

السياسة العامة الأمنية الجزائرية في ضوء التحديات السيبرانية المعاصرة

The Algeria's general security policy in light of contemporary cyber challenges

ملوكي سفيان*، مخبر التحولات الاستراتيجية والجيواقتصادية، جامعة عمار ثليجي - الأغواط-

s.melouki@lagh-univ.dz

جيلالي عمر، جامعة عمار ثليجي - الأغواط-

Omardjilali918@gmail.com

تاريخ إرسال المقال: 2025/06/16 تاريخ قبول المقال: 2025/10/22 تاريخ نشر المقال: 2025/11/29

الملخص:

تمثل السياسة الأمنية في الجزائر رؤية شاملة ومتكاملة للأمن، تتعدى المفهوم التقليدي الذي يقتصر على حماية الدولة لتشمل أيضاً حماية الفرد والمجتمع. وتعتمد هذه السياسة على إرث تاريخي غني، وتراعي الظروف الإقليمية المتغيرة، بالإضافة إلى التحديات العالمية الحديثة. وقد تجلّى ذلك عملياً من خلال تأسيس مؤسسات متخصصة مثل الوكالة الوطنية لأمن الأنظمة المعلوماتية ومراكز مكافحة الجريمة الإلكترونية، مع وضع الأمن السيبراني في صدارة أولويات الدفاع الوطني. على الصعيد التشريعي، أصدرت الجزائر قوانين حديثة تتماشى مع التطورات الرقمية، خاصة في مجالات حماية البيانات الشخصية ومكافحة الجرائم الإلكترونية. كما ركزت الدولة على تطوير الكفاءات البشرية عبر التعليم العالي وبرامج التدريب، مع تنظيم حملات توعية لتعزيز ثقافة الأمن الرقمي بين المواطنين. من الناحية التكنولوجية، حرصت الجزائر على تحديث بنيتها التحتية الرقمية واعتماد حلول محلية مدعومة بتقنيات الذكاء الاصطناعي، مع إيلاء اهتمام كبير لحماية المنشآت الحيوية. ورغم الإنجازات التي تحققت، لا تزال هناك حاجة ماسة لتعزيز الابتكار، وتوسيع نطاق التعاون الدولي، ودعم البحث العلمي في مجال الأمن السيبراني.

الكلمات المفتاحية: السياسة الأمنية الجزائرية، الأمن السيبراني، التهديدات السيبرانية، التشريعات السيبرانية، الحوكمة الرقمية.

Abstract:

Under a broad and inclusive perspective, Algeria's security policy considers both societal and national safety. It is shaped in part by historical context, regional dynamics, and global challenges. The modern Algerian state has established specialized institutions, including cybercrime centers and the National Agency for the Security of Information Systems. Today, Algerian military policy places significant emphasis on cybersecurity. Education and training programs prioritize the development of human capital, while public awareness campaigns play a key role in enhancing digital security. Technological initiatives aim to strengthen locally-developed digital infrastructure, with the protection of critical infrastructure being one of the main

objectives. Despite ongoing progress, cybersecurity research remains underdeveloped and innovation is still limited. Algeria's security policy reflects a dynamic system that continually evolves to meet future security demands.

Key words: Algerian Security Policy, Cybersecurity, Cyber Threats, Cyber Legislation, Digital Governance.

المقدمة:

تمثل السياسة العامة إطارا مركزيا في الحوكمة الحديثة حيث تتقاطع الأبعاد النظرية مع التطبيقات العملية لمواجهة التحديات المجتمعية المعقدة وفي ظل التحولات الجيوسياسية والتكنولوجية المتسارعة، تبرز السياسة الأمنية كأحد الركائز الأساسية التي تعتمد عليها الدول لضمان استقرارها، خاصة مع تنامي التهديدات العابرة للحدود كالجريمة المنظمة والاختراقات السيبرانية. وتكتسب هذه السياسة زخما متعظما في البيئة الدولية الحالية التي تتسم بغياب الفواعل الموحدة وهشاشة الحدود التقليدية في مواجهة المخاطر غير المتماثلة.

في هذا السياق، تواجه الجزائر بحكم موقعها الجيواستراتيجي الحساس بين دول المغرب العربي والساحل الأفريقي تحديات أمنية مركبة، تفاقمت مع التحول الرقمي المتسارع وزيادة الاعتماد على البنى التحتية الإلكترونية في القطاعات الحيوية كالطاقة، والمالية، والدفاع، وقد أدى تصاعد الهجمات الإلكترونية المنسوبة إلى فواعل غير دولية إلى تعريض الأمن القومي للخطر، ما استدعى تبني استراتيجيات أمنية استباقية تعتمد على تعزيز الوقاية، وتحديث الأنظمة التقنية، وتأهيل الكوادر البشرية المتخصصة.

أهمية الدراسة:

تسعى هذه الدراسة إلى تحليل الإطار الاستراتيجي الذي تتبناه الجزائر لمواجهة التهديدات السيبرانية مع التركيز على سياسات تأمين الفضاء الرقمي، وحماية البنى التحتية الحرجة، والتفاعل مع التوجه العالمي نحو حوكمة إلكترونية آمنة، كما تستكشف الدور المحوري للاستثمار في التكنولوجيا المتقدمة وتنمية القدرات البشرية كمدخلات جوهرية لتعزيز المرونة الأمنية في عصر التحولات الرقمية غير المسبوقة.

على ضوء ما تقدم فإن مشكلة هذا البحث تتلخص في:

إلى أي مدى تمكنت السياسة العامة الأمنية الجزائرية من مجابهة التهديدات السيبرانية الراهنة في

ظل التحول الرقمي المتسارع؟

وللإجابة على هذه الإشكالية الرئيسية وللإحاطة بالموضوع وبالجانب النظري للدراسة، قمنا بالاستعانة بالمنهج الوصفي الذي يعتمد على الوصف الدقيق للظواهر والمفاهيم المرتبطة بالسياسة العامة الأمنية في الجزائر، إضافة إلى الاستعانة بالمنهج التحليلي، وذلك لتحليل مختلف النصوص القانونية في التشريع الجزائري وإطارها الإستراتيجي الذي تتبناه في مواجهة التهديدات السيبرانية. كما تم الاستعانة أيضا بالمنهج الاستشرافي من خلال استشراف السيناريوهات المستقبلية والتطورات المحتملة في الأمن السيبراني الجزائري في ظل التحول الرقمي، وبموجب ذلك:

تم تقسيم هذه الدراسة إلى ثلاث محاور رئيسية مترابطة، تُعالج كل منها جانبًا محددًا من موضوع السياسة الأمنية السيبرانية في الجزائر. يتناول المحور الأول الإطار النظري والمفاهيمي، من خلال توضيح مفاهيم الأمن، والسياسة العامة، والسياسة الأمنية السيبرانية، إلى جانب عرض أبرز النظريات المفسرة لهذا المجال. أما المحور الثاني، فيركّز على تشخيص واقع السياسة الأمنية السيبرانية الجزائرية، من خلال تحليل أربعة أبعاد أساسية: البعد المؤسسي، البعد التشريعي، البعد التكنولوجي، والبعد البشري. بينما يُخصّص المحور الثالث لتقييم السياسات الحالية واستعراض أهم الاختلالات والتحديات، مع تقديم حلول تصحيحية واقتراح سيناريوهات وآفاق مستقبلية لتعزيز فعالية الأمن السيبراني الوطني.

1- السياسة العامة الأمنية: دراسة مفاهيمية ونظرية

1.1- مفهوم السياسة العامة الامنية:

1.1.1- التعريف اللغوي للأمن:

الأمن في اللغة هو العكس التام للخوف، والفعل الثلاثي "أمن" يعني تحقيق الأمان. وقد قال ابن منظور: "أمنت لنفسي، وأمنت الآخرين، أي حفظت سرهم"¹، وقد ورد هذا المفهوم في القرآن الكريم بقوله تعالى: {فَلْيَعْبُدُوا رَبَّ هَذَا الْبَيْتِ الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَآمَنَهُمْ مِنْ خَوْفٍ}².

وتتفق معظم الأدبيات التي قامت بتعريف مفهوم الأمن على أن المفهوم يشير عموماً إلى تحقيق حالة من عدم الشعور بالخوف، وإحداث شعور بالأمان في الجانبين النفسي، والجسدي.

2.1.1- التعريف الاصطلاحي للأمن:

الأمن اصطلاحاً يعني الحالة التي يتم فيها الحفاظ على سلامة الأفراد والمجتمع والدولة من الأخطار والتهديدات الداخلية والخارجية، والحفاظ على الاستقرار السياسي، والاقتصادي، والاجتماعي، والثقافي، والبيئي، والتكنولوجي، والعسكري والأمني بشكل عام³.

3.1.1- تعريف السياسة العامة:

يشابه مفهوم السياسة العامة العديد من المفاهيم في حقل العلوم الاجتماعية من حيث تعدد التعريفات واختلاف زوايا تناول، الأمر الذي حال دون وجود تعريف موحد أو جامع له. ولا يزال هذا المفهوم محل اجتهادات نظرية ومنهجية متواصلة من قبل الباحثين بهدف تقنينه وضبط حدوده المفاهيمية⁴.

فعرّفها أوستن ريني بأنها علاقة التبعية والطاعة من جانب، والسلطة والسيطرة من جانب آخر⁵. أما ماكس فيبر Weber فعرفها من زاوية التأثير على الآخرين بأنها "احتمال قيام شخص ما في علاقة الاجتماعية بتنفيذ رغباته رغم مقاومة الآخرين، بغض النظر عن الأساس الذي يقوم عليه هذا الاحتمال" يعكس هذا المنظور قدرة النخبة على الوصول إلى القيم⁶.

لقد وصف العديد من علماء السياسة النظام بشكل عام باعتباره مجموعة من الأجزاء تشكل فيما بينها نسقا من العلاقة المتبادلة في إطار تلك الوحدة الكلية، وعلى هذا الأساس يولي أصحاب هذا الاتجاه أمثال

ديفيد إستون Easton اهتماما بالسياسة العامة أي، من وجهة تحليل النظم كنتيجة ومحصلة في حياة المجتمع من منطق تفاعلها الصحيح مع البيئة الشاملة التي تشكل فيها المؤسسات والمرتكزات والسلوكيات أصولا للظاهرة السياسية التي يتعامل معها النظام السياسي فيعرفها بأنها "عملية تخصيص سلطوي للقيم المادية والمعنوية داخل المجتمع في تفاعلية بين المدخلات والمخرجات والتغذية العكسية. من خلال القرارات، والأنشطة الإلزامية الموزعة لتلك القيم⁷.

أما **جيمس أندرسون Anderson** فيعرفها بأنها "برنامجا موجهها يتبعه أداء فردي أو جماعي بهدف التصدي لمشكلة معينة أو معالجة قضية محددة، حيث يتم تطوير هذا البرنامج من قبل الهيئات الحكومية ضمن نطاق مسؤولياتها، مع الإشارة إلى أن بعض الفواعل غير الرسمية قد تساهم بدورها في صياغة وتطور هذه السياسات"⁸.

أما عن الكتاب العرب فقد برزوا أيضا في تعريف السياسة العامة ونذكر منهم:
يعرفها **خيري عبد القوي** بأنها "تلك العمليات والإجراءات السياسية وغير السياسية التي تتخذها الحكومة بقصد الوصول إلى اتفاق على تعريف المشكلة، والتعرف على بدائل حلها وأسس المفاضلة بينها تمهيدا لاختيار البديل الذي يقترح إقرارا في شكل سياسة عامة ملزمة تنطوي على حل مرض للمشكلة"⁹.
ويعرفها **أحمد سعيغان** بأنها "تعبير عن الرغبة الحكومية بالعمل، أو الامتناع عن العمل، وهي مجموعة مبنية ومتماسكة من القرارات، والإنجازات يمكن نسبها لسلطة عامة محلية، وطنية أو فوق وطنية، فتضم بذلك أربعة عناصر: الهدف؛ اختيار الأفعال التي تحققه؛ إعلان الفاعلين لهذه السياسة؛ تنفيذ هذه السياسة"¹⁰.
فإنها بذلك تترجم لما تقوله الحكومة وما تفعله إزاء المشاكل الحساسة، لذا، فتعريف السياسة العامة من المنظور الحكومي، يمثل منطلقا علميا من خلال دراسة جوانب السياسة وممارساتها المؤثرة في صنع السياسة العامة.

4.1.1 - مفهوم السياسة العامة الأمنية:

يعرف **سيباستيان روشيه Roché** السياسة العامة الأمنية في مؤلفه السوسيولوجيا السياسية للأمن على أنها "مجموع الترتيبات التشريعية والتنظيمية المستعملة لإدارة المجال الأمني، وكذلك الأنشطة والبرامج العامة التي تعمل النخب المحلية والوطنية على إنجازها، وحتى الإدارات، سواء أكانت بمفردها أم باشتراكها مع شركاء آخرين، جمعويين كانوا أم تجاريين". وحسب روشيه فإن السياسات العامة الأمنية كما تخاطب أصحاب العنف، فهي تخاطب أيضا الضحايا والرأي العام¹¹.

ترتبط السياسات الأمنية العامة بشكل وثيق بالإطار المؤسسي والديناميكيات السياسية، مما يجعل معالجة القضايا الأمنية رهينة بطريقة تعريفها وموقعها داخل النظام السياسي. فحين تُفسر الجريمة كمظهر لفشل اجتماعي أو فردي، يُركز التدخل على العقاب والرقابة، بدلا من الوقاية والمعالجة التربوية، والاجتماعية. وتكتسب السياسة الأمنية بعدها المفاهيمي من طبيعة العلاقة بين الأمن، والدولة، والمجتمع، كما أن تصورات

الفاعلين داخل القطاع الأمني تُسهم في رسم السياسات وفق منطق الحداثة ومتطلبات الحوكمة. ويُعد الأمن البشري مفهوماً محورياً في هذا السياق، إذ يربط الأمن بكرامة الإنسان وحقوقه الأساسية، والتنمية الشاملة. وتبرز الحاجة إلى مواءمة بين صياغة السياسات وتنفيذها، حيث أن الممارسة الميدانية قد تختلف تبعاً للخصوصيات المحلية، مما يستوجب تكيف السياسة الأمنية مع الواقع. كما يشير بعض الباحثين إلى أهمية إشراك مختلف الفاعلين في صياغة وتنفيذ هذه السياسات لضمان الفاعلية، والانسجام. وفي ظل هذه التحديات، يصبح التواصل الفعّال بين صناع القرار والمنفذين ضرورة استراتيجية لضمان استقرار السياسات الأمنية واستدامتها¹².

2.1- نظريات السياسة العامة الأمنية :

1.2.1- المدرسة الواقعية:

تعد النظرية الواقعية من أبرز النظريات في العلاقات الدولية، وقد نشأت لتحليل عوامل القوة والصراع والحروب، مع تركيزها الأساسي على الدولة باعتبارها الفاعل الرئيسي في النظام الدولي. تنطلق الواقعية من فرضية مفادها أن النظام الدولي يتسم بالفوضى لغياب سلطة مركزية عليا تنظم العلاقات بين الدول، ما يدفع كل دولة لتحمل مسؤولية أمنها بنفسها، والسعي لحماية مصالحها باستخدام أدوات القوة والحرب¹³.

يرى **كينيث والتز**، أحد أبرز منظري الواقعية الجديدة، أن بنية النظام الدولي فوضوية بطبيعتها، مما يجعل الأمن الهدف الأسمى للدول، في إطار ما يُعرف بمفهوم "كل دولة لنفسها". وترى الواقعية أن الحرب وسيلة لتصحيح اختلال ميزان القوى، بما يؤدي إلى إعادة تشكيل النظام لا تغييره جذرياً، حيث تظل الدولة المهيمنة تحتل مكانة مركزية، مع وجود قوى أخرى تدور في فلكها¹⁴.

يُعتبر مفهوم الأمن في هذا السياق عن "البقاء"، كما أشار **ولفرز Wolfers**، ويُنظر إليه كغاية رئيسية تتطلب التسلح واستخدام القوة، خاصة العسكرية، كوسيلة أساسية لحماية المصالح القومية¹⁵. وقد شدد **هانز مورغانثاو Morgenthau** عميد المدرسة الواقعية، على أن السياسة الدولية هي صراع دائم على القوة والنفوذ، مؤكداً أن أهداف الدول تتجسد في الحفاظ على القوة، زيادتها، ثم إظهارها، وأن العلاقات الدولية تخضع فقط لقانون المصلحة الوطنية¹⁶.

يرى الواقعيون أن الإنسان بطبعه أناني وعنيف، وهو ما يجعل الصراع حتمياً، كما يتفق مع أفكار مكيافيلي. ومع ذلك، وُجهت انتقادات كثيرة للمدرسة الواقعية من أبرزها، تجاهلها للأبعاد الاجتماعية والروحية، وتركيزها المفرط على القوة العسكرية، فضلاً عن الفصل الحاد بين السياسة الخارجية والداخلية، مما يحدّ من قدرتها على تفسير تعقيدات النظام الدولي المعاصر بشكل شامل ومتوازن¹⁷.

2.2.1- المدرسة الليبرالية:

تُعد المدرسة الليبرالية امتداداً للفكر المثالي في العلاقات الدولية، حيث ترفض افتراضات المدرسة الواقعية التي ترى الدولة كفاعل وحيد في النظام الدولي. في المقابل، تؤمن الليبرالية بتعدد الفاعلين، كالمؤسسات

الدولية، والمنظمات غير الحكومية، والشركات، وحتى الأفراد، وتعتبر أن لهم دوراً محورياً في تعزيز الأمن الدولي. تؤكد الليبرالية على أهمية الاعتماد المتبادل بين الدول في الجوانب الاقتصادية، والاجتماعية، والسياسية، لما له من دور في تقليل فرص الصراع وتعزيز التفاهم والسلام بين الشعوب.

ويرى فوكوياما أن انتشار الديمقراطية الليبرالية هو السبيل الأفضل للحد من الحروب، إذ تميل الدول الديمقراطية إلى حل خلافاتها بوسائل سلمية، مما يجعل الديمقراطية أداة لبناء السلام العالمي. ومن هذا المنطلق، تعارض الليبرالية اعتبار الحرب ظاهرة طبيعية، كما تدّعي الواقعية، بل تراها انحرافاً يجب الحد منه عبر الاتفاقيات والمؤسسات الدولية التي تسعى للحفاظ على المصالح المشتركة وتعزيز الاستقرار¹⁸.

وتولي الليبرالية اهتماماً شاملاً لا يقتصر على الجانب العسكري، بل يشمل قضايا مثل مكافحة الإرهاب، حقوق الإنسان، والتنمية المستدامة. كما تتجلى أبرز أفكار الليبرالية في طرح إيمانويل كانط، الذي اقترح إنشاء اتحاد دولي يعاقب أي دولة معتدية، ليس من خلال قوة عظمى، بل من خلال تكتل دولي منظم، مؤمناً بأن السلام هو الحالة الطبيعية وأن التعاون نابع من انسجام الطبيعة البشرية¹⁹.

وينقاطع هذا التصور مع أفكار روسو، الذي يرى أن الحروب ليست نتيجة لطبيعة الإنسان، بل تُهندسها الحكومات الاستبدادية من أجل توسيع نفوذها وثروتها. وعليه، تسعى الليبرالية إلى بناء نظام دولي يقوم على التعاون، والديمقراطية، وسيادة القانون، معتبرة أن السلام الدائم قابل للتحقيق من خلال ترسيخ القيم الإنسانية والمؤسسات الليبرالية²⁰.

3.2.1- نظرية السلام الديمقراطي:

تعود جذورها إلى أفكار الفيلسوف الألماني إيمانويل كانط في القرن التاسع عشر الميلادي، وتستخدم للترويج للقيم السياسية الليبرالية التي تدعم الديمقراطية لأن التاريخ لم يعرف الحروب بين الديمقراطيات، فهذه الديمقراطية تقوم على أساس الإجماع، والعقلانية، والحوار، وبالتالي فالدبلوماسية تتفوق على الحرب. والسلام الديمقراطي ما هو إلا نتاج وجود ثقافة وآليات ديمقراطية تركز الاختلاف والتعددية وتؤسس لحالة الحوار والمشاركة، لا الإملاء، والإقصاء. هو مشترك وتعاوني لجميع دول النظام الدولي. إن التعاون بين الدول ضرورة في عالم تتكاثر فيه الروابط في ضوء الموارد المحدودة²¹.

4.2.1- المدرسة النقدية:

شهد النظام الدولي بعد الحرب الباردة تحولات جوهرية مست مختلف أبعاده السياسية، والاجتماعية، والاقتصادية، بفعل الثورة التكنولوجية والمعلوماتية، وتراجع الحدود التقليدية بين الدول. رافقت هذه التحولات تهديدات أمنية جديدة غير تقليدية، حيث أصبحت النزاعات ذات طابع داخلي أكثر منها بين الدول، بفعل عوامل عرقية ودينية، وسياسية محلية. هذا الواقع جعل المنظور الواقعي التقليدي غير قادر على الإحاطة بجميع أبعاد الظاهرة الأمنية المعقدة والمتغيرة²².

أمام هذا التحدي، ظهرت الحاجة إلى توسيع مفهوم الأمن وتجاوز التصورات التقليدية التي حصرت التحليل في الدولة فقط كفاعل مرجعي. وفي هذا الإطار، برزت إسهامات المدرسة النقدية التي أعادت تشكيل الخطاب الأمني من خلال التركيز على الفرد والمجتمع كركيزتين أساسيتين لفهم الأمن، معتبرة أن حماية الإنسان وضمان حريته يشكلان جوهر السياسات الأمنية الجديدة.

ساهم ستيفن والت في توصيف هذه المرحلة بأنها "عصر النهضة للدراسات الأمنية"²³، بينما عمل باحثون مثل ويفر على إدخال مفاهيم جديدة كـ "الأمن المجتمعي"، الذي يعكس طبيعة التهديدات التي تتجاوز الدولة²⁴. كما تدعو النظرية النقدية إلى تفكيك البنى السلطوية العالمية التي تعيد إنتاج الهيمنة وتعيق التحرر الإنساني، وتحت على إعادة صياغة دور القوات المسلحة، من خلال إشراك الفاعلين غير الحكوميين في عمليات بناء السلم والأمن.

تهدف هذه المدرسة إلى بناء نظام عالمي أكثر عدالة، من خلال دعم المنظمات الحقوقية والتنمية، وإعادة النظر في مركزية الدولة في تحديد طبيعة التهديدات الأمنية. بذلك، تساهم المدرسة النقدية في تجاوز الرؤية الصلبة للأمن، وتكرس فهماً شمولياً يضع الإنسان في صميم الاهتمام الأمني²⁵. وفي المجمل، مثلت هذه المقاربة تطوراً كبيراً في حقل العلاقات الدولية، وأعادت تعريف مفهوم الأمن ليشمل مختلف التهديدات التي تمس بكرامة الإنسان وحريته، في تفاعل واضح مع الظواهر الاجتماعية والاقتصادية العالمية.

2- أبعاد السياسة العامة الأمنية الجزائرية:

سنتناول في هذا المحور أبعاد السياسة العامة الأمنية الجزائرية في ظل التهديدات السيبرانية الراهنة، وذلك من خلال دراسة لأربعة أبعاد رئيسية متكاملة: البعد المؤسسي، والبعد التشريعي، والبعد التكنولوجي، والبعد البشري. سيسعى التحليل إلى استكشاف الهياكل التنظيمية والفاعلين الرئيسيين في مجال الأمن السيبراني، وتقييم الإطار القانوني والتنظيمي الذي يحكم هذا المجال، ودراسة البنية التحتية والقدرات التقنية المتاحة لمواجهة التهديدات، وأخيراً، تحليل دور الكفاءات البشرية وبرامج التدريب والتوعية في تعزيز الأمن السيبراني.

1.2- البعد المؤسسي للسياسة الأمنية السيبرانية الجزائرية:

تتعدد الهيئات الوطنية الجزائرية المعنية بالأمن السيبراني، وتتوزع مهامها بين وضع الاستراتيجيات والتنفيذ، والتحقيق، والوقاية. نذكرها على النحو التالي:

أ/ **المجلس الأعلى للأمن:** هيئة استشارية لرئيس الجمهورية تختص بكافة مسائل الأمن القومي. تأسس بموجب دستور 1976، ومن الطبيعي أن يتناول التهديدات السيبرانية الكبرى التي تمس الأمن الوطني، ويضع التوجهات السياسية العليا لمواجهتها²⁶.

ب/ **وزارة الدفاع الوطني:** تلعب دوراً مركزياً وقيادياً في جهود الأمن السيبراني الوطنية. وقد نظمت الملتقى الوطني حول استراتيجية الأمن السيبراني، وتشرف على هيئات سيبرانية رئيسية.

ج/ المجلس الوطني لأمن الأنظمة المعلوماتية: أنشئ بموجب المرسوم الرئاسي 20-05، يرأسه وزير الدفاع الوطني أو من يمثله. ويتألف من ممثلين عن رئاسة الجمهورية، والوزير الأول والوزارات الرئيسية الخارجية، والداخلية، والعدل والمالية والطاقة، والاتصالات، والتعليم العالي. يختص في البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية؛ والإشراف على مخطط عمل الوكالة الوطنية، وتقارير نشاطها، والموافقة على اتفاقيات التعاون الدولي، وإقرار سياسات التصديق الإلكتروني، وتصنيف الأنظمة المعلوماتية، واقتراح تكييف الأطر الهيكلية والتنظيمية، وإبداء الرأي الملزم في مشاريع القوانين ذات الصلة.

د/ الوكالة الوطنية لأمن الأنظمة المعلوماتية (ANSSI Algérie): أنشئت بموجب المرسوم الرئاسي 20-05 كمؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ومقرها مدينة الجزائر. من المهام الرئيسية لها تحضير عناصر الاستراتيجية الوطنية وعرضها على المجلس، وتنسيق تنفيذها، واقتراح كفاءات اعتماد مدققي أمن النظم؛ وإجراء تحقيقات رقمية في الهجمات السيبرانية؛ وجمع وتحليل وتقييم البيانات لتأمين منشآت المؤسسات الوطنية، ومتابعة عمليات تدقيق أمن النظم وتقديم المساعدة للمؤسسات والإدارات، وضمان اليقظة التكنولوجية؛ ودعم معالجة الحوادث، وجرد وتصنيف الأنظمة المعلوماتية، وإعداد مشاريع النصوص التشريعية والتنظيمية، وتطوير المرجعيات والأدلة العملية، واعتماد منتجات أمن النظم والتصديق عليها، والقيام بأنشطة التكوين والتحسيس²⁷.

تعمل تحت إدارة مدير عام، وتضم مركزاً عملياتياً وطنياً لأمن الأنظمة المعلوماتية، ومصالح تقنية وإدارية، وتدعمها لجنة توجيه ولجنة علمية، ويبدو أن وكالة أمن الأنظمة المعلوماتية لدائرة الاستعمال والتحضير للأركان الجيش الوطني الشعبي في هذه الوكالة أو كيان وثيق الصلة بها ضمن هيكل وزارة الدفاع الوطني.

هـ/ الدرك الوطني، يضم:

مركز الوقاية من جرائم الإعلام الآلي: أنشئ عام 2008، وكان يعتبر الجهاز الوحيد المختص آنذاك، يقوم بتحليل بيانات الجرائم المعلوماتية، وتحديد هوية مرتكبيها، وتأمين الأنظمة المعلوماتية، كما يقوم بحملات توعية²⁸.

المعهد الوطني للأدلة الجنائية وعلم الإجرام: دخل حيز الخدمة سنة 2009، تابع لوزارة الدفاع الوطني، وتتولى مع مصلحة الإعلام الآلي التابعة له رصد ومراقبة عمليات الاختراق والقرصنة، والكشف عن المعلومات المسروقة، وتفكيك البرامج الضارة²⁹.

و/ المديرية العامة للأمن الوطني (DGSN) ، تضم:

المصلحة المركزية لمكافحة الجريمة المعلوماتية: أنشئت عام 2011، أدمجت في مديرية الشرطة القضائية عام 2015 تتولى التحقيق في الجرائم السيبرانية³⁰.

ي/ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (ONPLITIC):

أنشئت بموجب المرسوم الرئاسي 15-261، وكان قد نص على إنشائها سابقاً القانون 09-04. وهي سلطة إدارية مستقلة لدى وزير العدل، من المهام الرئيسية اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وتنشيط، وتنسيق عمليات الوقاية، ومساعدة السلطات القضائية، ومصالح الشرطة القضائية في مكافحة هذه الجرائم (جمع المعلومات الخبرة القضائية)، وإجراء مراقبة وقائية للاتصالات الإلكترونية لكشف الجرائم المتعلقة بالإرهاب، والتخريب، والمساس بأمن الدولة³¹.

2.2- البعد التشريعي للسياسة الأمنية السيبرانية الجزائرية:

يمثل الإطار التشريعي الركيزة الأساسية التي تُبنى عليها السياسة العامة للأمن السيبراني في أي دولة، والجزائر ليست استثناءً، فقد سعت السلطات الجزائرية، إدراكاً منها لخطورة التهديدات السيبرانية وتزايدها، إلى وضع ترسانة قانونية تهدف إلى الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وحماية الفضاء السيبراني الوطني.

لم يأت الاهتمام التشريعي بالأمن السيبراني دفعة واحدة، بل مر بمراحل عكست التطور التكنولوجي وتنامي التهديدات. ففي البداية، تم التعامل مع بعض جوانب الجرائم السيبرانية ضمن الأطر القانونية القائمة، مثل: اعتبار برامج الحاسب الآلي مصنوعات أدبية محمية بموجب الأمر رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة، لكن الحاجة الملحة لتأطير قانوني متخصص دفعت المشرع الجزائري إلى إدخال تعديلات جوهرية على المنظومة القانونية³².

شكل القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، خطوة أولى مهمة بإدراجه قسماً خاصاً يتعلق بـ "المساس بأنظمة المعالجة الآلية للمعطيات"³³، تلاه القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 الذي وسع نطاق التجريم ليشمل أفعالاً أكثر تحديداً مثل الدخول أو البقاء غير المشروع في نظام معلوماتي، إدخال أو حذف أو تعديل البيانات بطريق الغش، وتصميم، أو نشر، أو الاتجار في معطيات مخزنة بطرق غير قانونية³⁴.

يُعد القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، النص التشريعي المحوري في مجال الأمن السيبراني بالجزائر، وضع هذا القانون إطاراً شاملاً لمكافحة هذه الجرائم، معرّفاً إياها في مادته الأولى بأنها تشمل "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الإلكترونية"، هذا التعريف الواسع يعكس رغبة المشرع في استيعاب التطورات المستقبلية للجرائم السيبرانية³⁵.

أرسى القانون 09-04 مجموعة من الآليات الوقائية والإجرائية لمواجهة الجرائم السيبرانية، منها:

أ/ المراقبة الإلكترونية: أجاز القانون اللجوء إلى المراقبة الإلكترونية للاتصالات بموجب إذن قضائي في حالات محددة، مثل: الوقاية من الأفعال الإرهابية، أو التخريبية، أو الجرائم الماسة بأمن الدولة، أو وجود

تهديد وشيك للنظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني (المادة 4 من القانون 09-04)³⁶.

ب/ الاستعانة بمزودي الخدمات: ألزم القانون مزودي الخدمات بتقديم المساعدة للسلطات القضائية، لا سيما في جمع، وتسجيل، وحفظ -المعطيات المتعلقة بحركة السير- (بيانات التعريف، والتجهيزات، ووقت الاتصال ومدته، والوجهة، إلخ) ووضعها تحت تصرف السلطات، كما ألزمهم بالتدخل لسحب المحتوى غير القانوني أو حجب الوصول إليه (المادتان 11 و12 من القانون 09-04)³⁷.

ج/ التفتيش والحجز: نظم القانون إجراءات تفتيش وحجز المنظومات المعلوماتية والمعطيات التي تحتويها، بما في ذلك إمكانية التفتيش عن بعد، وأجاز تسخير الخبراء للمساعدة في هذه العمليات (المادتان 3 و7 من القانون 09-04)³⁸.

د/ تمديد الاختصاص القضائي: منحت المحاكم الجزائرية اختصاصاً للنظر في الجرائم السيبرانية المرتكبة خارج الإقليم الوطني إذا استهدفت مؤسسات الدولة أو مصالحها الاستراتيجية³⁹.

هـ/ التعاون القضائي الدولي: أكد القانون على أهمية تبادل المساعدة القضائية الدولية لجمع الأدلة الإلكترونية، وفقاً للاتفاقيات الدولية أو مبدأ المعاملة بالمثل، لا يعمل القانون 09-04 بمعزل عن باقي التشريعات، بل يتكامل مع قانون العقوبات وقانون الإجراءات الجزائية الذي استحدث بدوره إجراءات خاصة تتناسب مع طبيعة الجرائم السيبرانية، مثلك اعتراض المراسلات، والتسرب الإلكتروني⁴⁰.

يُظهر الإطار التشريعي الجزائري، وعلى رأسه القانون 09-04، جهداً واضحاً للتصدي للتهديدات السيبرانية من خلال التجريم ووضع آليات وقائية وإجرائية متخصصة، مع التأكيد على أهمية التعاون بين مختلف الفاعلين (السلطات القضائية، ومزودي الخدمات) والانفتاح على التعاون الدولي. ومع ذلك، قد تواجه هذه التشريعات تحديات في التطبيق العملي تتعلق بالجانب التقني والحاجة المستمرة لتحديث القوانين لمواكبة التطور السريع للجرائم السيبرانية.

3.2- البعد التكنولوجي للسياسة الأمنية السيبرانية الجزائرية:

يشكل البعد التكنولوجي عصب السياسة الأمنية السيبرانية، حيث تتشابك فيه الفرص الواعدة للتحول الرقمي مع التحديات المتزايدة التي تفرضها التهديدات السيبرانية المتطورة. تترك الجزائر أهمية هذا البعد، وتسعى جاهدة لتطوير بنيتها التحتية وقدراتها التقنية لمواجهة هذه التحديات، خاصة مع التوجه نحو تبني تقنيات الجيل الخامس (5G) وما يرافقه من تحولات عميقة.

الذي يمثل قفزة نوعية في مسار التحول الرقمي الجزائري، فاتحاً آفاقاً واسعة في مجالات الاتصالات فائقة السرعة، إنترنت الأشياء، الخدمات الذكية، والصناعات المتقدمة، تؤكد الخبرة فلة قوار، رئيسة مؤسسة "إنتلجينت نيتورك"، أن هذا التطور "يعكس توجهاً استراتيجياً نحو تأسيس بنية تحتية تكنولوجية قادرة على الاستجابة لتحديات العصر الرقمي"⁴¹.

لكن هذا التقدم التكنولوجي، وخاصة تبني الجيل الخامس، لا يخلو من تحديات أمنية جسيمة، تحذر قوار من أن "الجيل الخامس (G5) هو تغيير جوهري في منطق عمل البنى التحتية الرقمية"، مما يؤدي إلى "تعدد نقاط الهجوم" نتيجة الارتفاع الهائل في عدد الأجهزة المتصلة، وزيادة "هشاشة البنى التحتية الحيوية" كالصحة، والطاقة، والنقل التي ستعتمد بشكل أكبر على هذه التقنية، فضلاً عن "تعقيد بنية شبكة (G5)" الذي يصعب اكتشاف الثغرات، و"ضعف المراقبة والتتبع" الناتج عن الطابع اللامركزي للشبكة⁴².

لمواجهة هذه التحديات، تعمل الجزائر على تعزيز قدراتها التقنية وتبني استراتيجيات وطنية متكاملة، تشير التقارير الإخبارية إلى وجود "استراتيجية وطنية للأمن السيبراني" تهدف إلى بناء "جزائر صامدة سيبرانياً"، وتقوم هذه الاستراتيجية على مبادئ تشمل: تعزيز السيادة الرقمية؛ بناء أنظمة مرنة، مرافقة جهود الرقمنة الحكومية، إنشاء بيئة وطنية مواتية⁴³.

كما تسعى الجزائر لتعزيز شراكاتها الدولية في هذا المجال، حيث تشير الأنباء الحديثة إلى توقيع اتفاق جزائري-روسي يهدف إلى "دعم البنية التحتية السيبرانية وتطوير قدرات" الشركة الجزائرية "EPE PROXYLAN SPA" التابعة لمركز البحث في الإعلام العلمي والتقني "CERIST"⁴⁴.

يُعد البعد التكنولوجي ساحة سباق مستمر بين تطوير القدرات الدفاعية وتطور التهديدات السيبرانية، تظهر جهود الجزائر في تطوير بنيتها التحتية، وتبني استراتيجية وطنية، والسعي نحو شراكات دولية، وعياً بأهمية هذا البعد، إلا أن ضمان أمن الفضاء السيبراني الوطني يتطلب يقظة مستمرة، استثماراً متواصلًا في أحدث التقنيات، وتطويراً دائماً للقدرات التقنية لمواكبة المشهد السيبراني المتغير بسرعة، وجعل الأمن السيبراني جزءاً لا يتجزأ من عملية التحول الرقمي الشاملة.

4.2- البعد البشري للسياسة الأمنية السيبرانية الجزائرية:

لا تكتمل أي سياسة أمنية سيبرانية فعالة دون التركيز على العنصر البشري، فهو يمثل خط الدفاع الأول والأخير في مواجهة التهديدات الرقمية، وفي الوقت نفسه، قد يكون الحلقة الأضعف إذا لم يتم تأهيله وتوعيته بالشكل المناسب. تدرك الجزائر هذه الأهمية المحورية، وتولي اهتماماً متزايداً لبناء الكفاءات الوطنية وتعزيز الوعي السيبراني لدى مختلف فئات المجتمع والمؤسسات.

تُعدّ عملية بناء وتطوير الكفاءات البشرية المتخصصة في الأمن السيبراني حجر الزاوية في الاستراتيجية الوطنية. تشير المصادر إلى أن "تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات" تُعتبر من التوجهات الرئيسية، وتتجلى هذه الجهود في مبادرات ملموسة على أرض الواقع. ففي القطاع الصحي، على سبيل المثال، نظمت وزارة الصحة بالتنسيق مع مؤسسة "بروكسيلان" التابعة لمركز البحث في الإعلام العلمي والتقني (CERIST)، دورة تكوينية متخصصة في يونيو 2024 لتكوين المكونين حول أمن البيانات الصحية، استفاد منها أكثر من 90 مهندساً في الإعلام الآلي على المستوى الوطني. وتهدف هذه الدورات إلى "تعزيز المعرفة والمهارات لدى العناصر البشرية المختصة وتأهيل فريق

وطني متكامل للسهر على أمن وسلامة البيانات الصحية"، مما يعكس التزاماً ببناء قدرات وطنية قادرة على مواجهة التحديات في هذا القطاع الحيوي⁴⁵.

كما يمتد الاهتمام بالتدريب ليشمل قطاعات أخرى، مثل القطاع المصرفي، حيث تم الإعلان عن شراكة بين معهد التكوين المصرفي وشركة كاسبرسكي العالمية في أبريل 2025 بهدف "تعزيز الثقافة وتطوير الكفاءات والمهارات في مجال الأمن السيبراني داخل القطاع المصرفي، وتُظهر هذه الشراكات انفتاحاً على التعاون مع الخبرات الدولية لرفع مستوى الكفاءات المحلية⁴⁶.

بالإضافة إلى الدورات المتخصصة، هناك جهود لدمج الأمن السيبراني في المنظومة التعليمية والأكاديمية، وإن كانت التفاصيل حول المناهج الجامعية المخصصة أو عدد الخريجين المتخصصين تحتاج إلى مزيد من البحث والبيانات الرسمية، ومع ذلك، فإن وجود مؤسسات مثل المدرسة العسكرية المتعددة التقنيات يشير إلى وجود قنوات لتكوين الكفاءات في هذا المجال ضمن هياكل الدولة⁴⁷.

إلى جانب بناء الكفاءات المتخصصة، تُشدد الاستراتيجية الوطنية على أهمية "تعزيز التدريب والتوعية لدى المؤسسات والمواطنين حول مخاطر الأمن السيبراني"، فالتوعية بأفضل الممارسات الأمنية، مثل: التعامل الآمن مع الاتصالات، وتصنيف البيانات، والحذر من التصيد الاحتيالي والهندسة الاجتماعية، وحماية الخصوصية، تُعدّ أساسية لتقليل المخاطر الناجمة عن الخطأ البشري.

وتُقدم جهات مختلفة برامج تدريب وتوعية، سواء كانت عامة مثل تلك التي توفرها منصات عالمية أو برامج مخصصة للمؤسسات تهدف إلى تثقيف فرق العمل حول التهديدات الشائعة وأفضل الممارسات، وتُعتبر هذه البرامج ضرورية لخلق ثقافة أمنية قوية داخل المؤسسات والمجتمع ككل.

3- تحليل الاختلالات في السياسة الأمنية السيبرانية الجزائرية:

1.3- البعد المؤسسي: تحديات التنسيق والفعالية:

يمثل البعد المؤسسي حجر الزاوية في أي سياسة أمنية سيبرانية فعالة، إلا أن تحليل الواقع الجزائري يكشف عن مجموعة من الاختلالات والتحديات التي تحد من فعالية الجهود المبذولة، على الرغم من إنشاء هيئات متخصصة مثل الهيئة الوطنية للأمن السيبراني (ONSC) والمركز الجزائري للاستجابة للحوادث السيبرانية (CERT.dz)، فإن التحديات المتعلقة بالتنسيق، وتحديد المسؤوليات، وتوفير الموارد الكافية، وفعالية الأداء، لا تزال قائمة.

أحد أبرز التحديات التي تواجه الإطار المؤسسي هو ضعف التنسيق وتداخل الصلاحيات بين مختلف الجهات الفاعلة، كذلك، بناء سياسات واستراتيجية وطنية فعالة يتطلب "تكثيف التعاون بين المؤسسات الحكومية والقطاع الخاص"⁴⁸، مما يوحي بوجود فجوة حالية في هذا التعاون، قد ينجم هذا الضعف عن عدم وضوح الأدوار المنوطة بكل جهة، أو غياب آليات تنسيقية فعالة تضمن تكامل الجهود وتجنب الازدواجية في المهام.

إن تعدد الفاعلين في مجال الأمن السيبراني (وزارة الدفاع، وزارة الداخلية، وزارة البريد وتكنولوجيا الإعلام والاتصال، وغيرها)، قد يؤدي إلى تشتت الجهود إذا لم توجد قيادة مركزية واضحة وآليات تنسيق قوية⁴⁹.

تحدٍ آخر يتمثل في محدودية الموارد المخصصة والقدرات التشغيلية لبعض الهيئات، فبينما يتم إنشاء هياكل متخصصة، فإن فعاليتها تبقى مرهونة بتوفر الإمكانيات المادية والبشرية والتقنية اللازمة للقيام بمهامها على أكمل وجه، قد تعاني هذه الهيئات من نقص في الميزانيات المخصصة، أو قلة الكوادر المؤهلة، أو صعوبة الوصول إلى التقنيات المتقدمة اللازمة للرصد والتحليل والاستجابة، مما يحد من قدرتها على مواكبة التهديدات المتطورة⁵⁰.

كما تبرز إشكالية مدى فعالية الاستراتيجية الوطنية وتطبيقها على أرض الواقع. على الرغم من وجود استراتيجية وطنية للأمن السيبراني تهدف إلى بناء "جزائر صامدة سيبرانياً"، فإن تقييم مدى ترجمة هذه الاستراتيجية إلى خطط عمل تنفيذية واضحة ومؤشرات أداء قابلة للقياس يظل أمراً ضرورياً، قد يوجد قصور في آليات المتابعة والتقييم المستمر لضمان تحقيق الأهداف المرجوة وتكييف الاستراتيجيات مع المتغيرات المستجدة في بيئة التهديدات.

علاوة على ذلك، قد يعاني الإطار المؤسسي من بطء في التكيف مع التطورات التكنولوجية المتسارعة، فالطبيعة الديناميكية للفضاء السيبراني تتطلب هياكل مؤسسية مرنة قادرة على الاستجابة السريعة للمستجدات، قد تكون الإجراءات البيروقراطية أو الهياكل التنظيمية التقليدية عائقاً أمام تبني التقنيات الجديدة أو تطوير أساليب عمل مبتكرة لمواجهة التهديدات السيبرانية الحديثة.

2.3- البعد التشريعي: فجوات المواجهة والتطبيق:

يشكل الإطار التشريعي الدعامية الأساسية لتنظيم الفضاء السيبراني ومكافحة التهديدات الرقمية، ورغم أن الجزائر خضعت خطوات مهمة بسن تشريعات خاصة بالجرائم المعلوماتية، أبرزها القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إلا أن تحليل هذا البعد يكشف عن اختلالات وتحديات تحد من فعاليته في مواجهة المشهد السيبراني المتطور⁵¹.

أحد أبرز الاختلالات يتمثل في صعوبة مواكبة التشريعات للتطور المتسارع للتهديدات والتقنيات، فالجرائم السيبرانية تتخذ أشكالاً جديدة باستمرار، مستفيدة من تطور الذكاء الاصطناعي، وانتشار إنترنت الأشياء، وتعقيد الهجمات مثل برامج الفدية المتطورة. قد لا تكون النصوص القانونية الحالية، التي صيغت في سياقات تكنولوجية سابقة، قادرة على الإحاطة بكل هذه المستجدات وتوفير الأدوات القانونية اللازمة للتحريم والملاحقة الفعالة، يوجد جهود المبذولة لسن القوانين، لكن مقرونة بالتحديات المستمرة التي يفرضها التطور التكنولوجي، مما يلزم إلى أن التشريع قد يكون متأخراً عن مواكبة الواقع.

تحدٍ آخر يكمن في الثغرات المحتملة في نطاق التشريع. فبينما يركز القانون 09-04 بشكل كبير على الجرائم المعلوماتية التقليدية، قد توجد حاجة لمراجعة وتوسيع نطاقه ليشمل بشكل أكثر تفصيلاً جوانب حيوية أخرى مثل حماية البيانات الشخصية للمواطنين (بما يتجاوز القوانين العامة للخصوصية)، وأمن البنى التحتية الحيوية، وتحديد مسؤوليات القطاع الخاص في تأمين أنظمتهم⁵²، وتنظيم استخدام التقنيات الناشئة كما تبرز إشكالية تطبيق وإنفاذ القوانين القائمة. فحتى مع وجود نصوص قانونية، قد تواجه عملية التطبيق صعوبات عملية، يتطلب التحقيق في الجرائم السيبرانية وملاحقة مرتكبيها خبرات تقنية وقانونية عالية لدى أجهزة إنفاذ القانون والقضاء، بالإضافة إلى آليات فعالة للتعاون الدولي نظراً للطبيعة العابرة للحدود لهذه الجرائم، قد يوجد نقص في هذه القدرات أو بطء في إجراءات التعاون الدولي، مما يضعف من الأثر الرادع للتشريع، علاوة على ذلك، قد يفتقر الإطار التشريعي إلى المرونة الكافية للتكيف السريع.

فالعملية التشريعية بطبيعتها قد تكون بطيئة، بينما يتغير مشهد التهديدات بسرعة فائقة، يتطلب الأمر آليات تشريعية أو تنظيمية أكثر مرونة تسمح بتحديث القواعد والإجراءات بشكل أسرع استجابة للمستجدات التقنية والتهديدات الناشئة، ربما من خلال لوائح تنظيمية تصدرها الهيئات المختصة بناءً على تفويض تشريعي.

3.3- البعد التكنولوجي: تحديات الاعتمادية والتحديث:

يمثل البعد التكنولوجي ساحة المعركة الرئيسية في مواجهة التهديدات السيبرانية، ورغم الجهود الجزائرية لتطوير البنية التحتية الرقمية، إلا أن هذا البعد يعاني من اختلالات وتحديات جوهرية، تحد من قدرة البلاد على الصمود في وجه الهجمات المتطورة.

أحد أبرز الاختلالات هو الاعتماد الكبير على التكنولوجيا المستوردة وعدم كفاية الاستثمار في البحث والتطوير المحلي، فبينما تسعى الجزائر لتبني تقنيات حديثة مثل الجيل الخامس (5G)، فإن جزءاً كبيراً من البنية التحتية والحلول الأمنية يعتمد على موردين أجانب، هذا الاعتماد لا يثير فقط مخاوف تتعلق بالسيادة الرقمية⁵³، بل قد يؤدي أيضاً إلى صعوبة تكييف الحلول مع الاحتياجات المحلية الخاصة أو التأخر في الحصول على التحديثات الأمنية الضرورية، كذلك، غياب منظومة بحث وتطوير محلية قوية في مجال الأمن السيبراني يحد من القدرة على ابتكار حلول وطنية ومواجهة التهديدات بشكل استباقي.

تحدٍ آخر يتعلق بمستوى نضج وتأمين البنية التحتية الرقمية الحالية، على الرغم من التقدم المحرز، قد لا تزال بعض القطاعات أو المؤسسات تعتمد على أنظمة قديمة أو غير مؤمنة بشكل كافٍ، مما يجعلها أهدافاً سهلة للمهاجمين، كما أن عملية التحول الرقمي نفسها، إذا لم ترافقها إجراءات أمنية صارمة منذ البداية (Security by Design)، قد تخلق نقاط ضعف جديدة⁵⁴.

كما تبرز إشكالية بطء تبني وتطبيق التقنيات الأمنية المتقدمة. ففي مواجهة هجمات متطورة تعتمد على الذكاء الاصطناعي أو تستهدف سلاسل الإمداد البرمجية، قد تكون الحلول الأمنية التقليدية غير كافية، قد يوجد تأخر في تبني حلول أكثر تقدماً مثل أنظمة الكشف والاستجابة، أو منصات استخبارات التهديدات، أو

تقنيات تحليل سلوك المستخدم والكيانات على نطاق واسع، ربما بسبب التكلفة أو نقص الخبرات اللازمة لتشغيلها بفعالية.

ويرتبط بذلك تحدي تأمين التقنيات الناشئة مثل الجيل الخامس (5G) وإنترنت الأشياء، وكما حذرت الخبرة فلة قوار، فإن هذه التقنيات تزيد من سطح الهجوم بشكل كبير وتزيد من تعقيد تأمين الشبكات والبنى التحتية الحيوية التي ستعتمد عليها، يتطلب تأمين هذه التقنيات استثمارات ضخمة وتطويراً للمهارات واعتماد معايير أمنية صارمة، وهو ما قد يمثل تحدياً كبيراً للجزائر في المرحلة الحالية. وأيضاً، قد يوجد قصور في القدرة على الرصد والاستجابة للحوادث السيبرانية بشكل فعال وسريع، فعلى الرغم من وجود مركز CERT.dz، فإن فعاليته تعتمد على قدرته على جمع وتحليل كميات هائلة من البيانات الأمنية من مختلف القطاعات، والتنسيق السريع للاستجابة، ومشاركة المعلومات حول التهديدات، قد تعيق محدودية الموارد، أو ضعف التنسيق المؤسسي، أو نقص الأدوات التحليلية المتقدمة، قدرة المركز على القيام بدوره على أكمل وجه.

4.3- البعد البشري: فجوة المهارات وقصور الوعي:

يعد العنصر البشري خط الدفاع الأول والأخير في مواجهة التهديدات السيبرانية، لكنه في الوقت ذاته يمثل إحدى أبرز نقاط الضعف إذا لم يتم تأهيله وتوعيته بشكل كافٍ، ورغم الاعتراف بأهمية هذا البعد في الاستراتيجيات الجزائرية، إلا أن الواقع يكشف عن اختلالات وتحديات كبيرة تحد من بناء "جدار حماية بشري" فعال.

أحد أهم الاختلالات هو النقص الملحوظ في الكفاءات والخبرات المتخصصة، تعاني الجزائر كغيرها من دول العالم، من فجوة في المهارات اللازمة لتصميم وتطبيق وإدارة الحلول الأمنية المتقدمة، وتحليل التهديدات، والاستجابة للحوادث، ورغم وجود مبادرات تدريبية قطاعية، إلا أنها قد لا تكون كافية لسد الاحتياجات المتزايدة كما ونوعاً⁵⁵، قد يرجع هذا النقص إلى عدم كفاية البرامج الأكاديمية المتخصصة، أو ضعف جاذبية القطاع للمواهب، أو هجرة الكفاءات.

تحدٍ آخر يرتبط بمحدودية وفعالية برامج التدريب والتوعية المستمرة، فبينما توجد دورات تكوينية، قد لا تكون هذه البرامج شاملة بما يكفي لتغطية كافة القطاعات الحيوية والمؤسسات الحكومية والخاصة، وقد لا تكون مستمرة لمواكبة التطور السريع للتهديدات، الأهم من ذلك، قد يغيب التركيز الكافي على بناء ثقافة أمنية راسخة لدى الموظفين والمواطنين، فالتوعية لا تقتصر على معرفة المخاطر، بل تشمل تغيير السلوكيات والممارسات اليومية في التعامل مع التكنولوجيا، وهذه الحماية لا تكتمل دون وعي المستخدم نفسه.. قد يكون هناك قصور في حملات التوعية الوطنية واسعة النطاق التي تستهدف الجمهور العام، أو ضعف في إلزامية برامج التدريب الأمني للموظفين في القطاعين العام والخاص.

كما تبرز إشكالية عدم كفاية التركيز على المهارات غير التقنية اللازمة للأمن السيبراني، مثل التفكير النقدي، وحل المشكلات، والتواصل الفعال، والوعي بالسياقات القانونية والأخلاقية، فالأمن السيبراني ليس مجرد تحدٍ تقني، بل يتطلب فهماً شاملاً للجوانب الإنسانية والتنظيمية.

إن ضعف البعد البشري يؤدي مباشرة إلى زيادة المخاطر، حيث يعتبر الخطأ البشري (سواء عن غير قصد أو نتيجة نقص الوعي) سبباً رئيسياً في العديد من الاختراقات الأمنية الناجحة، مثل الوقوع في فخ التصيد الاحتيالي أو استخدام كلمات مرور ضعيفة أو تحميل برمجيات خبيثة.

5.3- حلول تصحيحية مقترحة لتعزيز السياسة الأمنية السيبرانية الجزائرية:

بناءً على تحليل الاختلالات في الأبعاد المؤسسية والتشريعية والتكنولوجية والبشرية، وبالاستناد إلى أفضل الممارسات الدولية والتوصيات الأكاديمية، يمكن اقتراح مجموعة من الحلول التصحيحية لتعزيز فعالية السياسة الأمنية السيبرانية الجزائرية:

أ/ الحلول على المستوى المؤسسي:

- تعزيز التنسيق وإنشاء آلية حوكمة مركزية: لمواجهة ضعف التنسيق وتداخل الصلاحيات، يُقترح إنشاء أو تعزيز دور هيئة وطنية عليا للأمن السيبراني تكون مسؤولة عن وضع الاستراتيجية العامة، وتنسيق جهود جميع الفاعلين (الحكوميين والقطاع الخاص والأكاديميين)، وتحديد المسؤوليات بوضوح، ومراقبة التنفيذ، تستلهم هذه الفكرة من نماذج الحوكمة المركزية المتبعة في العديد من الدول التي تضع هيئة وطنية في قمة هرم الأمن السيبراني.

- توفير الموارد الكافية وبناء القدرات المؤسسية: يجب تخصيص ميزانيات كافية ومستدامة للهيئات المعنية بالأمن السيبراني، لا سيما المركز الجزائري للاستجابة للحوادث (CERT.dz)، لتمكينها من اقتناء التقنيات اللازمة وتوظيف الكفاءات وتطوير قدراتها التشغيلية في مجالات الرصد والتحليل والاستجابة، يمكن الاستفادة من الشراكات الدولية لتبادل الخبرات وبناء القدرات.

- تفعيل آليات المتابعة والتقييم: يجب تطوير مؤشرات أداء واضحة وقابلة للقياس لتقييم مدى فعالية الاستراتيجية الوطنية والخطط التنفيذية بشكل دوري، ينبغي أن تشمل عملية التقييم مراجعة الأهداف، وقياس التقدم المحرز، وتحديد نقاط الضعف، وتكييف الاستراتيجيات بناءً على النتائج وبيئة التهديدات المتغيرة.

- تبني هياكل تنظيمية مرنة: يجب تشجيع الهيئات المعنية على تبني هياكل تنظيمية أكثر مرونة تسمح بالتكيف السريع مع التطورات التكنولوجية والتهديدات الناشئة، وتقليل الإجراءات البيروقراطية التي قد تعيق الاستجابة الفعالة.

ب/ الحلول على المستوى التشريعي:

- **المراجعة والتحديث الدوري للتشريعات:** لمواكبة التطورات، يجب إنشاء آلية للمراجعة الدورية (كل 3-5 سنوات مثلاً) للقانون 04-09 والتشريعات ذات الصلة، بهدف تحديث المصطلحات، وتجريم الأفعال المستجدة، وتكثيف العقوبات، يمكن الاستلزام من اتفاقية بودابست بشأن الجرائم السيبرانية وتحديثاتها المستمرة.

- **سد الثغرات وتوسيع نطاق الحماية:** يجب النظر في سن تشريعات أو تعديل القوانين القائمة لتغطية مجالات حيوية بشكل أكثر تفصيلاً، مثل: قانون خاص بحماية البيانات الشخصية يتماشى مع المعايير الدولية (مثل GDPR الأوروبي)، وتشريعات تلزم مشغلي البنى التحتية الحيوية باتخاذ تدابير أمنية محددة، وقواعد واضحة لمسؤولية القطاع الخاص ومقدمي الخدمات الرقمية، وتنظيم استخدام الذكاء الاصطناعي وإنترنت الأشياء من منظور أمني.

- **تعزيز قدرات الإنفاذ والتعاون الدولي:** يجب الاستثمار في تدريب وتأهيل القضاة ووكلاء النيابة وأعضاء الضبطية القضائية على الجوانب التقنية والقانونية للجرائم السيبرانية. كما يجب تفعيل وتعزيز آليات التعاون الدولي القضائي والأمني لتبادل المعلومات والأدلة وملاحقة المجرمين عبر الحدود، والانضمام إلى الاتفاقيات الدولية ذات الصلة أو تفعيل بنودها بشكل كامل.

- **اعتماد آليات تنظيمية مرنة:** يمكن منح الهيئات التنظيمية المختصة (مثل هيئة تنظيم الاتصالات أو الهيئة الوطنية للأمن السيبراني) صلاحيات لإصدار لوائح فنية ومعايير أمنية ملزمة وقابلة للتحديث السريع استجابة للمستجدات، دون الحاجة لانتظار تعديلات تشريعية قد تستغرق وقتاً طويلاً.

ج/ الحلول على المستوى التكنولوجي:

- **تشجيع البحث والتطوير والابتكار المحلي:** يجب وضع سياسات تحفيزية (ضريبية، تمويلية) لدعم البحث والتطوير في مجال الأمن السيبراني داخل الجامعات ومراكز البحث والشركات الناشئة الجزائرية، بهدف تطوير حلول وطنية وتقليل الاعتماد على الخارج وتعزيز السيادة الرقمية.

- **تحديث وتأمين البنية التحتية:** يجب وضع خطة وطنية لتحديث البنى التحتية الرقمية القديمة في القطاعين العام والخاص، وتطبيق معايير أمنية صارمة (مثل معايير ISO 27001 أو ضوابط الهيئة الوطنية للأمن السيبراني السعودية NCA ECC) على جميع الأنظمة الحالية والجديدة، مع التركيز على مبدأ "الأمن بالتصميم" (Security by Design).

- **تسريع تبني التقنيات الأمنية المتقدمة:** يجب تشجيع ودعم المؤسسات، خصوصاً الحيوية منها على تبني تقنيات أمنية متقدمة مثل SIEM (إدارة معلومات الأمن والأحداث)، SOAR (تنسيق الأتمتة والاستجابة الأمنية)، منصات استخبارات التهديدات، وحلول حماية نقاط النهاية المتقدمة (EDR)، مع توفير التدريب اللازم لتشغيلها.

- وضع معايير لتأمين التقنيات الناشئة: يجب تطوير وإصدار معايير وأطر تنظيمية وطنية خاصة بتأمين شبكات الجيل الخامس (G5) وأجهزة إنترنت الأشياء (IoT)، بالاستناد إلى أفضل الممارسات الدولية.

- تعزيز قدرات الرصد والاستجابة الوطنية (CERT.dz): يجب دعم المركز بالموارد البشرية والتقنية اللازمة، وتطوير منصة وطنية لتبادل معلومات التهديدات بين القطاعات، وتعزيز قدراته في التحليل الجنائي الرقمي والاستجابة للحوادث المعقدة.

د/ الحلول على المستوى البشري:

- تطوير منظومة التعليم والتكوين: يجب مراجعة وتطوير المناهج الدراسية في الجامعات والمعاهد التقنية لإدراج مسارات متخصصة ومعقدة في الأمن السيبراني، تتضمن الجوانب التقنية وغير التقنية، وتشجيع الشراكات مع القطاع الخاص لتوفير تدريب عملي.

- إطلاق برامج تدريب وتوعية وطنية شاملة ومستمرة: يجب تصميم وتنفيذ حملات توعية وطنية واسعة النطاق تستهدف فئات المجتمع (طلاب، موظفين، مواطنين) حول المخاطر السيبرانية وأفضل الممارسات الآمنة، كما يجب جعل التدريب الأمني إلزامياً ودورياً للموظفين في القطاعين العام والخاص، مع التركيز على بناء ثقافة أمنية.

- إنشاء برامج لتحفيز واحتضان المواهب: يجب وضع برامج لاكتشاف ورعاية المواهب الشابة في مجال الأمن السيبراني، وتوفير بيئة عمل جاذبة في القطاعين العام والخاص للاحتفاظ بالكفاءات المتخصصة والحد من هجرة الأدمغة.

- تشجيع الشهادات المهنية المتخصصة: يجب تشجيع المهنيين على الحصول على شهادات معترف بها دولياً في مجال الأمن السيبراني لدعم تطورهم المهني وضمان مستوى عالٍ من الكفاءة.

الخاتمة:

في ضوء التحليل المتعدد الأبعاد للسياسة العامة الأمنية الجزائرية وفي ظل التهديدات السيبرانية، يتضح أن الجزائر تبنت مقاربة شاملة تجمع بين الجوانب المؤسسية، التشريعية، التكنولوجية، والبشرية. ورغم التقدم الملحوظ في إنشاء أطر تنظيمية وتشريعية متخصصة، إلا أن التحديات المتعلقة بالتنسيق، التطبيق العملي، مواكبة التطورات التكنولوجية، وبناء الكفاءات لا تزال قائمة. ولتحقيق أمن سيبراني فعال ومستدام، تبرز الحاجة إلى تعزيز الحوكمة المركزية، تحديث الأطر القانونية، الاستثمار في البنى التحتية والبحث العلمي، وبناء ثقافة سيبرانية مجتمعية، إن النجاح في ذلك يتطلب رؤية استراتيجية منسجمة، وشراكة بين مختلف الفاعلين، واستشراكاً دقيقاً للمخاطر المستقبلية في الفضاء الرقمي.

على نحو ما سبق ذكره نكون قد توصلنا إلى النتائج التالية:

- وجود بنى مؤسسية متعددة تعنى بالأمن السيبراني، تصدرها وزارة الدفاع الوطني والمجلس الأعلى للأمن.

- مساهمة هيئات أمنية وقضائية متعددة، مع تسجيل ضعف في التنسيق وتداخل في الصلاحيات.
- الحاجة إلى آليات تنسيق فعّالة وقيادة موحدة لتجنب ازدواجية المهام وتحقيق التكامل المؤسسي.
- محدودية الموارد البشرية والتقنية لبعض الهيئات تؤثر على فعالية التنفيذ.
- تطور تدريجي في المنظومة التشريعية لمكافحة الجرائم السيبرانية، بدءًا من تعديلات قانون العقوبات إلى إصدار القانون 04-09 الذي يضبط التجريم، الوقاية، المكافحة، ويؤسس لآليات قضائية متقدمة
- تحديات تطبيقية تتعلق بسرعة تطور التهديدات، مما يفرض ضرورة التحديث المستمر للإطار القانوني.
- اهتمام الدولة بتطوير البنية التحتية الرقمية، مع التركيز على إدماج تقنيات الجيل الخامس (5G).
- وجود استراتيجية وطنية للأمن السيبراني تهدف إلى تعزيز السيادة الرقمية وبناء أنظمة مرنة.
- تفعيل شراكات دولية لدعم القدرات التقنية، من أبرزها التعاون الجزائري-الروسي في المجال السيبراني.
- الحاجة إلى استثمار مستدام في التكنولوجيا وربط الأمن السيبراني بشكل عضوي بالتحول الرقمي.
- إدراك مركزي لأهمية العنصر البشري في صلابة المنظومة السيبرانية.
- تنظيم دورات تدريبية متخصصة في قطاعات حساسة (الصحة، البنوك)، مع انفتاح على التعاون الدولي.
- مساعي لإدماج مفاهيم الأمن السيبراني في المنظومة التربوية والتكوينية.
- استمرار الحاجة إلى برامج تكوين وتوعية شاملة لتوسيع قاعدة الكفاءات وتعزيز الثقافة الأمنية الرقمية.
- في حين نقدم توصيات نراها تساعد الجزائر في النهوض بهذا القطاع الحساس في النقاط التالية:
- إقرار استراتيجية وطنية شاملة تركز على أولويات واضحة ومؤشرات أداء قابلة للقياس، تأخذ في الحسبان التهديدات السيبرانية الناشئة.
- تعزيز الحوكمة والتنسيق المؤسسي عبر تقوية دور الهيئة الوطنية للأمن السيبراني كمرجع مركزي، وإنشاء آليات تنسيق فعالة بين القطاعين العام والخاص والمجتمع المدني.
- تبني إطار وطني موحد لإدارة المخاطر السيبرانية وفق المعايير الدولية، مع إلزام المؤسسات الحيوية بإجراء تقييمات دورية وخطط استجابة للطوارئ.
- تحديث القانون رقم 04-09 والتشريعات ذات الصلة لتجريم الأفعال المستجدة وتبني قانون لحماية البيانات الشخصية وفقًا للمعايير الدولية.
- تعزيز القدرات القضائية من خلال تكوين كفاءات متخصصة في التحقيقات الرقمية، وتفعيل التعاون القضائي والأمني الدولي.
- إصدار لوائح ومعايير فنية إلزامية وقابلة للتحديث السريع في مجالات مثل أمن شبكات G5.
- دعم البحث والتطوير والابتكار المحلي لتعزيز السيادة الرقمية وتطوير حلول أمنية وطنية.

- تأمين البنى التحتية الحيوية من خلال تطبيق معايير أمنية صارمة مع اختبارات دورية لاكتشاف الثغرات.
 - تطوير قدرات الرصد والاستجابة الوطنية عبر تأهيل مركز CERT.dz ليكون منصة متقدمة مدعومة بالنكاء الاصطناعي وكفاءات مؤهلة.
 - إعداد استراتيجية وطنية لتكوين الكفاءات تشمل إدماج الأمن السيبراني في المناهج الدراسية وتوفير شهادات مهنية معتمدة.
 - تعزيز ثقافة الأمن السيبراني من خلال حملات توعية وطنية وتدريب إلزامي موجه للموظفين والمؤسسات.
 - استقطاب الكفاءات الوطنية والاحتفاظ بها عبر توفير بيئة عمل محفزة ومسارات مهنية واضحة.
 - سيناريوهات وآفاق مستقبلية للسياسة الأمنية السيبرانية الجزائرية.
- بناءً على تحليل الاتجاهات العالمية، وتأثير التقنيات الناشئة، والتحديات والفرص الخاصة بالجزائر، يمكن تصور عدة سيناريوهات أو آفاق مستقبلية محتملة لمسار السياسة الأمنية السيبرانية في البلاد.

1- السيناريو الأول: الصمود التفاعلي:

هذا السيناريو، تستمر الجزائر في الاستجابة للتهديدات السيبرانية بشكل تفاعلي بدلاً من استباقي. يتم تحديث التشريعات والمؤسسات بشكل تدريجي استجابة للحوادث الكبرى أو الضغوط الدولية، ولكن دون رؤية استراتيجية شاملة طويلة الأمد. يظل التركيز منصباً على الدفاع عن البنى التحتية الحيوية الأساسية، مع بقاء فجوة المهارات والاعتماد التكنولوجي تحديات قائمة.

2- السيناريو الثاني: التعزيز الاستراتيجي:

تتبنى الجزائر نهجاً أكثر استراتيجية وتصميماً لتعزيز أمنها السيبراني. يتم إقرار وتنفيذ استراتيجية وطنية متكاملة مع أهداف واضحة ومؤشرات أداء ومتابعة دورية. يتم تعزيز دور الهيئة الوطنية للأمن السيبراني (ONSC) كمنسق مركزي، وتُبذل جهود أكبر لسد فجوة المهارات وتحديث التشريعات.

3- السيناريو الثالث: الريادة الإقليمية والابتكار:

هنا لا تكتفي الجزائر بتعزيز دفاعاتها، بل تسعى لتصبح لاعباً رائداً في مجال الأمن السيبراني على المستوى الإقليمي (المغاربي والإفريقي). يتم تبني نهج استباقي للغاية يركز على الابتكار المحلي، وتطوير حلول وطنية، وتصدير الخبرات. يتم الاستثمار بكثافة في البحث والتطوير، وبناء الكفاءات، وتعزيز التعاون الدولي.

الهوامش:

- ¹ محمد بن مكرم ابن منظور، *لسان العرب*، تحقيق عبد الله علي الكبير ومحمد أحمد حسب الله، دار المعارف، 1990، ص. 146.
- ² القرآن الكريم، سورة قريش، الآية 3-4.
- ³ عبد النور بن عنتر، *البعد المتوسطي للأمن الجزائري*، الجزائر، أوروبا والحلف الأطلسي، المكتبة العصرية للطباعة والنشر، 2005، ص. 13.
- ⁴ فهمي خليفة الفهداوي، *السياسة العامة: منظور كلي في البنية والتحليل*، دار المسرة، 2001، ص. 32.
- ⁵ حسن أبشر الطيب، *الدولة العصرية دولة مؤسسات*، القاهرة، دار الفجر للنشر والتوزيع، 2000، ص. 295.
- ⁶ نصر محمد مهنا، *علم السياسة*، دار غريب للطباعة والنشر، 1995، ص ص. 120، 121.
- ⁷ David Easton, *A Systems Analysis of Political Life* (New York: Wiley, 1965), 134-135.
- ⁸ جيمس اندرسون، *صنع السياسات العامة*، ترجمة عامر الكيسي، عمان: دار المسيرة، 1999م، ص. 15.
- ⁹ تامر كامل محمد الخرجي، *النظم السياسية الحديثة والسياسات العامة*، دار مجدلاوي، 2005، ص. 21.
- ¹⁰ أحمد سعيغان، *قاموس المصطلحات السياسية والدستورية والدولية*، مكتبة لبنان، 2005، ص. 213.
- ¹¹ Roché, Sébastien. *Sociologie politique de l'insécurité*. Paris: Presses Universitaires de France, 1998, cité dans: Laurent Mucchielli, *Revue française de sociologie*, vol. 40, no. 1 (1999), p. 151.
- ¹² United Nations Development Programme. *Human Development Report 1994: New Dimensions of Human Security*. New York: Oxford University Press, 1994, p. 23.
- ¹³ منذر محمد، *مبادئ في العلاقات الدولية*، من النظريات إلى العولمة، المؤسسة الجامعية للدراسات والنشر والتوزيع، 2002، ص ص. 33- 34.
- ¹⁴ عبد النور بن عنتر، مرجع سابق، ص. 19.
- ¹⁵ Davida. Baldwin, "the concept security", p21, in: <https://www.jstor.org/stable/20097464>
- ¹⁶ منذر محمد، مرجع سابق، ص. 34.
- ¹⁷ منذر محمد، مرجع سابق، ص ص. 34-37.
- ¹⁸ Scott Burchill, "liberalism", in Scott Burchill and others, *Theories of international relations*. Third edition. New York, USA: PALGRAVE MACMILLAN. 2005, pp 56-63.
- ¹⁹ تكيوكي ياما مورا، *مفهوم الأمن في نظرية العلاقات الدولية*، ترجمة عادل زقاع، على الموقع الإلكتروني، 2010/03/26 تم الدخول 2024/09/04، على الرابط: <https://short-link.me/14GGp>
- ²⁰ Scott Burchill, and others, Op, Cit. p 58.
- ²¹ ساحلي مبروك، *نظرية السلام الديمقراطي: كآلية لتحقيق السلام المستدام دراسات وأبحاث*، م. 12، ع. 3، جويلية 2020، ص. 3.
- ²² عبد النور بن عنتر، مرجع سابق، ص. 24.

²³ تاكايوكي يمامورا، مرجع سابق

²⁴ عبد النور بن عنتر، مرجع سابق، ص ص. 24-25

²⁵ Scott Burchill, and others, Op, Cit. p 137

²⁶ دستور 1976، الجريدة الرسمية للجمهورية الجزائرية، العدد 5، 25 فبراير 1976، المادة 125. تنص على تأسيس المجلس الأعلى للأمن برئاسة رئيس الجمهورية لتقديم الآراء في مسائل الأمن الوطني.

²⁷ المرسوم الرئاسي رقم 05-20 المؤرخ في 13 يناير 2020، المتضمن إنشاء الوكالة الوطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 03، 2020.

²⁸ سفيان مهني، إنشاء مركز لمكافحة الجريمة المعلوماتية في الجزائر، جريدة الفجر، 17 ماي 2008، تم الدخول في 4 جوان 2025، <https://www.djazairress.com/alfadjr/71333>.

²⁹ المرسوم الرئاسي رقم 04-183 المؤرخ في يونيو 2004، المتضمن إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني. الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 41، 2004.

³⁰ إلياس شاهد، الحلاج عرابية، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، ع 3، 2016، ص. 130.

³¹ المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 بشأن إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، 8 أكتوبر 2015.

³² الأمر رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية، ع 04، 2005.

³³ لقانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات والمتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، الجريدة الرسمية للجمهورية الجزائرية، العدد 75، 2004.

³⁴ القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والمتعلق بتوسيع التجريم ليشمل أفعال الدخول أو البقاء غير المشروع في نظام معلوماتي، والتلاعب بالمعطيات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، 2006.

³⁵ القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 46، 2009.

³⁶ مهدي، رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، م 06، ع 02، 2021، ص. 118.

³⁷ مهدي، رضا، مرجع سابق، ص. 119.

³⁸ مهدي، رضا، مرجع سابق، ص ص. 119-120.

³⁹ مهدي، رضا، مرجع سابق، ص. 120.

⁴⁰ مهدي، رضا، مرجع سابق، ص. 120.

⁴¹ مصطفى بن ميرة، "G 5 في الجزائر: بين حلم التحول الرقمي وكابوس التهديد السيبراني"، الأيام نيوز، 06/05/2025، تم الخول 2025/05/16، على الرابط: <https://elayem.news/06-05-25-25-06949-5g-fy-aljzair-byn-hlm-althwl-alrqmy-wkabws-althdyd-alsybrany.html>.

⁴² مصطفى بن ميرة، مرجع سابق

⁴³ محمد قادري، الجزائر تواصل تعزيز أمنها السيبراني لمواجهة التهديدات الرقمية المتزايدة، الآن الجزائري، 13/05/2025، تم الخول 2025/05/21، على الرابط: <https://shorturl.at/uajMO>

⁴⁴ روسيا والجزائر توقعان مذكرة تفاهم للتعاون في مجال الأمن السيبراني، 25/05/2025، تم الخول 2025/05/29، على الرابط: <https://shorturl.at/fsb5p>

⁴⁵ وزارة الصحة الجزائرية. "دورة تكوينية حول أمن البيانات الصحية". منشور على الصفحة الرسمية للوزارة على فيسبوك. جوان 2024، تم الدخول 2025/01/12، على الرابط: <https://www.facebook.com/SanteDZA/posts/781511607498771>

⁴⁶ محمد صالح الإبراهيمي، تعزيز التدريب في مجال الأمن السيبراني لفائدة القطاع المصرفي، المستثمر، 29 أبريل 2025، تم الدخول 2025/05/20، على الرابط: <https://shorturl.at/0stv3>

⁴⁷ وزارة الدفاع الوطني الجزائرية. "المدرسة العسكرية المتعددة التقنيات، تم الدخول في 4 يونيو 2025، على الرابط: https://www.mdn.dz/site_em_anp/sommaire/formation/ar/emp-ar.php.

⁴⁸ بوريح سلمة، السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات، دفا تر السياسة والقانون، م 15 15، ع 1، 2023، ص 286.

⁴⁹ ENISA, National Cyber Security Strategies – Practical Guide on Development and Execution (European Union Agency for Cybersecurity, 2020), <https://www.enisa.europa.eu/publications/national-cyber-security-strategies-guide>.

⁵⁰ University of Oxford, Cybersecurity Capacity Maturity Model for Nations (CMM), Wikipedia, last modified May 2024, https://en.wikipedia.org/wiki/Cybersecurity_Capacity_Maturity_Model_for_Nations.

⁵¹ بن علي بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية. "المجلة الجزائرية للأمن الإنساني، م 7، ع 2، 2022، ص 312.

⁵² بوريح سلمة، مرجع سابق، ص 286.

⁵³ مصطفى بن ميرة، مرجع سابق

⁵⁴ UK Research and Innovation (UKRI), Secure by Design: Embedding Cybersecurity in Digital Innovation, UKRI Reports, 2023, on : <https://www.ukri.org/what-we-do/browse-our-areas-of-investment-and-support/digital-security-by-design/>

⁵⁵ بارة سمير، الأمن السيبراني في الجزائر: سياسات ومؤسسات، مجلة الدراسات القانونية والسياسية، م 2، ع 2، 2023، ص 279.