الأمن السيبيراني في الجزائر: بين المعالجة الأمنية والحماية القانونية

Cyber security in Algeria: between security confrontation and Legal treatment

محمودي سعيد

[1] جامعة بشار، mahmoudi.said@univ-bechar.dz

تاريخ الاستلام: 2023/07/24 تاريخ القبول: 2023/09/14 تاريخ النشر: 2023/10/31

ملخص:

يعتبر الأمن السيبيراني أحد أبرز المتغيرات الملازمة لفكرة التحول الرقمي المتعلقة بإدراج تكنولوجيات الاتصال في مجال الأنشطة الانسانية، حيث باتت تولي الدول أهمية قصوى لهذا الموضوع، نظرا للمخاطر والتهديدات التي اصبح يفرزها الاستغلال السيء لهذه التقنيات الحديثة.

لذا تحاول هذه الدراسة معالجة الموضوع من منظور قانوني وأمني في الجزائر، انطلاقا من الاستراتيجيات التشريعية والهيئات الأمنية والإدارية الفاعلة في مجال تحقيق الأمن السيبيراني وسبل تعزيزه، عبر حزمة من الاجراءات الهامة والهادفة نحو تحصين الخدمات والمعلومات من أي هجمات تستهدف المساس بها.

لتخلص الدراسة الى جملة من النتائج المتعلقة بتثمين الجهود الجزائرية في هذا الشق مبرزا من خلالها ضرورة التوجه نحو المزيد من السياسات الحمائية التشريعية والتقنية، والتوعية الأمنية والردعية في هذا الاطار.

كلمات مفتاحية: الهجمات الالكترونية – الأمن –الأمن السيبيراني – الحماية القانونية

Abstract:

The issue of cybersecurity is one of the most prominent variables inherent to the idea of digital transformation related to the inclusion of communication technologies in the field of humanitarian activities, as countries attach utmost importance to this topic, due to the risks and threats that have become produced by the bad exploitation of these modern technologies.

this study attempts to address the issue from a legal and security perspective in Algeria, based on legislative strategies and effective security and

administrative bodies in the field of achieving cybersecurity and ways to enhance it, through a package of important measures aimed at immunizing services and information from any attacks aimed at compromising them.
The study concludes with a number of results related to the appreciation of Algerian efforts in this aspect, highlighting the need to move towards more protectionist legislative and technical policies, and security and deterrence awareness in this context.
Keywords: Cyber-attacks– Security - Cyber Security - Legal protection

المؤلف المرسل: محمودي سعيد ، mahmoud.said@univ-bechar.dz

مقدمة:

مع نهاية القرن العشرين كان العالم يشهد تحولا فارقا في مجال استغلال وسائل تكنولوجيا الاتصال، ايذانا بانتقال مجتمعات المعلومات الى مرحلة التحول الرقمي الشامل في المجالات السياسية والتنموية والاتصال والخدمات، وقد ساهمت مظاهر هذا التحول الجديد في اعادة تعريف وتشكيل الكثير من المتغيرات استجابة لمدركات تفاعلها في شقيها الايجابي والسلبي.

ومع بداية القرن الواحد والعشرين استطاعت الثورة الرقمية احداث حراك معرفي واسع، في ادراك أنماط تفاعلات الفضاء الرقمي، فأصبح حجم وتأثير الدول ومكانتها معرفا بقدراتها في امتلاك وتوطين وسائل التكنولوجيا، وتم اعادة قراءة مفاهيم القوة والسيادة والسيطرة تماشيا مع أشكال التهديد الجديدة لأمن الدول، انطلاقا من حروب الجيل الرابع والخامس المنبعثة من استغلال الفضاء السيبيراني، أو كما يسميه باسكال بونيفاس ميدان المعركة الخامس بين القوى الدولية[1] عن طريق شن هجمات الكترونية وتنفيذ جرائم سيبيرانية تستهدف المساس بأمن المؤسسات والدول وحتى الأشخاص، مما أصبح يفرض استجابة أمنية وقانونية لأشكال جديدة من حروب ومصادر للتحدي تطال اضعاف أمن الدول.

تماشيا مع هذه المعطيات الجديدة انبرت حقول الدراسات الأمنية والتشريعية لاستيعاب هذه الحركيات الجديدة ضمن مصفوفات حماية الأمن الشامل، واتجهت الدول لصيانة أمنها السيبيراني عبر استراتيجيات دفاعية وحمائية سعيا منها للتصدي لمختلف مخاطر الجرائم السيبيرانية التي أصبحت تتحالف مع كثير من المظاهر التقليدية كالإرهاب وشبكات الجرائم العابرة للحدود...وغيرها

في سياق متصل تعتبر الجزائر أحد اكبر الدول تعرضا للهجمات السيبيرانية بشقيها الاجرامي والأمني، حيث تحصي الجزائر أرقاما كبيرة في هذا المجال، مما دفعها الى جعل قضايا الأمن السيبيراني في عمق الشواغل الأساسية والمستجدة لبرامج السياسات الأمنية والاستراتيجية، خاصة في ظل الجهد المتسارع للجزائر نحو تبني التحول الرقمي لحوكمة الانشطة والقطاعات، هذا الامر الذي يتطلب حوكمة سيبيرانية من خلال منظومة تشريعية تقنية وفنية وأمنية تلازم مسار هذا الانتقال الهام.

الاشكالية: تحاول اشكالية هذه الدراسة الانطلاق من موقع الجزائر في ظل تنامي العداء السيبيراني المجسد في أشكال جديدة للحروب تستهدف تعطيل الاجهزة وسرقة المعطيات وغيرها، ومدى استجابة الجزائر لهذه التهديدات من خلال بناء استراتيجيات أمنية متعددة في جوانب تقنية وأمنية وهيكلية وقانونية من شأنها تعزيز الأمن السيبيراني الشامل. وعليه فان **الاشكالية** المطروحة تكون كالآتي:

انطلاقا من الهجمات السيبيرانية التي تتعرض لها الجزائر، ما مدى قدرة الجزائر على بناء سياسة حمائية لمواجهة تحديات الأمن السيبيراني ؟

- من خلال الاشكالية المطروحة نشير الى بعض الأسئلة الفرعية:
- ما المقصود بالأمن السيبيراني؟ وماهي أشكاله؟.
- ماهي تحديات الأمن السيبيراني في الجزائر؟.
- ما مدى استجابة الدولة للجزائرية من الناحية القانونية والأمنية لفكرة الأمن السيبيراني؟.

– الفرضيات:

– كلما زاد تبني الجزائر للتحول الرقمي في برامجها، كلما زاد حجم التهديدات السيبرانية الماسة بأمنها.

– يرتهن تحقيق الأمن السيبيراني بضرورة توافر بنية تحتية ومنظومة تشريعية واستراتيجيات هيكلية وأمنية في الجزائر.

– **المنهج المعتمد:** يقتضي موضوع البحث الاستعانة بأدوات منهجية تساعد على ضبط الموضوع وتحقيق الهدف العلمي للدراسة، حيث اعتمدنا على منهج تحليلي وصفي لتحليل وتفسير متغيرات الدراسة، اضافة الى توظيف المقترب البنائي الوظيفي لفهم بنية وهيكلة مؤسسات الأمن السيبيراني في الجزائر من خلال التطرق للهيئات ذات اهمية بموضوع الدراسة.

–أهداف الدراسة:

التعرف على واقع التحول الرقمي في الجزائر

عرض وتحليل اهم المخاطر والتحديات السيبيرانية ضد الجزائر

ابراز أهم الخطوات والجهود التشريعية والأمنية لتحقيق الأمن السيبيراني في الجزائر

التطرق الى أهم الاستراتيجيات التقنية والفنية لتعزيز رؤية الأمن السيبيراني في الجزائر.

أولا: مدخل مفاهيمي لمتغير الأمن السيبيراني.

يقترن توظيف مصطلح السيبيرانية بمشاهد التطور الحاصل على مستوى استغلال وسائل تكنولوجيا الاعلام والاتصال في عصرنا الحالي، لكن أصل المصطلح تعود جذوره التركيبية والدلالية الى مراحل سابقة ومن مفاهيم اشتقاقية، فكلمة سيبيرانية مأخوذة من لفظة "cyber" المشتقة من كلمة cybernetics ، التي تم تشكيلها بالفرنسية في عام 1834 لتسمية "علم الحكومة"، وهي من اليونانية Kubernê-tiké والتي تعني "القيادة والحكم".

وفي القرن الماضي استعملتلأول مرة عام 1948من قبل عالم الرياضيات الأمريكي نوربرت وينر Winer Norbertوهو أستاذ الرياضيات في معهد ماساشوستس التقني MIT ومختص في علم التحكم الآلي، حيث استخدمها للتعبير عن وضع التحكم الآلي للتواصل بين الكائن الحي والآلة في ذلك الوقت2. وقد تحدث عن السبرنتيقا من خلال مؤلفه الشهير Cybernetics or control and communication in" the Animal and the machine . حيث أشار إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة، هذه الأخيرة التي أصبح يعبر عنها بالحاسوب فيما بعد.

ومع التوسع الشامل في استخدام تقنيات الحاسوب والفضاء الالكتروني أصبحت كلمة "سيبراني" تطلق على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، وصار الفضاء السيبيراني مرادفا للفضاء الإلكتروني Cyberspace، الذي يعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة، وكل الخدمات التي تقوم بتنفيذها والانشطة التي تمارسها أو تنفذها، في جميع مجالات الحياة على مستوى العالم[3].

ساهم انتشار الانترنت وسهولة الاعتمادية الالكترونية من طرف الأفراد والمنظمات والأمم في بروز مستجَد وملح لمصطلح الأمن السيبيراني كتعبير عن انتقال الفضاء السيبيراني من تخصص تقني إلى مفهوم استراتيجي. نتيجة للقوة الجديدة التي أصبحت تكتسبها مختلف الفواعل بفعل تكنولوجيا الشبكات المتطورة

باستمرار للجميع – الطلاب والجنود والجواسيس والمجرمون والمتسللون والإرهابيون – وفي مجالات جمع المعلومات والاتصالات وجمع الاموال ونشر الافكار والعلاقات العامة... وغيرها[4].

عرفه الباحث إدوارد أمورسو Amorso Edward في كتابه " الذي أصدره عام 2007 بعنوان "الأمن السيبيراني" على أنه :"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"[5].

حيث يركز هذا المفهوم على الجوانب التقنية والوسائل والبرامج التي تساهم في الحد من مخاطر التهديد السيبيراني وكل الانشطة ذات الطابع الاجرامي المستهدفة لأنظمة المعلومات والاتصال، مما يتطلب كفاءة عالية ودقة في مجال البرمجيات وأمن المعلومات وصيانة الاجهزة.

كما يعرف الأمن السيبيراني بأنه: النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانية الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الأضرار الى خسائر دائمة[6].

على عكس من التعريف السابق يركز هذا المفهوم على جملة الاهداف المتوخاة من تحقيق الأمن السيبيراني من خلال حماية واصلاح الأعطاب الماسة بالمواد والموارد المعرضة للتهديد، سواء كانت موارد بشرية أو مادية.

وفي تعريف دقيق قدمته وزارة الدفاع الامريكية حيث اعتبرت أنه " جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الالكترونية والمادية من مختلف الجرائم والهجمات، والتخريب والتجسس، والحوادث"[7].

–مهددات الأمن السيبيراني:

تتباين أشكال ومصادر التهديدات السيبيرانية حسب الاهداف المراد تحقيقها من قبل المعتدي والجهة المستهدفة من الهجمة، ويتخذ الطرف المهاجم لذلك عدة وسائل وأساليب يستخدمها لإلحاق الضرر المقصود بالطرف المعتدى عليه سواء كان دولة أو مؤسسة أو مجتمع أو فرد، ويمكن اجمال هذه التهديدات في عدة مظاهر:

1-الهجمات السيبيرانية: وهي "فعل يقوض من قدرات ووظائف الكومبيوتر لغرض قومي أو سياسي أو اجرامي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام" ولتحقيق هذه الاهداف تتخذ هذه الهجمات عدة أساليب منها نذكر:

1-1.الأسلوب المستخدم:

1-1-1.هجمات التصيدPhishing: ويتم تنفيذها عن طريق استيراتيجية التحفيز بطرق احتيالية كارسال محتويات مشابهة للمحتويات المعتادة او في شكل رابط، يودي فتحه او الولوج اليه الى اصابة الجهاز أو تدميره ببرامج فيروسية خبيثة.

1-1-2.**برامج الفديةRansoeware:** نوع من البرامج الضارة يتم السيطرة من خلاله على ملفات الكومبيوتر، وهو مصمم لابتزاز الاموال عن طريق منع الوصول الى الملفات أو نظام الكومبيوتر حتى تدفع الفدية

1-1-3.البرمجيات الخبيثة Malware : هي برامج خبيثة مصممة للحصول على وصول غير مصرح به لإلحاق الضرر بجهاز الكومبيوتر.

1-1-4.**هندسة اجتماعيةSocial engineering** : تستخدم هذه الاستراتيجية من طرف المعتدي لخداعك للكشف عن معلومات حساسة يمكنهم طلب دفع نقدي او الكشف عن بياناتك السرية وتعتمد على أسلوب الاغراء أو بناء الثقة[8].

1-2. القطاع المستهدف: قد يكونون أفرادا عاديين يتم اختراقهم بهدف الابتزاز، أو شركات خاصة لسرقة حقوق الملكية الفكرية وبراءات الاختراع، أو القطاع المالي والمصرفي بهدف الاضرار باقتصاد الدولة أو سرقة الأموال، أو خدمات حكومية، أو أجهزة أمنية بهدف سرقة معلومات استخباراتية أو خطط عسكرية أو تصميمات أسلحة، أو مؤسسات إعلامية.

1-3.حسب الهدف من الهجمة: فقد يكون الهدف "مالي" من خال اختراق الحسابات البنكية، أو هدف"عسكري"، مثل اختراق النظم العسكرية، أو هدف "سياسي" للتعبير عن الغضب من قرارات أو تصرفات سياسية، أو هدف "إنسان "للتعبير عن التعاطف مع قضية إنسانية .

4-1.حسب الفواعل المشاركة: قد يقوم بهذه الهجمات "قوات مسلحة" وجيوش إلكترونية في إطار الصراعات العسكرية والسياسية بين الدول، أو" مجموعات إجرامية "وعصابات منظمة من أجل السرقة وغسيل الاموال، أو" جماعات إرهابية "كأحد أنواع ممارسة الارهاب الالكتروني..[9].

2- **الحروب السيبيرانية:** تجسد الحروب السيبيرانية أبرز المخاطر الأمنية المرتبطة بمفهوم الأمن القومي للدول، حيث أن موضوع الدراسات الأمنية قد انفتح على عنصر الأمن السيبيراني انطلاقا من ظهور حروب الانترنيت بداية من سنة 1993 تزامنا وتوسع مفهوم الأمن واعادة تعريف العديد من المتغيرات الأمنية[10]، وعلى الرغم من جهود المنظمات الدولية، وبعض التحالفات الاقليمية و العديد من الخبراء، إيجاد تعريف موحد للحرب السيبيرانية، الا أن اختلاف طبيعة استراتيجيات الدول وأهدافها، و اختلاف مرتكزات التعريف لم تحقق ذلك، حيث تعتمد الولايات المتحدة الأمريكية وحلفائها، مقاربة اقتصادية و مادية، بينما تركز منظمة شنغهاي للتعاون، على أهداف الصراع في الفضاء السيبيراني ،مثل: السيادة الوطنية، والهوية الثقافية[11].

مما يوحي بأن الحروب السيبيرانية هو صراع هجومي ودفاعي ميدانه الانترنيت تقوده دول وفواعل أخرى ضد أهداف دولاتية أخرى عن طريق جيوش سيبيرانية تستهدف اضعاف أو انهاء مقدرات دول أخرى في مجالات محددة ويكون لها أثر خطير ومدمر على مقومات الدول المستهدفة، عن طريق التعطيل أو التخريب أو التدمير أو السرقة وتتم كلها عن طريق برمجيات الكومبيوتر. ومن بين مميزاتها أنها منخفضة التكاليف وأنها تستهدف البنية التحتية الحرجة، اضافة الى صعوبة تعقبها[12] وترتيب المسؤولية الدولاتية اتجاهها.

ثانيا: مدركات واقع الأمن السيبيراني في الجزائر:

برز اهتمام الجزائر بالتحول الرقمي مند منتصف تسعينات القرن الماضي، وذلك تماشيا مع بداية النفاذ العالمي لتحقيق مسار الحكم الراشد في المجالات السياسية والتنموية حسب نشريات الهيئات والمنظمات الدولية الداعية حينها الى ضرورة ولوج الدول نحو توطين عوائد التطورات الحاصلة في مجال تكنولوجيات الاتصال والبرمجيات في مختلف الأنشطة والبرامج والخدمات. وعلى الرغم من التباطؤ الملحوظ في وتيرة التبني الشامل للحكومة الالكترونية في الجزائر خلال مسار ممتد لثلاث عقود (مند 1996) حسب تقرير مؤشر تنمية الحكومات الرقمية EGDI لسنة 2022 الصادر عن دائرة الأمم المتحدة للشؤون الاقتصادية والاجتماعية[13] الذي يصنف الجزائر في المرتبة 112 سنة 2022، الا أن الجزائر تعد من الدول

الأكثر عرضة للهجمات السيبيرانية، حيث ووفقا لمؤشر التصنيف الصادر عن مؤسسة "كاسبيرسكي" الامريكية فقد احتلت الجزائر المرتبة الأولى عربيا في سنة 2018 ولم تتراجع عن المراتب الثلاث الاولى طيلة السنوات اللاحقة[14]، في حين صنف المؤشر العالمي للأمن السيبراني (جي سي آي) لسنة 2021 الصادر عن الاتحاد الدولي للاتصالات الجزائر في المرتبة 104عالميا في مجال تحقيق الأمن السيبيراني[15]، وهي مرتبة متأخرة نظرا للأهمية القصوى وحجم الامكانات البشرية والمادية التي تتيحها الجزائر لحماية أمنها القومي، خاصة وأن الجزائر حجم التهديدات اللاتماثلية التي تطال الجزائر في اقليمها الجغرافي تتميز بالكثافة والتعقيد والتكامل.

في هذا السياق تبرز مظاهر الهجمات الالكترونية التي تستهدف الجزائر من خلال عديد الانشطة الحربية والدعائية المصنفة ضمن حروب الجيل الرابع، وتتجلى أهم المخاطر في الحملات الماسة بأمن المواقع الحكومية والرسمية والمعطيات والبيانات كاستهداف موقع وكالة الانباء الجزائرية في شهر فيفري الماضي بسبب بيان نشره الموقع يبين موقف الجزائر من قضية تهريب رعية جزائرية الى فرنسا، حيث ان هذا النوع من الاجرام الالكتروني من شأنه الوصول الى تخريب وسرقة بيانات من موقع حساس يعد بمثابة المنصة الاعلامية الرسمية للدولة الجزائرية كما يتجلى الخطر من خلال ما يمكن أن يحدثه إمكانية التلاعب بالأخبار التي سيعمد المخترقون لنشرها بعد ذلك، ما قد يؤدي إلى أزمات دبلوماسية خطيرة للغاية اضافة الى التكلفة المادية لإصلاح الأعطاب والتصدي لها. اضافة لذلك تم استهداف عدد من هياكل البنية التحتية الأساسية الحرجة التابعة لمؤسسات اقتصادية حيوية واستراتيجية على غرار مؤسسة سونطراك وسونلغاز والوكالة الوطنية الجزائرية لتنمية الموارد الهيدروكربونية، ففي رقم رسمي كشفت عنه وزارة الدفاع الجزائرية عن تعرض الجزائر لـ 1,242.801 هجوم الكتروني سنة 2021 [16]، اضافة الى استغلال منصات التواصل الاجتماعي لمحاولة بناء شبكات اجرامية والتحريض على العنف والارهاب وضرب التماسك الاجتماعي والوحدة الوطنية للمجتمع الجزائري، وهو أحد أبرز أشكال الجرائم الالكترونية التي تستهدف الجزائر في السنوات الأخيرة، لاسيما في ظل تنامي استخدام الجزائريين لمواقع التواصل الاجتماعي نتيجة توسع انتشار الانترنيت في الجزائر، حيث بلغ معدل انتشار الإنترنت في الجزائر 70.9٪ من إجمالي السكان في بداية عام 2023، كما ان هناك 32.09 مليون مستخدم للإنترنت في الجزائر في ذات الفترة، منهم 23.95

مليون مستخدم لوسائل التواصل الاجتماعي في يناير 2023 ، أي ما يعادل 52.9 في المائة من إجمالي السكان[17].

ومع التوجه الاقتصادي الجديد الذي تبنته الحكومة الجزائرية باعتماد اقتصاد المعرفة والتشجيع على انشاء المؤسسات الناشئة وحاضنات الاعمال فمن المتوقع أن تتصاعد الهجمات الالكترونية ضد مواقع ومنصات هذه الشركات باعتبارها تدخل في اطار استيراتيجية التطوير الاقتصادي القائم على مبادرات الشباب، مما يجعل الحرب الالكترونية الدائرة لإضعاف مقدرات الجزائر قد توجه هجماتها لتعطيل هذه الجهود، خاصة وأن تنامي وزيادة التحول الرقمي للشركات الصغيرة والناشئة قد زاد من احتمال الهجوم الالكتروني، حيث يؤكد جاك فيليب روديرير، مدير عمليات المبيعات في شركة "سيسكو" أن التحول الرقمي للشركات الصغيرة والمتوسطة كان له تأثير في زيادة مساحات الهجوم والمخاطر الاقتصادية المرتبطة به.

ثالثا: استيراتيجية بناء الأمن السيبيراني في الجزائر:

تبرز الجهود الجزائرية للحد من مخاطر الحرب السيبيرانية التي تستهدف اضعاف مقدراتها في مجال الاعتمادية التقنية، من خلال الاهتمام بوضع سياسات واليات تساهم في تعزيز الأمن السيبيراني، وقد عكفت الجزائر مند سنة 1997 على الاستجابة لهذا الموضوع على مستوى الوسائل[18] والعديد من المؤسسات والهيئات الفاعلة أو المستحدثة في مجال التعاطي مع ما تتيحه مخاطر التهديدات السيبيرانية على الأمن القومي للبلاد، ولعل ادراك المخاطر الالكترونية ذات الطابع الاجرامي يستقي خطورته من الهجمات الالكترونية المتعددة والكثيفة التي تتعرض لها الجزائر باستمرار، لاسيما من مناطق ودول تتميز بعدائها للجزائر. وسنحاول التطرق الى أهم الآليات التي وضعتها الجزائر تماشيا مع النماذج العالمية لمؤشرات الأمن السيبيراني، ويتم قياس هذه البرامج الوطنية للجزائر من خلال النموذج الذي أعلنه الاتحاد الدولي للاتصال (ITU).

وضع الاتحاد الدولي لاتصالات نموذج لبناء الاستراتيجية الوطنية للأمن السيبيراني[19]، ويتضمن هذا النموذج عدد محاور أساسية: الأول يرتبط بالتدابير القانونية والتشريعية، والثاني يتعلق بالتدابير التقنية والبنى التحتية، والمحور الثالث خاص بالهياكل التنظيمية المؤسسية للأمن السيبيراني في الدولة، ، والمحور الرابع مرتبط ببناء القدرات الفنية في هذا المجال الذي يعاني ندرة المتخصصين، وأخيراً يتناول المحور الخامس التعاون الدولي وتبادل المعلومات بين الدول في مجال الأمن السيبيراني، والذي قد يقلل من خطورة الهجمات الإلكترونية.

1-الجانب التشريعي والقانوني: يكشف فحص الوثائق القانونية التي أصدرها المشرع الجزائري في هذا المجال عن مبدأ التدرج في التعاطي مع موضوع الأمن السيبيراني من خلال ترسانة قانونية مواكبة، والملاحظ أن الاهتمام بالجانب القانوني قد بدأ مبكرا، ففي سنة 2004 تم اصدار قانون رقم 04-15 المتضمن تعديل قانون العقوبات وقد ادرج في قسمه السابع مكرر موضوع المساس بأنظمة المعالجة الآلية للمعطيات من خلال اقرار العقوبات المتعلقة بأي سلوك أو تصرف من شأنه المساس أو الاضرار بالمعطيات والهيئات والمؤسسات المنصوص عليها في المادة 394منه (مكرر)[20].

وفي سنة 2009 صدر قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها[21] والدي حدد في مادته الثانية تفصيل لمفهوم الجرائم المتصلة بتكنولوجيات الاعلام والاتصال والقواعد الاجرائية المتعلقة بمراقبة الاتصالات الالكترونية وتفتيش المنظومات المعلوماتية.

وتماشيا مع مقتضيات التحولات في اجيال حقوق الانسان ومسار عصرنة العدالة في خضم التحولات في مجال تكنولوجيا الاتصال، تم اصدار قانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[22]، وقد تضمن هذا القانون تفصيلا للمقصود بهذه المعطيات وآليات المعالجة والمبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي في اطار حفظ الكرامة الانسانية وعدم المساس بها.

وبالتالي فان الاصدار المتوالي لحزمة قوانين وتشريعات في مجال حماية وتعزيز منظومة الانشطة السيبيرانية – لا يسعنا الموضوع لذكرها وتفصيلها- يحضى بأهمية كبيرة نظرا للديناميكية التي يتميز بها هذا الفضاء واستجابة للإفرازات المتعلقة بالأمن الشخصي للأفراد وتهديد الأمن المجتمعي، اضافة الى المساس بالأمن القومي للدولة من خلال مؤسساتها وهيئاتها الرسمية.

2-الجانب التقني والفني: يتطلب تحقيق الأمن السيبيراني ضرورة توافر عدد من الامكانيات المادية التي تساعد على الحد من مخاطر الهجمات والاجرام الالكتروني، ولا يمكن بلوغ ذلك الا من خلال الادوات والوسائل التقنية الثقيلة منها كالمحطات والردارات والشبكات والوسائل، اضافة الى بناء القدرات الرقمية المتعلقة بالبرمجيات والتطبيقات وانظمة الحماية الفيروسية وغيرها، .وقد وضعت الجزائر استراتيجية فضائية وطنية لمدى محدد 2020-2040 من بين أهدافها تأمين الاتصالات المؤسساتية والعمل على سد الهوة

الرقمية ومنح الفرصة للمواطن ليكون طرفا فاعل في المجتمع العالمي للمعلومات[23]، وتتوفر في ذات الاطار وزارة الدفاع الوطني على منظومات جد متطورة في مجال حماية المعطيات والبيانات والتصدي لكل أشكال الهجمات والحرب السيبيرانية وادارة أمن الشبكات وحماية المعطيات.

كما أنشأتالجزائر DZ.CERT وهو فريق الاستجابة لطوارئ الحاسوب Reponse Emergency Computer Team تابع لمركز البحث في الاعلام العلمي والتقني[24]، يعتبر أداة أساسية لحماية المعلومات الحساسة، بالعمل على رصد المخاطر المعلوماتية المستجدة مثل الفيروسات وبرامج التجسس ومكامن الضعف في الأنظمة التشغيلية والتعامل معها وإعطاء الحلول والتدابير بشأنها. كما يهدف إلى تمكين الأفراد والشركات من استباق الهجمات السيبيرانية وتفادي الأضرار قبل وقوعها، غير أن دورها لازال مقتصرا على التعامل مع المؤسسات العمومية والخاصة ولم يتوسع إلى التعامل مع المواطنين بتنفيذ برامج توعوية شاملة لهم.

اضافة لذلك فقد قامت مؤسسة اتصالات الجزائر بإطلاق عروض للمؤسسات والشركات الوطنية في مجال الأمن السيبيراني تتمثل في خدمات لحماية موارد الشركات والمؤسسات من الهجمات السيبيرانية والتهديدات الناجمة عن الانترنيت أو تلك التي تتم عبر الانترنيت[25]، خاصة في ظل اقبال المؤسسات والأفراد على اقتناء برامج وتطبيقات غير أصلية ومقلدة مما يجعل من معطياتها عرضة للاختراق والسرقة، وهي أحد أبرز الجوانب السلبية التي تقوض من فرض تمتين الأمن السيبيراني لدى الهيئات والمؤسسات والأفراد.

3-الهيئات والمؤسسات المختصة: تحصي الجزائر عددا معتبرا من المؤسسات والفروع التابعة لهيئات ومؤسسات وطنية ذات صلة بموضوع الأمن السيبيراني، ويمكن تقسيم هذه الهيئات الى نوعين:

3-1.هيئات الإدارية مكلفة بالأمن السيبيراني:

3-1-1.الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها: أنشئت سنة 2009 بموجب المادة 13 من المرسوم 09-04، تم وضعها تحت السلطة المباشرة لوزير العدل حافظ الأختام، ولم تدخل حيز التنفيذ الا بعد صدور المرسوم الرئاسي رقم 15-261 لسنة 2015، وقد تولت هذه الهيئة الإدارية مهمة اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتهما والوقاية 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 جرائم المتعلقة بالأعمال الارهابية والتخريبية والمساس بأمن الدولة. اضافة الى مهام التعاون والتكوين وتبادل الخبرات مع الهيئات الوطنية والاجنبية في مجال اختصاصها[26].

3-1-2.وكالة أمن الأنظمة المعلوماتية: هي مؤسسة ادارية استحدثت سنة 2020 لتتولى مهام واسعة في مجال تحضير وتنسيق وتنفيذ عناصر الاستراتيجية الوطنية لأمن الانظمة المعلوماتية اضافة الى مهام أخرى يتعلق جزء منها بإجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبيرانية واعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها.

3-1-3. المجلس الوطني لأمن الانظمة المعلوماتية: أنشئ سنة 2020 ويعتبر أهم مؤسسة في صلب موضوع الأمن السيبيراني، يرأسها وزير الدفاع الوطني ممثلة فيها قطاعات سبع قطاعات وزارية هامة، يرتبط عملها بشكل أساسي بالوكالة المذكورة سابقا، حيث تتولى هذه الهيئة مهمة البث في عناصر الاستراتيجية الوطنية لأمن الانظمة المعلوماتية المقترحة من قبل وكالة أمن الأنظمة المعلوماتية وتصادق على مخطط عملها وتدرس تقارير نشاطاتها وتواقف عليها كما تتمتع بالحق في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الانظمة المعلوماتية[27].

3-2.الهيئات العملياتية في مجال الأمن السيبيراني:

3-2-1. مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية: وهو تابع لقيادة الدرك الوطني تأسس مند سنة 2008 لمساعدة الأجهزة الأمنية الأخرى والتعاون مع الجهات القضائية من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم، وقد لعب هذا المركز دورا محوريا في فك ومعالجة العديد من القضايا المتعلقة بالتهديد الالكتروني و قضايا الاختراق و الهاكرز التي استهدفت أنظمة المؤسسات الأمنية والاتصالية و المواقع الحكومية الحساسة[28].

3-2-2. المعهد الوطني للأدلة الجنائية وعلم الاجرام: وهو معهد ذوي قدرات عالية في مكافحة الجريمة بجميع أشكالها يتميز بإدراج العلوم في العدالة الجزائية، كما أن التحكم في التقنيات الحديثة ساهم في دعم قدرات المؤسسة لمكافحة الإجرام المتطور باستمرار والذي يعتمد على التكنولوجيات الجديدة[29].

كما أن انشاء المصلحة المركزية لمكافحة الاجرام السيبيراني على مستوى قيادة الدرك الوطني قد سمح لهذه الهيئات بتطوير منظومات الكشف والتصدي للجرائم السيبيرانية التي تستهدف أمن الاشخاص

والمؤسسات وكذا في قضايا تتعلق بالجرائم العابرة للحدود وشبكات تهديد الأمن الوطني والارهاب الالكتروني... وغيرها[30]، حيث عالجت في هذا الصدد قيادات الدرك الوطني 4600 قضية تتعلق بالجرائم السيبيرانية خلال عام 2022[31].

3-2-3.المصلحة المركزية لمحاربة الجريمة الالكترونية للأمن الوطني: استجابة لتحولات الفضاء السيبيراني انشأت المديرة العامة للأمن الوطني أول فصيلة على مستواها سنة 2011، ثم تم توسيع استحداثها الى 48 ولاية سنة 2013، ومع تطور وانتشار مخاطر وشبكات الاجرام الالكتروني، تم انشاء مصلحة مركزية على مستوى مديرية الشرطة القضائية سنة 2015، وقد استجابت هذه الهيئة لعدد كبير من الشكاوى المحلية والدولية، وتمكنت من معالجة قضايا تتعلق بجرائم ماسة بخصوصية الأفراد والمؤسسات اضافة الى جرائم الارهاب الالكتروني وشبكات الجريمة العابرة للحدود واستغلال الأطفال، وكانت أول قضية دولية تعاملت معها الشرطة الجزائرية تتعلق بقرصنة بيانات بنكية اثر بلاغ من مكتب التحقيقات الأمريكية FBI سنة 2009، وتعد الشرطة الجزائرية ذات كفاءة وصمعة دولية نتيجة للمؤهلات البشرية والوسائل التقنية العالية، كما تساهم الجزائر في مجال التكوين الدولي وتبادل الخبرة والانخراط في مجال محاربة الجريمة الالكترونية العابرة للقارات بالتعاون مع مكتبي الانتربول والافريبول[32].

4-بناء القدرات الفنية والمتخصصة: تلازم الجزائر بين استراتيجياتها التقنية والتنظيمية من جهة، وفتح مجال التكوين وتعزيز الخبرات حول قضايا الأمن السيبيراني من جهة أخرى، ويستقي هذا الترابط أهميته من كون أن غياب المختصين أو الاعتماد على الخبرات الاجنبية من شأنه أن يقوض من فرص التحكم الشامل في هذا القطاع الأمني الحساس.

بدا الاهتمام بمجال التكوين في الأمن السيبيراني بشكل رسمي في سنة 2018 بعد ان تنبه المسؤولون الحكوميون الى أن تصدر الجزائر في ذات السنة قائمة الدول العربية الاكثر تعرضا للهجمات والجرائم السيبيرانية يستوجب بناء استيراتيجية بشرية وفنية ذات مستوى عال في مجال أنظمة المعلومات وحماية الشبكات، وبذلك ففي سنة 2018 أعلنت الجزائر عن تكوين 24 ألف مهندس وتقني مختص في الأمن السيبيراني لمجابهة الجرائم الإلكترونية[33]. كما أفردت الجزائر تكوين عال ومتخصص لخبراء أمنيين وقضائيين في مجال تقنيات وتشريعات الجرائم الالكترونية

اضافة لذلك فقد أتاح التوجه الحكومي الجديد للاهتمام بالابتكار التكنولوجي الى استحداث مؤسسات جزائرية ناشئة في مجال الأمن السيبيراني مثل شركة INTELLIGENT NETWOR

وSECURE NETWORK[34]، كما عكفت وزارة التعليم العالي والبحث العلمي على اطلاق عروض تكوينية بيداغوجية في تخصصات تهتم بحماية الانظمة والشبكات، وتم عقد عدد كبير من الملتقيات العلمية في تخصصات تقنية واجتماعية ومؤسساتية من شأنها الرفع من حجم الاهتمام بموضوع الأمن السيبيراني، خاصة من حيث تكوين الكفاءات الوطنية.

5-التعاون الدولي: تولي الهيئات الدولية أهمية بالغة لفرص تعاون الدول كمؤشر لمواجهة مخاطر التهديدات السيبيرانية، نظرا لما يمكن أن تتيحه الفجوة الرقمية بين الدول من معيقات لمكافحة المظاهر السلبية للفضاء السيبيراني، اضافة الى حجم انتشار وتعقد هذه المخاطر على أمن الدول، ويعد الاتحاد الدولي للاتصالات أحد أبرز المؤسسات التي توصي بضرورة الاهتمام بمجال التعاون الدولي في تبادل المعلومات والخبرات والتصدي لجرائم تكنولوجيا الاتصال بغرض بناء الثقة والأمان الشامل، ففي هذا الصدد وقعت الجزائر على حزمة من الاتفاقيات الدولية والاقليمية في مجال الأمن السيبيراني، من بينها اتفاقية بودابست لمكافحة جرائم المعلوماتية (المجر 2001)[35].

كما شاركت الجزائر في صياغة والمصادقة على اتفاقيات الجامعة العربية في مجال تبادل المعلومات والخبرات والتعاون في حماية المعطيات ومكافحة جرائم المعلوماتية وتسليم المجرمين في قضايا الأمن السيبيراني، من أهم الاتفاقيات نجد "الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية" (القاهرة 2010)، والمكتب الاقليمي الاتحاد العربي للاتصالات، والذي احتضنت الجزائر اجتماعه الاول في 25 و 26 فيفري 2013، والذي يتضمن فرق عمل لتنسيق الجهود العربية وتوحيد الرؤى ووضع أطر قانونية مشتركة[36].

وعلى مستوى الاتحاد الافريقي صادقت الجزائر على اتفاقية الاتحاد الافريقي حول الأمن السيبيراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014[37]، وهي الاتفاقية التي تعززت بعدد من الاتفاقيات واللجان الافريقية الفرعية بهدف مواءمة المنظومات التشريعية للدول الافريقية ومواكبة التطورات التقنية والتعاونية في مجال الأمن السيبيراني ومكافحة جرائم الانترنيت. كما تشرف الجزائر في اطار اتفاقية التعاون التي اطلقتها الأفريبول على تدريب خبراء جرائم الانترنيت في دول الاتحاد الافريقي[38].

وفي هذا الاطار كيف المشرع الجزائري الاجراءات القانونية في مجال المساعدة التعاون الدولي من خلال 09-04 حيث نص في المادة 15 على اختصاص المحاكم الجزائية بالنظر في الجرائم الالكترونية المرتكبة خارج التراب الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو

المصالح الاستراتيجية للاقتصاد الوطني، واسند مهام الرقابة على هده الجرائم للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بمقتضى المادة 13 التي حددت مسؤولياتها من بينها تبادل المعلومات مع نظيراتها في الخارج فقصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وتحديد مكان تواجدهم[39].

لم تكتفي الجزائر بالجوانب الاتفاقية القانونية والتشريعية في مجال التعاون الدولي، بل ركزت جهودها على الجوانب التقنية الميدانية، حيث شاركت الجزائر في عدد من الورشات الدولية التكوينية في اطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة الالكترونية Cyber Sud[40] ، كما ترأست الجزائر مجموعة خبراء الانتربول المختصة في مكافحة الجريمة المعلوماتية. نظرا لخبرة وجهود الشرطة الجزائرية في هذا المجال[41].

وفي اطار التبادل تشارك الجزائر باستمرار في عدد من المعارض الدولية الكبرى في مجال الابتكار والتطوير التكنولوجي، كمعرض جيتكس للتكنولوجيا 2019، ومعرض اكسبو، اضافة الى للتنظيم السنوي لمعرض ديجيتاك الدولي لتكنولوجيات الاعلام والاتصال (الطبعة الرابعة 2023) معارض وطنية بالشراكة مع شركات رائدة في مجال الاتصالات وتكنولوجيا المعلومات.

.خاتمة:

لقد عملت الجزائر على التكيف مع مقتضيات عصر المعلومات، من خلال التوجه الى الاعتمادية الرقمية وبناء منصات وشبكات رقمية في المجالات الحكومية والخدمات ومازال أمامها مسارات للاستثمار الرقمي والشراكات وتطوير فضاءات الانشطة والتفاعلات الرقمية في مجالات متعددة لاسيما في ظل عزمها خلال السنة الجارية على تسريع وثيرة تعميم الولوج الرقمي في كل المجالات.

في مقابل هذا الزخم سعت الجزائر الى بناء استراتيجيات للأمن السيبيراني تماشيا مع جهودها في تحقيق التحول الرقمي الشامل، خاصة في ظل اعتبار الجزائر كأحد أبرز القوى المستهدفة بأشكال التهديدات السيبيرانية لعدة اعتبارات سياسية واقتصادية وامنية استيراتيجية

وفي هذا الاطار فقد اعتمدت الجزائر على الالتزام بتحسين مناخ الأمن السيبيراني من خلال منظومة تشريعية متوجة باستحداث مؤسسات وهياكل ادارية فاعلة في مجال تحقيق السياسة السيبيرانية، وفيما تتعهد المؤسسات الدفاعية والأمنية مهمة حماية وتحقيق الأمن السيبيراني ضد الهجمات والحروب السيبيرانية من خلال أنظمة قدرات مادية ومؤهلات بشرية، وتسعى الجزائر كذلك الى تطوير بنى التحول الرقمي

للاتصالات نظرا لارتباطها الوثيق بفرض تعزيز الأمن السيبيراني الذي يعد معركة الفصل في ثورة التحول الرقمي التي تجتاح العالم.

لكن ذلك لا ينفي تلك الحاجة الملحة لمزيد من الجهود التي توائم بين مسار هذا التحول العالمي وموقع الجزائر فيه وحجم التهديد الذي يطالها منه، وقدراتها في الصمود والمواجهة بتحسين وتقوية بيئة الأمن السيبيراني، ويمكن في هذا الاطار الاشارة الى بعض التوصيات الأساسية:

– التوجه نحو سن قوانين تتعلق باقتناء الاجهزة والبرامج والتطبيقات الأصلية دون المقلدة خاصة لدى المؤسسات التي تعتمد على برامج مجانية متاحة للتحميل مجهولة المصدر، مما يجعلها عرضة للاختراق.

– العمل على الاهتمام بالوجه الاستغلالي الاخر المتعلق بالحملات الدعائية واستغلال الفضاء السيبيراني لزرع الأفكار المعادية والمساس بالأمن القومي للدولة، ويتم هذا من خلال انفتاح المؤسسات الفاعلة في مجال الأمن السيبيراني على المؤسسات الاعلامية والتعليمية والفضاءات العامة للتحسيس والوقاية. بهدف بناء يقظة اعلامية واجتماعية تساهم في صيانة الأمن السيبيراني والقومي للدولة.

– انشاء مرصد وطني للأمن السيبيراني من شأنه العمل على تقوية نشاط المؤسسات ورصد الاحصائيات والتكوين واقامة شراكات مع مؤسسات ومنظمات وطنية ومحلية.

. التهميش:

[1]باسكال بونيفاس، الجيوبوليتيك: مقاربة لفهم العالم في 48 مقالا، ترجمة: إياد عيسى، (دمشق: منشورات الهيئة العامة السورية للكتاب)، 2020 ،ص 81

[2]Solange Ghernaouti, sybersécurité : Analyser les risques Mettre en œuvre les solutions .dunod : Paris. 2019. P 01.

[3]مني عبد الله السمحان، متطلبات تحقيق الأمن السيبيراني لأمن المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد: 111، جامعة المنصورة، جويلية 2020، ص 09.

[4] Geers Kenneth.Strategic Cyber Security.1st ed. NATO CCD COE Publications; 2011.P 19.

[5] Edward Amoroso, Cyber Security, SiliconPress, 2007 , P01.

[6] منى الأشقر جبور، السيبيرانية: هاجس العصر، دراسات وأبحاث، منشورات جامعة الدول العربية، ص 26

[7] مُحَمَّد مسيكة، الفضاء السيبيراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، العدد الرابع، جامعة الجلفة، ديسمبر 2022، ص 458.

[8] What Is Cybersecurity? [Internet] : https://www.syr-res.com/article/22972.html

[9] مسيكة، ص 455.

[10] فراس قرة، الأمن السيبيراني، الموسوعة السياسية، نشر في 28 أوت 2019، متوفر على الرابط: https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A%A7%D9%86%D9%8

[11] جبور، ص 66.

[12] مسيكة، ص 457.

[13] الأمم المتحدة، دائرة الشؤون الاقتصادية والاجتماعية، مسح الحكومة الالكترونية 2022: مستقبل الحكومة الرقمية، نيويورك، 2022.

[14] Kaspersky Security Bulletin 2018, STATISTICS, KASPERSKY Iab.

[15] علي مجالدي، واقع الأمن السيبيراني في الجزائر، مقال منشور في جريدة الشعب، بتاريخ: 19 ماي 2021، متوفر على الرابط: http://www.ech-chaab.com/ar/%D8%A7%D9%84%D8%AD%D8%AF%D8%AB/%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A/item/171386.html?tmpl=component&print=1

[16] ا جنادي، حوار حول حصيلة 2021، مجلة الجيش، وزارة الدفاع الوطني، جانفي 2022، ص 39.

[17] Digital 2023 : ALGERIA. 13 February 2023. Sur site : https://datareportal.com/reports/digital-2023-algeria

[18] باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبيراني عبر البحر الابيض المتوسط، يوروميسكو euro mesco، المعهد الأوروبي للبحر الابيض المتوسط، جويلية 2021، ص 19.

[19]GUIDE TO DEVELOPING A NATIONAL CYBERSRCURITY STRATEGY. the International Telecommunication Union (ITU). 2018. GENEVA.

[20]قانون رقم 04-15 المعدل و المتمم للأمر 66-155 الصادر بتاريخ 10 نوفمبر 2004 المتضمن تعديل قانون العقوبات

[21]قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009. يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

[22]قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 .يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[23] سلمة بورياح، السياسات العامة الجزائرية في مجال السيبيرانية، مجلة دفاتر السياسة والقانون،، المجلد: 15، العدد: 01، جامعة ورقلة، ص 285.

[24] نفس المرجع، ص 286.

[25] الموقع الرسمي لاتصالات الجزائر: متوفر على الرابط:

https://www.algerietelecom.dz/ar/entreprises/packs-cybersecurite-prod142

[26]مرسوم رئاسي رقم 15-261 بتاريخ 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة t2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[27] مرسوم رئاسي رقم 20-05 بتاريخ 24 جمادى الاولى علم 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية.

رابح سعاد، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، العدد الاول، جوان 2021، ص 280.[28]

[29] نفس المكان.

[30] المصلحة المركزية لمكافحة الاجرام السبرياني، موقع وزراة الدفاع الوطني: متوفر على الرابط:

https://www.mdn.dz/site_cgn/sommaire/presentation/org_missions/org_missions_ar.php

[31] تصريح الرائد فريد درامشية، متوفر على موقع الشروط أونلاين: https://2u.pw/Gto7uT

[32] مصطفاوي عبد القادر، روبورتاج: جهود استباقية للأمن الوطني لتحقيق الأمن المعلوماتي والامتياز في الأداء، مجلة الشرطة، العدد: 129، ديسمبر 2015، ص 142

[33] يونس بورنان، الجزائر...24 ألف مختص في الأمن السيبيراني لمواجهة الجرائم الالكترونية، جريدة العين الاخبارية، أبوظبي، 17 أبريل 2018.

[34] شركة جزائرية ناشئة في مجال الأمن السيبيراني وتقنيات المعلوماتية: موقع الشركة:

https://dz.linkedin.com/company/secure-networkdz

[35] مجلس الاوروبا: مجموعة المعاهدات الاوروبية- رقم 185، الاتفاقية المتعلقة بالجريمة الالكترونية، بودابست، 23 نوفمبر 2001.

[36] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، العدد الثاني، مخبر الحقوق والحريات في الانظمة المقارنة، جامعة بسكرة، الجزائر، 2015، ص 14.

[37] Instrument Juridique de l'Union Africaine, convention de l'union africaine sur la cyber sécurité et la protection des données à caractère

personnel, Adopté par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014.

[38] باولاك وآخرون ، ص 21.

[39] قادري نور الهدى، الجريمة السيبيرانية واليات مكافحتها- مواجهة تحديات الأمن السيبيراني، المجلد:08، العدد: 01، 2023، ص 313.

[40] من موقع وزارة العدل: متوفر على الرابط: https://2u.pw/PLwU2S

[41] من موقع وكالة الأنباء الجزائرية، نشر بتاريخ 28 ماي 2017، متوفر على الرابط:
https://www.aps.dz/ar/algerie/43790-2017-05-28-16-06-05