أساليب الجريمة الإلكترونية: مسار الانتقال من الإرهاب التقليدي إلى الإرهاب الالكتروني في ظل المجتمع المعلوماتي

Methods of online crime: the path going from terrorism to cyber terrorism under information society

وهيبة بشريف

جامعة باتنة 1 (الحاج لخضر)

ملخص:

تسعى هذه الدراسة إلى تقديم توصيف للعمليات التي يلعبها الإرهاب الالكتروني في مختلف الميادين، خاصة في ظل المتغيرات الراهنة التي نشهدها، وتنامي ظاهرة الثورة المعلوماتية، التي ساهمت في ظهور المواقع الالكترونية المختلفة، و التي أصبحت تلعب دوراً رئيسياً في التأثير على الأفراد ككل، ومنه خلق ضرورة لتفعيل لدور الأمن المعلوماتي، وذلك للمشاركة في عمليات التوعية المعلوماتية أو الرقمية، وهذا من خلال خلق الوعي تجاه أساليب جرائم الفضاء الافتراضي، خاصة في ظل الأوضاع الراهنة، و هو ما جعل ضرورة لخوض غمار التوعية الرقمية، بعدما كان مقتصرا على استخدام الوسائل الرقمية، و مما سبق، نطرح الإشكالية المحورية: كيف ساهمت أساليب الجريمة الالكترونية في انتقال الإرهاب التقليدي إلى الإرهاب الالكتروني؟

وللإجابة على إشكالية هذه الورقة البحثية سنركز على البناء المفاهيمي لأهم المتغيرات، والتعريج على مراحل تطور الإرهاب الالكتروني، وهذا بغية الاطلاع على أبرز أساليب الجرائم الالكترونية في الإرهاب الالكتروني، وكذا دورها في انتقال الإرهاب العادي إلى الإرهاب الرقمي، وأهم السبل لمكافحة الإرهاب الالكتروني، ومنه نتوقع مساهمة وعي الأمن المعلوماتي أو الوعي السيبيراني في مكافحة الإرهاب الالكتروني، ومنه حماية المعلومات في المجتمع المعلوماتي.

الكلمات المفتاحية: الإرهاب الالكتروني، الإرهاب، المجتمع المعلوماتي.

Summary:

This study seeks to provide a profile of operations to play electronic terrorism in various fields, especially in light of the current variables that we are witnessing, and the growing phenomenon of the information revolution, which contributed to the emergence of various websites, which has played a major role in influencing the individuals as a whole, including the creation of the necessity to activate the role of information security, to participate in the operations of the informatics awareness or digital divide, this through creating awareness toward the methods of crimes default space, especially in light of the current situation, and is what made the need to contest the awareness of the digital divide, after it was limited to the use of digital means, and the foregoing, ask the pivotal forms: How have contributed to the working methods of electronic crime in the transfer of conventional terrorism to electronic terrorism?

Keywords: electronic terrorism, terrorism, the information society.

مقدمة:

احتلت الثورة التكنولوجية بوسائلها المختلفة مكانة اجتماعية واقتصادية وسياسية متميزة، حيث لعبت أدورا فاعلة في تسريع وتيرة العمل في مختلف المؤسسات، وزادت فعاليتها من خلال استخدامها في مختلف المؤسسات المجتمع، وذلك نتيجة التسهيل في القيام بالعمليات المتعددة، مما جعل تلك المؤسسات تطور من عمليات التعامل مع الزبائن في مختلف المراحل، وهذا ما جعلها تعتمد على ما أصبح يعرف بالرقمنة المعلوماتية، التي مكنت المواطنين من الحصول على التسهيلات، في مختلف الإجراءات المنتهجة، في حين، ظهر مع هذه الثورة المعلوماتية هاجس الجرائم الالكترونية، التي يعتبر الإرهاب الالكتروني من أخطر جرائمها تنظيما وتخطيطا، و الذي لا يكتفي بسرقة المعلومات بل بتدميرها وتخريبها، وبذلك تتنوع أساليب تجسيد الإرهاب الالكتروني، و مما سبق، نطرح الإشكال التالي: كيف ساهمت أساليب الجريمة الالكترونية في انتقال من الإرهاب التقليدي إلى الإرهاب الالكتروني؟

وتتفرع عن هذه الإشكالية، مجموعة من التساؤلات المحورية:

- ماذا نقصد بالإرهاب، و الإرهاب الالكتروني، و الأمن السيبيراني؟

- مدى فعالية الحماية المعلوماتية في مكافحة الإرهاب الإلكتروني ومختلف أشكال الجريمة الالكترونية المنظمة ؟

وللإجابة على هذا الإشكال، نعتمد على المحاور التالية:

المحور الأول: الإرهاب الالكتروني: الخصائص والوسائل المستعملة.

المحور الثاني: دور الأساليب الالكترونية في انتقال الإرهاب التقليدي إلى الإرهاب الإلكتروني الرقمي.

المحور الثالث: سبل مكافحة أساليب الإرهاب الإلكتروني.

أولا: الإرهاب الالكتروني: الخصائص والوسائل المستعملة

1.1. خصائص الإرهاب الرقمي:

كان أول استخدام لكلمة الإرهاب الإلكتروني في فترة الثمانينات في دراسة **"Barrycollin"** التي خلص فيها إلى صعوبة تعريف ظاهرة الإرهاب التكنولوجي بدقة، وأيضا الأساليب والحلول المطلوبة لمواجهته وكذلك تحديد دور الكمبيوتر والإنترنت في العمل الإرهابي.[1]

يتميز الإرهاب الالكتروني الذي يعرف بأنه كل " عدوان أو تخويف أو تهديد مادي أو معنوي باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الإنسان دينه أو نفسه أو عرضه ، أو

عقله ، أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض، وبالتالي فلكي ننعت شخصا ما بأنه إرهابياً على الإنترنت، وليس فقط مخترقاً، فلا بد وأن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب".[2]

وقد ذهب مركز حماية البنية التحتية الوطنية الأمريكية **NIPC** إلى عدّ الإرهاب المعلوماتي **Cyberterrorism** عبارة عن "فعل إجرامي يمارس بواسطة الحاسوب، أو أدواته، فيفضي إلى نشر العنف، والموت، مع إثارة الهلع".[3]

ان تعدد خصائص وسمات الإرهاب الالكتروني يرجع إلى تعدد طرق ووسائل هذا الأخير، حيث تمثلت سمات الإرهاب الالكتروني في:

- أن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسوب متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

- يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود.

- صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم.

صعوبة الإثبات في الإرهاب الإلكتروني، نظرا لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.

- يتميز الإرهاب الإلكتروني بأنه يجري عادة بتعاون أكثر من شخص على ارتكابه.

- أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسوب و الشبكة المعلوماتية.

- إن الإرهاب الإلكتروني لا يترك أي دليل مادي يعد ارتكاب جرائمه، وهذا ما يصعب عملية التعقب واكتشاف الجريمة أساسا.

- سهولة إتلاف الأدلة في حال العثور على أي دليل يمكنه إدانة الجاني.[4]

2.1. الوسائل المستعملة في الإرهاب الإلكتروني:

يعتبر الإرهاب حسب ما عرفته اتفاقية جنيف الخاصة بقمع الإرهاب لعام 1937 على أنه " الأعمال الإجرامية الموجهة ضد الدولة، والتي يكون من شأنها إثارة الفزع والرعب لدى شخصيات معينة أو جماعات من الناس أو لدى الجمهور".[5]

و يعتمد الإرهاب الإلكتروني على " استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم،

مثل ما حصل في العام **2000**، حينما أدى انتشار فيروس الحاسوب **"I love you"** إلى إتلاف معلومات قدرت قيمتها بنحو **10** مليارات دولار أمريكي، وفي العام **2003**، أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسوب، وقدّر "مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت" كلفة إصلاح الأضرار التي تسببها فيروسات المعلوماتية بنحو **12** مليار دولار أمريكي سنوياً".[6]

1- البريد الالكتروني: يعد البريد الالكتروني من أهم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك " من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي حدثت كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها، حيث يتم نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المرسلات الإلكترونية".

2- مو اقع الإنترنت: " يقوم الإرهابيون بإنشاء و تصميم مواقع لهم على شبكة المعلومات العالمية لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وكيفية الدخول إلى المواقع المحجوبة، وطريقة نشر الفيروسات".

و من بعض " المواقع الالكترونية العربية التي تم تصميمها من بعض التنظيمات الإرهابية، نذكر:

1- موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة، بعد أحداث 11 سبتمبر 2001.

2- ذروة السنام: وهي صحيفة الكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

3- صوت الجهاد: مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة، وهي تصدر بصيغتي **Word** و **PDF**، وتتضمن مجموعة من الحوارات مع قادة التنظيم ومنظريه.

4- البتار: مجلة عسكرية الكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية و الميدانية والتجنيد".[7]

ثانيا: دور الأساليب الإلكترونية في انتقال الإرهاب التقليدي إلى الإرهاب الإلكتروني الرقمي:

1- اختطاف المو اقع:

يستطيع المقتحم الاستيلاء على جهاز أو حاسبة اتصال، يقوم بها مستخدم انتهى من إثبات شخصيته، ويحدث هذا الاستيلاء في العادة على أحد الأجهزة التي تتصل عن بعد، وأحيانا يتم استيلاء على أحد الأجهزة الواقعة على المسار الذي يصل بين الحاسب البعيد وبين الجهاز الحاسب المحلي، الذي يعمل عليه المستفيد. [8]

2- سرقة المعلومات:Theft of information

لقد أصبحت مشكلة سرقة المعلومات من أهم المعضلات التي تشهدها المجتمعات الرقمية أو ما تعرف بالواقع الافتراضي: **Virtual Reality** الذي " يحاكى الواقع أو يناظره إلى درجة يخيل لنا معها أنه واقع، ويقصد بها كذلك ما يتجاوز هذا الواقع، والواقع الخائلي هو مفهوم آخر من المفاهيم التي أضافتها تكنولوجيا المعلومات إلى قاموس حياتنا، وينظر إليه على أنه بيئة اصطناعية لممارسة الخبرات بصورة أقرب ما تكون إلى تلك الموجودة في الواقع" [(9)]، و قد تعددت المصطلحات العربية المقابلة للمصطلح الانجليزي **Virtual Reality** من الواقع الافتراضي إلى الواقع الوهمي والواقع الخيالي.[(10)]

شهد عام **1992** ضبط لصوص المعلومات **Information on thieves** وهم يخترقون ملفات إدارة الأمن الاجتماعي ويسرقون سجلات شخصية مهمة للغاية، ثم يقومون ببيع المعلومات التي يحصلون عليها، كما قام اللصوص أيضا بالتسلل إلى أجهزة الكمبيوتر لمكاتب الائتمان الرئيسية وقاموا بسرقة معلومات ائتمانية، ثم استخدموا المعلومات ليدفعوا مقابل بعض المشتريات، ويقوموا بإعادة بيعها إلى أشخاص آخرين.[(11)]

و تنقسم السرقة الالكترونية على خمسة أصناف سرقة البرمجيات ومعدات الحاسوب، والاستخدام غير المخول لشفرات الدخول وكلمات السر المالية، سرقة عن طريق إدخال بيانات احتيالية عن الصفحات والسرقة عن طريق تعديل البرمجيات والسرقة عن طريق الاختلاس، وتعديل البيانات.

و التخريب المعتمد يحاول فيه مرتكبو التدمير المعتمد غزو أو تدمير أجهزة النظام والبرمجيات أو بيانات ويتراوحون بين المتلاعبين والموظفين المستائين إلى الجواسيس، على الرغم من بعض المتلاعبين.[(12)]

3- تدمير المو اقع:

قد تتعرض المواقع الانترنت إلى عمليات تخريب كلية أو جزئية بسبب زرع الفيروسيات في أنظمة أجهزة الكمبيوتر، مما يسبب خالا في برامج نظام التشغيل أو المعالجة، ويشكل الفيروس خطر حقيقيا على الانترنت بما أن انتشاره لا يفرق بين برامج أجهزة الحاسوب والشبكات الالكترونية، كما ساعد النظام الشبكي للانترنت بدوره على انتشار الفيروسات، فحسب الدراسة التي أعدتها الجمعية الدولية لأمن الحاسوب **International computer Security association (ICSA)** أن هذه الوسيلة تعد السبب الرئيسي في **70%** من الإصابات بفيروس الحاسوب سواء من خلال البريد الالكتروني، وذلك بنسبة **56%**، أو عن طريق التحميل بنسبة **11%**، أو عن طريق تصفح الانترنت بنسبة **3%**.[(13)]

وهناك العدد من البرمجيات المستخدمة في التدمير والتخريب، أهمها:

- الباب المسحور: تعد مجموعة التعليمات التي تسمح للمستخدم بتجنب إجراءات الأمن القياسية لنظام الحاسوب، يعضها المبرمجون لتسهيل تعديل البرمجيات وقد تستغل إحدى الأبواب المسحورة التي تركها المبرمجون في تعطيل **6000** جهاز حاسوب.

- حصان طروادة: برنامج يحتوي على تعليمات مخفية يمكن أن تسبب الضرر فمثلا يمكن أن يحدد حصان طروادة رقم معين ويهمله أو يجمع الاختلافات التي تؤدي إلى التدمير ويضعها في حساب معين.

- القنبلة المنطقية: تعد نوعا من حصان طروادة يقوم بتنظيم أعمالها التدميرية لكي تظهر حيث يظهر طرف معين كبدء برنامج معين، وتستخدم عادة في الانتقام و التخريب، كما حدث في عام **1988** في إحدى قضايا المحكمة الفيدرالية بقيام أحد المبرمجين العاملين في شركة **Omege Engineering** في **Bridgeport Jersey** بابتكار قنبلة منطقية، انفجرت بعد **20** يوما حاذفة لكل البرمجيات الإنتاج والتصميم للشركة ومعطلة تسهيلاتها لدعم والتجديد وقدر الضرر الكلي بـ **10** مليون دولار بسبب طرده منها بدافع الانتقام.[14]

- الفيروسات: البرامج و الدودية وأحصنة طروادة، عبارة عن " برامج ضارة تسبب الضرر للحواسيب وللمعلومات الموجودة فيه أو قد تسبب إبطاء سرعة الإنترنت، ويرى **Obrier** أن الفيروس عبارة عن عامل للإصابات المعدية، وهو عبارة عن جسيمة حية متناهية في الصغر تسبب التفسخ، ومن هنا جاءت تسمية البرامج التخريبية للكومبيوتر بالفيروسات نظر الصغر حجمها، واستطاعتها الاختباء في ثنايا البرامج، بشكل ديناميكي حيوي متحرك إذ تعمل على نسخ نفسها والانتشار بما يسمى بالدوائر الحلقية المغلقة للبرامج متخطية كل الاحتياطات والموانع جدران النار".

وكان أول ظهور عام **1983** حيث تفش فيروس في برنامج **Xun**، ويرى **"العبيدي"** أن أول مكتشف للفيروس يعد أحد المبرمجين، الذي قام بحماية معلومات حاسوبه من عمليات النسخ والتقليد والتكبير يقوم بتخريب النسخ المقلدة عن برنامجه أو معلوماته.[15]

فحسب خبير اسباني في محاربة الفيروسات يوجد حاليا في عالم الإنترنت حوالي **45 ألف** فيروسا معلوماتيا، وقد قدر عدد الفيروسات النشطة شهريا ما بين **600** و**800** فيروسا، ومن أشهرها: مليسا، تشرنوبيل، وفيروس الحب، لقد تسبب هذا الفيروس ذو الاسم المغربي (**I love you**)، والذي بلغ ذروته انتشاره من خلال البريد الالكتروني.[16]

4-تسريب المعلومات والوثائق:

وتخترق أمن الدولة والمؤسسات والبنوك والمصاريف وحتى التجسس على الرسائل الالكترونية ولاسيما تزويرها.[17]

ويؤكد خبراء التقنية والمعلوماتية على أن الانترنت هو "عالم من الآثار الخفية"، وفي مسح أجرى عام **1999** في مركز معلومات الخصوصية الالكترونية (**EPIC**) وهي منظمة غير حكومية ، ورد أن أكثر من أربع مائة موقع هم أكثر شعبية ورواجا على الانترنت، تحبذ مخبرين مسربين وقطاع طرق إلكترونين للحصول على صور وتفاصيل كاملة عن مستخدمي الشبكة، كما يجري في محيط الشبكة العديد من عمليات السطو والقرصنة الالكترونية، إذ يستخدم المحتالون وسائل الكترونية مختلفة.[18]

حجم الخسارة المالية للتعديات على أمن المعلومات للفترة من **1997- 1999** [19]

مسمى التعدي	العدد	إجمالي الخسارة بالدولار
-سرقة المعلومات	64	96 .089.000
-تخريب البيانات	66	10.848.850
-التنصت	28	2.508.000
-ولوج النظام من الخارج	69	7.433.700
-سوء استخدام الشبكة داخليا	203	12.302.750
-الاحتيال المالي	82	75.837.000
-منع الخدمة	64	6.042.000
-تغير بروتوكول الاتصال	4	512.000
-فيروسات	424	25.646.150
-دخول غير قانوني داخلي	40	58.123.605
-احتيال اتصالات	96	40.689.300
-تسجيل	6	265.000
-سرقة الحاسب المحمول	472	42.420.200
الإجمالي		360.720.555

و وفقا لمعطيات أحد مكاتب الأبحاث المعنية فإن الشركات الأمريكية أنفقت **6 مليارات** دولار لمقاومة هجمات " قراصنة الكمبيوتر" خلال عام **2000**، وأن هذا سيتجاوز **20 مليار** دولار عام **2004**.

وقد أبلغ " الفريق الأمريكي للتعامل مع الطوارئ الكمبيوترية" (سيرت) بأكثر من **15 ألف** عملية اختراق (قرصنة) خلال الشهور التسعة الأولى **2000**.[20]

و خلقت هذه الجرائم الالكترونية ما يسمى بـ "الحرب الالكترونية"، حيث تكون المعلوماتية هي الساحة التي يتحارب فيها الأعداء، ومثال على ذلك "حرب الهاكرية" بين مجموعات عربية ويهودية، التي استمرت عدة أشهر عامي **2000** و**2001** حيث قام كل طرف بتعطيل وتخريب مواقع الطرف الأخر، فقد تم في الشهر الأول لهذه المعركة في أكتوبر **2000** بتخريب **40** موقع يهودي مقابل **15** موقع عربي.[21]

حيث نقلت وكالة رويترز بتاريخ **2010**، أن شركة المعلومات والبحث العملاقة **غوغل** قد بدأت حملة داخلية لاستبدال نظام "ويندوز" بعد المخاوف الأمنية الالكترونية، التي نتجت عن نجاح هاكرز صينيين باختراق العديد من أنظمة غوغل، نتيجة لضعف وخلل أمني في متصفح الإنترنت الخاص بمايكروسوفت.[22]

5. التجسس المعلوماتي: حيث يتم التجسس على الموظفين فقد جاء في مسح ميداني أجرته حديثا الجمعية الأمريكية لإدارة أن نسبة **63%** من أرباب العمل، يمارسون نوع من الرقابة أو التجسس على موظفيهم وتشمل هذه الممارسات تحري ملفات الكمبيوترية، وسجلات ترددهم على شبكة الإنترنت.[23]

6. السطو على أرقام البطاقات الائتمانية: إن استخدام البطاقات الائتمانية عبر شبكة الإنترنت سهل في عمليات الشراء البيع عبر الإنترنت، وكذا ازدياد في نمو التجارة الإلكترونية، حيث " قام شخصان في عام **1994** بإنشاء موقع على الإنترنت مخصص لشراء طلبات يتم إرسالها بمجرد سداد قيمتها إلكترونيا، إلا أنه كان الغرض من إنشاء هذا الموقع هو الاستيلاء على أرقام البطاقات الائتمانية الخاصة بالمشتريين من هذا الموقع".[24]

ثالثا: سبل مكافحة أساليب الإرهاب الإلكتروني:

هناك العديد من السبل لمكافحة خطر الإرهاب الالكتروني، فبظهور هذا الخطر بدأ التفكير في أساليب وبرمجيات لحماية المعلومات والأجهزة الالكترونية، وترجم هذا التفكير والانشغال ببروز عدة وسائل لمواجهة خطر الإرهاب الالكتروني ومخلفاته، ومنه تحقيق "الأمن الالكتروني" نذكر منها:

-الحماية التقنية:

يمكن اتخاذ بعض الإجراءات الوقائية، لتكون المعلومات والبيانات في مأمن من العبث والانتهاك، بالاعتماد على مجموعة من الوسائل الحمائية، يذكر منها:

أ- برامج الحماية: هي تلك البرامج التي تحقق الأمن عن طريق تصفية وحجب المواقع الممنوعة والخطيرة ، ويتضمن إدارة الوقت لتحديد زمن ومدة اتصال بالمواقع، وهناك برامج حماية خاصة للأطفال تقوم بتحديد البرامج التي يستخدمها، وتمنعهم من إرسال معلومات شخصية أثناء المحادثة.

- برنامج جدار النار:

قامت شركات، خدمات المعلومات، البرامج، وبطاقات الائتمان الكبيرة بتطوير أنظمة حماية، يذكر منها "جدار النار" **Faire Wall Software** كواحد من الاستراتيجيات المتبعة، لمنع عمليات الدخول غير الشرعية من الانترنت، ويعتبر "جدار النار" بمثابة ممر الكتروني يراقب الدخول على الشبكة والخروج منها، وتؤكد الإحصائيات أنه ما يزيد عن ثلث مواقع الواب على الانترنت محمي ببعض أشكال "جدار النار".[25]

ب- الحماية من الفيروسات:

بوضع برنامج اكتشاف في الحواسيب، للقيام بالفحص الدوري، والسريع للبرامج المخزنة، والمعلومات المتداولة بين مختلف الأجهزة المتصلة فيما بينها، وعند اكتشاف فيروس ما يتم التنبيه لوجوده للتمكن من محاصرته ومنعه من التكاثر وإبطال نشاطه التدميري.[26]

ج- اكتشاف التطفل وسوء الاستخدام:

في حين يهدف التحكم بالدخول والترشيح لمنع الأنشطة غير المصرح بها، والأنشطة الضارة بالمعلومات، نجد أن اكتشاف التطفل وسوء الاستخدام يهدف لاكتشاف النشاط الضار في بدايته، ويمكن أن يتحقق ذلك عن طريق مراقبة هذه الأنشطة فيها، وان تم اكتشاف في وقت مبكر ربما يكون في الإمكان إجهاض المحاولة قبل حدوث الضرر، كما تكون بنية الاكتشاف دليل يمكن استخدامه أمام المحاكم لجلب مرتكبي هذه الأعمال غير المشروعة للعدالة، ولكن " مبدأ اكتشاف التطفل وسوء الاستخدام" يقوم على قاعدة أنه ليس عمليا، لأنه، لا يمنع كل الهجمات فيصير الاكتشاف هو الأسلوب العلمي.[27]

2-التنظيمات التشريعية:

- حماية الملكية الفكرية: تعتبر الإبداعات والفنية مثل الصور والرسومات والصور المتحركة، أعمالا محمية بواسطة القانون، في هذا الشأن صادق الكونجرس الأمريكي على قانون العقوبات المعروف بـ: **No Electronic Theft Act**. [28]

لذا تصدت الدول العربية والإسلامية في منطقتنا، وما زالت للإرهاب الإلكتروني، وكل يوم تسد فيه ثغرة من هذه الثغرات، ففي مصر يجري العمل في وزارة الاتصالات والمعلومات لإصدار نظام عن الجريمة الالكترونية، يتضمن عقوبات رادعه لمن يقوم من الأفراد أو المؤسسات بتزوير أو إفساد مستند الكتروني على الشبكة، أو الكشف عن بيانات ومعلومات بدون وجه حق، وغيرها من صور الجريمة الالكترونية.[29]

ورأى الأكاديمي الدكتور "**محمد العقيل**" بكلية الشريعة في فرع جامعة الإمام في الأحساء بالسعودية، خلال ورقة عمل قدمها في المؤتمر "الإرهاب الإلكتروني"، أن الإرهاب جريمة مستجدة، استغلها الإرهابيون في التخطيط والتنسيق والتنفيذ لأعمال إرهابية، وينشرون فكرهم ويدعون إليه بالتحريض والتهديد .

فيما اقترح عضو هيئة التدريس في جامعة الإمام الدكتور "**حمد صليح**"، إنشاء «جيش إلكتروني» لمكافحة الإرهاب.[30]

أما في ألمانيا، فقد أمرت محكمة ألمانية بإيقاف خدمة **Bing Streetside** من مايكروسوفت في ألمانيا وجاء هذا القرار بعد اتهامات من قبل مواطنين ألمان بانتهاك الخدمة الأخير لخصوصياتهم حيث أنها تقوم بتصوير منازلهم الأمر الذي لا يريده هؤلاء.[31]

خاتمة:

إن العالم دولا وشعوب أصبح أمام تحد كبير، يتطلب تنسيقا إلكترونيا عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلا تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذا المشكلة وبخاصة الأنتربول لمواجهة كافة أشكال جرائم الإرهاب على الإنترنت، وهذا من خلال وضع اتفاقيات بين الدول، وتفعيل تلك الاتفاقيات، و تجسيد الأساليب الوقائية و الحمائية لمواجهة خطر الجرائم المستحدثة، من بينها جرائم الإرهاب الالكتروني الذي يشكل تهديدا ماديا و معنويا باستخدام الوسائل الإلكترونية، الصادرة من الدول أو الأفراد على الإنسان دينه أو عرضه، أو ماله بغير حق، لنتمكن من الحديث عن وجود الأمن المعلوماتي أو الأمن الرقمي الذي يكفل حماية المعلومات والبيانات الموجودة على شبكة الانترنت من عمليات التخريب والسرقة، وكل أشكال الإجرام الممارسة عبر الانترنت، بإتباع استراتيجيات وقائية وعلاجية، ومنه المساهمة في الحفاظ على المعلومات الموجودة في العالم السيبيراني، و ضرورة تكريس ثقافة الأمن الرقمي، من خلال تدريس هذه المادة في مختلف الأطوار التعليمية.

و تكمن فعالية الحماية المعلوماتية في مكافحة الإرهاب الإلكتروني ومختلف أشكال الجريمة الالكترونية المنظمة في تحيين التطبيقات الخاصة بالحماية التقنية التي تشهد تطور كبير في ابتكارها، وكذا الحرص على تطبيق مختلف التشريعات القانونية التي جاءت بها مختلف البنود و المواد القانونية المنصوص عليها في الدساتير والقوانين المعمول بها، و منه العكف على صرامة تنفيذ المنظومة القانونية التي بدورها ستكفل حماية الفضاء الرقمي من مختلف الجرائم الالكترونية المستحدثة.

الهوامش:

1- صابرو شعنبي، **"الإرهاب الالكتروني: الإشكال والدو افع"**، مجلة العلوم الاجتماعية والإنسانية، العدد 10، جوان 2015، جامعة تبسة، ص 108 -109.

2- http://diae.net/16243 ; 04-01-2016 ; 15:00 h.

3- حسن مظفر الرزو، **الفضاء المعلوماتي**، ط1، بيروت، مركز دراسات الوحدة العربية، 2007، ص214.

4- أيسر محمد عطية، **دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الإلكتروني وطرق مواجهته**، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية و الدولية، 2-4 – 2014، كلية العلوم الاستراتيجية، عمان، ص 11، 12.

5- عبد الرحمن بن سالم بن فهاد الطريف، **اتجاهات الطلاب الجامعيين نحو ظاهرة الإرهاب: دراسة ميدانية على طاب الجامعات في الرياض**، مذكرة لنيل شهادة الماجستير في العلوم الاجتماعية تخصص تأهيل ورعاية اجتماعية، قسم العلوم الاجتماعية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، 2006، ص 21.

6- http://diae.net/16243 ; 04-01-2016 ; 15:00h.

7- أيسر محمد عطية، **المرجع السابق**، ص 15، 16، 17، 18.

8- حسن طاهر داود، **أمن شبكات المعلومات**، الرياض، مركز البحوث للمملكة العربية السعودية، 2004، ص145.

9- مجبل لازم المالكي، **المكتبات الرقمية**، ط1، عمان، مؤسسة الوراق، 2005، ص 253-.254

10- إبراهيم بعزيز، **دور وسائل الإعلام الجديدة في تحول المتلقي إلى مرسل وظهور صحافة المواطن**، مجلة الإذاعات العربية، العدد3، 2011، ص.47

11- شريف درويش اللبان، **تكنولوجيا الاتصال: المخاطر والتحديات والتأثيرات الاجتماعية**، ط1، القاهرة: الدار المصرية اللبنانية، 2005، ص 120،119.

12- عثمان قاسم داود اللامي، أميرة ستكرولي البياتي، **تكنولوجيا المعلومات في منظمات الأعمال: الاستخدامات والتطبيقات**، ط1، {د، ب}، مؤسسة الوراق، 2010، ص.214

13- قندوشي ربيعة، **الإعلان الالكتروني**، {د،ط}، الجزائر، دار هومة للنشر والتوزيع، 2012، ص 102.

14- عثمان قاسم داود اللامي، أميرة ستكرولي البياتي، المرجع السابق، ص 214-.215

15- عثمان قاسم داود اللامي، أميرة ستكرولي البياتي، المرجع نفسه، ص 216-.217

16- فضيل دليو، وآخرون، **التحديات المعاصرة: العولمة، الإنترنت، الفقر، اللغة**: فعاليات اليوم الدراسي الأول لمخبر علم اجتماع الاتصال، قسنطينة، جامعة منتوري، 2002، ص 20.

17- مجد هاشم الهاشمي، **الإعلام الكوني وتكنولوجيا المستقبل**، ط1، عمان، دار المستقبل للنشر والتوزيع، 2010، ص268.

18- مجد الهاشمي، **تكنولوجيا وسائل الاتصال الجماهيري**، ط1، عمان، دار أسامة للنشر، 2004، ص257.

19- ذياب البدانية، **الأمن وحرب المعلومات**، ط1، عمان، دار الشروق، 2002، ص104.

20- محمد فتحي، **الإنترنت شبكة العجائب: أهم أحداث القرن العشرين و أفاق المستقبل**، القاهرة، دار الطائف للنشر والتوزيع، 2003، ص.73

21- طارق محمود عباس، **المكتبات الرقمية وشبكة**، ط1، القاهرة، المركز الأصيل للنشر والتوزيع، 2003، ص 47.

22- عباس بدران، **الحرب الالكترونية: الاشتباك في عالم المعلومات**، بيروت، مركز دراسات الحكومة الالكترونية، 2010، ص.13

23- أحمد نافع المدادحة، محمد عبد الدبس، **تكنولوجيا المعلومات والشبكات في المكتبات ومؤسسات التعليم**، ط 1، عمان، مكتبة المجتمع العربي للنشر والتوزيع، 2012، ص .191

24- منير الجنبيهي، ممدوح الجنبيهي، **البنوك الإلكترونية**، الإسكندرية، دار الفكر الجامعي، 2006، ص .239

25- قندوشي ربيعة، **المرجع السابق**، ص114.

26- قندوشي ربيعة، المرجع السابق، ص114.

27- ذياب البدانية، المرجع السابق، ص.390

28- قندوشي ربيعة، المرجع السابق، ص116.

29- http://diae.net/16243 ; 04-01-2016 ; 15:00h.

30- https://units.imamu.edu.sa/deanships/dialogue_civilizations/news/Pages/erha b -5.aspx;04-01-2016;15M20h.

31- http://www.alukah.net/library/0/80823/;04-01-2016;14:30h.