الاستلام 7/14 القبول 8/20 النشر
2025/1/25

# مظاهر الإرهاب الإلكتروني وأشكاله

# *Cyber Terrorism Manifestations and Forms*

**بحث من إعداد:**

**الدكتورة منى عصري حمد**

***Dr. Mona Asri Hamad***

**munaasree@gmail.com**

***Criminal Law*** **– القانون الجنائي**

**كلية دجلة الجامعة**

**2024**

## المستخلص

ينطلق الإرهاب بجميع أشكاله من دوافع متعددة، ويستهدف غايات محددة، ويتميز الإرهاب الإلكتروني عن غيره من الإرهاب باستخدامه الموارد المعلوماتية والوسائل الإلكترونية هدف للإرهابيين.

ونظراً لارتباط المجتمعات العالمية فيما بينها بنظم معلومات تقنية عن طريق الأقمار الصناعية وشبكات الاتصال الدولية، فقد زادت الخطورة الإجرامية للجماعات الإرهابية، فقامت بتوظيف طاقتها للاستفادة من هذه التقنية والاستفادة منها في إتمام عملياتها الإجرامية.

كما اصبح من الممكن اختراق الأنظمة والشبكات المعلوماتية، واستخدامها في تدمير البنية التحتية التي تعتمد عليها الحكومات والمؤسسات العامة والشركات الاقتصادية الكبرى مما يشير إلى إمكانية انهيار البنى التحتية لها، حيث يقوم الإرهابي بعمله وهو بعيد عن أنظار السلطة والمجتمع.

ويمكننا القول أن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم لتعدد أشكاله واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح مع توفير قدر من السلامة والأمان للإرهابين.



**الكلمات المفتاحية :**

الارهاب ،الالكتروني ،الشبكة المعلوماتية .



**Abstract**

In all its forms, terrorism stems from multiple motives and targets specific goals. Cyber terrorism is different from other types of terrorism by using information resources and electronic means as target for terrorists.

Given that global communities are connected to each other through technical information systems via satellites and international communication networks, the criminal risk of terrorist groups has increased. Moreover, they invested their energy to take advantage of such technology and benefit from it in completing their criminal operations.

It has also become possible to hack information systems and networks, and use them to destroy the infrastructure on which governments, public institutions, and major economic companies depend, the fact that causes the possibility of the collapse of their infrastructure, as the terrorist carries out his work hidden from authority and society.

We can say that electronic terrorism is the future's terrorism, it is the upcoming danger for its multiple forms and wide range of targets that can be attacked through communications means and information technology in a comfortable atmosphere while providing terrorists with a measure of safety and security.

Keywords:

Terrorism ,electronic,Information network

## المقدمة

تطورت تكنولوجيا المعلومات والاتصالات تطوراً كبيراً ومتسارعاً مما أحدث انفجاراً معرفياً، فالحواسيب وشبكات الإنترنت اختصرت كثيراً من الوقت والجهد وكذلك الإجراءات التقليدية الورقية، فإن العبث بأيّ من هذه الأنظمة عبر الدخول غير المشروع أو غير ذلك من الوسائل بقصد إثارة الرعب والخوف في مجتمع أو بلد معين، مسبّب لأضرار وخيمة هو ما سيكون صلب وجوهر الإرهاب الإلكتروني[0].

ولذلك أصبح كل ما يحتاجه الإرهابي متوافراً من أجل القيام بعملياته التخريبية وهو جالس أمناً في مكانه، وقد قيل إن الإرهاب الإلكتروني أصبح أكثر ضراوة من الإرهاب العادي لاعتماده على التكنولوجيا المتطورة، مما زاد من اتساع مسرح العمليات الإرهابية[1].

تعد جريمة الإرهاب باستخدام الوسائل الإلكترونية من الجرائم الخطيرة كونها تهدف إلى الإخلال بالأمن والنظام العام في المجتمع ولضمان تفادي النتائج السلبية التي تتركها هذه الجريمة أفردت هذه التشريعات في العديد من هذه الدول قوانين خاصة لمعالجتها ومنها الأردن والعراق ومن ثم أستقلت هذه القوانين استقلالاً تاماً في القواعد العامة غير أن هذا الاستقلال لا يغني عن الرجوع إلى القواعد العامة كلما اقتضت الحاجة لسد النقص وإزالة الغموض والعمل كنظام قانوني متكامل.

**أهداف البحث:**

يهدف هذا البحث إلى التعرف عن مظاهر الإرهاب الإلكتروني وأشكالها.

حيث تستخدم الجماعات الإرهابية الشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينها لارتكاب جرائمها.

**أهمية البحث:**

يشهد العالم تحولاً رقمياً كبيراً مما أدى إلى ظهور تهديدات جديدة من بينها الإرهاب الإلكتروني.

---

[1] د. عمار عباس الحسيني، جرائم الحاسب والإنترنت، منشورات زين الحقوقية، بيروت، 2017، ص 350.

**إشكالية البحث:**

يرتبط الإرهاب الإلكتروني بالمستوى المتقدم للغاية التي باتت وسائل الاتصالات وتقنية المعلومات تؤديه في جميع مجالات الحياة وفي العالم بأسره.

لذلك برزت لدينا الإشكالية الرئيسية التالية:-

ماهي مظاهر الأرهاب الألكتروني وأشكاله.ومنها تتفرع التساؤلات الاتية:

- كيفية تبادل المعلومات الإرهابية ونشرها؟
- ماهي طرق تدمير المواقع والنظم المعلوماتية؟
- ماهي المخططات التي يستخدمها الأرهابيين لتهديد وترويع افراد المجتمع؟
- كيف يتم استخدام المواقع الالكترونية للتجسس؟

**منهجية الدراسة:**

تناولنا في هذا البحث مظاهر الإرهاب الإلكتروني وأشكاله، باستخدام المنهج الوصفي التحليلي الذي يقوم على وصف هذه المظاهر وأشكالها.

**هيكلية البحث:**

بهدف تحديد موضوع البحث، تم تقسيمه إلى مبحثين، حيث تناولنا في المبحث الأول المظاهر التقنية للإرهاب الإلكتروني، وفي المبحث الثاني تكلمنا عن اشكال الإرهاب الالكتروني.

## المبحث الأول

## المظاهر التقنية للإرهاب الإلكتروني

يرتبط الإرهاب الإلكتروني بالمستوى المتقدم للغاية التي باتت وسائل الاتصالات وتقنية المعلومات تؤدّيه في جميع مجالات الحياة وفي العالم بأسره ومن خلال الأنظمة الإلكترونية والشبكات المعلوماتية. اتخذ الإرهاب أبعاداً جديدة وازدادت خطورته على المجتمعات الدولية[1].

وسيتم تقسم هذا المبحث إلى مطلبين:

**المطلب الأول: تبادل المعلومات الإرهابية وإنشاؤها ونشرها من خلال شيكة الانترنت.**

**المطلب الثاني: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية.**

## المطلب الأول

## تبادل المعلومات الإرهابية ونشرها من خلال شبكة الإنترنت

إذ تقوم المنظمات والجماعات الإرهابية باستخدام برنامج البريد الإلكتروني وبقية برامج وسائل التواصل الاجتماعي (الفيسبوك، الإنستغرام، التليجرام، التويتر، دي شات، الفايبر، الواتساب وغيرها) نظرا لقلة تكاليفها في الاتصال والتنسيق والتخطيط والتدريب فيما بينها لتنفيذ العمليات الإرهابية أو الأختراق الإلكتروني أو نشر أفكارهم الإرهابية المتطرفة والترويج لها أو نشر البيانات الإرهابية أو الحصول على التمويل والتعبئة والتدريب وتجنيد أكبر عدد من الأتباع الجدد. نظراً إلى قلة تكاليف الاتصال من جانب، فضلاً عن اتّسامه بالسرية التامة في اللقاءات، وجمع بعض المعلومات الحساسة، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن قيادة السيطرة، ومواعيد الرحلات الجوية، ويمكن تحديد أهم الاستخدامات من خلال تقسيمها وفق الآتي:

أ- الاتصال والتخفّي.

ب- جمع المعلومات الإرهابية.إذ

ج- التخطيط والتنسيق.

د- الحصول على التمويل.

---

[1] علي عدنان الفيل، الإجرام الإلكتروني، ط1، منشورات زين الحقوقية، بيروت، 2011، ص 77.

هـ- تجنيد الإرهابيين.

و- التدريب الإرهابي الإلكتروني.

ز- إصدار البيانات الإلكترونية.

## أولاً: الاتصال والتخفي

تستخدم الجماعات والمنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينهم نظراً إلى قلة كلفة الاتصال والرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى كما إن الشبكة توفر للإرهابيين فرصة ثمينة في الاتصال والتخفي عن طريق البريد الإلكتروني أو المواقع والمنتديات وغرف الحوار الإلكتروني حيث يمكن وضع رسائل مرمّزة تتخذ طابعاً لا يلفت الانتباه ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته كما أنها لا تترك أثراً واضحاً يمكن أن يدل عليه[1].

لذا يمكن القول إن مظاهر الإرهاب الإلكتروني اليوم بالدرجة الأساسية تتجسد برامجها في الدول المتطورة في مجال الاتصالات فالدول التي تعتمد على وسائل الاتصالات والشبكات الالكترونية سيكون عاملاً فاعلاً في فتح المجال أمام الإرهابيين لتحقيق أهدافهم وتدمير منتجات التقنية الحديثة فالإرهاب الإلكتروني يهدف إلى تدمير البنية التحتية المعلوماتية وتعريض المجتمعات العالمية لمخاطر غير متوقعة. لكن في المقابل، هذا الأمر لا يعني أن الدول التي لم تستخدم تقنيات المعلومات تكون بعيدة عن مخاطر الإرهاب الإلكتروني بل يمكن القول أيضاً إن الدول التي بدأت حديثاً باستخدام التطبيقات الإلكترونية – كما هو الحال في العراق فإنها تكون على استعداد وتأهب لمواجهة مثل هذه الأخطار المحتملة والتصدي لها بشكل جديد ومن أبرز ما يميّز الإرهاب الإلكتروني هو إمكانية الدخول إلى أي موقع سواءً كان بيتاً أو مكتباً أو من أي مكان خاص أو عام أن ينفذ جريمته وخلال ثوان يعطل آلاف الحواسيب ويخرب الأنظمة المعلوماتية[2].

---

[1] د. حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى، بغداد، 2013، ص 335.

[2] علي عدنان الفيل، مرجع سابق، ص 80.

## ثانياً: جمع المعلومات الإرهابية

تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها كما أنها تعتبر الموسوعة الإلكترونية الشاملة المتعددة الثقافات والمتنوعة المصادر وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها كمواقع المنشآت النووية ومصادر توليد الطاقة وأماكن القيادة والسيطرة والاتصالات ومواعيد الرحلات الجوية الدولية والمعلومات المختصة بسبل مكافحة الإرهاب ونحو ذلك من المعلومات التي تعدّ بمنزلة الكنز الثمين بالنسبة إلى الإرهابيين نظراً إلى ما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية[1].

## ثالثاً: التخطيط والتنسيق للعمليات الإرهابية

العمليات الإرهابية عمل على جانب كبير من التعقيد والصعوبة فهي تحتاج إلى تخطيط محكم وتنسيق شامل وتعد الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية إذ تتيح لهم حرية التخطيط الدقيق والتنسيق لشن هجمات إرهابية محددة في جو مريح بعيداً عن عيون الناظرين مما يسهل على الإرهابيين ترتيب تحركاتهم وتوقيت هجماتهم[2].

## رابعاً: الحصول على التمويل

من خلال هذه الشبكة العالمية، وعن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية ومن خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثمّ يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين ويتم ذلك بوساطة رسائل البريد الإلكتروني أو من خلال ساحات الحوار الإلكترونية بطريقة ذكية وأسلوب مخادع ولا يشك المتبرع بأنه سيساعد أحد التنظيمات الإرهابية[3].

---

[1] علي عدنان الفيل، مرجع سابق، ص 81.

[2] حسن تركي عمير، الإرهاب الإلكتروني ومخاطرة في العصر الراهن، مرجع سابق، ص 337.

[3] علي عدنان الفيل، مرجع سابق، ص 81-82.

## خامساً: التعبئة وتجنيد الإرهابيين

تستخدم الجماعات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها وبث الأفكار والفلسفات التي تنادي بها كما تسعى جاهدة لتوفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها. ومن خلال الشبكة المعلوماتية تقوم هذه التنظيمات بتكوين قاعدة فكرية لدى من لديهم ميول واستعداد للانخراط في الأعمال التدميرية والتخريبية مما يوفر لديها قاعدة ممن تجمعهم الأفكار والتوجهات فيسهل لتنفيذ هجمات إرهابية في المستقبل.

إن استقدام عناصر جديدة داخل التنظيمات الإرهابية يحافظ على بقائها واستمرارها لذلك فإن الإرهابيين يقومون باستغلال تعاطف بعض الافراد مع قضاياهم فيجتذبونهم بأسلوب عاطفي وعبارات حماسية براقة وذلك من خلال غرف الحوار والمنتديات والمواقع الإلكترونية[1].

## سادساً: التدريب الإرهابي الإلكتروني

تحتاج العمليات الإرهابية إلى تدريب خاص ويعدّ التدريب من أهم هواجس الجماعات الإرهابية وقد أنشأت معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام لكن مشكلة معسكرات التدريب الإرهابية أنها دائماً معرضة للخطر ويمكن اكتشافها ومداهمتها في أي وقت لذلك فإن الشبكة المعلوماتية بما تحتويه من خدمات وميزات أصبحت وسيلة مهمة للتدريب الإرهابي كما قامت بعض الجماعات بإنتاج أدلة إرشادية لعملياتها الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي وهي ادلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم[2].

وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة المدمرة.

---

[1] علي عدنان الفيل، مرجع سابق، ص 82.

[2] حسن تركي عمير، الإرهاب الإلكتروني ومخاطرة في العصر الراهن، مرجع سابق، ص 338.

**سابعاً: إصدار البيانات الإلكترونية**

تقوم الجماعات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة وذلك عن طريق المواقع الإلكترونية أو بوساطة رسائل البريد الإلكتروني أو من خلال منتديات الحوار وقد ساعدت القنوات الفضائية التي تسارع للحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات ووصولها إلى مختلف شرائح المجتمع.

وتأخذ البيانات الصادرة عن الجماعات اتجاهات متنوعة فتارة ترسم أهدافاً وخططاً عامة للتنظيم الإرهابي وأحياناً تكون للتهديد والوعيد بشن هجمات إرهابية معينة في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية كما تصدر تارة أخرى بالنفي أو التعليق على أخبار أو تصريحات صادرة عن جهات أخرى[1].

قامت الجماعات الإرهابية بإنشاء مواقع إرهابية إلكترونية توضح فيها برامج صناعة المتفجرات وشرح طرائق اختراق البريد الإلكتروني وتدمير المواقع الإلكترونية، واستطاعت تلك الجماعات إنشاء آلاف المواقع الإلكترونية الجاهزة التي تستخدمها في حال إيقاف أحد المواقع أو تستخدمها للتخفي والاختباء لتظهر بشكل جديد ومن موقع آخر بعنوان مغاير وكشفت بعض الدراسات أن هنالك حوالي ٥٠٠٠ إلى ٦٠٠٠ موقع للتنظيمات الإرهابية[2].

وبناءا عليه يقوم الإرهابيون بإنشاء مواقع لهم على الشبكة العالمية للمعلومات لبث أفكارهم الضالة والدعوة إلى مبادئهم المنحرفة ولإبراز قوة التنظيم الإرهابي وللتعبئة الفكرية وتجنيد إرهابيين جدد ولإعطاء التعليمات والتلقين الإلكتروني وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية فقد أنشأت مواقع إرهابية إلكترونية لبيان كيفية صناعة القنابل والمتفجرات والأسلحة الكيماوية الفتاكة، ولشرح طرائق اختراق البريد الإلكتروني، وكيفية اختراق المواقع الإلكترونية وتدميرها والدخول إلى المواقع المحجوبة ولتعليم طرق نشر الفيروسات.

---

(1) عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد في المدة 2-4 يونيو 2008، ص 17.

(2) مصطفى محمد موسى، الإرهاب الإلكتروني، ط1، مطابع الشرطة، القاهرة، 2009، ص 222.

فالموقع مستودع معلومات مخزّنة بشكل صفحات وكل صفحة تشتمل على معلومات معينة تشكلت بوساطة مصمم الصفحة باستخدام مجموعة من الرموز تسمى لغة تحديد النص الأفضل من أجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العالمية ويقوم بحل رموز وإصدار التعليمات لإظهار الصفحات المكتوبة[1].

وإذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً بالنسبة إلى الإرهابيين فإن إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات لخدمة أهدافهم وترويج أفكارهم أصبح سهلاً وممكناً ولذلك فإن معظم التنظيمات الإرهابية لها مواقع إلكترونية وهي بمنزلة المقر الافتراضي لها.

إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة فإذا ظهر موقع إرهابي اليوم فسرعان ما يغير نمطه الإلكتروني غداً ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان إلكتروني مختلف بل تجد لبعض الجماعات الإرهابية آلاف المواقع حتى يضمنوا انتشاراً أوسع ولو تمّ منع الدخول إلى بعض هذه المواقع أو تعرّض بعضها للتدمير تبقى المواقع الأخرى ويمكن الوصول إليها[2].

## المطلب الثاني

## تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم الجماعات الإرهابية بشن هجمات إلكترونية عبر الشبكة المعلوماتية بهدف تدمير الأهداف العسكرية كأنظمة الدفاع الجوي وأنظمة التحكم، وفي مقدّمتها مراكز القيادة والتحكم العسكرية ثم مؤسسات المنافع كالمؤسسات الكهربائية والمياه، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية.

---

[1] سايمون كولن، التجارة على الإنترنت، نقله إلى العربية يحيى مصلح، بيت الأفكار الدولية بأمريكا، 1999، ص26.

[2] علي عدنان الفيل، مرجع سابق، ص 85.

والهدف من التدمير هو الدخول غير المشروع إلى نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي أو مجموعة نظم مترابطة شبكياً بهدف تخريب نقطة الاتصال أو النظام.

وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم. فالمتغيرات التقنية والإمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء سواء كان ذلك في مكونات نقطة الاتصال أو في النظم أو في الشبكة أو في البرمجة جعلت الحيلولة دون الاختراقات صعبة جداً إضافة إلى ذلك هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع ومن المعروف أن المؤسسات لديها من الإمكانات والقدرات ما ليس لدى الأفراد.

لذلك بأمكان قراصنة الحاسبة الإلكترونية التوصّل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة والسبب في ذلك يراجع إلى أن التطور المذهل في عالم الحاسب الآلي والشبكات المعلوماتية يصحبه تقدم أعظم في الجرائم المعلوماتية وسبل ارتكابها، ولاسيما أن مرتكبيها ليسوا مستخدمين عاديين بل قد يكونون خبراء في مجال الحاسبة الإلكترونية[1].

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الأساسية والرموز الخاصة ببرامج شبكة الإنترنت وهي عملية بالإمكان القيام بها من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له للحد من الاختراقات المعلوماتية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي تتصف به نظم تشغيل الحاسبة الإلكترونية والشبكات المعلوماتية[2].

ويمكن لمزود خدمات الإنترنت أن يكتشف كل أفعال مستخدم الإنترنت عندما يتصل بالشبكة ويشمل ذلك عناوين المواقع التي زارها ومتى تم ذلك والصفحات التي اطلع عليها والقضايا التي جلبها، والكلمات التي تم البحث عنها والحوارات التي شارك فيها وكذلك البريد الإلكتروني الذي أرسله أو استقبله واستمارة الشراء للسلع التي طلب شراءها والخدمات التي شارك فيها، لكن تختلف

---

[1] د. سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، الإمارات العربية المتحدة، العدد 91.

[2] موزة المزروعي، الاختراقات الإلكترونية خطر كيف تواجهه، مجلة آفاق اقتصادية، الإمارات العربية المتحدة، العدد 9، 2000، ص 54.

من الناحية الفعلية كمية المعلومات التي يجمعها مزوّد خدمات الإنترنت عن مستخدم الشبكة باختلاف التقنيات والبرامج التي يستخدمها فإذا لم يكن مزود الخدمة يستخدم مزودات (بروكسي) تتسلم كل الطلبات وتنظمها ويستخدم برامج تحسس الرقم الخاص (IP) التي تحلل حركة المرور بتفصيل كبير فأنه قد لا يسجل سوى البيانات الشخصية للمستخدم وتاريخ الاتصال وزمنه والانفصال عن الشبكةالمعلوماتية وبعض البيانات الأخرى. إن معرفة البيانات التفصيلية للمستخدم تجعل الإقدام على الاعتداء الإلكتروني أقل ضرراً وذلك لأن بعض الذين يحصل منهم الاعتداء الإلكتروني يتم ذلك بسبب ظنهم أن بياناتهم التفصيلية لا يمكن الإطلاع عليها فيظن أنه بمجرد دخوله على الشبكة بإسم وهمي تصبح بياناته غير معلومة وهذا خطأ[1].

وبالامكان تصور هجوم إلكتروني على أحد المواقع الإلكتروني بقصد تدميرها وشلها عن العمل فيمكن أن يقوم الإهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على شبكة المعلومات وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات ومحطات توليد الطاقة والماء ومواقع الأسواق المالية فيؤدي توقفها عن العمل إلى حدوث آثار تدميرية تفوق ما تحدثه القنابل والمتفجرات من آثار.

كما انه بالأمكان تصور هجوم إلكتروني على أحد المواقع الإلكترونية بقصد الإستيلاء على محتوياتها إذا قامت أحد الجماعات الإرهابية بشن هجوم إرهابي عن طريق الشبكة المعلوماتية على أحد البنوك والمصارف المالية بقصد سرقة الأموال والاستيلاء عليها من أجل تمويل التنظيم الإرهابي.

فمن المتصور اختراق مواقع معينة بقصد السيطرة والتحكم بها، وقد هيمن الذعر على المختصين بمكافحة الإرهاب الإلكتروني عندما تمكن أحد الأشخاص من السيطرة على نظام الحاسبة الإلكترونية في أحد المطارات الأمريكية الصغيرة حيث قام بإطفاء مصابيح إضاءة ممرات هبوط الطائرات.

ومن الممكن تصور شن هجوم إلكتروني على البنية التحتية للشبكة المعلوماتية بقصد تدميرها وتوقفها عن العمل مما يحدث آثاراً مادية واقتصادية وسياسية وثقافية خطيرة لأن توقف الشبكة

---

[1] د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظار أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومرك تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3، ص 42.

الانترنت يعني توقف القطاعات والمرافق الحيوية عن العمل بالإضافة إلى توقف الحكومات الإلكترونية عن عملها وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية[1].

إن من الوسائل المستخدمة في الوقت الحالي لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية من جهاز الحاسبة الإلكترونية الخاص بالمدمر إلى الموقع المستهدف للتأثير في السعة التخزينية للموقع فتشكل هذه الكمية الهائلة من الوسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسروبالتالي الحصول على كل ما تحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه[2].

وفي الواقع إن هناك أسباباً لوقوع عملية تدمير المواقع ومن هذه الأسباب ما يأتي:

**أولاً:** ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها وبالتالي سسهولة عملية كسر الكلمات السرية وتخمينها من المخترق.

**ثانياً:** عدم وضع برامج كافية لحماية الموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج التي تعمل على التنبيه عند وجود حالة اختراق للموقع.

**ثالثاً:** استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر أو تستخدم برامج وأنظمة غير موثوقة أمنياً ولا يتم تحديثها باستمرار.

---

(1) عبد الله بن عبد العزيز بن فهد العجلان، المرجع نفسه، ص 19.

(2) د. عماد علي خليل، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3، ص 4.

**رابعاً:** عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان يمكن اكتشاف المزيد من الثغرات الأمنية فيه وهذا يستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية[1] تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها.

**خامساً:** عدم القيام بالنسخ الاحتياطي للموقع وذلك للبرامج والمجلدات الموجودة فيه وعدم القيام بنسخ قاعدة البيانات الموجودة في الموقع لان ذلك يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خصوصاً مع تفاقم مشكلة الاختراقات في الفترة الأخيرة. ويعد عام 2002 من أكثر الأعوام اختراقاً فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات[2].

وتعد الفيروسات من أخطرالافات للشبكة المعلوماتية، والفيروس هو برنامج حاسوبي يلحق ضرراً بنظام المعلومات والبيانات ويقدر على التضاعف والانتشار والانتقال من جهاز إلى آخر.

إن فايروس الحاسبة الإلكترونية يتشابه مع الفيروس الطبيعي من نواحٍ عديدة، فهو يغيّر خصائص البرامج كما يقوم الفيروس الطبيعي بتغيير خصائص الخلايا المصابة، وهو يتكاثر وينتشر ويغيّر من شكله تماماً كالفيروس الطبيعي وللفايروس أنواع متعددة وهي متدرجة من ناحية الأضرار التي تلحقها بالأجهزة بدءاً من الأضرار اليسيرة إلى تدمير النظام بأكمله ويمكن للإرهابي استخدام الفيروسات لنشر الدمار عبر الشبكات المعلوماتية والأنظمة الإلكترونية كما يمكن استخدامها في الاختراق والتجسس أيضاً.

وبناء على ما سبق ذكره يتبيّن أن الجماعات الإرهابية استطاعت أن تدخل بشكل غير مشروع وغير قانوني على نقاط أساسية أو فرعية متصلة بالشبكة المعلوماتية خلال عدة أنظمة آلية

---

[1] حذرت شركة مايكروسوفت من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز، وتقول الشركة: إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة بأنها حرجة، ودعت المستخدمين إلى تركيب ترقيعي لحل المشكلة، جريدة الرياض، العدد (12542)، السبت 1423/8/20 هـ، ص 19.

[2] جريدة الرياض، العدد (12460)، يوم الإثنين 1423/5/26 هـ، ص 32.

أو مجموعة انظمة مترابطة الشبكات إذ يتمكن قراصنة الحواسيب (Hackers) من التوصل إلى المعلومة السرية والشخصية واختراق الخصوصية وسرية المعلومات بكل سهولة ويسر ومن أبرز الوسائل المستخدمة في تدمير المواقع هو ضخ آلاف الرسائل الإلكترونية من جهاز الحاسوب الخاص بالإرهابي إلى الموقع المراد استهدافه للتأثير في سعة الخزن الكبيرة التي تؤدي من ثم إلى تفجير الموقع وتشتيت البيانات نقلها إلى جهاز المعتدي[1].

[1] د. حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مرجع سابق، ص 336.

## المبحث الثاني

## اشكال الارهاب الإلكتروني

إن اعتماد الدول على وسائل الاتصالات وشبكات الانترنيت يعد عاملاً فاعلاً في فتح المجال أمام الإرهابيين لتحقيق أهدافهم وتدمير منتجات التقنية الحديثة التي تخدم الإنسانية، وتسهّل التواصل المعرفي والعلمي والثقافي، ولذلك فإن المعلومات في هذه الحالة تصبح عرضة لكل المخاطر المحتملة من هذا النمط المتجدد من الإرهاب المعاصر، فالإرهاب الإلكتروني يهدف إلى تدمير البنية التحتية المعلوماتية فياخذ بناءا على ذلك أشكالاً مختلفة حتى يتمكن المجرم من التوصول الى مبتغاه وهذا ما سيتم إيضاحه من خلال تقسيم هذا المبحث إلى مطلبين:

**المطلب الأول: مخططات الإرهاب الإلكتروني والتهديد والترويع الإلكتروني.**

**المطلب الثاني: التجسس الإلكتروني.**

### المطلب الأول

### مخططات الإرهاب الإلكتروني

قام خبراء الجرائم الإلكترونية والأمن المعلوماتي بوضع أكثر من مخطط محتمل للهجمات الإرهابية وأودعوها في البحوث والدراسات والتقارير التي تعالج هذه المسألة. ويمكن تقسيم هذه المخططات إلى ما يأتي:

**<u>أولاً: استهداف النظم العسكرية</u>**

تستهدف هذه الهجمات عادة الأهداف العسكرية غير المدنية والمرتبطة بشبكات الانترنيت ويعدّ هذا السيناريو من أخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر إذ تبدأ المرحلة الأولى من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية ونظم الدفاع الجوي، والصواريخ النووية فقد تتوافر لإرهابي المعلومات فرصة فك الرموز السرية للتحكم بتشغيل

منصات إطلاق الصواريخ الاستراتيجية والأسلحة الفتاكة فيحدث ما لا تحمد عقباه على المستوى العالمي[1].

ومثال ذلك اختراق المنظومات الخاصة بالأسلحة الاستراتيجية نظم الدفاع الجوي والوثائق العسكرية، ومن أبرز الأمثلة على ذلك ما قام به موقع ويكيليكس عام 2010 بنشر تسريبات ووثائق عسكرية مهمة.

## ثانياً: استهداف البنية التحتية الاقتصادية

أصبح الاعتماد على شبكة الانترنيت شبه مطلق في عالم المال والأعمال مما يجعل هذه الشبكات نظراً إلى طبيعتها المترابطة وانفتاحها على العالم هدفاً حيوياً للمجرمين والإرهابيين ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل كبير بالانطباعات السائدة والتوقعات والتشكيك في صحة هذه المعلومات أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة وبالتالي أضعاف الثقة بالنظام الاقتصادي.

يشمل هذا السيناريو إحداث خلل واسع في نظم الشبكات التي تتحكم بسريان أنشطة المصارف وأسواق المالية العالمية ونشر الفوضى في الصفقات التجارية الدولية بالإضافة إلى ذلك يمكن إحداث توقف جزئي أو كلي في منظومات التجارة والأعمال ومن ثم تتعطل الأنشطة الاقتصادية وتتوقف عن العمل[2].

## ثالثاً: استهداف نظم المواصلات

يتضمن هذا اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية وإحداث خلل في برامج هبوط الطائرات وإقلاعها مما قد ينجم عنه حصول تصادم فيما بينها أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات كما يحتمل تمكن قراصنة المعلومات من السيطرة على التحكم بتسيير القطارات وتغيير مواعيد الانطلاق فتسود الفوضى أو تتصادم هذه القطارات فيما بينها وكذلك بالنسبة إلى السفن والناقلات والغواصات البحرية[3].

---

[1] علي عدنان الفيل، مرجع سابق، ص 92.

[2] المرجع نفسه، ص 93.

[3] عبد الله بن عبد العزيز بن فهد العجلان، المرجع نفسه، ص 21.

**رابعاً: استهداف نظم الاتصالات**

ويشمل هذا السيناريو اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية وإيقاف محطات توزيع الخدمة الهاتفية وقد تمارس سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية وهذا الأمر قد ينشر حالة من الرعب والفوضى وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية[1].

**خامساً: استهداف محطات توليد الطاقة والماء**

أصبح الاعتماد على شبكة المعلومات وخصوصاً في الدول المتقدمة من الوسائل المهمة لإدارة نظم الطاقة الكهربائية ويمكن لهجمات من هذا النوع من شبكات المعلومات، أن تؤدي إلى نتائج خطيرة وخصوصاً في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية ولذلك فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الإلكتروني.

كذلك يشمل هذا السيناريو مباشرة سلسلة من الهجمات المعلوماتية على نظم الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية الوطنية وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في البلاد وسيادة الفوضى نتيجة لانعدام مصادر الطاقة الكهربائية وشل الحركة في عموم البلاد وكذلك بالنسبة إلى شبكات مصادر المياه وطرائق توزيعها.

ولا يتوقف الأمر عند هذا الحد فقط وأنما هناك العديد من الأهداف الأخرى التي يمكن للمجرمين والإرهابيين المتمكنين من خلالها أن يشيعوا الفساد وينشروا الفوضى في العالم فهناك على سبيل المثال شبكات المعلومات الطبية التي يمكن مهاجمتها واختراقها ومن ثم التلاعب بها حصول خسائر بشرية ومن أمثلة ذلك في العالم الغربي ما قام به أحد المجرمين من الدخول إلى سجلات المستشفيات والتلاعب ببيانات المرضى بشكل يؤدي إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة إليهم. حتى لو افترض أن شبكات المعلوماتية الخاصة بالمؤسسات الطبية منيعة فإن رسالة

---

[1] علي عدنان الفيل، مرجع سابق، ص 92.

واحدة تنشر مثلاً بالبريد الإلكتروني مفادها أن هنالك دماء ملوثة في المستشفيات وما إلى ذلك يمكن لها أن تحدث آثاراً مدمرة على الصعيد الاجتماعي[1].

ومثال ذلك مؤسسات الطاقة وغيرها إذ هدد خبير بلجيكي بكسر رمز أجهزة كمبيوتر محولات الكهرباء في بلجيكا يوم الأربعاء 1999/9/29 في الفترة بين الساعة الواحدة والنصف وبين الثالثة والنصف بعد الظهر بقطع التيار الكهربائي عن بلجيكا كلها.

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ومن خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرائقه وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية ومن أجل الحصول على التمويل المالي و أظهار قوة التنظيم الإرهابي من ناحية أخرى.

فالتهديد يعني الوعيد بزرع الخوف ونشره في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أن ضرراً ما سيلحقه أو سيلحق أشخاصاً أو أشياء تربطه بها صلة.

قد يلجأ الارهابي الإلكتروني إلى التهديد وترويع الآخرين بوساطة الاتصالات والشبكات المعلوماتية لغرض تحقيق النتيجة الإجرامية المرجوة. ومن الطرائق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة تهديداً وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار الإلكترونية.

اختلفت الأساليب الإرهابية في التهديد فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع وتارة يكون التهديد بالقيام بتفجير منشآت وطنية ويكون تاريخ أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية، ونحو ذلك[2].

---

[1] علي عدنان الفيل، مرجع سابق، ص 94 – 95.

[2] عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، ص 22.

## المطلب الثاني

## التجسّس الإلكتروني

يقوم الإرهابيون بالتجسّس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسّس الإلكتروني بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والأنظمة الإلكترونية التي جلبتها التقنية في عصر المعلومات والتي تستهدف عمليات التجسّس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية، وهي: التجسّس العسكري، والتجسّس السياسي، والتجسّس الاقتصادي.

ومع وجود وسائل التقنية الحديثة، فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي وقد تحولت وسائل التجسّس من الطرائف التقليدية إلى الطرائق الإلكترونية خصوصاً مع ظهور الشبكات المعلوماتية وانتشارها عالمياً. ومع توسّع التجارة الإلكترونية عبر الشبكة العالمية للمعلومات حولت مصادر المعلومات التجارية إلى أهداف للتجسّس الاقتصادي.

إن محاولة اختراق الشبكة والمواقع الإلكترونية من قبل العابثين من مخترقي الأنظمة المعلوماتية لا يعد إرهابياً فمخاطر هؤلاء محدودة وتقتصر كثيراً على العبث أو إتلاف المحتويات التي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع آمن ويكمن الخطر في عمليات التجسس التي تقوم بها الجماعات الإرهابية وأجهزة الاستخبارات المختلفة من أجل الحصول على الأسرار ومعلومات الدولة ومن ثم إفشائها لدول أخرى معادية أو استغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة.

حيث تتم عملية إرسال نظم التجسس الإلكتروني بعدة طرائق ومن أشهرها البريد الإلكتروني إذ يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، وهناك طرائق أخرى لزرع حصان طروادة وكذلك عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها وكذلك

يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص كما يمكن للإرهابي استخدام الفيروسات في الاختراق والتجسس المعلوماتي[1].

ومن الأساليب الحديثة للتجسس الإلكتروني أسلوب إخفاء المعلومات داخل المعلومات ويتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة داخل معلومات أخرى عادية، داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها حتى لو تم ضبط الشخص متلبساً كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية. ومما يقوم به الإرهابيون هو اختراق البريد الإلكتروني للآخرين، وهتك أسرارهم والإطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية أو تهديدهم لحملهم على إتيان أفعال معينة يخططون لاقترافها.

تتجلى الخطورة في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولا يمكن الاعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية فهي ليست أمينة ولا يمكن الإطمئنان إليها تماماً.

مما تجدر الإشارة إليه أن الطرق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية نظراً إلى أهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية وخاصة العسكرية والسياسية والاقتصادية وهذه المعلومات إذا ما تعرضت للتجسّس وتم الحصول عليها فسوف يُساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن[2].

وبناءً على ما تقدم يمكن أن نستنتج أن هذه المظاهر وغيرها ليست من قبيل الخيال العلمي إنما هي مظاهر تمثل أخطار محتملة نتيجة الاعتماد الكبير على تكنولوجيا المعلومات أضافةً إلى استفادة الجماعات الإرهابية من هذه التكنولوجيا الحديثة وسائر الاتصالات الحديثة التي تعتمد الإنترنت في عملها مما وفر لهم الاتصال المجاني والسريع فيما بينهم والتنسيق بشان عملياتهم الإرهابية وبالتالي فرض الإرهاب الإلكتروني نفسه كظاهرة سلبية على المجتمعات بعد التطور

---

[1] علي عدنان الفيل، مرجع سابق، ص 96 – 97.

[2] عبد الله عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، ص 23.

الإلكتروني الذي وصل إليه هذا الأخير، فبدأ التأثير السلبي لهذا الإرهاب واضحاً مهدداً للأفراد والجماعات والأموال والحكومات على حد سواء.

## الخاتمة

في ختام هذا البحث حول مظاهر الإرهاب الإلكتروني واشكاله ، يتضح أن هذه الظاهرة أصبحت من أخطر التهديدات الي تواجه العالم في العصر الرقمي.يشمل الإرهاب الالكتروني مجموعة واس عة من الأنشطة التخريبية التي تهدف إلى إلحاق الضرر بالبنية التحتية الرقمية للدول ،او استغلال الانترنيت لنشر الأفكار المتطرفه والتحريض على العنف.

وقد أظهرت الدراسة ابرز مظاهر الإرهاب الألكتروني على الانظمه الحيوية، واستخدام وسائل التواصل الاجتماعي كأداة لنشر الفكر المتطرف.

وبينا أيضا أشكال الإرهاب الألكتروني التي يتبعها الإرهابي عادةً للوصول إلى هدفه عن طريق المواقع الإلكترونية المختلفة.

فلابد من توحيد الجهود والعمل الجاد من أجل السيطرة على هذا السلاح الخطر الذي اصبح متاح لهذه الجماعات والذي من خلاله ضرب الأمن والسلم.

بعد الانتهاء من دراسة جريمة الإرهاب عبر الوسائل الإلكترونية تمّ الوصل إلى جملة من النتائج والمقترحات.

### أولاً: النتائج

1 - أعتماد الارهابين على التكنولوجيا الحديثة مثل الشبكات الاجتماعية والبرمجيات الخبيثه، في التخطيط للهجمات ونشر الأفكار المتطرفة وتجنيد الأفراد.

2 - من ابرزمظاهر الإرهاب الألكتروني استهداف الانظمه الحيوية مثل شبكات الكهرباء،المياه، الانظمه المالية، الهجمات على هذه البنى التحتية قد تؤدي إلى تعطيل المجتمعات.

3 - يعتبر تتبع مرتكبي الهجمات الالكترونية تحدياً كبيراً للجهات الأمنية، نظرا لأن هذه الهجمات غالبا ماتكون عابرة للحدود ويتم تنفيذها بأستخدام تقنيات متقدمة لإخفاء الهوية.

4 - يأخذ الإرهاب الألكتروني اشكال مختلفة تتنوع بناءا على الأهداف والأدوات المستخدمة مما يعكس تعقيد الظاهرة وصعوبة مواجهتها.

5 - الانترنت اصبح وسيلة رئيسية للجماعات الإرهابية لنشر الأيديولوجيا المتطرفة، التحريض على العنف والتجنيد، مما يجعل من الضروري مراقبة هذه الأنشطة بشكل اكثر صرامة من قبل الحكومات والشركات التقنية.

## ثانياً: التوصيات:

1 - توجيه المزيد من الجهود لمراقبة المحتوى الالكتروني الإرهابي عبر الإنترنت بما في ذلك مواقع التواصل الاجتماعي ومنصات البث والمواقع المظلمة (Dark web). هذا يشمل خطر المحتويات المتطرفة والتحريضية بشكل فعال.

2 - يجب على الدول تحديث قوانينها الوطنية بما يتناسب مع التطورات التكنولوجية لمكافحة الإرهاب الألكتروني بشكل اكثر فاعلية. يجب أيضا العمل على سن تشريعات دولية موحدة للتعامل مع الهجمات العابرة للحدود.

3 - رفع مستوى الوعي لدى المواطنين والشركات حول التهديدات الالكترونية وكيفية حماية أنفسهم من الهجمات. يمكن تحقيق ذلك من خلال حملات توعية، ورش عمل، برامج تدريبية.

4 - يجب تطوير استراتيجيات لمكافحة الدعاية الالكترونية التي تسخدمها الجماعات الإرهابية لتجنيد الافراد.

من الضروري دعم الأبحاث الأكاديمية المستمرة حول الإرهاب الألكتروني وأساليبه المتجددة وذلك لتوفير رؤية مستقبلية شاملة حول الطرق المثلى لمواجهته.

# قائمة المصادر


1- عمار عباس الحسيني، جرائم الحاسب والإنترنت، منشورات زين الحقوقية، بيروت، 2017.

2- راستي الحاج، الإرهاب في وجه مساءلة الجزائية محلياً ودولياً "دراسة مقارنة"، ط1، منشورات زين الحقوقية، بيروت، 2012.

3- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات والمتاح على الموقع: http://www.shaimaaatalla.com/vb/showthread.php?t=3937، تاريخ الزيارة ٢٠٢٣/٩/25.

4- علي عدنان الفيل، الإجرام الإلكتروني، ط1، منشورات زين الحقوقية، بيروت، 2011.

5- حسن تركي عمير، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى، بغداد، 2013.

6- عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد في المدة 2-4 يونيو 2008.

7- مصطفى محمد موسى، الإرهاب الإلكتروني، ط1، مطابع الشرطة، القاهرة، 2009.

8- سايمون كولن، التجارة على الإنترنت، نقله إلى العربية يحيى مصلح، بيت الأفكار الدولية بأمريكا، 1999.

9- د. سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، الإمارات العربية المتحدة، العدد 91.

10- موزة المزروعي، الاختراقات الإلكترونية خطر كيف تواجهه، مجلة آفاق اقتصادية، الإمارات العربية المتحدة، العدد 9، 2000.

11- د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظار أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومرك تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3.

12- د. عماد علي خليل، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-2000/5/3، ص 4.

13- حذرت شركة مايكروسوفت من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز، وتقول الشركة: إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة

بأنها حرجة، ودعت المستخدمين إلى تركيب ترقيعي لحل المشكلة، جريدة الرياض، العدد (12542)، السبت 1423/8/20 هـ.

14- جريدة الرياض، العدد (12460)، يوم الإثنين 1423/5/26 هـ.

## List of sources


1- Ammar Abbas Al-Hussaini, Computer and Internet Crimes,Zain Legal Publications, Beirut, 2017

2- Rasti Al-Hajj, Terrorism in the Face of Criminal Accountability Locally and Internationally "A Comparative Study", 1st ed., Zain Legal Publications, Beirut, 2012.

3- Abdullah bin Abdulaziz bin Fahd Al-Ajlan, Terrorism Electronic in the information age and available on the website:http://www.shaimaaatalla.com/vb/showthr Date of visit: 9/25/2023

4- Ali Adnan Al-Feel, Electronic Crime, 1st ed., Publications -ead.php?t Zain Legal, Beirut, 2011.

5- Hassan Turki Omair, Electronic Terrorism and its Dangers in the Current Era, Journal of Legal and Political Sciences, Special Issue, College of Law and Political Science, University of Diyala, Baghdad, 2013.

6- Abdullah bin Abdulaziz bin Fahd Al-Ajlan, Electronic Terrorism in the Information Age, a paper presented to the First International Conference on "Protecting Information Security"

7- Mustafa Muhammad -Privacy in Internet Law, held during the period 2- Musa, Electronic Terrorism, 1st ed.Police Press, Cairo, 2009.

8- Simon Colin Online Business, translated into Arabic Yahya Musleh, International Ideas House, America, 1999.

9- Dr. Suhair Hijazi, Criminal Threats to E-Commerce, Research and Studies Center, Dubai Police, United Arab Emirates, Issue 91.

10- Moza Al Mazrouei, Electronic Hacking: How Dangerous Facing it, Economic Horizons Magazine, United Arab Emirates, Issue No. 9, Dr. Mamdouh Abdel Hamid Abdel Muttalib, -=3937 11.June 4, 2008.2000

Crimes of Using the World Wide Web (Cybercrime from a Security Perspective), a paper presented to the Law, Computer and Internet Conference organized by the College of Sharia and Law in cooperation with the Emirates Center for Strategic Studies and Research and the Information Technology Center at the United Arab Emirates University in Period 1-5/3/2000.

-12 Dr. Imad Ali Khalil, Legal Conditioning of MisuseCard numbers over the Internet (a scientific study inLight of the Provisions of the Jordanian Penal Code), a research paper submitted to the Law, Computer and Internet Conference organized by the College of Sharia and Law in cooperation with the Emirates Center for Strategic Studies and Research and the Information Technology Center at the United Arab Emirates University United Arab Emirates, 05/03/2000-15, p. 4.

-13 Microsoft warned of a vulnerability in the help tools in most versions of Windows, and the company says: This vulnerability could allow hackers to control users' computers, while the company classified the vulnerability as critical, and called on users to install a patch to solve the problem, Al-Riyadh newspaper, issue (12542), Saturday 1423/8/20 AH.