الاستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية

The Security Strategy of the Algerian State in the Fight against Cybercrime

د/ دندن جمال الدين [1] ،

[1] كلية الحقوق ، جامعة الجزائر 1، denden.djameleddine@yahoo.fr

تاريخ الإرسال: 2020/03/11 تاريخ القبول: 2020/05/05 تاريخ النشر: 2020/11/09

ملخص:

عرفت الجزائر في السنوات الأخيرة حركة متسارعة في مجال الجريمة السيبرانية ، خاصة في ظل الاستعمال الواسع لشبكة الانترنت، وضعف المراقبة والمتابعة الدورية لإستخدامها، وحرصا من المشرع الجزائري على التصدي للجريمة السيبرانية، قام باستحداث آليات إجرائية تتناسب وطبيعة هذه الجرائم، وذلك نظرا لعجز الإجراءات التقليدية في مواجهة هذا النوع من الجرائم التي تتميز بالتطور المستمر.

كلمات مفتاحية: الجريمة السيبرانية، الأمن السيبراني ، الإرهاب الالكتروني.

Abstract:

In recent years, Algeria has experienced an accelerating movement in the field of cybercrime, especially in light of the widespread use of the internet and weak monitoring and periodic follow-up to its use.And in order to confront cybercrime, the Algerian legislator has created procedural mechanisms that are commensurate with the nature of these crimes, due to the inability of traditional procedures to confront this relatively newtype of crime, which is characterized by continuous development.

Keywords: *cybercrime; cyber security; cyberterrorrisms.*

1- المؤلف المرسل: دندن جمال الدين، **الإيميل:** denden.djameleddine@yahoo.fr

مقدمة :

أصبحت الجرائم الالكترونية تشكل خطرا كبيرا على استقرار الدول، وذلك بعد أن استطاعت تكنولوجيا الانترنيت اختراق جميع الحواجز والقيود التي تسيطر على المجتمعات، ومن منطلق هذه المخاطر الالكترونية التي تعرف على المستوى الدولي بـ "الارهاب الالكتروني" والذي يمثل بدوره تهديدا على الأمن القومي للدول.

لذا فالإرهاب الإلكتروني يعد أحد الأشكال وصور الإرهاب فلقد أصبح الإرهاب الإلكتروني هاجساً 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 أضراراً جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

لقد أصبح الفضاء السيبراني حاضنة لبروز ونمو أشكال جديدة من الإرهابيين، كمؤشر على الإرهاب غير التقليدي الذي يستهدف مهاجمة البنيات التحتية الكونية للمعلومات، وليس هذا فحسب، بل حمل الفضاء الرقمي معه تحديات أمنية وقانونية وسياسية وتقنية، خاصة في ظل ضعف منظومات الحماية وعدم وجود أطر قانونية واضحة لتنظيم هذا الفضاء، بالإضافة إلى عدم التوافق بين تدابير المكافحة والانتشار الهائل لتكنولوجيا الاتصال

والمعلومات وزيادة الاعتماد الدولي عليها، فضلا عن محدودية أدوار المواجهة القانونية والأمنية والتقنية في مقابل التهديدات الحاصلة والتحديات والتداعيات على الأمن الدولي عامة [1].

وانطلاقا مما سبق نطرح الاشكالية التالية: إلى أي مدى نجح المشرع الجزائري في تبني استراتيجة أمنية وقانونية من أجل حماية الانظمة المعلوماتية في مجال الجرائم الالكترونية ؟

1. عموميات عن الأمن السيبراني والجريمة السيبرانية

1.1. تعريف الأمن السيبراني:

يعني الأمن السيبراني أو الالكتروني مجمل القوانين السياسية، الأدوات، النصوص، المفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيات المعلومات والتصالات المستخدمة لحماية الدول والمنظمات والأشخاص. كما يعرف على أنه 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.

يمكن تعريف الأمن السيبراني بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الأضرار إلى خسائر دائمة.

وعليه فإن الأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو اتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات، وهذا يتطلب حماية الشبكات

وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، وبعبارة أخرى فإنه لا يعني أكثر من حماية البيانات [2].

2.1. الجريمة السيبرانية:

1.2.1. تعريف الجرائم السيبرانية: تشكل الجرائم الالكترونية تحدي كبير للبيئة التي ترتكب فيها، إذ يمكن لمجرمي الانترنيت العمل من أي مكان في العالم، واستهداف أعداد كبيرة من الناس أو الشركات عبر الحدود الدولية، وتزداد التحديات التي تفرضها استنادا إلى نطاق وحجم الجرائم، والتعقيد التقني لتحديد هوية الجناة وكذلك ضرورة العمل على الصعيد الدولي لتقديمهم إلى العدالة، فالانترنيت تفتح فرصا جديدة لمجرميها، على أساس الاعتقاد بأن إنقاذ القانون لا يعمل في عالم الانترنت.

وقد عرف المشرع الجزائري الجرائم السيبرانية واطلق عليها تسمية الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب الفقرة (أ) المادة 02 من القانون رقم 09-04 على أنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية" [3].

2.2.1. خصائص الجرائم السيبرانية: تتميز الجرائم الالكترونية بخصائص تختلف إلى حد ما عن الجريمة العادية على النحو التالي:

- جرائم عابرة للدول: وهي الجرائم التي تقع بين أكثر من دولة ولا تعترف بالحدود الجغرافية مثلها مثل جرائم غسيل الأموال والمخدرات وغيرها، ففي عصر الحاسوب والانترنت أمكن ربط أعداد هائلة من الحواسيب عبر العالم، وعند وقوع جريمة الكترونية غالبا يكون الجاني في بلد والمجني عليه في بلد آخر كما قد يكون الضرر في بلد ثالث.

- جرائم صعبة الإثبات: يستخدم فيها الجاني وسائل فنية معقدة وسريعة في كثير من الأحيان قد لا تستغرق أكثر من بضع ثواني، بالإضافة إلى سهولة

محو الدليل والتلاعب فيه والأهم عدم تقبل القضاء في كثير من الدول للأدلة التقنية المعلوماتية التي تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة بالحواس الطبيعية للإنسان.

- جرائم سهلة الارتكاب: فهي جرائم ناعمة soft crime واطلق عليها البعض إسم جرائم الياقات البيضاء، وعند توفر التقنية اللازمة للجاني يصبح ارتكاب الجريمة من السهولة بمكان ولا تحتاج إلى وقت ولا جهد.

- عدم قيام ضحايا الإجرام السيبراني بتقديم الشكوى أو التبليغ: أي أنه لا يتم في غالب الأحيان تقديم شكوى أو الإبلاغ عند إرتكابها، إما لعدم إكتشاف الضحية لها وإما خوفا من التشهير، لذا نجد أن معظم جرائم الانترنت تكتشف بالمصادفة، وأحيانا بعد وقت طويل من إرتكابها، زيادة على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها، فالرقم المظلم بين حقيقة عدد الجرائم المرتكبة والعدد التي تم اكتشافه هو رقم خطير [4].

2. مخاطر وتهديدات الارهاب الالكتروني وتأثيره على الاستراتيجية الأمنية:

تشهد الساحة الأمنية الجزائرية كغيرها من الدول العديد من المخاطر والتهديدات التي فرضتها الثورة التكنولوجية الحديثة، خاصة بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكارا هدامة تهدد استقرار الوطن ووحدته، وتدعو إلى نشر الفوضى والعنف والتطرف والكراهية والانقسام، ومن أهم المخاطر التي تترتب عن استخدام التكنولوجيا الحديثة على الأمن الجزائري الارهاب الالكتروني [5].

1.2. مخاطر وتهديدات الارهاب الالكتروني:

لقد أصبح الفضاء الالكتروني منبرا للجماعات الارهابية عبر نشر رسائل الكراهية والعنف، والاتصال ببعضها البعض وبمؤيديها والمتعاطفين، وليست المواقع الالكترونية سوى واحدة من خدمات الانترنت التي سطا عليها الارهابيون، فهنالك تسهيلات عديدة أخرى كالبريد الالكتروني، غرف المحادثة والمجموعات الالكترونية.

وعليه ظهر ما يسمى العالم الافتراضي للإرهابيين The Cyber-terrorists والذي يعتبرون المجموعة الأحدث والأكثر خطورة، والدافع الأساسي لهم ليس المال فقط ولكن أيضا لديهم قضية ما والتي يدافعون عنها، وعادة ما ينغمسون في إرسال رسائل التهديد وتدمير البيانات المخزنة في الغالب في نظم المعلومات الحكومية لمجرد أن يسجلوا وجهة نظرهم، ويمكن مقارنة تهديد الإرهاب الالكتروني بتهديدات السلاح النووي. هذه المسألة المثبطة للهمم هي أنهم لا يعملون داخل حدود الدولة، بل يمكن أن يعملوا في أي مكان في العالم، وهذا ما يجعل من الصعب اقتناصهم ففي مجال الإرهاب أظهرت دراسة سالم وريد وشين سنة 2008 والتي درسوا فيها محتوى فيديوهات للجماعات المتطرفة الإرهابية باستخدام تحليل المحتوى وأدوات الترميز في الوسائط المتعددة لاستطلاع وتحليل أنماط الفيديوهات وطريقة العمل operandi modus وخصائص المنتج الذي قاد إلى دعم هذه الجماعات المتطرفة، أظهرت الدراسة إن هذه الفيديوهات قد مررت رسائل قوية وكافية لتعبئة الأفراد والمتعاطفين وحتى لتنفيذ هجمات مثل الذي يحتويها الفيديو ونشرها عالميا من خلال النت [6].

2.2 . تأثير الارهاب الالكتروني على الاستراتيجية الأمنية:

يمكن القول أن الارهاب السيبراني قد شكل قاعدة للتغيير والتعبير عن الرؤى المتطرفة التي تتبنى العنف أسلوبا ووسيلة، مستفيدا في ذلك مما آل إليه الانترنت من تقسيم الجمهور إلى فئات وجموعات صغيرة، وأخذ هذا التنوع في تنمية ظاهرة التشتت الثقافي، بوصفه إعلاما فئويا يستخدم لإذكاء نيران الصراعات العنصرية وتنمية اتجاهات الكراهية لدى الكثير من الفئات المناهضة للفئات الأخرى، وفي المقابل تلك النظرة الانقسامية للمجتمعات، جاء ذلك الإعلام للترويج لرؤى عالمية، ففي حين تستغله الدول الغربية للترويج للرأسمالية، تستغله التنظيمات الارهابية للترويج للخلافة الاسلامية والجهاد العالمي [7].

لقد قوض الارهـاب السيبراني من سلطة الدولة بنقل الحوادث الارهابية إلى الرأي العام، بما يشكل خطرا نفسيا وضغطا على الحكومات بإجبارها على المثول للمطالب السياسية التي تتبناها الجماعات الارهـابية ، وتهديدا لشرعية النظم السياسية الحاكمة، وعمل ذلك على الحد من استخدام القوة في صنع القرار من جانب الدولة التي فرض انسحابها من قطاعات استراتيجية لصالح القطاع الخاص تحديات أمنية متـزايدة، وتطرح مسألة المواجهة الامنية قضية حرية الرأي والتعبير عبر الانترنت وارتباطها بالقيم الديمقراطية، وكذلك مسألة الاستغلال السياسي للنظم الحاكمة لمواجهة معارضيها بشكل لا يعكس الفصل بين أمن النظام وأمن المجتمع، وفي المقابل تلك الجهود لإغلاق مواقع الانترنت، تزداد قدرة الارهابيين على استخدام الفضاء الرقمي بشكل أكثر عمقا [8].

3. مواجهة الجريمة السيبرانية: الآليات والووسائل

خلال السنوات الأخيرة، أصبح استعمال تكنولوجيا المعلومات والاتصال لأهداف إجرامية يشكل تحديا حقيقيا لجل الدول، حيث غدت محاربة الجريمة الالكترونية من بين التهديدات الدولية الأولى، وأمام هذه الوضعية، اعتمدت الدولة في اطار استراتيجيتها الأمنية المبنية على مواكبة التطورات الحاصلة على مجموعة من الأجهزة التي من شأنها وضع حد والتقليل من هذه الجرائم السيبرانية.

1.3. مركـز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

أنشأ هذا المركز سنة 2008، ويعتبر الجهاز الوحيد المختص بهذا المجال في الجزائر، ويهدف أساسا إلى تأمين منظومة المعلومات لخدمة الأمن العمومي واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، هذا المركز يعمل على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أفراد أو جماعات، وهذا كله من أجل تأمين الأنظمة

المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها، وفي ذات السياق استطاع المركز معالجة العديد من الجرائم الالكترونية والرقمية وكذا تلك المتعلقة بوسائل التواصل الاجتماعي وكذلك الجرائم المتعلقة باختراق مواقع رسمية لمؤسسات عامة وخاصة، استهدف مجرموها أنظمة المعالجة الآلية للمعطيات [9].

2.3. المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بموجب المرسوم الرئاسي رقم 04-183 المؤرخ بتاريخ 26 جوان 2004، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحاليل الحديثة والمدعومة بالتكنولوجيات المناسبة. ولعل الخدمة الأساسية التي يقدمها هذا المعهد هي خدمة العدالة ودعم وحدات التحري في إطار الشرطة القضائية، ولهذا فإن المعهد الوطني للادلة الجنائية وعلم الاجرام مكلف بالمهام الآتية :

- القيام بالخبرات العلمية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة من أجل كشف الحقيقة بالأدلة العلمية لتحديد هوية مرتكبي الجنايات والجنح.
- مساعدة المحققين للسير الحسن للمعاينات خاصة عن طريق الوضع تحت تصرف الأفراد المؤهلين أثناء الحاجة.
- المبادرة وإجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.

- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

3.3. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

استجابت مصالح الأمن الجزائرية لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية من خلال انشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية [10].

وقد كانت المصلحة عبارة عن فصيلة شكلت النواة الاولى لتشكيل أمني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للامن الوطني DGSN، والتي أنشأت سنة 2011، ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بجرائم تكنولوجيات الاعلام والاتصال بقرار من المدير العام للامن الوطني واضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.

وبخصوص أول قضية عالجتها المصلحة، كانت قضية ذات بعد دولي وقعت في نهاية سنة 2009 على إثر بلاغ من مكتب التحقيقات الفدرالية أف . بي.أي ، وتنقل ممثلين عنهم لتقديم بلاغ إلى السلطات الجزائرية بسبب تعرّض شركة أمريكية إلى عملية قرصنة بخصوص بيانات بنكية، وتبيّن من التحقيق أنها منظمة إجرامية تنشط في مجال الإختراق والقرصنة ولها شريك في الجزائر، وبعد وصول البلاغ الأجنبي تم توجيه الملف إلى مصالح مديرية الشرطة القضائية فشكل فوج للتحقيق متكون من ثلاثة عناصر،ورفع التحدي، حيث أسفرت التحريات المكثفة عن تحديد مكان وهوية الشخص الذي اتضح أنه يقطن بإحدى ولايات الشرق الجزائري، وقد تم التمكن من إثبات كفاءة الشرطة الجزائرية بتحديد هويته وتقديمه للعدالة.

4.3. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

انشئت هذه الهيئة بموجب المرسوم الرئاسي رقم 15-261 [11]، وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت اشراف ومراقبة لجنة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وتضم الهيئة كذلك قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

وكلفت الهيئة باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الارهابية والتخريبية والمساس بأمن الدولة [12].

5.3. المنظومة الوطنية لأمن الأنظمة المعلوماتية:

تبنى المشرع الجزائري استراتيجية جديدة لمكافحة الجرائم المعلوماتية، والتي استفحلت في السنوات الأخير، حيث قام بإنشاء منظومة وطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 [13].

1.5.3. تعريف المنظومة الوطنية لأمن الأنظمة المعلوماتية:

تعتبر المنظومة على أنها أداة الدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها.

تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، على كل من مجلس وطني لأمن الأنظمة المعلوماتية، ويكلف عادة بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها، وكذلك على وكالة لأمن الأنظمة المعلوماتية، وتكلف بتنسيق وتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية. ولممارسة مهامه يتوفر المجلس بالإضافة إلى الوكالة، على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال.

2.5.3. هياكل المنظومة الوطنية لأمن الأنظمة المعلوماتية: من بين أهم هياكله نجد كل من :

- المجلس الوطني لأمن الأنظمة المعلوماتية: يتولى في إطار إعداد الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، على الخصوص المهام الآتية:

- البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها. وكذا دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما.
- العمل على دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها.
- الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.
- الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني والموافقة على تصنيف الأنظمة المعلوماتية.
- اقتراح ملاءمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، عند الحاجة. وكذلك يبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.

- وكالة أمن الأنظمة المعلوماتية: تكلف الوكالة على الخصوص بما يأتي:

- تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، وعرضها على المجلس.
- تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.
- اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.
- إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.
- السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشأت المؤسسات الوطنية.
- متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية.
- تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية .
- ضمان اليقظة التكنولوجية في مجال أمن الانظمة المعلوماتية.
- مرافقة الإدارات والمؤسسات والهيئات، بالتشاور مع الهياكل المختصة في هذا المجال، في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية.
- جرد الأنظمة المعلوماتية وعرضها على المجلس للموافقة على تصنيفها، وكذلك اعداد وتحيين خارطة للأنظمة المعلوماتية المصنفة.
- اقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية ، بعد الرأي المطابق للمجلس.
- إعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية.
- اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها.
- اعتماد منظومات إنشاء وفحص الإمضاء الالكتروني

- تحديد معايير وإجراءات منح علامة الجودة والتصديق واعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية ، طبقا للتشريع والتنظيم المعمول بهما.
- القيام بنشاطات التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية.
- تقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية، في مجال أمن الأنظمة المعلوماتية.
- اقتراح تدابير الترقية والبحث والتطوير للحلول الوطنية في مجال أمن الأنظمة المعلوماتية.
- تنشيط وتوجيه أنشطة البحث والتطوير في مجال أمن الانظمة المعلوماتية.
- اقتراح مشاريع اتفاقات التعاون والاعتراف المتبادل مع الهيئات الدولية في مجال اختصاصها، وكذا إبرام مشاريع شراكة في مجال أمن الأنظمة المعلوماتية بعد موافقة المجلس.

الخاتمة :

من خلال ما تطرقنا إليه تبين أنه بات لزاما على دول العالم مواكبة التطور التكنولوجي الحاصل في العالم الافتراضي الجديد ، الذي صارت فيه المعلومة مصدرا للقوة والمعرفة والسلطة والمال ، بل وأكثر من ذلك أصبحت معيارا لتطور الشعوب.

وقد تبين أن الترسانة القانونية الجزائية تبدو ضعيفة عن مواجهة الاجرام السيبراني، وهذا على الرغم من المجهودات المبذولة من طرف الدولة الجزائرية من تحديث وحماية الانظمة المعلوماتية في مجال الامن السيبراني، وعليه قد توصلنا لمجموعة من الاقتراحات الاتية :

- تعزيز الهياكل الوطنية ومصالح الأمن المختصة في الوقاية من الجريمة ذات الصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما بالموارد البشرية المتخصصة والوسائل التكنولوجية المتطورة.

- تدعيم وتعزيز الانجازات الحالية في مجال مكافحة الجريمة السيبرانية، مع اشراك جميع الجهات الوطنية الفاعلة والأخذ بعين الاعتبار كل التهديدات السيبرانية على وجه الخصوص و تلك المربطة بالخدمات الالكترونية.
- تشجيع اطلاق حاضنة وطنية لدعم الشركات الجزائرية الناشئة في مجال أمن المعلومات، من أجل تعزيز تطوير تكنولوجيا جزائرية باعتبارها الضامن الوحيد لفضاء سيبراني وطني آمن.
- تعزيز التعاون في مجال الامن السيبراني، خاصة مع البلدان التي لديها خبرة مثبتة في هذا المجال وكذا ضرورة انشاء لجنة متخصصة تسهر على انجاز مخطط عمل في هذا الشأن.
- العمل على تعزيز ثقافة تأمين الأنظمة المعلوماتية.

التهميش و الإحالات :

(1) حكيم غريب، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية للعلوم السياسية، المجلد 05، العدد 02، ديسمبر 2018، ص 105.

(2) عنتره بن مرزوق، محمد الكر، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والاجتماعية ، جامعة باتنة 1، العدد 38، جوان 2018، ص 36.

(3) أنظر المادة 02 من القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(4) عبد الرحمان جميل محمود حسين، الحماية القانونية لبرامج الحاسب الألي، مذكرة ماجستير، جامعة النجاح الوطنية نابلس، كلية الدراسات العليا، فلسطين، 2008، ص 09.

(5) عنتره بن مرزوق، محمد الكر، مرجع سابق، ص 37.

(6) ذياب موسى البداينة، الجرائم الإلكترونية: المفهوم والأسباب مداخلة ألقيت في الملتقى العلمي الموسوم بـ " الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية " ، كلية العلوم الاستراتيجية، عمان ، المملكة الأردنية الهاشمية، 2014.

(7) حكيم غريب، مرجع سابق، ص 111.
(8) حكيم غريب مرجع سابق، ص ص 112..
(9) سمير بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني ، جامعة باتنة 1، العدد الرابع جويلية 2017، ص 271.
(10) https://www.djazairess.com/essalam/52564 (28/02/2020)
(11) أنظر المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 ، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
(12) إلهام غازي، الوقاية ومكافحة الجريمة المعلوماتية وفي التشريع الجزائري، مجلة الجيش، العدد 630، جانفي 2016، ص 44.
(13) أنظر المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.