| | |
|---|---|
| العنوان: | الإرهاب الإلكترونى : حرب الشبكات |
| المصدر: | المجلة العربية الدولية للمعلوماتية |
| الناشر: | اتحاد الجامعات العربية - جمعية كليات الحاسبات والمعلومات |
| المؤلف الرئيسي: | الشهري، حسن بن أحمد |
| المجلد/العدد: | مج4, ع8 |
| محكمة: | نعم |
| التاريخ الميلادي: | 2015 |
| الشهر: | يناير |
| الصفحات: | 1 - 23 |
| رقم MD: | 865991 |
| نوع المحتوى: | بحوث ومقالات |
| قواعد المعلومات: | science, HumanIndex, EduSearch |
| مواضيع: | الإرهاب الإلكترونى، الجرائم الإلكترونية، تكنولوجيا المعلومات والاتصالات، مكافحة الإرهاب |
| رابط: | http://search.mandumah.com/Record/865991 |

# الإرهاب الإلكتروني ـ حرب الشبكات ـ

**حسن بن أحمد الشهري**(*)


## الملخص

ثورة تقنية المعلومات والاتصالات من الفوائد العظيمة للبشرية، إلا أنها في الوقت ذاته مهدت السبيل إلى بروز أنماط جديدة من الجرائم بالغة الخطورة، ظهرت تلك الجرائم بعد أن تم ربط شبكات الحاسب وأنظمة المعلومات بالشبكة العالمية للإنترنت، وهذه الجرائم تتميز بسرعة التنفيذ وحداثة الأسلوب والقدرة على محو آثارها، وتعدد صورها وأشكالها. وتستمد هذه الدراسة أهميتها كونها تسلط الضوء على الدلائل والمؤشرات الملموسة التي تتكهن بأن الإرهاب الإلكتروني سيكون المكوّن الأساسي للحرب العالمية حاضراً ومستقبلاً. ويحاول الباحث من خلال هذه الدراسة الإجابة عن سؤال حول الإرهاب الإكتروني واقعه، مفهومه، دوافعه، أشكاله، وسائل ارتكابه ومراحله بالإضافة إلى ماهية الآليات والإستراتيجيات الواجب اتخاذها لمواجهته، وعليه فإن هذه الدراسة تناقش عدة موضوعات منها التعرف على ظاهرة وبيئة الإرهاب الإلكتروني وتسلط الضوء على العلاقة بين الجريمة الإلكترونية وجريمة الإرهاب الإلكتروني بالإضافة إلى سيناريوهات التهديد الإلكتروني وآليات الدفاع والتقليل من أخطار جريمة الإرهاب الإلكتروني، كما تستخلص الدراسة بنهايتها بعض التوصيات والاقتراحات لمواجهة هذا النوع من الجرائم.


**كلمات مفتاحية:** الإرهاب الإلكتروني، تقنية المعلومات والاتصالات، الجرائم الإلكترونية.

## المبحث الأول: الإطار العام للدراسة

### المقدمة

بقدر ما حققته ثورة تقنية المعلومات والاتصالات من فوائد عظيمة للبشرية، إلا أنها في الوقت ذاته مهدت السبيل إلى بروز أنماط جديدة من الجرائم بالغة الخطورة، ظهرت تلك الجرائم بعد أن تم ربط شبكات الحاسب وأنظمة المعلومات بالشبكة العالمية للإنترنت، هذه الجرائم تتميز بسرعة التنفيذ وحداثة الأسلوب والقدرة على محو آثارها، وتعدد صورها وأشكالها، ليس هذا فحسب بل اتصفت بالعالمية وبأنها عابرة للحدود، ومع التوسع في استخدام الإنترنت من قبل شرائح كبرى من الناس بدأت تشهد هجمات إجرامية من منظمات وجماعات وأفراد منتشرين حول العالم لتحقيق أهدافهم المختلفة، إحدى أهم وأحدث هذه الجرائم ما يمكن تسميته بالإرهاب الإلكتروني، الذي هو نسخة إلكترونية من الإرهاب التقليدي المادي. لقد وجد المجرمون الإلكترونيون أنفسهم في بيئة عالية التقنية سهلة الاستخدام قليلة التكلفة، مكنتهم من تنفيذ جرائمهم في أي مكان وأي زمان دون ترك أثر ملموس يساعد في ملاحقتهم وتقديمهم للعدالة.

لقد وجد العالم نفسه وجها لوجه أمام منظمات وعصابات إرهابية أوجدت لنفسها موطئ قدم على الشبكة العالمية للإنترنت فأوجدت لنفسها آلاف المواقع على هذه الشبكة، وتمكنوا عبر هذه المواقع إلى التواصل مع الممولين والمساندين والمؤيدين لهم، بل ذهبوا إلى أكثر من ذلك فتم عبر الشكبة العنكبوتية تجنيد الإرهابيين، وبث الأفكار الضالة والتدميرية لكل ما حققه الإنسان لخدمته. في هذه المواقع يتم التخطيط والتنسيق وتبادل الخبرات في مجالات عملياتهم الإرهابية، إضافة إلى استحداث التعليم الإلكتروني الإرهابي عبر الشبكة كتعليم صناعة الأسلحة والمتفجرات والألغام وطرق ووسائل تنفيذ العمليات الانتحارية، ليس هذا فحسب بل أصبحت هذه الجريمة خطراً يهدد البنى التحتية للدول كاختراق المؤسسات المالية والاقتصادية كالبنوك، واختراق البريد الإلكتروني ونشر البرامج التخريبية للأنظمة المعلوماتية. يتطرق هذا البحث إلى محاولة إلقاء الضوء على هذه الجريمة وتحديد معالمها وعلاقاتها وخصائصها وأشكالها وسيناريوهات

(*) عميد كلية أمن الحاسب والمعلومات، جامعة نايف العربية للعلوم الأمنية.

تهديداتها والخطط الإستراتيجية لمواجهتها.

## ١ ـ مشكلة الدراسة

برز الإرهاب في السنوات الأخيرة باعتباره من أهم مهددات الأمن والاستقرار في معظم دول العالم، ومع عدم الاتفاق العالمي على تعريف موحد للإرهاب، إلا أن الكل يجمع على أنه من أبشع جرائم العصر وأكثرها دموية، حيث يقوم على استباحة الحرمات وترويع الآمنين الذين لا صلة لهم في الغالب بما يزعم الإرهابيون أنهم يناضلون من أجلهم (١٠). مع تنامي وتطور أنظمة الكمبيوتر والمعلومات انتهز الإرهابيون والمنظمات الإرهابية فرصة ثمينة آلا وهي استخدام البنية الإلكترونية المتقدمة ونقل وتحديث الارهاب التقليدي إلى إرهاب إلكتروني بداياته كانت جريمة معلوماتية هدفها السرقة والكسب المالي، ثم تطورت إلى جريمة إرهابية إلكترونية بدوافع مختلفة محدثة أضرار بالغة في الأرواح البشرية البريئة وتدمير البنية التحتية بكافة أنواعها للدول المستهدفة وتجنيد وتمويل الإرهابيين ونشر الفيروسات، وتقديم محاضرات مجانية مباشرة في كيفية صنع المتفجرات والقنابل والغازات السامة. من هنا انبثقت فكرة هذه الدراسة التي تقوم على فرضية أساسية وهي أن الإرهاب الإلكتروني يشكل تهديداً حقيقياً لكل ما بناه الإنسان لخدمته من نظم معلومات وشبكات وحكومات إلكترونية ومحطات توليد الطاقة وتنقية المياه ووسائل المواصلات والطيران والمؤسسات المالية والاقتصادية فليس هناك حصانة حقيقية لأي بنى تحتية في نظام في أي دولة تواجه مثل هذا الإرهاب الحديث، ومن هنا يستلزم التأكيد على أهمية التعرف على هذه الظاهرة وسيناريوهات تهديداتها للوصول إلى اقتراح آليات المواجهة للتقليل من مخاطرها.

## ٢ ـ أهمية الدراسة

تستمد هذه الدراسة أهميتها من موضوعها ـ الإرهاب الإلكتروني ـ الذي يتكهن اختصاصيو تقنية المعلومات والاتصالات بأنها ستكون الحرب العالمية حاضراً ومستقبلاً، تفاقمت هذه الظاهرة في الكثير من دول العالم مستفيدة من خصوصيتها التي لا تعترف بالحدود بين الدول، ونشأت في بيئة إلكترونية عالية التقدم تقنياً في مجالات أنظمة الكمبيوتر والمعلومات وازداد التوسع في استخدام الشبكات العالمية للإنترنت (Internet) حيث وصل عددهم ما يقارب المليار وثمانمائة مليون مستخدم وقدرت المباحث الفدرالية الأمريكية (FBI) خسائر الولايات المتحدة الأمريكية وحدها بسبب هذه الجريمة بأربعمائة بليون دولار سنوياً(١٩).

إن جريمة الإرهاب الإلكتروني ما هي إلا نسخة إلكترونية لجريمة الإرهاب التقليدية المادية وجدت البيئة المناسبة لتحديث وتطوير وسائل ارتكاب الجريمة، سهلة التكاليف، واستهدفت ضحاياها في أي مكان وأي زمان في العالم دون عناء التنقل والقدرة على التخفي والهروب من العدالة، حيث زاد عدد مواقع جريمة الإرهاب الإلكتروني من ١٢ موقعاً في العام ١٩٩٨م إلى ٤٨٠٠ موقعاً في العام ٢٠٠٦م (٢١)، من هنا كان لازماً البحث في الجهود الدولية والوطنية لمكافحة هذه الظاهرة.

## ٣ ـ أهداف الدراسة

تتجسد أهداف هذه الدراسة فيمايلي:

١ ـ التعرف على ظاهرة وبيئة الإرهاب الإلكتروني.

٢ ـ العلاقة بين الجريمة الإلكترونية وجريمة الإرهاب الإلكتروني.

٣ ـ سيناريوهات التهديد الإلكتروني.

٤ ـ العلاقة بين الإرهاب التقليدي والإرهاب الإلكتروني.

٥ ـ آليات الدفاع والتقليل من أخطار جريمة الإرهاب الإلكتروني.

٦ ـ الخروج ببعض التوصيات والاقتراحات لمواجهة هذه الجريمة.

## ٤ ـ التساؤل الرئيسي للدراسة

تتمثل مشكلة الدراسة في السؤال الرئيس التالي: ما واقع الإرهاب الإلكتروني: مفهومه، دوافعه، أشكاله، وسائل ارتكابه ومراحله؟ ويتفرع عن هذا السؤال السؤال الفرعي: ما الآليات والإستراتيجيات الواجب اتخاذها لمواجهته؟

## ٥ ـ منهج الدراسة

استخدم المنهج الاستقرائي والاستنتاجي في تحليل الدراسات السابقة والوصول إلى النموذج الذي تقترحه

الدراسة، وهذه الطريقة تسهم في الوصول إلى اكتشاف حقائق ومعلومات جديدة . إن الباحث يتنقل من مرحلة استقراء الجزئيات ومراقبتها إلى استخراج المقترحات واستنباط الحلول التي يتوصل بها إلى نتائج منطقية وحلول مقبولة.

## ٦ ـ مفاهيم الدراسة

ليس هناك تعريف محدد متفق عليه للإرهاب الإلكتروني، فحداثة الجريمة وعدم ارتباطها بمكان أو معنى معين يمكن التوافق عليه، أدى إلى وجود تعريفات متعددة وبما أن الإرهاب الإلكتروني ما هو إلا نسخة إلكترونية للإرهاب التقليدي المادي فإنه لزاماً البدء بتعريف الإرهاب التقليدي ليتم بعد ذلك التوصل إلى تعريف للإرهاب الإلكتروني.

**الإرهاب في اللغة:** مشتق من اللغة اليونانية بمعنى إظهار حركات جسدية ينتج عنها تخويف الآخرين(١٠).

**الإرهاب في الاصطلاح:** لعل من أهم وأفضل التعاريف الاصطلاحية للإرهاب من حيث الشمولية وتحديد سلوك الإرهاب ما توصل إليه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي فقد عرف الإرهاب بأنه: العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً على الإنسان دينه ودمه وعقله وعرضه ويشمل صنوف التخويف والأذى والتهديد والقتل بغير وجه حق وما يتصل بصور الحرابة، إخافة السبيل وقطع الطريق وكل فعل من أفعال العنف أو التهديد يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أحوالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو المرافق العامة والأملاك الخاصة أو الموارد الطبيعية(١٠).

أما على المستوى الدولي فقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات ولم يصل المجتمع الدولي حتى هذه اللحظة إلى تعريف موحد ومتفق عليه، يرجع ذلك إلى تنوع أشكاله ومظاهره وتعدد أساليبه وأنماطه واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والأيديولوجيات التي تنتهجها الدول تجاهه، فما يراه البعض إرهاباً يراه الآخر عملاً مشروعاً (١٤) وعليه فسنعرض عددًا من التعريفات كما يلي:

ـ عرفته وزارة الخارجية الأمريكية بأنه العنف المتعمد ذو الدوافع السياسية والذي يرتكب ضد المدنيين، أو غير المتنازعين وذلك بواسطة مجموعات قومية أو مجموعات شاذة منحرفة، وذلك بغية التأثير على المواطنين وترويعهم وإرهابهم(٢٧).

ـ أما وزارة العدل الأمريكية فعرفته على أنه أسلوب جنائي عنيف يقصد به التأثير على حكومة ما عن طريق الاغتيال أو التدمير أو الخطف أو ما شابهها وقد يتم على أرض الدول نفسها أو على أرض دول أخرى (٣٢).

ـ وعرفته وكالة المخابرات الأمريكية (CIA) بأنه التهديد باستعمال العنف لتحقيق أهداف سياسية من قبل أفراد أو جماعات سواء كانوا يعملون لمصلحة سلطة حكومية أو ضدها وتستهدف هذه الأعمال أحداث صدمة أو حالة من الذهول أو التأثير على جهات تتجاوز ضحايا الإرهاب المباشر أو جماعات تسعى إلى الانقلاب على أنظمة حكم معينة أو معالجة ظلم معين، أو إضعاف النظام الدولي باعتبار ذلك غاية في حد ذاته (٣١).

ـ أما المشروع الفرنسي فعرف الإرهاب بأنه خرق للقانون يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف إثارة اضطراب خطير في النظام العام عن طريق التهديد الترهيب (١١).

ـ عرفته الأمم المتحدة بأنه تلك الأعمال التي تعرض للخطر أرواحاً بشرية بريئة أو تهدد الحريات الأساسية أو تنتهك كرامة الإنسان (١١).

ـ أما القانون الدولي فقد عرفه بأنه جملة من الأفعال التي حرمتها القوانين الوطنية لمعظم دول العالم (١٠).

فيما سبق عرضه من تعاريف الإرهاب التقليدي فإنه يمكن التوصل إلى عدد من التعاريف للإرهاب الإلكتروني فيمايلي بعضاً منها:

ـ الإرهاب الإلكتروني هو إرهاب يستخدم الإنترنت وفي إمكانه التسبب في إلحاق الضرر والشلل بأنظمة المعلومات والاتصالات المدنية والعسكرية، وقطع الاتصال بين الشبكات المختلفة، وتعطيل أنظمة الطيران والدفاع الجوي، واختراق النظام المصرفي وارباك حركة المسافرين براً وجواً وشل محطات الطاقة الكهربائية ومحطات تنقية المياه أو حتى

مهاجمة القواعد الإستراتيجية المهمة مثل المواقع النووية (٣).

ـ في تعريف آخر للإرهاب الإلكتروني بأنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفيات سياسية أو عرقته أو دينية (٣).

ـ عُرف كذلك على أنه شكل آخر للإرهاب يقوم باستخدام التكنولوجيا الضاغطة بشكل سلبي متعمد من أجل إحداث آثار مدمرة وأضرار بالغة قد تشمل جميع مرافق الدولة من معلومات وخدمات بدوافع سياسية أو عرقية أو دينية(٩).

**التعريف الإجرائي**: يعرف الإرهاب الإلكتروني إجرائيًا في هذا البحث على أنه نسخة إلكترونية من الإرهاب التقليدي المادي، نشأ هذا الإرهاب في أحضان تقنية المعلومات والاتصالات والإنترنت واستفاد ارهابيو هذه الجريمة من هذه التقنية للقيام بهجمات غير شرعية ضد أهداف وبنى تحتية أوجدت لخدمة الإنسانية، من هذه الأهداف شبكات الطاقة والكهرباء وشبكات المياه، وشبكات الحاسب وأنظمة المعلومات، المواقع العسكرية والمدنية وحركة الطيران والمواصلات وغيرها من البنى التحتية والهدف من هذه الهجمات اخضاع الحكومات ونشر الخوف والرعب في أوساط الشعوب تحقيقاً للأهداف الإرهابية سواء كانت دينية أو سياسية أو اجتماعية أو اقتصادية.

## ٧ ـ الدراسات السابقة

رغم ندرة الدراسات السابقة التي تناولت الإرهاب الإلكتروني، خصائصه وأسبابه وأهدافه وأشكاله وطرق التصدي له. فقد حصل الباحث على عدد قليل من الدراسات العربية وأما الغربية التي تناولت هذه الظاهرة فكان لها النصيب الأوفر ويرجع الباحث السبب في ذلك إلى أن تقنية الإنترنت وظاهرة الإرهاب الإلكتروني إنتاج غربي، فقد سبق الجميع للتصدي له، بعكس العالم العربي والإسلامي الذي كان النشاط البحثي والأكاديمي في هذا الموضوع لم يرق إلى مستوى وخطورة هذه الظاهرة.

**أ ـ دراسة السند بعنوان وسائل الإرهاب الإلكتروني**

وسائل الإرهاب الإلكتروني، حاولت الدراسة الكشف عن خصائص وتصنيفات جريمة الإرهاب الإلكتروني وإلى حماية الفرد والمجتمع من آثارها الضارة والدعوة إلى العمل الجماعي لتطوير زيادة القدرات الأمنية العلمية والعملية للتعامل مع هذه الجريمة والوقاية منها بدءاً بإجراءات الكشف عنها وجمع أدلتها الرقمية إلى تقديمها للجهات القضائية(٩).

**ب ـ دراسة ناجري Nagri بعنوان**

Cyber Terrorism; Vulnearabilities and Policy "Issues، "Facts behind the Meth

الإرهاب الإلكتروني؛ نقاط الضعف، قضايا وإجراءات حقائق ليست وهم:

ركزت هذه الدراسة على أنه بعد الحادي عشر من سبتمر، تم التركيز بشكل عريض على كل ما له علاقة بظاهرة الإرهاب، وتم التركيز بشكل قوي على أحد فروعه المستجدة وهو الإرهاب الإلكتروني. ورغم هذا النقاش والاهتمام بهذه الموضوعات إلا أنه لم يكن هناك اهتمام وإنتاج مساو لأهمية وخطورة هذه الظاهرة وذلك من الجانب الأكاديمي والبحثي . فلم تظهر لنا أبحاث ذات عمق تقدم أعداد وأماكن المجموعات الإرهابية التي تستخدم الإنترنت في عملياتها الإرهابية. حاول هذا البحث سد النقص الحاصل وإجراء دراسة عميقة مع إحصائيات لأعداد ومراكز وأماكن الجماعات الإرهابية التي تقوم بأعمالها بدوافع سياسية واقتصادية ودينية، وتحقيق أكبر نتائج من التدمير في الأهداف التي تستهدفها جماعات الإرهاب الإلكتروني(٣٣).

**ج ـ دراسة الشثري بعنوان الإرهاب الإلكتروني**

تطرقت هذه الدراسة إلى الجرائم الإلكترونية الإرهابية ضد حق الملكية بأنواعها، كسرقة البطاقات الائتمانية، وسرقة الملكية الفكرية للمكونات الرقمية، وسرقة وقت الإنترنت، وتطرقت كذلك إلى وسائل الإرهاب الإلكتروني المستخدمة في مثل هذه الجرائم كالبريد الإلكتروني، والدخول إلى المواقع وسرقة محتوياتها ومن ثم تدميرها، وانتهت الدراسة بعرض شامل لسبل مواجهة هذا النوع من الجرائم(١٠).

**د ـ دراسة عبد الغني بعنوان جهود المملكة العربية السعودية في التصدي للإرهاب الإلكتروني**

قامت الدراسة باستعراض جهود المملكة العربية

السعودية في التصدي للإرهاب الإلكتروني، وأوضحت الدراسة أن التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة، تخضع للأحكام الشرعية المستمدة من الكتاب والسنة، وفي حدود تلك الأحكام تقوم جهات التصدي للجريمة الإرهابية الإلكترونية بوضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة، كما تقوم الجهات الأمنية والقضائية والحقوقية بتطبيق تلك الأحكام واللوائح على القضايا المختلفة(١١).

**هـ ـ دراسة ويلسون بعنوان**

Botnets, Cybercrime, and Cyber Terrorism Unlnerabilities and Policy Issues for Congress

فيروس الشبكات، والجريمة المعلوماتية وجريمة الإرهاب الإلكتروني مواطن الضعف، وقضايا إجرامية تقرير مقدم لمجلس الشيوخ الأمريكي.

ناقش هذا التقرير الذي قدمته الخدمات البحثية لمجلس الشيوخ Congressional Research Services الخيارات المفتوحة في الوقت الحاضر للجماعات الإرهابية والمتوفرة على الشبكة العالمية للإنترنت والتي بواسطتها يستطيع مجرمو الإرهاب الإلكتروني والمنطلقين بدوافع سياسية ودينية واجتماعية من إحداث ضربات تدميرية مستهدفة البيئة التحتية والإستراتيجية للولايات المتحدة الأمريكية(١٤).

**و ـ دراسة الشهري بعنوان قانون دولي موحد لمكافحة الجرائم المعلوماتية (تصور مقترح)**

قدم الباحث تصوراً مقترحاً لقانون دولي موحد لمكافحة الجرائم المعلوماتية، استعرض الباحث العديد من القوانين الوطنية للعديد من دول العالم وظهر للباحث أن جميع هذه القوانين سنت بطريقة مستقلة تفتقر إلى إطار يجمعها، هذه الاستقلالية برهنت على الغياب التام للتنسيق وتبادل الخبرات استعرض كذلك اتفاقية مجلس أوروبا لجرائم الحاسوب الذي اعتبره الإطار والأساس للقانون الدولي المقترح(٧).

**ز ـ دراسة سلطان بعنوان الحماية الدولية والقانونية للبيئة الإلكترونية من الجريمة والإرهاب**

ركز الباحث في هذه الدراسة على مشكلة الإرهاب الإلكتروني والجريمة الإلكترونية، من خلال الحديث عن الحماية الدولية والقانونية للبيئة الإلكترونية من الجريمة والإرهاب وتوصل في هذه الدراسة إلى أنه حتى وقتنا الحاضر لا توجد طرق مضمونة لحماية النظام الإلكتروني، وليس هناك صعوبة كبيرة تواجه مجرموا الأنظمة الإلكترونية(١٣).

**ح ـ دراسة الناصر بعنوان الإرهاب الإلكتروني:**

أشارت الباحثة إلى أن الإرهاب الإلكتروني يرتبط بالتطورات التي تحدث في مجتمع المعلومات، فهو يزداد خطورة وفتكاً كلما زاد التقدم في المجال المعلوماتي، وأضافت الباحثة من أنه إذا لم يدرس هذا الإجرام ولم يخطط لمواجهته فإن الدمار الذي قد يلحقه بأنظمة المعلومات التي تتحكم في كل مرافق الحياة في المجتمعات المعتمدة على الكمبيوتر والإنترنت قد لا يتصوره العقل(١٤).

**ط ـ دراسة لويس بعنوان تقييم خطورة جرائم الإرهاب الإلكتروني وحرب الفضاء وغيرها من جرائم الإرهاب الفضائي**

Assessing the Risks of Cyber Terrorism, Cyber war and Other Cyber threats

قدمت هذه الدراسة إلى مركز الإستراتيجيات والدراسات الدولية Center for strategic and International Studies Washington, Dc. وبينت أنه لإعادة تقييم خطر الإرهاب الإلكتروني فإنه يستلزم دراسة أربعة عناصر رئيسة هي:

- الحاجة إلى وضع جريمة الحرب الإلكترونية والإرهاب الإلكتروني في السياق التاريخي للهجمات ضد البنية التحتية.
- الحاجة إلى دراسة الهجمات الإرهابية الإلكترونية على خلفية فشل البنية التحتية (كانقطاع التيار الكهربائي، تأخير الرحلات الجوية وتعطل الاتصالات التي تحدث عادة والتي يمكن استغلالها من قبل الإرهابيين لزيادة تأثير هجماتهم الإرهابية).
- الحاجة إلى قياس اعتماد البنية التحتية على شبكات الحاسب.
- الحاجة إلى استخدام وسائل مكافحة هذه الجريمة على الإنترنت في سياق الأهداف الاقتصادية وبواعث الإرهابين والتأكد من نجاح هذه الوسيلة(٢١).

**ي ـ دراسة جانيت Janet بعنوان**

Janet Cyber Terrorisn: Astudy of the Extent of Coverage in Computer Security Textbooks

**الإرهاب الإلكتروني: دراسة حول مدى تغطية كتب ومقررات الحماية من جرائم الكمبيوتر للإرهاب الإلكتروني:**

تطرقت الدراسة إلى أنه بعد الحادي عشر من سبتمبر، اضطرت الولايات المتحدة الأمريكية إلى مراجعة جميع إجراءاتها الأمنية، إضافة إلى توعية الشعب بكافة وسائل الإعلام بخطورة جريمة الإرهاب الإلكتروني وما يمكن أن يقدم عليه مجرموا هذه الجريمة من أفعال تدميرية للأفراد والممتلكات وأوضحت هذه الدراسة إلى أنه لمواجهة هذا النوع من الجرائم فإنه يجب الاستعداد لها بكافة الوسائل، من هذه الاستعدادات الحرص على انخراط عدد كافي من الطلبة في تخصصات مواجهة الجرائم الإلكترونية وجرائم الإرهاب الإلكتروني بشكل خاص، قام الباحث باختيار ستة عشر مقررًا دراسياً في اختصاص مواجهة الجرائم الإلكترونية لمعرفة مدى تغطية هذه المقررات لهذه الجريمة، كانت حصيلة الدراسة إلى أن هذه الجريمة لم يتم تغطيتها في هذه المقررات بالقدر الكافي، وأوصت الدراسة بوجوب تزويد مدرسي مثل هذه المواد بقوائم بالمواقع الإلكترونية المتخصصة في مواجهة هذه الجريمة بالإضافة إلى قائمة أخرى بعناوين الكتب المختصة لإعطاء الطالب فرصة الاستعداد لمواجهة جريمة الإرهاب الإلكتروني(٣٥).

**ك ـ دراسة يوجين Engene بعنوان**

Cyber warfare and Cyber terrorism: the need for a New U.S Strategic Approach

الحرب الإلكترونية، والإرهاب الإلكتروني: حاجة الولايات المتحدة إلى خطط إستراتيجية جديدة:

قدمت هذه الدراسة إلى معهد سلامة الإنترنت the Cyber Security Institute بواشنطن الولايات المتحدة الأمريكية، وقد قام الباحث باستعراض وتقييم جاهزية الولايات المتحدة الأمريكية لمواجهة الإرهاب الإلكتروني، وخلصت الدراسة إلى أن خطط الدفاع الإستراتيجي للولايات المتحدة الأمريكية لمواجهة تهديدات هذه الجريمة لا زالت ضعيفة وليست جاهزة وأضاف أنه لدى أعداء الولايات المتحدة الأمريكية القدرة على شن هجمات مدمرة من أي مكان في العالم ضد الولايات المتحدة(٣٤).

**ل ـ دراسة العجلان بعنوان حماية أمن المعلومات والخصوصية في قانون الإنترنت**

في هذه الدراسة بيان أن خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات، تستطيع الجماعات والمنظمات الإرهابية تدمير البنية التحتية المعلوماتية وإغلاق المواقع الحيوية وشل محطات إمداد الطاقة والمياه، واختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، وخلص الباحث إلى أن الإرهاب الإلكتروني هو إرهاب المستقبل، وهذا الخطر القادم نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها من بعد وتوفير السلامة والأمن للإرهابيين(١٠).

**م ـ دراسة موداي Mudawi بعنوان**

Cyber Terrorism: The new Kind of Terrorism

**الإرهاب الإلكتروني: الإرهاب الجديد:**

ركزت هذه الدراسة على مفهوم جريمة الإرهاب الإلكتروني من منظور ثلاث إدارات رئيسة لمواجهة الإرهاب بالولايات المتحدة الأمريكية وهي المباحث الفدرالية (FBI) وزارة الخارجية وجهاز الإستخبارات الخارجية (CIA)، كما تطرقت إلى خطورة هذه الجريمة والجهود الوطنية والدولية لمكافحتها(٣٦).

**ن ـ أصدر مركز تقييم التهديدات المترابطة بكندا Integroled (threats Assessment Center (ITAC**

دراسة بعنوان A framework for Understanding Terrorist Use of the Internet

إطار لفهم استخدام الإرهابيين للإنترنت

ووضعت هذه الدراسة الخطوط العريضة لبيان كيفية استخدام الإرهابيين للإنترنت، بفاعلية للحصول على أكبر

قدر من النتائج التي تنصب في صالح المنظمات الإرهابية، أتى على رأس القائمة تجنيد ودعم وتخطيط العمليات الإرهابية في الأماكن المختارة من قيادات هذه المنظمات، واستطردت الدراسة إلى أن هناك ثلاث طرق من النشاطات على الإنترنت:

الأولى: الأعمال النشيطة (Activism) ويقصد بها استخدام الإنترنت لدعم قضاياهم دون تعطيل أو تخريب الإنترنت والمثال على ذلك البحث عن المعلومات، إنشاء مواقع وملئها بالدعايات، إرسال إصدارات ووسائل عبر البريد الإلكتروني واستخدام الإنترنت للنقاش، خلق تحالفات وتنسيق النشاطات.

الثانية: القرصنة (Hacktivism) وهذه تجمع بين العمليات النشطة والقرصنة ومثال هذه الطريقة، العمليات التي تستخدم القرصنة ضد مواقع إنترنت بقصد التعطيل وبدون إحداث أضرار جسيمة مثل قنابل البريد الإلكتروني اقتحام أجهزة الحاسب، نشر ديدان وفيروسات الكمبيوتر.

الثالثة: الإرهاب الإلكتروني (Cyber Terrorism) ويقصد به إلتقاء الإنترنت مع النشاطات الإرهابية والمثال على ذلك استخدام قرصنة الإنترنت بدافع سياسي بقصد إحداث خسائر فادحة في الأرواح والممتلكات، اقتحام وتعطيل أنظمة الدولة للطاقة، والمواصلات والمؤسسات المالية أو حتى مواقع الطاقة النووية، استهداف المواقع الأمنية العسكرية تعطيل الاتصالات وتعطيل أسواق رأس المال، هذه العمليات جزء من نشاطات جريمة الإرهاب الإلكتروني(٣٧).

## المبحث الثاني: الجريمة الإلكترونية

### ٢ . ١ نشأة الجريمة الإلكترونية

بدأ نشاط الجريمة الإلكترونية قبل وجود الحاسب الآلي، ففي العام ١٨٧٨م حينما كان الهاتف اللاسلكي متداولاً في ذلك الوقت، كان أغلب العاملين في شركاته من جيل الشباب المتحمس ولمعرفة المزيد من هذه التقنية الجديدة قام بعض من هذه الفئة من الشباب بارتكاب ما نسميه في الوقت الحاضر الجرائم الإلكترونية عندما قاموا بالتنصت على المكالمات الهاتفية، لم يكتفوا بذلك بل قاموا بإجراء مكالمات على حساب شركات أخرى وزوروا بعض الفواتير، فكانت تلك بداية الجرائم الإلكترونية، وفيما بين الأعوام ١٩٤٦ إلى ١٩٦٩م عندما ظهر الحاسب الآلي حاول العديد من موظفي شركات الحاسب من ارتكاب جرائم إلكترونية إلا أنهم جوبهوا بصعوبات كبيرة منها الحراسات القوية التي كانت تفرض على هذه الأجهزة، بالإضافة إلى كبر الأجهزة وكان المخرب الإلكتروني في ذلك الوقت (hacker) هو من مبرمجي شركات الحاسب الآلي، أما العصر الذهبي للمجرمين الإلكترونيين فقد بدأ منذ العام ١٩٨٠م حتى وقتنا الحاضر (١٩).

### ٢ . ٢ العلاقة بين الجريمة الإلكترونية وجريمة الإرهاب الإلكتروني

العلاقة المشتركة بين الجريمة الإلكترونية والإرهاب الإلكتروني أن كل منهما جرائم وأن محل ارتكاب الجريمة في كلاهما واحد وهو البيئة الإلكترونية، قد تكون ضد فرد أو منظمة أو دولة أما الإرهاب الإلكتروني فهو ضد المجتمع الدولي بأكملة فعندما يقع الهجوم على دولة معينة فكأنه وقع على المجتمع كله، يقول Ashish Pandey أن جميع الأعمال الإرهابية هي جرائم إلكترونية ولكن ليست جميع الجرائم الإلكترونية تدخل ضمن الأعمال الإرهابية(٣٦).

### ٢ . ٣ تصنيف الجرائم الإلكترونية

هناك عدة تصنيفات لجرائم الحاسب الآلي، إلا أنها تعددت وتباينت ولم تتفق على تصنيف واحد، إلا أن هذه التصنيفات، وأن تبدو مختلفة في ظاهر الأمر، إلا أن هناك قاسماً مشتركاً بينها، وهو أن هناك طائفة من الجرائم ترتكب بواسطة المعلوماتية وطائفة أخرى يتركز الاعتداء فيها على تكنولوجيا المعلومات، وهذا القاسم المشترك يمكن القول بأنه يشمل كل الأفعال التي تعد من جرائم الحاسب الآلي، ذكر القاسم (٢٠) إلى أن الجرائم الإلكترونية يمكن أن تصنف إلى:

١ ـ المعلومات هي الهدف: وهذه تكون فيها المعلومات هي الهدف وتتضمن سرقة المعلومات والسجلات وإلغاء وتعطيل البرامج ونظم تشغيل وغيرها من جرائم الاختراق والتطفل على الأنظمة المعلوماتية، وفي هذه الجريمة يستخدم الجاني تقنية المعلومات في جريمته.

٢ ـ نشر معلومات بطريقة غير مشروعة: كاستخدام المواقع الإلكترونية والبريد الإلكتروني لنشر الرذيلة كالاتجار بالجنس البشري ونشر الأفلام الإباحية وأنشطة القمار والاتجار بالمخدرات وغسل الأموال.

٣ ـ استخدام تقنية المعلومات كوسيلة لارتكاب الجريمة والجرائم من هذا النوع تتضمن الاحتيال واستعمال أجهزة الصرف الآلية وبطاقات وحسابات مزورة وسرقة البيانات وتحويل الأموال غير المشروعة، والتحويل من حساب لآخر وسرقة بطاقات الإئتمان، ويدخل ضمنها استخدام الهواتف المتنقلة للتشهير بالآخرين وانتهاك خصوصيات الناس.

٤ ـ تأثير الحاسب في الجرائم الأخرى: في هذا النوع من الجرائم الإلكترونية ليس ضرورياً أن تكون وسائل تقنية المعلومات استخدمت في الجريمة ولكن لها علاقة بالارتكاب ومن أمثلتها ارتكاب جريمة القتل، وذلك بتغيير مقدار جرعة الدواء لمريض في نظم معلومات مستشفى معين.

٥ ـ جرائم لها علاقة بانتشار تقنية المعلومات ومن أمثلة هذه الجرائم قرصنة البرامج واعادة بيعها بدون إذن من المالك.

## ٢ . ٤ خصائص الجرائم الإلكترونية

تتصف الجرائم الإلكترونية بخصائص تميزها عن غيرها من الجرائم ومن هذه الخصائص مايلي:

١ ـ سهولة ارتكاب هذه الجرائم نظراً لاستخدام الوسائل ذات الطابع التقني.

٢ ـ سهولة إخفاء معالم الجريمة وصعوبة تتبع مرتكبها.

٣ ـ حرفية ارتكاب الجريمة مما يتطلب قدراً كبيراً من الذكاء والمعرفة من جانب مرتكبها وقدراً أكبر من الحرفية من جانب من يتولى الإشراف على جهود مكافحتها.

٤ ـ سرعة ارتكاب هذا النوع من الجرائم لاعتمادها على وسائل الاتصال الحديثة.

٥ ـ آثارها مدمرة فيمكن أن تحدث هزات كبيرة لاقتصاديات الدول.

٦ ـ ترتكب الجرائم عبر الشبكة العالمية للإنترنت (Internet) بدقة بالغة نتيجة دقة أدوات الجريمة.

٧ ـ جرائمها تتسم بالغموض حيث يصعب إثباتها والتحقيق فيها كما هو الحال في الجرائم التقليدية.

٨ ـ هذا النوع من الجرائم تعتبر من الجرائم الإلتكرونية غير المادية.

٩ ـ مرتكبو هذه الجرائم لهم صفات مميزة من حيث الثقافة والعلم التكنولوجي.

١٠ ـ لا حدود جغرافية لها، حيث ألغت شبكة الإنترنت أي حدود جغرافية فيما بين الدول فالجاني قد يكون في بلد وضحيته في قارة بعيدة وشهود الجريمة في بلدان أخرى (٣).

## ٢ . ٥ أهداف الجرائم الإلكترونية

من المعروف أن أكثر الجرائم الإلكترونية التي يتم ارتكابها يكون الهدف منها هو الحصول على الأموال غير المشروعة، يتم الحصول عليها من سرقة الحسابات البنكية وأرقام البطاقات الائتمانية وسرقة الممتلكات الفكرية (Intellectual Property)، وتزوير المستندات والشيكات ونسخ البرامج وإعادة بيعها بدون تصريح، كما أن هذه الجرائم يتم ارتكابها بهدف الحصول على المعلومات الإلكترونية التي تكون محفوظة إما في أجهزة الحاسب الآلي أو تلك الموجودة على شبكة الإنترنت، إلا أن ذلك لا يعني أن هناك جرائم أخرى يكون لها هدف آخر غير الحصول على المعلومات مهما كانت أهمية تلك المعلومات الإلكترونية:

١ ـ المعلومات (Information): الحصول عليها أو تغييرها أو حذفها يعتبر من الجرائم التي يكون الهدف منها المعلومات، ومعظم تلك الجرائم التي يكون الهدف منها المعلومات هي في الغالب الأعم جرائم هدفها اقتصادي للحصول على مزايا أو مكاسب مالية.

٢ ـ أجهزة الكمبيوتر: إذا كان الهدف من ارتكاب الجرائم الإلكترونية غير شبكة الإنترنت هو أجهزة الكمبيوتر فالغالب الأعم يكون الهدف هو تخريب وإعطاب واتلاف تلك الأجهزة أو تعطيلها والفيروسات هي الأداة في الغالب الأعم.

٣ ـ الأشخاص أو الجهات : معظم الجرائم المعلوماتية التي ترتكب عبر شبكة الإنترنت تستهدف أشخاص أو جهات بعينها (١٧).

## ٢ . ٦ أسباب ودوافع ارتكاب الجرائم الإلكترونية

هناك العديد من الغايات التي تدفع الشخص لكي يرتكب إحدى جرائم الكمبيوتر من هذه الأسباب:

١ ـ حب المغامرة والإثارة: يبدأ بعض القراصنة قبل ارتكاب جريمته باصطياد جريمته عن طريق المحادثة وتبادل المعلومات، يحتفظ بها بعض الوقت ثم يعاود في وقت لاحق اختراق هذه المواقع أما للشهره والاثارة أو ايقاع الأذى.

٢ ـ اشباع غريزة بعض القراصنة بحب الظهور أمام الأقران كاثباته قدرته على إختراق الأنظمة المحصنة واكتشاف نقاط ضعفها.

٣ ـ تقوم بعض الشركات الشهيرة بتوظيف بعض القراصنة لاستخدامهم في فحص قدرة أنظمة الحماية والسرية في برامج الشركات.

٤ ـ المؤثرات الشخصية: ومن أمثلته سعي بعض الشركات التجارية والصناعية إلى الحصول على برامج ومعلومات مسروقة بواسطة موظفي أنظمة الحاسب والمعلومات من الشركات المنافسة مقابل الرشوة أو الإغراء أو الخداع أو استغلال نقاط ضعف هؤلاء الموظفين.

٥ ـ تحقيق مكاسب مالية: المساومة على البرامج أو المعلومات المتحصلة عن طريق السرقة أو الاختلاس تعتبر في بعض الأحيان الهدف من ارتكاب الجريمة(١٣).

## ٢ . ٧ خسائر الجريمة الإلكترونية

صدر عن معهد فنومن دراسة شملت عدد ٤٥ شركة كبرى في الولايات المتحدة تعرضت لهجمات إلكترونية كانت نتائج هذه الدراسة مايلي:

١ ـ الجريمة الإلكترونية واحدة من أخطر الجرائم في العصر الحاضر.

٢ ـ بلغ المتوسط الحسابي لخسائر هذه الشركات المختارة حوالي أربعة ملايين دولار في السنة لكل شركة.

٣ ـ كانت الحدود الدنيا لهذه الشركات المليون دولار فأعلى وكانت خسائر بعضها في السنة الواحدة يصل ٥٢ مليون دولار.

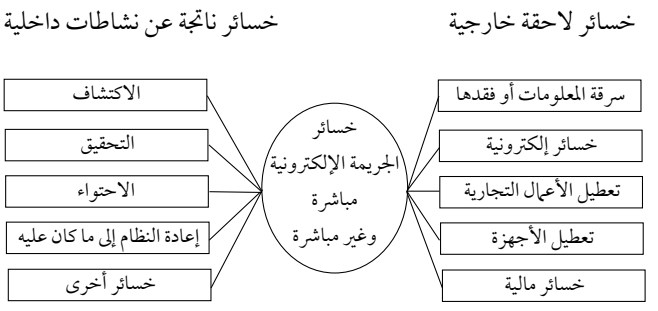
٤ ـ لم تنجو أي شركة من هذه الشركات من الاعتداءات الإلكترونية فقد بلغ معدل الاعتداءات الأسبوعية لكل شركة من هذه الشركات خمسين هجوماً في الأسبوع الواحد.

٥ ـ حدثت الهجمات الإلكترونية الأكثر فداحة عن طريق مواقع الإنترنت كاقتحام المواقع ونشر الفيروسات.

٦ ـ ومن الجرائم الأكثر فداحة التي حدثت للغالبية العظمى لهذه الشركات هي سرقة ممتلكات الشركة الفكرية (Intellectual Property) سرقة الحسابات البنكية (Bank Accounts) نشر الفيروسات المتعمد. نشر معلومات سرية بهدف تدمير البنية التحتية الإلكترونية لهذه الشركات، نشر إحصائيات نجاحات مجرمي أنظمة المعلومات على أعداد كبيرة من المواقع بقصد التأثير على الشركات.

٧ ـ تحملت هذه الشركات خسائر باهظة لإعادة الأنظمة إلى وضعها الطبيعي بعد الهجمات (Recovory)(٣٧).

المحصلة النهائية لهذه الدراسة يوضحها الشكل رقم (١) التالي:




الشكل رقم (١) يبين خسائر الجريمة الإلكترونية للشركات الأربع والخمسين

لخصت خسائر الشركات المشتركة في هذه الدراسة في الشكل رقم ١ والذي قد يكون هو الإطار المرجعي لأي دراسة تختص بالجرائم المعلوماتية حيث أنه يوضح وبشكل واضح أنواع الخسائر يظهر فيه الخسائر الداخلية والخارجية والتي كانت تعامل في السابق على أنها قائمة واحدة يضع هذا الشكل بنية تحتية لايجاد نموذج مواجهة مبنى على مواجهة تعمل بشكل متوازي وفي اتجاهات متعددة وباتجاه مصادر انطلاق هذه الجرائم، فكما هو ملاحظ في الشكل قسمت الخسائر إلى قسمين تشكل في مجموعها الخسائر الكلية للمنظمة فالقسم الأول يشمل نشاطات داخلية من مهام المنظمة أتت بعد أن وقعت الجريمة أما القسم الثاني فهو الناتج الخارجي للخسائر الحاصل من الهجوم على المنشأة وكما ذكرت سابقاً هذا التقسيم يساعد مجموعات مواجهة

هذه الجريمة لوضع نموذج الحل المبني على الدراسة المتعمقة للجريمة.

إضافة إلى ما سبق إيضاحه فقد اشارت دراسة أخرى إلى أن المباحث الفيدرالية الأمريكية FBI قدرت خسائر الولايات المتحدة الأمريكية بسبب الجرائم الإلكترونية ما يقارب أربعمائة بليون دولار سنوياً(٣٥).

## المبحث الثالث: جريمة الإرهاب الإلكتروني

ظهر الارتباط بين الإرهاب وشبكة الإنترنت بشكل واضح بعد أحداث سبتمر ٢٠٠١، وانتقلت المواجهة ضد الإرهاب المادي المباشر إلى مواجهة الإنترنت وبدأت تظهر نتائج هذه المواجهات لتعكس أن جرائم الإنترنت الإرهابية حقيقية ومدمرة وخصوصاً عندما أدخل عنصر الإرهاب بشكل رئيسي فيها (١٤)، أن النظرة إلى الإرهاب الإلكتروني كانت تنحصر في الأعمال الإرهابية التخريبية مثل اختراق المواقع الإلكترونية العسكرية والمدنية، واغفلت تماماً أنشطة أكثر خطورة ألا وهي الاستخدام اليومي في وقتنا الحاضر للإنترنت من قبل المنظمات الإرهابية لتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم، وتم اغفال حقيقة أن الوجود الإرهابي النشط على الشبكة العنكبوتية هو متفرق ومتنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم، فسرعان ما يغير نمطه الإلكتروني، ثم يختفي ليظهر مرة أخرى بشكل مغاير وعنوان جديد بعد فترة قصيرة وأفضل مثال على ذلك بأن الجهود الحثيثة لمنع منظمة القاعدة من استخدام شبكة الإنترنت باءت بالفشل، فعند اختراق أحد مواقفهم واستئصاله من الشبكة تظهر عدة مواقع جديدة (٢١. إن الإرهاب الإلكتروني لا يختلف عن الإرهاب المادي التقليدي إلا في نوعية الأداة المستخدمة لتحقيق الغرض الإرهابي، فبينما الإرهاب المادي وسائله مادية بحتة من سلاح ومتفجرات وغيرها من الأسلحة المادية يقوم الإرهاب الإلكتروني ليعتمد على استغلال الإمكانات والتقنية واستخدام وسائل الاتصال والإنترنت من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم.

### ٣ . ١ نشأة الإرهاب الإلكتروني

قدمت دِنِنْج Denning أستاذة الحاسب الآلي بجامعة جورج تاون في شهادتها أمام اللجنة الخاصة بمتابعة الإرهاب بمجلس الكونجرس بالولايات المتحدة، عرضاً مختصراً لنشأة الإرهاب الإلكتروني كمايلي:

- في العام ١٩٩٧م استطاع الآلاف من المكسيكيين تدمير أحد المواقع الإلكترونية المتخصص في بيع مواد فيديو على الإنترنت وذلك بإغراقه بآلاف الرسائل الإلكترونية.
- في العام ١٩٩٨م استطاعت منظمة نمور تأميل إيلام في سيرلانكا تدمير مواقع سفارات سيرلانكا بواسطة بعث ما يقارب ٨٠٠ رسالة إلكترونية يومياً لكل سفارة.
- في العام ١٩٩٩م فجرت أجهزة الحاسب الآلي بالناتو بواسطة ما يسمى بقنابل البريد الإلكتروني التي أرسلها المحتجون على حرب كوسوفو.

وعلقت دِنِنْج على أن الأمثلة السابقة قد يسميها البعض جرائم حاسب آلي، وتورد أمثلة لنشأة الإرهاب الإلكتروني كمايلي:

- في العام ١٩٩٧م استطاع أحد المحترفين من إنشاء برنامج له القدرة على تحويل الفواتير الخاصة به إلى أشخاص آخرين.
- وفي العام ١٩٩٩م استطاع أحد المجرمين الإرهابيين من اغتيال أحد خصومه السياسيين وذلك بالدخول على ملفه بأحد المستشفيات وتغيير مقادير العلاج الذي يصرف له واستطاع قتله.
- في العام ٢٠٠١م وبعد حادثة اصطدام إحدى الطائرات الجوية الأمريكية بطائرة صينية واسقاطها قام القراصنة الصينيين بتدمير آلاف المواقع الإلكترونية الأمريكية المهمة منها وزارة الدفاع والخارجية مسببة ملايين الدولارات من خسائر إعادة هذه المواقع لوضعها قبل التدمير.
- بعد الحادي عشر من سبتمبر ٢٠٠١ ظهر الإرهاب الإلكتروني بشكل مكثف بل وفي كافة أنحاء العالم.
- في العام ٢٠٠٧ قامت الولايات المتحدة الأمريكية

بالتعاون مع الناتو في إرسال فريق متخصص في جرائم الإرهاب الإلكتروني إلى استونيا لمساعدة هذا البلد الذي تعرض لهجوم إلكتروني وجه لجميع أنظمة المعلومات وإيقافها(٢٤).

## ٣ . ٢ تطور الإرهاب التقليدي إلى الإرهاب الإلكتروني

الإرهاب الإلكتروني ما هو إلا النسخة الإلكترونية للإرهاب التقليدي، والذي نشأ وترعرع في أحضان بيئة تقنية المعلومات والاتصالات وشبكة الإنترنت. تم خطف هذه التقنية من قبل مجرمي الإرهاب وتم تسخيرها لأهدافهم الإجرامية وتم استقطاب العديد ممن لهم خبرة وعلم في هذه التقنيات فوجدوا ضالتهم في هذه البيئة الجذابة وتم التركيز عليها في العديد من عملياتهم للأسباب التالية:

١ ـ بيئة تقنية المعلومات والاتصالات والإنترنت أسرع وأرخص وأدق من الطرق التقليدية للإرهاب.

٢ ـ استطاعتهم التخفي عن أعين جهات المواجهة.

٣ ـ لا يوجد حواجز مادية في طريقهم، ولا يوجد حدود دولية أو جغرافية تحول دونهم وارتكاب جرائمهم في أي بقعة من بقاع الدنيا.

٤ ـ ترتكب الجريمة الإلكترونية عن بعد.

٥ ـ تأثيرها مدمر ومروع وعنيف والخسائر البشرية والمادية كثيرة (٢٤).

لايضاح كيفية تحول الجريمة العادية التقليدية إلى جريمة إرهاب إلكتروني، نعرض فيما يلي مثالاً يوضح جرائم ارتكبت بواسطة منظمتين تعتبرها الولايات المتحدة منظمات إرهابية وهاتين المنظمتين هما منظمة نمور تحرير إيلام السيرلانكية ومنظمة UAM اليابانية، وقبل الخوض بتفاصيل جرائم تلك المنظمتين فإنه يستلزم التذكير بتعريف الإرهاب التقليدي وكذلك تعريف الإرهاب الإلكتروني.

فلقد عرفت الجريمة الإرهابية على أنها: التهديد باستعمال العنف أو استعماله لتحقيق أهداف سياسية من قبل أفراد أو جماعات سواء كانوا يعملون لمصلحة سلطة حكومية أم ضدها، وتستهدف هذه الأعمال إحداث صدمة أو حالة من الذهول أو التأثير على جهة تتجاوز ضحايا الإرهاب المباشرين (٢٥) أما جريمة الإرهاب الإلكتروني فقد عرفت على أنها: استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية (٢٦)ولتفكيك التعريفين السابقين نجد أن عناصرهما كمايلي: المكان، العمل، الوسيلة، الهدف ـ الانتماء ـ الدافع ـ المنفذ، ففي الجريمة الإرهابية التقليدية يوضح الجدول رقم (١) التالي هذه الجريمة الإرهابية المادية بعد تفكيكها إلى عناصرها الأصلية:

| عناصر الجريمة الإرهابية | المنظمة الإرهابية | المنظمة الإرهابية |
|---|---|---|
| مرتكب الجريمة | مجموعة نمور تحرير إيلام السيرلانكية | UAM اليابان |
| المكان | سيرلانكا | اليابان |
| العمل | تهديد وعنف | عنف |
| الوسيلة | خطف تحرش | غاز الأعصاب |
| الهدف | مسؤولين حكوميين (مجندين) | UAM |
| الانتماء | فعلي / إدعاء | فعلي / إدعاء |
| الدافع | تغيير اجتماعي ـ سياسي | السيطرة على اليابان والعالم |

الجدول رقم (١)

في هذا الجدول يتضح أن العنصر الأول ـ مرتكب الجريمة ـ فرداً أو مجموعة مسلحين بما يمكنهم الحصول عليه، يقومون فعلياً بمواجهة الهدف المراد، فهناك حواجز وتضاريس وحدود ووسائل مواصلات، أما عنصر المكان فهو جزء محدد من الدول اختير للفعل الإجرامي شخصاً أو مجموعة أو ممتلكات أما عنصر العمل فيعني تنفيذ العمل الجرمي أو التهديد بتنفيذه، أما عنصر الجريمة فقد تكون خطف أو تحرش أو استخدام أسلحة دمار شامل كغاز الأعصاب أما الهدف فقد يكون موظف أو مجموعة من موظفي الدولة أو العسكريين من جهات المكافحة، أما عنصر الانتماء فقد يقوم المنفذين بإعلان انتمائهم لمنظمة معينة معروفة، أو وهمية أما عنصر الدافع لإرتكاب الجريمة، فقد تكون الدوافع سياسية واجتماعية ودينية أو إحداها والتي تدعوا إلى تغيير اجتماعي أو سياسي أو فرض النفوذ، كما يظهر من أهداف منظمة UAM اليابانية، عند تحليل هذه الجريمة إلى عناصرها تتحقق الفائدة لجهات المواجهة لإعداد نموذج المكافحة المبني على دراسة كل عنصر من عناصر هذه الجريمة. أن المجرمين في ممارستهم لهذه الجريمة، ليس لديهم المرونة الكافية ولا

السرعة اللازمة، وقد يصادفهم عوائق عديدة منها العوائق الطبيعية كالحدود الدولية، التضاريس الطبيعية والمسافات البعيدة، وأيضاً يصادفهم ضعف التواصل لضعف وسائل اتصالهم التي يمكن أن يعتمد في أغلبها على التنقل من مكان لآخر لتسليم وتسلم الأوامر وتنفيذها على الطبيعة، وفي المقابل فإن سلطات مكافحة الجرائم يتمتعون بميزات عديدة على هذه المنظمات منها سهولة المراقبة، وسهولة حرمانهم من وسائل الاتصالات، وذلك بايقافها عنهم كما أنه يمكن تحديد أماكنهم بسهولة ويسر والإيقاع بهم ومواجهتهم وإحالتهم للعدالة. بعد أن انتقلت هذه الجريمة إلى درجة أعلى في ممارستها للجريمة بعد استفادتها من تقنية المعلومات والاتصالات والشبكة الدولية للإنترنت، أصبح لزاماً إعطائها ما تستحق من أهمية إبتداءً بإعطائها المسمى الذي يميزها عن الجريمة الإرهابية التقليدية وأفضل ما أطلق عليها هو جريمة الإرهاب الإلكتروني (Cyber Terrorism)، ولايضاح الفرق بينها وبين الجريمة التقليدية يجب الإشارة إلى أن ثورة المعلومات والاتصالات وتوسع استخدام شبكة الإنترنت وفرت للمجرمين الإلكترونيين ما يسمى بغرف الدردشة والمنتديات والبريد الإلكتروني، كما سهلت لهم إخفاء هوياتهم وراء أسماء مستعارة يصعب عملية التعرف عليهم ومتابعتهم، وهنا يبرز مشكلة إعداد نموذج موحد لمواجهة هذه الجريمة في الجدول التالي يوضح عناصر جريمة الإرهاب الإلكتروني، ويظهر الفارق عند مقارنته بالشكل رقم (١).

| عناصر الجريمة | منظمة تحرير ايلام | منظمة UAM اليابانية |
|---|---|---|
| مرتكب الجريمة | مجموعة/ أفراد | مجموعة / أفراد |
| المكان | سيرلانكا/ لندن/ استراليا/ حول العالم | اليابان/ أمريكا/ حول العالم |
| العمل | تهديد/ عنف/ تجنيد/ تعليم/ ودعاية إستراتيجيات | عنف/ تجنيد/ تعليم دعاية/ إستراتيجيات |
| الوسيلة | خطف/ تحرش/ دعاية/ تعليم ودعاية | غاز الأعصاب/ تعليم ودعاية |
| الهدف | موظفين حكوميين / مجندين | UAM |
| الانتماء | فعلي / ادعاء | فعلي / ادعاء |
| الدافع | تعبير اجتماعي / سياسي | السيطرة على العالم |

الشكل رقم (٢)

في الجدول السابق يلاحظ النقلة الهائلة لجريمة الإرهاب التقليدية لهاتين المنظمتين الإرهابيتين منظمة نمور تحرير إيلام ومنظمة UAM اليابانية في نوعية عملياتها بعد أن أدخلت تقنية المعلومات وأنظمة الحاسب والإنترنت في عملياتها، فالجريمة التي كانت ترتكب بواسطة مجموعات فقط لم تعد كذلك، وأصبحت ترتكب بواسطة أفراد أو فرد أو مجموعات، أما مكان الجريمة فلم يعد مكاناً واحداً بل أصبح العالم تحت تصرفهم فقد يمارسون جرائمهم من أماكن مختلفة من العالم لاجتياز جريمة الإرهاب الإلكتروني الحدود والتضاريس والمواقع الطبيعية واستعاضوا عنها بشبكة الإنترنت، أما تنفيذ أعمالهم فلم يعد تهديد وعنف فقط بل تعداه إلى أعداد دعايات ضخمة لهم وتجنيد وتدريب إرهابيين في مواقع مختلفة من العالم، كما أن أعداد الخطط والإستراتيجيات أصبحت من اليسر والسهولة من حيث الإعداد والتوزيع على منسوبيها بصورة فورية، وأصبح جمع الأموال والتبرعات لمنظماتهم الإرهابية لم يعد ذلك المشكلة المعقدة أما الوسائل في هذه الجريمة فلم تعد عملاً ميكانيكياً حسياً كالخطف والتحرش كما كان في الجريمة الإرهابية التقليدية، تم إضافة عمليات التعليم كصنع المتفجرات والقنابل وطريقة استخدامها وتوزيعها عبر الشبكة لأفراد المنظمات في أي بقعة في العالم، أهداف هذه الجريمة المختارة كما هي في الجريمة التقليدية إلاّ أن تنفيذها عن بعد لتستهدف موظف مكافحة الجريمة ومنسوبي الحكومات، والمجندين . منتسبي جرائم الإرهاب التقليدي والإلكتروني ينتمون إلى أماكن فعلية أو يقومون بالادعاء بانتمائهم لمكان أو دين معين كما أن دوافع جريمة الإرهاب الإلكتروني لا تختلف عن سابقتها جريمة الإرهاب التقليدي، فالهدف هو تغيير اجتماعي أو سياسي واقتصادي أو يكون ذو هدف راديكالي أعلى كالسيطرة على العالم واخضاع أمم الأرض لهذه المنظمات، خير مثال على الفرق بين جريمة الإرهاب التقيدي وجريمة الإرهاب الإلكتروني فقد يقوم مجرم إرهابي بالدخول إلى مبنى أنظمة حاسب آلي ويقوم بتدمير أجهزة الحاسب الآلي بآلات ثقيلة كالمطارق وغيرها، وقد يقوم نفس الشخص بتدمير نفس الأنظمة من مكان بعيد بواسطة فيروس حاسب آلي ولا يلزمه أي وسيلة عتاد. أو التنقل أو أي جهد يذكر.

## ٣ . ٣ خصائص الإرهاب الإلكتروني

الإرهاب الإلكتروني شكل متطور من جريمة الإرهاب التقليدي المادي يختلف عن الإرهاب المادي بأنه يقوم على استخدام التكنولوجيا بشكل سلبي متعمد من أجل إحداث آثار مدمرة بالغة وكبيرة وفي الغالب الأعم يستهدف البنى التحتية لأنظمة المعلومات والشبكات ومحطات الكهرباء والماء والمواصلات والطيران وغيرها من منشآت مدنية وعسكرية كل ذلك بدوافع سياسية أو اقتصادية أو عرقية أو دينية (٦) من خصائص الإرهاب الإلكتروني مايلي:

١ ـ لم يغير مسميات الإرهاب التقليدي ومفرداته بشكل كبير والتي عادة تستخدم في الجريمة الإلكترونية ومن أمثلتها:

ـ متطفل (Hacker) قرصان يقتحم أنظمة الحاسب بدون إذن.

ـ المخرب (Cracker): قرصان الكتروني لديه القدرة على اقتحام أنظمة الحاسب مع وجود الدافع الإجرامي.

ـ المتطفل النشط (Acktivisim) قرصان يجمع بين التطفل والتخريب.

ـ المخرب النشط (Hacktivisim): قرصان الكتروني له دوافع سياسية وتتسم أعماله بأنها ليست تدميرية من أمثلتها نشر الفيروسات بقصد الشهرة أو غيرها من المطامع الشخصية. ومن أمثلته نشر الدعايات وتشويه السمعة في المواقع الإلكترونية، تعطيل خدمات أنظمة المعلومات (Information Systems) وسرقة الهويات الشخصية(٦).

٢ ـ ينتمي الإرهابي الإلكتروني إلى جماعة إرهابية قامت باستقطابه لخبرته بأنظمة الحاسب الآلي والإنترنت وتجنيده للقيام بأعمال إرهابية إلكترونية ودربته على استخدام العديد من الأسلحة الإلكترونية الفتاكة وله القدرة والرغبة على استخدامها ومن هذه الأسلحة مايلي:

ـ أولاً: القدرة على منع الوصول لمواقع معينة على الشبكة ـ حجب المواقع ـ وذلك بايقافها وتعطيلها عن طريق إرسال الملايين من الرسائل الإلكترونية التي تؤدي في النهاية إلى حجب للمواقع المستهدفة ومنع الوصول إليها والهدف من ذلك تحقيق هدفين أولها منع الوصول والحجب والثاني نشر الدعايات الضخمة لهذا العمل وعلى نفس الموقع المستهدف نفسه.

ـ ثاني هذه الأسلحة: استخدام البريد الإلكتروني بإرسال العديد من الرسائل في آن واحد إلى أهداف معينة (Ping attack) وايقاف وتدمير المواقع المستهدفة ومن الأمثلة على ذلك (١٩) ما حدث لموقع المعهد العالمي للاتصالات بمدينة سان فرانسيسكو وهذا المعهد هو المزود الرئيسي لخدمات الإنترنت (ISP) ويستضيف مواقع لمجلات إلكترونية داعمة لنشاطات منظمة الباسك الإسبانية الانفصالية (ETA) حيث تلقى في دقائق معدودة ملايين الرسائل الإلكترونية على شكل هجمات بريد الإلكتروني ضخمة واستطاعت إيقافه بل وصل بمصدر هذه الرسائل الجرأة إلى التهديد بتدمير مواقع أخرى مساندة لهذا المعهد إن لم يستجب لطلبهم بإيقاف التعامل مع المجلة الإلكترونية التابعة لمنظمة ايتا (ETA)، وعلى أثر ذلك أجبر المعهد إلى الإذعان لطلباتهم وثم إيقاف التعامل مع هذه المجلة الإلكترونية متهما الحكومة الإسبانية بالوقوف وراء هذا الإجراء(٢٢).

ـ أما السلاح الثالث فهو القدرة على مهاجمة المواقع والدخول إليها للحصول على المعلومات المخزنة بانظمة الحاسب(٢٠).

ـ أما السلاح الرابع فهو قدرة هؤلاء المجرمين الإلكترونيين على نشر أنواع الفيروسات وتدمير وإيقاف الملايين من أجهزة الحاسبات الآلية من مواقع عديدة من أنحاء العالم.

٣ ـ صعوبة تعقب هذه الجريمة لسرعة اختفاء الأدلة المادية وسهولة إتلافها.

٤ ـ تنفذ بواسطة فرد أو مجموعة أفراد.

٥ ـ المجرم الإرهابي الإلكتروني يتميز بقدرات في استخدام التقنية الحديثة وبرمجة الكمبيوتر والتعامل معه.

٦ ـ بيئة مريحة بواسطة برنامج صغير وجهاز حاسب آلي صغير وغرفة صغيرة يستطيع المجرم انزال أفدح الخسائر المادية في أماكن تبعد عنه بمسافات بعيدة(٢٢).

٧ ـ من خصائص جريمة الإرهاب الإلكتروني أنه حتى يمكن

الإعتراف بوقوعها، هناك خمس مراحل يمر بها المجرم الإلكتروني، وهذه المراحل يجب أن تنفذ كاملةً وجميعاً وبالتوالي ليعتبر الهجوم ناجحاً:

- المرحلة الأولى: يجري المجرم استطلاعاً للضحية.
- المرحلة الثانية هي مرحلة الإختراق والدخول إلى الضحية، وفي هذه المرحلة يكون المجرم في وسط مكان الضحية وليس هناك سرقة معلومات أو تخريب في هذه المرحلة.
- المرحلة الثالثة: تنفيذ العملية الإجرامية ولازال المجرم داخل النظام لتوسيع قدراته التخريبة.
- المرحلة الرابعة: حصول التخريب والسرقة.
- المرحلة الخامسة القيام بالتعديل وحذف الأدلة لمسح ملفات دخول النظام للحماية وإبعاد التهمة عنهم.

يضيف العجلان (١٠) أن من خصائص الإرهاب الإلكتروني:

- أنه لايحتاج في إرتكابه إلى العنف والقوة، إنما يتطلب وجود حاسب آلي متصل بالشبكة العالمية بالإنترنت، ومن أهم خصائصه كونه جريمة إرهابية متعدية الحدود، وعابرة للقارات، وغير خاضعة لنطاق إقليمي محدود.
- صعوبة إكتشاف هذا النوع من الجرائم لنقص الخبرة لدى الأجهزة الأمنية والقضائية في التعامل معها.
- يتم إرتكاب هذا النوع من الجرائم بواسطة أكثر من شخص.

## ٣ . ٤ أسباب ودوافع الإرهاب الإلكتروني

لاتختلف أسباب ودوافع الإرهاب الإلكتروني عن أسباب ودوافع الإرهاب المادي وتختلف الأسباب والدوافع في مدى تأثيرها باختلاف المجتمع المعتدى عليه تبعاً لاختلاف الاتجاهات الاقتصادية والسياسية والاجتماعية.

### ٣ . ٤ . ١ أسباب الإرهاب الإلكتروني

لخص العجلان (١٠) أهم أسباب ظاهرة الإرهاب إلى دوافع شخصية ودوافع فكرية ودوافع سياسية ودوافع اقتصادية ودوافع اجتماعية:

**الدوافع الشخصية**

كالإحباط والفشل في تحقيق الأهداف، حب الشهرة والرغبة بالظهور ولفت الإنتباه، الشعور بالنقص، عدم الشعور بالإنتماء للوطن.

**الدوافع الاقتصادية:**

- تفاقم المشكلات والأزمات الاقتصادية الدولية والمحلية.
- فشل محاولات التعاون الدولي.
- انتشار البطالة والفقر والديون.
- التقدم العلمي والتقني للأنظمة المصرفية أدى إلى سهولة انتقال الأموال وتحويلها وتبادلها.

**الدوافع الفكرية:**

- الفهم الخاطئ للأديان.
- التشدد والقلق في نشر الأفكار والتعصب لدين معين والاعتقاد لصحته لوحده.

**الدوافع السياسية:**

- عدم المساواة والإستيلاء على الأموال العامة وغياب الحكم العادل.
- الظلم والاضطهاد والسياسات غير العادلة التي تنتهج من طرف بعض الدول ضد مواطنيها والكبت والتهميش وانتهاك الحقوق.
- غياب الحزم في إنزال العقوبات وردع محترفي الإجرام.(١٤)

**الدوافع الاجتماعية:**

- التفكك الأسري.
- ضعف التعليم والتربية.
- الفراغ والبطالة (٢٣).

وهناك أسباب اخرى تتعلق بالبنية التحتية لنظم المعلومات والشبكات، وضعف وسائل الحماية بها إضافة إلى ما تم ذكره من غياب الحدود الجغرافية وسهولة الاستخدام وقلة التكلفة وصعوبة اكشتاف هذه الجرائم والفراغ التنظيمي والقانوني وغياب جهات(٢٥).

**٣ . ٤ . ٢ أهداف الإرهاب الإلكتروني:**

ـ زعزعة الأمن ونشر الخوف والرعب واخلال بأنظمة الدول.

ـ الإخلال بالنظام العام والأمن المعلوماتي.

ـ إلحاق الضرر بالبنى التحتية للدول.

ـ التهديد والإعلان وجذب الانتباه وإثارة الرأي العام.

ـ تجنيد إرهابيين جدد(١٢).

ـ جمع الأموال والتبرعات.

## ٣ . ٥ مظاهر الإرهاب الإلكتروني

في أول استجواب لمدير إدارة الأمن الداخلي (Homeland Security) في الولايات المتحدة عند انشائها بعد الحادي عشر من سبتمبر ٢٠٠١ أمام الكونجرس اعترف صراحة بأن الثورة التقنيـة المعلوماتية جعلت من جريمـة الإرهاب الإلكتروني حقيقـة واقعة، وأضاف أنه لمواجهة هـذه الجريمة فإن إدارته تحتاج إلى دعم مالي لا يقل عن بليون دولار لإعادة البنية التحتية لأجهزة مواجهة هذه الجريمة لم يحصل عل هذا المبلغ فقط بل دعم بألف متخصص في علـم تقنية المعلومات والاتصالات للبدء الفوري في هذا المشروع (٢٢).

لقد نشـأ العديد من الحروب الجديدة تحمل مسـميات مختلفة ولكنها تشـترك في أن محصلـة إنتاجها جريمة إرهاب إلكتروني من هذه الحروب:

١ ـ حروب الشبكات (Network War).

٢ ـ الحروب السياسية (Political War).

٣ ـ الحروب الاقتصادية (Economic War).

٤ ـ حرب الفضاء (Cyber War).

كل هذه الحروب التي تشن بواسطة الإنترنت (Internet) تستمد قوتها من اسـتخدامها لتقنية المعلومات والاتصالات والتي تكون محصلتها النهائية الإضرار بالمجتمعات الإنسانية ولا ينحصر تأثيرها على مجتمع معين بذاته (٢٥).

من الصعب تحديد مظاهر الإرهاب الإلكتروني بجميع أنواعه ولهذا سنعرض هنا بعض أنواعه:

ـ إنتهاك خصوصيـة (Privacy Violation) الأفراد ومواطني الدولة، وكبار مسؤوليها والعبث بها وتغييرها أو تدميرها أو إبتزاز أصحابها.

ـ سرقة بيانـات ومعلومات سرية تتعلق بأمن الدولة (Secret Information Appropriation and Data Theft)، وكشف هذه الأسرار ونشرها وتوزيعها، بل يصار أحياناً إلى تحريفها وتزويرها بهدف هز الثقة في الدولة من قبل مواطنيها.

ـ هـدم قواعد الحكومة الإلكترونية للدولة : (Demolition of E-Government)، في سـبيل راحة المواطن والمقيم في الدولة، يسرت الدوله حكومة إلكترونية، يسـتطيع من خلالها إنجاز أعماله بيسر وسـهولة، وقلة تكاليف فيسـتطيع تسـديد فواتيره وتجديده للبطاقات الوطنية والبنكية ورخص القيادة وغيرها من الخدمات بواسطة هـذه الحكومة فعند ضرب هـذه الحكومة تفقد الدولة هيبتهـا في أعـين مواطنيها وهـذا ما تسـعى إليه هذه المنظمات الإرهابية.

ـ حرمان مواطني الدولة من الخدمات الضرورية: (Distributed denial of Services) الماء والكهرباء والمواصلات والتعليم والصحة وغيرها من الخدمات المكفولة للمواطن يستطيع المجرم الإلكتروني ضربها وحرمان المواطن منها، هدفه من ذلك إخضاع الدولة لأهدافه(٢٠).

ومن أشكال الإرهاب الإلكتروني أيضاً مايلي :

ـ التهديد الإلكتروني: كتهديد شـخصيات سياسية بالقتل أو التهديد بتفجيرات في أماكن عامة ومراكز سياسية ورياضية أو اتلاف أنظمة المعلومات.

ـ تعطيل شـبكة وانظمة المعلومات المرتبطة بالشبكة بواسطة توجيه الملايين من الرسائل مما يجعلها عرضة للتوقف.

ـ تدمـير أنظمة المعلومات: هو اختراق لشـبكة المعلومات الخاصة بالأفـراد أو الشركات العالميـة بهدف تخريب نقطة الاتصال، كما حصل في أسـتراليا في العام ٢٠٠٠ عندما تمكنت منظمة إرهابية من تدمير شـبكة الصرف الصحي في إحدى المدن الرئيسـة ممـا نتج عنها أضرار صحية واقتصادية (٢٠).

ـ التجسـس: هو التلصـص وسرقة المعلومـات من الأفراد والمؤسسـات أو الدول أو المنظمات لأهـداف اقتصادية وسياسية وعسكرية.

ومن أبرز مظاهر الإرهاب الإلكتروني التي استطاعت المنظمات الإرهابية من خلالها نشر أفكارها المتطرفة والدعوة إلى مبادئها والسيطرة على الدولة، وإخضاع قطاعات الخدمات العامة للخطر مايلي:

- إنشاء المواقع الإرهابية الإلكترونية: استطاع مجرموا الإرهاب الإلكتروني من إنشاء وتصميم مواقع لهم على الشبكة العالمية لإبراز قوتهم وللتعبئة الفكرية ولتجنيد إرهابيين جدد وجمع المال وتلقين أفراد المنظمة التدريب والتعليم والوسائل المتعددة لشتى الهجمات الإرهابية وتحديد المواقع المستهدفة.
- تدمير المواقع المهمة للقطاعين العام والخاص:
  - استهداف نظم البنى التحتية للاقتصاد.
  - استهداف البنى التحتية لنظم الاتصالات والمعلومات.
  - استهداف النظم العسكرية وهذه من أخطر البنى التحتية المستهدفة، حيث يمكن لهؤلاء الإرهابيين اختراق منظومات الأسلحة الإستراتيجية، ونظم الدفاع الجوي والصواريخ النووية.
  - استهداف محطات توليد الطاقة والماء.
- التهديد والترويع الإلكتروني: التهديد بالقتل للشخصيات السياسية والدينية والعامة أحد الاساليب المستخدمة في التهديد الذي تمارسه المنظمات الإرهابية، بل وصل التهديد إلى إبتزاز رجال المال والأعمال ومدراء الشركات لإخضاعهم لمطالب تلك المنظمات(٣١).

## ٣ . ٦ أبرز وأهم استخدامات الإرهابيون الإلكترونيين للشبكة العالمية

بين ويمان كيف يستخدم الإرهابيون شبكة الإنترنت في أغراضهم الإرهابية كما يلي:

- التنقيب عن المعلومات: إن شبكة الإنترنت في حد ذاتها تعتبر مكتبة إلكترونية هائلة الحجم وتكتظ بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها مثل أماكن المنشآت النووية، والمطارات الدولية والمعلومات الخاصة بسبل مكافحة الإرهاب وبذلك يكون ٨٠٪ من مخزونهم المعلوماتي معتمداً في الاساس على مواقع الكترونية متاحة للكل دون خرق لأي قوانين أو بروتوكولات للشبكة.
- الاتصالات: تساعد شبكة الإنترنت المنظمات الإرهابية المتفرقة في الاتصال ببعضها البعض والتنسيق فيما بيها، وذلك نظراً لقلة التكاليف للاتصال باستخدام الإنترنت مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها، وقد أصبح عدم وجود قائد ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية كل هذا بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية.
- التعبئة وتجنيد الإرهابيين: إن انخراط عناصر جديدة داخل المنظمات الإرهابية يحافظ على بقائها واستمرارها وهم يستغلون تعاطف الأخرين من مسخدمي الإنترنت مع قضاياهم، ويجذبون السذج من الشباب بعبارات براقة حماسية من خلال غرف الدردشة الإلكترونية.
- إعطاء التعليمات والتلقين الإلكتروني يمتلئ الإنترنت بكم هائل من المواقع التي تحتوي على كتيبات وإرشادات تشرح طرق صنع القنابل والأسلحة الكيميأية الفتاكة ويوجد على الشبكة ما يقارب ثمانية آلاف موقع لهذه الخدمات.
- التخطيط والتنسيق: تعتبر شبكة الإنترنت وسيلة للاتصال بالغة الأهمية بالنسبة للمنظمات الإرهابية حيث تتيح لهم حرية التنسيق الدقيق لشن هجمات إرهابية محددة، ومثال هذا التخطيط ما حدث في هجمات الحادي عشر من سبتمبر (٢٠٠١).
- الحصول على التمويل: يستعين الإرهابيون ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية في التعرف على الأشخاص ذوي القلوب الرحيمة ومن ثم استجداؤهم لدفع تبرعات مالية لأشخاص يعتبرون واجهة لهؤلاء الإرهابيين، يتم كل هذا بواسطة البريد الإلكتروني بطريقة لا يشك فيها المتبرع بأنه يساعد منظمة إرهابية.
- مهاجمة المنظمات الإرهابية الأخرى: تستخدم الإنترنت كحلبة مصارعة بين المنظمات الإرهابية وبعضها وبين أعضاء المنظمة الواحدة، وتكثر المناظرات والخلافات بين هذه المنظمات(٢١).

## المبحث الرابع: طرق مواجهة الإرهاب الإلكتروني

لمواجهة الإرهاب الإلكتروني طرقاً متعددة نعرض فيمايلي الأهم منها:

### ٤ . ١ المواجهة الفنية

لا يمكن تقديم حماية مطلقة وتامة لنظم المعلومات المرتبطة بشبكة الإنترنت هناك سبيل واحد حاسم وهو عزل الأجهزة التي تحتوي هذه المعلومات عن العالم، ولكن مثل هذه الطريقة يمكن لها أن تؤدي إلى نتائج أكثر ايذاء على المدى الطويل تتمثل في حرمان المجتمع من وسائل زيادة الإنتاجية والفعالية، ومع ذلك فإن استخدام مجموعة من الإجراءات الأمنية الأساسية يمكن لها أن تقلل بشكل كبير من مخاطر الاختراقات والإرهاب الإلكتروني، وتشمل إجراءات الحماية التي يجب مراعاتها مايلي (٢٩):

**١ ـ تامين خطوط الدفاع الأمامية باستخدام تطبيقات الجدران النارية**

وتقوم هذه الفئة من التطبيقات بتأمين المنافذ (Ports) التي تحصل من خلالها على خدمات إنترنت. وهذه المنافذ تحدد برمجياً ضمن نظم التشغيل أو التطبيقات المستخدمة، وفي كثير من الأحيان لا يستعمل المستخدم كافة هذه المنافذ مما يجعله يسهو عن تأمينها وحمايتها، مما يشكل فرصة مثالية للهكرة للنفاذ إلى النظام. وتعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة وذلك بالاعتماد على مجموعة من السياسات Policies التي يحدد بموجبها مدراء الشبكة طبيعة المؤسسات على مستوى الاجهزة المزودة وبالتالي الأجهزة المرتبطة بهذه النظم المزودة طالما بقيت مرتبطة بالشبكة ولكن في عصر المستخدم النقال، والعمل من المنزل حيث لا يوجد جدران نارية وأجهزة مزودة تكتسب الجدران النارية الشخصية، أهمية خاصة وقد بدأ مدراء المعلوماتية في الغرب مؤخراً بتثبيت الجدران النارية الشخصية على الأجهزة المحمولة التي يستخدمها العاملون في المؤسسات، ويجب أن نذكر هنا أن الجدران النارية ليست الحل السحري الذي يوفر الأمن الشامل، وأنه يجب استخدام طبقات أخرى من الأمن تتجاوز الخطوط الأمامية.

**٢ ـ تأمين حسابات المستخدمين ونظم التحقق من الهوية**

رغم وجود العديد من تقنيات التحقق من الهوية وخصوصاً أساليب التحقق البيولوجي من الهوية (بالاعتماد على الصفات الشخصية والسمات الجسدية للأشخاص) تبقى كلمات السر وأسماء المستخدمين هي الوسيلة الأكثر شيوعاً للتحقق من الهوية، رغم أن هذه الأساليب بدأت تصبح أضعف وأضعف بتطور التقنيات التي يستخدمها الهكرة لكشفها وخرقها، ومع ذلك فهناك الكثير من الوسائل التي يمكن من استخدامها للحد من قدرة الهكرة على اختراق واكتشاف هذه الرموز. وتعتمد هذه الوسائل أساساً على تحديد دخول المستخدمين إلى الشبكات وحصرها بما يحتاجه كل مستخدم، ولكن هذه التقنيات ورغم قوتها ليست حلولاً سحرية، إذ أنها تتطلب الكثير من المهارة والتخطيط الواعي قبل تطبيقها كي تحقق النجاح، وتتكون نظم التحقق من الهوية ضمن ثلاث تقنيات مهمة هي خدمات الأدلة Directory Services وهيكلية المفاتيح العامة Public Key Infrastructure والشبكات الافتراضية الخاصة Virtual Private Networks. وتشكل هذه التقنيات الثلاث هيكلية شاملة للتحقق من هوية المستخدمين وضمان تحديد حقوق النفاذ.

**٣ ـ خدمات الأدلة**

برمجيات خدمات الأدلة هي عبارة عن قواعد بيانات خاصة ذات مستو عال من الأمان تضم عادة لجمع وإدارة المعلومات المتعلقة بمستخدمي الشبكات، ولا يقتصر دور هذه البرمجيات على جمع كلمات السر وأسماء المستخدمين بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين، ويتم استخدام هذه المعلومات لتحديد حقوق المستخدمين على الشبكة بجميع مكوناتها كالتطبيقات والأجهزة الخادمة والمجلدات وحتى شكل الشاشة التي يستعملها المستخدم، وتدار هذه كلها بشكل مركزي من مكتب مدير الشبكة دون الحاجة للقيام بأية زيارات إلى الأجهزة أو المسخدمين.

**٤ ـ تقنية التشفير بالمتفاح العام**

تعتمد هذه التقنية على تشفير البيانات آو بعثرتها scrambling اعتماداً على علاقات رياضية خاصة تجمع ما بين مفتاحين (أو بالأحرى كلمتين سريتين) أحدهما عام والآخر خاص. فعند إرسال رسالة message (*) يقوم التطبيق الموجود على الجهاز بتشفيرها أو بعثرة بياناتها باسخدام كلمة سر غير معروفة لأي شخص آخر، ثم تشفيرها ثانية بالمفتاح العام للمستقبل، والسبيل الوحيد الذي يمكن به للمستقبل أن يتعامل مع هذه الرسالة يتمثل في فك تشفيرها أو إعادة ترتيب بياناتها باستخدام مفتاحه الخاص (أو كلمته السرية) أولاً ومن ثم استخدام المفتاحي العام لفك الشفرة الخاصة. وتقوم هيئات عالمية وشركات خاصة بإصدار شهادات رقمية للمصادقة على صحة هذه المفاتيح.

**٥ ـ الشبكات الافتراضية الخاصة**

لا توجد طريقة أكثر أمناً من الشبكات الافتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى شبكتك وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة لا ينفذ من خلالها إلا من يقوم بتحديده مدير الشبكة، وفي هذه الحالة يمكن للمستخدمين المعنيين النفاذ إلى الشبكة عبر الإنترنت وإسقاط الحزم الواردة من أية جهات أخرى غير هؤلاء المستخدمين.

**٦ ـ أمن البرمجيات**

بالطبع لا يمكن اعتبار أية سياسة أمنية شاملة ما لم يتم الاعتناء بأمن البرمجيات المستخدمة على الشبكة، وللأسف فإن هذه هي النقطة الأصعب حيث يجب اعتبار أو تثقيف المستخدمين ليقوموا بتحديث برمجياتهم واعتماد كافة التصحيحات التي تعتمدها الشركات المنتجة، وضمن المؤسسات يجب أن يعي مدراء الشبكة أهمية تحديث البرمجيات وتطبيق التصحيحات بشكل مستمر كي يضمنوا شمولية السياسات الأمنية المعتمدة لديهم(٢٩).

**٧ ـ نشرت كلية دارت ماوث (Dart Mouth) دراسة بعنوان «الهجمات الإرهابية أثناء ممارسة الحرب على الإرهاب: من بين توصياتها:**

١ ـ تحديث أنظمة التشغيل.

٢ ـ وضع سياسة لعمل المفاتيح السرية القوية ومتابعة الالتزام بها.

٣ ـ إقفال الأنظمة بشكل مستمر.

٤ ـ تحديث أنظمة الحماية.

٥ ـ تحميل وتركيب الجدران النارية وأجهزة كشف الدخلاء على النظم الحاسوبية.

٦ ـ الاحتفاظ دائماً بنسخ احتياطية لجميع المعلومات المهمة خارج المنظمة.

٧ ـ إنشاء نظام آلي صارم لمتابعة تنفيذ والالتزام بالتوصيات الأمنية(٢١).

ونشرت دائرة المتابعة الفدرالية في الولايات المتحدة توصيات منها (١٨):

١ ـ إنشاء وتطوير بنية وطنية تحتية شاملة لأنظمة المعلومات.

٢ ـ تمكين تبادل المعلومات فيما يخص التهديدات ونقاط الضعف بين الأجهزة الحكومية أو القطاع الخاص والحكومة الفدرالية.

٣ ـ تطوير القدرات التحذيرية لكل من الهجمات الإلكترونية والتقليدية.

٤ ـ تشجيع جميع الوحدات خارج الحكومة الفدرالية للحذو حذو الحكومة في اتباع وسائل التقليل قدر الإمكان من الهجمات الإرهابية الإلكترونية.

٥ ـ إنشاء إدارات متابعة بين أجهزة الحكومة والقطاع الخاص.

٦ ـ إشراك القطاع الخاص في وضع الإستراتيجيات طويلة الأمد والقصيرة والمتوسطة للحماية من هجمات الإرهاب الإلكتروني.

٧ ـ توحيد أنظمة الإنذار المبكر.

٨ ـ وضع آلية تبادل المعلومات بصورة ملزمة.

١٠ ـ مشاركة القطاع الخاص في جميع هذه الأنشطة(١٨).

---

(*) تعني كلمة رسالة هنا تشمل أي نوع من المعلومات المتناقلة بيم النظم الإلكترونية بما في ذلك الأوامر التي تتناقلها التطبيقات بين بعضها البعض.

### ٤ . ٢ المواجهة الفكرية

إذا كانت مشكلات التنظيمات الإرهابية والجرائم الإلكترونية مشكلات فكرية فيجب أن تعتمد الإجراءات المحلية والإقليمية والدولية على الوسائل الفكرية الفنية والقانونية في مواجهة هذه المشكلات وأن تقتصر الإجراءات الأمنية على الخارجين على القانون فقط لأن الاعتماد على الإجراءات الأمنية وحدها قد يؤدي إلى نتائج عكسية. فعندما انطلقت الطائرات الأمريكية لضرب أفغانستان انطلقت معها حركة تنظيم القاعدة على الإنترنت والمنظمات الأخرى الحليفة لها. واكتملت تلك الحلقة باحتلال العراق، وليكتسب تنظيم القاعدة أرضاً جديدة لبث أفكاره التنظيمية المعادية للولايات المتحدة وللغرب بوجه عام. من هنا فقد زادت المواقع الإرهابية لتنظيم القاعدة على الإنترنت من ١٣ موقعاً عام ٢٠٠١ لتصل إلى ما يقارب ٢٠٠٠ موقع في العام ٢٠٠٦ وفق بعض التقديرات. السبيل الأمثل لمواجهة مثل هذه الظاهرة يكمن في:

١ـ الاستخدام الأمثل لوسائل الإعلام من خلال:

أ ـ نشر الأفكار المعتدلة.

ب ـ تجنب نشر أعمال العنف أو الأفكار المتطرفة.

٢ـ كشف مواقع المتطرفين ومناقشة أفكارهم وبيان ما تشتمل عليه من مخالفات.

٣ـ التوسع في إنشاء المواقع البديلة لنشر الوسطية والاعتدال ومحاربة الأفكار المتطرفة.

٤ـ تشكيل لجان وطنية لحماية الشباب وتحصينهم من الأفكار المتطرفة.

٥ـ إعداد وتنفيذ برامج إعادة تأهيل المتطرفين فكرياً وعملياً.

٦ـ اتخاذ الإجراءات الفنية المناسبة لحماية المواقع المعتدلة واختراق المواقع المتطرفة وتغذيتها بالأفكار المعتدلة.

٧ـ وضع معايير دولية لأمن المعالجة الآلية للبيانات.

٨ـ تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية.

٩ـ اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول(١٤).

يدعو ويمان (weiman) لأهمية عدم مقايضة الحريات المدنية للأفراد بالقضاء على ما يسمى بالإرهاب الإلكتروني، فهو يقترح أن تسلك الولايات المتحدة سبيلاً آخر يسميه ويمان (الطريق الذهبي) أو الطريق الوسط مع الأخذ في الاعتبار أن الإرهابيين سوف يكونون أكثر اعتماداً على تكنولوجيا الاتصالات الإلكترونية في المستقبل نظراً للتطور الهائل في هذا المجال وسوف يصبح الإرهاب أكثر تأثيرًا وخطورة فلا يجب البتة المبالغة في حجم الأخطار الحالية حتى يتسنى مواجهة تلك التحديات بشئ من حسن التصرف.

ويضيف ويمان أنه كما يستطيع الإرهابيون استخدام تلك الشبكة بكفاءة كذلك يستطيع صانعوا السلام استخدام الإنترنت لمجابهتهم بنشر الأفكار السامية والمتحضرة التي تدعو للسلام والمحبة والتعايش السلمي بين الحضارات المختلفة(٢١).

### ٤ . ٣ المواجهة القانونية

سن العديد من دول العالم قوانين لمكافحة الجرائم الإلكترونية بعد أن ظهر جلياً مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها وأجمع أغلب هذه القوانين أن هذه الجرائم ما هي إلا تعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام الوسائل التقنية وخصص جزء كبير من هذه القوانين عقوبات رادعة لجرائم الإرهاب الإلكتروني الذي يمتد أثره ليس على دولة معينة بحد ذاتها بل ضرر هذه الجرائم يمتد ليشمل المجتمع الدولي بأسره(٢٧) وفيما يلي بيان أسماء بعض دول العالم التي سنت قوانين لمكافحة هذه الجريمة.

السويد، الولايات المتحدة الأمريكية، أستراليا، كندا، الصين، مقاطعة هونج كونج التابعة للصين، مملكة الدنمارك، فرنسا، ألمانيا، جمهورية إيرلندا، الهند، اليابان وغيرها العديد من دول العالم التي أضافت إلى قانونها الجزائي ملحقاً خاصاً لمكافحة الجرائم الإلكترونية ومنها (لبنان، البحرين، الجزائر، المغرب، تونس، الأردن، مصر، المغرب السودان وهناك ثلاث دول عربية فقط هي السعودية والإمارات وعُمان التي سنت قوانين مستقلة لمكافحة الجرائم المعلوماتية (٧).

**٤ . ٣ . ١ الجهود الدولية:**

- يقوم الإنتربول بأعضائه المائة وثمان وسبعين دولة بعمل جبار لمحاربة جرائم الإرهاب الإلكتروني خاصة والجرائم الإلكترونية عامة، وتقييم العديد من الدورات لأعضائه وكذلك العديد من مجالات التدريب.
- مجلس أوروبا في إطار سعيه لمواجهة الجرائم الإلكترونية سن القانون الاسترشادي لمكافحة جرائم الحاسب الآلي وهو إطار يجمع الخمس وأربعين دولة ولم يقتصر على الدول الأوروبية بل شمل أمريكا وكندا واليابان وعدد من الدول الإفريقية وأمريكا الجنوبية (٢٦).
- منظمة جنوب شرق آسيا وضعت الخطوط العريضة لتبادل المعلومات والخبرات بخصوص مواجهة الجرائم الإلكترونية عامة وجرائم الإرهاب الإلكتروني خاصة بل وقعت على إنشاء وحدة إقليمية لهذه الدول لمكافحة الجرائم الإلكترونية(٢٨).
- وافقت الجامعة العربية على اعتماد قانون دولة الإمارات العربية المتحدة كقانون استرشادي لقانون مشابه للقانون الاسترشادي لدول أوروبا لمكافحة جرائم الإرهاب الإلكتروني (٦).

**٤ . ٣ . ٢ جامعة نايف العربية للعلوم الأمنية**

انطلاقاً من تخصص الجامعة كجامعة تهتم بالأمن الشامل وتختص كذلك بتنفيذ الجانب العلمي من الخطط والإستراتيجيات الأمنية العربية لمكافحة الإرهاب التي أقرت من وزراء الداخلية في الدول العربية وتم الانتهاء من تنفيذ الخطة المرحلية الرابعة لهذه الإستراتيجية في العام ٢٠٠٩م وتنفذ الجامعة العديد من المناشط العلمية المعتمدة ضمن الخطط كما نفذت عدداً من الدورات التدريبية والندوات العلمية والمحاضرات العلمية والدراسات والأبحاث الميدانية وتمكنت من الاستفادة من الخبرات الدولية حيث نظمت عدداً من الأنشطة العلمية في مجال مكافحة الإرهاب في كل من فرنسا وألمانيا وإسبانيا والنمسا وإيطاليا وهولندا والتشيك والصين، كما ضمت مناهجها العلمية العديد من المقررات الدراسية التي تناولت مشاكل وأنواع الإرهاب وطرق مواجهته.

**٤ . ٤ مواجهة استخباراتية وعسكرية:**

- تقوية ودعم أجهزة جمع المعلومات والاستخبارات: تستطيع الدولة للمحافظة على أمن مواطنيها تسخير الأموال لتقوية أجهزة جمع المعلومات عن الإرهابيين والجماعات الإرهابية ليس ها فحسب بل لابد من تجنيد عناصر ذوو خبرة في مجال أنظمة المعلومات وإنشاء المواقع الإلكترونية وبرمجة الحاسب الألي وغيرها من تقنياته المختلفة(٣٢).
- الردع واستخدام القوة: خيار صعب تقوم به الدول ضد القواعد الإرهابية والقيام باغتيالات قياداتهم وتصفيتهم والتضييق عليهم، وتجفيف منابع مصادرهم البشرية والمالية. إن اللجوء لهذا الخيار له بعض المساوئ، إن إرهابيو الإنترنت يتخفون وراء أسماء مستعارة وملاحقتهم سريعة التبديل وتغيير العناوين، وكذلك صعوبة تحديد أماكنهم إضافة إلى احتمال انتهاك حقوق الإنسان إضافة إلى أن استخدام الخيار العسكري عادة يأتي في وقت متأخر يكون عندها الإرهاب الإلكتروني توسع بشكل كبير.

## المبحث الخامس: الخلاصة والنتائج والتوصيات

### ٥ . ١ الخلاصة

لقد استهدفت الدراسة إلقاء الضوء على جريمة العصر ـ الإرهاب الإلكتروني ـ باعتباره من أهم مهددات الأمن والاستقرار في معظم دول العالم، ومن هنا تم التركيز على التعرف على هذه الظاهرة والعلاقة بينها وبين الجريمة الإلكترونية، وسيناريوهات التهديد الإلكتروني، والعلاقة بين الإرهاب التقليدي والإرهاب الإلكتروني، وآليات المواجهة للتقليل من أخطارها، وتم تغطية هذه الموضوعات في خمسة مباحث بالإضافة إلى المراجع، غطى المبحث الأول مدخل الدراسة وأسباب اختيار موضوع الدراسة ومشكلتها وأهميتها وأهدافها والتساؤلات التي تجيب عنها وأهم المصطلحات التي استخدمها الباحث في دراسته بالإضافه إلى الدراسات السابقة وجاء المبحث الثاني بعنوان الجريمة الإلكترونية: نشأتها، تصنيفاتها، وخصائص وأهداف الجريمة بالإضافة الى أسباب ودوافع إرتكابها وبيان الخسائر الناتجة عن هذه الجريمة ، أما المبحث الثالث فقد تناول الباحث جريمة الإرهاب الإلكتروني:

نشأتها وتطور الإرهاب التقليدي إلى إرهاب إلكتروني بالإضافة إلى خصائص الإرهاب الإلكتروني وأسباب ودوافع ارتكاب هذه الجريمة هـذا بالإضافة إلى مظاهر الإرهاب الإلكتروني، أما المبحث الرابع فقد تناول الباحث طرق ووسـائل مواجهة الإرهاب الإلكـتروني الفنية والفكريـة والقانونية والدولية والاسـتخباراتية والعسـكرية واختتم الباحث هذه الدراسة بالمبحث الخامس الـذي تناول فيه خلاصة الدراسـة وأهم نتائجها وتوصياتها.

## ٥ . ٢ النتائج

أبرز ما توصلت إليه في هذا البحث مايلي:

أولاً: إن جرائم الإرهاب الإلكتروني ما هي إلا امتداد للجرائم الإرهابية المادية التقليدية، بل هي النسخة الإلكترونية لها.

ثانياً: إن العلاقة المشـتركة بين جرائم الكمبيوتر والمعلومات وجرائم الإرهاب الإلكتروني أن كل منهما جرائم وأن محل ارتكاب الجريمة في كليهما واحدوهو البيئة الإلكترونية.

ثالثاً: تسـتهدف الجرائم الإلكترونية في الغالب الأعم الأفراد والمنظـمات أو حتى دولـة بعينها أما جرائـم الإرهاب الإلكتروني، فهي تستهدف المجتمع الدولي بأكمله، فعندما يقع الهجوم على دولة معينة فكأنه وقع على المجتمع كله.

رابعـاً: ترتكب الجرائم الإلكترونية لأسـباب متعددة أغلبها كسـب المال، أما جرائم الإرهـاب الإلكتروني فترتكب بدوافـع سياسـية واقتصادية واجتماعيـة بهدف زعزعة واستقرار وتدمير البنى التحتية المستهدفة.

خامساً: إن من أعظم مظاهر الإرهاب الإلكتروني إنشاء المواقع الإرهابية وتدمير مواقـع مهمة للقطاعين العام والخاص للدول، واسـتهداف البنـى التحتيـة الاقتصادية ونظم الاتصالات والمعلومات واسـتهداف المواقع العسكرية ومحطات توليد الطاقة ومحطـات المياه، كما أن من مظاهر الإرهاب الإلكـتروني التهديد والترويع للشـخصيات السياسية والدينية للدول بهدف زعزعة أمنها واستقرارها.

سادساً: هناك العديد من الطرق والأساليب لمواجهة الإرهاب الإلكـتروني منها المواجهة الفنية بتأمـين خطوط الدفاع الأمامية باسـتخدام تطبيقات الجـدران النارية، وتأمين حسابات المستخدمين ونظم التحقق من الهوية، وخدمات الأدلة، وتقنية المفتاح العام، وإنشاء الشبكات الافتراضية التركيز على أمن البرمجيـات. وإلى جانب المواجهة الفنية هناك المواجهة الفكريـة والمواجهة القانونية والمواجهات الاستخباراتية والعسكرية التي يجب أن لا تغفل في مواجهة جرائـم الإرهاب الإلكـتروني ، إلا أنه يجب اسـتخدام المواجهة العسـكرية كحل أخير بعد استنفاذ كافة الطرق والوسائل لمواجهة هذه الجرائم.

سابعاً: هناك خطوة مهمة لمكافحة جرائم الإرهاب الإلكتروني وهو التركيز على البحـث العلمي للبحث في جذور هذه الظاهرة والمكان الطبيعي لهذه الإجراءات هو المؤسسات الأكاديمية والحكومية ومؤسسات الدفاع والأمن في ظل وجـود تقنيات حديثة لديها القـدرة على جمع المعلومات وتحليلها وتقديم دراسات أكاديمية مبنية على الإحصاءات الدقيقة.

## ٥ . ٣ التوصيات

في ضوء الدراسة فقد رأى الباحث تبني التوصيات التالية ووضعها موضع التنفيذ:

أولاً: اتخاذ الإجراءات الفنية المناسبة لحماية أنظمة المعلومات ومواقع الإنترنت المهمة من الاختراق واستحداث الأجهزة الأمنية القادرة على التحقيق في الجرائم الإلكترونية.

ثانياً: تجنيد الشـباب الوطني المتخصـص في تقنية المعلومات وتدريبـه على اسـتخدام الإنترنت والوصـول للمواقع المتطرفة والتعامل معها بطرق علمية مدروسة.

ثالثاً: التوسع في إنشاء المواقع البديلة لنشر الوسطية والاعتدال ومحاربـة الأفكار المتطرفـة ونشر الوعي العـام بجرائم الكمبيوتر والعقوبات المترتبة عليها.

رابعاً: دعم المواقع التي تدعو إلى التعايش السلبي بين الحضارات المختلفة ونشر المحبة والتسامح والسلام للجميع.

خامساً: تطوير القدرات الأمنية للتعامل مع جرائم الكمبيوتر والوقاية منها وتطوير إجراءات الكشف عن هذه الجرائم، وجمـع الأدلة الرقمية من مسرح الحـوادث بطرق علمية وتقديمها للجهات القضائية لتطبيق العقوبات المحددة.

سادساً:تعزيز التعاون والتنسيق بين الدول والمؤسسات الدولية المعنيـة وتوحيد الجهود لغرض الرقابة الكامنة على ما يتم

نشره على الشبكة العالمية وتقوية حماية المواقع المهمة، وتوفير التقنيات اللازمة لمواجهة هذه الجرائم، ولفت نظر المجتمع الدولي لإبرام اتفاقيات تكافح هذه الجرائم والوصول إلي سن قانون دولي لمحاربة الجرائم الإلكترونية تحت مظلة الأمم المتحدة تلتزم به كافة دول العالم.

# المراجع

## المراجع العربية


١ ـ المومني، نهلا (٢٠٠٨م)، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان:الأردن.

٢ ـ عبدالمنعم، محمد (١٩٧٥م). ٦ أكتوبر الحرب الإلكترونية الأولى المصرية العامة للكتاب.

٣ ـ سعيد، محمد قدري (٢٠٠٦م). الحرب وتكنولوجيا المعلومات، نهضة مصر للطباعة والنشر.

٤ ـ عبابنة، محمود أحمد (٢٠٠٩م). جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع، عمان: الاردن.

٥ ـ الحسيناوي، علي (٢٠٠٨م). جرائم الحاسوب والإنترنت، اليازوري العلميد للنشر والتوزيع، عمان: الأردن.

٦ ـ سلامة، محمد (٢٠٠٧م). جرائم الكمبيوتر والإنترنت، المكتب العربي الحديث، الاسكندرية: مصر.

٧ ـ الشهري، حسن أحمد (٢٠١١م). قانون دولي موحد لمكافحة الجرائم المعلوماتية تصور مقترح، الرياض.

٨ ـ جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث التقرير السنوي ٢٠١٠م.

٩ ـ محمد أحمد عبرالغني، دور المملكة العربية السعودية في مكافحة الإرهاب.

١٠ ـ عبدالله عبدالعزيز العجلان، الإرهاب الإلكتروني، مؤتمر حماية أمن المعلومات والخصوصية في قانون الإنترنت.

١١ ـ عبدالرحمن عبدالله السند، وسائل الإرهاب الإلكتروني، ندوة الأمن والمجتمع، كلية الملك فهد الوطنية، الرياض، ٢٠٠٦م.

١٢ ـ محمد سيد سلطان، الحماية الدولية والقانونية للبنية الإلكترونية من الجريمة والإرهاب، المؤتمر السادس لجمعية المكتبات والمعلومات، الرياض، ٢٠١٠م.

١٣ ـ إيمان بنت عبدالكريم الناصر، الإرهاب الإلكتروني، مركز التميز لأمن المعلومات، المقالات العلمية، الرياض، ٢٠١٠م.

١٤ ـ تقارير كونجرس الولايات المتحدة الأمريكية عن الإرهاب الإلكتروني للعام ٢٠٠٨م.

١٥ ـ جمال محمد غيطاس، أمن المعلومات والأمن القومي، دار نهضة مصر،القاهرة، ٢٠٠٧م.

١٦ ـ محمد عبدالله القاسم، أساسيات أمن المعلومات، دار أمن المعلومات، الرياضن ٢٠٠٨م.

١٧ ـ عبدالله عبدالكريم عبدالله، وعبدالعزيز الحمدان، جرائم المعلومات والإنترنت، منشورات الحلبي، بيروت ـ لبنان ٢٠٠٧م.


## المراجع الأجنبية


18.Cyber threats, information warfare, and critical in fasturcture protection: defending the US homeland, CSIS (Washington, DC.) Justin G. co desman, Anthony H. Co desman, 2007.

19. Cyber warfare and Cyber terrorism. Lech Jaycee Wish, Idea Group Inc. 2008.

20. Cyber terrorism: Political and economic implication, Andrew M. cleric, Idea Group Inc. 2006.

21. Black Ice: the invisible threat of Cyber-terrorism Dan Vernon Mc Crow-Hill Professional, 2003.

22. Terror on the internet: the N\new arena, the New Challenges, Gabriel Weimar , Us Institute of Peace Press, 2006.

23. Fighting terror in Cyber space, Abraham, Kendal, Mark Last World Scientific, 2005.

24. The Changing Face of terrorism Rohan Ganaratna, Michionm Eastern University Press, 2004.

25. Cyber Terrorism before the special oversioght Panel on Terrorism Committee on Armed services, U.S. House of represontatives, Dorothy E. Denning, Gearosetown University May 23,2000.

26. Assessing the risks of Cyber Terrorism, Cyber war and other Cyber Threats, James, A. Lewis, Center for Strategic and International studies, Washington, Dc. 2002.

27. Armistead E. Information Warfare, Washington, Dc. Potomac books Inc, 2007.

28. Terrorism Question and answers': Cyber Terrorism Europe conical on foreign relation
http:// www.terrorismwors.com/coalitioneurope.html
29. National cyber security alliance
http:// www.staysafeonline.infohtml
30. cyber Terrorism resource, center
http://www.globaldisaster/ cyberterrorism.html
31. The Myth of cyber terrorism: there are many ways Terrorists, can kill you-computers are not one of them
http:// www.washingtonmonthly.com/features/2011/2001green.html
32. Center for Strategic and international studies Washington, D.c.
http:// www.csis.org
33. http:// www.anderw.cmu.edu/user/dangor
34. Cyber Terrorism: A study of the Extert of Coverage in Computer Security text book, Janet J and other, Journal of information technology education volume 2004.
35. cyber warfare and cyber terrorism: Thinned for a New U.S. Strategic Approach eugere E. The cyber scene institute provoking cyber Security chanal Feb, 1,2010.
36. http://www.crime-research.org/articaes/cyber/2011/20/1.
37. Canadian Center for Intelligence and security studies, Volume 2-2006.
38. A shish piney, cyber Crime-Detection and prevention, Connell, 2000.
39. First Annual Cost of Cyber Crime Study, Peneman Institute, Research Report MI.2010.

عميد كلية أمن الحاسب والمعلومات بجامعة نايف العربية للعلوم الأمنية، حاصل على درجة الدكتوراه عام (١٩٩٧م) والماجستير عام (١٩٨٦م) في علوم الحاسب من الولايات المتحدة الأمريكية، عمل أستاذًا جامعيًّا في العديد من الجامعات العربية والعالمية كجامعة وين الحكومية في الولايات المتحدة الأمريكية، وكلية الحاسب وتقنية المعلومات بالجامعة العربية المفتوحة بالرياض، نشر العديد من الأبحاث المحكمة في مجال أمن الحاسب وأشرف على العديد من الرسائل العلمية، عمل مديرًا عامًا لتقنية المعلومات في حرس الحدود التابع لوزارة الداخلية بالمملكة العربية السعوديةفي الفترة من ١٩٨٦م وحتى ٢٠٠٤م.

# Electronic Terrorism - Network Wars

**Hassa A. Al-Shehri**

The revolution of Information and Communication Technology is a great benefit of the mankind , but at the same time paved the way to the emergence of new types of very serious crimes, such crimes have emerged after been linking computer networks and information systems to the global network “the Internet”, these crimes is characterized by the speed of implementation and novelty of the method and the ability to erase its effects, and the multiplicity of its forms. . This study derives its importance through shedding the light on concrete evidence and indicators, which predicts that cyber terrorism will be the main component of World War in the present time and the future. The researcher of this study is trying to answer a question about the cyber terrorism Means, concept, motives, forms, and means of committing it and stages as well as what mechanisms and strategies to be taken in countering such crimes. Accordingly, this study is discussing several issues, including identification of the phenomenon and environment of cyber terrorism, shedding the light on the relationship between cyber crime and cyber terrorism offense in addition to the e-threat , defense mechanisms , reduce the risk of crime and cyber terrorism scenarios. The study then drawn its recommendations and suggestions to address this type of crime.

**Key words:** Cyber Terrorism, Information and Communication Technology, Cyber crimes

Sent from my iPhone.