

إستراتيجية الدفاع الجزائرية لمواجهة التهديدات السيبرانية

Algeria's Defense Strategy for Addressing Cyber Threats

د. محمد جواد بمراح^{1*}، د. رفيقة زبدة²¹ جامعة أبي بكر بلقايد تلمسان/ كلية الحقوق والعلوم السياسية (الجزائر)، bemrah.djawad@gmail.com² جامعة الجلفة/ كلية الحقوق والعلوم السياسية (الجزائر)، rafika.zebda@univ-djelfa.dz

تاريخ القبول: 2025/03/13

تاريخ الاستلام: 2025/01/18

ملخص:

أرست التحولات الكبرى في المجال التكنولوجي بعد الحرب الباردة قاعدة جديدة للتواصل بين الشعوب، عرفت بالفضاء السيبراني. وقد أدى ذلك إلى تحولات على مستوى طبيعة العلاقات الدولية، وموازن القوى العالمية، وأصبحت قوة الدول تعتمد بشكل متزايد على التكنولوجيا وقدرتها على التحكم في تطبيقاتها. هذا الوضع أفرز صراعات بين الدول عرفت بالحرب السيبرانية، حيث تسعى بعض الدول إلى مهاجمة شبكات المعلومات الخاصة بدول أخرى وإلحاق الضرر بها. كهجمات التحكم في أنظمة الدفاع، التشويش عليها، شل منظومات الأسلحة واختراق الأمن الوطني للدول المستهدفة. وعليه سارعت الجزائر إلى إقامة إستراتيجية متكاملة لمواجهة التهديدات السيبرانية. تعتمد على تكييف المنظومة الأمنية الوطنية مع متطلبات الثورة المعلوماتية العالمية. كما تركز على مواجهة التهديدات السيبرانية والاستعداد لها بناء على درجة خطورتها مع تبني منطق التوقع والاحتمال.

الكلمات المفتاحية: إستراتيجية الدفاع، التهديدات السيبرانية، الجزائر، الأمن السيبراني، المواجهة.

Abstract:

The major technological transformations following the Cold War established a new foundation for communication among nations, known as Cyberspace. This development introduced new dynamics in international relations, leading to a global shift in the balance of power. Consequently, the strength of nations increasingly depends on their technological capabilities and their ability to effectively control and utilize these technologies. This situation has given rise to conflicts known as cyber warfare, when some nations aim to attack and damage the information networks of others. These attacks include manipulating the defense systems of targeted countries, disrupting them, paralyzing their weapon systems, and breaching their national security. As a result, cybersecurity has become one of the most significant challenges confronting nations at both regional and global levels.

Algeria has developed a comprehensive strategy to address cyber risks, involves adapting its national security system to align with the requirements of the global information revolution. It focuses on addressing cyber threats based on their severity while adopting an approach grounded in anticipation and preparation for future scenarios.

Keywords: Algeria, confrontation, cyber threats, cyber-security, Defense strategy

مقدمة

أدى التطور الكبير لتكنولوجيا المعلومات والاتصال إلى تحولات سريعة في جميع مجالات الحياة نتيجة الإقبال الكبير من طرف الأفراد ومختلف المؤسسات على استخدام هذه الوسائل في وسط عرف بالفضاء السيبراني باعتباره العالم المادي الذي توجد فيه جميع هذه الأنظمة، والتحدي الكبير الذي يواجهه الدول هو البحث عن تحقيق الأمن السيبراني في هذا الفضاء الذي أصبح حاضنة لظهور وتطور أشكال جديدة من الإرهابيين نسبة للإرهاب غير التقليدي الذي يهدف إلى مهاجمة مختلف البيانات والمعلومات الإلكترونية ونظم الاتصالات، ألا وهو الإرهاب الإلكتروني. هذه التهديدات السيبرانية أصبحت مشكلة عويصة تتفاقم يوما بعد يوم وهي في غالب الأحيان تجاوزات ناتجة عن أطراف تتعمد استغلال الإنترنت واستخدامها لأغراض غير قانونية، وهذا ما يعرف بالجرائم السيبرانية نتيجة سوء استخدام النظم الحاسوبية والشبكات وعلى رأسها الإنترنت، وفي مجال العلاقات الدولية بإمكان الحروب السيبرانية أن تكون عاملا حاسما وفاصلا في العديد من الصراعات التي يشهدها العالم بين مختلف وحدات النظام الدولي، مما دفع بالكثير من الدول لوضع استراتيجيات لمكافحة هذا النوع من التهديدات، والجزائر من الدول التي تعمل على تحقيق أمنها السيبراني اعتمادا على استراتيجية أمنية شاملة لضمان أمنها السيبراني.

إشكالية الدراسة

من خلال ما سبق ذكره نطرح الإشكالية التالية: فيما تتمثل إستراتيجية الدفاع الجزائرية في مواجهتها للتهديدات السيبرانية من أجل تحقيق أمنها السيبراني؟ وتفرع عن هذه الإشكالية مجموعة من التساؤلات المتمثلة فيما يلي:

- 1- ما المقصود بالأمن السيبراني والمفاهيم المرتبطة به؟
- 2- فيما تتشكل أبعاد الأمن السيبراني وأنماط تهديداته؟
- 3- ما هي أهم الهيئات والأجهزة التي أنشأتها الجزائر لمواجهة التهديدات السيبرانية في مسعى جاد لتحقيق أمنها السيبراني؟

الفرضيات

تتمثل استراتيجية الدفاع الجزائرية في مواجهتها للتهديدات السيبرانية في اعتمادها على هيئات وأجهزة مختصة في مكافحة الهجمات السيبرانية.

- 1- يعتبر الفضاء السيبراني مجالا افتراضيا من صنع الإنسان معتمدا على شبكة الإنترنت متضمنا تهديدات سيبرانية كالإرهاب الإلكتروني والحرب السيبرانية.
- 2- يعد الأمن السيبراني مفهوما مرتبطا بأمن الشبكات والأنظمة المعلوماتية والبيانات والأجهزة المتصلة بشبكة الإنترنت.
- 3- اعتمدت الجزائر العديد من الهيئات والأجهزة والمراكز لمكافحة التهديدات السيبرانية من بينها الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها وكذا مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية التابع للدرك الوطني.

أهداف البحث

تهدف هذه الدراسة إلى إبراز إستراتيجية الدفاع الجزائرية لمواجهة التهديدات السيبرانية وتكييفها مع المتطلبات العصرية في العمل الأمني وتجديد مختلف القوانين المتعلقة بمكافحة الهجمات السيبرانية وخلق عدة هيئات وأجهزة لحماية وتحقيق أمنها السيبراني.

مناهج البحث

اعتمدنا في دراستنا على المنهج الوصفي الذي يصف لنا وظيفة ومهام الأجهزة والهيئات الوطنية التي تتولى تنفيذ استراتيجية الدفاع الجزائرية في مواجهتها للتهديدات السيبرانية، وكذا المنهج التاريخي من خلال ذكر تاريخ إنشاء أهم الهيئات والأجهزة المستحدثة من طرف الجزائر التي أوكلت لها مهمة تحقيق الأمن السيبراني. وللإجابة على الإشكالية المطروحة قسمنا موضوع الدراسة إلى العديد من الجزئيات:

أولاً: مدخل مفاهيمي

ثانياً: أبعاد الأمن السيبراني وأنماط التهديدات المحتملة

ثالثاً: إستراتيجية الدفاع الجزائرية لمكافحة التهديدات السيبرانية

أولاً: مدخل مفاهيمي.

أدى ظهور الحاسب الآلي والتوسع في استخدام شبكة الإنترنت في مجالات الحياة المختلفة إلى ظهور العديد من الآثار السلبية والمخاطر المترتبة على هذا التوسع الكبير، إذ كلما زاد الاعتماد على هذه التقنيات زادت المخاطر الناتجة عنها في الفضاء السيبراني وأصبحت التهديدات السيبرانية من أهم التحديات التي تواجه الدول لصدها وتحقيق أمنها السيبراني.

1. الفضاء السيبراني.

تم تعريف الشبكة الاجتماعية الافتراضية بأنها "البنية الجديدة لعصر المعلومات، عصر المجتمع الشبكي المؤلف من شبكات الإنتاج والقوة والتجربة، حيث تقوم هذه الشبكات بدورها في بناء ثقافة افتراضية في إطار التدفقات المعولة، متجاوزة في ذلك مفهومي الزمان والمكان، وقد حصل في عصرنا هذا اختراق جميع المجتمعات بالفعل الجارف للمجتمع الشبكي" (عبدالواحد، 2022).

عرفت قمة الأمن السيبراني الروسية-الأمريكية الفضاء السيبراني بأنه أداة الكترونية يتعين من خلالها إنشاء البيانات والمعلومات ونقلها وتلقيها ومعالجتها والغاءها. (Mbanaso & Dandaura, 2015, p. 18).

كما عرف بأنه "مجال لشبكة محولة مجسدة لنقل حركة المعلومات والبيانات الضخمة، ويتميز بدرجات متفاوتة من الوصول للمعلومات وتعزيزها". (Folsom, 2007, p. 80).

في إطار تقديم تعريفاً أكثر مرونة للفضاء السيبراني، يعتبره Choucri أنه مجال بلا حدود أنشأ من خلال الربط البيئي لملايين الحواسيب بواسطة شبكة عالمية متعددة الطبقات كالإنترنت، حيث تتيح العناصر المادية اطاراً منطقياً رياضياً للترابط يسمح بمعالجة البيانات وتعزيزها ومعالجتها وحتى التلاعب بها، ويتميز باللامركزية في التفاعل بين الجهات الفاعلة (Mbanaso & Dandaura, 2015, p. 19).

2. الأمن السيبراني.

بدأ مفهوم الأمن السيبراني يحظى بالاهتمام الواسع منذ استخدامه من طرف الرئيس الأمريكي "باراك أوباما" عام 2009، حيث اعتبره سبباً لتعزيز الأمن القومي لبلاده، كما اعتبرت التهديدات القادمة من الفضاء السيبراني من أكبر التحديات الأمنية والاقتصادية التي واجهتها الولايات المتحدة الأمريكية (باي، 2023، صفحة 35).

السيبرانية كمصطلح شاعت لأول مرة عام 1984 من قبل «توربرت وينر»، لوصف العمليات النظامية الثلاث وما يتعين داخلها من تفاعلات (مدخلات-مخرجات- تغذية استرجاعية)

يعرف الأمن السيبراني من خلال نوع الأنشطة التي ينشئها مصدر التهديد، بأنه ممارسة اجراءات لمنع التهديدات المحتملة أو الهجمات والبرمجيات الخبيثة التي تستهدف اتلاف المعلومات أو تعطيل العمليات الرقمية بشكل غير قانوني واخلاقي.

(Mbanaso & Dandaura, 2015, p. 7)، في حين تعتبر الوقاية والاكتشاف والاستجابة عناصر حاسمة لتحقيق ذلك المفهوم في إطاره التنظيمي والمؤسسي لتطوير واختبار ميزاته بشكل مستمر.

3- إستراتيجيات الدفاع.

إن مسألة التعلم واكتساب الخبرات من الواقع أمر بالغ الأهمية في ظل المشهد المتطور وبشكل مخيف للأمن السيبراني، ففحص الاستراتيجيات الدفاعية الناجحة وفهم متطلباتها من شأنه أن يعزز بشكل فائق من قدرة الدول والمنظمات والأفراد على مواجهة التهديدات السيبرانية، وسيظل مشهد الأمن السيبراني ديناميكيًا ويتطلب الابتكار المستمر والتعاون اللوجستي والانتقال إلى السحابة ونموذج الثقة الصفري، كنهج استراتيجي لحماية المجال الرقمي وأمن الدول بشكل عام. (Chimezie, Onyinyechi, & Samuel, 2024)

ثانياً: أبعاد الأمن السيبراني وأنماط التهديدات المحتملة.

لأمن السيبراني أبعاد عدة منها الاقتصادي والاجتماعي، السياسي وكلها تعكس صور للاستخدام متعدد الأوجه لتلك التقنيات، وسعت ظهور فرص وابتكارات مترابطة غير مسبوقة، وفي الوقت نفسه دفعت إلى أن تكون مدخلا لبروز العديد من أشكال التهديد.

1- أبعاد الأمن السيبراني.

من الجدير، فهم الأمن السيبراني على أنه مهمة متعددة الأبعاد. دون الادعاء بأنها شاملة، ما يعني أن جميع الدول بحاجة إلى زيادة مستويات نضج ومرونة الأمن السيبراني مع تطور التهديدات المحتملة.

1.1 البعد الاقتصادي:

يعتبر الأمن السيبراني ومرونته من المتطلبات الأساسية للنمو الاقتصادي، وزيادة الرخاء والانتاجية عبر آليات متعددة، من بينها تعزيز ما يعرف بالحوسبة السحابية باعتبارها عامل تمكين أساسي للتحويل الرقمي لاقتصادات الدول والشركات والمنظمات من خلال الوصول إلى موارد وخدمات الحوسبة القابلة للتطوير بطريقة آمنة وأقل تكلفة للعملاء والوكلاء. حتى فكرة التسعير التمييزي في المعاملات الدولية أصبح أكثر سهولة في التنفيذ بسبب التطور المعلوماتي، (U.S, 2024, p. 23)

كما يتيح الأمن السيبراني تفاعلات نشطة مثل التجارة الإلكترونية، المصارف الرقمية وغيرها، ما يعني أن الشركات بمختلف نشاطاتها التجارية والاقتصادية أصبحت تسعى جاهدة إلى جذب أكبر عدد من مختبري البرمجيات والتقنيين في السيطرة والتحكم على معلوماتها للاكتساح الأسواق والكشف الاستباقي والوقائي عن الثغرات الأمنية.

1.2 البعد السياسي:

عززت الدول من أجنداتها الأمنية بعيداً عن الأطر التقليدية، بعد بروز التهديدات المرتبطة بالترابط العالمي والحوادث المصنعة، ابتداءً من هجمات 11 من سبتمبر، الاحتجاجات العربية عام 2010، التغيرات المناخية، جائحة كوفيد 19 وغيرها، وهو ما يستلزم النظر في أمنها السيبراني الذي لا يعني فقط بقدرة الدولة على تحقيق أهدافها والتأثير على الجهات الفاعلة الأخرى، بل تطوير برمجيات تمكنها من البقاء والتقدم، ومن بين البرمجيات التي اعتمدتها العديد من الدول تمكين الروبوتات من توجيه التحليلات السياسية على مواقع التواصل الاجتماعي، برمجيات تحسين النزاهة الانتخابية وكشف التضليل، برامج تخطيط العمليات اللوجستية العسكرية وغيرها.

إلا أنه بعض الحالات تصطدم الحكومات بتطلعات شعوبها في ممارسة تطلعاتها التغييرية للنظام الحاكم والقوانين والمبادئ المؤسسية داخل الفضاء الافتراضي. وربما ما يوضح ذلك بشكل جلي، ما أحدثته وسائل التواصل الاجتماعي وتقنيات الرقمنة في الثورات العربية عام 2010، التي سمحت للأفراد والتجمعات من التحكم في إنتاج ونشر واستقطاب المعلومات التي تمكنها من تحقيق توقعاتها وأهدافها المشتركة (الديمقراطية) في مواجهة السلطة الحاكمة، في هذا الصدد

نجد انفسنا أمام احد صعوبات تحقيق حوكمة الأمن السيبراني، ذلك أن الفضاء السيبراني يعترف بالنظم الديمقراطية وغير الديمقراطية، ففكرة الانفتاح وحرية التعبير وحماية البيانات تنطبق على المستخدمين بغض النظر عن النظام السياسي للدولة .

في حين، كشفت مقابلة أجرتها خدمات الرادار مع 105 من خبراء الأمن إلى أنه بين عامي 2018 و2025، من المتوقع حدوث زيادة بنسبة 300 ٪ في الهجمات الإلكترونية سنويا، ما يدفع بسياسات الدول الى التكيف واستباق ما يمكن ان تحدثه التهديدات المتسارعة والمتغيرة، ولتوضيح ذلك أدى هجوم برمجيات الفدية الاستعمارية على خطوط الأنابيب لعام 2021، على سبيل المثال، إلى إغلاق أحد أهم أنظمة البنية التحتية للطاقة في الولايات المتحدة الأمريكية لمدة 6 أيام، مما أثر على إمدادات الطاقة والأسواق العالمية (Hubbard, 2023, pp. 4,5).

1.3 البعد الثقافي والاجتماعي:

لفترات طويلة، شكل موضوع الأمن السيبراني متغيرا مهما من قبل الأكاديميين والباحثين مرتكزين على أبعاده الاقتصادية والسياسية والتكنولوجية متجاهلين الأبعاد الاجتماعية والثقافية بالرغم من أن مصدره من الإنسان وإليه. مثلت الشبكات الرقمية مقياسا جديدا لفهم السلوك الفردي والمجمعي بناء على متغير الوعي والثقافة وارتباطه بمبدأ الأمن السيبراني. وقد شرح سيمونسون الثقافة بأنها تمنح الأفراد قواعد أو مبادئ مختلفة توفر إرشادات لاتخاذ القرارات، والحاجة إلى تقديم أسباب تنشط هذه المعرفة الثقافية (Collier, Charlotte , Dalal , & Jan , 2023, p. 145). باعتبارها مفهوما مرنا ومتغيرا تتحكم فيه القواعد المجتمعية وتغيره بتطورها، وهو ما يقودنا الى فكرة تغير الوعي بالموضوعات، وما يهم موضوعنا هو مسألة الوعي بالأمن السيبراني وكيفية التعامل معه ومع تهديداته. وقد عرف الوعي بالأمن السيبراني على أنه "درجة فهم المستخدمين لأهمية أمن المعلومات ومسؤوليتهم ويعمل على ممارسة مستويات كافية من التحكم في أمن المعلومات لحماية بيانات المنظمة وشبكاتها. (Collier, Charlotte , Dalal , & Jan , 2023, p. 144)

ما يعني أن مسألة نشر الوعي الإلكتروني الأمني على مستوى الأفراد، العائلة، والمؤسسات يشكل عاملا مهما للحماية من الثغرات والابتزاز الإلكتروني واستغلال الهندسة الاجتماعية الرقمية، والانترنت المظلم، نظرا لضعف الخبرة التقنية والتوجه نحو النظام الافتراضي بدون معارف مسبقة عن أضراره.

1.4 البعد الأخلاقي والقانوني:

تكتسب المسائل الأخلاقية والقانونية التي يثيرها الأمن السيبراني أهمية كبيرة، وتشكل قضايا الخلاف حول الإطار المحدد لتلك المسائل في الموازنة بين مصالح الأطراف حول الخصوصية والمساءلة والعدالة وغيرها. أصبحت هجمات برامج الفدية من أكثر الهجمات شيوعا، والتي تعمل إما على تشفير البيانات او حظر الوصول الى البيانات، بهدف تحقيق مكاسب مالية (دفع الفدية)، والتي في الغالب بعدها يتمكن المستخدمين من الوصول الى بياناتهم ، وما يزيد من تعقد الامر وجود خطأ تأمين المسؤولية السيبرانية وهو ما يفرض خطرا أخلاقيا من خلال الحد من دوافع المنظمات للتعرض لبرامج الفدية، حيث لن تضطر الى تحمل كل تكاليف لتلك الهجمات. (Formosa, Michael , & Deborah , 2021, p. 11). من جهة ثانية، وحول مبدأ المسؤولية ، من يعتبر المسؤول المباشر عن الاختراق هل المستخدم او الآلة خاصة بعد ظهور من يعرف بالذكاء الاصطناعي التوليدي ، ناهيك عن مسألة التتبع وانتهاك الخصوصية التي تعتبر ايضا من القضايا الشائكة قانونيا في تسيير المنظمات ومعاملة الدول لشعوبها ، ما يعني أنه يجب تطوير اطار معياري لمتخصصي الأمن السيبراني يتناول الردع الاخلاقي والقانوني للاستغلال الضار للرقمنة.

2 أنماط التهديدات السيبرانية

يتم التطرق هنا لأهم ما يعترض الدول والمجتمعات من تهديدات إلكترونية تستدعي اللجوء للتعاون من أجل التصدي لها، حيث يضم الفضاء السيبراني مجموعة متنوعة من التهديدات الإلكترونية بعضها يمس الاقتصاد وبعضها يهدد الأنظمة السياسية والإستراتيجيات العسكرية والبعض الآخر يهدد المجتمعات وثقافتها، وعليه سنتطرق لأهم هذه التهديدات:

2.1 الإرهاب الإلكتروني:

عرفته "دينينغ دورتي" على أنه: هجمات غير قانونية وتهديدات بالهجوم ضد الحاسبات والشبكات والمعلومات المخزنة وذلك لتخويف وإجبار حكومة أو شعبها بهدف تعزيز أهداف سياسية أو اجتماعية والتسبب بضرر ينتج عنه توليد الخوف، أما "جيمس لويس" من مركز الدراسات الإستراتيجية والدولية فيعرفه على أنه: استخدام أدوات شبكات الكمبيوتر لتعطيل البنية التحتية القوية مثل الطاقة والمواصلات وعمليات الحكومة أو إكراه أو ترهيب الحكومة أو السكان المدنيين (حموم، 2021).

وتعرفه وكالة المخابرات المركزية الأمريكية بأنه: أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر وبرامجه والبيانات والمعلومات والتي تنتج عن عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين (رافعي، 2021).

2.2 حرب المعلومات (الهجمات الإلكترونية):

يعبر هذا المصطلح عن ارتباط العلاقة بين أطراف مستخدم نظم البيانات ككل في مواجهة الآخر عبر شبكات رقمية يسعى كل منهما الى احراز تقدم على حساب الطرف الآخر للسبق والتقدم على نظمه العسكرية والاقتصادية، يعني أن الحرب الإلكترونية تنقسم إلى شقين: شق هجومي وشق دفاعي.

ويرى "واين وارتو" أن حرب المعلومات تشن على ثلاث مستويات هي:

- حرب المعلومات الشخصية: تلك التي تستهدف خصوصية الأفراد.

- حرب المعلومات بين الشركات والمؤسسات، وذلك في إطار المنافسة الاقتصادية بهدف تعطيل المنافس.

- حرب المعلومات العالمية بين الدول أو بين دول معينة والقوى الاقتصادية العالمية، خاصة في حالة وجود عداوة بينهما (عادل، 2009).

كما يعتبر التجسس عادة شكلا أقل حدة من أشكال الهجوم الإلكتروني من تلك التي تنطوي على تدمير البيانات أو الانكار أو التلاعب (Devey, 2023, p. 22)

وعرفه دليل تالين - القانون الدولي المطبق على الحروب السيبرانية بأنه أي فعل يتم القيام به بصفة سرية أو تحت ذرائع كاذبة يستخدم فيها القدرات السيبرانية لجمع المعلومات بقصد استهداف الطرف الخصم (Weber, 2022)

وهو نفسه ما ذهب إليه المشرع الأردني في قانون الجرائم الإلكترونية عندما عرف التجسس الإلكتروني بأنه: دخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات أو بأي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية أو السلامة العامة أو الاقتصاد الوطني (شاكرعبد، 2020).

لم تسلم أي دولة من عمليات التجسس التي تشكل خطرا على أمنها القومي، من بينها الجزائر، ففي 16 أفريل 2021 تعرض موقع وزارة المالية الجزائرية لهجوم مقرر من طرف مجموعة مغربية مسماة Morocco Hack Team، وقد نشرت بعد مدة صحيفة هسبريس المغربية معلومات عن اختراق عشرات المواقع الإلكترونية المرتبطة بقطاع الحكومة الجزائرية (Sipos, 2023, p. 66)

2.3 الحرب السيبرانية:

مر نشاط الحروب السيبرانية بتطورات متسارعة من تشوييع المعلومات والتجسس الى الهجمات الضارة ضد البنية التحتية الحيوية، بما في ذلك هجمات برامج الفدية وحملات التأثير السيبرانية المصممة، والذي يمس مختلف القطاعات للإضرار بمصالح الدول والمنظمات في الفضاء الإلكتروني وتمكين التهديد المتزايد.

الحرب السيبرانية هي امتداد للحروب التقليدية والمادية، إذ يتألف جنودها من المدنيين والعسكريين في آن واحد، كما أنها حرب أدمغة بالدرجة الأولى كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالا عدة كشكل الاتصالات بين الجيوش وقياداتها وإضعاف شبكات النقل والإمدادات اللوجستية وضرب المعلومات الاقتصادية والعبث بالمحتوى التقني والرقمي وغيرها(شرقي، 2020).

ويمكننا اسناد مثال واضح على ذلك، فبعد أن ألحق الهجوم السيبراني Stuxnet لعام 2010 أضرارا جسيمة بمئات أجهزة الطرد المركزي للمنشآت النووية الإيرانية المتواجدة بالقرب من نطنز، والذي شنته إسرائيل والولايات المتحدة باعتباره هجوما مباشرا وعلنيا (Devey, 2023, p. 3).. ما دفع الدول الى القلق بشأن الامكانات المتطورة للأسلحة السيبرانية، وفعلنا تعتبر تقنيات الذكاء الاصطناعي الحالية نموذجا لدخول مفاهيم جديدة كحرب الروبوتات، الطائرة ذاتية القيادة وغيرها.

ثالثا: إستراتيجية الجزائر الدفاعية لمكافحة التهديدات السيبرانية.

خلال السنوات الأخيرة أصبح استعمال تكنولوجيا المعلومات والاتصال لأهداف إجرامية يشكل أحيانا تحديا حقيقيا لكل الدول لحماية أمنها السيبراني، حيث وضعت الجزائر مسألة تحقيق الأمن السيبراني أحد أولوياتها وركن أساسي ضمن استراتيجية الدفاع الوطنية بالإضافة إلى الجانب القانوني حيث سن المشرع الجزائري الأحكام القانونية وفق تصور يتوفر على العلاج الوقائي والردعي لمكافحة التهديدات السيبرانية.

وأمام هذه الوضعية اعتمدت الدولة الجزائرية في إطار استراتيجيتها الدفاعية على مجموعة من الأجهزة والهيئات التي تعمل على مكافحة الهجمات السيبرانية.

1. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني

لقد تم إنشاء هذا المركز سنة 2008، اختصاصه الوقاية من الجرائم المعلوماتية والإلكترونية ومكافحتها، يعمل على تأمين المنظومة المعلوماتية لتحقيق الأمن العمومي، حيث جاء على لسان رئيس مركز مكافحة الجرائم الإلكترونية للدرك الوطني العقيد جمال بن رجم أن المركز سجل سنة 2017 معالجة مئة (100) قضية تتعلق بالطفولة والمراهقين بسبب الاستعمالات السيئة للإنترنت وعشرون (20) جريمة مالية واقتصادية إلكترونية من ضمن ألف (1000) قضية تمت معالجتها خلال سنة 2017. (الجزائرية، 2018، صفحة 02)

2. المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني

يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني دعامة لقدرات الدرك الوطني في مكافحة الجريمة بجميع أشكالها وذلك بإدراج العلوم في العدالة الجزائية، وهو قوة ردع في خدمة العدالة، أنشئ بموجب المرسوم الرئاسي رقم 133/04 بتاريخ 26 جوان 2004، وظيفته الأساسية هي خدمة العدالة ودعم وحدات التحري في إطار الشرطة القضائية، كما أن للمعهد العديد من المهام كإنجاز الخبرات والتحليل بناء على طلبات القضاة والمحققين والسلطات المؤهلة، والمشاركة كذلك في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام. (الوطني-الجزائر، 2015، صفحة 02)

كما للمعهد نشاطات وطنية ودولية، حيث شارك في مدينة لاهاي لسنة 2024 في حفل تسليم جوائز من طرف "منظمة حظر الأسلحة الكيميائية" وتسلم جائزة عرفانا للمعهد بإسهامه المتميز في تحقيق هدف المنظمة من أجل عالم خال من الأسلحة الكيميائية، وذلك مناصفة مع مجلس المواد الكيميائية للهند، كما أنه خلال المناسبة ذاتها تم انتخاب

الجزائر عن منطقة إفريقيا لتولي منصب نائب رئيس الدورة (29) مؤتمر الدول الأطراف في اتفاقية حظر الأسلحة الكيميائية وانتخاب الجزائر كذلك لعضوية اللجنة السرية لمنظمة حظر الأسلحة الكيميائية. (الجزائرية، الإذاعة، 2024، صفحة 03)

3. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني

تضم هذه المصلحة موردا بشريا متخصصا ومجهز بكافة الوسائل التقنية عالية المستوى المتصلة بالتكنولوجيات الحديثة وهي مؤهلة مهنيا لتنفيذ مهامها وطنيا ودوليا، وتندرج مهامها ضمن مساعي عصبة المصالح العملياتية للشرطة للارتقاء بالعمل الأمني في مواجهة التحديات المرتبطة بكل أشكال الجرائم المعلوماتية والتهديدات السيبرانية التي أفرزتها حروب الجيل الخامس (الوطني، 2023، صفحة 03)، وأضيفت للهيكل التنظيمي لمديرية الشرطة القضائية شهر جانفي 2015، وتم تدشين مقرها الجديد في شهر أكتوبر 2023 بالجزائر العاصمة.

4. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

حدد المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها.

وبموجب المرسوم توضع الهيئة تحت سلطة وزارة الدفاع الوطني، كما حدد مقرها بمدينة الجزائر مع إمكانية تغييره إلى مكان آخر بموجب قرار من وزير الدفاع الوطني، وتضم هذه الهيئة إلى جانب المديرية العامة لمجلس توجيه يرأسه وزير الدفاع الوطني أو ممثله ويتشكل من وزارات الداخلية، العدل، المواصلات السلكية واللاسلكية، كما يقوم مجلس التوجيه دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين عملية المراقبة الواجب القيام بها والأهداف المرجوة بدقة.

أما المديرية العامة للهيئة تتولى السهر على حسن سيرها وإعداد مشروع ميزانيتها وإعداد وتنفيذ برنامج عملها وتعمل على مبادلة المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي هذه الجرائم والتعرف عليهم، كما تضم المديرية العامة مديرية تقنية تتكفل بمهمة المراقبة الوقائية للاتصالات الإلكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة، كما تعمل على مساعدة السلطات القضائية ومصالح الشرطة في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتلك التي تتطلب اللجوء إلى أساليب التحري للهيئة. (الجزائرية و، 2019، صفحة 02)

رجوعا لمختلف الدراسات العلمية والعملية التي أجمعت على أهمية توفر درجة عالية من الوعي لدى الأفراد والمجتمعات لاجتناب الجرائم السيبرانية، فإنه يجب على الأجهزة والهيئات المختصة بمكافحة التهديدات السيبرانية أن تعطي عناية لازمة لمسألة توعية من لهم علاقة مباشرة أو غير مباشرة بمجال المعلوماتية بغية تحقيق الأمن السيبراني، ومتى تحقق ذلك فإن الجانب التوعوي يكون مكملا للجوانب الأخرى كتفعيل القوانين والتنسيق والتعاون لتحقيق الأمن والتعاون الدولي، (للاتصالات، 2017، صفحة 10) وبالرغم من توجه الجزائر حديثا نحو "الحكومة الإلكترونية" تم تسجيل عدد كبير من الجرائم السيبرانية مما يدل حجم المخاطر التي تترص بالجزائر، وهو ما جعلها تواجه تحديات كبيرة من أجل تحقيق أمنها السيبراني حاضرا ومستقبلا.

وحتى تكون إستراتيجية الدفاع الجزائرية أكثر نجاعة في مواجهتها لمختلف الهجمات والجرائم السيبرانية تم استحداث مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة يوم 11 جوان 2015 على مستوى دائرة الاستعمال والتحضير لأركان الجيش الشعبي الوطني، مهمتها حماية مختلف المنظومات والمنشآت الحيوية للبلد من مختلف أنواع الجرائم السيبرانية وخلق تعاون دولي مع العديد من المؤسسات العسكرية الأجنبية خاصة التي لها باع طويل في هذا المجال بغية تبادل التجارب الخبرات والاستفادة منها. (العسكرية، 2017، صفحة 35)

بالإضافة إلى تبني المشرع الجزائري إستراتيجية جديدة لمكافحة الجرائم المعلوماتية، حيث قام بإنشاء "منظومة وطنية لأمن الأنظمة المعلوماتية" بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، (الرئاسي، 2020، صفحة 22) حيث تعتبر المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية وتنسيق تنفيذها، حيث تشتمل المنظومة الأمنية الموضوعة لدى وزارة الدفاع الوطني على كل من وكالة أمن الأنظمة المعلوماتية التي تكلف بتنسيق وتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، كذلك تحتوي على المجلس الوطني لأمن الأنظمة المعلوماتية" يكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها وتوجيهها، ومن أجل ممارسة مهامها يحوز المجلس على مختلف الهياكل المختصة لدى وزارة الدفاع الوطني في هذا المجال.

أما فيما يتعلق بمجال التعاون الدولي فقد سبق للجزائر أن وقعت مع الدول الأعضاء في الشراكة الأورو متوسطية بتاريخ 22 أبريل 2002 على التعاون في المجال الأمني والقضائي لمحاربة مختلف الجرائم، بالإضافة إلى الاتفاق الذي أبرمته الجزائر مع فرنسا بتاريخ 25 فبراير 2003 الذي يتضمن التعاون في مجال الأمن ومكافحة الإجرام المنظم، فاعتمدت الجزائر آنذاك خطة جديدة تمثلت في التعاون لمواجهة الجرائم السيبرانية في المنطقة الجنوبية، من أجل أن تستفيد من التجربة الأوروبية، فعقدت الجزائر لقاءات عديدة جمعت بين فريق من الخبراء من مختلف المؤسسات الناشطة في هذا المجال وبين فريق من الخبراء الأجانب. (الأوروبي، 2004/2001، صفحة 15)

كذلك عمل المشرع الجزائري على تدارك نقص النصوص التشريعية في مجال الجرائم السيبرانية، فاستحدث نصوص خاصة كقانون "الحماية المتعلقة بالأطفال القصر" رقم 14-01 المؤرخ في 04 فيفري 2014 الذي يجرم ترك الأطفال والعاجزين وتعريضهم للخطر وبيعهم، وقانون "الحماية المتعلقة بالبريد والاتصالات الإلكترونية" رقم 18-04 المؤرخ في 10 ماي 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الذي نص على جملة من التدابير الجديدة المنظمة والأحكام الجزائية المترتبة عن مخالفة النظام القانوني لخدمة المواصلات السلكية واللاسلكية، والعمال لدى متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات المستقبلية أو المرسلة أو الصادرة عملاً بنص المادة 137 من قانون العقوبات.

كذلك قانون "الحماية المتعلقة بالتأمينات الاجتماعية" رقم 08-01 المؤرخ في 23 جانفي 2008 المتعلق بالتأمينات الاجتماعية ضد الجرائم المعلوماتية التي ترتكب على البطاقة الإلكترونية، وكذا الحماية من خلال "قانون الملكية الأدبية والفنية" حيث عمل المشرع الجزائري على مكافحة الجريمة الإلكترونية المتعلقة بحقوق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم 03-05 المؤرخ في 23 جويلية 2003، وشدد العقوبات على المساس بحقوق المؤلفين. (بوقرين، 2022، الصفحات 348-350)

وحرص المشرع الجزائري على مواكبة كل التطورات التي تحدث في المنظومة التشريعية الدولية من أجل تحقيق الأمن السيبراني، فأجرى العديد من التعديلات على قانون العقوبات للوقاية من الجرائم التي لها صلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ثم يصدر المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021 الذي ينص على إعادة تنظيم عمل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال. (المرسوم، 2021، صفحة 32) عموماً لقد أثبتت الجزائر جداتها في التعاطي مع الأشكال الجديدة من الإجرام خاصة في تجربتها الطويلة في مكافحة الإرهاب، كذلك الشأن بالنسبة للجرائم الإلكترونية التي أدت بالجزائر إلى إعادة النظر في ترسانتها القانونية وهندسة ميكانيزمات وآليات تسهر على تنفيذها هيئات وطنية مخولة قانوناً بما يمكن من مواجهة التحديات والتهديدات السيبرانية التي تترص بأمنها السيبراني.

كما أن المشكل في الجرائم السيبرانية أنها ترتبط بالتطور التكنولوجي، لذلك فإن ظهور الجرائم يسبق وجود نصوص تشريعية تمنعها، لذلك تجتهد الجزائر في استراتيجيتها للدفاع الوطني من خلال الهيئات المختصة على التحسين المستمر لآليات المواجهة للتهديدات السيبرانية وتعزيز أطرها القانونية لتحقيق الأمن السيبراني.

الخاتمة

على ضوء ما تطرقنا له في دراستنا، ومع تطور المجتمعات والثورة التكنولوجية الهائلة في المعلومات والاتصال تشكل لنا فضاء جديد هو الفضاء السيبراني الذي يستعمله الأفراد كما الدول، تبين لنا أن هذا الفضاء أحدث تغييرات جذرية في مفاهيم العلاقات الدولية كمفهوم القوة والصراع والحرب، وتحول الصراع إلى صراع سيبراني، حيث أصبحت التهديدات السيبرانية خطر الحاضر والمستقبل، مدمرة مختلف القطاعات الاقتصادية والاجتماعية والسياسية وحتى الشخصية.

خلصنا إلى أن تحقيق الأمن السيبراني يبدأ بتحقيق أمن الدولة ثم أمن المجتمع وكذا أمن الأفراد، لذلك اعتبرت الجزائر التهديدات السيبرانية من أهم التحديات الجديدة لاستراتيجية الدفاع الوطنية التي فرضتها التطورات التكنولوجية المتسارعة، فبات من الضروري على الجزائر أن ترسم استراتيجية شاملة تعمم فيها ثقافة مواجهة الأخبار في أوساط مستخدمي تكنولوجيا الإعلام وتطوير التشريعات السيبرانية تماشيا مع التطورات الحاصلة في عالم التكنولوجيا من أجل بناء مجتمع معرفي وتأهيل المناخ للحد من التهديدات السيبرانية وحماية الأنظمة المعلوماتية بالانضمام إلى الاتفاقيات الدولية على غرار اتفاقية بودابست، مما يحفز على التنسيق والتعاون مع الناشطين من خبراء ومؤسسات في ميدان الأمن السيبراني إقليميا ودوليا.

أهم النتائج المتوصل إليها ما يلي:

- أحدث الفضاء السيبراني تغييرات جذرية في مفهوم القوة والصراع بين الدول في العلاقات الدولية بسبب تزايد العلاقة بين الأمن والتكنولوجيا وتعرض المصالح الإستراتيجية لدول لتهديدات سيبرانية تؤثر على الأمن السيبراني للدول.
- تحقيق الأمن السيبراني يبدأ بتحقيق أمن الدولة ثم أمن المجتمع وأفراده.

أما أهم التوصيات تتمثل فيما يلي:

- يجب على الجزائر وضع إستراتيجية شاملة لمواجهة التهديدات السيبرانية للحد منها.
- يجب أن تتماشى هذه الإستراتيجية الشاملة مع التطورات الحاصلة في عالم التكنولوجيا والأنظمة المعلوماتية.

قائمة المراجع:

باللغة العربية:

1. أبوذر شاكر عبد. (2020). التجسس الإلكتروني في ظل التشريع الأردني. (المركز الديمقراطي العربي، المحرر) (06)،
2. الإتحاد الدولي للاتصالات. (2017). تأمين شبكة المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني. سويسرا-جنيف: لجنة الدراسات.
3. الرئاسي المرسوم. (07 نوفمبر، 2021). المرسوم الرئاسي رقم 439-21 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. الجمهورية الجزائرية الديمقراطية الشعبية.

4. المجلس الأوروبي. (23 11, 2004/2001). إتفاقية بودابست الأوروبية حول الإجرام المعلوماتي. بودابست: المجلس الأوروبي.
5. المرسوم الرئاسي. (20 جانفي, 2020). المرسوم الرئاسي رقم 05-20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية. الجمهورية الجزائرية الديمقراطية الشعبية.
6. المسؤول المباشر على مصلحة الأمن السيبراني في المؤسسة العسكرية. (أكتوبر, 2017). حوار مع المسؤول المباشر على مصلحة الأمن السيبراني: فضاء العمليات. 35. الجزائر: مجلة الجيش.
7. حكيم غريب، صبرينة شرقي. (2020). تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة الهجوم الإلكتروني على إيران (فيروس ستكسنت). 12(02).
8. حميدة لحر، فريد حموم. (2021). التعاون الأمني في جنوب شرق آسيا في مواجهة تهديدات الأمن السيبراني. 04(01).
9. د. إدريس عطية. (2019). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. (01).
10. د. إسماعيل زروقة. (أفريل, 2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. 10(01).
11. ربيع رافعي. (2021). الإرهاب الدولي وعلاقته بالجريمة المنظمة: الإرهاب الإلكتروني نموذجاً. 07(01).
12. رجال عبدالواحد. (نوفمبر, 2022). الفضاء السيبراني وتنوع الروافد الهوياتية. 07(07).
13. سليمان قطاف، عبد الحليم بوقرين. (2022). الآليات القانونية الموضوعة لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري. (01).
14. سمير باي. (جوان, 2023). التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول وإستراتيجيات المقاومة. 08(02).
15. عادل عبدالصادق. (2012). القوة الإلكترونية: أسلحة الدمار الشامل في عصر الفضاء الإلكتروني. (188)،
16. عباس بدران. (2010). الحروب الإلكترونية. 04. بيروت / لبنان: مركز دراسات الحكومة الإلكترونية.
17. عبدالصادق عادل. (2009). الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة.
18. محمد مختار. (2015). الأمن السيبراني: مفاهيم المستقبل، اتجاهات الأحداث. (06)،
19. منى الأشقر جبور. (2017). هاجس العصر. 25. بيروت/ لبنان: المركز العربي للبحوث القانونية والقضائية.

باللغة الإنجليزية

1. Chimezie, O., Onyinyechi, V., & Samuel, O. (2024, February 03). COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIE. IT Research Journal, 5(2).
2. Collier, H., Charlotte, M., Dalal, A., & Jan, K. (2023). Cultural Influences on Information Security. European Conference on Cyber Warfare and Security.
3. Devey, E. M. (2023). PUBLIC CYBERATTACK ATTRIBUTION AND DOMESTIC POLITICAL CONSIDERATIONS: AN ANALYSIS OF STATE DECISION MAKING. A thesis submitted in partial fulfillment of Master of Science in Political Science. Utah State University.
4. Folsom, T. C. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). Georgetown .

5. Formosa, P., Michael , W., & Deborah , R. (2021, jun 19). A principlist framework for cybersecurity ethics. Elsevier-computers and security,.
6. Hubbard, G. A. (2023, 8 9). State-level Cyber Resilience:A Conceptual Framework. ACIG, 2(1).
7. Mbanaso, U. M., & Dandaura, E. S. (2015, Jun). The Cyberspace: Redefining A New World. IOSR Journal of Computer Engineering, 17(3).
8. National Cyber Security .(2016) .National Cyber Security .U.K.
9. Sipos, Z. (2023, March 30). CYBERSECURITY IN ALGERIA. Journal of Security and Sustainability Issues, 13.
10. U.S, S. D. (2024). United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future. U.S: U.S. Department of State.
11. Weber, K. (2022, January-March). CYBERSECURITY AND ETHICAL, SOCIAL,AND POLITICAL CONSIDERATIONS: WHENCYBERSECURITY AND ETHICAL, SOCIAL,., Humanities and Social Sciences, 29(1).