جامعة الأمير عبد القادر للعلوم الإسلامية ـــ قسنطينة ـــ

كلية الشريعة والاقتصاد مخبر البحث في الدراسات الشرعية

يوم دراسي:

الأمن الرقمي ومكافحة الجرائم الإلكترونية

الأستاذة/الدكتورة:

ليلى بعتاش ـــ أستاذ محاضر أ

بجامعة الأمير عبد القادر ـــ قسنطينة ـــ

Batacheleile2018@gmail.com

ط/د **إبتسام بومعزة**

تسجيل سادس تخصص: حقوق الإنسان

بجامعة الأمير عبد القادر قسنطينة

ibtissemboumaazaconstantine@gmail.com

المحور: الثالث: أثر الجرائم الإلكترونية على الأمن الرقمي

مداخلة الموسومة ب: الإرهاب الإلكتروني وأثره على الأمن الرقمي

ملخص:

أصبح الإرهاب الإلكتروني هاجسا للدول نتيجة لهجمات الإرهابيين عبر الانترنيت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وتزداد هذه المخاطر يوما بعد يوم؛لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية.

حيث سببت هذه الأخيرة أضرار جسيمة على الأفراد والمنظمات والدول، نتيجة لما تنتهجه من سياسات تخويف وترهيب عبر مواقع التواصل الاجتماعي من جهة واختراق وتجسس للمواقع الإلكترونية من جهة أخرى، مما يؤثر سلبا على الأمن الإلكتروني الداخلي للدولة محّل التعرض للهجوم.

لهذا سعت الكثير من الدول إلى اتخاذ تدابير لمواجهته وتحقيق الأمن الرقمي ممثلة في الوسائل الإلكترونية لهذا الأخير، وتدابير قانونية من بينها الجزائر بإصدارها قانون يسعى لتحقيق الأمن الإلكتروني القانون 04 ــ 09

الكلمات المفتاحية:

الإرهاب الإلكتروني، الأمن الرقمي، التشفير، الجدار الناري، البريد الإلكتروني

Abstract*:*

Cyber terrorism has become an obsession for states as a result of online terrorist attacks those who carry out their sabotage activity from anywhere in the world, this risks increase day by day; because modern technology alone is unable to protect from cyber terrorist operations.

Ase the latter caused enormous damage to individuals,organitation,and states,as a result of its policies of intimdation and intimid through social media on the hand, and hacking and espionage of websites on the other hand,this nigatively affects the internal cyber security of the country under attak.

That is why many countries have sought to take measures to confront it and achieve digital security represented by the electronic means of the latter,and legal measures,including algeria by issuing a law that seeks to achieve cyber security law 09-04

Key words : cyber terrorism,digital security,encryption,firewall,e-mail

مقدمة

مرّت الجريمة عبر مختلف المراحل التي عرفها الإنسان، وتطورت بتطوره في مختلف مجالات الحياة، وتغيرت حسب دوافعه وظروفه الاجتماعية، وذلك باختلاف الزمان والمكان، فالمجرمون استفادوا من التقدم التقني، ولاسيما و العالم اليوم يعيش في عصر ثورة المعلومات والتكنولوجيا المتطورة، لذا فمن البديهي أن تظهر أنماط من الجرائم التي لم تكن معروفة من قبل، فقد نتج عن ثورة المعلومات والتكنولوجيا المتطورة ظهور وسائل اتصالات متطورة، جعلت من العالم قرية صغيرة، ومن هذه الوسائل الانترنت التي قدمت وتقدم خدمات هائلة ومنافع عظيمة للبرية إلا أنها في الوقت نفسه وسيلة من وسائل الدمار والخراب للدول والشعوب إذا استخدمت

استخداما سيئا، فهي سلاح ذو حدين فكما يمكن أن تستخدم للمنفعة والخير، يمكن أن تستخدم للمضّرة والشر وللأسف ها هي اليوم قد استخدمت وتستخدم من قبل ضعاف النفوس في أعمال إجرامية تهدد الأمم والشعوب، فالجرائم التي ترتكب اليوم عن طريقها كثيرة ومن بينها جرائم الإرهاب الالكتروني التي برزت بشكل كبير بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكار هدامة، وتدعوا إلى نشر الفوضى والعنف والتطرف والكراهية والانقسام.

ونتيجة لهذه التطورات لم تعد الجهود الدولية عامة وسياسات الدفاع الجزائرية خاصة تقتصر على مكافحة الإرهاب من خلال الاعتماد على الطرق التقليدية بل تجاوزتها لتشمل التهديدات الجديدة التي أفرزتها الثورة التكنولوجية الحديثة وذلك من خلال العمل على تحقيق الأمن الرقمي الإلكتروني.

وهذا ما تهدف إليه هذه الورقة البحثية من خلال توضيح الأثر الذي يخلّفه الإرهاب الالكتروني على الأمن الرقمي مع تحديد أشكاله ونماذجه الجديدة التي يعتمدّ عليها لإرهاب الناس وبث الرعب والخوف في نفوسهم من خلال مواقع التواصل الاجتماعي بالتعدي على أمنهم وأمانهم، وهنا تبرز أهمية بحثي في إظهار الوسائل المعتمدّة لتامين تلك المواقع والتدابير الوطنية المتّخذة في شكل قوانين لدعم هذا الحق ألاّ وهو الأمن الرقمي.

ومن بين الأسباب التي دفعتني إلى اختيار هذا العنوان هو طبيعة تخصصي في مجال حقوق الإنسان التي تفرض عليّ ذلك، إضافة إلى خطورة هذه الظاهرة وانتشارها، وما تخلفه تكنولوجيا المعلومات من أثار سلبية على الحقوق والحريات الفردية في المجال الرقمي الالكتروني نتيجة الاستخدام السيئ لها من قبل الإرهابيين

وقد اقتضت مني طبيعة الموضوع إتباع **المنهج الوصفي** من خلال التعريف بالإرهاب الإلكتروني وذكر صوّره و مظاهر تهديده، وكذلك **المنهج التحليلي** من خلال تحليل النصوص التشريعية لحماية هذا الحق ودرء ذلك النوع من الإرهاب.

وسنحاول في هذه الدراسة تناول أثر الإرهاب الالكتروني على الأمن الرقمي مع توضيح دور هذا الأخير في التصدي له، مما تطلب منا طرح الإشكالية التالية: **ما هو أثر الإرهاب الإلكتروني على الأمن الرقمي؟**

للإجابة على ها ته الإشكالية، قمنا بتقسيم الفكرة الأساسية إلى فكرتين فرعيتين بموجب مبحثين تطرقنا إلى فكرة الإرهاب الإلكتروني أهدافه ووسائله (المبحث الأول) ودور الأمن الرقمي في مكافحة الإرهاب الإلكتروني (المبحث الثاني)، بالإضافة إلى خاتمة شملت النتائج المتوصل إليها.

المبحث الأول: الإرهاب الالكتروني أهدافه ووسائله

تعتبر جرائم الإرهاب الإلكتروني عبر الانترنيت من أخطر الجرائم التي ترتكب في الوقت الحاضر، والتي تهدد حياة الناس وأمنهم لذلك سنتناول في هذا المبحث التعريف بالإرهاب الإلكتروني وخصائصه، وأهدافه ووسائل تحقيقه.

المطلب الأول: ماهية الإرهاب الالكتروني وخصائصه

يعتبر الإرهاب من أهم القضايا الجدلية على المستوى الدولي، وذلك لعدم وجود تعريف جامع مانع له متفق عليه، نتيجة لتنوع أشكاله ومظاهره وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية حوله فما يراه البعض عملا إرهابيا، يراه الآخر عملا مشروعا، ولغاية توضيح ماهية الإرهاب الالكتروني لابد من بيان تعريف الإرهاب كما هو وارد لدى بعض الاتفاقيات الدولية والفقهاء القانونيين.

الفرع الأول: مفهوم الإرهاب الإلكتروني

لضبط مفهوم الإرهاب الالكتروني لابد لنا أن نعرج إلى مفهوم الإرهاب التقليدي لغة واصطلاحا وذلك لإسقاط مفهومه على المفهوم المراد إيجاد تعريف له ألا وهو الإرهاب الالكتروني

أولا: التعريف اللغوي.

لمعرفة مفهوم الإرهاب علينا إعادته إلى جذوره اللغوية لمعرفة استعمالاته ودلالاته[1] فهي كلمة مشتقة من اللاتينية وهي(ters) والتي تعني الترهيب والخوف والفزع[2] ويعتبر هذا الأخير مصدر أرهب يرهب إرهابا وترهيبا[3] وأصله مأخوذ من الفعل الثلاثي رهب بالكسر، يرهب رهبة ورهبا بالضم ورهبا بالتحريك أي خاف ورهب الشيء، رهبا ورهبة: خافه[4]

ثانيا: التعريف الاصطلاحي

1 ــ تعريف الإرهاب عامة.

عرّفه الفقهاء الغربيين ومنهم أنطوان "سوتيل" بأنه «العمل الإجرامي المرتكب بواسطة الرعب والتخويف للوصول إلى هدف معين»[5] بمعنى إفزاع الآخرين،[6] وهذا الهدف حسب رأي " جنكيز" هو طلب فدية، أو القيام بأفعال القتل المثيرة[7]

أمّا بالنسبة لمفهومه لدى فقهاء العرب ومنهم "البسيوني" فهو: «استراتيجية عنف محرم دوليا تحفزها بواعث عقائدية إيديولوجية، وتتوخى إحداث عنف مرعب داخل شريحة خاصة من مجتمع معين لتحقيق الوصول إلى السلطة أو للقيام بدعاية لمطلب أو لمنظمة، بغض النظر عما إذا كان مقترفو العنف يعملون من أجل أنفسهم أو

---

[1] ــ رنا مولود شاكر، مستقبل حقوق الإنسان في ظل الإرهاب دراسة حالة حقوق الإنسان في الأراضي الفلسطينية المحتلة، مجلة مركز الدراسات الفلسطينية،جامعة بغداد، العدد15، 2012، ص 262

[2]- James Dear Derain, "the Terrorist Discouerse:signs,states and system of Global policitical violencec" in word Secuirity:trends and challenges at centry's End,ed by michaelT,klare and Daniel C,Thomas,new York: ST Martin's perss,1991,p237

[3] ــ الرازي أحمد بن فارس القز ويني، مقاييس اللغة، دار الفكر، مادة رهب، ج2، ص4470

[4] أبي الفضل ابن منظور، لسان العرب، مجلد1، دار لسان العرب، بيروت، د س ن، ص 1237

[5]ــ محمد سعادي، الإرهاب الدولي بين الغموض والتأويل، دار الجامعة الجديدة، الإسكندرية، 2009، ص188.

[6] ــ عبد الرحيم صادق، الإرهاب السياسي والقانون الجنائي، دار النهضة، القاهرة، 1985، ص15

[7] ــ هبة الله أحمد خميس بسيوني، الإرهاب الدولي، منشأة المعارف، الإسكندرية، 2011، ص 48

نيابة عنها، أو نيابة عن دولة من الدول»،[1] كما عرّفه "عبد العزيز سرحان" «كل اعتداء على الأرواح والأموال والممتلكات العامة أو الخاصة بالمخالفة لأحكام القانون الدولي العام بمصادره المختلفة، بما في ذلك المبادئ الأساسية لمحكمة العدل الدولية».[2]

بناءا على التعريفات السابقة فان الإرهاب هو حدث مفاجئ وغير متوقع، منظم، غير مشروع يقوم به فرد أو جماعة ويكون عادة موجها ضد مدنيين أبرياء[3] باستخدام القوة أو العنف أو التهديد أو الترويع يلجأ إليه الجاني بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر،[4] بهدف التأثير على موقف أو سلوك مجموعة مستهدفة بغض النظر عن الضحايا المباشرين[5]

نلاحظ أنّ هذه التعريفات قد تعددت واختلفت وتباينت بين الفقهاء والقانونيين والسبب الرئيسي في ذلك هو تباين مصالح الدول وانعكاس ذلك على مفهوم الإرهاب فمثلا الولايات المتحدة الأمريكية تريد أن تدخل المقاومة المسلحة للشعوب تحت خانة الإرهاب[6] ودليل ذلك ما قام به الكيان الصهيوني باستبداله مصطلح العمل الفدائي والفدائيون الذي أطلق على اللذين قاموا بالثورة الفلسطينية آنذاك بمصطلح المخربين أو العمل التخريبي لكن هذا الأخير لم يلقى انتشارا على المستوى العالمي بما يتناسب والمطامح الصهيونية فتمّ استبدالها بمصطلحات أخرى هي" العمل الإرهابي" والإرهاب وما يشتق منهما[7]

2 ــ تعريف الإرهاب الالكتروني.

بعد تطرقنا لمفهوم الإرهاب التقليدي والذي كان محّل خلاف بين الفقهاء القانونيين والمنظمات الدولية، نستخلص أنّ الإرهاب الإلكتروني هو: «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 الإفساد» فهذا الأخير يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم[8] فهو يعدّ شكل من أشكال الجرائم المستحدثة، وتوصف بالمستجدة

---

[1] ــ مجمع الفقه الإسلامي، الإرهاب والسلام، ط1، دار الكتب العلمية، بيروت، 2007، ص 18.

[2] ــ حمدان رمضان محمد، الإرهاب الدولي وتداعياته على الأمن والسلم العالمي دراسة تحليلية من منظور اجتماعي، مجلة أبحاث كلية التربية الأساسية، المجلد11، العدد1، 2011، ص 271

[3] ــ محمد مسعود قيراط، الإرهاب دراسة في البرامج الوطنية واستراتيجيات مكافحته مقاربة إعلامية،ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص64

[4] ــ محمد محي الدين عوض، واقع الإرهاب واتجاهاته، الرياض، جامعة نايف للعلوم الأمنية والعربية، الرياض، 1999، ص12

[5] ــ زينب علي عبد، الإرهاب فساد حقوق الإنسان وكرامته ــ دراسة تحليلية، مجلة أهل البيت، العدد18، ص 415

[6] ــيوسف محمد صادق، الإرهاب والصراع الدولي، دار سردم للطباعة والنشر، 2013، ص28

[7] ــ عبد الرحمان عمار، قضية الإرهاب بين الحق والباطل، منشورات اتحاد الكتاب العرب، دمشق،2003، ص34

[8] ــ رفد عيادة الهاشمي، الإرهاب الإلكتروني، ص7، على الرابط: https://drive.googl.com بتاريخ2020/4/29، عل الساعة 11:45

لأنها تبتكر أدوات وأساليب جديدة في تنفيذها باستخدام التكنولوجيا الحديثة التي تحررها من الأبنية الاجتماعية التي نشأت فيها، وتدويلها سواء فيما يتعلق بالتخطيط أو التمويل أو التنفيذ والأهم من ذلك ضحايا الجريمة الإرهابية في الوقت الراهن، الأمر الذي يصعب من إجراءات متبعاتها.[1]

و على ما سبق، فإن الإرهاب الالكتروني هو استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.[2]

الفرع الثاني: خصائص الإرهاب الالكتروني

يتميز هذا الأخير بعددٍ من السمات التي يختلف فيها عن سائر صور الإرهاب والجريمة والتي تتمثل في أنّه:

ـــ عمل عدائي غير مشروع من حيث الوسائل المستخدمة والأهداف المنشودة، إذ يشتمل على تطوير وإرسال شفرات الحاسب الآلي إلى الشبكة الدولية للمعلومات بغية تحقيق أغراض عدة تتمثل بالتدمير وإفساد للمعلومات أو البرامج الموجودة، أو التهديد بإيقاع الضرر بصورة تخالف كل القوانين والمواثيق والاتفاقيات الدولية والقيم الأخلاقية وحتى الدينية.

ـــ جرائمه تتميز بالنعومة، فهي لا تحتاج في ارتكابها إلى العنف والقوة ولا أثر فيها لأيّ دماء، وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من دليل السجلات المخزونة في ذاكرة الحاسبات الآلية ؛ كما أنها سهلة التنفيذ ،لا تحتاج إلى وقت ولا إلى جهد.(3).

ـــ يعتمد على خبرات وقدرات ذهنية عالية في استخدام الحاسوب واختراق أنظمة الحماية المتوافرة .[4]

ـــ يتسم بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود أو مسرح واحد إذ يمكن أن يستهدف الفاعل أماكن وأهداف متفرقة في وقت واحد،[5] حيث أن الجريمة المعلوماتية تخطت حدود الدولة التي ترتكب فيها لتتعدى أثارها إلى كافة البلدان على مستوى العالم.[6]

ـــ صعوبة اكتشاف جرائم الإرهاب الإلكتروني أو مصدرها أو القائم بها أو حتى إثبات الدليل على حصولها أو حصر وتحديد حجم الضرر الناجم عنها[7].

---

[1] ـــ معتز محي عبد الحميد، الإرهاب وتجدد الفكر الأمني، ط1، دار زهران، الأردن، 2014، ص13

[2] ـــ بن يحي الطاهر ناعوس، مكافحة الإرهاب الالكتروني ضرورة بشرية وفريضة شرعية، بحث منشور على شبكة الألوكة، ص6، على الرابط التالي: www.alukah.net، بتاريخ: 2020/4/29،على الساعة: 11:25،

[3] ـــ مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، مجلة العلوم القانونية والسياسية، جامعة ديالى، المجلد الثالث، العدد الأول ، 2014 ، ص 343 .

[4].عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ـــ دراسة مقارنةـــ، منشأة المعارف ، الإسكندرية ، بلا سنة طبع ، ص 33

[5]ـــ جلال محمد الزغبي وأسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2010، ص 91.

[6] ـــ مشتاق طالب، مصدر سابق، ص 347.

[7] ـــ محمود الرشيدي، العنف في جرائم الانترنت، الدار المصرية اللبنانية، القاهرة، 2011، ص 38-39.

المطلب الثاني: أهداف الإرهاب الالكتروني ووسائل تحقيقه

إن الجماعات الإرهابية هي من أكثر الفئات استخداما للتقنيات الحديثة، والأكثر استغلالا لمعطيات التكنولوجيا ابتداء من نشرهم لفكر الإرهاب وتمجيده، وصولا إلى استخدامهم كل الوسائل والأساليب الممكنة في عملياتهم الإرهابية، مستخدمين في عملهم هذا وسائل التواصل الاجتماعي ومواقع الانترنيت والبريد الالكتروني لتحقيق أهدافهم الضالة عبر الشبكة العالمية للمعلومات. وهذا ما سنوضحه في الفرعين التاليين:

الفرع الأول: أهداف الإرهاب الإلكتروني

مما لاشك فيه أن وراء كل فعل سواء كان يحمل في طياته جانب الخير أم الشر إلا وخلفه غرض أو غاية، والفعل الإرهابي ألمعلوماتي شأنه شأن أهداف الإنسان الأخرى، يسعى إلى تحقيق عدد من الأهداف ومنها الغير مشروعة،[1] ويمكن الإشارة إلى أهم تلك الأهداف وفق الآتي:

ـــ نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة

ـــ الإخلال بالنظام العام والآمن المعلوماتي وزعزعة الطمأنينة

ـــ تعريض سلامة المجتمع وأمنه للخطر

ـــ إلحاق الضرر بالبني المعلوماتية الأساسية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة

ـــ تهديد السلطات العامة والمنظمات الدولية وابتزازها

ـــ الدعاية والإعلان وجذب الانتباه وإثارة الرأي العام

ـــ جمع الأموال والاستيلاء عليها[2]

ـــ الإخلال بالنظام العام والآمن المعلوماتي، وزعزعة الطمأنينة، وتعريض سلامة المجتمع وأمنه للخطر[3]

الفرع الثاني: وسائل الإرهاب الالكتروني

من أكثر وسائله شيوعا هو استخدام الجماعات الإرهابية للبريد الالكتروني بهدف نشر أهدافها وثقافتها وتجنيد أعضائها، بالإضافة إلى إنشاء مواقع خاصة بهذه الجماعات على الانترنيت لخدمة أهدافها وتحقيق أغراضها، إلى جانب نشاطات التنظيمات الإرهابية في مجال تدمير المواقع الالكترونية الرسمية منها وغير الرسمية خدمة لأهداف هذه التنظيمات وهذا ما سأتناوله باختصار تباعا فيما يلي

أولا: البريد الالكتروني

---

[1] ـــ جعفر حسن جاسم الطائي، الإرهاب ألمعلوماتي وآليات الحد منه، مجلة العلوم القانونية والسياسية، جامعة ديالي، عدد خاص، كلية القانون والعلوم السياسية، ص498

[2] ـــ حسنين شفيق، الإعلام الجديد والجرائم الالكترونيةـــ التسريبات، التجسس، الإرهاب الالكتروني، دار فكر وفن، 2014، ص190،191

[3] ـــ عبد القادر الشيخلي، طبيعة الإرهاب الإلكتروني، الملتقى الدولي الموسوم ب مكافحة الإرهاب، رابطة العالم الإسلامي، مكة المكرمة، فبراير 2015، ص8

يعدّ البريد الالكتروني من أهم الوسائل المستخدمة في الإرهاب الالكتروني وذلك من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي حدثت كان البريد الالكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها، ويستغل الإرهابيون البريد الالكتروني أسوأ استغلال أيضا من خلال قيامهم بنشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الالكترونية[1]

ثانيا: إنشاء المواقع الإرهابية على الانترنيت

يتم بث ثقافة الإرهاب عبر الانترنيت عن طريق تأسيس مواقع افتراضية تمثل المنظمات الإرهابية، وهي مواقع آخذة في الازدياد مع ازدياد المنظمات الإرهابية،[2] حيث تتيح هذه المواقع للجماعات الإرهابية قدرا كبيرا من التحكم في المعلومات والرسائل الإعلامية التي تريد توجيهها،[3] فهي تستخدم وسائط الكترونية خاصة بها، فهي لا تستخدم جوجل، لكنها تستخدم ما يطلق عليها وسائط الكترونية سوداء.[4]

وذلك بهدف تجنيد عناصر إرهابية جديدة من خلال الانترنت تساعدهم على تنفيذ أعمالهم الإجرامية، وهم في ذلك يعتمدون على فئة الشباب، خصوصا ضعاف العقل والفكر، فتعلن الجماعات الإرهابية عبر مواقعها على الانترنت في حاجتها إلى عناصر انتحارية كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني، فدائما ما تصف الأهداف التي تستهدفها عملياتهم بالكافرة، وتقوم بدعوى الشباب للجهاد وحثهم على الاستشهاد في سبيل الله والفوز بالجنة[5]

كما تسعى أيضا إلى الدعاية والترويج في نشر معلومات بهدف شن حرب نفسية ضد أعدائها، وهو ما يتحقق من خلال نشر معلومات مضللة أو مغلوطة، نشر تهديدات وصور ولقطات فيديو مرعبة (مثل مواد الفيديو التي تصور احتجاز الرهائن المختطفين من قبل الجماعة)[6]

ثالثا: تدمير المواقع والبيانات والنظم المعلوماتية

---

[1] ــأيسر محمد عطية القيسي، دور الآليات الحديثة للحد من الجرائم المستحدثة ــ الإرهاب الإلكتروني وطرق مواجهته ــ الملتقى الدولي الموسوم ب الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المملكة الأردنية الهاشمية، عمان، 2 ــ 2014/9/4، ص15

[2] ــ محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، 2012، على الموقع التالي: www.Nashiri.net

[3] - Debray stéphane, internet face aux substances illicties:complice de la cybercriminalité ou outil de prevention?,DEES media électronique and internet,University de paris8,2002-2003, p13

[4] ــ نبيل السمالوطي، الكتائب الإلكترونية وصناعة الإرهاب ــ التشخيص وأساليب المواجهةــ العدد21، يونيو2018، ص 30

[5] ــ محمد سيد سلطان، مرجع سابق

[6] ــ مها عبد المجيد صلاح، استراتيجيات الاتصال في مواقع الجماعات المتطرفة على شبكة الانترنيت دراسة تحليلية، الندوة العلمية الموسومة باستعمال الانترنيت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 2010، ص 12

تقوم التنظيمات الإرهابية بشن هجمات الكترونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية، وإلحاق الضرر ببنية المعلوماتية التحتية وتدميرها وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاث أهداف أساسية غالبا وهي: العسكرية والسياسية والاقتصادية[1]

ولا يهدف التدمير هنا إلى مجرد الحصول على منفعة النظام ألمعلوماتي أيا كان شكلها ولكن يبقى ببساطة إحداث ضرر بالنظام ألمعلوماتي وإعاقته عن أداء وظيفته،[2] مثال على ذلك ما فعله "ماريو كاستلو" بتخطيه الحاجز الأمني المسموح له والدخول على أحد أجهزة المكتب[3]

المبحث الثاني: دور الأمن الرقمي في مكافحة الإرهاب الإلكتروني.

بعدما أصبحت الحروب حرب معلومات جيوشها الدخلاء والقراصنة والهواة والجواسيس، فقد تمّ استبدال البيانات بالرصاص والصفر والواحد، والجندي بالدخلاء والمتسللين والجواسيس، الذين يسعون إلى وضع المجتمع في حالة فوضى بتدميرهم وتعطيلهم للبنى التحتية للمعلومات الحساسة كتهديد إرهابي لهم بشتى أشكاله (فرع أوّل)

مما استدعى هذا اهتمام الحكومات بتوفير سبل فعالة ضد التجسس الإلكتروني، وخرق الدخلاء لنظم المعلومات بتغيير المفاهيم الأمنية وحلّت محلّها مفاهيم أمنية معلوماتية تتماشى مع البناء التحتي المعلوماتية (فرع ثاني)

المطلب الأول: مظاهر تهديد الإرهاب الإلكتروني وأثره على الأمن الرقمي

نتيجة للهجمات التي يمارسها الإرهابيون عبر مواقع التواصل الاجتماعي، باستخدامهم لأساليب ووسائل متعددة واختراقهم للأمن الرقمي الإلكتروني مما يؤثر سلبا على هذا الأخير وهذا ما سنوضحه في الفرعين التاليين

الفرع الأول: مظاهر تهديد الإرهاب الإلكتروني

للإرهاب الالكتروني تداعيات مختلفة من بينها أنه:

1ـــ تهديد أمني سياسي: تعمل المنظمات الإرهابية على إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو تعطيل أنظمة الدفاع الجوي، إضافة إلى اختراق البريد الالكتروني لرؤساء الدول وكبار الشخصيات السياسية، واختراق المواقع الالكترونية لنشر رسائل مضللة ففي عام 2010 قام "ويكيليكس" بتسريب وثائق تحوي معلومات سرية متداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم

2 ـــ تهديد اقتصادي: اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك أسواق المال، وتعطيل عمليات التحويل المالي، وإلحاق الأذى بالاقتصاد الوطني، ومن أمثلتها قيام الإرهابيين بتحويل ملايين الدولارات من

---

[1] ـــ حسنين شفيق، مرجع سابق، ص198

[2] ـــ بوكثير خالد، الجرائم المعلوماتية، مذكرة نهاية التدريب مقدمة للمنظمة الجهوية للمحامين، سطيف 2005، 2006، ص12

[3] ـــ محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، ج2، مركز الإعلام الأمني، دبي، 2010، ص10

بعض الحسابات الشخصية لكبار العملاء بعد اختراق نظام التحويلات الدولي بين البنوك، وقيام بعض الهاركز المحترفين بسرقة بيانات بطاقات الائتمان من بعض أكبر مراكز التسوق الالكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقات لتوفير تمويل لأعمالها الإرهابية في الدول التي تمّ بيع السندات فيها

أكدت شركة " كاسبرسكي" الرائدة في مجال الأمن ألمعلوماتي أن مجموعة من الهاركز تمكنوا من السيطرة على حسابات في مصارف عالمية وسرقوا نحو مليار دولار.

3 ــ تهديد اجتماعي: توجه المنظمات الإرهابية رسائلها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول، فهي تعرض أفلام مرعبة للرهائن والأسرى أثناء إعدامهم مما يؤثر على المدنيين نفسيا.[1]

الفرع الثاني: أثر الإرهاب الإلكتروني على الأمن الرقمي.

نتيجة الاختراقات التي يقوم بها الإرهابيون على المواقع الالكترونية باستخدامهم وسائل مختلفة والتي سبّق ذكرها بهدف تحقيق غاية محددة وأهمها تهديد أمن الدولة بشتّى الأنواع كما ذكرت سابقا مما يخلف أثارا سلبية على حق الأمن الرقمي الإلكتروني وذلك من خلال:

ــ تدمير المواقع بضخ مئات الآلاف من الرسائل الكترونية من جهاز الحاسوب الخاص بالمعتدي إلى الموقع نتيجة لضعف الكلمات السرية المستخدمة وعدم وضع برامج حماية كافية لحماية المواقع من الاختراق والتدمير.

ــ تشويه المواقع: عن طريق تغيير الصفحة الرئيسية للموقع بصفحة أخرى يعلن المخترق فيها انتصاره[2]

ــ انعدام الشعور بالأمن الالكتروني وعدم الطمأنينة والخوف في مجال الحياة العادية نتيجة حالة القلق الدائم التي يعيشها الفرد حيث لا يدري متى سيصيبه الخطر الناتج عن الإرهاب الالكتروني.

ــ نشر فيروسات من اجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية مما يؤثر على شعبية رجال الأمن الالكتروني والمسئولين عنه والنيل من سمعتهم وفقدا الثقة بالقوانين والأنظمة التي تنظم الأمن الالكتروني وتساهم في تحقيقه في المجتمع

ــ تعمل الجماعات الإرهابية عبر الوسائل الالكترونية إلى التحكم بالأنظمة الأمنية من خلال فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية والأسلحة الفتاكة وتعطيل مراكز القيادة

---

[1] ــ سليم دحماني: أثر التهديدات السيبيرانية على الامن القومي الولايات المتحدة الأمريكية أنموذجا (2001، 2017)، المسيلة: جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، 2017، 2018، ص: 47، 48

[2] ــ ليتيم فتيحة، ليتيم نادية: الأمن ألمعلوماتي للحوكمة الالكترونية وإرهاب القرصنة، بسكرة: مجلة المفكر، جامعة محمد خيضر، العدد 12، ص: 246، 247

والسيطرة العسكرية ووسائل الاتصال يهدف عزلها عن القوات وعبثها بالنظم العسكرية واستخدامها بتوجيه الجنود إلى نقطة غير آمنة قبل قصفها وتفجيرها[1]

ومن الأمثلة التطبيقية على الآثار الأمنية ما قامت به مجموعة "سايبر بيركوت" الأوكرانية في 2014 عندما قامت بمهاجمة المواقع الالكترونية لحلف الناتو مما أدى إلى تعطيل مواقع الحلف لعدة ساعات وأقر مفتش وحدة الجرائم السيبيرانية الأمريكي في أوت 2014 بأن قراصنة أجانب تكنوا من اختراق حسابات تابعة لهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية[2]

المطلب الثاني: سبل مواجهة الإرهاب الالكتروني وتحقيق الأمن الرقمي في الجزائر

بعد تطرقنا لمظاهر الإرهاب الالكتروني وما يخلفه من أثاره سلبية على الأمن الإلكتروني نسعى إلى مكافحة هذه الجريمة والتصدي لها باستخدام وسائل الأمن الرقمي ومن هنا يتبادر إلى ذهننا طرح التساؤل التالي: هل يمكن تفادي هذه المخاطر والأضرار؟ وما هي الوسائل التي يمكن عن طريقها تجنب حدوث مثل هذه الاختراقات؟ وهذا ما سنناقشه في العناصر التالية.

الفرع الأول: وسائل الأمن الرقمي ودورها في مكافحة الإرهاب الإلكتروني

نتيجة للتطور المسجل في وسائل ارتكاب الجريمة المعلوماتية وتنوع الوسائل التي قد يلجأ إليها المجرمون أصبحت تلك التقنيات غير كافية خاصة إذا قام المجرمون باستخدام طرق أخرى كاختراق الحسابات، لذا سعى العاملون في الميدان الالكتروني على ابتكار وسائل حديثة لحماية امن وسرية المراسلات والمعلومات عن طريق:

أولا: برامج مكافحة الفيروسات:

هي من أهم وسائل الحماية، حيث تقوم بمنع دخول الفيروسات على النظام، واكتشافها قبل حدوث ضرر، ومن ثم القضاء عليها، فضلا عن قيامها بتحديث نفسها بشكل آلي عن طريق الانترنيت لتزيد من كفاءتها وقدرتها على مكافحة الفيروسات الجديدة بالرغم من قدرة برامج مكافحة الفيروسات على التعرف على الفيروسات المعروفة وإزالتها من النظام، إلا أن الفيروسات تنشأ وتتطور يوميا لذلك يجب، تحديث برامج مكافحة الفيروسات بصفة دورية ومستمرة لكي تتمكن من التعرف على الفيروسات الجديدة والقضاء عليها.

تقوم بعملها عن طريق البحث عن الفيروسات المعرفة باستخدام تقنية البحث، ومحاولة الكشف عن الفيروسات غير المعروفة لبرنامج معين من خلال تقنية تفحص السلوك، وأخيرا مراقبة جميع الملفات الموجودة على الجهاز لرصد أي تغيير يحدث من خلال تقنية اختبار التكامل، وذلك ببناء سجل يتضمن أسماء جميع

---

[1] ـــ شاشوة ياسمينة: الإرهاب الالكتروني بين مخاطره واليات مكافحته، مذكرة ماستر، البويرة، جامعة آكلي محند أولحاج، كلية الحقوق والعلوم السياسية ص: 62، 63

[2] ـــ هاجر حسونة: الارهاب الالكتروني هل يتحول الى مصدر التهديد الاول في العالم، على الرابط:
http://alkhaleejonline.net/articles بتاريخ 2021/3/29 على الساعة 2.15

الملفات الموجودة على الكمبيوتر إضافة إلى أحجامها وتواريخ إضافتها، ومتابعة أي تغير أو نشاط غريب يصدر عنها[1]

ثانيا: تشفير[2] البيانات

عملية قديمة استعملت لإرسال رسائل القادة العسكريين خلال الحروب بكل أمان[3] بحيث ثبت استخدامه منذ حوالي عام قبل الميلاد لحماية الرسائل السرية[4] فهو فن لحماية المعلومات عن طريق تحويلها إلى رموز معينة غير مقروءة لا يمكن حلها إلا من خلال مفتاح سري يقوم بتحويل تلك الرموز إلى نص عادي مقروء.[5]

فهو يعتبر أفضل تقنية لحماية البيانات والمعلومات المرسلة عبر الشبكات[6] في مجال توفير الأمن وسلامة وسرية المعلومات والمعاملات والصفقات،[7] من قبّل المتخصصون بأمن المعلومات فهم يسعون لتأمين سرية الرسائل الالكترونية وسرية البيانات المتناقلة،[8] باستخدام الشبكة الافتراضية الخاصة أو نظام "نت سكيب"

---

[1] ـــ خديجة حامي: الأنظمة المعلوماتية في مواجهة القرصنة والتخريب (المخاطر المحدقة والحلول الناجعة)، مداخلة ألقيت بالملتقى الوطني: الأمن المعلوماتي مهدداته وسبل الحماية، تيزي وزو: جامعة مولود معمري، كلية الآداب واللغات، 3،4/ نوفمبر 2015، ص: 49

[2] ـــ التشفير يتكون من ثلاثة عناصر مترابطة وهي:

ـــ المعلومات التي سيتم تشفيرها

ـــ خوارزمية التشفير التي ستطبق على المعلومات، وخوارزمية فك التشفير التي تعيدها إلى حالتها الأصلية.

ـــ المفتاح وهي سلسة أو أكثر من الرموز تستند إلى صيغ رياضية معقدة في شكل خوارزميات[عقوني محمد، بلمهدي إبراهيم: الآليات التقنية والقانونية لحماية التوقيع الالكتروني، مجلة المفكر، بسكرة: جامعة محمد خيضر، العدد18، فيفري 2019، ص: 303]

[3] ـــ محمد السعيد رشدي: التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الإثبات، الإسكندرية: منشأة المعارف، 2008، ص: 58

[4] ـــ أول استخدام للتشفير يعود إلى قبل أربعة عشر سنة تقريبا، فقد استخدم المصريون القدماء التشفير كعلامة لتزيين قبور الملوك، ألا إن غايتهم من التشفير لم تكن حماية سر معين وإنما كنوع من الفخامة والقدسية لقبور الملوك، هذه البداية الأولى البسيطة لاستخدام التشفير ثم ستخدم لنقل عباراتهم العسكرية واستخدمه أيضا الحكام في الهند للتواصل مع جواسيسهم، ومع توالي الحضارات تطورت طرق التشفير فقد استعمل الرومانيون آليات متعددة للتشفير ككتابة النص على ورقة على قطعة من الخشب ذات قطر معين، ولكي يفتح النص يجب إعادة لف الورقة على قطعة من خشبية قطرها مساو لقطر الخشبة الأولى، وقد شهد علم التشفير تطورا ملحوظا مع اختراع الكهرباء وأجهزة التلغراف والبث اللاسلكي، وفي الحربين العالميتين الأولى والثانية كان للتشفير دول فعال إذ استخدمته الدول التي خاضت الحرب لضمان عدم تسرب المعلومات السرية إلى العدو، وفي المقابل سعت الدول إلى كسر رموز التشفير لكشف خطط العدو العسكرية، ويشكل التشفي في وقتنا الحاضر حربا باردة بين الدول العظمى كالولايات المتحدة الأمريكية، وروسيا والصين، إذ تسعى هذه الدول إلى كسر شفرات السفن الحربية والأقمار الصناعية التجسسية، ومع دخول العالم عصر تكنولوجيا المعلومات والاتصالات وابتداع شبكة الانترنيت واستخدامه في نقل البيانات، فقد استخدم التشفير للمحافظة على سرية البيانات وحمايتها من تطفلات الغير. [لالوشي راضية: أمن التوقيع الإلكتروني، رسالة ماجستير، تيزي وزو: جامعة مولود معمري، كلية الحقوق والعلوم السياسية، 2012، ص: 97، 92

[5] ـــ هداية بوعزة، يوسف فتيحة: الحماية التقنية للمعلومات ودورها في تأمين نظام الدفع الإلكتروني، مرجع سابق، ص: 30

[6] ـــ وسيم شفيق الحجار: الإثبات الإلكتروني، بيروت: المنشورات الحقوقية، 2002، ص: 198

[7] ـــ طوني ميشال عيسى: التنظيم القانوني لشبكة الانترنيت ـــ دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، بيروت: المنشورات الحقوقية، 2001، ص: 197

[8] ـــ أمال قارة – حماية الجزائية للمعلوماتية في التشريع الجزائري– دار هومة الطبعة الأولى 2006 ص 21.

للتأمين أو نظام بروتوكول الاتصال الآمن أو نظام تأمين المعاملات الالكترونية.[1] وذلك إمّا باستعمال تقنية التشفير المتماثل يعمل بواسطة مفتاح واحد يعرف بالخصوصي يمتلكه كل من مرسل الرسالة ومتلقيها حيث يتم الاتفاق بين طرفي العلاقة في البداية على كلمة المرور ليتم استخدامها في التشفير وفك التشفير التي تم إعدادها أو عن طريق التشفير غير المتماثل حيث يستعمل مفتاحين سريين مختلفين من اجل فك تشفيرها، الأول خصوصي يملكه مستخدم معين لمستعمل الوسائط الالكترونية ويبقيه سريا وخاصا به، أما الثاني عمومي يوزعه إلى المتعاملين الآخرين الذي يود تلقي رسائل مشفرة منهم[2].

ثالثا: الجدار الناري

هو مجموعة أنظمة تُوّفر سياسات أمنية بين الانترنيت والشبكة أو الخروج منها تمر من خلال الجدار الناري الذي يصد المستعملين غير المرغوب فيهم، فهذا الأخير يقوم بالتحقق من صلاحية المستعمل المحلي والمستعمل الخارجي، ونظام الدخول والخروج، وتشفير المعلومات، وإجراءات الحماية من الفيروسات.[3]

ويعتبر أكثر الطرق فاعلية، ومن أهم مزاياه توفير الحماية اللازمة للشبكة والمعلومات، توفير خدمات التشفير في تكنولوجيا الجدار الناري، تخزين العمليات والمعلومات التي تمر من طريق الجدار الناري، متابعة المستخدمين للشبكة ومن يحاول العبث بها[4].

رابعا : استخدام عناوين بريد الكتروني

وهذا الحل يعتبر من أسهل الحلول لمشكلة خصوصية البريد الالكتروني، فالكثير من المنتديات والمواقع تتطلب التسجيل لكي تستطيع التصفح عليه، وعند التسجيل ببريدك الإلكتروني الأساسي فيكون احتمال سرقته وانتهاك الخصوصية كبير، لذلك يمكن استخدام عناوين البريد الإلكتروني التي يمكن لتخلص منها بسهولة.[5]

الفرع الثاني: الجهود الجزائرية المبذولة في الأمن السيبيراني (الالكتروني) والوقاية من الإرهاب ومكافحته بين الواقع والأفاق

---

[1] ــ محمد أمين الرومي: التعاقد الالكتروني عبر الانترنيت، مصر: دار المطبوعات الجامعية، ط1، 2004، ص: 32، 33، 34

[2] ــ عقوني محمد، بلمهدي إبراهيم: الآليات التقنية والقانونية لحماية التوقيع الالكتروني، مرجع سابق، ص: 305، 306

[3] ــ عبد الرحمان بن عبد الله السند: الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات (الانترنيت)، ط1، بيروت: دار الوراق، 2004، ص: 297

[4] ــ عبد الرحمان بن عبد الله السند: مرجع سابق، ص: 297

[5] ــ محمد سيد سلطان: قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، دار ناشري: 2012، ص: 26

بناءا على واجب الدولة في الوقاية من الجرائم الرقمية وحماية أمنها وسيادتها فقد نظمّ المشرع الجزائري بموجب القانون 09 ــ 04[1] مجموعة من الهيئات والآليات التقنية الرقابية لتعزيز آليات حق الإنسان في الأمن الرقمي والتي تتمثل في:

1 ــ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

تتشكل من لجنة مديرة وثلاث مديريات ومركز للعمليات التقنية، وملحقات جهوية،[2] تتمتع بالشخصية المعنوية والاستقلال المالي،[3] تقوم بتنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية[4] كما تساهم في مساعدة السلطات القضائية ومصالح الشرطة القضائية، في التحريات التي تجريها بشأن مرتكبيها،[5] وذلك بهدف تحقيق وتطوير الآمن السيبيراني الرقمي.[6]

2ــ مصلحة الدفاع السيبيراني ومراقبة امن الأنظمة: بهدف حماية مؤسسات الدولة والجيش من أي مخاطر وتهديدات سيبيرانية، باعتبارها جهاز توجيهي وخبراتي على المستوى الاستراتيجي.[7]

4ــ إنشاء مراكز للوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني: بهدف تأمين منظومة المعلومات لخدمة الأمن المعلوماتي الرقمي، يعمل على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تامين الأنظمة المعلوماتية والحفاظ عليها، واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لإفرادها والملتقيات الدولية والوطنية وتبادل خبرات مع الدول الأخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، وهذا من اجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها، وقد استطاع المركز من معالجة أزيد من 100 جريمة الكترونية في 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، منها 300

---

[1] ــ المرسوم الرئاسي 15 ــ 261، المؤرخ في 8/أكتوبر/2015، **يحدد تشكيل وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها**، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد53، المؤرخ في 2015/10/8

[2] ــ المادة 6 من المرسوم الرئاسي 15 ــ 261 مؤرخ في 8/10/ 2015، يحدد **تشكيلة وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها**، الجريدة الرسمية، العدد53، صادرة في 2015/10/8،

[3] ــ المادة 2 من المرسوم الرئاسي رقم 15ــ 261، سبق ذكره

[4] ــ المادة 14 من القانون 09ــ 04 **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال**، قانون سابق ذكره.

[5] ــ المادة 4 من المرسوم الرئاسي 15 ــ 261، سبق ذكره

[6] ــ جمال بوازدية: **الاستراتيجية الجزائرية في مواجهة الجرائم السيبيرانية " التحديات والأفاق المستقبلية**، مجلة العلوم القانونية والسياسة، المجلد 10، الوادي: جامعة حمه لخضر، العدد1، 2019، ص: 1281 ــ 1282

[7] ــ يوسف بوغرارة: **الأمن السيبيراني الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيراني**، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، المجلد1، العدد3، 2018، ص: 114

جريمة تتعلق بمواقع التواصل الاجتماعي "فايسبوك"، و20 جريمة رقمية تعلقت باختراق مواقع رسمية لمؤسسات خاصة وعامة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات[1].

نظرا لكون الآليات التقنية السابقة الذكر لوحدها لم تعد كافية لضمان آمن مختلف الأنظمة المعلوماتية تدخل المشرع الجزائري بعدّة خطوات تشريعية من نوع خاص تهدف لتكوين مؤسسات عامة انطلاقا من سنة 2009 إلى غاية سنة 2020 بموجب المرسوم الرئاسي رقم 20 ــ 05 والمتمثلة أساسا في:

4ــ المجلس الوطني لأمن الأنظمة المعلوماتية[2]: يعد أحد العناصر المكونة للمنظومة الوطنية لأمن الأنظمة المعلوماتية يترأسه وزير الدفاع الوطني أو ممثله يمكن أن يستعين المجلس بأي شخص او مؤسسة من شأنه تنويره في إعماله[3] وتتلخص مهامه في:

ــ البث في العناصر الاستراتيجية الوطنية لأمن الأنظمة من قبل الوكالة وتحديدها.

ــ دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليها

ــ دراسة التقارير المتعلقة بالاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها

ــ الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال الأنظمة المعلوماتية

ــ الموافقة على سياسة التصديق الالكتروني للسلطة الوطنية للتصديق الإلكتروني

ــ اقتراح سلامة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة، ويبدي المجلس رأيه في أي مشروع بنص تشريعي، أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية، يترأس المجلس الوطني، ووزير الدفاع أو ممثله من رئاسة الجمهورية ممثل عن الوزير الأوّل، المكلف بالشؤون الخارجية، الوزير المكلف بالطاقة، المكلف بالتعليم العالي، ضف إلى الاستعانة بأي شخص أو مؤسسة من شأنه تنوير المجلس في أعماله[4].

6ــ إنشاء الوكالة المختصة في أمن الأنظمة المعلوماتية: مقرها الجزائر العاصمة هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي[5] تتميز بعدّة مهام حدّدها القانون كالتالي:

ــ تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس

ــ تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس

---

[1] ــ بارة سمير: **الأمن السيبيراني في الجزائر السياسات والمؤسسات**، المجلة الجزائرية للأمن الإنساني، باتنة: جامعة باتنة1 الحاج لخضر العدد4، جويلية 2017، ص: 270

[2] ــ المرسوم الرئاسي المؤرخ في 2020/1/20 **يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية**، الجريدة الرسمية، عدد04، صادر بتاريخ 2020/1/26، ص: 5 ــ 10

[3] ــ المادة 5 من المرسوم الرئاسي رقم 20 ــ 05

[4] ــ عبد الصدوق خيرة، بولغاب آمال: **الإطار القانوني لأمن المعلوماتي**، مجلة البحوث في الحقوق والعلوم السياسية، تيارت: جامعة بن خلدون، المجلد7، العدد2، 2021، ص: 378

[5] ــ مرسوم رئاسي رقم 20ــ 05 السابق ذكره

ـــ الاحترافية في مجال المعلوماتية من طرف قانونيين وفنيين في نفس الوقت.

ـــ توفير أكبر قدر من الدراية المعلوماتية والأمن المتعلق بها.

ـــ محاولة تفادي الهفوات المتعلقة بالأمن المعلوماتي خاصة المواقع الحكومية.

ـــ إدخال الطرق التقنية الحديثة في تثبيت الأمن المعلوماتي من خلال البرمجيات الحمائية لصد هجمات الهاكر.

ـــ نظرا لتعقيدات متعلقة بالأمن المعلوماتي على الدولة تكوين كوادر وإطارات فنية رفيعة المستوى لتغطية الأمن المعلوماتي[1].

7ـــ **إنشاء هيئات قضائية جزائية متخصصة** تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني حسب المادة 15 من القانون رقم09/04[2].

ولابدّ من منح صلاحية التحري في الجرائم المعلوماتية التي تمس الجيش الوطني الشعبي للمصلحة المركزية للشرطة القضائية لأمن الجيش وفقا للمرسوم الرئاسي رقم 21 ـــ 284[3] الذي يتضمن وضع أحكام هذه المنظومة وتنظيم سير هياكلها.[4]

8ـــ إنشاء معهد وطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: يقوم بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية أو ضباط الشرطة القضائية أو السلطات المؤهلة، قانونيا خاصة أثناء معالجة القضايا المعقدة.

إضافة إلى الإسهام في تنظيم دورات الإتقان والتكوين ما بعد التدّرج في تخصص العلوم الجنائية، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الاجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها مصلحة البصمات، مصلحة البيئة أما فيما يخص مجال الأمن السيبيراني هناك مصلحة الإعلام

---

[1] ـــ عبد الصدوق خيرة: المرجع السابق، ص: 379

[2] ـــ إسماعيل جابوربي: **دور الأمن السيبيراني في مواجهة التهديدات الإلكترونية دراسة حالة الجزائر**، مجلة تحولات، ورقلة: جامعة قاصدي مرباح ورقلة، 2020، ص: 77

[3] ـــ المرسوم الرئاسي رقم 21 ـــ 284، المؤرخ في 13 يوليو 2021، يعدّل ويتمم المرسوم الرئاسي رقم 19 ـــ 179 المؤرخ في 2019/7/19، **المتضمن إحداث مصلحة مركزية للشرطة القضائية لأمن الجيش ومهامها وتنظيمها**، الجريدة الرسمية، عدد56، صادر بتاريخ18/7/ 2021، ص6

[4] ـــ نو عبد الله: **حرية التعبير والإعلام الرقمي في القانون الجزائري ـــ بين المنظور الحقوقي والمنظور السيادي** ـــ المجلة النقدية للقانون والعلوم السياسية، جامعة تيزي وزو، كلية الحقوق والعلوم السياسية، المجلد16، العدد4، 2021، ص: 312

الآلي، والتي يتم فيها رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية[1]

نستخلص مما سبق أنه رغم تلك الجهود المبذولة لمكافحة الجريمة المعلوماتية والإرهاب الإلكتروني وتطبيق الأمان الرقمي إلا أن مصالح الدرك الوطني والأمن الوطني مازالت تواجه العديد من العوائق والتحديات التي تعيقها من تحقيق الأمان الرقمي حاليا ومستقبلا وذلك بسبب التطور التكنولوجي الذي أضفى إلى ظهور صور أخرى للأنترنيت مثل wifi /3G/4G مما يستدعي من الجهات الأمنية رفع التحدي للاستعداد بأحدث التقنيات لمواجهة تلك الجرائم ومواكبة التطور التكنولوجي لها فحسب التكييف القانوني للجرائم الالكترونية لها فهي جرائم عابرة للحدود والقارات، ما يعني أن المجرم يمكنه النفاذ إلى أنظمة الحاسوب في احد الدول للتلاعب واختراق البيانات في بلد آخر، إضافة إلى اعتماد هذا الأخير على خاصية التخفي أثناء استخدام خدمات شبكة الانترنيت ما يشكّل عائقا أمام التحقيق مما يتطلب التعاون مع جهات متعددة واستخدام وسائل حديثة متطورة لفك ورصد الشفرات المستخدمة.

نتائج وتوصيات:

ـــ جرائم الانترنيت عامة والإرهاب الالكتروني خاصة من أكثر الجرائم التي عرفها العالم خطورة وما يزيد من خطورتها هو سهولة استخدام هذه التقنيات

ـــ تدمير الإرهاب الإلكتروني للبنى التحتية المعلوماتية نتائج سلبية كبيرة على الأمن الإلكتروني والأمن الوطني.

ـــ كشفت الجرائم المرتكبة بواسطة التقنيات الحديثة القصور التشريعي للنصوص العقابية

ـــ التهديد عن بعد لا يتطلب الحضور الشخصي للجناة وإنما مكن التخطيط والتنظيم والتنفيذ عن بعد.

ـــ لنجاح سياسة تحقيق الأمن الالكتروني ومكافحة جريمة الإرهاب الالكتروني ضرورة الاستفادة من التجارب الرائدة في هذا المجال

ـــ تكوين نخب مختصة في مجال الأمن الإلكتروني مع ضرورة إجراء مؤتمرات علمية يشارك بها المتخصصون العلميين يهدف الاستفادة من خبراتهم.

ـــ السعي للاستفادة من تجارب الدول الرائدة في مجال تحقيق الأمن الالكتروني والتعرف على أفضل التقنيات المعتمدة لمكافحة الجرائم الالكترونية من قرصنة، تجسس، إرهاب الكتروني.....الخ

---

[1] ـــ إدريس عطية: **مكانة الأمن السيبيراني في منظومة الأمن الوطني الجزائري**، مجلة مصداقية، الجزائر: المدرسة العليا العسكرية للإعلام والاتصال، ص: 113

ـــ تحديث البنية التحتية لتقنية المعلومات والاتصالات وحمايتها، وتحديد نقاط القوة والضعف الموجودة في القانونية المتعلقة بمكافحة جرائم المعلومات، والعمل على تجاوز عقبات تطبيقها.

قائمة المصادر والمراجع

أولا: معاجم

1 ـــ أبو الفضل ابن منظور، لسان العرب، مجلد1، دار لسان العرب، بيروت، د س ن.

2 ـــ الرازي أحمد بن فارس القز ويني، مقاييس اللغة، دار الفكر.

ثانيا: كتب

3 ـــ أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري- دار هومة الطبعة الأولى 2006.

4 ـــ جلال محمد الزغبي وأسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2010.

5 ـــ حسنين شفيق، الإعلام الجديد والجرائم الالكترونيةـــ التسريبات، التجسس، الإرهاب الالكتروني، دار فكر وفن، 2014

6ـــ حمدان لافي حمدان الويبار الشمري: أمن شبكة الحاسب وشبكة الانترنيت، المملكة العربية السعودية، جامعة حائل

7 ـــ طوني ميشال عيسى: التنظيم القانوني لشبكة الانترنيت ـــ دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، بيروت: المنشورات الحقوقية، 2001

8 ـــ عبد الرحمان بن عبد الله السند: الأحكام الفقهية للتعاملات الإلكترونية الحاسب الآلي وشبكة المعلومات (الأنترنيت)، ط1، بيروت: دار الوراق، 2004

9 ـــ عبد الرحمان عمار، قضية الإرهاب بين الحق والباطل، منشورات اتحاد الكتاب العرب، دمشق، 2003.

10 ـــ عبد الرحيم صادق، الإرهاب السياسي والقانون الجنائي، دار النهضة، القاهرة، 1985

11 ـــ عبد القادر الشيخلي، طبيعة الإرهاب الإلكتروني، الملتقى الدولي الموسوم ب مكافحة الإرهاب، رابطة العالم الإسلامي، مكة المكرمة، فبراير 2015

12 ـــ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون ـــ دراسة مقارنةـــ، منشأة المعارف، الإسكندرية، بلا سنة طبع

13 ـــ مجمع الفقه الإسلامي، الإرهاب والسلام، ط1، دار الكتب العلمية، بيروت، 2007.

14 ـــ محمد السعيد رشدي: التعاقد بوسائل الاتصال الحديثة ومدى حجيتها في الاثبات، الإسكندرية: منشأة المعارف، 2008

15 ــ محمد أمين الرومي: التعاقد الالكتروني عبر الانترنيت، مصر: دار المطبوعات الجامعية، ط1، 2004

16 ــ محمد سعادي، الإرهاب الدولي بين الغموض و التأويل، دار الجامعة الجديدة، الإسكندرية

17 ــ محمد سيد سلطان: قضايا قانونية في امن المعلومات وحماية البيئة الإلكترونية، دار ناشري: 2012

18 ــ محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، ج2، مركز الإعلام الأمني، دبي، 2010، ص10

19 ــ محمد محي الدين عوض، واقع الإرهاب واتجاهاته، الرياض، جامعة نايف للعلوم الأمنية والعربية، الرياض، 1999

20 ــ محمد مسعود قيراط، الإرهاب دراسة في البرامج الوطنية واستراتيجيات مكافحته مقاربة إعلامية، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011

21 ــ محمود الرشيدي، العنف في جرائم الأنترنت، الدار المصرية اللبنانية، القاهرة، 2011.

22 ــ معتز محي عبد الحميد، الإرهاب وتجدد الفكر الأمني، ط1، دار زهران، الأردن، 2014.

23 ــ هبة الله أحمد خميس بسيوني، الإرهاب الدولي، منشأة المعارف، الإسكندرية، 2011

24 ــ وسيم شفيق الحجار: الإثبات الإلكتروني، بيروت: المنشورات الحقوقية، 2002

25 ــ يوسف محمد صادق، الإرهاب والصراع الدولي، دار سردم للطباعة والنشر، 2013

ثالثا: ملتقيات وندوات

26 ــ أيسر محمد عطية القيسي، دور الآليات الحديثة للحد من الجرائم المستحدثة ــ الإرهاب الإلكتروني وطرق مواجهته ــ الملتقى الدولي الموسوم ب الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، المملكة الأردنية الهاشمية، عمان، 2 ــ 2014/9/4

27 ــ خديجة حامي: الأنظمة المعلوماتية في مواجهة القرصنة والتخريب (المخاطر المحدقة والحلول الناجعة)، مداخلة القيت بالملتقى الوطني: الأمن المعلوماتي مهدداته وسبل الحماية، تيزي وزو: جامعة مولود معمري، كلية الآداب واللغات، 3،4/ نوفمبر 2015

28 ــ مها عبد المجيد صلاح، استراتيجيات الاتصال في مواقع الجماعات المتطرفة على شبكة الانترنيت دراسة تحليلية، الندوة العلمية الموسومة باستعمال الانترنيت في تمويل الإرهاب وتجنيد الإرهابيين، مركز الدراسات والبحوث، قسم الندوات واللقاءات العلمية، الرياض، 2010

29 ــ نبيل السمالوطي، الكتائب الإلكترونية وصناعة الارهاب ــ التشخيص وأساليب المواجهة ــ العدد21، يونيو2018،

رابعا: مجلات

30 ــ بن مرزوق عنترة، الكر محمد: البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الارهاب، مجلة العلوم الانسانية والاجتماعية، العدد38، جوان: 2018

31 ــ جعفر حسن جاسم الطائي، الإرهاب ألمعلوماتي وآليات الحد منه، مجلة العلوم القانونية والسياسية، جامعة ديالي، عدد خاص، كلية القانون والعلوم السياسية

32 ــ حمدان رمضان محمد، الإرهاب الدولي وتداعياته على الأمن والسلم العالمي دراسة تحليلية من منظور اجتماعي، مجلة أبحاث كلية التربية الأساسية، المجلد11، العدد1، 2011

33 ــ رنا مولود شاكر، مستقبل حقوق الإنسان في ظل الإرهاب دراسة حالة حقوق الإنسان في الأراضي الفلسطينية المحتلة، مجلة مركز الدراسات الفلسطينية، جامعة بغداد، العدد15، 2012.

34 ــ زينب علي عبد، الإرهاب فساد حقوق الإنسان وكرامته ــ دراسة تحليلية، مجلة أهل البيت، العدد18.

35 ــ عقوني محمد، بلمهدي براهيم: الآليات التقنية والقانونية لحماية التوقيع الالكتروني، مجلة المفكر، بسكرة: جامعة محمد خيضر، العدد18، فيفري 2019.

36 ــ ليتيم فتيحة، ليتيم نادية: الأمن ألمعلوماتي للحوكمة الالكترونية وإرهاب القرصنة، بسكرة: مجلة المفكر، جامعة محمد خيضر، العدد 12.

37 ــ مشتاق طالب وهيب ، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها ، مجلة العلوم القانونية والسياسية، جامعة ديالى، المجلد الثالث، العدد الأول ، 2014.

خامسا: رسائل جامعية

38 ــ بوكثير خالد، الجرائم المعلوماتية، مذكرة نهاية التدريب مقدمة للمنظمة الجهوية للمحامين، سطيف 2005، 2006

39 ــ سليم دحماني: أثر التهديدات السيبيرانية على الامن القومي الولايات المتحدة الأمريكية أنموذجا (2001، 2017)، المسيلة: جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، 2017، 2018

40 ــ شاشوة ياسمينة: الإرهاب الالكتروني بين مخاطره وآليات مكافحته، مذكرة ماستر، البويرة، جامعة آكلي محند أولحاج، كلية الحقوق والعلوم السياسية

41ــ لالوشي راضية: أمن التوقيع الإلكتروني، رسالة ماجستير، تيزي وزو: جامعة مولود معمري، كلية الحقوق والعلوم السياسية، 2012

سادسا: مراجع أجنبية

42 - Debray stéphane, internet face aux substances illicties:complice de la cybercriminalité ou outil de prevention?,DEES media électronique and internet,University de paris8,2002-2003

43 - James Dear Derain, ”the Terrorist Discouerse:signs,states and system of Global policitical violencec” in word Secuirity:trends and challenges at centry’s End,ed by michaelT,klare and Daniel C,Thomas,new York: ST Martin’s perss,1991

سابعا: مواقع الكترونية

44 - http://alkhaleejonline.net/articles
45 - https://drive.googl.com
46 - www.alukah.net
47 - www.Nashiri.net