصدد نظام معلوماتي لا يوجد به ثغرات أمنية يجب أن يتم تصميمه على هذا الأساس، فإذا تم تصميه على هذا الأساس وبالشكل الصحيح، قد يمنع ذلك الهجمات؛ لأنها سوف تصبح غير مجدية، أو في حالة إطلاقها لن تسبب أي ضرر.

إلا أن الغالبية العظمي من أنظمة تكنولوجيا المعلومات، لم يكن الأمن معيارًا رئيسًا في تصميمها، إن لم يكن في كافة النظم على الإطلاق. ويرجع ذلك إلى ثلاثة عوامل رئيسة: **أولها**، أن جميع الأنظمة الإلكترونية تقريبا لم تأخذ مسألة الأمان في الاعتبار عند التصميم. **وثانيها**، أن معيار الأمن في كثير من الأحيان يتعارض مع المعايير الفضلي في التصميم التي تتعلق بتعزيز المقاصد الأولية في الوصول والإنتاج. **ثالثها**، أن الأمان الإضافي في النظم الإلكترونية ليس مكلفًا فحسب بل يؤدي إلى الحد من الكفاءة والفعالية وحسن الأداء وهو ما يعيب النظم المعلوماتية[1].

لذا أعتقد أن تحسين الأمن في النظم الإلكترونية أو إعادة تصميم الأنظمة المعلوماتية بما يحقق الأمان لن يتأتي- كما تشير التكهنات- إلا في أعقاب "بيرل هاربور رقمي"، أو "١١ سبتمبر رقمي" ، أو استجابة لقوي المسئولية القانونية، أو لضرورات ومعايير التأمين، في ظل غياب الحافز الذي من شانه أن يدفع المصممين والمطورين لتصميم النظم أو إعادة تصميمها لتكون أكثر أمانًا.

(1) **See**. **Seymour E. Goodman**, Cyberterrorism and Security Measures…, Op. cit., pp. 46-47.

وعليه يظل البديل القابل للتنفيذ – حتي اليوم – هو محاولة منع الهجمات عن طريق البحث الذاتي عن الثغرات وتحديدها قبل أن يحاول أحد المهاجمين استغلالها. ويمكن استخدام الفرق الحمراء أو أسرة الاختبار أو المحاكاة للقيام بذلك. وثمة أسلوب آخر، يستخدم في كثير من الأحيان – على الأقل– لتفادي الهجمات المحتملة من داخل المؤسسة، وذلك عن طريق فحص الموظفين المحتمل ضلوعهم بدرجة أكبر مستقبلًا(١).

وهناك طريقة عامة أخرى لمحاولة منع هذه الهجمات وتتمثل في التجريم. وهي الطريقة الأكثر وضوحًا والتي تتم من خلال القانون وإدراجها ضمن الأعمال الإرهابية. لكن يجب أن يكون هناك أيضًا معايير دقيقية وفنية معترف بها دوليا في ظل قسوة العقوبات المقررة على من يرتكب مثل هذه الأعمال، تلك القسوة تجعل الإرهابيين يفكرون جديًا قبل أن يقدموا على تنفيذ الهجمات الإلكترونية، وبالتالى قد يتراجعوا عن ارتكاب مثل هذه الهجمات خوفا من التعرض لهذه العقوبات. من ناحية أخري، من الأهمية بشكل خاص للدفاع منع الهجمات وتحديد هوية المهاجمين المحتملين، أو إلقاء القبض عليهم، أو معاقبة أي منهم.

من منظور مخاطر القيام بالدفاع يختلف الإرهابيون الأفراد والمنظمات الإرهابية حتي تلك التي تدعمها الدول القومية عن الدول القومية ذاتها. إذ لا يملك الإرهابيون والمنظمات الإرهابية الإ القليل من الأصول المادية، كما لا يتمتعون بإقليم سيادي يحميهم من أي هجوم مادي، أو غيره من الهجمات المضادة. ونتيجة لذلك، فهم غير مكترثين للعواقب المحتملة حينما يتم تحديد هويتهم بخلاف الدول القومية حتي المارق منها، كذلك قد يكونوا أكثر استعدادًا للهجرة قبل شن الهجوم الانتقامي أو أثناء القيام به وبالتالى هم أقل حساسية من التدابير الوقائية للردع بخلاف

(1) **Seymour E. Goodman**, Critical Information Infrastructure Protection, In: Responses to Cyber Terrorism Centre of Excellence Defence Against Terrorism, Ankara, Turkey (eds.), IOS Press, 2008. pp. 30-31.

المجرمين أو الجواسيس الصناعيين أو عملاء الدول القومية والذين ينخرطون في أشكال أخري من الصراع الإلكتروني.

ونظرًا لتزايد معدل التهديدات الإلكترونية في السنوات الأخيرة وخطورة الهجمات الموجهة ضد البنية التحتية الحرجة بحث خبراء الأمن، والدارسون، وصناع القرار إعادة إحياء نظريات الحرب الباردة – ومنها نظرية الردع – للتصدي لتلك الهجمات وردعها وتطبيقها في الفضاء الإلكتروني(١)، وتخفيفًا من حجم النشاط العدائي الناجح ضد شبكات القطاعين العام والخاص ولكي لا تظل البنية التحتية والبيانات عرضة لكافة أشكال الاعتداء(٢).

لذا نجد لزاما علينا أن نلقي الضوء على نظرية الردع عبر التعرف على المقصود بالردع، وما أنواعه ؟ وذلك للتعرف على مدي إمكانية تطبيقه في الفضاء الإلكتروني. وسوف نتناول ذلك في ثلاثة مطالب على النحو التالى:

---

(1) International Strategy for Cyberspace, The White House, May 2011. Available at:http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Department of Defense's Strategy for Operating in Cyberspace, U.S. Department of Defense, July 2011. available at: http://www.defense.gov/news/d20110714cyber.pdf.

ومكمن الخطورة أن التهديدات السيبرانية لا تتأتي في الغالب من الدول القومية وإنما تتأتي من الدول المارقة والإرهابيين ومجرمي الإنترنت والمتسللين من مستويات مختلفة من التطور والراغبين في استخدام قدراتهم لدعم الأهداف الشائنة مما يتطلب وجود تدابير وقائية.

Susan W. Brenner & Leo L. Clarke, "Civilians in Cyberwarfare: Casualties," SMU Science & Technology Law Review, Vol. 13. No. 2, 2010. p. 249; **Graham H. Todd**, Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, Air Force Law Review, Vol. 64, 2009. pp. 65-102; **William J. Lynn**, The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack, Foreign Affairs (September 28, 2011). available at: www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

(2) **Emilio Iasiello**, Is Cyber Deterrence an Illusory Course of Action?. Journal of Strategic Security, Vol. 7, No. 1, 2013. pp. 54-67.

المطلب الأول: تعريف الــردع.

المطلب الثاني: أنواع الــردع.

المطلب الثالث: تطبيق الردع في الفضاء الإلكتروني.

المطلب الأول

تعــريف الــــردع

الردع بصفة عامة هو منع الخصم من القيام بفعل عدائي، إما بسبب تخوفه من هجوم مضاد يفوق قدراته الدفاعية، أو ارتفاع تكلفة الهجوم مقارنة بالمكاسب التي يمكن أن يحققها. ولكي يتحقق الردع يجب توافر مكونين رئيسين: أولهما، نوايا يعبر عنها من الطرف المدافع برغبته في الدفاع عن مصلحة ما. وثانيهما، إدراك الطرف المهاجم أن التعارض مع الطرف الثاني حول هذه المصلحة سوف يكون مكلفًا وبصورة تمنعه من اتخاذ أي موقف عدائي تجاهه. وبذلك يتحقق الهدف الرئيسي من الردع هو جعل الطرف الأول سلبي تجاه الثاني بحيث لا يتخذ أي موقف هجومي نحوه، بمعني آخر هو السعي نحو البقاء على الوضع الراهن[١].

ووفقا لنظرية الردع التقليدية يعرف الردع بأنه إقناع الخصم بعدم البدء بعمل عدائي لأن التكاليف والمخاطر تفوق أي منافع محتملة[٢]. ولعل التعريف الأبرز والأشهر للردع – والمتداول بكثرة في الأدبيات – هو تعريف الجنرال أندريه بوفر الذي عرف الردع بأنه: « منع دولة معادية من اتخاذ قرار باستخدام أسلحتها أو بصورة أعم منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير

---

(١) إيهاب خليفة، إمكانيات تحقيق الردع فى صراعات الفضاء الإلكترونى، مركز المستقبل للأبحاث والدراسات المتقدمة ، العدد ١٣ – ٢٠١٥، ص ٤٩.

(2) **John J. Mearsheimer**, Conventional Deterrence, Ithaca, New York: Cornell University Press, 1983.

والإجراءات التي تشكل تهديدًا كافيًا حيالها، والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية»[١].

أما الردع الإلكتروني فيقصد به منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الإلكتروني[٢]. أو على الأصح هو استراتيجية تسعي الدولة المدافعة بواسطتها للحفاظ على الوضع الراهن بالإشاره إلى نواياها لردع النشاط المعادي في الفضاء الإلكتروني عن طريق الاستهداف والتاثير على جهاز صنع قرار لدي الخصم، لتجنب الانخراط في الأنشطة المدمرة على الإنترنت خوفا من انتقام أكبر من قبل المعتدي عليه[٣].

ويرتكز الردع الإلكتروني على ثلاثة ركائز رئيسة تعتمد عليها أي استراتيجية للردع الإلكتروني: أولها، مصداقية الدفاع Credible Defense، إذ يتطلب الدفاع عن أنظمة المعلومات، ردع أي محاولة لاختراقها – من بين متطلبات أخرى – توافر أنظمة نسخ احتياطية، مما يعني أن أي هجوم ناجح عليها، لن يسفر عن التدمير التام لها أو الفقدان الكلي لما تحويه من معلومات؛ ورغم تزايد تكلفة هذا الحل إلا أنه الحل العملي الأكثر فعالية. وثانيها، القدرة على الانتقام An Ability to Retaliate، فلابد أن يتكبد المهاجم ضررًا يفوق ما وقع على المدافع من أضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي، بعد التعرف عليه وهو صعب التحقق.

---

(١) أندريه بوفر، الردع والاستراتيجية. ترجمة: أكرم ديري، دار الطلعية للطباعة والنشر، بيروت، ١٩٧٠، ص ٣١.

(2) **Michael Krepon**, Space and Nuclear Deterrence, In: Michael Krepon and Julia Thompson (eds.), Anti-Satellite Weapons Deterrence and Sino-American Space Relations, United States: Stimson Center, September 2013. p. 15.

(3) **Emilio Iasiello**, Op. cit., p. 55.

أما الركيزة الثالثة فتتمثل في الرغبة في الانتقام A Will to Retaliate، فعلى المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، ذلك أن امتلاك القدرة على الانتقام لا تكفي بمفردها للردع [١].

المطلب الثاني
أنواع الـــــــردع

يعتمد الردع الإلكتروني على عنصرين هما: ردع الهجمات الإلكترونية فيما يعرف "الردع بالمنع"، والردع بالتهديد بشن هجمات سيبرانية فيما يعرف "الردع بالإنتقام". وسوف نوضحهما كالآتي:

أولًا: الردع بالمنع:

وهو إقناع الخصم بأنك تملك ما تحصن به نفسك ضد عدوانه وبما يقنعه أن عدوانه غير مجديًا أو أن خسائره من الهجوم ستفوق مكاسبه[٢]. والسبيل إلى تحقيق ذلك يكون بالعمل على إظهار عناصر القوة والبأس وإبراز ما يتمتع به من قدرات ردعية حتي يظهر للطرف الأخر أن ما سيقوم به لن يعود عليه بنفع، ولن يجلب له فائدة[٣].

والردع بالمنع Deterrence by denial ينطوي تحت لوائه نوعين: الردع بالمقاومة "Resistance"، والردع بالصمود ″Resilience″. والصمود هنا يعني القدرة على استعادة الشئ لشكله الأصلي بسرعة بعد الهجوم، الأمر الذي من شأنه

---

(1) **MAJ Lee Hsiang Wei's**, The Challenges of Cyber Deterrence, Journal of the Singapore Armed Forces, Vol. 41, No. 1, 2015. p. 13.

(2) **Ryan, N. J.**, Five Kinds of Cyber Deterrence, Philosophy & Technology, Published Online: 27 January 2017. pp.2-3. Available at: https://link.springer.com/content/pdf/10.1007%2Fs13347-016-0251-1.pdf

(٣) د/ يوسف نصر الله، تداعي الأسطورة: مقاربات نقدية لمشهدية الحرب السادسة، دار الفارابي – بيروت– لبنان، الطبعة الأولي ٢٠١١، ص ١٠٩.

أن يحد من المكاسب المحتملة ويمكن أن يقنع الخصم بعدم الهجوم خاصة إذا كانت التكلفة مُفرطة. ويظل الهدف من "المقاومة والصمود" هو تقليل خيارات الطرف الذي ينوي الهجوم، سواء من خلال بناء هياكل دفاعية يصعب التغلب عليها أو من خلال ضمان التعافي السريع للشيء بعد الهجوم ليعود لأصله(١).

ثانيًا: الردع بالانتقام:

يشير هذا النوع من الردع إلى التهديد بالعقاب الرهيب إذا أقدم الخصم على إجراءات تتعارض مع مصلحة الطرف الرادع(٢)، ويعتبر كثير من الباحثين أن هذا النوع هو الشكل العام للردع والأكثر شيوعًا؛ لأنه الطريق الوحيد الذي يكفل تحقيق مستلزمات الردع الفعال شريطة أن يكون التهديد بالانتقام ذا مصداقية في ذهن الخصم بحيث يتم تعديل سلوكه، كما يجب أن يكون العقاب موجها نحو الأصول القيمة(٣).

ولردع الجناة المحتملين عن الهجوم عادة ما يميز البعض بين وسيلتين: المنع "Denial" والانتقام "Retaliation "(٤): وفي إطار علم الجريمة أيضا نجد بنثام يصف الردع عن طريق الانتقام أو الردع عن طريق العقاب بأنه: « مثل القبض على الجاني في قضية ما وصولًا إلى محاكمته، وهو ما يؤثر ليس فقط على

(1) **Annegret Bendiek & Tobias Metzger**, Deterrence Theory in the Cyber-Century: Lessons from a State-of-the-art Literature Review, German Institute for International and Security Affairs (SWP). Mai 2015. p. 6. Available at: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

(2) **Annegret Bendiek & Tobias Metzger**, Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review, Op. cit., p. 6.

(3) **Ryan, N. J.**, Five Kinds of Cyber Deterrence, Philosophy & Technology, Published online: 27 January 2017. Available at: https://link.springer.com/content/pdf/10.1007%2Fs13347-016-0251-1.pdf

(4) For the first debates. refer to **Glenn Snyder**, Deterrence and Defense. Princeton: Princeton University Press, 1961. and Deterrence by Denial and Punishment. Princeton: Center of International Studies, 1958.

سلوك هذا الجاني في المستقبل، وإنما أيضًا على سلوك الآخرين عبر ما يعرف بالردع العام »[١].

المطلب الثالث

تطبيق الردع في الفضاء الإلكتروني

إذا كان الردع الإلكتروني يعبر عن الشكل الضمني أو الصريح للترهيب والتخويف والذي يفترض أن الطرف الذي يمارسه مستعد لمباشرته ولديه من القدرة على الاستجابة إلى أي حادث والتصرف بفعالية في ذات لحظة التعرض للهجوم. فيمكننا تصور أوجه التشابه مع العالم المادي إذ تتكون سياسات الردع في الفضاء الإلكتروني من التصريحات التي يمكن دعمها بالقدرات التقنية مثل نظم الإنذار المبكر والمجسات الإلكترونية التي توفر احتماليات عالية للكشف عن التهديدات المحتملة ومن ثم تحديد الهوية[٢].

وعليه هل سيكون من المناسب ممارسة الأشكال المختلفة للردع في الفضاء الإلكتروني؟ إذ ينظر للاستباقية – الردع بالعقاب– كضربة مضادة لخصم على وشك الهجوم، إذ يعتقد المرء أن الولايات المتحدة كانت وراء هجوم ستكسنت الذي استهدف أجهزة الطرد المركزي لمفاعل ناتانز والذي كان بمثابة ضربة استباقية ضد إيران تأتي ضمن سلسلة من المساومات السياسية والعقوبات الاقتصادية لاستمرارها في إجراءات تخصيب اليورانيوم[٣]. أما الاعتراض – الردع بالمنع– فيكون عن طريق وقف هجوم تم اطلاقه من الوصول إلى الهدف، وكلاهما يمكن اعتبارهما وبشكل كبير نوعين من أنواع الوقاية العاجلة أيضًا[٤].

---

(1) **Lawrence Freedman**, Deterrence, Cambridge, Polity Press, 2004, pp. 60-61.

(2) **Seymour E. Goodman**, Cyberterrorism and Security Measures..., Op. cit., p. 47.

(3) **Emilio Iasiello**, Op. cit., p. 55.

(4) **Seymour E. Goodman**, Cyberterrorism and Security Measures…, Op. cit., p. 47.

وقد تكون الضربات الاستباقية أو الاعتراضات إما إلكترونية أو مادية. ففي الفضاء الإلكتروني، يكون الكشف عن النوايا والتخطيط بالأخص من الأعمال الاستخبارية الذكية[١]، أو من أعمال نظم الإنذار المبكر، كما يستدل عليه عبر الآثار التي يتركها من يتجولون في الفضاء الإلكتروني بحثًا عن المعلومات أو المؤشرات الاستخبارية[٢].

وبالرغم من أوجه التشابه المتعددة اختلف الكتاب حول إمكانية تطبيق نظرية الردع التقليدية في الفضاء الإلكتروني ويوجد في هذا الصدد ثلاثة اتجاهات على النحو التالى:

الاتجاه الأول:

يذهب إلى عدم جدوى تطبيق نظرية الردع في الفضاء الإلكتروني، مشككًا في جدواها وفعاليتها، نظرًا لأن طبيعة العمليات الإلكترونية تُقوض من الدور المحتمل للردع، بل قد تجعله عديم الفائدة كليًا. ويركز أنصار هذا الاتجاه على الإشكاليات التي تواجه الردع الإلكتروني، ومنها: صعوبة تحديد هوية مرتكبي الهجمات ابتداءً، فضلًا عن غياب القوانين اللازمة والرادعة، على نحو يوفر لمرتكبيها الملاذ الآمن، مما يحول دون ملاحقتهم. بالإضافة إلى عدم إمكانية تطبيق القوانين الدولية الراهنة على الهجمات الإلكترونية إلا بشكل غير مباشر طالما لم يعلن الجاني عن مسئوليته. ومن ثم سيبدو الرد الانتقامي عملا عدوانيا غير مبرر أو مخالفًا لقواعد القانون الدولي[٣].

---

(١) ففي الولايات المتحدة الأمريكية، يضطلع بالعديد من هذه الانشطة المركز الوطني لحماية البنية الاساسية.

(2) **Seymour E. Goodman**, Cyberterrorism and Security Measures ..., Op. cit., p. 47.

(3) **Uchenna Jerome Orji**, "Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States'. Defence against Terrorism Review, Vol. 6, No. 1, 2014. pp. 31-45; **Emilio Iasiello**, Op. cit., p.

الاتجاه الثاني:

يرى – أنصاره– أن نظرية الردع لا تنطبق فحسب في المجال الإلكتروني، ولكنها ضرورة أيضًا؛ فبدون الردع الإلكتروني، ستظل البيانات عرضة لأشكال بدائية وخطيرة من الاستغلال والاعتداء، ومنها سرقة البيانات، وانتهاك حقوق الملكية الفكرية، وتعطيل الأعمال التجارية، وإيقاف نظم تشغيل البنية التحتية الحيوية واستهدافها. لذلك يجب أن يكون الردع السيبري جزءًا لا يتجزأ من استراتيجيات الأمن القومي للدول [١].

الاتجاه الثالث

يرى أن نظرية الردع يمكن أن تتلاءم والفضاء الإلكتروني، ولكن بشروط وضوابط محددة، منها تبني مفهوم واسع للردع، والمزج بين خيارات عدة في سبيل الوصول إلى استراتيجية متكاملة له، أخذًا في الاعتبار أن الردع في عصر المعلومات يختلف كثيرًا عنه في عصر الحرب الباردة في النوع والنطاق، مما يتطلب

56; **Jensen Eric Talbot,** Cyber Deterrence, Emory International Law Review, No. 26, 2012. pp. 1-52; **MAJ Lee Hsiang Wei's**, Op. cit., p. 15; **Martin C. Libicki**, Cyberdeterrence and Cyber War, Santa Monica, CA: RAND, 2009; **Martin C. Libicki**, Deterrence in Cyberspace, High Frontier, Vol. 5, No. 3, May 2009, pp. 15–20; **Jonathan Solomon**, Cyber Deterrence Between Nation-States: Plausible Strategy or a Pipe Dream?, Strategic Studies Quarterly, Vol. 5, No. 1, Spring 2011, Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA538310

(1) **Haylen Cohen**, The Approaches and Limitations of Cyber Deterrence, Introduction to Computer Security, Tufts University Department of Computer Science, December 15, Fall 2015. pp. 1-11. Available at: http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf
The Department of Defense Cyber Strategy, April 2015, Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

نهجًا شاملًا يدمج كل المقومات العسكرية والاقتصادية والاستخباراتية والقانونية، تعزيزًا لأمن المعلومات من ناحية، وخلقًا للردع من ناحية أخرى(١).

وبالرغم من وجاهة الاعتبارات التي ساقها الرافضون لتطبيق نظرية الردع في الفضاء الإلكتروني(٢)، إلا أن العديد من الجهات تعمل على التأكيد على إمكانية تحقق الردع بالمنع والحرمان في الفضاء الإلكتروني مستقبلا انطلاقا من شبكة الأنظمة الدفاعية الإلكترونية المتطورة التي تسعى كل دولة إلى استحداثها، وإيجاد ثغرات عبرها لتحديد هوية الأعداء للقيام بالرد الانتقامي أو إجبارهم على عدم التعرض لها لأن التبعات ستكون أكثر ضررا وبالتالى تحقيق معادلة الردع.

وفي النهاية يبقى الردع الإلكتروني مظهر من مظاهر التطور التكنولوجي في عصرنا الحالى إلا أن تطبيقه يحتاج لمزيد من المناقشات حول القيود القانونية الدولية، وكيفية التغلب على المشكلات القانونية المتعلقة بالإسناد، وتحديد الهوية لإدخاله حيز العمل(٣).

---

(1) **Kevin R. Beeker,** Strategic Deterrence in Cyberspace: Practical Application, Graduate Research Project Presented to the Faculty Department of Electrical & Computer Engineering Graduate School of Engineering and Management, Air Force Institute of Technology Air Education and Training Command in Partial Fulfillment of the Requirements for the Degree of Master of Cyber Warfare, 2009, p. 7; Report on Cyber Deterrence Policy, Available at: http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

(٢) لاستعراض إشكاليات تطبيق نظرية الردع في الفضاء السيبراني، راجع:

Patrick Cirenza, An Evaluation of the analogy between nuclear and cyber deterrence, Thesis submitted to Center for International Security and Cooperation Freeman Spogli Institute for International Studies Stanford University, June 2015. pp.67-85.

(٣) د/ عبلة مزوزي، استراتيجية الردع وانعكساتها على الواقع الإقليمي والدولي بعد نهاية الحرب الباردة، رسالة دكتوراه، جامعة باتنة، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٧-٢٠١٨، ص ١٠٩.

ولا شك في أن التوسع في سن التشريعات المتعلقة بمكافحة جرائم تقنية المعلومات علي المستوي الدولي من شأنه أن يساعد علي وضع نهاية للإجرام المعلوماتي والأنشطة الإرهابية في الفضاء الإلكتروني، أو علي الأقل سيؤدي إلى تقليل الكم الضخم من الأنشطة الضارة في هذا الفضاء، وبالتالى يفسح المجال لسلطات إنفاذ القانون في التعرف علي الأنشطة الأكثر خطورة ومن ثم اعتراضها بسهولة أكبر. كما سيوفر أيضًا الأساس الضروري لتشجيع المجني عليهم للإبلاغ عن الهجمات الإلكترونية الضارة، بالإضافة إلى تشجيع التعاون الدولي للتعامل مع المشاكلات التي تثيرها الجرائم الإلكترونية والتي تتطلب في كثير من الأحيان الملاحقة الدولية للجناة[١]، والتعاون في مجال تدريب رجال العدالة علي مواجهة هذا النوع من الجرائم [٢].

ونلفت الانتباه إلى أن معظم أشكال الدفاع النشط لا يجب أن تترك للافراد أو المؤسسات بل يجب أن تقتصر علي الحكومات. وفي هذا الصدد من المرجح أن يكون التعاون الحكومي الدولي حافزًا لمواصلة تطوير استراتيجيات الدفاع النشطة في مجالات مثل تبادل المعلومات الاستخبارية. في كثير من الحالات، تتعرض الكيانات الخاصة المشاركة في الدفاع النشط لخطر التعرف عليها وإساءة فهم المجرمين. ومن ناحية أخري، بالنظر إلى إمكانيات الإرهاب الكارثي، من المهم بشكل خاص للدفاع

---

[١] ففي كثير من جرائم بث ونشر الفيروسات قد يكون مرتكب الهجوم يحمل جنسية دولة ما، ويشن الهجوم الفيروسي من حواسيب موجودة في دولة أخري، وتقع الآثار المدمرة لهذا الهجوم في دولة ثالثة. ومن ثم تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها.

[٢] بالنظر إلى أن أجهزة العدالة في كثير من الدول النامية ليست لديها الجاهزية لمواجهة الجرائم السيبرانية لعدة أسباب منها: الافتقار إلى الموارد الكافية سواء المادية أو البشرية، أو لأن سلطات التحقيق لديها محدودة، أو لأن لديها قوانين ونظم سبقها الزمن أو تفتقر لأي قوانيين من شأنها التصدي لهذه النوعية من الجرائم.

منع الهجمات وتحديد هوية المهاجمين المحتملين أو إلقاء القبض عليهم أو معاقبة أي منهم.

المبحث الثاني

إدارة حوادث الإرهاب الإلكتروني والتخفيف من حدة الهجوم

مثل أي جريمة أخري لا يمكن استئصال الإرهاب الإلكتروني تمامًا، ولكن يمكن استخدام عدد من الاستراتيجيات للتخفيف من حدة الهجمات في محاولات لمكافحة وتقليل أي أضرار قد يلحقها بالأنظمة المحوسبة حيث يتجه الأمن الإلكتروني إلى أبعد من الاستثمار في أحدث الأجهزة والبرامج(١). وقد عرف الاتحاد الدولي للاتصالات الأمن الإلكتروني بأنه: « مجموعة الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به علي شبكات الكمبيوتر، وسوء الاستغلال، واستعادة المعلومات الالكترونية التي تحتويها بهدف ضمان واستمرار عمل نظم المعلومات، وتأمين حماية وسرية خصوصية البيانات سواء الخاصة بالأفراد أو الجهات في الفضاء الإلكتروني»(٢).

---

(1) **Israa G. Seissa, et al.**, "Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review", International Journal of Science and Research (IJSR), Vol. 6, Issue. 1, January 2017. p. 183.

(2) **Gurpreet Dhillon**, "The Changing Faces of Cybersecurity Governance: What to do before and after a cybersecurity breach?," Kogod Cybersecurity Governance Center (KCGC), 2016.

ففي وقتنا الحاضر أصبح الأمن السيبراني سلاحًا استراتيجيًا بيد الحكومات والأفراد، لا سيما بعد أن أصبحت التهديدات السيبرانية جزءًا لا يتجزأ من التكتيكات الحديثة للحروب بين الدول؛ حيث بات الأمن السيبراني يشكل جزءًا أساسيًا من أي سياسة أمنية وطنية، حيث بات معلومًا أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، الهند وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني أو الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية حيث أصبحت الهجمات السيبرانية أخطر ما يهدد سيادة الدول والأفراد حيث تستطيع أي دولة أو حتى محترف "محتال الكتروني/ قراصنة" في العالم أن تستغل ثغرات ونقاط ضعف تقنية

ويتطلب الأمن الإلكتروني في الوقت الحاضر أن ينظر إليه كما لو كان مسألة تجارية، بمعني أن الإدارة العليا هي المسئولة عن ضمان أن تفي استراتيجية الأمن بأهداف العمل بحيث لا يكون هناك خطر. اتساقا مع ذلك ينبغي علي الإدارة أن تقوم بتقييم المخاطر في ضوء إشراك جميع أصحاب المصلحة في استراتجية الأمن وذلك لضمان معالجة جميع جوانب تكنولوجيا المعلومات بما في ذلك الأجهزة والبرمجيات وتدريب وتوعية الجانب البشري الذي يمثله الموظفون داخل أي مؤسسة أو منظمة أو إدارة(١).

وعلي مستوي المخاطر الأمنية يجب أن تشمل المناقشات تحديد المخاطر الإلكترونية وكيفية تجنبها، وقبولها إذا حدثت، والتخفيف من حدتها، ونقل المخاطر عن طريق التأمين الإلكتروني مثلا، بالإضافة إلى تقييم الخطط الدقيقية المتصلة بكل فرع من فروع استراتجية أمن الفضاء الإلكتروني(٢).

لذلك يجب وضع خطط إستراتيجية شاملة لضمان حماية الدول ومواطنيها، ومواجهة الآثار السيئة للإرهاب الإلكتروني. وعليه سوف نناقش الخطوات التي يمكن أن تتخذها الأطراف المعنية للتعامل مع تهديدات الإرهاب الإلكتروني بشكل فعال. وذلك ستة مطالب علي النحو التالى:

المطلب الأول: الاستراتيجيات الإدارية.

المطلب الثاني: الحلول التكنولوجية.

المطلب الثالث: الجانب البشري.

و توجه ضربات الكترونية الى أي مكان في العالم وتستغل المعلومات الحساسة والهامة بأشكال مختلفة ضارة وخطيرة وذات تكلفة هائلة.

(1) **Frederick Wamala**, "ITU National Cybersecurity Strategy Guide," ITU, 2011. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

(2) **Israa G. Seissa, et al.,** Op. cit., p. 183.

المطلب الرابع: التحالفات الوطنية والمحلية.

المطلب الخامس: التحالفات الدولية.

المطلب السادس: التعليم والتدريب وعلم النفس.

المطلب الأول

الاستراتيجيات الإدارية

من بين الاستراتيجيات الرئيسة للتصدي للإرهاب تطوير تشريعات الأمن الإلكتروني وآليات المراجعة بما يضمن في النهاية تصميم وتنفيذ أحدث السياسات المحلية والدولية في الأمن الإلكتروني[١]. على سبيل المثال، أقرت وزارة الدفاع بالولايات المتحدة الأمريكية العديد من السياسات الإلكترونية التي تشمل سياسات تكنولوجيا الإنترنت لتأمين نظم المعلومات [٢]. وفي هذا الصدد أشارت إلى أنه المستحسن بمجرد وضع نظام وسياسة للأمن، وجوب توخي الحذر بإجراء مراجعة للسجلات اليومية، وأداء تحديثات للبرامج، والإبلاغ عن الهجمات حال حدوثها وتحليلها، ومراجعة المواقف الحالية [٣].

(1) **Dimitrios Choupis**, "Challenges and Objectives for the National Cyber-Security Strategy Beyond 2020". Journal of Computations & Modelling, Vol. 4, No. 1, 2014. pp. 1-10. Available at: http://www.scienpress.com/Upload/JCM/Vol%204_1_1.pdf

(2) **Maurice Dawson, et al.,** "DoD Cyber Technology Policies to Secure Automated Information Systems". International Journal of Business Continuity and Risk Management, Vol. 4, No. 1, 2013. pp. 1–22.

(3) **Saint-Claire, Steven**, "Overview and Analysis on Cyber Terrorism". School of Doctoral Studies, European Union Journal, Vol. 3, No. 1, 2011. pp.85-98**; Beggs, C. & Warren, M.**, Safeguarding Australia from Cyber-terrorism: A Proposed Cyberterrorism SCADA Risk Framework for Industry Adoption. Australian Information Warfare and Security Conference. Australia, Edith Cowan University. 2009.

ومن بين الاستراتيجيات الأخرى الموصى بها تطوير استراتيجيات شاملة للأمن الإلكتروني، والأهداف الاستراتيجية، وتصميم المعايير والمبادئ التوجيهية لحماية الأصول والبنى التحتية الوطنية [١].

وقد اعتمد رئيس الولايات المتحدة الأمريكية الاستراتيجية الوطنية لتبادل المعلومات وحمايتها (NSISS) للهيئات والحكومات الفيدرالية للمشاركة في تبادل المعلومات والدفاع عنها وحماية سلامة المواطنين الأمريكيين عام ٢٠١٢[٢]. كما أوصي الخبراء بضرورة تصميم وتطوير إطار الأمن الفضاء الإلكتروني والمعايير اللازمة لمكافحة الإرهاب الإلكتروني[٣].

المطلب الثاني
الحلول التكنولوجية

تحدثت العديد من التقارير عن ضعف النظم الأمنية وإمكانية اختراقها. حتى أن مكتب التحقيقات الفيدرالي أظهر أنه على الرغم من استخدام النظم الأمنية بالولايات المتحدة الأمريكية للتقنيات المتطورة، إلا أن نقاط الضعف ما زالت موجودة. والحقيقة التي لا تقبل الجدل هي أن هذه التقنيات غير قادرة وحدها على احتواء عدد كبير من المتطفلين والفيروسات، وبالتالى سيكون بمقدرة الإرهابيين تجاوز الجدران النارية وأنظمة حماية كلمات المرور ... إلخ [٤].

لذلك يتطلب أي برنامج للأمان الإلكتروني الفعال تحديد المخاطر الإلكترونية واختيار تدابير الرقابة التي من شأنها أن تمنع أو تخفف من تأثير هذه

(1) **Maurice Dawson, et al.,** "DoD Cyber Technology…, Op. cit., pp.16–17.
(2) **Federal Bureau of Investigation,** FBI Information Sharing and Safeguarding Report 2012. US, Available at: https://www.fbi.gov/file-repository/stats-services-publications-national-information-sharing-strategy-1-fbi-information-sharing-and-safeguarding-report-2012/view
(3) **Jarvis, L., Macdonald, S. & Chen, T.,** Op. cit., pp. 19-20.
(4) **Christopher Beggs & Matthew Butler**, Op. cit., pp. 388 - 390.

المخاطر، حيث تلعب التكنولوجيا دورًا رئيسيًا في الأمن الإلكتروني الفعال. ويمكن تنفيذ العديد من احتياطات التخفيف عبر عدد من الأنظمة التكنولوجية مثل الجدران النارية، وأنظمة حماية كلمات المرور، وتشفير المفاتيح السرية، وتشفير المفاتيح العامة، والتخطي، وأنظمة كشف التسلل Secure Socket Layer ، وتشفير البيانات داخل الشبكة باستخدام IPSec ، وقوائم التحكم في الوصول Access Control Lists وغيرها من بروتوكولات الأمن(١).

وبالرغم من إدراك العديد من المنظمات لدور التكنولوجيا في التخفيف من الهجمات الإلكترونية، إلا أن قدراتها التكنولوجية واستراتيجياتها ومنهجياتها غير كافية لردع الهجمات الموجهة ضد الأمن الإلكتروني(٢). ومن ثم تقع الهجمات عبر استغلال نقاط الضعف في البنى التحتية والاستراتيجيات والمنهجيات التكنولوجية حتى بعد النظر في الاحتياطات الأمنية – لن يكون الأمن مضمونًا تمامًا– فعلى سبيل المثال، قامت دودة بلاستر "Blaster Worm" في أغسطس ٢٠٠٣ بمهاجمة أنظمة الأمن البارزة مما كان لها تأثير على ملايين من النظم المعلوماتية وأجهزة الكمبيوتر (٣).

لذا تحتاج النظم المعلوماتية إلى التقييم الدائم والمستمر للتقنيات الأمان المستخدمة والأساليب والاستراتيجيات الحالية والمستقبلية وما إذا كان من شانها أن تمنع الإرهاب الإلكتروني بشكل كاف(٤). بالإضافة إلى ذلك، هناك العديد من

---

(1) **Ahmed H. Anjariny et al.,** Op. cit., p. 5.

ولمزيد من التفاصيل حول التقنيات الفنية، وإليات عملها، راجع:

د/ أسامة غانم العبيدي، جريمة الدخول غير المشروع للظام المعلوماتي، دراسة قانونية في ضوء القوانين المقارنة، منشور بدراسة المعلومات، العدد الرابع عشر، ٢٠١٢، ص ٢٤ وما بعدها. متاح على الرابط التالى: https://search.mandumah.com/Record/206884

(2) **Christopher Beggs & Matthew Butler**, Op. cit., p. 389.

(3) **Ahmed H. Anjariny et al.,** Op.cit., p. 5.

(4) **Christopher Beggs & Matthew Butler**, Op. cit., p. 389.

الممارسات لإعداد أفضل لنظم البنية التحتية للتصدي للهجمات الإلكترونية مثل تحديث أنظمة التشغيل والبرامج بانتظام، وفرض استخدام كلمات السر القوية، وتأمين جميع النظم، وتعطيل الخدمات غير الضرورية، وتثبيت وتحديث برامج مكافحة الفيروسات باستمرار، واستخدام الجدران النارية، ونظم الكشف عن التسلل عالية الدقة(١).

المطلب الثالث

الجانب البشري

ركزت المنظمات تقليديًا على التدابير الأمنية الفنية والإجرائية لتنفيذ حلول أمن المعلومات مع نسيان العامل البشري هو الجزء الأكثر ضعفًا في النظام الأمني(٢). إذ تعتمد إدارة مخاطر أمن المعلومات بشكل كبير على تكوين ثقافة الوعي الأمني Security Awareness (SA) الفعالة والمُقنعة حيث يتطلب الأمن الإلكتروني الفعال أن يكون المستخدمون على دراية بالتدابير والواجبات الأمنية المتاحة والالتزام بها في سياساتهم الخاصة بنظام إدارة أمن المعلومات Information Security Management System (ISMS)(٣).

كذلك يمكن للعوامل البشرية، مثل الإهمال والمكاسب الشخصية، أو عدم التحفيز أن تؤثر بالسلب على أمن وسلامة النظام. على سبيل المثال، قد تؤدي

---

(1) **Michael A. Vatis**, Cyber Attacks During the War on Terrorism: A Predictive Analysis (Institute for Security Technology Studies (Dartmouth College, September 22, 2001), Available at: http://www.ists.dartmouth.edu/projects/archives/cyber_a1.pdf.

(2) **R. Alavi, S. Islam & H. Mouratidis**, "A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS)". Human Aspects of Information Security, Privacy, and Trust Volume 8533 of Lecture Notes in Computer Science, Springer International Publishing, 2014, pp. 297-305.

(3) ITU-T, "Rec ITU-T X.1500 SERIES-X: Data Networks, Open System Communications And Security Overview of cybersecurity information," International Telecommunication Union, Geneva, 2012.

سياسات الأمان الصارمة التي تتطلب من الموظفين إنشاء كلمة مرور معقدة، أو تحديث كلمات المرور بشكل دوري إلى قيام بعض الموظفين بتدوين كلمات المرور الخاصة بهم وتركها في وضع العرض العادي، مما يفتح الباب للمتطفلين للولوج إلى الشبكة المستهدفة [١].

وهناك أربع خطوات لمعالجة جانب الأشخاص: أولها، تحفيز الموظفين ليكونوا أكثر ميلًا للمشاركة في السياسات الأمنية. **وثانيها**، إدراج جميع أصحاب المصلحة في المشاركة في العملية الأمنية. **وثالثها**، تحديد الأدوار الفردية والمسئوليات بوضوح لمختلف العاملين. **أخيرًا**، التدريب على توفير جميع المهارات والمعارف الأساسية بالأمن لجميع الأطراف[٢].

وتحتاج برامج التوعية والتدريب للموظفين إلى معالجة مستويين رئيسين: **أولهما**، الموظفون الفنيون يتم اختيارهم من ضمن أصحاب المؤهلات العليا والعمل علي تحديث مهاراتهم في مجال الأمن الإلكتروني باستمرار، وانتقاء اصحاب الكفاءات منهم لإشراكهم في استراتيجيات الأمن[٣]؛ وذلك لأن تخطيط وتنفيذ استراتيجية فعالة للأمن الإلكتروني يعد من الأنشطة المعقدة للغاية والتي تتطلب معرفة متخصصة. وبناء عليه، يمكن أن يؤدي اغفال تدريب موظفي الأمن أو تدريبهم علي نحو سيئ إلى عدم كفاءة إدارة المخاطر الأمنية في تنفيذ استراتيجيات

---

(1) **Idem.**

(2) **Idem**; **R. Alavi, S. Islam & H. Mouratidis**, "A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS)". Op.cit., pp. 297-305.

(3) **Vince Farhat, et al.**, Prevention and Proactive Responses, Practical Law Publishing Limited and Practical Law Company, 2011. p. 4. Available at: https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf [Accessed 14 Aug. 2015].

الأمن الإلكتروني. بالإضافة إلى ذلك، فإن قدرة المؤسسات على الاستجابة والاسترداد وتلافي الاختراقات تعتمد بصفة أساسية على كفاءة الموظفين الفنيين(١).

وثانيهما، الموظفون غير التقنيين يجب أن يكون لديهم وعي كامل بدورهم في منع وتقليص التهديدات الإلكترونية. إذا ما تم تنفيذ ذلك بكفاءة، فسوف تعمل برامج الوعي الأمني Security Awareness على تحسين الاتصال بين الفرق المختلفة على جميع المستويات داخل المؤسسات مما يساعد على تحديد المشاكل الأمنية المحتملة، ويساعد أصحاب المصلحة على فهم عواقب سوء ممارسات الأمن في النظام، وضمان التنفيذ الموثوق للإجراءات الأمنية(٢).

المطلب الرابع
التحالفات الوطنية والمحلية

لقد سلط العديد من الأكاديميين والحكومات ومسئولي الاستخبارات في العديد من الدول الغربية الضوء علي عواقب الهجمات الإلكترونية التي تشنها المنظمات الارهابية علي الأمن الوطني(٣). لذلك وافق وزراء دفاع حلف شمال الأطلنطي على سياسة الناتو المتعلقة بالدفاع الإلكتروني من أجل تأسيس تحالف يمكن الاعتماد عليه وذلك بغرض مواجهة التهديدات الإلكتروني، وذلك في يونيو ٢٠١١.

وتشمل التحديات التي تواجه أعضاء الحلف على المستوى الوطني للتخفيف من الإرهاب الإلكتروني، عدة أنواع: أولها، تأمين مصادر البيانات داخل الحوسبات

(1) **Israa G. Seissa, et al.,** Op. cit., p. 184.

(2) **Idem.**

(3) **Maurice Dawson, et al.,** The Future of National and International Security on the Internet. In: A. Kayem & C. Meinel (eds.), Information Security in Diverse Computing Environments. 2014. pp. 149–178.

السحابية الوطنية والعالمية[١]. وثانيها، التعامل مع خفة الحركة المتزايدة لكل من أنظمة الأجهزة والبرمجيات، ثالثها، ضرورة إقامة تعاون دولي والتغلب على الصعوبات التي تواجه تنفيذ هذا التعاون على المستوي الوطني والمستوى الدولي[٢].

والجانب الأخير من هذه التحديات يتعلق بضرورة أن يكون هناك نوع من التنسيق بين الأنشطة الوطنية والعسكرية والمدنية والعمليات البشرية لتيسير تخفيف الإرهاب الإلكتروني[٣].

وفي هذا الصدد اقترح مكتب التحقيقات الفيدرالي[٤] عددا من المبادرات للتخفيف من الإرهاب الإلكتروني والتي تشمل: تطوير استراتيجيات شاملة للأمن

---

(١) يشير مصطلح الحوسبة السحابية Cloud computing إلى المصادر والأنظمة الكمبيوترية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية دون التقيد بالموارد المحلية بهدف التيسير على المستخدم وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطية والمزامنة الأوتوماتيكية كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الالكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تبسط وتتجاهل الكثير من التفاصيل والعمليات الداخلية. راجع:

د/ محمد شوقي شلتوت، الحوسبة السحابية بين الفهم والتطبيق، بحث منشور بمجلة التعليم الإلكتروني، بتاريخ الأول من يناير ٢٠١٦. على الرابط التالى:

http://emag.mans.edu.eg/index.php?sessionID=43&page=news&task=show&id=365

ولمزيد من التفاصيل حول الحوسبة السحابية وأنواعها، ومكوناتها، والفرق بينها وبين التخزين السحابي، راجع: د/ ممدوح على محمود، استخدام التخزين السحابي للبيانات في المكتبات ومراكز المعلومات وأمن المعلومات، بحث منشور على الرابط التالى:

https://platform.almanhal.com/Reader/2/84002

(2) **Dimitrios Choupis**, Challenges and Objectives for the National Cyber-Security Strategy Beyond 2020. Op. cit., p. 5.

(3) **Maurice Dawson, et al.,** DoD Cyber Technolog ..., pp.19–22.

(4) **FBI** (2012) FBI Information Sharing and Safeguarding Report 2012. US, FBI. Available at: https://www.fbi.gov/file-repository/stats-services-publications-national-information-sharing-strategy-1-fbi-information-sharing-and-safeguarding-report-2012/view

الإلكتروني تتماشى مع الرؤية الوطنية لمكافحة الإرهاب من ناحية. زيادة موارد الأمن الإلكتروني وقدراته على نحو كبير بما يمكنه من الدفاع عن الشبكات العاملة طوال أيام الأسبوع وعلى مدار الساعة من ناحية أخري. كما اقترح Choupis بضرورة إيجاد تعاون وتنسيق بين أنشطة البحث والتطوير للتعاطي مع التهديدات المستقبلية للإرهاب الإلكتروني(١).

وتتمثل إحدى استراتيجيات التخفيف من الإرهاب الإلكتروني الأخرى في تطوير التشريعات، وآليأت التدقيق المتعلقة بالأمن الإلكتروني والتي ينبغي أن تتماشى مع استراتيجيات حلف الناتو الأخرى. وفي هذا المجال يمكن أن يكون وجود قوة عاملة ماهرة تقنيًا وصاحبة مهارة على الإنترنت استراتيجية مهمة للتخفيف أيضًا (٢).

المطلب الخامس

التحالفات الدولية والتعاون الدولي

لما كانت هجمات الإرهاب الإلكتروني يتم تنظيمها بواسطة التحالفات والتعاون العالمي بين المنظمات الإرهابية، ومن ثم فإن مكافحة هذه الهجمات يجب أن تتم أيضا من خلال تحالفات على المستوي الدولي، كذلك يجب النظر بعناية نحو إنفاذ القانون الدولي على هذا النوع من الهجمات (٣).

ويتطلب إقامة تعاون دولي لمكافحة الإرهاب الإلكتروني بداية من وضع إطار واستراتيجيات سياسات لهذا التعاون. يتم من خلاله مراقبة وفحص مواقع

(1) ***Dimitrios Choupis***, Challenges and Objectives for the National Cyber-Security Strategy Beyond 2020. Op.cit, p. 6.

(2) **Ibid**. p. 8.

(3) **Macdonald, S., Jarvis, L., & Chen, T.**, A Multidisciplinary Conference on Cyberterrorism: Final Report, Cyberterrorism Project Research Report. Paper presented at the A Multidisciplinary Conference on Cyberterrorism, Swansea University, 2013.

الجماعات الإرهابية على شبكة الإنترنت ودراسة سلوكها الإلكتروني بالتوازي مع قيام المجتمع الدولي بعمليات متسقة لتبادل المعلومات الاستخبارية حول هذه المنظمات وتجميعها(١).

وتمثل نقطة البداية في بناء التعاون الدولي لمكافحة الإرهاب الإلكتروني في تجميع المعلومات الاستخباراتية حول المنظمات الإرهابية ومصادر تمويلها من أجل إنشاء مجمع استخباراتي "Intelligence Pool" تتقاسمه الدول المعنية. شريطة ألا يكتفي هذا المجمع برصد وجمع المعلومات من المواقع الشبكية الارهابية وإنما يعمل على جمع الأدلة الالكترونية عن الهجمات الإلكترونية المحتملة(٢). وفي سياق متصل أشار البعض إلي وجوب إنشاء شبكة معلوماتية يدرج بها كافة المعلومات الجيدة والمتحصلة من العمليات السابقة على أن تكون الحكومات الطرف الوحيد المسموح باستخدام هذا المورد(٣).

ومن الأساليب التي يمكن استخدامها في هذا الصدد أسلوب المراقبة Monitoring ومنهج التعطيل Disrupting. ويصلح الشكل الأول – أي المراقبة– لرصد المدونات ومواقع الإلكترونية الإرهابية المحدثة باستمرار وذلك لجمع المعلومات عن المنظمات الإرهابية مثل الدوافع، والعقليات، والجماهير، والخطط التنفيذية، والسكان المستهدفين، والأهداف المحتملة للهجمات. ويمكن ان يساعد "استخدام" البيانات المسترجعة هنا في الحصول على معلومات مفصلة عن الدعاية، والأعضاء، والصلات بين الأشخاص والمنظمات والبلدان التي تدعم الإرهابيين عن طريق التمويل والسياسة(٤).

---

(1) **Dogrul Murat, et al.,** Op. cit., p. 36.
(2) **Ibid**. p. 37.
(3) **Ahmed H. Anjariny et al.,** Op. cit., p. 6.
(4) **Idem.**

أما أسلوب التعطيل فيقوم على إصابه المواقع الإلكترونية الإرهابيه بواسطة الفيروسات والديدان لتدمير محتويات هذه المواقع(١). كما يمكن استخدام أسلوب المراقبة والرصد لفهم كيفية تغرير المنظمات الإرهابية بالشباب ودفعهم إلي براثن التطرف، ومن ثم يمكن إزاله التطرف بعد فهم أسبابه ودوافعه (٢).

وينبغي ان يقترن الدفاع الذي ستضطلع به هذه التحالفات بإنشاء شبكات تعاون واسعة النطاق. يمكن تصنيف التعاون إلى فئتين: الأولى، تشمل المنظمات أو المجموعات التي تستخدم نظما مماثلة أو التي تواجه تهديدات مماثلة؛ على سبيل المثال، التعاون بين مزودي خدمات الإنترنت (ISP). والثانية، هي مجموعة المنظمات التي تعمل في إطار من التطابق بين القانون الوطني والدولي، إذ ينبغي أن يعمل القانون الدولي على إنفاذ القوانين المتعلقة بالإرهاب الإلكتروني(٣).

اتساقا مع ذلك، يعمل حلف الناتو على سبيل المثال، على تسريع استجابته لخطر الهجمات الإلكترونية من خلال حماية أنظمة الاتصالات والقيادة الخاصة به، مما يساعد الأعضاء في الحلف على تحسين قدرتهم على منع الهجمات والتعافي منها، وتطوير مجموعة من قدرات الدفاع الإلكتروني التي يمكن أن تكشف الهجمات الإلكترونية وتردعها بفعالية (٤).

المطلب السادس

التعليم والتدريب وعلم النفس

(1) ***Thomas, T. L.,*** Al Qaeda and the Internet: Thedanger of "cyberplanning." Parameters, Spring 2003, pp. 112-123.

(2) **Dogrul Murat, et al.,** Op.cit., pp. 37-38.

(3) **Shinde, V. N.**, Challenges and Opportunities Created by Terrorism: Present Scenario. Online International Interdisciplinary Research Journal, Vol. 2, 2013. pp. 202-209.

(4) **NATO (2010) NATO 2020**, Assured Security; Dynamic Engagement Analysis and Recommendations of the Group of Experts on A New Strategic Concept for NATO. Experts Report on New Concept. NATO.

تظهر أهمية البرامج التعليمية والتدريبية التي تركز على أمن المعلومات في أنها يمكن أن تساعد الحكومات والقطاعات الصناعية والمنظمات المختلفة في ردع الإرهاب الإلكتروني. وقد قامت وكالة الأمن القومي الأمريكي (NSA) بالتعاون مع وزارة الأمن الداخلي (DHS) بالرعاية المشتركة لمركز التمييز الأكاديمي في تعلم تأمين المعلومات Center of Academic Excellence in Information Assurance Education (CAEIAE) ، باعتماد مناهج دراسية لمده عامين، ولمدة أربع سنوات، والدراسات العليا وبرامج البحوث. والغرض الرئيسي من هذه البرامج هو إعداد محللين ومديرين وصانعي سياسات لديهم الجاهزية والقدرة على التصدي للأخطار الحالية والمستقبلية التي تهدد الأمن القومي [١].

وفي هذا الصدد أشار البعض إلي ضرورة تتخذ البرامج الأكاديمية المتعلقة بأمن المعلومات نهجا جديدا يمكن الدارس في نهاية المطاف من مواجهة التهديدات الإلكترونية المتطورة والاستجابة لها؛ لأن الأمن الإلكتروني لا يعتمد على الحلول التكنولوجيا فقط وإنما يشمل مجموعة من العمليات الأخري، ومن ثم يجب أن يكون الرد على مختلف التحديات الأمنية ليس تقنيًا فقط، وبالتالي يتعين أن تشمل هذه البرامج العديد من التخصصات مثل الدفاع الوطني، والاقتصاد، وعلم الاجتماع، والعلوم السياسية، والدبلوماسية، والتاريخ [٢]. كذلك ينبغي أن يتعرض الطلاب لمختلف التخصصات مثل الإرهاب، الاستخبارات، وتحليل التهديدات، ووضع السياسات، والتخطيط الاستراتيجي، والإدارة، وتحليل المخاطر والتخفيف من آثارها [٣].

المبحث الثالث

(1) **Jim Ramsay, et al.**, Op. cit., p. 4.

(2) **Christopher Beggs & Matthew Butler**, "Developing new strategies to combat cyber-terrorism". In: M. Khosrow-Pour (eds.), Innovations Through Information Technology, Australia, Idea Group Inc. 2004. p. 390.

(3) **Jim Ramsay, et al.**, Op. cit., p. 13.

إدارة عواقب حوادث الإرهاب الإلكتروني

هناك بديلان رئيسان في هذه المرحلة من مراحل الدفاع: أولهما، الاستعادة Recovery وتدور حول إعادة تكوين أصول تكنولوجيا المعلومات بحيث يمكن للمؤسسة التي تعرضت لهجمات الإرهاب الإلكتروني أن تعمل أقرب ما تكون إلى طبيعتها – قدر الإمكان– في أقرب وقت ممكن، وهو الشكل السلبي للدفاع. ثانيهما، الاستجابة Response وهي المعنية بتحديد ومعاقبة الجناة، ووضع دروس التعلم لتمكين المنظمة من الدفاع عن نفسها بشكل أفضل في المستقبل، هو بالتالي شكل أكثر نشاطًا للدفاع[1].

وتندرج ضمن طائفة استعادة ما كانت عليه المؤسسة قبل الهجوم الإرهابي عينة من الهام تتمثل في الأتي:

- إزالة أو إيقاف الكيانات المعادية أو المعيبة.
- مسح تقييم الأضرار لما تم كسره، أو تغييره، أو ما هو غير ذلك.
- عملية آلية أو شبه آلية لتقييم وتقنين وإعادة توزيع ما يتم تصحيحه بسرعة فعالة.
- تحديد أولويات الوظائف التي يعاد تشكيلها.
- إعادة الحالة إلى ما قبل الحادث أو قبل الهجوم دون تدمير الأدلة.

وتجدر الإشارة إلي أن التعافي من تأثير الهجمات الإلكترونية ليس سهلًا بل قد يكون بعيد المنال، وذلك إذا ما تم تصميم الهجمات الإلكترونية وتنفيذها بعناية فائقة. على سبيل المثال، قد يؤدي تنفيذ الهجمات الإلكترونية أو إدراج شفرة خبيثة بشكل متكرر على مدى فترات زمنية طويلة بواسطة المتسللين إلي تدمير البيانات بحيث يكون من الصعب معرفة مكان يتم العثور فيه على نسخة احتياطية غير ملوثة. يمكن أن يحدث مثل هذا الفساد على مدى فترة زمنية طويلة، مع إضافة

(1) **Seymour E. Goodman**, Cyberterrorism and Security Measures …, Op. cit., p. 50.

العديد من المعاملات المشروعة التي لا يرغب المالك في خسارتها أثناء فترة النقاهة. وحتى الآن، يبدو أن معظم المنظمات التي عانت من هجمات قصيرة المدي تمكنت من استعادة عافيتها بسرعة وفعالية، أو على الأقل لا يتحدثوا عن فشلهم في هذا الصدد.

وتشمل المهام التي يمكن أن تندرج تحت طائفة الاستجابة ما يلي:

• الحصول على الجاني الصحيح: أشكال قوية من التتبع الدقيق للخلفية، وأدوات الطب الشرعي، وربما أنواع من "بالصمات".

• الانتقام بشكل مدروس: المبادي القانونية للانتقام المتناسب والمتكافئ.

• عدم التناظر: ما يجب فعله بشأن المهاجمين الذين لديهم القليل من أصول تكنولوجيا المعلومات أو نقاط ضعف ؟

• التصعيد: تقييم الأضرار التي لحقت بالمؤسسة، ثم اتخاذ القرار بما إذا كان ذلك يستدعي توجيه رسالة قوية جدا أم أقل حدة ؟!

وكما كان الحال في مناقشة أسلوب المنع، فإن بعض السمات الفريدة للإرهابيين ذوى التأثير الكبير تجعل الانتقام أكثر صعوبة، بالرغم من أن الانتقام من الإرهابيين يبدو أشد إلحاحًا من الحالات التي نكون فيها بصد مجرم إلكتروني أو جواسيس صناعيين أو وكلاء للحكومات الأجنبية. فمن المحتمل أن يكون الإرهابيون أشخاصًا خطرين بشكل خاص ينوون الاستمرار في ارتكاب المضايقات والأفعال الضارة. هنا من المفترض في هذه المرحلة أن نعرف أننا تعرضنا لهجوم شديد من قبل الإرهابيين.

وقد قام جودمان[١] في بحثه القيم حول الإرهاب الإلكتروني وإجراءات الأمن، بتقييم موجز للقدرات الشاملة للولايات المتحدة الأمريكية للتعامل مع

(1) **Ipid.** pp. 50-51.

الإرهابيين باستخدام الفضاء الإلكتروني، وقد خلص إلي أنه بالنسبة لمعظم الأهداف التي أشار إليها الكتاب فهي محتملة من الناحية التكنولوجية والإجرائية، ففي كل جانب من المراحل الثلاثة للدفاع الإلكتروني لن يجدي الردع بسهولة مع المهاجمين المهرة، والأقل درجة، والمصممين على ارتكاب المضايقات والأفعال الضارة، وعلى الرغم من المناقشات المستفيضة والبحوث الدائمة المتعلقة بمكافحة الإرهاب الإلكتروني، إلا أن هناك نقص كبير في التقدم صوب التطبيق الواسع للتكنولوجيا الأمنية[١]. ففي كل مرة يبحث فيها المهاجمون داخل النظم الأمنية سيجدون نقاط ضعف، حتي أن النظم الأكثر تعقيدًا لن يغلب المهاجمون في أن يجدوا ثغرات فيها، أو قد يؤدي إصلاح ما بها من ثغرات إلي حدوث ثغرات جديدة، إذ لا يزال عدد الهجمات الناجحة – التي لم تخلف ضحايا من البشر – في اضطراد مستمر على

---

[١] حول هذه الأبحاث، راجع:

Computer Research Associates. November 16-19, 2003. Four Grand Challenges in Trustworthy Computing. Washington, D.C. Available at: http://www.cra.org/Activities/grand.challenges/security/

Advanced Research Projects Agency. 2003. Advanced Technology Office, Program Overview: Information Assurance. Briefing for the National Security Telecommunications Advisory Committee, December 16, 2003. Several Defense Advanced Research Projects Agency offices have extensive research and development agendas related to cybersecurity. Available at: http://www.ncs.gov/NSTAC/nstac.htm

Institute for Information Infrastructure Protection. 2003. Cyber Security Research and Development Agenda. Hanover, NH. Available at: http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf

National Research Council. 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Academy Press, Washington, D.C. at: http://www.nap.edu/html/stct/

President's National Security Telecommunications Advisory Committee (NSTAC), the White House Office of Science and Technology Policy (OSTP), and the Georgia Tech Information Security Center (GTISC). May 13-14, 2003. Research and Development Exchange Proceedings: Research and Development Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness. Georgia Institute of Technology, Atlanta, GA. at: http://www.ncs.gov/nstac/r&d2003theme.html

الأقل بنفس سرعة نمو واتساع شبكة الإنترنت. ففي عام ٢٠٠٣ كان عدد الهجمات التي تسببت في نشر الديدان والفيروسات والبريد العشوائي كانت قريبة من الاعوام الماضية إلا أن اللافت للنظر أنها لم تستخدم التكنولوجيات القديمة ككلمات المرور والجدران النارية على نطاق واسع وفعال، وإنما استخدم في الكثير منها الاختراقات على الرغم من الوعي المتزايد بالمشاكل والاحتياجات الأمنية.

والواقع أن جزءًا من المشاكل التي تعوق مكافحة الإرهاب الإلكتروني والقضاء عليه هو مزيج من الاتصال الهائل بالشبكة الدولية مع التركيز على وصول واسع النطاق لمستخدمي الإنترنت، وعدد كبير من المالكين والمشغلين ومستخدمي الفضاء الإلكتروني مع احتياجات ودوافع وموارد متنوعة، ومجال الهجمات الفاعلة أكبر بكثير وأكثر تنوع مما هو عليه الحال مع القضايا الأمنية التقليدية. وذلك في ظل ندرة وجود أنظمة فعالة للأمن باستثناء في مناطق قليلة فقط، وتشتمل الأنظمة الأخيرة بالطبع على تقنيات التشفير عالية جدًا وبرمجيات عالية الكفاءة لمكافحة الديدان والفيروسات وهجمات الحرمان من الخدمة الموزعة المشابهة لتلك التي تمت مواجهتها بالفعل ومحدثة باستمرار وشكل دائم.

وفي هذا الصدد ثار التساؤل الآتي: هل الفضاء الإلكتروني أصبح الأن أكثر أمانًا عما كان عليه الحال منذ ست سنوات أو العشر سنوات الماضية ؟

الإجابة قطعًا تكون بالنفي؛ لأن النمو الذي شهدته شبكة الإنترنت في هذه الفترة سواء في الحجم أو الاتساع ترتب عليه تنوع البرامج. بالإضافة إلي الزيادة في تعداد المتصلين الجدد وهو ما جلب بطبيعة الحال مواطن ضعف إضافية ناتجة عن هذا الاتصال، مما يفوق على الأرجح الأمان الإضافي الذي تفرضه المؤسسات والأفراد.

لذا نجد العديد من البلدان قد أولت اهتماما واضحا للخطط أو الاستراتيجيات الوطنية لتأمين الفضاء الإلكتروني[١]. لكن بالاطلاع على الاستراتيجية الوطنية الأمريكية لحماية الفضاء الإلكتروني والتي يتم تحديثها باستمرار نجدها إلي الأن طوعية إلى حد كبير وموحية في نفس الوقت، إلا أنها لم تؤد إلي تحسينات كبيرة سواء داخل الحكومة الأمريكية أو في البنية التحتية الوطنية للمعلومات التي تملكها وتديرها بشكل خاص الحكومة الفيدرالية[٢].

وفي هذا الشأن أعتقد أن هناك ثلاثة مجالات تكنولوجية هامة أغفلتها هذه الاستراتيجية كانت تتطلب الاهتمام الفوري للتعامل مع الإرهاب المحتمل – الشديد التأثير–: **أولها**، التكنولوجيا المستخدمة لجمع وتقييم فعالية المعلومات الاستخبارية. **وثانيها**، التكنولوجيا المستخدمة في نظم التحكم وإدارة الهياكل المادية للبني التحتية الحرجة والاتصالات السلكية واللاسلكية المعروفة بـ SCADA بما يجعلها أكثر أمانًا. **وثالثها**، يتعلق بتحسين قدرات أمن تكنولجيا المعلومات للمتلقين لحالات الطوارئ.

وفي النهاية يجب على أولئك الذين يسعون إلى اتخاذ تدابير لمكافحة الإرهاب أن يضعوا في الاعتبار أن الإرهابيين يمكن ان يختبئوا بسهوله داخل المجتمعات التي ينوون استهدافها، متجنبين التعرض إلى أن ينفذوا فعلا هجوما. وذلك ينطبق على الفضاء المادي والفضاء الإلكتروني على حد سواء، وبالتالي فإن مكافحة الإرهاب في كل من الفضاء المادي والفضاء الإلكتروني تعتمد بالضرورة على كثافة المعلومات الاستخباراتية.

---

(1) **Stephen J. Lukasik et al.**, Protecting Critical Infrastructures Against Cyber-Attack, Adelphi Paper 359, International Institute for Strategic Studies, London, 2003.

(٢) راجع:

The White House, The National Strategy to Secure Cyberspace (Washington, DC: The White House, February 2003). Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

كما أن الإرهابيين المسافرين للانخراط في الأنشطة الإرهابية من الطائفة الأولي والتي تضم العديد من الأشخاص لا يهتمون صراحة بما يمكن تسميته بالإرهاب الإلكتروني، وفي إطار الفئة الثانية والثالثة للإرهابيين نجد المستخدمين للإنترنت هؤلاء قد يكشفون عن أنفسهم في الفضاء الإلكتروني الذي يشاركهم فيه بطبيعة الحال من يضطلعون بمكافحة الإرهاب. لذا من المحتم أن يتعلم من يكافح الإرهاب الاستفادة من هذا التعرض بشرط أن يمارس ذلك دون المساس المفرط بالحريات المدنية أو الحقوق الشخصية مثل الحق في الخصوصية لكل من ليس إرهابيًا.

الخاتمة

وبعدُ ... يِنْتَهِي بِنَا المطافُ في شَأْن دراستنَا للإرهاب الإلكتروني ذلك الموضوع الذي شغل بال المهتمين بالجرائم الإلكترونية والمتخصصين في مكافحة الإرهاب. بعد أن بات الإرهاب الإلكتروني هو الخطر الجديد الذي يهدد العالم بأسره في عصر المعلوماتية. وقد أبرزت الدراسة مفهوم الإرهاب الإلكتروني وأسباب ظهوره وأشكاله، وكذلك الأدوات التي يستخدمها، وتأثيره على الأمن القومي للدول ومنها مصر، وكيف أنه يشكل تهديدا أمنيا وسياسيا واقتصاديا واجتماعيا؛ ما يهدد الأمن القومي بشكل عام، بالإضافة لبيان صور جريمة الإرهاب الإلكتروني في التشريعات المقارنة، وأخيرا استراتيجية مكافحته والتصدي له.

وقد خلصنا في نهاية دراستنا لموضوع السياسة الجنائية في مواجهة الإرهاب الإلكتروني إلي جملة من النتائج [1] والمقترحات نتناولها على التفصيل التالي:

أولًا: النتائج:

(٠١) كشفت الدراسة عن خطورة الإرهاب الإلكتروني على جميع دول العالم الذي أصبح عرضة للهجمات التخريبية بواسطة الإرهابيين عبر توظيف الطبيعة المفتوحة للوسائل الإلكترونية، لتنفيذ أنشطتهم الإجرامية، مستفيدين من التقدم الهائل لتكنولوجيا المعلومات والاتصالات وتطور الحاسبات الآلية. لكن الجدل ثار حول تحديد ماهية الإرهاب الإلكتروني ولعل ما أسهم في إذكاء هذا الجدل هو تطور مفهوم الإرهاب على مدار السنوات الأخيرة حتي أصبحت الأنشطة الإلكترونية – أيًا كان نوعها – يتم إدراجها في إطار المعني الواسع للإرهاب.

وقد عرضت الأراء التي تناولت الإرهاب الإلكتروني، وبالرغم من اختلافها في التفاصيل إلا أن النتيجة التي انتهت إليها واحدة وهي أن الإرهاب الإلكتروني يتعلق بالاعتداء على البنية التحتية للنظم المعلوماتية. وخلصت إلى تعريف الإرهاب

---

[1] غني عن الإيضاح أن خاتمة الدراسة لا تحتل سرد كافة النتائج التي انتهينا إليها في كل جزئية من جزئيات البحث؛ لذا سنكتفي بإبراز النتائج التي تمثل معالم رئيسة لموضوع الدراسة.

الإلكتروني بأنه: « الأفعال أو الأنشطة التي يقوم بها أفراد أو جماعات باستخدام تكنولوجيا المعلومات وشبكة الإنترنت، بقصد إحداث دمار للبنى التحتية المرتبطة والمدارة بواسطة هذه التكنولوجيا، والتي من شأن تدميرها أن يحدث أضرارًا مباشرة وغير مباشرة بالمواطنين والدول».

(٠٢) توصلت الدراسة إلى أن جرائم الإرهاب الإلكتروني ما هي إلا امتداد للجرائم الإرهابية التقليدية، بل هي النسخة الإلكترونية لها، وأن هناك رابطة مشتركة بين جرائم الكمبيوتر والإنترنت وجرائم الإرهاب الإلكتروني في أن كل منهما جرائم وأن محل ارتكاب الجريمة في كليهما واحد هو البيئة الإلكترونية، وأن كلاهما قد يوجه ضد فرد أو منظمة أو دولة. لكنهما يختلفان في الدافع، ففي الجرائم الإلكترونية يكون الدافع في أغلب الأحوال تحقيق الكسب المادي أما في جرائم الإرهاب الإلكتروني يكون الدافع سياسي أو اجتماعي أو اقتصادي وصولًا إلى زعزعة استقرار الدول وتدمير البنية التحتية المستهدفة، كذلك يختلفان في النتيجة، فالإرهاب الإلكتروني قد يخلف نتائج جد خطيرة مثل الوفاة أو الإضرار المادي بالأشخاص أو الممتلكات أو يترك أثارًا مدمرة تشيع الرهبة في النفوس بخلاف الجرائم الإلكترونية فهي لا تخلف مثل هذه النتائج؛ لأنها يغلب عليها الاعتداء على الجانب المالي أو المعنوي للأشخاص.

(٠٣) بينت الدراسة الأسباب التي أدت إلى ظهور الإرهاب الإلكتروني وانتشاره، ولعل أهمها ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق؛ نظرًا لتصميمها بشكل مفتوح ورغبة في التوسع وتسهيل دخول المستخدمين، واحتوائها على ثغرات معلوماتية تسمح بالتسلل وممارسة الأنشطة التخريبية، فضلا عن عدم وضوح الهوية الرقمية للمستخدمين، وصعوبة اكتشاف الجرائم الإرهابية الإلكترونية، وسهولة الاستخدام التقني وقلة التكلفة المادية مقارنة بالجريمة الإرهابية التقليدية، بالإضافة إلى الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والذي يعتبر من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني. لكل

هذه الأسباب أصبح الإرهاب الإلكتروني هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية، بل وبعض الأفراد المرضى.

كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على شبكة الإنترنت وتسيطر على مدخلاتها ومخرجاتها يعدُّ سببًا مهمًا في تفشي ظاهرة الإرهاب الإلكتروني، حيث يمكن لأي شخص الدخول ووضع ما يريد على هذه الشبكة، وكل ما تملكه سلطات إنفاذ القانون هو رصد هذه المواقع لمنع الوصول إليها وذلك بحجبها أو إغلاقها أو تدميرها.

(٠٤) بينت الدراسة الأدوات المستخدمة في عمليات الإرهاب الإلكتروني، ولعل أهمها القرصنة والفيروسات بمختلف أنواعها، وهجمات الحرمان من الخدمة، وتشويه مواقع الويب للجهات الحكومية، واستخدام تقنيات التشفير ذوو التردد العالى. بالإضافة إلى استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات والتنسيق فيما بينهم.

(٠٥) كشفت الدراسة عن الوجهات المختلفة لهجمات الإرهاب الإلكتروني، ولعل أهم الجهات المستهدفة هي القوات المسلحة والأهداف العسكرية المرتبطة بشبكات المعلومات. وتصنف الهجمات التي تستهدف المنظومة العسكرية من أخطر سيناريوهات الإرهاب الإلكتروني، وتبدأ المرحلة الأولي منها باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي، والصواريخ النووية، وتتعاظم الخطورة إذا سنحت الفرصة للارهابيين في فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة.

ولا تقل خطورة عن الهجمات السابقة الهجمات التي تستهدف البني التحتية الحيوية بالدولة مثل أنظمة معالجة المياه، أنظمة تشغيل السدود، أنظمة الاتصالات، ومرافق الطاقة، والخدمات الدولية، وخدمات الطوارئ ... إلخ في ظل اعتماد الدولة في إدارة بنيتها التحتية الحيوية وسائر مرافقها الاستراتيجية على أجهزة الكمبيوتر

ونظم المعلومات والبرمجيات والاتصالات حيث ينشأ عن مثل هذه الاعتداءات تعطيل مرافق الحياة بالدولة المستهدفة وسيادة الفوضي.

(٠٦) أثبتت الدراسة استغلال مجرمي الإرهاب الإلكتروني غياب السيطرة والرقابة على الشبكة المعلوماتية في إنشاء مواقع على شبكة الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية. بالإضافة إلى استخدم هذه المواقع في نشر كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية، وشرح طرق اختراق البريد الإلكتروني، وكيفية الدخول إلى المواقع المحجوبة، وتعليم طرق نشر الفيروسات ... إلخ. وعندما تنبهت الحكومات الغربية إلى خطورة انتشار الفكر المتطرف على المواقع والصفحات الإلكترونية وما أسفر عنه من تجنيد تنظيم داعش لمقاتلين أجانب وتوجيههم للقيام بأعمال إرهابية داخل الدول التي ينتمون إليها قررت عدد من هذه الحكومات ازالة المحتوي المتطرف من على شبكة الإنترنت.

ونتيجة للرقابة الإلكترونية الأمنية وعمليات الرصد والتتبع لمواقع الجماعات الإرهابية على شبكة الإنترنت السطحية في الفترة الأخيرة وتحديدًا عقب عملية باريس وما أسفر عنها من إزالة المئات من هذه المواقع، توجهت الجماعات والتنظيمات المتطرفة نحو استخدام شبكة الويب المظلمة؛ للتواصل فيما بينها، والقيام بنشر أفكارها، وتجنيد الشباب من خلال غرف الدردشة المنتشرة على هذه الشبكة، إضافة إلى إنشاء مواقع وتطبيقات داخل الشبكة المظلمة لجمع التبرعات المالية غير المشروعة لتمويل هذه التنظيمات، وإن كانت لا تزال المنتديات وغرف الدردشة باللغتين الإنجليزية والفرنسية تتوافر على نطاق واسع على شبكة الويب السطحية، إلا أن الجزء الأكبر من الخطاب المتطرف يحدث حاليا داخل الشبكة المظلمة.

وقد ذهبت الجماعات والتنظيمات الإرهابية إلى ما هو أبعد من مجرد استخدام مواقع الشبكة المظلمة، إذ عمل تنظيم «داعش» على تطوير قدراته التقنية في الشبكة المظلمة، حيث أطلق في يناير ٢٠١٥ تطبيقًا مشفرًا عبر هذه الشبكة

ومن خلال روابط سرية يتداولها أفراد التنظيم بهدف ترويج دعايته الإعلامية والأخبار ومقاطع الفيديو، والذي يصعب الوصول إليه أو ملاحقته أو مراقبة محتواه من قبل الحكومات والجهات الأمنية بسبب درجات الأمان وتعقيدات الشبكة المظلمة.

(٠٧) بينت الدراسة تجريم المشرع الفرنسي الإعتداءات على المواقع الإلكترونية والنظم المعلوماتية وذلك من خلال حظر الدخول أو البقاء غير المشروع على المواقع الإلكترونية باعتباره بوابة المرور لارتكاب سائر الجرائم الإلكترونية ومنها جرائم الإرهاب الإلكتروني مقررًا عقوبة الحبس مدة سنتين والغرامة التي مقدارها ٦٠ ألف يورو، كما شدد المشرع العقوبة على الجاني إذا ما نشأ عن هذا الدخول محو أو تعديل في البيانات المخزنة في النظام المعلوماتي، أو إتلاف تشغيل النظام لتصبح العقوبة الحبس لمدة ثلاث سنوات وغرامة قدرها ١٠٠ ألف يورو. كما نص على ظرف تشديد بتوافره ترتفع العقوبة السابقة إلى الحبس خمس سنوات والغرامة إلى ١٥٠ ألف يورو وذلك في حالة الدخول غير المشروع على نظام معالجة البيانات الشخصية تنفذه الدولة (المادة ٣٢٣-١ عقوبات).

من ناحية أخري جرم المشرع الفرنسي إتلاف المواقع الإلكترونية حيث عاقب كل من أفسد أو إعاق نظام المعالجة الآلية للبيانات بالحبس خمس سنوات وغرامة قدرها ١٥٠ ألف يورو. في حين شدد العقوبة إلى الحبس لمده سبع سنوات وغرامة قدرها ٣٠٠ ألف يورو إذاما ارتكبت الجريمة ضد نظام للمعالجة الآلية للبيانات الشخصية تنفذها الدولة (المادة ٣٢٣-٢ عقوبات).

(٠٨) كما جرم المشرع الأمريكي الدخول المتعمد غير المشروع إلى الحاسبات الآلية التابعة للحكومة الفيدرالية الأمريكية ولو لم يحدث ضرر (المادة ١٠٣٠ (a) (1) من قانون الاحتيال وإساءة استخدام الحاسبات الآلية لسنة ١٩٨٦)، كما جرم هذا القانون الدخول المتعمد غير المشروع إلى الحاسبات الآلية أو تجاوز القدر المصرح به للدخول للحصول على معلومات مخزنة في السجلات لمؤسسة مالية، أو معلومات تخص أحد الوزارات أو المصالح الحكومية للولايات المتحدة

الأمريكية، أو معلومات مخزنة في حاسب آلي محمي إذا تضمن هذا السلوك اتصالات بينية عبر الولايات أو اتصالات أجنبية (المادة ١٠٣٠ (a) (2) من قانون الاحتيال وإساءة استخدام الحاسبات الآلية).

أما على مستوي الولايات فنجد أن معظم الولايات لديها تشريعات تعتبر الدخول إلى أنظمة الكمبيوتر أو الشبكات بدون ترخيص جريمة وهي ما تعرف بتشريعات القرصنة، كذلك تقرر معظم الولايات عقوبات مشددة على الدخول غير المشروع بقصد إلحاق الضرر أو تعطيل عمل النظام أو الإضرار بأية صورة بالنظام أو المعطيات.

(٠٩) كذلك جرم المشرع المصري إنشاء المواقع الإلكترونية أو استخدامها في الترويج الإرهابي أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو الأعمال المتعلقة بأعمال أو تحركات الإرهابيين في الداخل أو الخارج (المادة ١/٢٩ من قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥). كما جرم الدخول غير المشروع لموقع إلكتروني تابع لأية جهة حكومية بقصد الحصول على البيانات أو المعلومات أو الاطلاع عليها ... إلخ، من أجل ارتكاب جريمة الترويج الإرهابي أو تضليل السلطات الأمنية أو التأثير في سير العدالة في شأن جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو الأعمال المتعلقة بأعمال أو تحركات الإرهابيين في الداخل أو الخارج (المادة ٢/٢٩ من قانون مكافحة الإرهاب).

(١٠) كما جرم المشرع الإماراتي الدخول بغير تصريح على المواقع الإلكترونية أو النظم المعلوماتية إذا كان الدخول بقصد الحصول على بيانات حكومية أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية (المادة ٤ من المرسوم الاتحادي بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الاتحادي)، كما شدد المرسوم العقوبة على الجاني إذا ما نشأ عن هذا الدخول تعرض البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف ... إلخ (المادة

٢/٤)، كما جرم أيضًا الدخول بغير تصريح لموقع إلكتروني بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه (المادة ٥).

وإدراكًا لخطورة المواقع الإلكترونية في نشر الفكر المتطرف جرم المشرع الإماراتي إنشاء المواقع الإلكترونية أو استخدامها في الترويج الإرهابي، أو لتسهيل الاتصال فيما بين الإرهابيين أو للاستقطاب والتمويل، أو استخدامها في نشر أساليب تصنيع الأجهزة الحارقة والمتفجرات، أو أي أدوات أخري تستخدم في الأعمال الإرهابية (المادة ٢٦ من المرسوم الاتحادي بقانون رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات الاتحادي).

(١١) كذلك جرم المنظم السعودي الدخول غير المشروع إلى المواقع الإلكترونية، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه أو تعديله أو شغل عنوانه (المادة ٣ من نظام مكافحة الجرائم المعلوماتية الصادر بموجب المرسوم الملكي رقم ١٧ لسنة ١٤٢٨ هـ). وقد شدد العقوبة على الجاني إذا ما نشأ عن الدخول غير المشروع إلغاء البيانات أو تدميرها أو إتلافها أو تغييرها أو إعادة نشرها، أو في حالة إيقاف الشبكة المعلوماتية عن العمل أو تعطيلها أو تدميرها، أو إذا حصل إعاقة في الوصول إلى الخدمة أو تشويشها أو تعطيلها (المادة ٥). كما جرم الدخول غير المشروع إلى موقع إلكتروني، أو أي نظام معلوماتي بغرض الحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني (المادة ٧). وقد شدد النظام العقوبة على الجاني إذا ما قام بارتكاب أحد الأفعال المنصوص عليها في المادة السابقة من خلال عصابة منظمة (المادة ٨)

وإدراكًا لخطورة المواقع الإلكترونية في نشر الفكر المتطرف جرم المنظم السعودي إنشاء المواقع الإلكترونية أو استخدامها في الترويج الإرهابي، أو لتسهيل الاتصال فيما بين الإرهابيين أو للاستقطاب والتمويل، أو استخدامها في نشر أساليب تصنيع الأجهزة الحارقة والمتفجرات، أو الأدوات التي تستخدم في الأعمال الإرهابية

(المادة ٧). وقد شدد المنظم العقوبة على الجاني إذا ما قام بارتكاب أحد الأفعال المنصوص في المادة السابقة من خلال عصابة منظمة (المادة ٨)

(١٢) بينت الدراسة الاستراتيجية الشاملة للدفاع عن الأنظمة المعلوماتية والتي يمكن استخدامها في مكافحة الأنشطة الإرهابية، وتنقسم هذه الإستراتيجية إلى ثلاث مراحل: الأولي، الوقاية والمنع ويطرح فيها الخبراء أساليب متعددة لمنع الهجمات الإرهابية منها أسلوب البحث الذاتي عن الثغرات الأمنية ومعالجتها قبل أن يشرع الإرهابيون في استغلالها، واسلوب فحص الموظفين المحتمل تواطؤهم مستقبلا في الهجمات، بالإضافة إلى أسلوب التجريم من خلال تصنيف الهجمات الإلكترونية للإرهابيين ضمن الأعمال الإرهابية.

المرحلة الثانية، إدارة حوادث الإرهاب الإلكتروني والتخفيف من حدتها عبر عدد من الحلول يأتي في مقدمتها تطوير تشريعات الأمن السيبراني لضمان تصميم وتنفيذ أحدث السياسات المحلية والدولية في الأمن الإلكتروني، والمواجهة الفنية عبر الأنظمة التكنولوجية مثل تطبيق الجدران النارية، حماية كلمات المرور، وتشفير المفاتيح السرية، وتشفير المفاتيح العامة، التخطي، أنظمة كشف التسلل عالية الدقة، تشفير البيانات داخل الشبكة باستخدام IPSec، وقوائم التحكم في الوصول وغيرها من بروتوكولات الأمن، أضف إلى رفع مستوي الوعي الأمني لدي الموظفين عبر برامج التوعية والتدريب، وتحفيزهم ليكونوا أكثر ميلا للمشاركات في السياسات الأمنية. بالإضافة إلى إقامة التحالفات الوطنية والمحلية والدولية وإيجاد نوع من التعاون الدولي لمكافحة الإرهاب الإلكتروني، والتغلب على الصعوبات التي تحول دون تنفيذ هذا التعاون على المستوي الوطني والمحلي، والتنسيق بين أنشطة البحث والتطوير للتعاطي مع التهديدات المستقبلية للإرهاب الإلكتروني.

المرحلة الثالثة، إدارة عواقب حوادث الإرهاب الإلكتروني وتعمل إلى استعادة الهدف المصاب لما كان عليه قبل الهجوم الإرهابي بإزالة وإيقاف الكيانات المعادية وتقييم وتقنين الأوضاع الحالية وتصحيحها، واستخلاص الدروس المستفادة من نجاح

الهجوم؛ لتمكين الإدارة أو المنظمة أو المؤسسة ... إلخ من الدفاع عن نفسها بشكل أفضل في المستقبل.

ثانيًا: التوصيات:

في ضوء ما أسفرت عنه الدراسة من نتائج نود أن نسوق بعض التوصيات التي قد تساعدنا في التعامل مع الإرهاب الإلكتروني والتقليل من أثاره السلبية؛ وذلك لأنه من الصعب القضاء عليه بشكل كامل نتيجة ارتباطه بالتطور التكنولوجي. ومن أهم التوصيات:

١- نظرًا للطبيعة المتعدية الحدود لجرائم الإرهاب الإلكتروني، ولما تثيره من مشكلات قانونية، يتعين على الدول التدخل على محورين: أولهما، محلي من خلال ملاءمة تشريعاتها مع هذا النوع الجديد من الجرائم. وثانيهما، دولي عن طريق تنسيق جهود الدول نحو وضع تعريف موحد تحت مظلة الأمم المتحدة للإرهاب بصفة عامة والإرهاب الإلكتروني بصفة خاصة، والتعاون والاتفاق بين الحكومات على سن قوانين وعقوبات لمرتكبي جرائم الإرهاب الإلكتروني، وإبرام اتفاقيات جماعية وثنائية على حد سواء، مع تفعيل اتفاقيات تسليم المجرمين في جرائم الإرهاب الإلكتروني.

٢- ضرورة تعديل قوانين الإجراءات الجنائية، بالقدر الذي يسمح ببيان الأحكام اللازم اتباعها حال تفتيش الحاسبات، وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتي يستمد الدليل مشروعيته، ووضع صيغة تشريعية وفنية لسد ثغرات هذه الجريمة ومنع مرتكبيها من الإفلات من العقاب.

٣- حث الدول على المصادقة والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة الإرهاب بجميع صوره، وذلك لتجاوز الصعوبات التي تطرحها بعض مبادئ القانون الجنائي الداخلي، خاصة مبدأ الإقليمية وما ينجم عنه من تنازع للقوانين الوطنية بين مجموعة من الدول.

٤- أهمية وضع إستراتيجية وطنية شاملة في مجال مكافحة الإرهاب الالكتروني، تعمل على تنسيق وتوحيد الجهود بين أجهزة الدولة المختلفة، ووضع سيناريوهات لمواجهة أي هجمات إلكترونية محتملة تتعرض لها البلاد والتعامل معها، بالإضافة إلى التعاون والتنسيق بين القطاعين العام والخاص في التصدي للإجرام والإرهاب الإلكتروني.

٥- تأهيل الموظفين المكلفين بإنفاذ القانون عن طريق تطوير معلوماتهم في مجال تكنولوجيا المعلومات، وتحديث أساليب البحث والتحري عن الأدلة في هذا النوع من الجرائم ليتسنى لهم مواكبة ورصد الأنماط السلوكية المستحدثة، وذلك عن طريق برامج تداريب عملية وفعالة، واستحداث أجهزة متخصصة بمكافحة الإجرام المعلوماتي.

٦- إنشاء إدارات لمكافحة الإرهاب الإلكتروني في أنظمة الأمن خصوصًا في الدول التي تشهد تقدم مضطرد في اعتمادها على تكنولوجيا المعلومات والاتصالات، خاصة وأن التطور الحاصل في هذا المجال يتسارع والثغرات الأمنية تتسع الأمر الذي يستلزم مواجهة متخصصة عالية الكفاءة للحد من احتمالات نجاح التهديدات الإرهابية.

٧- العمل على تعزيز إجراءات الأمن السيبراني في القطاعات الحيوية والمؤسسات الاقتصادية وسائر مرافق الدولة وفقًا لأحدث تكنولوجيا في مجالات التأمين والتشفير. وفي هذا الصدد أقترح إنشاء هيئة وطنية من الخبراء والمتخصصين لوضع تطوير استراتيجية وطنية للأمن الإلكتروني، وسبل حماية البني التحتية لشبكات المعلومات ونظم البرمجيات.

٨- التقييم الدائم والمستمر للأساليب والاستراتيجيات الحالية والمستقبلية المستخدمة في تأمين تأمين البنية التحتية الحيوية بالدولة وما إذا كان من شانها أن تمنع الإرهاب الإلكتروني بشكل كاف. بالإضافة إلى تحديث أنظمة التشغيل والبرامج المستخدمة فيها بانتظام، وفرض استخدام كلمات سر قوية، وتامين جميع

النظم، وتعطيل الخدمات غير الضرورية، وتثبيت وتحديث برامج مكافحة الفيروسات باستمرار واستخدام الجدران النارية، ونظم الكشف عن التسلل عالية الدقة.

٩- رصد ومتابعة المواقع الإلكترونية المشبوهة من خلال فرق متخصصة في هذا المجال ونشر أسمائها وتحذير الأفراد من التعامل معها. والسماح بمراقبتها على أن يكون ذلك بتصريح من القضاء درءًا لأي تعسف أو افتئات على الحريات الفردية شريطة أن يكون ذلك بمناسبة التحقيق في قضية معينة.

١٠- تعزيز التعاون مع المؤسسات الدولية المهتمة بالظاهرة، وبخاصة المنظمة الدولية للشرطة الجنائية (الأنتربول) وذلك عن طريق توسيع وتطوير الآليات التقليدية للتعاون الدولي على المستوى الجنائي، على شكل يواكب اتساع شبكات الاتصالات وتقدمها.

وأخيرًا يتعين وضع إطار للتعاون الدولي تحت مظلة الأمم المتحدة لمكافحة الإرهاب الإلكتروني يتم من خلاله رسم سياسات واضحة لمراقبة وفحص مواقع الجماعات الإرهابية على شبكة الإنترنت ودراسة سلوكها بالتوازي مع قيام المجتمع الدولي بعمليات متسقة لتبادل المعلومات الاستخبارية حول هذه المنظمات وتجميعها.

وتمثل نقطة البداية في إقامة مثل هذا التعاون في تجميع المعلومات الاستخباراتية حول المنظمات الإرهابية ومصادر تمويلها في مجمع استخباراتي Intelligence Pool تتقاسمه الدول المعنية، على ألا يقتصر هذا المجمع على رصد وجمع المعلومات عن المواقع الشبكية الارهابية وإنما يعمل على جمع الأدلة الالكترونية عن الهجمات السيبرانية المحتملة.

لذا أقترح إنشاء شبكة معلوماتية يدرج بها كافة المعلومات الجيدة المتحصلة من العمليات السابقة، بالإضافة إلى تغذيتها بالمعلومات المتعلقة بالجماعات والتنظيمات الإرهابية على مستوي العالم بشكل دائم ومستمر على أن تكون الحكومات الطرف الوحيد المسموح باستخدام هذا المورد.

وفي نهاية هذه الدراسة نهيب بالأجهزة الإعلامية العمل على مواجهة المواقع التي تروج للفكر المتطرف والإرهاب عبر شبكة الإنترنت، كما نؤكد على ضرورة التعاون الكامل بين وسائل الإعلام والأجهزة الأمنية في مواجهة الإرهاب الإلكتروني، بأن تزود الأخيرة وسائل الإعلام بكل ما لديها من معلومات عن المواقع التي تغذي الفكر المتطرف المعلومة لديها، كما نؤكد أيضا على أهمية تعظيم دور المواطن في التصدي لجرائم الإرهاب الإلكتروني وخلق الشعور لديه بأن دوره لا يقل أهمية عن دور أجهزة الأمن؛ لأن المواطن من أهم الفئات المستهدفة بالإرهاب الإلكتروني.

كما نهيب بالمؤسسات الدينية وعلى رأسها الأزهر الشريف التدخل للتوعية بخطورة الإرهاب الإلكتروني وتقوية الوازع الديني الوسطي غير المتشدد وتصحيح المفاهيم المضللة التي تروجها التنظيمات الإرهابية عبر الإنترنت وشبكات التواصل الاجتماعي بغرض استدراج الشباب وتجنيدهم.

تم بحمد الله

قائمة المراجع

أولا: المراجع باللغة العربية:

المراجع العامة والخاصة:

الدكتور/ أحمد جلال عز الدين:

- الإرهاب والعنف السياسي: كتاب الحرية، دار الحرية للصحافة والطباعة والنشر، ١٩٨٦.

الدكتور/ أحمد فتحي سرور:

- المواجهة القانونية للإرهاب، مركز الأهرام للترجمة والنشر- مؤسسة الأهرام، الطبعة الثانية، ٢٠٠٨.
- الوسيط في قانون العقوبات القسم الخاص "الكتاب الأول"، نادي القضاة ٢٠١٦.

الدكتور/ أحمد محمد رفعت:

- الإرهاب الدولي في ضوء أحكام القانون الدولي والاتفاقيات الدولية، دار النهضة العربية، ١٩٨٨.

الدكتور/ أحمد شوقي أبوخطوة:

- تعويض المجني عليهم عن الأضرار الناشئة عن جرائم الإرهاب، دار النهضة العربية، ١٩٩٩.

الدكتور/ أحمد محمود مصطفي:

- جرائم الحاسبات الآلية في التشريع المصري دراسة مقارنة، دار النهضة العربية، الطبعة الأولي ٢٠١٠.

الدكتور/ إمام حسانين خليل:

- نحو اتفاق دولي لتعريف الإرهاب – الجرائم الإرهابية في التشريعات المقارنة، مركز الخليج للدراسات الاستراتيجية، الطبعة الأولي ٢٠٠٨.

الدكتور/ ثامر إبراهيم:

- مفهوم الإرهاب في القانون الدولي، دار حوران للطباعة، دمشق، ١٩٩٨.

الدكتور/ جميل عبد الباقي الصغير:

- الإنترنت والقانون الجنائي– الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، ٢٠٠٢.
- مذكرات في الحاسب الآلي، محاضرات لطلبة كلية الحقوق الفرقة الثالثة – جامعة عين شمس، مكتبة الجامعة ١٩٩٨.

الدكتور/ حاتم عبد الرحمن منصور:

- الإجرام المعلوماتي، دار النهضة العربية، الطبعة الأولي ٢٠٠٣.

الدكتور/ حسين المحمدي بوادي:

- الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦.

الدكتور/ راشد محمد المري:

- الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر دراسة مقارنة، دار النهضة العربية، ٢٠١٨.

الدكتور/ طارق عبد العزيز حمدي:

- التقنين الدولي لجريمة إرهاب الدولة، دار الكتب القانونية، ٢٠٠٩.

الدكتور/ عادل عبد الصادق:

- الإرهاب الإكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، المركز العربي لأبحاث الفضاء الإلكتروني، الطبعة الثانية، ٢٠١٣.
- الفضاء الإلكتروني والعلاقات الدولية دراسة في النظرية والتطبيق، المكتبة الأكاديمية، ٢٠١٦.

الدكتور/ عبد العزيز مخيمر عبد الهادي:

- الإرهاب الدولي مع دراسة في الاتفاقيات الدولية والقرارات الصادرة عن المنظمات الدولية، دار النهضة العربية، ١٩٨٦.

الدكتور/ عدنان جمعان محمد الزهراني:

- أحكام التجارة الالكترونية في الفقه الاسلامي، دار القلم، لبنان، الطبعة الأولي ٢٠٠٩.

الدكتور/ علي حسين الخلف:

- المبادئ العامة في القانون، بدون دار نشر، ١٩٨٢.

الدكتور/ عمر أبو الفتوح الحمّامي:

- الحماية الجنائية للمعلومات المسجلة إلكترونيًا، دار النهضة العربية، ٢٠١٠.

الدكتور/ عمر محمد أبو بكر:

- الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، ٢٠٠٤.

الدكتورة/ غادة نصار:

- الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ٢٠١٧.

الدكتور/ فكري عطا الله:

- الإرهاب الدولي- المتفجرات، دار الكتب الحديثة، ٢٠٠٠.

الدكتور/ كمال أحمد:

- الوسيط في شرح قانون مكافحة الإرهاب، دار النهضة العربية، ٢٠١٧.

الدكتور/ محمد أمين أحمد الشوابكة:

- جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان ٢٠٠٤.

الدكتور/ محمد سيد سلطان:

- قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، ٢٠١٢.

الدكتور/ محمد عبيد الكعبي:

- الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية ٢٠١٠.
- السياسة الجنائية في مواجهة جرائم الإنترنت «دراسة مقارنة»، دار النهضة العربية ٢٠٠٩.

الدكتور/ محمد عزت عبد العظيم:

- الجرائم المعلوماتية الماسة بالحياة الخاصة، دار النهضة العربية، الطبعة الأولي ٢٠١٦.

الدكتور/ محمد علي العريان:

- الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية ٢٠٠٤.

الدكتور/ محمد محيي الدين عوض:

- مبادي القانون الجنائي، القسم العام، ١٩٨١.

الدكتور/ محمد مؤنس محب الدين:

- الإرهاب في القانون الجنائي، دراسة قانونية مقارنة على المستويين الوطني والدولي، مكتبة الأنجلو المصرية، ١٩٧٣.

الدكتور/ محمود الرشيدي:

- العنف في جرائم الانترنت: الحماية والتأمين، الدار المصرية اللبنانية، القاهرة، ٢٠١١ .

الدكتور/ محمود نجيب حسني:

- علاقة السببية في قانون العقوبات، دار النهضة العربية، ١٩٨٣.

الدكتور/ مدحت عبد الحليم رمضان:

- الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، ٢٠٠١.

الدكتور/ مصطفي محمد موسي:

- الإرهاب الإلكتروني، بدون دار نشر، الطبعة الأولي ٢٠٠٩.

الدكتور/ مصطفى مصباح دبارة:

- الإرهاب مفهومه وأهم جرائمه في القانون الدولي الجنائي، منشورات جامعة قاريونس، ليبيا ١٩٩١.

الدكتور/ وليد الزيدي:

- القرصنة علي الإنترنت والحاسوب، دار أسامة للنشر والتوزيع، عمان ٢٠٠٣.

الدكتورة/ هدي حامد قشقوش:

- جرائم الحاسب الآلكتروني في التشريع المقارن، دار النهضة العربية، ١٩٩٢.

هلال محمد البوسعيدي:

- الحماية القانونية والفنية لقواعد المعلومات المحوسبة، دار النهضة العربية، ٢٠٠٩.

الدكتور/ هلالي عبد اللاه أحمد:

- المواجهة الجنائية لجرائم المعلوماتية في النظامين المصري والبحريني في ضوء إتفاقية بودابست، دار النهضة العربية، الطبعة الثانية ٢٠١٣.

الدكتور/ يوسف نصر الله:

- تداعي الأسطورة: مقاربات نقدية لمشهدية الحرب السادسة، دار الفارابي – بيروت– لبنان، الطبعة الأولي ٢٠١١.

الرسائل العلمية:

الدكتور/ أحمد عبد العظيم مصطفى المصري:

- المواجهة التشريعية لجرائم الإرهاب في التشريع المصري والقانون المقارن، رسالة دكتوراه –حقوق القاهرة، ٢٠٠٣.

أسراء طارق جواد كاظم:

- جريمة الإرهاب الإلكتروني– دراسة مقارنة، رسالة ماجستير، كلية الحقوق – جامعة النهرين، العراق، ٢٠١٢.

الدكتور/ ديش موسي:

- النظام القانوني لتعويض ضحايا الجرائم الإرهابية – دراسة مقارنة، رسالة لنيل درجة الدكتوراه، كلية الحقوق جامعة ابي بكر بلقيد– تلمسان، الجزائر ٢٠١٦.

الدكتور/ صباح عبد الرحمن حسن الغيص:

- السياسة الجنائية لمواجهة الجرائم الإرهابية، رسالة دكتوراه – حقوق عين شمس، ٢٠٠٩.

الدكتور/ عبلة مزوزي:

- استراتيجية الردع وانعكساتها علي الواقع الاقليمي والدولي بعد نهاية الحرب الباردة، رسالة دكتوراه، جامعة باتنة، كلية الحقوق والعلوم السياسية، الجزائر، ٢٠١٧-٢٠١٨.

الدكتور/ علي محمد عامر العجمي:

- الإرهاب في القانون الجنائي، رسالة دكتوراه- حقوق طنطا، ٢٠٠٩.

الدكتور/ فهد سيف راشد الحوسني:

- جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، رسالة دكتوراة – أكاديمية الشرطة، مصر ٢٠٠٧.

محمد سليمان الخوالدة:

- جريمة الدخول غير المشروع على المواقع الإلكترونية أو نظام المعلومات وفق التشريع الإردني، رسالة ماجستير، كلية الدراسات العليا، الجامعة الاردنية ٢٠١٢.

<u>البحوث والمقالات:</u>

الدكتور/ أسامة غانم العبيدي:

- جريمة الدخول غير المشروع للظام المعلوماتي، دراسة قانونية في ضوء القوانين المقارنة، منشور بدراسة المعلومات، العدد الرابع عشر، ٢٠١٢. متاح على الرابط التالى:

https://search.mandumah.com/Record/206884

الدكتور/ أيمن سيد العسقلاني:

- الإرهاب الإلكتروني في إطار القانون الدولي، بحث مقدم لمؤتمر القانون والتكنولوجيا المنعقد في الفترة ٩-١١ ديسمبر ٢٠١٧، مجموعة أعمال المؤتمر، الجزء الثاني ديسمبر ٢٠١٧.

إيهاب خليفة:

- إمكانيات تحقيق الردع فى صراعات الفضاء الإلكترونى، مركز المستقبل للأبحاث والدراسات المتقدمة ، العدد ١٣ – ٢٠١٥.

الدكتور/ حسن أحمد الشهري:

- الإرهاب الإلكتروني- حرب الشبكات، المجلة العربية الدولية للمعلوماتية، المجلد ٤ العدد ٨، يناير ٢٠١٥.

الدكتور/ رائد العدوان:

- المعالجة الدولية لقضايا الإرهاب الإلكتروني، الدورة التدريبية حول توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب المنعقدة في الفترة من ٢٣-٢٧ فبراير ٢٠١٣، كلية التدريب قسم البرامج التدريبية بجامعة نايف للعلوم الأمنية، الرياض ٢٠١٣.

الدكتور/ عادل عبد الصادق:

- الاحتجاج الإلكتروني والفاعلون الجدد في الحياة السياسية، ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد ١٦٢، يونيه ٢٠٠٨.

الدكتور/ عادل محمد علي مصطفي:

- جرائم الإرهاب عبر الإنترنت، مجموعة أعمال مؤتمر القانون والتكنولوجيا والذي نظمته كلية الحقوق – جامعة عين شمس في القترة من ٩-١١ ديسمبر ٢٠١٧، الجزء الأول، ديسمبر ٢٠١٧.

الدكتور/ عبد الله عبد العزيز العجلان:

- الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الإنترنت والمنعقد بالقاهرة في الفترة ٢- ٤ يونيو ٢٠٠٨.

الدكتور/ عبد الرحمن أحمد السند:

- وسائل الإرهاب الإلكتروني حكمها في الإسلام ... وطرق مكافحتها، مجلة الأمن والحياة، العدد ٣٢٥ – جمادي الآخرة ١٤٣٠هـ .

الدكتور/ عبيد صالح حسن:

- سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية، مجلة الفكر الشرطي، المجلد الرابع والعشرين، العدد ٩٥ – أكتوبر ٢٠١٥.

علي الوشلي:

- هجمات الحرمان من الخدمة. منشور بتاريخ ٣١ أكتوبر ٢٠١٣ على الرابط التالى: https://www.isecur1ty.org

الدكتور/ علي عدنان الفيل:

- د/ علي عدنان الفيل، الإرهاب الإلكتروني، مجلة الجامعة الخليجية، المجلد الثاني – العدد الثاني، ٢٠١٠، ص ٢٣. منشور على الموقع التالى: https://platform.almanhal.com/Files/2/7983

الدكتور/ مايا حسن ملا خاطر:

- الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة الناصر، العدد الخامس ، المجلد الأول، يناير – يونيو ٢٠١٥، ص ١٣٢.

الدكتور/ محمد أبو الفتوح غنام:

- تعريف الإرهاب، مجلة الأمن العام، العدد ١٤٣ س ٣٥، أكتوبر ١٩٩٣.

الدكتور/ محمد عبدالله آل فايع العسيري، الدكتور/ حسن أحمد الشهري:

- الإرهاب الإلكتروني وبعض وسائله والطرق الحديثة لمكافحته، بحث مقدم إلى الندوة العلمية «استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين» والتي نظمتها جامعة نايف العربية للعلوم الأمنية بالرياض في الفترة ٩–١١ مايو ٢٠١١.

الدكتور/ محمد مونس محب الدين:

- الإرهاب والعنف السياسي، مجلة الأمن العام، عدد ٩٤، سنة ٢٤ يوليو ١٩٨١.

الدكتور/ محمد يونس عرب:

- الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنت للأغراض الإرهابية، بحث مقدم إلى الندوة العلمية «استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين» والتي نظمتها جامعة نايف العربية للعلوم الأمنية بالرياض في الفترة ٩–١١ مايو ٢٠١١، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولي ٢٠١٢.

ثانيا: المراجع باللغة الإنجليزية:

I- BOOKS, CHAPTERS IN BOOKS:

Ackerman. G., Abhayaratne. P., Bale. J., Bhattacharjee. A., Blair. C., Hansell. L., Jayne. A., Kosal. M., Lucas. S., Moran. K., Seroki. L., & Vadlamudi. S.:

- "Assessing Terrorist Motivations for Attacking Critical Infrastructure," Center for Nonproliferation Studies, Monterey Institute of International Studies, California, Jul. 2007.

Ashish Pandey:

- Cyber Crime Prevention and Detection, Ist Ed, 2006.

Bhavani Thuraisingham:

- Data mining for counter-terrorism. In: KARGUPTA, H., JOSHI, A., SIVAKUMAR, K. & YESHA, Y. (eds.), Data Mining: Next Generation Challenges and Future Directions. Maryland, MIT/AAAI Press.2004.
- Developing and Securing the Cloud, CRS Press, 2013.

Christopher Beggs & Matthew Butler:

- "Developing new strategies to combat cyber-terrorism". In: M. Khosrow-Pour (eds.), Innovations Through Information Technology, Australia, Idea Group Inc. 2004.

Clay Wilson:

- Cyber Crim, In Franklin D. Kramer, Stuart H. Starr &Larry K. Wentz (eds.), Within the Cyberpower and National Security, National Defense University Press, WASHINGTON, D.C. 1st ed. 2009.
- Cyber Threats to Critical Information Infrastructure. In: Thomas M. Chen, Lee Jarvis and Stuart Macdonald (eds.), Cyberterrorism: Understanding, Assessment and Response. Springer, New York, 2014.

Dawson, M., Omar, M., Abramson, J., & Bessette, D.:

- "The Future of National and International Security on the Internet. In: A. Kayem & C. Meinel (eds.), Information Security in Diverse Computing Environments. 2014.
- DCSINT, Critical Infrastructure Threats and Terrorism: Handbook Kansas, Deputy Chief of Staff for Intelligence. 2006. Available at: https://fas.org/irp/threat/terrorism/sup2.pdf

Dorothy E. Denning:

- Activism, Hacktivism and cyber terrorism, the internet as a tool for influencing, Foreign policy. In: Arquilla & D. Ronfold (eds.), Networks and net wars, the future of terror crime and miletences, National Defense Research Institute, 2001.
- Hacktivism is the marriage of hacking and activism. In: Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija (eds.), Hacktivism, Cyber Terrorism and Cyberwar the Activities of the uncivil, 2003.

Freedman Laweence, Christopher Hill, Adam Roberts, R. J. Nincent, Paul Wilkinson & Philip Windsor:

- Terrorism and International Order, The Royal Institute of International Affairs, Routbedge, 1988.

George W. Reynolds:

- Ethics in Information Technology, Congage Learning, Boston, USA, Sixth Edition, 2018.
- Information Technology for Managers, Congage Learning, Boston, USA, second Edition, 2015.

Georg Disterer:

- Ame Alles and Axel Hervatin, Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation.

In: Lech J. Janczewski and Andrew M. Colarik (eds.), Cyber Warfare and Cyber Terrorism, Information Science Reference (an imprint of IGI Global), Hershey - New York, 2007.

Ian Rivers:

- Homophobic Bullying. Research and Theoretical Perspectives, New York: Oxford University Press, 2011.

Irving Lachow:

- Cyber Terrorism: Menace or Myth?. In: Larry K. Wentz, Stuart H. Starr, Franklin D. Kramer (eds.), Cyberpower and National Security. National Security Center for Technology and National Security Policy, National Defense University and Potomac Books, Inc., 2009.

James A. Lewis:

- Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: Center for Strategic and International Studies, Washington, DC, December 2002.

John Arquilla & David Ronfeldt:

- The Advent of Netwar (Revisited). In: Networks and Netwars: The Future of Terror, Crime, and Militancy, (eds.), RAND: National Defense Research Institute, 2001.

Jose Nazario:

- Politically Motivated Denial of Service Attacks. In Christian Czosseck and Kenneth Geers (eds.), The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press BV, 2009.

Katharina Ziolkowski:

- "Peacetime cyber espionage- new tendenceies public international law" In: Katharina Ziolkowski (eds.), Peacetime Regime for state activities in Cyber-space: International law, International Relations Diplomacy, (NATO CCDCOE Publications, Tallinn 2013).

Kevin Curran:

- Cryptography. In: Lech J. Janczewski and Andrew M. Colarik (eds.), Cyber Warfare and Cyber Terrorism, Information Science Reference (an imprint of IGI Global), Hershey - New York, 2007.

Kevin Curran, Kevin Concannon & Sean McKeever:

- Cyber terrorism: attacks cyber warfare and cyber terrorism. In: Lech J. Janczewski & COLARIK, A. M. (eds.), Cyber Warfare and Cyber Terrorism. Hershey-New York. 2008.

Lawrence Freedman:

- Deterrence, Cambridge, Polity Press, 2004.

Michal Choras, Babak Akhgar, Ben Brewster, Francesca Bosco, Elise Vermeersch, Vittoria Luda, Damian Puchalski & Douglas Wells:

- Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In: Akhgar, Babak. and Brewster, Benjamin. (eds.), Combatting Cybercrime and Cyberterrorism. Springer 2016.

Michael Cross & Debra Littlejohn Shinder:

- Scene of the Cybercrime, 2nd Revised Edition., Syngress, 2008.

Michael Krepon:

- Space and Nuclear Deterrence, In: Michael Krepon and Julia Thompson (eds.), Anti-Satellite Weapons Deterrence and Sino-American Space Relations, United States: Stimson Center, September 2013.

Michael Erbschloe:

- Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code, Oxford, Elsevier Butterworth-Heinemann, 2005.

Michael N. Schmitt & Liis Vihul:

- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

Maura Conway:

- Cyberterrorism: Hype and reality. In: Leigh Armistead (eds.), Information Warfare: Separating Hype from Reality, Potomac Books, Inc. Washington, D.C. 2007.
- Terrorism and new media: the cyber-battl espace. In: Forest, James F., (eds.), Countering terrorism and insurgency in the 21st century. Greenwood Publishing Group, Inc., Westport, CT, 2007. pp. 363-384.

Maurice Dawson, Marwan Omar & Jonathan Abramson:

- Understanding the Methods behind Cyber Terrorism. In: Mehdi Khosrow-Pour (eds.), Encyclopedia of Information Science and Technology, 3rd ed., 2015. pp. 1539–1549. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-5888-2.ch147

Molly Sauter:

- The Coming Swarm, DDoS Actions, Hacktivism, and Civil Disobedience on the Internet, Bloomsbury Academic, 2014.

Nina Olesen:

- European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism. In: Babak Akhgar and Ben Brewster (eds.), Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities, Springer International Publishing, 2016.

Panayotis A. Yannakogeorgos:

- Rethinking the threat of cyberterrorism. In: Thomas M. Chen, Lee Jarvis and Stuart Macdonald (eds.), Cyberterrorism: Understanding, Assessment, and Response. Springer, New York, 2014.

PhillipW. Brunst:

- "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet". In: Marianne Wade and Almir Maljevic (eds.), A War on Terror? The European Stance on a Changing Laws and Human Rights Implications, New York: Springer, 2010.

R. Heickero:

- "Terrorism Online and the Change of Modus Operandi," Swedish Defence Research Agency, Stockholm, Sweden, 2007.

Richard A. Clarke & Robert knake:

- Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins Publishers, 2010.

Ruseell Buchan:

- "Cyber espionage and international law". In: Nicholas Tsagourias and Russell Buchanand Russell Buchan (eds.), Research. Handbook on International Law and Cyberspace, (Edward Elgar Publishing 2015).

Seymour E. Goodman:

- Critical Information Infrastructure Protection, In: Responses to Cyber Terrorism Centre of Excellence Defence Against Terrorism, Ankara, Turkey (eds.), IOS Press, 2008.
- Cyberterrorism and Security Measures. In: Roddam Narasimha, Arvind Kumar, Stephen P. Cohen & Rita Guenther (eds.), Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop, International Strategic and Security Studies Programme of the National Institute of Advanced Studies, National Academy of Sciences, National Academies Press, Washington, D.C. 2007.
- "Toward a treaty-based international regime on cyber crime and terrorism," Cyber Security: Turning National Solutions into International Cooperation, Center for Strategic and International Studies Press, Washington, D.C., 2003. Available at: http://csis.org/pubs/2003_cyber.html

Sliwouski George:

- Legal Aspects of Terrorism in International World Security, Halsted Press Book, New York, Toronto, 1974.

Sieber Ulrich, & Phillip W. Brunst:

- Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In Council of Europe (eds.), Cyberterrorism – The Use of the Internet for Terrorist Purposes. Strasbourg: Council of Europe Publishing, 2007.

Stephen J. Lukasik, Seymour E. Goodman & David W. Longhurst:

- Protecting Critical Infrastructures Against Cyber-Attack, Adelphi Paper 359, International Institute for Strategic Studies, London, 2003.

Thomas M. Chen, Lee Jarvis & Stuart Macdonald:

- Cyberterrorism: Understanding, Assessment, and Response, New York, Springer 2014.

Valerie E. Besag:

- Understanding Girls' Friendships, Fights and Feuds. A Practical Approach to Girls' Bullying, Maidenhead, UK, Open University Press. 2006.

II- THESIS:

Alexandra Whitney Samuel:

- Hacktivism and the Future of Political Participation, AThesis Doctor of Philosophy in the subject of Political Science Harvard University Cambridge, Massachusetts September 2004.

Devost M.G.:

- National security in the information age, Unpublished Master Thesis, University of Vermont, Burlington, May 2007.

Eliza Watt:

- Cyberspace, Surveillance, Law and Privacy, A Thesis submitted in partial fulfilment of the requirements of the University of Westminster for the degree of Doctor of Philosophy, September 2017. Available at: http://westminsterresearch.wmin.ac.uk/20610/1/Watt_Eliza_thesis.pdf

Nazli Zeynep BOZDEMİR:

- "Re-Conceptualizing Cyberterrorism: Towards a New Definitional Framework", Master of Arts, Hacettepe University Graduate School of Social Sciences

Department of International Relations International Relations MA, Ankara, 2016.

III- JOURNALS, MAGAZINE & RESEARCH PAPER:

Adam Chuipka:

- The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorist? Major Research Paper: Graduate School of Public International Affairs University of Ottawa, Ottawa, Ontario, November 2016. Available at: https://ruor.uottawa.ca/bitstream/10393/35695/1/CHUIPKA%2c%20Adam%2020169.pdf

Ahmed H. Anjariny, Shakeel A. Habib & Emmanuel Nyakwende:

- "Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies", International Journal of Cyber Warfare and Terrorism (IJCWT) Vol. 6, Issue. I, 2016.

Alan E. Brill:

- From Hit and Run to Invade and Stay: How Cyberterrorists Could Be Living Inside Your Systems, Defence Against Terrorism Review. Vol. 3, No. 2, Fall 2010.

Alexander Meleagrou-Hitchens & Seamus Hughes:

- The Threat to the United States from the Islamic State's Virtual Entrepreneurs, CTC sentinel, Vol. 10, Issue. 3, March 2017.

Ali Jahanger:

- cyber space, cyber terrorism and information warfare: A perfect recipe for confusion world wide selected speakers, Note 20. 2009.

Amalie M. Weber:

- The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal, Vol. 18, Issue. 1, January 2003.

Annalaura Nocentini, Juan Calmaestra, Anja Schultze-Krumbholz, Herbert Scheithauer, Rosario Ortega & Ersilia Menesini.:

- 'Cyberbullying: Labels, Behaviours and Definition in Three European Countries' Australian Journal of Guidance & Counselling, Vol. 20, No. 2, 2010.

Anna – Maria:

- Cyber terrorism in theory or in practice, Defense against terrorism Review, Vol. 2, Fall 2010.

Anup Sharma, Robin Gandhi , Qiuming Zhu, William Mahoney & William Sousan:

- A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference, International Journal of Information and Computer Security, Vol. 5, Issue. 4, Dec 2013. Available at: https://digitalcommons.unomaha.edu/compscifacpub/24/

Ayn Embar-Seddon:

- "Cyberterrorism: Are We Under Siege?" American Behavioral Scientist, Vol. 45, No. 6, Feb. 2002, At: http://abs.sagepub.com/content/45/6/1033.full.pdf+html [Accessed 06.09.2013].

Barry C. Collin:

- "The Future of Cyberterrorism, Crime and Justice International". Vol. 13, Issue 2, March 1997.
- "The Future of CyberTerrorism: Where the Physical and virtual Worlds Converge". 11th Annual International Symposium on Criminal Justice Issues, 1997.

Ben Saul & Kathleen Heath:

- Cyber terrorism, Sydney law of school, Legal studies Research paper, No. 14/11, January 2014. Available at:
- http://ssrn.com/abstract=2387206.

Bogdanoski, M. & Petreski, D.:

- Cyber Terrorism– Global Security Threat Contemporary Macedonian Defense - International Scientific Defense, Security and Peace Journal, Vol. 13, 2013.

Colette Langos:

- Cyberbullying: The Challenge to Define, Cyberpsychology, Behavior and Social Networking, Vol. 15, No. 6, June 2012.
- "Regulating Cyberbullying: A South Australian Perspective", Flinders Law Journal, Vol. 16, No. 1, 2014.

Daniel Moore & Thomas Rid:

- "Cryptopolitik and the Darknet", Survival, vol. 58. no. 1, February–March 2016, Available at: https://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true

David Talbot:

- Intelligent Machines: New Malware Brings Cyberwar One Step Closer. MIT Technology Review, 2011. https://www.technologyreview.com/s/425832/new-malware-brings-cyberwar-one-step-closer/. [Accessed 20 October 2011].

David Weissbrodt:

- Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, Minnesota Journal of International Law, Vol. 22, Issue. 2, Summer 2013.

Dhiraj Kukreja:

- Securing Cyberspace, Liberal Studies Journal, Vol. 2, Issue. 2, July-December 2017. Available at: http://sls.pdpu.ac.in/downloads/Dhiraj%20Kukreja.pdf

Dimitrios Choupis:

- "Challenges and Objectives for the National Cyber-Security Strategy Beyond 2020". Journal of Computations & Modelling, Vol. 4, No. 1, 2014.

Dogrul Murat, Adil Aslan & Eyyup Celik:

- "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," 3rd International Conference on Cyber Conflict, Tallinn, 7-10 June 2011. Available at: http://www.ccdcoe.org/publications/2011proceedings/DevelopingAnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf

Elizabeth Renieris:

- "Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and the United Kingdom and the Need for an International Solution," Vanderbilt Journal of Entertainment and Technology Law, vol. 11, Issue. 3, 2009.

Emilio Iasiello:

- Is Cyber Deterrence an Illusory Course of Action?. Journal of Strategic Security, Vol. 7, No. 1, 2013.

E. Noor:

- "The Problem with Cyber Terrorism," Proceeding of Southeast Asia Regional Center for Counter Terrorism's (SEARCCT) Selection of Articles, Ministry of Foreign Affairs Malaysia, Vol. 2, 2011.

Enver Bucaj:

- The Need for Regulation of Cyber Terrorism Phenomena in Line with Principles of International Criminal Law, Acta Universitatis Danubius. Juridica, Vol. 13, No. 1, 2017. Available at: http://journals.univ-danubius.ro/index.php/juridica/article/view/3882/4033

Ersilia Menesini, Annalaura Nocentini & Pamela Calussi.:

- The Measurement of Cyberbullying: Dimensional Structure and Relative Item Severity and Discrimination', Australian Journal of Guidance & Counselling Vol. 14, No. 5, 2011.

Fadi A. Aloul:

- The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, Vol. 3, No. 3, August 2012.

FOLTZ, C. Bryan:

- "Cyberterrorism, computer crime, and reality", Information Management & Computer Security, Vol. 12, Issue. 2, 2004.

Gabriel Weimann:

- "Cyberterrorism: The Sum of All Fears?" Studies in Conflict & Terrorism, Vol. 28, No. 2, 2005. Available at: http://dx.doi.org/10.1080/10576100590905110
- Terrorist Migration to the Dark Web, Perspectives on Terrorism, Vol. 10, No. 3, June 2016. Available at: http://www.terrorismanalysts.com/pt/index.php/pot/article/viewFile/513/1013

Geoffrey B. Demarest:

- Espionage in International law, Journal of International Law and Policy. Vol. 24, 1996.

Graham H. Todd:

- Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, Air Force Law Review, Vol. 64, 2009.

Herbert S. Lin:

- Offensive Cyber. Operations and the Use of Force, Journal of National Security Law & Policy, Vol. 4, 2010.

Ido Kilovaty:

- World Wide Web of Exploitations – The Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach, Columbia Science and Technology Law Review, Vol. 18, 2016.

Israa G. Seissa, Jamaludin Ibrahim & Nor-Zaiasron Yahaya:

- "Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review", International Journal of Science and Research (IJSR), Vol. 6, Issue. 1, January 2017.

Jensen Eric Talbot:

- Cyber Deterrence, Emory International Law Review, No. 26, 2012.

Jim Ramsay, Daniel Cutrer& Robert Raffel

- Development of an Outcomes-based, Undergraduate Curriculum in Homeland Security. Homeland Security Affairs Journal, Vol. 6, No. 2, MAY 2010. Available at:

https://www.hsaj.org/articles/679

Jonathan Matusitz:

- Cyberterrorism: How Can American Foreign Policy Be Strengthened in the Information Age? American Foreign Policy Interests, Vol. 27, Issue. 2, 2005.

Jonathan Solomon:

- Cyber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?, Strategic Studies Quarterly, Vol. 5, No. 1, Spring 2011, Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA538310

Kinner, W.F. & Fream, A.M:

- "A social learning theory analysis of computer crime among college students", The Journal of Research in Crime and Delinquency, Vol. 34, No. 4, 1997.

Kuboye Oluwafemi Samuel, Osman, W. R. S., Al-Khasawneh, Y. & Duhaim, S.:

- Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Scienceand Mobile Computing, Vol. 3, Issue. 5, May 2014.

Lewis T.G., Mackin T.J., & Darken R.:

- "Critical Infrastructure as Complex Emergent Systems", International Journal of Cyber Warfare & Terrorism, vol. 1, No. 1, 2011.

MAJ Lee Hsiang Wei's:

- The Challenges of Cyber Deterrence, Journal of the Singapore Armed Forces, Vol. 41, No. 1, 2015.

Martin C. Libicki:

- Deterrence in Cyberspace, High Frontier, Vol. 5, No. 3, May 2009.

Martin Rudner:

- Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge, International Journal of Intelligence and CounterIntelligence, Vol. 26, No. 3, 2013.

Maurice Dawson, Miguel Crespo & Stephen Brewster:

- "DoD cyber technology policies to secure automated information systems". International Journal of Business Continuity and Risk Management, Vol. 4, No. 1, 2013.

Mary M Calkins:

- They Shoot Trojan Horses, Don't They? An EconomicAnalysis of Anti-Hacking Regulatory Model, Georgetown Law Journal, November, 2000.

Michael Stohl:

- "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Game?," Crime, Law and Social Change, Vol. 46, No. 4-5, 2006.

Mitko BOGDANOSKI & Drage PETRESKI:

- Cyber Terrorism–Global Security Threat. Contemporary Macedonian Defense - International Scientific Defense, Security and Peace Journal, 2013. Available at: http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf

Mohamed Chawki & Mohamed S. Abdel Wahab:

- Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, vol. 11, No. 1, Spring 2006.

Noah C.N. Hampson:

- Hacktivism: A New Breed of Protest in a Networked World, Boston College International & Comparative Law Review, Vol. 35, 2012.

Namosha Veerasamy & Marthie Grobler:

- Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure, https://www.researchgate.net/publication/266173850 [Published online January 2011.]

Peter J. Phillip:

- The hunt for cyber terrorism, University of Southern Queenland, Faculty of business, 15 April 2013. At: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2253632

Peter Fleming & Michael Stohl:

- Myths and realities of cyber terrorism, reserachgate, January, 2001.

P. Santhosh Raj, G. Silambarasan & M. Phil Scholar:

- Role of Data Mining in Cyber Security, International Journal of Engineering Science and Computing, Vol 7. Issue, No.7, July 2017.

Rabiah Ahmad & Zahri Yunos:

- A Dynamic Cyber Terrorism Framework, International Journal of Computer Science and Information Security, Vol. 10, No. 2, 2012.

Robin A Gandhi, Anup Sharma, William Mahoney, William Sousan & Phillip Laplante:

- Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, IEEE Technology and Society Magazine, Spring 2011.

Rohas Nagpal:

- Cyber terrorism in the context of globalization. Paper presented at II World Congress on Informatics and Law. Madrid, Spain. September 2002. available at: http://www.asianlaws.org/aboutus/spain.pdf

Ryan Ehney & Jack D. Shorter:

- Deep Web, Dark Web, Invisible Web and The Post Isis World, Issues in Information Systems, Volume 17, Issue IV, 2016. accessible at:

  http:// www.iacis.org/iis/2016/4_iis_2016_36-41.pdf

Saheli Naik:

- A Biggest Threat to India – Cyber Terrorism and Crime, Journal of Research in Humanities and Social Science, Quest Journals, Vol. 5, Issue. 4, 2017.

S. Berner:

- "Cyber-Terrorism: Reality or Paranoia?" South African Journal of Information Management, vol. 5, No. 1, 2003.

Shamsuddin Abdul Jalil:

- Countering Cyber Terrorism Effectively: Are We Ready to Rumble?. US, System Administration, Networking, and Security Institute (SANS). 2003. Available at: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154

Shubham Chaudhary:

- Cyber Terrorism: World Wide Weaponisation! International Journal of Law and Legal Jurisprudence Studies, Vol. 3, Issue. 2, April 2016.

Slonje, R., & Smith, P. K.:

- 'Cyberbullying: Another Main Type of Bullying?' Scandinavian Journal of Psychology, Vol. 49, No. 2, 2008.

Smith, P. K., J. Mahdavi, M. Carvalho, S. Fisher, N. Russell, & N. Tippett.:

- "Cyberbullying: Its Nature and Impact in Secondary School Pupils", Journal of Child Psychology & Psychiatry, Vol. 49, 2008.

Soumen Ganguly:

- Impact of Cyberterrorism in digital world, International Journal of Computer Science, Information Technology & Security (IJCSITS), Vol.1, No. 1, October 2011.

Susan W. Brenner:

- At Light Speed: Attribution and Response to Cybercrime/ Terrorism/ Warfare. Journal of Criminal Law and Criminology, Vol.97, Winter, 2007.
- Cyber- Crime, Cyber-Terrorism and Cyber- Warfare, Revue Internationale de Droit Pénal, Vol. 77, No. 3, 2006.

Susan W. Brenner & Leo L. Clarke:

- "Civilians in Cyberwarfare: Casualties," SMU Science & Technology Law Review, Vol. 13, No. 2, 2010.

Timothy L. Thomas:

- Al Qaeda and the Internet: The Danger of "Cyberplanning", Parameters, Vol. 23, Issue. 1, 2003.

Yibin Xiang:

- Intrusive Viruses Depth Analysis and Teaching Research, 6 th International Conference on Information Technology for Manufacturing Systems (ITMS 2016).

V- REPORT:

A Multidisciplinary Conference on Cyberterrorism: Final Report, Cyberterrorism Project Research Report (No. 2), Swansea University, UK, July 2013. ***By. Jarvis, L., Macdonald, S. & Chen, T.***
http://www.cyberterrorism-project.org/wp-content/uploads/2013/07/CTP-Conference-Report.pdf

Challenges and Opportunities Created by Terrorism: Present Scenario. Online International Interdisciplinary Research Journal, Vol. 2, 2013. ***By. Shinde, V. N***.

Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, 2003. ***By. Clay Wilson***. Available at:
https://fas.org/irp/crs/RL32114.pdf

Cyberterrorism. How Real Is the Threat, United States Institute of Peace, Washington, ***By. Gabriel Weimann***. Available at: https://www.usip.org/sites/default/files/sr119.pdf
[Accessed 13 May 2004].

Cyberwarfare: A "Nuclear Option"? Washington, D.C.: Center for Strategic and Budgetary Assessments, 2012. ***By. Andrew F. Krepinevich***. Available at:
http://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf

Department of Defense's Strategy for Operating in Cyberspace, U.S. Department of Defense, July 2011, Available at:
http://www.defense.gov/news/d20110714cyber.pdf

Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites, The Berkman Center for Internet & Society at Harvard University, December 2010. by. Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York & John Palfrey Available at:
http://www.refworld.org/pdfid/4d3025492.pdf

Information Sharing and Safeguarding US, Report 2012. ***By. Federal Bureau of Investigation (FBI)***. available at: https://www.fbi.gov/file-repository/stats-services-publications-national-information-sharing-strategy-1-fbi-information-sharing-and-safeguarding-report-2012/view

Motivation for Cyberterrorism, Defence, Peace, Safety and Security (9 th Annual Security of South Africa (ISSA), Johannesburg, 2-4 August 2010). ***By. Namosha Veerasamy***. Available at: http//icsa.cs.up.ac.za/issa/2010/Proceedings/Research/02_paper.pdf [accessed 1 August 2015].

Report on Cyber Deterrence Policy, Available at**:** http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

Terrorist use of the Internet: an analysis of the current threat and its potential evolution, Technical Report, Information Security Group Royal Holloway, University of London Egham, Surrey TW20 0EX, United Kingdom, September 2014. ***By. Matteo Cavallini***. Available at: https://www.ma.rhul.ac.uk/static/techrep/2014/RHUL-MA-2014-11.pdf

Terror on the Internet: The New Arena, the New Challenges, United States Institute of Peace Press, Washington, D. C. 2006. ***By. Gabriel Weimann***. Available at: https://www.researchgate.net/publication/238077713_Terror_on_the_Internet_The_New_Arena_The_New_Challenges

The department of Defense Cyber Strategy, April 2015, ***By. Shinde, V. N***. Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack, Foreign Affairs (September 28, 2011), ***By. William J. Lynn***. Available at: www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

Threat Assessment: The cyber threat against Denmark, ***by. Centre of Cyber Security (F.E)***, January 2016. At: https://fe-ddis.dk/cfcs/CFCSDocuments/Threat%20Assessment%20-%20The%20cyber%20threat%20against%20Denmark.pdf

The UK cyber security strategy: protecting and promoting the UK in a digital world. Cited 12 February 2012. by. Minister for the Cabinet Office and Paymaster General. Retrieved from: http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_UK_Cyber_Security_Strategy.pdf; 2011.

The White House, International Strategy for Cyberspace, May 2011. Available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

"www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace (USIP), Special Report 116, March 2004. ***By. Gabriel Weimann***. Available at: https://www.usip.org/sites/default/files/sr116.pdf

VI- News Online:

- **ABC News**, "'Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011," 6 November 2014. By. Jack Cloherty and Pierre Thomas. Available at: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476

- **BBC News**, "Estonia fines man for 'cyber war", 25 January 2008. Available at: http://news.bbc.co.uk/2/hi/technology/7208511.stm [Retrieved 23 February 2008]
- **CNN**, "Japanese textbook dispute sparks cyber attack" CNN.com, Available at: http://edition.cnn.com/2001/WORLD/asiapcf/east/03/31/japan.korea.website/index.html [Accessed 31 March, 2001].
- **Homeland Security News Wire,** "Virginia medical records hijacking;" May 8, 2009, Available at: http://www.homelandsecuritynewswire.com/virginia-medical-records-hijacking-update
- **ITP. Net**. "UAE bank targeted in major phishing attacks", ITP, 2010. By. Vineetha Menon Available at: http://www.itp.net/579059-uae-banktargeted-inmajor-phishing-attack [Accessed January 23, 2010]
- **MIT Technology Review**, Intelligent Machines: New Malware Brings Cyberwar One Step Closer. By. David Talbot. https://www.technologyreview.com/s/425832/new-malware-brings-cyberwar-one-step-closer/. [Accessed 20 October 2011].
- **MIT Technology Review,** Stuxnet tricks copied by computer criminals. By. Tom Simonite. Available at: https://www.technologyreview.com/s/429173/stuxnet-tricks-copied-by-computer-criminals/ [Accessed 19 Sep 2012].
- **Network World,** "China becoming the world's malware factory," MAR 24, 2009. By. Robert McMillan. Available at: https://www.networkworld.com/article/2265827/data-center/china-becoming-the-world-s-malware-factory.html
- **Network World**, "Ukrainian cybercriminals raked in $10K/day, Finjan reports" MAR 23, 2009. By Ellen Messmer. Available at: https://www.networkworld.com/article/2265257/lan-wan/ukrainian-cybercriminals-raked-in--10k-day--finjan-reports.html

- **The Guardian**, "Russia accused of unleashing cyberwar to disable Estonia", 17 May 2007. By. Ian Traynor. Available at: https://www.theguardian.com/world/2007/may/17/topstories3.russia
- **The New York Times,** Israeli Test on Worm Called Crucial in Iran Nuclear Delay, by. William J. Broad, John Markoff and David E. Sanger. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html [Accessed 15 Jan 2011].
- **The New York Times,** Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots from Afar, By. Rukmini Callimachi. Available at: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html [Accessed Feb 4, 2017]

VII- Online:

Annegret Bendiek & Tobias Metzger:

- Deterrence Theory in the Cyber-Century: Lessons from a State-of-the-art Literature Review, German Institute for International and Security Affairs (SWP). Mai 2015. Available at: https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

Brett Pladna:

- Cyber terrorism and information security, East Carolina University, 2008. http://www.infosecwriters.com/text_resources/pdf/BPladna_Cyber_Terrorism.pdf

David Cantón:

- Classification of DoS Attacks, Instituto Nacional de Ciberseguridad de Espana S.A. [ES]. Available at: https://www.certsi.es/en/blog/classification-dos-attacks [accessed feb 26 2015]

Dorothy E. Denning:

- "Cyberterrorism", Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, Washington, D.C., 23 May 2000, p. 1. available at: http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

Elizabeth Minei & Jonathan Matusitz:

- Cyberspace as a new arena for terroristic propaganda: an updated examination. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3510409/ [Published online 2012 Aug 9]

Haylen Cohen:

- The Approaches and Limitations of Cyber Deterrence, Introduction to Computer Security, Tufts University Department of Computer Science, December 15, Fall 2015. Available at: http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf
- **INFOSEC INSTITUTE**, Cyberterrorism Defined (as distinct from "Cybercrime"), posted in General Security on 21 December 2012. Available at: http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/#gref

Kent Beckert:

- What is a Denial of Service (DoS) Attack? - Definition, Types & Examples, Available at: https://study.com/academy/lesson/what-is-a-denial-of-service-dos-attack-definition-types-examples.html

Margaret Rouse:

- Cyberterrorism: Publish in December 2017. Available at: http://searchsecurity.techtarget.com/definition/cyberterrorism
- Definition Hactivism. Available at: http://searchsecurity.techtarget.com/definition/hacktivism\

M. Handelman:

- "French embassy in Beijing under cyber-attack," infosecurity.us, Dec. 12, 2008. http://infosecurity.us/?p=4408

Nick Collins:

- "Cyber terrorism is biggest threat to aircraft" The Telegraph, Dec 27, 2013, Available at: https://www.telegraph.co.uk/finance/newsbysector/transport/10526620/Cyber-terrorism-is-biggest-threat-to-aircraft.html

Robert S. Mueller:

- War on Terrorism, Testimony Before the Select Committee on Intelligence of the United States Senate (2003). Available at: https://archives.fbi.gov/archives/news/testimony/war-on-terrorism

Robert Lemos:

- Cyberterrorism: The real risk, 2002. Available at: http://www.crime-research.org/library/Robert1.htm

Ryan, N. J.:

- Five Kinds of Cyber Deterrence, Philosophy & Technology, Published online: 27 January 2017. pp.2-3. Available at: https://link.springer.com/content/pdf/10.1007%2Fs13347-016-0251-1.pdf
- The Difference Between Hacktivism and Cyber Terrorism, Info Barrel Technology, Dec 18, 2009. Available at: http://www.infobarrel.com/The_Difference_Between_Hacktivism_and_Cyberterrorism

Victoria Baranetsky:

- What is cyber terrorism? Even experts cant agree, Harvard Law Record, Vol. 129, No. 4, 5 November 2009. Available at: http://hlrecord.org/2009/11/what-is-cyberterrorism-even-experts-cant-agree/

Vince Farhat, Bridget McCarthy, Richard Raysman & Holland Knight LLP.:

- Prevention and Proactive Responses, Practical Law Publishing Limited and Practical Law Company, 2011. p. 4. Available at: https://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf [Accessed 14 Aug. 2015].

VIII- Sites Internet:

http://www.cabinetoffice.gov.uk
https://www.certsi.es/en
https://www.defense.gouv.fr
http://www.infosecwriters.com
https://www.isecur1ty.org
http://edition.cnn.com
https://www.networkworld.com
https://www.nytimes.com
https://resources.infosecinstitute.com
https://www.tandfonline.com
https://www.theguardian.com
https://www.technologyreview.com
http://www.usdoj.gov/criminal/cybercrime/lyttlePlea.htm
http://www.whitehouse.gov

ثالثا: المراجع باللغة الفرنسية:

Alix DESFORGES:

- "Cyberterrorisme: quel périmètre?", Fiche de l'Irsem n° 11, décembre 2011, p. 3. disponible sur: https://www.defense.gouv.fr/content/download/153102/1551441/file/Fiche_n11_perimetre_cyberterrorisme.pdf

Bouloc (B):

- Le terrorisme problèmes actuels de science criminelle, 11ème presses universitaires d'Aix Marseille 1989.

De La Cuesta (J-L):

- Traitement Juridique du Terrorisme en Espagne, Rev. Sc. crim, 1997.

Galmard (M.H):

- Vers une nouvelle approche du phénomène terroriste? Apports de la loi no 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives aux contrôles transfrontaliers, Revue pénitentiaire, mars 2007.

Joas Marcello de Arago Junior:

- L'extractions dans la constitution Brésilienne de 1988. Rev. Dr. Pén. Int. 1991.

Rivero (J):

- Responsabilite de l'état et droits des victimes d'actes terrorisme, AJDA,1993.

Romain BOOS:

- La lutte contre la cybercriminalité au regard de l'action des États. Thèse, Université de Lorraine, 2016.

Uves Jeanclos:

- Terrorisme et securité international: collection Études stratégiques internationales, Bruylant, 2004, pp. 13-45.