دور الأمن السيبراني في علاج الإرهاب التجاري

بقلم: ط. د. ريمة مشطوب

ط. د. نورة لخويدر

جامعة محمد لمين دباغين - سطيف2

ملخص:

ظهر مفهوم الإرهاب في بلدان عديدة وبات بذلك يترجم الاستخدام غير القانوني للقوة أو العنف ضد أفراد أو مؤسسات أو مجتمعات، ومع ظهور شبكة الانترنت أصبح في السنوات الأخيرة وسيلة اتصال بامتياز لما يسمى بالجماعات الإرهابية، فأدى الإعلام الجديد وواكب ظهور مصطلحات ومفردات جديدة، تزامنت مع ظهور ما يسمى بالإرهاب الالكتروني الذي غزى الفضاء الافتراضي بصور وتشكيلات متنوعة منها الإرهاب التجاري؛ أين أصبحت هناك الآلاف من المواقع التي تستغلها هذه الجماعات الإرهابية لأغراض الدعاية، نشر المعلومات الخاطئة عن المؤسسات والمنتجات والخدمات، جمع الأموال عبر التخطيط اللاقانوني، بفضل ما أتاحه الإعلام الفائق من حرية وتفاعلية وتشاركية وتزامنية.

فأصبح الإرهاب التجاري يهدد الاقتصاد باقتحام مواقع البورصة العالمية، التزوير، القرصنة، غسيل الأموال، المتاجرة غير شرعية، السطو على المؤسسات التجارية، سرقة أرقام البطاقات الائتمانية، سرقة الأرقام السرية ونشرها، الحصول على الأموال وعدم إرسال المنتجات المطلوبة، وغيرها من المخالفات والمخاطر.

لهذا أتت هذه الورقة البحثية الراهنة لتسليط الضوء على الدور الذي يقوم به الأمن السيبراني لحماية المنتج والمستهلك للقضاء على عدوان الإرهاب التجاري في الفضاء السيبراني لتنفيذ الجرائم وخرق العمليات التجارية الالكترونية.

تمهيد:

إن عصرنة قطاع العدالة يتوقف على إرساء منظومة معلوماتية مركزية خاصة بوزارة العدل، تسمح بتقديم الخدمات في وقت وجيز وتقضي على تلك الممارسات الكلاسيكية التي أثقلت كاهل المواطن، وتسببت في غياب الجودة بسلك القضاء عموما، سعيا منها لحماية المجتمع من مختلف أشكال الإجرام، وتكييف المنظومة القانونية، من خلال مراجعة عدد من النصوص والمراسيم على غرار" قانون العقوبات"، "قانون الإجراءات الجزائية"، "القانون المتعلق بالوقاية وقمع استعمال المخدرات والمؤثرات العقلية والاتجار غير شرعي"، علاوة على "القانون التجاري".

وقد صرح سفير رئيس المفوضية الأوربية في الجزائر جون لوك أن دعم قطاع العدالة في الجزائر هو الهدف الذي تصبو إليه من خلال إطلاق برنامج تعاون مع الاتحاد الأوربي، علما أنها باشرت في إصلاحات العدالة منذ عام 2000 وقد حققت جملة من التغيرات والتطورات[1].

ومما لاشك فيه أن قطاع العدالة بشكل عام تواجه العديد من العراقيل والمشاكل لتفعيل دورها لعل من أبرزها الإرهاب الذي أصبح يمثل مشكلة العصر، خاصة الإرهاب الإلكتروني الذي اتخذ من الفضاء السيبراني وسيط تستند إليه الجماعات الإرهابية باعتمادها على وسائل عمل معينة غير قانونية تمكنها من تحقيق أهدافها وتجنيد اكبر عدد ممكن من الشباب والنساء وحتى الأطفال في صفوفها حسب تقديرات وإحصائيات منظمة الأمم المتحدة تعتبر الجرائم الالكترونية من جرائم القرن القادم ذلك لارتفاع نسب ارتكابها و كثرة أعداد مرتكبيها، خاصة، وأنه أصبح ظاهرة اجتماعية أتت تزامنا مع تحول المجتمعات من المجتمع التقليدي إلى المجتمع الرقمي، ومن فضاء الواقع المادي إلى فضاء الواقع الافتراضي العابر للحدود والقارات .

كما ازداد خطر الإرهاب الالكتروني نتيجة لاستخدام الدولة للتكنولوجيا المتطورة في مختلف الميادين ،ل لسهولة الاستخدام ورخص التكلفة بهدف تحقيق الرخاء والتقدم البشري، لكن الجماعات الإرهابية استغلت الظروف وبدأت تشن هجمات على مختلف القطاعات السياسية، الاقتصادية العسكرية والاجتماعية من خلال اختراقها للمواقع الالكترونية لرؤساء الدول والحكومات والوزارات والتجسس عليها وتدميرها، والإطلاع على مختلف المعلومات الأساسية للدولة

[1]- مختارات الصحف باللغة العربية: "**العدالة بين العصرنة والإصلاح**"، 2017، ع2، ص 6.

خاصة الأمنية منها، إضافة إلى المؤسسات الاقتصادية كالبنوك والبورصات العالمية، مما يؤثر سلبا على الأمن الاقتصادي للدولة[1].

وتؤكد الدكتوراه كونوي في دراستها: "الإرهاب والانترنت": إعلام جديد خطر جديد، على أنّ الانترنت أصبح وسيلة إستراتيجية توظفها الجماعات الإرهابية لتنفيذ برامجها وتحقيق أهدافها، بل أكثر من ذلك أصبحت تبحث عن كيفية ترشيد استغلال هذه التكنولوجية الجديدة.

ويرى وأيمن في دراسته "كيف يستخدم الإرهاب الحديث الانترنت" أنّ هذه الجماعات استغلت واستفادت من خصائص ومميزات الانترنت كسهولة الدخول إلى الشبكة، انعدام التشريعات والقوانين، الوصول إلى جماهير عريضة....الخ[2].

لذلك يعتبر الكثيرون الإرهاب الالكتروني عموما والتجاري خصوصا أخطر بكثير من الإرهاب التقليدي، لكونه أكثر انتشارا فهو يصل إلى مئات الملايين في ثوان معدودات، فأصبح اليوم الفيديو والصورة والكاميرا أكثر خطورة من الكلاشينكوف.

وهذه الآفات تعيق عمل التجارة الإلكترونية و تنتهك قانون التجارة الالكترونية، فقد أوضحت إيمان هدى فرعون وزيرة البريد وتكنولوجيات الإعلام والاتصال والاقتصاد الرقمي أنّ مشروع قانون التجارة الالكترونية تمّ المصادقة عليه ليدخل حيز التنفيذ، وهو قانون يؤطر حقوق وواجبات التاجر والمستهلك وجميع الترتيبات المتعلقة بتنفيذ المعاملة على الانترنت، إلى جانب التدابير المرتبطة بحماية وسرية العمليات التجارية الالكترونية، من معطيات حول الأرصدة والبطاقات البنكية والبريدية للمواطن مع تأمين المعاملات المالية.

كما يعتبر الأمن السيبراني من بين التحديات الأمنية المعاصرة التي لاقت إشكالا عويصا من طرف فواعل عديدة لتحقيقه و بالأخص الدول، حيث أصبح بعدا مفاهيميا تجدر دراسته من طرف الأوساط الأكاديمية و المعرفية و إيجاد نسق معرفي يسهل على صانع القرار إيجاد الحلول و

[1]- سارة بوحادة: "**أثر الإرهاب الالكتروني على أمن واستقرار الدول**"، المدرسة الوطنية العليا للعلوم السياسية ، الجزائر، د.ص.

[2]- محمد قيراط: "**الإعلام الجديد والإرهاب الالكتروني**: آليات الاستخدام وتحديات المواجهة"، مجلة الحكمة للدراسات الإعلامية والاتصالية، 2017، ع09، ص10.

الأفاق على المستوى الإمبريقي، حيث تعتبر الجزائر من بين الدول التي دخلت مصاف الإدارة الإلكترونية و العالم السيبراني، مما ترتب عليه انعكاسات أدى بالدولة الجزائرية إلى تبني إصلاحات و إستراتيجية أمنية لتحقيق أمنها السيبراني في الفضاء السيبيري.

وفي خضم هذه التوترات والانتهاكات الأمنية العابرة للحدود التي تعيق مسار العدالة السيبرانية واستتباب الأمن والسلام للأرواح والممتلكات وتزعزع أمن الدولة والمجتمع ،وتشوه التجارة الإلكترونية التي تسهل التواصل بين العملاء والشركاء، وتوفير احتياجات المستهلكين ومنه تحقيق أهداف كل مشروع تجاري باستخدام تكنولوجيات المعلومات والاتصال وتوفير أكثر فعالية وأكثر الأرباح لكل الأطراف في المعاملات التجارية السيبرانية، وعليه يمكن الإشكالية المطروحة :

- كيف يساهم الأمن السيبراني في علاج الإرهاب التجاري؟

- ما السبل التي يستخدمها الأمن السيبراني لمواجهة الجريمة التجارية السيبرانية؟

أولا- الأبعاد المفاهيمية للأمن السيبر اني والإرهاب التجاري الإلكتروني:

1.1- مفهوم الإرهاب:

أثير الكثير من الجدال والتساؤل بشأن تحديد مفهوم الإرهاب، وهو ما ساهم في الالتباس والتداخل والفوضى في الطرح والمعالجة والتحليل، فحتى اليوم لا يوجد تعريف متفق عليه دوليا للإرهاب.

نجد في لسان العرب، ما يأتي: (رَهِبَ بمعنى خاف والاسم الرَّهَبُ، كقوله تعالى: (مِنْ الرَّهْبِ) أي بمعنى الرهبة، ومنه: "لا رهبانية في الإسلام"... كاعتناق السلاسل، والاختصاء، وما أشبه ذلك مما كانت الرهابنة تتكلفه، وقد وضعها الله عز وجل عن أمة محمد صل الله عليه وسلم، وأصلها من الرَّهْبَنَةِ: الخوف، وترك ملاذ الحياة كالنساء..)[1].

يؤكد علماء اللغة أنّ أصل كلمة "إرهاب" مشتقة من الفعل: رهب، يرهب، ويقصد منها التخويف والفزع.

[1]- بن مكرم أبو الفضل، جمال الدين محمد: **لسان العرب لابن منظور**، دار صادر ودار بيروت، بيروت، 1955م / 1374 هـ، ج 8، ص 337.

وعرفته الاتفاقية العربية لمكافحة الإرهاب بأنّه: " كل فعل من أفعال العنف أو التهديد به، أيا كانت دوافعه أو أغراضه، يقع تنفيذه لمشروع إجرامي فردي أو جماعي، يهدف إلى إلقاء الرعب بين الناس أو ترويعهم، أو تعريض حياتهم أو حرياتهم وأمنهم للخطر، أو إلحاق الضرر بالبيئة، أو بأحد المرافق أو الأملاك أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر".[1]

عرف أحد الفقهاء الإرهاب بأنه: "العمل الإجرامي المصحوب بالرعب أو العنف أو الفزع بقصد تحقيق هدف معين".

كما يشار للإرهاب بالمفهوم الواسع: كل جناية أو جنحة سياسية أو اجتماعية ينتج عن تنفيذها والتعبير عنها ما يثير الفزع العام لما لها من طبيعة ينشأ عنها خطر عام، أما المفهوم الضيق فالإرهاب يعني" الأعمال الإجرامية التي يكون هدفها الأساسي نشر الخوف والرعب، كعنصر شخصي وذلك باستخدام وسائل تستطيع خلق حالة من الخطر العام كعنصر مادي"[2].

ويرى walter أن الإرهاب عملية رعب تتكون من ثلاثة عناصر هي: فعل العنف أو التهديد باستخدامه، رد الفعل الناجم عن أقصى درجات الخوف الذي أصاب الضحايا المحتملين وأخيرا التأثيرات التي تصيب المجتمع بسبب العنف أو التهديد باستخدامه ونتائج الفعل ".

وهناك تعريف آخر للإرهاب، يشير إلى أن الإرهاب "هو استعمال العنف للتأثير في الأفراد أو الجماعات أو الحكومة وخلق مناخ من الاضطراب وعدم الأمن لتحقيق هدف معين يرتبط بتوجهات الجماعات الإرهابية ولمنه بصفة عامة يتضمن تأثيرا في المعتقدات أو القيم أو الأوضاع

[1]- **المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب 1998**، جامعة الدول العربية ، الأمانة الفنية لمجلس وزراء العدل العرب، اعتمادها مجلسا وزراء العدل والداخلية العرب في اجتماعهما المشترك يوم 1998/04/22 بتاريخ ودخلت حيز النفاذ 1999/5/7، ص 3.

[2]- خالد السيد: **الإرهاب الدولي والجهود المبذولة لمكافحته**، مركز الإعلام الأمني، على الموقع الإلكتروني: https://www.policemc.gov.bh/، يوم2019/02/20،على الساعة : 16:45 مساءا، ص 2.

الاجتماعية والاقتصادية والسياسية السائدة التي تم التوافق عليها بين المؤسسات والأفراد، والتي تمثل مصلحة قومية عليا للوطن[1].

2.1- مفهوم الإرهاب الالكتروني:

يعرفه الأستاذ عبد الله العجلان بأنّه: "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الالكترونية بشتى صنوف العدوان وصور الفساد، فهو يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم[2].

كما يعرف بأنه استخدام الحاسوب والوسائل العلمية والتكنولوجية من أجل تنفيذ أعمال إرهابية ليس من السهل تنفيذها على أرض الواقع، ويتم تنفيذها من قبل شخص واحد بشرط أن تتوفر فيه القدرة والكفاءة والخبرة اللازمة في استخدام التقنية المعلوماتية.

ظهر مصطلح الإرهاب الإلكتروني في عقد الثمانينات من القرن الماضي على يد باري كولين، عندما تبنى تعريفا للإرهاب الإلكتروني مضمونه: هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية، و أن الهجمة يجب أن تكون ذات أثر مدمر وتخريب مكافئ الأفعال المادية للإرهاب[3].

كما أنه الجريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية، ينتج منه حصول المجرم على فوائد مادية أو معنوية مع تحميل

---

[1]- مصطفى هويدا: **دور الفضائيات العربية في تشكيل معارف الجمهور و اتجاهاته نحو الإرهاب، دراسة ميدانية على عينة من الجمهور العربي**، اتحاد إذاعات الدول العربية، جامعة الدول العربية، سلسلة بحوث ودراسات إذاعية (63) تونس،2008، ص 36-37.

[2]- العجلان عبد الله بن عبد العزيز بن فهد: "**الإرهاب الالكتروني في عصر المعلومات**"، بحث مقدم إلى المؤتمر الدولي الأول حول: حماية أمن المعلومات والخصوصية في قانون الانترنت، القاهرة، 2008، ص 23.

[3]- الإرهاب الإلكتروني وطرق مواجهته، شبكة النبأ المعلوماتي، الموقع الإلكتروني:
http://m.annabaa.org.arabic/information/11123/، يوم 2019/02/15، على الساعة 11:55مساء).

الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات[1].

تعريف وزارة الدفاع الأميركية لمفهوم الإرهاب الإلكتروني، حيث تحدد بأنه «كل عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات، وينتج عنه عنف وتدمير أو بثّ الخوف تجاه متلقي الخدمات بما يسبب الارتباك وعدم اليقين، وذلك بهدف الضغط على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة[2].

ويقصد به كذلك استخدام الوسائل الإلكترونية والتقنيات الرقمية، الصادر عن الدول أو الجماعات أو الأفراد، ضد أي شخص طبيعي أو اعتباري، بدوافع سياسية، بغرض إخافته أو تهديده والتأثير فيه ماديا أو معنويا، أو بقصد التأثير في القرارات الحكومية أو الرأي العام[3].

ويقصد بإرهاب السيبر أو الإرهاب العالم الإلكتروني Cyber Terrorism، وهي هجمات تستهدف نظم الكمبيوتر والمعطيات لأغراض دينية أو سياسية أو فكرية أو عرقية وفي حقيقتها جزء من السيبر باعتبارها جرائم إتلاف للنظم والمعطيات أو جرائم تعطيل للمواقع وعمل الأنظمة.

لكنها تتميز عنها بسمات عديدة أبرزها أنها ممارسة لذات مفهوم الأفعال الإرهابية لكن في بيئة الكمبيوتر والإنترنت وعبر الإفادة من خبرات الكريكرز- أي مجرمي الكمبيوتر الحاقدين– العالية، وفي إطار ذات السمات التي تتوفر في جماعات الجريمة المنظمة[4].

---

[1]- بوعلي بوجلطية أحمدي: "**الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي دراسة للتجربتين السعودية والقطرية**"، الأكاديمية للدراسات الاجتماعية والإنسانية، قسم العلوم الاقتصادية والقانونية، العدد 16، جوان 2016، ص 183.

[2]- المطيري عادل عبد الله: **الإرهاب الإلكتروني والأمن السيبراني**، على الموقع الإلكتروني: http://alarab.qa/story/1333816، يوم 2019/02/12، على الساعة 16:57مساءا.

[3]- مايا حسن ملا خاطر: "**الإطار القانوني لجريمة الإرهاب الإلكتروني**"، مجلة جامعة الناصر، العدد الخامس، المجلد الأول، يناير- يونيو 2015، كلية الحقوق ،جامعة دار العلوم، المملكة العربية السعودية، ص 133 .

[4]- مهد مهد الألفي، ورقة العمل حول: "**تشريعات مكافحة جرائم الإرهاب الإلكتروني الأحكام الموضوعية والأنماط**"، القاهرة، د.ن، ص 10.

3.1- مفهوم الإرهاب التجاري:

ومن خلال التفحص في التراث النظري أنه لم نجد مفهوما واضحا للإرهاب التجاري، فعمدت إليه هذه الدراسة إلى انتقاء مفهوم إجرائي يتماشى وهدفها، وكان كالآتي:

وهو أحد أصناف الإرهاب الإلكتروني الذي يعتمد على الحاسوب وبرمجياته وسيلة للإتجار غير المشروع والمعاملات التجارية في السلع والخدمات لتشويه سمعة المؤسسات الاقتصادية عبر الوسائط الإلكترونية، ونشر المعلومات المكذوبة وتشويه سمعة الأشخاص، غسيل الأموال والتجسس التجاري، والسطو على البطاقات الائتمانية، والاعتداء على التوقيع الإلكتروني، تجارة الأسلحة، وتجارة المخدرات والقمار عبر الإنترنت...، وكل هذه الأصناف تؤدي إلى تخويف وترويع الآخرين وإلحاق الضرر بهم وبمعاملاتهم التجارية عبر المبادلات الإلكترونية.

ويمكن أيضا أن يعرف بأنه سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية في التجارة الإلكترونية، ينتج عنه حصول المجرم على فوائد مادية أو معنوية للإخلال بهذه التجارة، فتصبح وسيلة لتخويف الضحية واستفزازه بالأموال أو وسائل أخرى، ولا يمارس هذا النوع من الإرهاب إلا من طرف من يملك كفاءة وخبرة في المجال الرقمي.

4.1- مفهوم الأمن السيبراني:

عرف ريتشارد كمرر (Richara A.Kemmerer) الأمن السيبراني بأنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة".

أما إدوارد أمورسو (Edward Amoroso) الأمن السيبراني بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة... إلخ[1].

[1]- عنترة بن مرزوق، محي الدين حرشاوي: "**الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**"،د.ن،على الموقع الالكتروني:*https://manifest.univ-ouargla.dz*، يوم 2019/20/21 ،على الساعة 16:55 مساءا، ص 02.

كما يعني الأمن الإلكتروني أي أداة أو تقنية أو عملية مستخدمة لتحمى أصول المعلومات لنظام الأمن الإلكتروني، حيث يتيح الأمن الإلكتروني ويضيف قيم الشبكات وموجه للبنية الأساسية المرنة والصلبة. والمكونات البنية الأساسية الصلبة تعني الأجهزة الصلبة Hardware والبرمجيات Software المطلوبة لحماية النظام والبيانات من التهديدات والأمن من خارج أو داخل النظام، أما المكونات البنية الأساسية المرنة تعني السياسات، والعمليات والبروتوكولات، والتوجيهات التي تحمى النظام والبيانات من مصادرها المختلفة[1].

والملاحظ أن مصطلح سيبار أو الفضاء الإلكتروني وفي كثير المراجع الفضاء السيبراني، ظهر مع ظهور الانترنت وتعميم استخدام الرقمنة، موازاة مع كم هائل من المصطلحات مثل الفضاء الرقمي، الدفاع الإلكتروني، الهجوم الإلكتروني، الجريمة الإلكترونية وغيرها، في حين أن الأمن السيبراني أو الإلكتروني ظهر حديثا وهو يعني: مجمل القوانين السياسية، الأدوات، النصوص، المفاهيم، وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية الدول والمنظمات والأشخاص.

ويقصد أيضا بالأمن السيبراني بأنه الحالة المرغوب فيها لعمل أنظمة المعلومات والاتصالات والتي تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني، والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التجسس[2].

ويعرف كذلك الأمن السيبراني بأنه: "عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به، وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحامية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني[3].

---

[1]- بوعلي أحمدي بوجلطية، مرجع سابق، ص 183.

[2]- عنترة بن مرزوق ، محي الدين حرشاوي، مرجع سابق، ص 03.

[3]- حمزة صيوان، الفتلاوي عطية: "**الأمن السيبراني والحروب السيبرانية**"، جريدة خيمة العراق الصادرة عن وزارة الدفاع العراقية، العدد 357، 04 مارس2015، ص10.

والملاحظ من التعاريف للأمن السيبراني كثيرا ما يذكر بالموازاة مع الفضاء السيبراني والذي يقصد به- الفضاء السيبراني- كما عرَفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي على أنَه: "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية".

إذن فهو هو مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمو كل هذه العناصر".

كما أن عملية تعزيز الجانب الدلالي لهدا الفضاء تستدعي تحليل البنية التركيبية له، إذ يُمكن اعتبارها بنية ذي ثلاث طبقات هي:

01- الطبقة المادية: تشمل معدات الحواسيب، والبرمجيات، والمعدات الضرورية لعملية الربط البيني.

02- الطبقة المنطقية: تشمل مجموع البرامج المترجمة للمعلومة على شكل معطيات رقمية، حيث يتم الانتقال من لغة الإنسان إلى لغة الآلة في شكل خوارزمية، ومنها إلى برامج مطوَرة بلغة البرمجة.

03- الطبقة الإعلامية: وتتمثل هذه الطبقة في البعد الاجتماعي الذي يضاف إلى الطبقتين السابقتين، حيث أنه في الفضاء الرقمي يمكن أن يكون لكل إنسان عدة هويات رقمية (عنوان بريده الالكتروني، رقم هاتفة النقال، صور رمزية على مواقع التواصل الاجتماعي...)[1].

ثانيا- فروق دلالية بين الأمن المعلوماتي والأمن السيبراني:

أمن المعلومات يهدف إلى حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل، كما يهدف إلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين.

[1]- إسماعيل قادير: **إدارة الحروب النفسية في الفضاء الالكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط**، جامعة الجزائر3، الندوة الدولية: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، د.ن، ص 4-5.

كما أنه يعنى أمن المعلومات بالوسائل الضرورية لاكتشاف وتوثيق وصد كل هذه التهديدات، وأمن المعلومات يشمل كل ما من شأنه حماية (المعلومة) التي قد تكون في نظام حاسوبي، أو قد لا تكون. فهو المضلة الكبرى التي تغطي كل الأفرع الأخرى المرتبطة بحماية البيانات والمعلومات وتأمينها، ويهتم بمجالات ضخمة، كالتشفير، والتخزين، والتأمين الفيزيائي، والمعايير الأمنية، وإدارة أمن المعلومات والمخاطر.

فأمن المعلومات والأمن السيبراني هما مصطلحان متشابهان، لكنهما ليسا متطابقين، فالأمن السيبراني هو سلاح إستراتيجي بيد الحكومات والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزءا لا يتجزأ من الأساليب الحديثة للحروب والهجمات بين الدول[1].

ثالثا- هدف وأهمية الأمن السيبر اني:

إن هدف الأمن السيبراني هو المساعدة على حماية الأصول وموارد المنظمات من النواحي التنظيمية، والبشرية، والمالية، والتقنية، والمعلوماتية بحيث يسمح لها بمواصلة مهمتها، والهدف النهائي هو ضمان عدم تضررها ضررا دائما وهذا يتألف من تقليل احتمالات تجسد أي تهديد، والحد من الضرر الناجم أو سوء الأداء، وضمان استعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة، في أعقاب وقوع حادث أمني. وتستغرق عملية الأمن السيبراني المجتمع بأسره، من حيث يكون كل فرد فيه معنيا بتنفيذها، ويمكن دعم ذلك بتطوير مدونة سلوك سيبرانية لأجل الاستخدام السليم لتكنولوجيات المعلومات والاتصالات، وإعلان سياسات أمن حقيقية تفنن المعايير التي يكون متوقعا من مستخدمي الأمن السيبراني (الكيانات والشركاء والموردون) الوفاء بها[2].

[1]- صالح بن علي بن عبد الرحمن الربيعة: **الأمن القومي وحماية المستخدم من مخاطرالإنترنت**، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، 2030، ص 10-11.

[2]- توريه حمدون: "**دليل الأمن السيبر اني للدول النامية**"، الاتحاد الدولي للاتصالات، تصدير 03، 2006.

رابعا- خصائص الإرهاب التجاري:

- ✓ هو إرهاب لا يحتاج إلى ارتكاب العنف والقوة بل يتطلب وجود حاسوب متصل بالشبكة ومزود ببعض البرمجيات والتطبيقات.
- ✓ يمثل جريمة إرهابية عابرة للحدود والدول والقارات (لا حدود جغرافية).
- ✓ صعوبة اكتشاف الجرائم التي ينفذها، خاصة مع نقص الخبرة لدى أجهزة الأمن السيبراني.
- ✓ صعوبة إثبات المخالفات التي يرتكبها الإرهاب التجاري، بسبب سرعة غياب الدليل الرقمي
- ✓ مرتكب الجريمة التجارية السيبرانية هو شخص ذو خبرة فائقة في مجال الحواسيب والتقنيات.
- ✓ جريمة تحتاج إلى خبرة فنية، ويصعب على المحقق التقليدي التعامل معها[1].

خامسا- أشكال الإرهاب التجاري:

1.5- غسيل الأموال:

اختلف الكثير في تعريف غسيل الأموال وقد يكون التعريف الشامل هو: كل عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسبت منه الأموال"، ومن البديهي أن يأخذ المجرمون بأحدث ما توصلت إليه التقنية لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسيل الأموال التي استفادت من عصر التقنية فلجأت إلى الإنترنت لتوسيع وتسريع أعمالها في غسيل أموالها غير المشروعة، ويجد المتصفح للانترنت مواقع متعددة تتحدث عن هذه العمليات منها: http://www.laundryman.u.net.com كما يجد المواقع التي تستخدم كساتر لعمليات غسيل الأموال ومنها المواقع الافتراضية لنوادي القمار التي قام مكتب المباحث الفدرالية (FBI) الأمريكي بمراقبة بعض هذه المواقع.

[1]- عطية أيسر محمد: "**دورالآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته**"، ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان، 2014، ص 11-12.

فجريمة غسيل الأموال بأنها " كل ما يدير أو يحاول أن يدير تعامل مالي يوظف عائدات بطريقة ما لنشاط غير قانوني عارفا بأن المال المستخدم هو عائدات بطريقة ما لنشاط غير قانوني أو كل من ينقل أو يرسل أو يحيل وسيلة نقدية أو مبالغ تمثل عائدات بطريقة ما لنشاط غير قانوني عارفا بأن هذه الوسيلة النقدية أو المال يمثل ما لنشاط غير قانوني[1].

وقد ظهر اصطلاح (غسل الأموال) لأول مرة في اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والتي عقدت في فينا عام 1998، وقد نص في المادة الثالثة منها على أن غسل الأموال يتمثل إما في تحويل الأموال أو نقلها مع العلم بأنها من نتاج جرائم المخدرات، أو في إخفاء أو تمويه حقيقة الأموال أو مصدرها أو في اكتساب أو حيازة أو استخدام الأموال مع العلم وقت تسليمها أنها من حصيلة جريمة من الجرائم المنصوص عليها في الاتفاقية[2].

2.5- تزوير البيانات:

تعتبر من أكثر جرائم نظم المعلومات انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك.

وقد وقعت حادثة في ولاية كاليفورنيا الأمريكية حيث عمدت مدخلة البيانات بنادي السيارات وبناء لاتفاقية مسبقة بتغيير ملكية السيارات المسجلة في الحاسب الآلي بحث تصبح باسم أحد لصوص السيارات والذي يعمد إلى سرقة السيارة وبيعها وعندما يتقدم مالك السيارة للإبلاغ يتضح عدم وجود سجلات للسيارة باسمه وبعد السيارة تقوم تلك الفتاة بإعادة تسجيل السيارة باسم مالكها وكانت تتقاضى مقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى أن قبض عليها، وفي حادثة أخرى قام مشرف تشغيل الحاسب بأحد البنوك الأمريكية بعملية تزوير حسابات أصدقائه في البنك بحيث تزيد أرصدتهم ومن ثم يتم سحب تلك المبالغ من قبل أصدقائه وقد نجح في ذلك

[1]- حسين علي محسن: "**جريمة غسيل الأموال الإلكترونية**"، كلية القانون، الجامعة المستنصرية، د.ن، ص 01.

[2]- رشدي مراد، 2003: على الموقع الإلكتروني:

http://www.maher.sandroses.com/m706.htm،

يوم: 2019/02/15، على الساعة 19:47مساءا.

وكان ينوى التوقف قبل موعد المراجعة الدورية لحسابات البنك إلا أن طمع أصدقاءه أجبره على الاستمرار إلى أن قبض عليه .

ومما شك فيه أن البدء التدريجي في التحول إلى الحكومات الإلكترونية سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمة أهدافهم الإجرامية[1].

تعتبر هذه الجريمة من أكثر جرائم نظم المعلومات والانترنت انتشارا فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك .

ومما لاشك فيه ان البدء التدريجي في التحول إلى الحكومات الإلكترونية E-Government سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالإنترنت مما يسهل الدخول على تلك الأنظمة من قبل محترفي اختراق الأنظمة وتزوير البيانات لخدمة أهدافهم الإجرامية.

وجرائم التزوير ليست بالجرائم الحديثة، ولذا فانه لا تخلوا الأنظمة من قوانين واضحة لمكافحتها والتعامل معها جنائيا وقضائيا و تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها.[2]

3.5- القرصنة:

يقصد بالقرصنة الاستخدام أو/ والنسخ غير المشروع لنظم التشغيل أو/ ولبرامج الحاسب الآلي المختلفة. وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الإنترنت تطورت صور

[1]- العريان عبد الحميد إبراهيم محمد: "**العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة**": ما هو رد فعل القطاع الخاص، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية خلال الفترة، كلية التدريب، قسم البرامج التدريبية، المغرب، القنيطرة، 2006 ، ص 41.

[2]- **أضرار جرائم شبكة الانترنت**، على الموقع الإلكتروني: *https://vb.ckfu.org/attachments/*، يوم2019/02/15،على الساعة 19:47مساءا.

القرصنة واتسعت وأصبح من الشائع جدا العثور على مواقع بالإنترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي.

وقد أدت قرصنة البرامج إلى خسائر مادية باهظة جدا وصلت في العام 1988 إلى 11مليار دولار الأمريكي في مجال البرمجيات وحدها، ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وأن شاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الأعمال أو ما تعرف اختصارا بـ:(BSA)، والتي أجرت دراسة تبين منها أن القرصنة على الإنترنت ستطغى على أنواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الإنترنت ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الإنترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة إلا أن تلك الشركات تراجعت عن هذا التهديد إثر محاربته من قبل جمعيات حماية الخصوصية لمستخدمي الإنترنت[1].

4.5- المو اقع المتخصصة في القذف وتشويه سمعة الأشخاص:

المواقع الموجهة ضد أشخاص محددين فهي موجودة ولكنها ليست منتشرة انتشارا المواقع الأخرى وتركز هجومها غالبا على أبرز سلبيات الشخص المستهدف ونشر بعض أسرار سواء التي يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه والعبث به أو بتلفيق الأخبار عنه[2].

5.5- القمار عبر الانترنت:

في الماضي كان لعب القمار يستلزم وجود اللاعبين معا على طاولة واحدة ليتمكنوا من لعب القمار، أما الآن ومع انتشار شبكة الانترنت على مستوى العالم فقد أصبح لعب القمار أسهل حيث التف اللاعبين على صفحة واحدة من صفحات الانترنت على مستوى العالم ومن أماكن متفرقة أسهل من ذي قبل.

[1]- إبراهيم محمد: "**العلاقة بين الإرهاب المعلوماتي والجر ائم المنظمة**"، ص 34.

[2]- إبراهيم محمد، مرجع سابق، ص 41.

سادسا- استغلال الإرهاب التجاري للفضاء السيبر اني:

مكن الإعلام الجديد الإرهاب التجاري من تكوين جماهير على اختلاف الفئات الاجتماعية، نظرا لمجانيته وانتشاره، خصوصا مع ظهور الويب 2.0 وما أنتجه من منصات وشبكات وردهات تفاعلية جذبت الصغير والكبير، ومن أهممها نجد:

أ- **الفايسبوك**: يمثل الشبكة الاجتماعية الأضخم والأكبر والأكثر استخداما، لذلك يقول أحد خبراء الاتصال: "لو كان الفايسبوك دولة... سيكون ثالث أكبر دولة بالعالم بعد الصين والهند...عدد مستخدميه تجاوز 300 مليون...كل دقيقة تأتي بالمزيد[1].

فاستغلته الجماعات الإرهابية من خلال نشر فيديوهات وصور كاذبة عن مؤسسات اقتصادية وحتى رجال أعمال لتشويه سمعتهم، وفقدان مركزهم.

ب- **يوتيوب**: يعتبر من أهم المنابر المستخدمة من قبل الجماعات الإرهابية لنشر ثقافتهم و كسب أطراف جدد لتوسيع معاملاتهم وخلق مجتمع إرهابي افتراضي، وحسب إحصائيات يوتيوب تمت مشاهدة ألف مليار فيديو سنة 2011، وهناك مليار مستخدم اليوتيوب يشاهدون 6 مليارات ساعة من الفيديوهات كل شهر.[2]

هي صفحات وغيرها من الشبكات التي يمارس الإرهاب التجاري نشاطه عبرها مستفيدا من مختلف التقنيات والأساليب للإقناع والتأثير قصد استقطاب الجماهير و نجد مثلا: صفحة "فايسبوك شوب" أو Facebook Shop.

حيث سجلت عشرات الآلاف من المشاركين والمتفاعلين معها، إلى جانب استغلالها في جمع الأموال والحصول على التبرعات والدعم المالي، كلها مسائل عانى معها الأمن السيبراني لإيجاد سبل لمواجهتها والتقليل من توسعاتها.

كما أن الإرهاب التجاري هو تهديد اقتصادي وذلك اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، وتعطيلُ عمليَّات التحويل المالي، مما يُلْحِقُ الأذى بالاستثمار

[1]- علي عبد الفتاح: **الإعلام الاجتماعي**، دار اليازوري، عمان، ص 168.

[2]- Weiman, Gabriel :**New terrorism and new media**, Washington. D. c, Wilson centre, commons, lab, research series,Vol2.

الأجنبي وبالثقة بالاستثمار عامةً، وإلحاق الأذى بالاقتصاد الوطني، وتعديلُ ضغط الغاز عن بُعد في أنابيب الغاز لتفجيرها، ونُظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، ومن أمثلتها قيام بعض الإرهابيين بتحويل ملايين الدولارات من بعض الحسابات الشخصية لكبار العملاء بعد اختراق نظام التحويلات الدولي بين البنوك، وقيام بعض الهاكرز المحترفين بسرقة بيانات بطاقات الائتمان من بعض أكبر مراكز التسوق الإلكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقات، وكذلك قيام بعض المنظمات الإرهابية بالعمل على تدمير اقتصاد إحدى دول الشرق الأوسط بشراء سندات دولية لتلك الدولة من داخلها عبر البورصات العالمية وبيعها بالخارج بأسعار أقل من قيمتها مما أدى لانهيار عملتها ولتوفير تمويل لأعمالها الإرهابية في الدول التي تم بيع السندات فيها.

سابعا- الأمن السيبراني والجريمة التجارية السيبرانية:

يؤدي الأمن السيبراني دورا هاما في التنمية الراهنة لتكنولوجيا المعلومات، فتعزيز الأمن السيبراني وحماية البنى التحتية، عنصرين أساسين في أمن كل أمة ورفاهها الاقتصادي، فأصبح بذلك أمان الانترنت وحماية المستخدمين، جزء لا يتجزأ من تنمية الخدمات الجديدة ومن السياسات الحكومية[1].

ويمثل ردع الجريمة السيبرانية التجارية عنصرا جوهريا في الأمن السيبراني لحماية المنتج والمستهلك، ومن بين استراتيجيات الأمن السيبراني نجد تنمية نظم الحماية التقنية أو توعية المستخدمين لوقايتهم من الوقوع في براثن الجريمة التجارية.

في هذا الصدد أطلق الأمين العام للاتحاد الدولي للاتصالات في 2007 البرنامج العالمي للأمن السيبراني الذي يستند إلى خمسة (05) مجالات عمل واستراتيجيات وهي: التدابير القانونية، التدابير التقنية والإجرائية، الهياكل التنظيمية، بناء القدرات، التعاون الدولي.

[1]- ماركو جيركي: "**فهم الجريمة السيبرانية: الظواهر والتحديات والاستجابة القانونية**"، الاتحاد الدولي للاتصالات، 2012، ص 10.

ثامنا- الأمن السيبراني وسبل مواجهة الإرهاب التجاري:

حذر الكثير من المختصين من خطر التعدي على الديمقراطية والحرية باسم محاربة الإرهاب، لانّ الانترنت تتناغم مع مبادئ الشفافية وحرية الرأي والتعبير والعدالة الاجتماعية والمساواة، ويرى الدكتور الحمامي في هذا الشأن: "تعاظم النقاش حول إمكانات تنظيم الميديا الاجتماعية بالتوازي مع تنامي استخداماتها وتنوعها"[1].

فالمطلوب هو التعامل مع المشكلة بمهنية واحترافية وبطرق منهجية ومنظمة، لذا على الأمن السيبراني التركيز على فهم آليات الإرهاب التجاري وخصائصه وتطوره، ومن أهم الإجراءات التي يجب على المنظمات الأمنية اتخاذها ما يلي:

- رصد أنشطة الجماعات الإرهابية على الشبكات الاجتماعية.
- تحليل خطاب العنف والكراهية والتحريض على الإرهاب على اختلاف أشكاله.
- إشراك المجتمع المدني للتعاون على الإبلاغ على كل المواقع ذات العلاقة بالإرهاب مع نشر ثقافة الوقاية وتوعية المجتمع بمخاطر الإرهاب التجاري، ونشر ثقافة الحوار.
- سن القوانين والتشريعات التي تنظم الأنشطة الاقتصادية السيبرانية، التي تسد كافة الثغرات التي تكتنف جريمة الإرهاب التجاري كالقوانين المتعلقة مثلا بكيفية اكتشاف الأدلة الالكترونية وحفظها.
- تنظيم مؤتمرات وندوات علمية في الجامعات ومراكز البحوث في مختلف دول العالم تضم خبراء ومختصين من مختلف التخصصات لدراسة الظاهرة واقتراح الحلول الناجعة.[2]

وقد كان للجهود الجزائرية دورا في مجال تحقيق الأمن السيبراني، وكان الترتيب العالمي للجزائر حسب الرقم القياسي العالمي للأمن السيبراني، حيث احتلت الجزائر المرتبة 23عالميا من أصل 29 مرتبة في مستوى التأهب في مجال الأمن السيبراني في الترتيب العالمي بالرقم القياسي

[1]- الصادق الحمامي: "**الميديا الاجتماعية والإرهاب**": ورقة بحثية مقدمة في الورشة الدولية حول: التعاطي الإعلامي مع ظاهرة التطرف والإرهاب، اتحاد إذاعات الدول العربية، تونس، 2015.

[2]- محمد قيراط، مرجع سابق، ص 26.

0,176، وعلى المستوى العربي احتلت المرتبة العاشرة حسب التزامها بتلك التدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني.

جدول رقم (1 0): يوضح ترتيب بلدان منطقة الدول العربية حسب الرقم القياسي العالمي للأمن السيبر اني

الدول العربية	قانونية	تقنية	تنظيمية	بناء القدرات	التعاون	الرقم القياسي	الترتيب الإقليمي
عمان	0.7500	0.667	1.0000	0.7500	0.6250	0.7647	1
قطر	0.7500	0.8333	0.5000	0.6250	0.5000	0.6176	2
مصر	0.5000	0.5000	0.3750	1.0000	0.5000	0 .5882	3
المغرب	0.5000	0.6667	0.7500	0.5000	0.3750	0.5588	4
تونس	1.0000	0.5000	0.6250	0.2500	0.5000	0.5294	5
السودان	0.7500	0.5000	0.5000	0.2500	0.3750	0.4412	6
الإمارات العربية المتحدة	0.7500	0.3333	0.2500	0.5000	12.50	0.3529	7
البحرين	0.7500	0.1667	0 .1250	0.3750	0.2500	0.2941	8
ليبيا	0.2500	0.3333	0.3750	0.1250	0.3750	0.2941	8
المملكة العربية السعودية	0.7500	0.3333	0.1250	0.3750	0.1250	0.2941	8
الأردن	0.5000	0.0000	0.5000	0.0000	0.1250	0.2059	9
الجزائر	0.7500	0.0000	0.0000	0.1250	0.2500	0.1765	10

المصدر: عنترة بن مرزوق ، محي الدين حرشاوي: الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، د.ن، ص 8.

من خلال الجدول أعلاه يمكن القول أن جهود الجزائرية في مجال تحقيق الأمن السيبراني تبقى ضئيلة ،حيث تركزت أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الأخرى، ويتضح ذلك من خلال صدور القانون رقم 09-04 المؤرخ في 05أوت 2009،الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي تم

فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الالكترونية بناءا على ما ورد في المادة 4 التي نصت على ما يلي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

- في حالة توفر المعلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني .

- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء المراقبة الإلكترونية .

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا تم من خلال صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر سنة 2015،وهيئات أخرى.[1]

خلاصة:

أصبح الإرهاب التجاري واقع يفرض نفسه على المجتمعات، فأصبحت جرائمه هاجسا يشغل العقول خاصة مع الثورة المعلوماتية والتقنية، التي سمحت لهذه المجموعات ممارسة نشاطاتها عبر كل مناطق العالم، وفي أي لحظة، لذلك سعت المنظمات الأمنية إلى اتخاذ جملة من التدابير والإجراءات اللازمة للمواجهة، لكنها تبقى الجهود قليلة وبحاجة إلى بحوث ودراسات التنسيق والتشريع والتنظيم لاحتواء الظاهرة، ويمكن القول أن الإرهاب الإلكتروني بشكل عام والإرهاب التجاري بشكل خاص أصبح تهديدا أمنيا سيبرانيا يزعزع أمن الدولة وأفرادها، خاصة مع الاجتياح الرقمي الرهيب الذي أصبح يدخله كل شرائح المجتمع، وبهذا بدل أن يصبح نعمة لتطورها المجتمعات أصبح نقمة تقوض حريات الأفراد والمؤسسات، وبما أن التجارة الإلكترونية في الفضاء السيبراني رغم مزاياها إلا أنها كانت منفذا يستخدم بشكل سلبي من خلال استخدامها من طرف الجماعات الإرهابية وقيامها بهجومات وجرائم الكترونية على مختلف القطاعات التجارية،

[1]- عنترة بن مرزوق ، محي الدين حرشاوي، مرجع سابق، ص9.

الاقتصادية، مما ينتج عنها خسائر فادحة تمس بجميع الميادين خاصة الأمني منها مما يتطلب على أطراف المجتمع الدولي اتخاذ كافة التدابير اللازمة لمجابهة هذه الاعتداءات والتهديدات أو الحد منها.

و يمكن عرض مجموعة من التوصيات للحد من أخطار الإرهاب الالكتروني التجاري وتحقيق الأمن المادي السيبراني وتوفير استقرار الدول:

- ضرورة تفعيل وتحيين المراسيم القانونية التي تندد بمخاطر الإرهاب التجاري على المستوى الإقليمي الوطنية والدولي.
- تكوين وتأطير فرق وخبراء يمتازون بالكفاءة والدقة في البرمجيات الحاسوبية لمواجهة الاعتداءات على الممتلكات والأشخاص على الفضاء الإلكتروني.
- تطوير تقنيات مراقبة شبكة الانترنت وتعزيز إجراءات الأمن والحراسة للمواقع الرسمية.
- العمل على عقد مؤتمرات دولية تعزز أهمية وفائدة التعاون الثنائي والدولي لمكافحة ظاهرة الإرهاب التجاري لتسليم المجرمين وتحقيق أمن واستقرار الدول.
- الاستفادة من تجارب الدول الرائدة في مجال الأمن السيبراني ودوره في مواجهة الإرهاب بكل أشكاله خاصة في الفضاء الرقمي.

*** قائمة المراجع:**

أ- باللغة العربية:

1. الحمامي الصادق:الميديا الاجتماعية والإرهاب: ورقة بحثية مقدمة في الورشة الدولية حول: التعاطي الإعلامي مع ظاهرة التطرف والإرهاب، إتحاد إذاعات الدول العربية، تونس، 2015.
2. العجلان عبد الله بن عبد العزيز بن فهد: الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول: حماية أمن المعلومات والخصوصية في قانون الانترنت، القاهرة، 2008.
3. العريان عبد الحميد إبراهيم محمد: العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة: ما هو رد فعل القطاع الخاص، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية خلال الفترة، كلية التدريب، قسم البرامج التدريبية، ،المغرب، القنيطرة ،2006.
4. المادة الأولى من الاتفاقية العربية لمكافحة الإرهاب 1998، جامعة الدول العربية، الأمانة الفنية لمجلس وزراء العدل العرب ،الاتفاقية العربية لمكافحة الإرهاب ،اعتمادها مجلسا وزراء العدل والداخلية العرب في اجتماعهما المشترك يوم 1998/04/22بتاريخ ودخلت حيز النفاذ1999/5/7.
5. بن مكرم أبو الفضل جمال الدين محمد: لسان العرب لابن منظور، دار صادر ودار بيروت، بيروت، 1955م / 1374 هـ، ج 8.
6. بوحادة سارة: أثر الإرهاب الالكتروني على أمن واستقرار الدول، المدرسة الوطنية العليا للعلوم السياسية –الجزائر.
7. بوعلي بوجلطية أحمدي: الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي دراسة للتجربتين السعودية والقطرية، الأكاديمية للدراسات الاجتماعية والإنسانية، قسم العلوم الاقتصادية والقانونية، العدد 16،جوان 2016.
8. توريه حمدون: دليل الأمن السيبراني للدول النامية، الإتحاد الدولي للاتصالات، تصدير 2006،3.
9. جيركي ماركو: فهم الجريمة السيبرانية: الظواهر والتحديات والاستجابة القانونية، الاتحاد الدولي للاتصالات، 2012.
10. صالح بن علي بن عبد الرحمن الربيعة: الأمن القومي وحماية المستخدم من مخاطر الإنترنت،هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية ،2030.

11. صيوان حمزة، الفتلاوي عطية: "الأمن السيبراني والحروب السيبرانية"،جريدة خيمة العراق الصادرة عن وزارة الدفاع العراقية، العدد 357، 4 مارس2015.

12. عطية أيسر محمد: دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته، ورقة مقدمة في الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الإستراتيجية، عمان، 2014.

13. علي عبد الفتاح: الإعلام الاجتماعي، دار اليازوري، عمان، 2014.

14. قادير إسماعيل: إدارة الحروب النفسية في الفضاء الالكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط، جامعة الجزائر3،الندوة الدولية: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية.

15. قيراط محمد: الإعلام الجديد والإرهاب الالكتروني؛ آليات الاستخدام وتحديات المواجهة، جامعة قطر، مجلة الحكمة للدراسات الإعلامية والاتصالية، ع2017،9.

16. مايا حسن ملا خاطر: الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، العدد الخامس، المجلد الأول، يناير- يونيو 2015،كلية الحقوق ،جامعة دار العلوم، المملكة العربية السعودية.

17. مختارات الصحف باللغة العربية: التجارة الالكترونية مباشرة بعد مصادقة البرلمان على مشروع القانون، العدد02، 2017.

18. مختارات الصحف باللغة العربية: العدالة بين العصرنة والإصلاح، العدد2017،02.

19. مهد مهد الألفي، ورقة العمل حول: تشريعات مكافحة جرائم الإرهاب الإلكتروني" الأحكام الموضوعية والأنماط"، القاهرة.

20. هويدا مصطفى: دور الفضائيات العربية في تشكيل معارف الجمهور واتجاهاته نحو الإرهاب؛ دراسة ميدانية على عينة من الجمهور العربي، إتحاد إذاعات الدول العربية، جامعة الدول العربية سلسلة بحوث ودراسات إذاعية(63) تونس،2008.

21. حسين علي محسن: جريمة غسيل الأموال الإلكترونية، كلية القانون، الجامعة المستنصرية.

ب- باللغة الأجنبية:

22. Weiman, Gabriel : New terrorism and new media, Washington. D.c, Wilson centre,commons, lab, research series, Vol2.

ج- المو اقع الإلكترونية:

23. المطيري عادل عبد الله :الإرهاب الإلكتروني والأمن السيبراني، على الموقع الإلكتروني: http://alarab.qa/story/1333816 ، يوم 2019/02/12، على الساعة 16:57مساءا.

24. رشدي مراد:غسل الأموال عبر الوسائل الإلكترونية، المؤتمر العلمي الأول: حول الجوانب القانونية والأمنية للعمليات الإلكترونية، منظم المؤتمر: أكاديمية شرطة دبي ، مركز البحوث والدراسات ، 26 و28 /2003/4،دبي،الأمارات العربية المتحدة، على الموقع الإلكتروني: http://www.maher.sandroses.com/m706.htm، يوم2019/02/15،الساعة 19:47مساءا.

25. أضرار وجرائم شبكة الانترنت (Damages and Crimes of Internet) على الموقع الإلكتروني: https://vb.ckfu.org/attachments/، يوم2019/02/15،على الساعة 19:47مساءا.

26. الإرهاب الإلكتروني وطرق مواجهته،شبكة النبأ المعلوماتية،الموقع الإلكتروني:/http://m.annabaa.org.arabic/information/11123 ،يوم 2019/02/15،على الساعة 11:55مساء.

27. بن مرزوق عنترة ، حرشاوي محي الدين: الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، د.ن ،على الموقع الإلكتروني:https://manifest.univ-ouargla.dz،يوم 2019/20/21 ،على الساعة 16:55 مساءا .

28. خالد السيد: الإرهاب الدولي والجهود المبذولة لمكافحته، مركز الإعلام الأمني، على الموقع الإلكتروني: https://www.policemc.gov.bh/.، يوم 2019/02/20،على الساعة :16:45مساءا.