# الإرهاب السيبراني كأحـــدث صُـور التّطـــرف المُعاصـــــر في إطـــار إستراتيجية مقترحـــــة للمكافحـــة

د. مُحي الدّين أحمد المدنـــي ـ الأكاديمية الليبية للدّراســـات العليا.
**mohyedein@yahoo.com**
د. عُمر المبروك اسباقة ـ كلية الاقتصاد والعلوم السياسية ـ جامعة بني وليد
**omarasbaga@gmail.com**

**Cyber terrorism as the latest forms of contemporary extremism within the framework of a proposed strategy for combating it**

Summary:
The study looks at the new and emerging technology and evaluates the rapidly absence of the educational aspect by many institutions, extremist takfiri groups claiming adherence to religion have engaged in what is called contemporary terrorism or electronic terrorism, which has become an epidemic whose dangers have escalated and affected the international community. On the other hand, there are innovative methods that have been identified to confront these threats, and to address the most pressing issues today, related to technology, combating terrorism, and limiting the use of artificial intelligence in terrorist operations such as sabotage, piracy, and independent lethal weapons in intercontinental cyberspace with an abundance of effort, time, and money
Keywords: electronic terrorism, cyber security, contemporary extremism, strategy.

## الملخـــــص :

**تنظـــر** الدّراســـة في التكنولوجية الجديدة ، وتقيّـــم التهديد ســـريع التّطور وسوء استخدامه من قبل الإرهابيين للهذه التقنية ، ونتيجة لغياب الجانب التّـــوعوي من قِبل العديد من المؤسسات قامت جماعات متطرفـــة بالإنخراط فيما يســـمّى بالإرهاب المعاصر أو الإرهاب الإلكتروني، والذي أصبح وباء تصاعدت أخطاره وأصاب المجتمع الدّولي بأســـره ، وفي المقابل هناك أساليب مبتكرة تم تحـــديدها لمواجهة هذه التهديدات، ومعالجة القضايا الأكثر إلحاحا اليوم، والمتعلقة بالتكنولوجيا

ومكافحة الإرهاب والحدّ من توظيف الذّكاء الأصطناعي في العمليات الارهابيـــة كالتّخريب والقرصنة والأسلحة الفتّاكة المستقلة في فضاء سيبراني عابر للقارات مع توفـيرللجهد والوقت والمال .

**الكلمات المفتاحيــة :** الارهاب الإلكتروني ، الأمــن السيبراني ، التّطرف المعاصر، الإستراتيجية.

**المُقدّمـــة** :

وضعت ثــورة الذكاء الاصطناعي البشــرية على أعتاب مرحلة تاريخية جديدة؛ لكن الفرص الواعدة التي يحملها هذا الابتكار المدهــش يوازيها ما ينطـوي عليه من مخاطر مُحدقة بالأمن العالمي، ولن تتـــورع التنظيمات المتطرفة في توظيفه لخدمة مشاريعها الخاصة ، ويتضاعف مخاطره ؛ لأنه لا يتطلب خلفية تقنية ومعرفية عالية؛ بل فقط يعتمد على أن يكون للمتطرف خيالا تخريبيًا خصبا وأوامـر سهلة على لوحة المفاتيح ، ولقد كثر في الآونة الأخــيرة تداول العديد من المفاهيم يطلق عليها سلسلة من الجرائم والسلوكيات الإجرامية، والتي هي في الواقع غير محدّدة وغير متفق عليها(1)

إن التزييف العميـق من أكبر المُعضلات التي يطرحها شـيوع تطبيقات الذّكاء الاصطناعي، ويشير المصطلح إلى القدرة المدهشة التي يستطيع من خلالها الذكاء الاصطناعي إنتاج مقاطع مزيفة تمامًا؛ لكنها في الحقيقة لا تبدو كذلك، فتلك العملية التي كانت تحتاج في السابق إلى استديوهات عملاقة وموارد ضخمة باتت الآن لا تحتاج سـوى إلى نقرات بسيطة على لوحة مفاتيح الهاتف أو الكمبيوتر، وبالنسبة للمنظمات الارهابية المتطرفة فإن نشاطها يقوم على التضليل والتلاعب بالحقائق ودمــج أشكال متعددة من المؤثرات الخاصة على موادّها البصرية فإن تطبيقات التزييف العميق يمكن أن تكون مغرية جدًا لها .

لم يمنع الانبهار والإعجاب الذي قوبلت به منتجات الذّكاء الاصطناعي والتطلع إلى آفاقها الواعــدة الخبراء وصنّاع السياسة من دقّ ناقوس الخطر، والتحذير من تداعياتها الخطيرة على الأمن العالمي، وقد وقع أكثر من 3000 مطــوّر وعالم تكنولوجيا مذكرة في مارس الماضي تطالب " بوقف أبحاث تطوير الذكاء الاصطناعي ستة أشهر لإتاحة الفرصة نحو مزيد من الحوكمة لهذا النظام ولضمان عدم تضرر البشرية منه "(2) ، ولا جدال أن الإرهاب أصبح وباءً تصاعدت أخطاره وأصابت المجتمع الدولي بأسره، وقد اجتمعت كافة دول العالم المتحضرة على

محاربته والتصدي له بكل الإجراءات والتدابير المناسبة لدرأ خطورته والتصدي لتصاعده، وتعويض ضحاياه ، وأجمع الباحثون على أن الإرهاب لا يتصف بدين ولا لون ولا جنسية .

وفي ضوء إلتزام المملكة العربية السعودية بواجباتها نحو المجتمع الداخلي والدّولي وإستجابة ووفاء بهذه الإلتزامات، فقد إستخدمت عديد من الأنظمة التي تجسّد هذا الوفاء والتي تنبع من عقيدتها الإصلاحية الراسخة وتستمد جذوره وأصوله من شريعتنا الإسلامية، ولا سيما في ضوء الهجمات الشّرسة التي تصف الإسلام بالإرهاب(3)

وأدّت التّطورات الراهنة خلال السنوات المنصرمة على المستوى السياسي والاقتصادي والاجتماعي سواءً على الصعيد العالمى أو الإقليمى أو على الصعيد الدّاخلي ، إلى تغيرات واسعة فى مفهوم الأمن ووسائل تحقيقه ، فقد اتسع المفهوم بحكم تعقد الأنشطة الإنسانية وتعدّد مصادر تهديد الاستقرار والأمن فى المجتمع الواحد؛ بل وارتباط أمن المجتمع بغيره من المجتمعات المجاورة والأوضاع المُتصاعدة فى المجتمع الدّولى والتّطورات التكنولوجية المتلاحقة.

ونظرًا لهذا الاتساع فى المفهوم، فلم تعد مهمة تحقيقه مسؤولية جهة أو مؤسسة ما داخل المجتمع؛ بل أضحت مسؤولية مؤسسات متعددة تتظافر جهودها بشكل متواصل، مع الأخذ فى الحسبان أن هذا التداخل الذى فرضته التطورات الأخيرة فى مفهوم الأمن لا يعنى أن تقف المؤسسات الأمنية على قدم المساواة مع غيرها مع مؤسسات المجتمع الأخرى فى تعاملها أو نظرتها للأمن بمفهومه الشامل ، بل تظل المؤسسة الأمنية هى الأكثر تأثرًا بأي محاولة لنشر أفكار متطرفة أو إرهابية ، والتي تكون لها آثارها السلبية على استقرار المجتمع أو المساس بأمنه ، كما تظل - أيضًا - حجر الزّاوية فى الربط والتنسيق بين مختلف المؤسسات التى تؤثر وظائفها فى أمن المجتمع وفق المفهوم الشامل له، دون أن يعنى ذلك احتكار المؤسسات الأمنية وحدها مهمة تحقيق الأمن وفق هذا المنظور(4)

ومن ثَـمّ تسعى الدّراسة إلى تحديد وتقييم التهديد سريع التّطور من جراء سوء استخدام الإرهابين للهذه التقنية والتكنولوجية الجديدة والناشئة وإلى إستخلاص نتائج الجهود الحالية في مواجهة الإرهاب والتطرف الفكري عبر الشبكات الإجتماعية وتقييمها وتحديثها ، حتى تؤدى بدورها إلى تحقيق قدر كبير من الاستقرار الذي

ينعكس أثره على الأمن الوطني، وكذلك وضع إستراتيجية لمكافحة الأفكار المتطرفة التى تُبث عبر شبكات الفضاء السيبراني ؟

## إشكالية الدراســـة:

إن سوء استخدام التقنيات الحديثة والمتطورة جدّا من قبل الارهابيين سيعزز حملات التّضليل الرقمي وسيساعدهم على تصنيع وإنشاء وتخصيص صفحات الويب الضارة وعمليات الاحتيال التي تعتمد على الهندسة الاجتماعية.

وبالتالي يمكن صياغة مشكلة الدراسة على هيئة تساؤل رئيس :

ماهي أحدث صور الإرهاب والتطرف وكيف يمكن صياغة إستراتيجية مقترحة لمكافحة الأفكار المتطرفة التى تبث عبر الفضاء السيبراني ؟

## أسئلة الدراسة :

1- ما تعريف الإرهاب الإلكتروني؟ وما صور ابعاده التقليدية والحديثة؟

2- كيف يمكن صياغة مفهوم الأمن السيبراني في ضوء تباين المصالح المجتمعية المعنية بالتجريم؟

3- ما مدى إستثمار الشبكات الإجتماعية في التصدي لترويج الإرهاب؟

4- ما هو التصور المقترح لإستراتيجية أكثر فعالية لمكافحة الأفكار المتطرفة عبر الفضاء السيبراني ؟

## أهداف الدراسة :

1- التعرف على مفهوم الإرهاب السيبراني و صوره المختلفة .

3- تفعيل وتحديث وتقويـم الأمن السيبراني للتصدي للارهاب الالكتروني بجميع صـــوره .

4- وضع إستراتيجية أكثر فعالية عبر الشبكات الإلكترونيــة من خلال الإستناد على أسس وركائز محددة مثل التشريعات المقترحة والتعاون التشريعي على المستوى العربي والدّولي، إلى جانب آليات مقترحة للمواجهة.

## أهمية الدراسة :

يمكن إبراز أهمية الدراسة الحالية على النحو التالـــي :

**أولاً ـ الأهمية النظرية:**

نظـــرًا لحداثة موضوع الدراسة على المستوى العربي؛ إذ يجـد الباحث ندرة في الكتابات الاكاديمية العربية التي سعت للخوض في هذا الموضوع. ونحاول إبراز الدور الدولي في التصدي لمكافحة الإرهاب عبر الشبكات الإجتماعية ،كأحدث صور

الجرائم الحديثة، وتسعى الدراسة لاستكشاف ورصد ظاهرة الإرهاب الفكري في طوره الحديث وتحديد معالمها والجهود المبذولة لمكافحته محليا و إقليميا ودوليا.

**ثانيا ـ الأهمية العملية:**

تســعى الدراسة إلى إستخلاص نتائج الجــهود الحالية في مواجهة الإرهاب والتطرف الفكري عبر الشبكات الإجتماعية وتقييمها وتحديثها حتى تؤدى بدورها إلى تحقيق قدر كبير من الاستقرار ينعكس آثره على الأمن الوطني، كما تتطلع هذه الدراسة إلى زيادة فاعلية دور الشبكات الإجتماعية في رصد موجات ترويج الإرهاب والتطرف الفكري من خلال تخطيط علمي ملموس يناسب واقع ينتظم في قواعد ومعاييرالأمن القانوني ويرقى إلى مستوى الطموحات المحلية والعالمية .هذا إلى جانب تحديث آليات مواجهة التطرف الفكري وترويج الإرهاب عبر الشبكات الإجتماعية من خلال إستثمار معطيات العلوم والتكنولوجيا المعاصرة .

## منهج الدراسة :

يتم تطبيق المنهج الوصفي الاستقرائي، وذلك من خلال استجلاء أسباب وصور الإرهاب الإلكتروني الصامت من خلال دراسة وتحليل بعض التشريعات التي تتناول العقوبات المتعلقة بجريمة نشر الأفكار الإرهابية والمتطرفة عبر الشبكات الإجتماعية، وسبل ردعها.

## المطلب الأول ـ الإرهاب االسيبراني وصوره وأنماطه التقليدية والحديثة

لقد أفـرز مفهوم الارهاب الإلكتروني ظهور حشد كبير من المفردات الاصطلاحية التي تُسهم بالقاء الضوء على المساحة التي تمتد اليها تأثيراته ،كما تعد دليلا يمكن الاسترشاد به للتعامل الصحيح مع ما تطرحه هذه الظاهرة على ارض الواقع من تداعيات جديدة، ويشمل الارهاب الإلكتروني الهجمات المعلوماتية التي تستهدف مكونات البنية التحتية المهمة مثل : محطات توليد الطاقة الكهربائية أو خدمات الطوارئ(5)

**أولاً ـ ماهيـــــة الإرهاب السيبراني :** لقد ذهب مركز حماية البنى التحتية الوطنية الأمريكي ( NIPC) إلى عدّ الارهاب المعلوماتي عبارة عن دافع إجرامي يمارس بواسطة الحاسوب أو أدواته فيقضي إلى نشـر العنف والموت أو التدمير مع اثارة الهلع والارهاب لاكراه حكومة او نظام سياسي على تغيير سياسته(6)

وقد عمد أحد الباحثين إلى إعادة صياغة تعريف الارهاب المعلوماتي ، وهو : " عبارة عن استخدام المحرض سياسيا للحاسوب بوصفه سلاحا ، أو هدفا بواسطة

مجاميع أو عملاء تهدف إلى اثارة الرعب ونشره للتأثير في أفراد المجتمع أو أكراه الحكومة على تغيير سياسيتها الوطنية لصالح أهداف هذه المجاميع. ، وأما الإرهاب الالكتروني فلا يختلف عما ذكرنا بمتغير واحد هو استعمال واستغلال الوسائل تكنولوجيا الإعلام و اتصال بغرض تهديد و ترهيب الأفراد، وقد أصدر مجمع الفقه الإسلامي الدولي قرارًا في دورته الرابعة عشرة المعقودة في الدوحة في شهر ذي القعدة من عام 1423هـ ذكر فيه تعريف مصطلح الإرهاب بأنه : العدوان أو التخويف أو التهديد ماديًا أو معنويًا 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 [7]

من هذه التعاريف نتوصل إلى أن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد ماديًا أو معنويًا 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.

وهناك كثير من العوامل التي تجعل من ظاهرة الارهاب عبر الشبكات الإجتماعية موضوعا شيقا وسلاحا مناسبا يمتلك مجموعة من المميزات الفريدة التي تجعل منه موضوعا يستأثر باهتمام الكثير من الفئات الارهابية المنتشرة على عموم رقعة البسيطة وتشمل هذه المميزات ما يأتي :

1-قابلية الاختراق (Vulner ability) :تحتوي نظم المعلومات على ثغرات معلوماتية موجودة في معماريتها وتوفر هذه الثغرات للارهابيين اكثر من فرصة مناسبة لاستغلالها في التسلل للبنى التحتية ، وممارسة عمليات تخريبية بمستويات مختلفة .

2-غياب الحدود (A nonymity) : ان غياب الحدود المكانية عن الفضاء المعلوماتي وعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعد ميزة مهمة تستأثر باهتمام الفئات الارهابية التي تسعى الى تغيب هويتها بعيدا عن انظار السلطة والمجتمع .

3-توسيع رقعة الاهتمام : ان السمة العولمية لشبكات المعلومات توفر للارهاب المعلوماتي فرصة ثمينة للاعلان عن انشطتها والظفر باهتمامات متزايدة على رقعة عولمية واسعة تتجاوز حدود السلطة او المجتمع الذي تقيم فيه ما يزيد من قدرتها التأثيريه بشكل ملموس .

4-السهولة وتدني الكلفة : ان توافر الادوات المعلوماتية على شبكة الانترنيت وقيام قراصنة المعلومات بفك الشفرات البرمجية يوفر عددا ضخما من النظم والبرمجة والوسائل التي يمكن للارهابيين استغلالها في توجيه ضربات موجعة لخصومهم بسهولة ، ومن دون الحاجة الى مصادر تمويل ضخمة .

5-غياب العنصر المادي للمخاطرة : ان قدرة قراصنة المعلومات على ممارسة الانشطة الارهابية من دون الحاجة الى الاحتكاك بخصومهم او تعريض النفس لمخاطر مباشرة يزيد من الاهتمام بهذا الجانب من عمليات الارهاب .

ان هذه العوامل باتت تشكل بيئة خصبة لنمو تيار الارهاب المعلوماتي في مجتمعنا المعاصر بوصفه بديلا مناسبا للارهاب التقليدي(8)

**ثانيا ـ دور شبكة الانترنت في الإرهاب الإلكتروني :**

يمكن تحديد أبرز الطرق لإستخدام شبكة الإنترنت في الإرهاب الإلكتروني كما يلي(9)

**1-تبادل المعلومات :** في الواقع الملموس يصعب على المنظمات العاملة في حقل الإرهاب الاجتماع في نقطة مكانية و زمنية محددة نظرا للرقابة الأمنية المشددة، لكن بفضل الطرق المعلومات السريعة أصبح الأمر ميسورا؛ إذ يمكن من خلال غرف الدردشة والمنتديات جمع في وقت محدد عدد من أشخاص في أماكن جغرافية متفرقة ، للتشاور وتبادل المعطيات و الاستراتجيات، فضلا عن البريد الإلكتروني الذي يسمح من جهة بنقل الملفات و المعلومات بسرعة مذهلة و آمنة ومن ناحية أخرى بنشر الأفكار المتطرفة والترويج لها لكسب الدعم و الأتباع.

2- **انعدام الهوية :** توفر الشبكة المعلوماتية لهذه الجماعات عن طريق غرف الدردشة و المنتديات و البريد الإلكتروني (الرسائل المشفرة) مجالا للإخفاء الهوية، إذ يصعب التعرف على من يختفي وراء هذه الشخصيات التي تستفيد من عدم وجود أثار ثابتة للجريمة(10)

3- **الشبكة كنز من المعلومات للإرهاب الإلكتروني:** توفر شبكة الانترنت كنزا من المعلومات الدقيقة و الثمينة يصعب في الواقع الحصول عليها، فهي فرصة للاضطلاع على مواقع المنشآت النووية، ومصادر توليد الطاقة و محطات الكهرباء، وأماكن الاتصالات، ومواعيد الرحلات الجوية الدولية، والمعلومات الخاصة بطرق مكافحة الإرهاب و غيرها من البيانات مدعومة بالصوت والصور. وعن طريق العالم الرقمي تسعى الجماعات الإرهابية إلى كسب تأييد و دعم و تجنيد الأشخاص الراغبين في الانخراط في مثل هذه النشاطات (11)

**4- تعليم كيفية التعامل مع الأنشطة الإرهابيـــة:** لقد سمحت الانترنت للمنظمات الإرهابية الفرصة بفتح مواقع هي بمثابة مقرها المركزي، و ذلك للترويج لمنتجاتها القائمة على نشـــر المبادئ والأيديولوجيات لتجنيد الأفراد المتعاطفين مع مثل هذه الأعمال (12)

**ثالثا ـ آليات استخدام الإنترنت في الإرهاب عبر الشبكات الإجتماعية:**

يمكن تحديد اليات استخدام شبكة الإنترنت في الإرهاب الإلكتروني كما يلي:

1- **استخدام الفيروسات Virus:** هو برنامج صغير اوجد من برنامج ما . يربط نفسه ببرنامج اخر ولكنه يغير عمل ذلك البرنامج كليا او جزئيا لكي يتمكن من التكاثر عن طريقه (13)

**2- حصان طـــروادة Trojan horse :** هي برامج توحي للمستخدم بانها تقوم بعمل معين بينما هي في حقيقة الامر تقوم بعمل اخر ويكون ضارة على الاغلب وتتميز عن الفايروسات بكونها غير قادرة على انتاج نفسها .

**3- القنبلة المنطقية .**Bombard Logical : هي برامج شبيهة الى حد ما بالفايروس ويتم تنشيطها بوقوع حدث او حالة معينة ويمكن أن تكون جـــزءا من برنامج الفايروس Virus او حصان طروادة. ويلجأ ارهابيوا المعلوماتية الى تحميل ملفات مفورسة على الشبكة في بعض المواقع الاكثر زيارة . بعض الملفات المفورسة تنتقل مباشرة عبر الشبكة الى الحاسوب بمجرد فتح الموقع وبعض اخر يكمن للمستخدم في ملفات معينة ما ان يقوم بفتحها حتى ينتقل الفايروس الى حاسوبه(14) .

**4- الرسائل الاقتحامية (Spam) :** بينما تتزايد القدرات العالمية على الاتصال يتزايد قبول افكار وطرق جديدة في العمل والحياة ومنها اعتماد البريد الالكتروني وسيلة اساسية امام وصول رسائل الكترونية غير مرغوب فيها وكمية الرسائل غير المرغوب فيها ( الاقتحامية ) التي ترسل عبر العالم تتزايد كثيرا وقد اشارت بعض الاحصاءات والدراسات الحديثة الى ان تلك الرسائل تخطت نسبة الخمسين في المائة من مجموع الرسائل المتبادلة عالميا(15)

ومن الصعب في الوقت الراهن منع الرسائل الاقتحامية من الوصول . ولكن تتركز الجهود الان على التحقيق من اثار هذه الظاهرة ويجب على المجتمع العالمي التوجه نحو الوقاية بدلا من العلاج(16)، وقضية الرسائل الاقتحامية وصلت الى مفترق طرق ففي حين تقوم بعض الدول بتصنيف المرسل على انه خارج عن القانون . يلحظ غياب

التشريعات في بعض البلدان الاخرى نتيجة لكونها في بداية الطريق الى سن القوانين والتشريعات المتعلقة بالتكنولوجيا(17)

**رابعا ـ سوء إستخدام شبكات التواصل الإجتماعي وأبعادها المعاصرة :**

لقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضرارًا جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا نزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

**أولا ـ دور إنشاء مواقع الشبكات الإجتماعية في الإرهاب الإلكتروني :**

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت 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، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك (18)

وتسعى الجهات الرسمية، والمؤسسات، والشركات، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الإنترنت في شهر 10/ 2000م إلى أكثر من 22مليون موقع. (19)

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام، وتبادل الآراء والأفكار والمعلومات صعبا في الواقع فإن الإنترنت تسهل هذه العملية كثيرًا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، ويتبادلوا الحديث والاستماع لبعضهم عبر الإنترنت، بل يمكن أن يجمعوا لهم أتباعًا وأنصارًا عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الإنترنت، ومنتديات الحوار، وما يسمى بغرف الدردشة، فإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين غدا سهلًا ممكنًا، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمنوا انتشارًا أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها.

**ثانيا ـ تدمير المواقع على شبكات التواصل الاجتماعي :**

يستطيع قراصنة الحاسب الآلي (Hackers) التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي يصحبه تقدم أعظم في الجريمة المعلوماتية وسبل ارتكابها، ولا سيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي [20].

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي [21]

يمكن لمزود خدمات الإنترنت (ISP) من الناحية النظرية أن يكتشف كل أفعال مستخدم الإنترنت عندما يتصل بالشبكة، ويشمل ذلك: عناوين المواقع التي زارها، ومتى كان ذلك، والصفحات التي اطلع عليها، والملفات التي جلبها، والكلمات التي بحث عنها، والحوارات التي شارك فيها، والبريد الإلكتروني الذي أرسله أو استقبله، وفواتير الشراء للسلع التي طلب شراءها، والخدمات التي شارك فيها، لكن تختلف من الناحية الفعلية كمية المعلومات التي يجمعها مزود خدمات الإنترنت عن مستخدم الشبكة باختلاف التقنيات والبرمجيات التي يستخدمها، فإذا لم يكن مزود الخدمة يستخدم مزودات (بروكسي) تتسلم وتنظم كل الطلبات، ويستخدم برامج تحسس الرقم الخاص (IP) التي تحلل حركة المرور بتفصيل كبير، فقد لا يسجل سوى البيانات الشخصية للمستخدم، وتأريخ وزمن الاتصال والانفصال عن الشبكة، وبعض البيانات الأخرى، إن معرفة البيانات التفصيلية للمستخدم تجعل الإقدام على الاعتداء الإلكتروني أقل، وذلك لأن بعض الذين يحصل منهم الاعتداء الإلكتروني يتم منهم ذلك بسبب ظنهم أن بياناتهم التفصيلية لا يمكن الاطلاع عليها، فيظن أنه بمجرد دخوله على الشبكة باسم وهمي تصبح بياناته غير معلومة، وهذا خطأ [22]

إن من الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية (mails-e) من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطًا 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 ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه (23)

## المطلب الثاني ـ إستخدام الفضاء السيبراني وأبعاده المعاصرة على المستويين الوطني والدولي:

يمكن القـول أن البشــرية شهدت عبر القرون الماضية ثورتين غيرتا وجه التاريخ وطبيعة الحياة وهما الثورة الزراعية والثورة الصناعية ، لذا من المؤكد اليوم أن العالم يعيش الثورة الثالثة وهى ثورة تكنولوجيا المعلومات ، وهذه الثورة الجديدة أساسها المعلومات والمعرفة التى أصبحت أساساً للتنمية وزيادة الإنتاج وسرعة اتخاذ القرار الصحيح ، ولكن هذه الثورة الثالثة لم يتم استخدامها فى أعمال الخير فحسب، بل تم توجيهها- أيضاً - للقيام بإعمال الشر، حيث استخدمها الإرهابيون فى القيام بالإعمال الإرهابية سواء فى العالم العربى أومختلف دول العالم(24) ، كما أضحت تلك الوسائل الأداة الأهم فى يد الجماعات المسلحة لنشر أفكارها ومعتقداتها ووضع خططها وتنفيذ أهدافها وتجنيد أعضائها، حيث استخدمت هذه الجماعات مواقع التواصل المتعددة سواء أكانت( فيسبوك ، توتير ، يوتيوب ، واتس أب ، الإنستجرام ) فى تجنيد العديد من الشباب(25)

**أولا ـ الإستخدام الإرهابي لشبكات التواصل الإجتماعي :**

لاشك أن لمواقع التواصل الاجتماعي دور كبير في ربط عدد هائل من أفراد المجتمعات فى كافة بلدان العالم ، مما أدى إلى استخدام الحكومات فى معظم بلدان العالم لهذه الشبكات ، لكى تستطيع أن تصل لفئات الشعب المختلفة ، إضافة إلي دور بعض المواقع التى لها تأثير كبير فى المجتمعات العربية والأجنبية ، ومنها موقع الفيسبوك Facebook " الذي كان له دوراً كبيرا فى حدوث كثير من الثورات فى العالم العربى ، والتى تعرف بثورات الربيع العربى ، وايضاً موقع التدوين المصغر تويترTwitter الذى لعب دوراً هاماً من خلال تغريداته أن يؤثر على الرأى العام ، ومن خلاله نستطيع أن نعرف آراء العديد من الأفراد حول قضايا معينة ، وايضاً موقع اليوتيوب "You Tube " الذى لعب هو الآخر دوراً مؤثراً ولكن بطريقة مختلفة ، وذلك من خلال نشر ما يحدث حول العالم ولكن من خلال الفيديوهات المختلفة ، التى أثارت جدل العديد من الأفراد فى كثير من الأوقات(26).

ومن هنا ظهر مفهوم الإرهاب الحديث وهو الإرهاب الذي ارتبط بوسائل التكنولوجيا الحديثة والذي عرف بالإرهاب عبر الإنترنت أو بمعني أصح الإرهاب الإلكتروني، وقد ظهر هذا المفهوم مع استخدام الجماعات الإرهابية للإنترنت ولوسائل التواصل الحديثة وخاصة مواقع التواصل الإجتماعي وذلك من خلال إنشاء صفحات لهم علي هذه المواقع وتواصلهم مع الفئات المختلفة ونجاحهم في تجنيد العديد من الشباب ، بالإضافة إلي نجاحهم في الحصول علي الأموال التي يريدوها ، وكان من أبرز هذه التنظيمات ( تنظيم داعش) ، الذي نجح بالفعل من خلال استراتيجته الإعلامية والإلكترونية أن يؤسس لنفسه قاعدة أساسية علي مواقع التواصل الإجتماعي ، ربما أكثر من تنظيم القاعدة ، الذي انشق منه تنظيم داعش(27).

ومع نمو شبكة الإنترنت بشكل واسع فى جميع أنحاء العالم ، ظهرت العديد من التغيرات والتطورات ، فقد كان لظهور الإنترنت جانبين أحداهما إيجابى وذلك من خلال سرعة اتصال العالم ببعضه البعض واستخدام الحكومات له ، والآخر سلبي حيث أستخدمته الجماعات الإرهابية لكى تنشر أخبارها وأعمالها الإرهابية ومحاولتها لجذب الأفراد إليها ، وأصبح ظهور الإنترنت مرتبط بالعديد من التهديدات التى شهدها العالم من خلال العديد من الجماعات الإرهابية ، ومنها على سبيل المثال تنظيم " داعش ، والعديد من التنظيمات الإرهابية ، وذلك أدى إلى ظهور ما مصطلح " الإرهاب الإلكترونى (28)

وقد كانت بداية استخدام هذه الكلمة "cyber terrorism " أو " electronic terrorism" فى فترة الثمانيات فى دراسة : (بارى كولن) ، والتى أشار فيها إلى صعوبة تعريف ظاهرة الإرهاب الإلكتروني بدقة، ناهيك عن الأساليب والحلول المطلوبة لمواجهته وكذلك تحديد دور أجهزة الحاسب الآلي والإنترنت فى العمل الإرهابي (29)، كما أن الإرهاب الإلكتروني يتكون من عالمين : العالم المادي والعالم الافتراضي والذي من خلالهم تتم عمليات الإرهاب الإلكتروني والتدمير والتخريب ، حيث يشير العالم المادي إلى قضايا وظواهر متعددة مثل : الطاقة والضوء والظلام والبرودة والحرارة وجميع الأمور المادية، ويمارس الوظائف والأدوار من خلاله ، أماالعالم الافتراضي فيشير إلى التمثيل الرمزي والمجازي للمعلومات وهوالمكان الذي تعمل به البرامج والأنظمة الإلكترونية وتتنقل فيه البيانات(30)

يعرفه مركز حماية البنية التحتية القومية الأمريكية بإنه: عمل إجرامى يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية ينتج عنه تدمير

أو تعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان ، وذلك بهدف التأثير على السكان لخدمة أجندة سياسية أو اجتماعية أو أيديولوجية " (31)

من خلال ماسبق يمكن القول أن أغلبية التعريفات اتفقت عن كونه شكل من أشكال الإرهاب الذي تمارسه الدول أو الجماعات أو الأفراد من خلال استخدام تقنية المعلومات كسلاح أو بهدف تحقيق تخويف وتهديد سواء أكان مادي أو معنوي ، وذلك علي الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق ، فالإرهاب الإلكتروني يعتمد علي استخدام الإمكانيات العلمية والتقنية ، واستغلال وسائل الاتصال والشبكات المعلوماتية ، وذلك من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديده(32)

ولقد أدّى التزايد المستمر في استخدام شبكة الإنترنت ، فضلاً عن اتساع حجم الشبكة ذاتها وسهولة الدخول إليها وما تتسم به من طبيعة سرية تغلب علي المعلومات التي تتم من خلالها إلي أن أصبحت مسرحاً لكثير من الأفعال غير المشروعة ، والتي أطلق عليها جرائم الإنترنت أو الجرائم الإلكترونية (33) ، و- أيضاً - يمكن تعريفها بأنها ": الجرائم التي ترتكب عبر استخدام شبكة الإنترنت ، وهي تختلف في أنماطها وترتكب ضد مجموعة أو أفراد لإحداث الضرر بمن ارتكبت ضده عمداً" ، وتشتمل هذه الجريمة علي العديد من الأفعال ، مثل : الاحتيال المالي والابتزاز ، القرصنة ، انتهاك حقوق التأليف ، وخصوصية الآخرين عند استخدام معلومات تخصهم بشكل غير قانوني ، ولا تقتصر الجرائم الالكترونية علي الأفراد بل تمتد إلي المؤسسات ؛ بل والدول - أيضاً - ، و بعض هذه الجرائم قد تهدد أمن وسلامة الدول(34).

إن الإرهاب الإلكتروني يهدف إلي تحقيق مجموعة من الأهداف غير المشـــروعة ، ومنها تحقيق تواصل تنظيمي آمن لبعض عناصر التنظيمات الإرهابية ، وإثبات تواجدهم علي الساحة من خلال بث العديد من مواقع ومنتديات الحوار الإرهابية واتخاذها كأبواب دعائية لهم ، والتهديد والترويع من خلال بث بعض المواد الإعلامية ، وذلك من خلال الدعاية والإعلان و جذب انتباه الرأى العام ، وذلك لإبراز قوة هذه التنظيمات وترويع أي من المتعاونين مع الأجهزة الأمنية، وايضاً جمع الأموال والإستيلاء عليها بطرق غير مشروعة وذلك في إطار تمويل عملياتهم الإرهابية ، والإخلال بالأمن المعلوماتي وزعزعة الطمأنينة ، وتدمير البني المعلوماتية التحتية وتدميرها ، والإضرار بوسائل الاتصالات وتقنية المعلومات ، أو بالأموال والمنشآت العامة والخاصة(35)

**ثانيا ــ استخدام بعض الجماعات الإرهابيـــة لشبكات التواصـــل الإجتماعـــي :**
قد يســـعى الإرهابيون للحصول علي معلومات استخباراتية عن أحد الخصوم ، أو لجمع معلومات يحظر اطلاع الجمهور عليها ، وذلك للسلامة الوطنية ، وذلك من خلال أجهزة حاسب آلي معينة ، وكذلك يمكن أن يقوم أعضاء التنظيمات الإرهابية بإرسال واستقبال الرسائل فيما بينهم وذلك يكون من خلال إخفاء محتوياتها ، ويتم ذلك في أحوال كثيرة من خلال التشفير أو إخفائها بين الصور، إضافة إلى سعيهم تجنيد أعضاء جدد، وتعد المدن الأوروبية مأوي لكثير من الشباب المنضمين لهذه التنظيمات ، مما يسهل من عملية استقطاب بعضهم للانضمام للميليشيات المسلحة ، وايضاً قد تستخدم هذه التنظيمات الإنترنت لأغراض تعليمية لتدريس فنيات وأساليب تنفيذ الهجمات الإرهابية(36)

من خلال ما سبق يتضح أننا لابد أن نعي أننا أمام إرهاب إلكتروني بمعني أننا أمام مجتمع افتراضي تحكمه ديمقراطية وحرية وفوضى بلا حدود ولا قيود ،حيث يساعد التنظيمات الإرهابية على بناء علاقات بين أعضائه في الفضاء الخارجي بعيداً عن المراقبة الأمنية، ويستفيد من ذلك أعداد هائلة من المشاركين من مختلف الجنسيات واللغات مما يمكن لهذه التنظيمات أن تجند بعضهم وأن تكسب تعاطف بعضهم الآخر(37) ، وتقوم العلاقات بين الأفراد في التنظيم الإرهابي الإلكتروني على النمط الشبكي الأفقي الذي يتساوى أفراده في الحقوق والواجبات فلا يملك أحدهم السلطة على الآخر فهو مجتمع بلا قوانين ملزمة لسلوك الأفراد ويستطيعون الدخول والخروج من هذه الشبكة متى يشاؤون ، حيث أن العلاقات داخل التنظيم الإرهابي الإلكتروني قائمة على الهيكل الأفقي و على مبدأ المرونة والتنسيق والدعم والتخطيط الاستراتيجي والفكري دون إملاء للقرارات التكتيكية ، وهذا المنطق يجعلها أكثر قدرة على تجنب الضربات الأمنية.

وقد أصبحت ظاهرة انضمام أشخاص ولدوا أو نشئوا منذ الصغر فى مجتمعات غربية إلى تنظيم (داعش) تثير اهتمام الحكومات الغربية ومراكز الأبحاث على حد سواء ، وقد أجريت العديد من الدراسات حول الخلفيات الاجتماعية والنفسية لبعض المقاتلين الأجانب المنضمين لهذا التنظيم ، وقد توصلت فى مجملها إلى وجود تباينات وفروق فردية بينهم، وأنه لا يوجد تفسير واحد أو نمط مشترك يمكن تعميمه على الجميع ، وقد كشفت هذه الدراسات عن أن العديد من الخصائص الاجتماعية والنفسية التى كان ينظر إليها كتفسير للتطرف ، مثل الفقر أو نقص التعليم ، لم تعد صالحة بعد

أن اتضح أن كثيرا ممن ينتمون من الطبقات المتوسطة وذوي مستويات التعليم المرتفعة قد انضموا إلى هذه التنظيمات (38)

وتشكّل الظروف السياسية والاقتصادية عاملاً مهماً فى عملية تجنيد الأعضاء فى تنظيم (داعش) ، حيث أن السياسيات العدائية للولايات المتحدة و سياسة المحاصصة الطائفية والصراع الطائفي والمذهبي فى العراق ، كلها أمور تغذي صناعة الكراهية والعداء ضمن النسيج الاجتماعي العراقي ، لذا شكلت هذه الأمور حجر الأساس فى خطاب تنظيم داعش ومن قبله تنظيم القاعدة ، والحركات السلفية الجهادية ، وذلك فى العراق بصفة خاصة ومجتمعات المنطقة العربية بصورة عامة ، إضافة إلي الظروف الاقتصادية والاجتماعية الآخري كالفقر والبطالة والجهل(39)

ويعد تنظيم (داعش) التنظيم الأكثر جذباً للمقاتلين سواء الأجانب أو العرب ، لكن أسباب انضمامهم تتباين، ويمكن بشكل عام إجمال أهم الدوافع التى تدفعهم للسفر والقتال فى صفوفه ، وهذه الدوافع قد تتمثل في الآتي :

**دوافـــع معنويـــة :** يتمتع الغالبية العظمي من المجاهدين الأوروبين بمستويات معيشية متوسطة أو مرتفعة ، فى مجتمعات توصف بالديمقراطية والاستقرار السياسي ، ولذلك فإن سفرهم للجهاد فى سوريا يرتبط بمجموعة مختلفة من العوامل ، من بينها : الملل ، والبحث عن الإثارة والمغامرة ، والبحث عن الشهرة وأدوار البطولة فى تنظيم يعمل بعقول شبابية لديها فرص القيادة والسيطرة ، ولكن الدافع المرتبط بفكرة الجهاد فى سبيل نصرة الدين الإسلامي هو الأقل تأثيراً فيما يخص المقاتلين الأجانب غير العرب ، حيث أن 1% فقط منهم على علم بالعقيدة الإسلامية ، بل إنهم يسافرون فى الغالب بحثاً عن المغامرة والإثارة (40)

**دوافـــع إنسانيـــة :** يبدو البُعد الإنساني أكثر وضوحاً لدى من سافروا فى بداية الحرب فى سوريا للمساعدة والقتال إلى جانب الشعب السوري استجابة لمواقف الدول والحكومات الغربية فى ذلك الحين والتى كانت تندد بنظام الأسد وتدعو العالم ضمنياً لمناهضة ممارسته ، يتم استقطابهم وينضموا للقتال فى صفوف الجماعات المتطرفة ، علي سبيل المثال ( إبراهيم المزواجي ) البريطاني الجنسية والشهير بلقب (أبو الفداء) بعد أن توجه إلى سوريا فى بداية الحرب ليقتال فى صفوف المعارضة ضد الحكومة السورية لينتهي به المطاف عضواً فى أحد الجماعات المتطرفة (41)

وفي ضوء ما سبق يمكن التأكيد أن الجهاد الإلكترونى يقوم بالدور الأكبر في إرهاب الذئاب المنفردة والإرهاب العشوائى وذلك عن طريق مواقع التواصل تحديدًا

، حيث تقوم التنظيمات الإرهابية بتكوين ما يمكن أن نطلق عليه"خلية التجنيد" والتي مهمتها إغراء المستهدفين بفكرة الخلافة، ويغير عناصرها دائمًا محل إقامتهم ، وذلك للهروب بعيدا عن أعين الأمن ، ويعتمد عناصر خلية التجنيد على شفرة معينة خلال حديثهم، وكل كلمة لها مدلول مختلف لاختيار المجندين الجدد في التنظيمات المسلحة، بعيدًا عن الخطوات التقليدية القديمة التي كانت تعتمد على المساجد(42)

وتبدأ مراحل التجنيد بمحاولة جذب الهدف بعد معرفة حالته النفسية ويتم خلال هذه المرحلة التركيز على مسائل : التوحيد والحاكمية والولاء والبراء وأهمية الحكم بالقرآن والتأكيد أن الجهاد هو الحل ، و يلى ذلك زرع الأفكار التكفيرية والمتطرف في عقل الشاب المستهدف، ثم دفعه إلى الاستماع إلى كل ما يجعله حزينًا عبر الاستعانة بالخطب الصوتية الحزينة على يوتيوب والاستماع للأناشيد الحماسية، ثم يتم له ما يمكن أن نسميه " التنويم المغناطيسى "، وذلك اعتمادًا على فكرة أن الإسلام الموجود في المجتمـــع هو إسلام بعيد عن الحقيقـــي ، وهذا ما يفعله تنظيم (داعش ) عند تجنيد العديد من الأفراد (43) .

## المطلب الثالث ـ آليات وإسترتيجية مكافحة الإرهاب عبر الأمن السيبراني:

كل الاستخدامات السابقة قد لا تعني ارهاب سيبراني ؛ لأنهم ببساطة يستخدمون الانترنت كوسيلة لبلوغ هدفهم لتنفيذ أعمالهم الارهابية على أرض الواقع ، فالإنترنت هنا مجرد وسيلة ففي حين تكشف تهديدات تنظيـــم (داعش) بجمعها ما بين أنشـطة إلكترونية وقرصنة تخريبية وأخرى عسكرية، ببزوغ عهد جديد يخلط ما بين المفاهيم المختلفة للجرائم والعمليات التخريبية والإرهاب ، فالقراصنة الذين لم تكن لهم توجهات سياسية من قبل أصبحوا جزءاً من المنظومة المتطرفة التي احتضنتهم وشجعتهم على التمادي في هجماتهم. فعلى سبيل المثال، ظهر إلى الملأ جيش الخلافة الإلكتروني مرتبطاً بتنظيم داعش ليقوم بالتهديد من خلال بث مرئي ظهر إلكترونياً باللغة العربية: « نحن قراصنة (داعش) سنواجهكم عبر حرب إلكترونية هائلة». ووصف المواجهة بـ« الأيام السوداء التي ستتذكرونها» والتي ستفسر عملياً من خلال عمليات تم وصفها: « سنخترق مواقع الحكومات والوزارات العسكرية والشركات والمواقع العالمية الحساسية». وكعادة الوسائل الإعلامية للمتطرفين، هناك استمرار في التهويل وتضخيم الأنشطة الإرهابية بغرض التخويف والإبهار.(44)

وبالرغم من الخسائر الناجمة عن جرائم الحاسوب إلا أنها لا تلفت أنظار النشاط الإرهابي المحتمل ما لم تكن الحواسب مرتبطة مع بعضها في شبكة اتصال فهنا تزيد المغريات أمام الإرهابي لممارسة جرائمه ومن هذه السمات عدم وضوح الجريمة وصعوبة إثباتها وصعوبة التوصل إلى الجناة وإمكانية حدوثها في زمن قصير الى جانب سهولة امتصاص الغرض لارتكاب هذه الجرائم الوقت الحالي.(45)

إن الجريمة المرتكبة بواسطة الانترنت ليست جريمة على النطاق الوطني لكل دولة ؛ وإنما هي جريمة عابرة للدول والقارات كما لا يوجد دليل مادي كالبصمات أو أية آثار للجريمة .(46)، هذا بالإضافة الى صعوبة تحديد هوية مرتكبي جرائم الانترنت واستخدام الانترنت لنشر الفكر الإرهابي والتحريض على التطرف والعنف وحتى أن العديد من الجماعات الإرهابية أنشئت لها صفحات خاصة على الانترنت ويمكن أن ترسل التهديد والوعيد للخصوم.(47)

وفي فجر الثورة الرقمية، في منتصف العقد الماضي، انتبه الغرب إلى قضية الإرهاب الإلكتروني ومخاطره ، حيث قام الرئيس الأمريكي ( بيل كلنتون) في العام 1996م بتشكيل لجنة حماية منشآت البنية التحتية الحساسة . www.nipc.gov وكان أول استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات إضافة شبكات الكمبيوتر إلى ضرورية بشكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة، وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة، بإنشاء هيئاتها ومراكزها الخاصة، للتعامل مع احتمالات الإرهاب الإلكتروني، فقامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفا من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني، وقامت القوات الجوية الأمريكية باتخاذ خطوات مماثلة، ومثلها المباحث الفدرالية، كما تقوم قوات الأمن في أوروبا، وخصوصا الدول التابعة لحلف الأطلسي، باتخاذ إجراءات مماثلة .

وفي سبيل ذلك يمكن التعرض لأبرز التدابير الواجب إتباعها سعيا لمكافحة جرائم الإرهاب الإلكتروني عبر شبكات التواصل الإجتماعي وذلك على النحو التالي:

**أولا ـ التدابير الواجب مباشرتها على المستوى الوطني :**

يمكن تقسيم هذه التدابير إلى نوعين احداهما تدابير موضوعية والأخرى اجرائية . وذلك على النحو التالي :

**1- التدابير الموضوعيـــة:** من الأهمية بمكان مباشرة التدابير الآتية:

**أ.** يجب على كافة الدول أن تتبنى الإجراءات التشريعية وغيرها من التدابير اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء نظام الكمبيوتر كجريمة جنائية وفقا لأحكام قوانينها الوطنية.

**ب-** ينبغي على أن تتبنى التدابير التشريعية وغيرها من التدابير اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية كعمليات نقل الكمبيوتر إلى أو من خلال حاسب آلي آخر وكذا الاشارات الالكترومغناطيسية الصادرة من أحد نظم المعلومات.

**ج-** يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو الاتلاف أوالتعديل أو الإعاقة التي تستهدف بيانات الحاســب الآلي بدون وجه حق .

**د-** يجب على الدول أن تتبنى التدابير التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الكمبيوتر من خلال ادخال أو نقل أو الإضرار أو محو أو اتلاف أو تعديل أو اعاقة بيانات الكمبيوتر وادراكها باعتبارها جريمة جنائية إذا ارتكبت بصفة عمدية .

**هـ -** يجب على الدول أن تتبنى التدابير التشريعية اللازمة لامكانية مساءلة الأشخاص المعنوية جنائيا عن الجرائم الناشئة عن نظم المعلومات وذلك في الأحوال التي يؤدي فيها قصور الاشراف أو الرقابة من قبل الشخص الطبيعية إلى تسهيل ارتكابها.

**2- التدابير الاجرائيـــة:** وتتمثل هذه التدابير على النحو التالي :

**أ-** يجب على الدول أن تتخذ التدابير التشريعية التي تخولها سلطة تفتيش ما يلي:

ـ أحد أنظمة الكمبيوتر أو جزء منه وبيانات الكمبيوتر المختزنة به .

ـ أحد الوسائط التي قد تكون بيانات الكمبيوتر مختزنة به ،وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق .

**ب-** يجب على الدول أو تتخذ التدابير التشريعية اللازمة لتخويل سلطاتها المعنية في اصدار الأمر لأي شخص سواء كان متواجدا في إقليمها في أي مكان آخر عليه سلطاتها السيادية لكي يقدم أي بيانات محددة واقعة تحت سيطرته ومخزنة في أحد أنظمة الكمبيوتر أو أحد الوسائط المستخدمة في تخزين البيانات.

**ج-** يجب على الدول أن تتبنى التدابير التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الكمبيوتر وذلك لأغراض التحقيقات وذلك إذا تبين أنها معرضة بصفة خاصة للفقد والتّعديل .

**ثانيًا ـ التّدابير الواجـــب اتّباعها علـــى المُســـتوى العربي:**

بوجه عام هناك حاجة إلى تحقيق ما يلي على المستوى العربي:

1-وجود التشريعات اللازمة لحماية ملكية الكمبيوتر، وللبيانات،والمعلومات والمعدات اللازمة للتشغيل والتوصيل.

2-زيادة الوعي الوطني في عالمنا العربي لجرائم الكمبيوتر وللعقوبات المترتبة عليها.

3-إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة.

4-إيجاد نوع من التعاون العربي في الحماية والوقاية من هذه الجرائم.

**ثالثا ـ التدابير الواجب مباشرتها على المستوى الدولي :**

يمكن تقسيم هذه التدابير إلى نوعين كما يلي:

**1- تسليم الإرهابي المعلوماتي:** يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب يجب تسليم مرتكبيها.

**2- تفعيل إجراءات التعاون الدولي:** وتتمثل المعونة المتبادلة في الاجراءات التالية :

**أ-** يجب على الدول أن تقدم لبعضها البعض المعونة المتبادل وذلك بأكبر قدر ممكن لاغراض التحقيق والاجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم وبيانات الحاسب الآلي .

**ب-** يجب على الدول أن تقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفيس بوك وتويتر ،بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

**ج-** تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المدعي عليها بموجب اتفاقيات المعونة المتبادلة .

**د-** في الأحوال التي يسمح فيها للطرف المدعي عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة.

**هـ-** تحدد كل دولة سلطة مركزية تنهض بالمسئولين ارسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

**و-** تنفذ طلبات المعونة المتبادلة وفقا للاجراءات التي تحددها الطرف المدعي فيما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المعدي عليه .

## الخاتمـــــة :

تناولنا فى هذا البحث جرائم الإرهاب الإلكتروني عبر شبكات التواصل الإجتماعي فى العالم العربى فى أسلوب مقارن مع الدول الأوروبية والولايات المتحدة الأمريكية، ولاشك أن الجريمة الإلكترونية، ليست حكرا على بعض الدول دون الآخر، إذ أن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتى والذى أكده التطور المستمر فى وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة فى الانتشار فى ربوع الأرض، فليس غريبا أن نجد مجرمى المعلوماتية والإنترنت فى العالم العربى، كما أن الدول الأوربية والولايات المتحدة الأمريكية ظلت لفترة طويلة – وما زالت- مرتعا خصبا للإجرام الإلكترونى بل إن هذه الدول بما حققته من تقدم علمى وتكنولوجى كانت أحد الأسباب الرئيسية لانتشار الجريمة الإلكترونية فى ربوع العالم.

وأمام هذا الانتشار الكبير لهذا النوع من الجرائم اتجهت الدول إلى تضمين أنظمتها القانونية قوانين لمكافحة الجريمة الإلكترونية من أجل إنزال حكم القانون على المجرم المعلوماتى أينما وجد وتوقيع العقاب عليه. فضلا عن اتجاه الكثير من الدول إلى تفعيل مبدأ التعاون الدولى فى مجال مكافحة الجريمة الإلكترونية.

وعلى الرغم من انتشار جرائم الارهاب الالكتروني في عالمنا العربي فى ظل جهود الحكومات العربية، من أجل جذب الاستثمارات في مجال التكنولوجيا إلا ان هناك فراغا تشريعيا في هذا المجال خاصة في قضايا النشر الالكتروني وقوانين جرائم الانترنت الخاصة باقتحام النظم وغيرها، فلا يوجد فى عالمنا العربي نظام قانوني متكامل خاص بجرائم المعلومات، إلا أن القانون يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعا من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكونة لأركان الجريمة المعلوماتية.

وقد أرجع المتخصصون هذا الفراغ من أية عقوبات خاصة بجرائم الانترنت فى التشريع العربى إلى حداثة هذا المجال الذي لم يتعد عمره سنوات قليلة وما يطبق حاليا علي جرائم الانترنت هو القانون التقليدى الذى يتم بموجبه على الجرائم العادية مثل جريمة سرقة، حيث يعاقب مرتكبها بالحبس مدة لاتقل عن 24 ساعة ولاتزيد علي ثلاث سنوات وجريمة النصب التى يعاقب مرتكبها بعقوبة النصب المدرجة في قانون العقوبات.

ويؤكّــد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في السنوات الأخيرة، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب على شبكة الإنترنت دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق هواة الإجرام الإلكتروني، ويحاكمهم أمام محاكم دولية، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب. والمحكمة الالكترونية تتطلب إصدار تشريعات متخصصة فى مجال مكافحة الجريمة الإلكترونية، فضلا عن توفير القضاة المتميزين للقيام على أعمال الفصل فى القضايا المطروحة على هذه المحاكم.

## نتائج الدراســــــــة :

إن من أبرز ما توصلت إليه في البحث الآتي:

**أولًا**: أن التعاملات المرتبطة بتقنية المعلومات كغيرها من مجالات الحياة يجب أن تخضع للتشريعات، وفي ضوء تلك الأحكام تقوم الجهات المعنية بوضع اللوائح المحددة لحقوق والتزامات الأطراف المختلفة، كما تقوم الهيئات القضائية والأمنية والحقوقية بتنزيل تلك الأحكام واللوائح على القضايا المختلفة، وفض النزاعات الناتجة عنها.

**ثانيًا**: أن من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرًا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها.

**ثالثا**: يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع وطرق اختراق حسابات مواقع التواصل الإجتماعي.

**رابعا**: على الرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية والتي تعتبر وسيلة من وسائل مكافحة الإرهاب الإلكتروني، فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام لا يزال في مراحله الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات المنفصلة واللوائح الجزئية التي لا تستوعب القضايا المستجدة في أعمال تقنية المعلومات.

**خامسا:** إن أجهزة الأمن تحتاج إلى كثير من العمل لتطوير قدراتها للتعامل مع جرائم الكمبيوتر والوقاية منها، وتطوير إجراءات الكشف عن الجريمة، خاصة في مسرح الحادث، بحيث تتمكن من تقديم الدليل المقبول للجهات القضائية، وأيضًا يلزم نشر الوعي العام بجرائم الكمبيوتر، والعقوبات المترتبة عليها، واستحداث الأجهزة الأمنية المختصة القادرة على التحقيق في جرائم الكمبيوتر، والتعاون مع الدول الأخرى في الحماية والوقاية من هذه الجرائم.

**سادسا:** على مستوى دول العالم ومع مواكبة التطور الهائل لتقنية المعلومات سنت أنظمة لضبط التعاملات الإلكترونية، وتضمنت تلك الأنظمة عقوبات للمخالفين في التعاملات الإلكترونية ومكافحة الإرهاب الإلكتروني.

## توصيات الدراسة :

1- ضـــرورة تقنين قواعد جديدة لمكافحة الجرائم الإرهابية ؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم ؛ سواء في ذلك الدعاوى الجنائية والمدنية والتأديبية.

2ـ ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم. وضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية .

3ـ ضرورة تخصيص شرطة خاصة لمكافحة الجرائم المعلوماتية ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت. ويتعين تدريب وتحديث رجال الادعاء العام – أو النيابة لعامة – والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت .

4ـ ينبغي أن تنص التشريعات العربية على اعتبار أن الانترنت يعتبر وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بالجرائم المعلوماتية.

5- يلزم تعديل قوانين ونظم الإجراءات الجزائية ( الجنائية ) ؛ بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته .

6- ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل ؛ والكشف عن الحقيقة . ويلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب ألي أخر؛ يمكن ان تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات. ويشترط في هذه الحالة أن

يكون هذا الإجراء ضروريا، والقاعدة العامة – في هذا الشأن – الضرورة تقدر بقدرها .

7- ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني – بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات ؛ طالما أن ضبط هذه الأدلة جاء وليدة إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير؛ وبما يحقق مبدأ المواجهة بين الخصوم .

8- يتعين النص صراحة على تجريم الدخول غير المصرح به على البريد الإلكتروني لإتلاف محتوياته أو إرسال صور إباحية أو تغيير محتواه أو إعاقة الرسائل أو تحويرها عبر الانترنت.

9ـ ضرورة سن التشريعات لمكافحة جرائم الإرهاب الإلكتروني وذلك بإدخال كافة صور السلوك الضار والخطر على المجتمع التي يستخدم فيها انترنت . ويتعين اتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم الإرهابية الإلكترونية.

## الهوامـــــــــش :

[1] البداينة، ذياب (2000) تكوين الاتجاه والمعتقد والرأى العام: بعض التطبيقات الامنية فى تكوين رأى عام واق من الجريمة، الرياض، اكاديمية نايف العربية للعلوم الامنية،ص. ص.10-11

2ـالذكاء-الاصطناعي-يمكن-يتحول-سلاح-بيد-الارهاب

https://www.radiosawa.com/features/2023/06/23

[3] العبيدان، عبد الهادي (2012) الإرهاب في المملكة العربية السعودية، رسالة ماجستير غير منشورة، القاهرة، جامعة القاهرة، كلية الإقتصاد والعلوم السياسية،ص. 13

[4] اسماعيل، محمد صادق (2013)جرائم شبكات التواصل الإجتماعي والإنترنت، المنامة، مركز معلومات المرأة والطفل، ص. 9

[5] الجهني، علي بن فايز (2000) "الإعلام الأمني والرقابة والوقاية من الجريمة"، الرياض، أكاديمية نايف العربية للعلوم الأمنية،ص.ص.8-9

[6] الدعجة، هايل ودعان (2010) التحصين الامنى للرأى العام ضد الشائعات: دور مؤسسات المجتمع المدنى فى التوعية الامنية، الرياض، جامعة نايف العربية للعلوم الامنية، الرياض،ص.ص. 9-10

(7) انظر: قرارات وتوصيات الدورة الرابعة عشرة لمجلس مجمع الفقه الإسلامي ، الدوحة - قطر ، 8-13 ذو القعدة 1423هـ.

[8] بيلي، أولجا جوديس (2009)، بيلي كاميرتس، نيكوكاربنتيير، "فهم الإعلام البديل"، ترجمة: علا أحمد إصلاح، القاهرة، مجموعة النيل العربية،ص.ص.8-9

[9] الهيصمي، خديجة احمد (2005)، مفهوم الإرهاب في عالم متغير ، الكويت : مؤسسة التقدم العلمى،ص.ص. 10-11

[10] صادق، عباس مصطفى (2011)، "الإعلام الجديد:دراسة في مداخله النظرية وخصائصه العامة"، البوابة العربية لعلوم الإعلام والاتصال،ص.8

[11] الفتوح، عبد القادر بن عبد الله (2003)، الشائعات من المنظور التقني في عصر المعلومات، في "الشائعات في عصر المعلومات"، أكاديمية نايف العربية للعلوم الامنية، الرياض، ص.ص. 10-11

[12]- رحومه، علي محمد (2007)، الانترنت والمنظومة التكنو-اجتماعية، بيروت، مركز دراسات الوحدة العربية،ص.6

[13]- عسيري، على عبد الله (2004) عسيرى، الآثار الأمنية لاستخدام الشباب للانترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الامنية، الرياض،ص.7

[14]- اللبان، شريف (2008) تكنولوجيا الاتصال. المخاطر والتحديات والتأثيرات الإجتماعية، القاهرة، الهيئة المصرية العامة للكتاب،ص.ص. 7-8

[15]-في تفصيل هذا الجانب يمكن الرجوع إلى:

- محي الدين، محمد مؤنس (2015)، الأشكال الجديدة للإرهاب المعاصر : منشورات كلية الشرطة، الشارقة، الإمارات العربية المتحدة

– محي الدين، محمد مؤنس (2006)، الإرهاب كجريمة من الجرائم ضد الإنسانية في نظام المحكمة الجنائية الدولية، الرياض، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية

16- المطيري، غسان خلف (2008) الإعلام والتكنولوجيا، الكويت، مؤسسة التقدم العلمي،ص.ص.8-9

[17]- الفطافطة، محمود (2011)، علاقة الإعلام الجديد بحرية الرأى والتغيير في فلسطين: الفيسبوك نموذجًا، المركز الفلسطينى للتنمية والحريات الاعلامية (مدى)، فلسطين،ص.ص.11-12

(18) اسايمون، كولن (1999) التجارة على الإنترنت ، ترجمة يحيى مصلح ، بيت الأفكار الدولية بأمريكا، ص26.

(19) انظر موقع: com.yahoo. www تاريخ الدخول 3 مارس 2020

(20) حجازي، سهير، التهديدات الإجرامية للتجارة الإلكترونية ، مركز البحوث والدراسات ، شرطة دبي ، دولة الإمارات العربية المتحدة ، العدد (91).

(21) تامزروعي، موزة (2000) الاختراقات الإلكترونية خطر كيف نواجهه ، موزة المزروعي ، مجلة آفاق اقتصادية ، دولة الإمارات العربية المتحدة ، العدد التاسع ، سبتمبر ، ص54.

(22) عبد المطلب، محمود عبد الحميد (2000) جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت) منظور أمني ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 مايو ،ص.42.

(23) الخليل، عماد على (2000) 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 الإستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 مايو ، ص4.

[24]- بشير، هشام (2014)، الإرهاب الإلكترونى فى ظل الثورة التكنولوجية وتطبيقاتها فى العالم العربى ، آفاق سياسية ، العدد السادس ، يونيو ، ص76.

[25]- عبد الغفار، هدية الله نبيل محمود (2014) ، أثر الاتصالات وتكنولوجيا المعلومات على التحول الديمقراطى :دراسة حالة مصر وثورة يناير 2011 ، - رسالة ماجستير " ، ( القاهرة :كلية الاقتصاد والعلوم السياسية.

[26]- جابر، عماد الدين على أحمد (2014) ، دور شبكات التواصل الاجتماعى فى تشكيل اتجاهات الشباب العربي نحو الثورات العربية ، المؤتمر العلمى الدولى العشرين لكلية الإعلام جامعة القاهرة ، 22-23يونيو ، ص156.

[27]- الحسيني، أمانى عمر (2015) ، " العلاقة بين استخدام الشباب لشبكات التواصل الاجتماعى والفاعلية السياسية الداخلية والخارجية (دراسة ميدانية على عينة من شباب الجامعات المصرية ) " ، المجلة المصرية لبحوث الإعلام ، العدد 50 ، يناير-مارس ، ص.1

[28]- فرح، محمد على(2014) صناعة الواقع الإعلام وضبط المجتمع (أفكار حول السلطة والجمهور والوعى والواقع ) ، (بيروت : مركز نماء للبحوث والدراسات ) ، ص.230

[29] عبد الصادق ، عادل (2007) " هل يمثل الإرهاب الإلكترونى شكلا جديدا من أشكال الصراع الدولى " ، ملف الاهرام الاستراتيجى ، مركز الدراسات السياسية والاستراتيجية بالاهرام ، العدد 156 ، ديسمبر ، ص.81

[30] الألفي، محمد محمد الالفي ، الإرهاب الإلكترونى من التدمير إلى المواجهة، موقع الإهرام ، تاريخ الإطلاع : 4 مارس 2020، متاح على : ttp://aitmag.ahram.org.eg/News/2855.aspx

[31] عبد الصادق، عادل ، مرجع سابق ، ص81.

[32] عبد الوهاب، علي محمود (2011) ، الإرهاب الالكتروني ، مجلة مركز بحوث الشرطة ، العدد 39 ، مارس ، ص.321

[33] الخيلي، شمان ناجي صالح (2009) ، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت ، (القاهرة : دار النهضة العربية) ، ص35.

[34] بهجت ، أمانى (2015)" أمن المعلومات : تفعيل تشريعات مكافحة الجرائم الالكترونية فى الإقليم " ، حالة الإقليم ، العدد19 ، يوليو، المركز الإقليمى للدراسات الاستراتيجية بالقاهرة ، ص 18.

[35] طه، نجلاء عبد الفتاح (2015) ، دور الإعلام في حل القضايا المعاصرة (الارهاب –جرائم الانترنت- قضايا العولمة ) ، (الاسكندرية :دار التعليم الجامعي ) ، ص24.

[36] الرميح، يوسف بن أحمد ، الإرهاب والإعلام الجديد «الإرهاب الرقمي» ، موقع الجزيرة للصحافة ، تاريخ الإطلاع 5 مارس 2020 ، متاح علي : http://www.al-jazirah.com/2015/20150308/ar1.htm

[37] الدليمى، عبد الرزاق محمد (2010) ، الدعاية والإرهاب ، ( الأردن : دار جريرللنشروالتوزيع ، الطبعة الأولى) ، ص17.

[38] هاشم، عزة (2015)، لماذا ينجذب الشباب الغربي إلى داعش ، حالة العالم ، العدد15 ، مارس ، ص13.

[39] علو، عماد ، قراءة فى تداعيات تصاعد الأنشطة الإرهابية ، جريدة الزمان ،متاح على:www.azzaman.com/?p=68274، تاريخ الإطلاع : 9 مارس 2020

[40] العربي، محمد مسعد (2015) ، من هو الإرهابي؟ الدوافع الاجتماعية والنفسية للانضمام إلى التنظيمات الإرهابية ، حالة الإقليم ، العدد 23 ، نوفمبر- ديسمبر، ص .4

[41] فرغلي، ماهر ، قصة تجنيد "داعش" لـ"شيكو" على "فيسبوك" ، موقعجريدةالبوبةنيوز ، متاح علي : http://www.albawabhnews.com/1708382 ، تاريخ الاطلاع: 9 مارس 2020

[42] فرغلي، ماهر، قصة تجنيد "داعش" لـ"شيكو" على "فيسبوك" ، موقعجريدةالبوبةنيوز ، متاح علي : http://www.albawabhnews.com/1708382 ، تاريخ الاطلاع: 9 مارس 2020

[43] كيف يستخدم داعش "فيسبوك" لاختراق عقول الشباب ، موقع الأمد ، متاح علي : http://www.amad.ps/ar/Details/106928 ، تاريخ الاطلاع : 9 مارس 2020

https://ar.wikipedia.org/wiki/%D8%A5%D8%B1%D9%87%D8%A7%D8%A8_%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A([44])

([45]) الزيدي، وليد (2003) القرصنة على الانترنت الحاسوب والتشريعات القانون عمان. دار اسامة للنشر،ص.ص.10-12

([46]) الكساسبة ، فهد (2001) التطور التقني وتطور الجريمة، مجلة الأمن والحياة –الرياض أكاديمية نايف للعلوم الأمنية

([47]) أبو داس، ذكريا- (204) أثر التطور التكنولوجي على الإرهاب- رسالة ماجستير الجامعة الأردنية.

**المراجع باللغة الأجنبية**

1- Aren karbiniski (2010) face book and the technology revolution N , Y cestrum publications

2- Andrew M. Ledbetter, Joseph P. Mazer, Jocelyn M. DeGroot, Kevin R. Meyer, Yuping Mao and Brian Swafford.(2011) "Attitudes toward Online Social Connection and Self-Disclosure as Predictors of Facebook Communication and Relational Closeness" Communication Research Journal, Vol.38, No.1
3- Bahgat, Korany and others(2009). The faces of national security in the Arab World, England: Macmillan.
4- Bert, Swart,(2011) "Modes of International Criminal Liability", in: Antonio Cassese, The Oxford Compaion to International Criminal Justice, Oxford University Press
5- Burgess, Jean, (August 18, 2009), YouTube: Online Video and Participatory Culture, UK : Polity; 1 edition.
6- Daved smoloon (2009) the impact of the use of face book on the building society in the context of globalization, N Y sprctrum publication.
7- Diaz-Ortiz,Claire. (August 30, 2011), Twitter for Good: Change the World One Tweet at a Time, USA: Jossey-Bass; 1 edition
8- Michele. Vinson(2010) face book and the invasion of technological communities, N . Y Newyurk.
9- Olusola oyenyinka oyewo, Rumor(2007) :An Alternative Means Of Communication In A Developing Nation: The Nigerian Example ,international journal of African &African American studies ,vol,vI,no1,jan
10- Prell, Christina. (November 9, 2011), Social Network Analysis: History, Theory and Methodology, USA/Austalia: Sage Publications Ltd.
11- Rowell, Rebecca. (January 2011), Youtube: The Company and Its Founders, UK Essential Library
12- Seitel, Fraser P.(2009). The Practice of Public Relations. 9th ed, Prentice Hall. University of Stirling, Stirling
13- Sanders, CE; Field, TM.; Diego, M; and Kaplan (2000). The Relationship of Internet Use to Depression and Social Isolation among Adolescents. Adolescence. 35(138):237-42
14- Tye, Larry.(2002) The Father of Spin: Edward L. Bernays and the Birth of Public Relations . Henry Holt, London
15- Uslie, Lipson(2000) The great issues of politics, Englewood Clifs
16- Vonderau, Patrick. (December 30, 2009),The YouTube Reader, Sweden: National Library of Sweden
17- Weber, Max (2005) Political sociology (translated from German into English), London
18- Wilcox, Ault and Agee(2009) , Public Relations: Strategies and Tactics, Happer Collins Publishers, London
19- Wittkower, D:E. (October 1, 2010), Face book and Philosophy: What's on Y::our Mind?. USA: Open Court