

المدرسة الوطنية العليا للعلوم السياسية
الشهيد زدور محمد ابراهيم قاسم



قسم السياسات العامة والنظم المقارنة

محددات الأمن الوطني الجزائري في عصر الذكاء الاصطناعي (2019-2026)

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: سياسات عامة

إشراف الأستاذ:
بولعراس فتحي

إعداد الطالبة:
بن زواش مريم

أعضاء لجنة المناقشة:

الصفة	مؤسسة الانتساب	اسم ولقب الأستاذ
رئيسا	المدرسة الوطنية العليا للعلوم السياسية	هارون مليكة
مشرفا ومقررا	المدرسة الوطنية العليا للعلوم السياسية	فتحي بولعراس
عضوا مناقشا	المدرسة الوطنية العليا للعلوم السياسية	بن بخيتة وردة

السنة الجامعية: 2025/2026.

المدرسة الوطنية العليا للعلوم السياسية
الشهيد زدور محمد ابراهيم قاسم



قسم السياسات العامة والنظم المقارنة

محددات الأمن الوطني الجزائري في عصر الذكاء الاصطناعي (2019-2026)

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: سياسات عامة

إشراف الأستاذ:
بولعراس فتحي

إعداد الطالبة:
بن زواش مريم

أعضاء لجنة المناقشة:

الصفة	مؤسسة الانتساب	اسم ولقب الأستاذ
رئيسا	المدرسة الوطنية العليا للعلوم السياسية	هارون مليكة
مشرفا ومقررا	المدرسة الوطنية العليا للعلوم السياسية	فتحي بولعراس
عضوا مناقشا	المدرسة الوطنية العليا للعلوم السياسية	بن بخيتة وردة

السنة الجامعية: 2025 / 2026.

ملخص:

تهدف هذه الدراسة إلى تحليل تأثير الذكاء الاصطناعي في إعادة تشكيل الأمن الوطني الجزائري خلال الفترة الممتدة بين 2019 و2026، من خلال دراسة التحولات التي فرضتها التقنيات الذكية على البيئة الأمنية الوطنية، سواء على مستوى الأمن السيبراني، أو إدارة المعلومات، أو حماية السيادة الرقمية، أو تطوير القدرات المؤسساتية للدولة. وتنطلق الدراسة من إشكالية مركزية مفادها: إلى أي مدى أسهمت تطبيقات الذكاء الاصطناعي في إعادة تعريف أولويات الأمن الوطني الجزائري وآليات حمايته في ظل التحولات الرقمية والتكنولوجية المتسارعة؟ اعتمدت الدراسة مقاربة تحليلية تجمع بين البعد المفاهيمي والبعد التطبيقي، عبر تحليل الإطار النظري المرتبط بالذكاء الاصطناعي والأمن الوطني، ودراسة التجربة الجزائرية من خلال تتبع السياسات العمومية، والإصلاحات التشريعية، والاستراتيجيات المؤسساتية التي تم تبنيها خلال الفترة محل الدراسة، مع مراعاة تأثير البيئة الإقليمية والدولية على توجهات الجزائر في هذا المجال. وتوصلت الدراسة إلى أن الجزائر شهدت تطوراً تدريجياً في إدماج تقنيات الذكاء الاصطناعي ضمن مقاربتها الأمنية، خاصة في مجالات الأمن السيبراني، والتحول الرقمي، وحماية البنى التحتية المعلوماتية، غير أن هذا المسار ما يزال يواجه تحديات متعددة ترتبط بضعف التأطير التشريعي، ومحدودية الكفاءات البشرية المتخصصة، والحاجة إلى تطوير البنية التكنولوجية والبحث العلمي. كما بينت الدراسة أن فعالية توظيف الذكاء الاصطناعي في تعزيز الأمن الوطني الجزائري تظل مرتبطة بقدرة الدولة على بناء رؤية استراتيجية شاملة تقوم على الاستباق، وتطوير القدرات الوطنية، وتعزيز السيادة الرقمية في مواجهة التهديدات التكنولوجية المتصاعدة.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن الوطني الجزائري، الأمن السيبراني، السيادة الرقمية، التحول الرقمي، التهديدات السيبرانية.

Abstract:

This study analyzes the role of artificial intelligence in reshaping the determinants of Algerian national security by examining the conceptual and theoretical framework, as well as Algeria's experience from 2019 to 2026. The analysis specifically assesses Algeria's institutional responses, legislative mechanisms, and implemented policies, while considering the interaction between internal and external environmental factors.

The findings demonstrate that Algeria has achieved progress in this domain but continues to encounter regulatory, human, and technical challenges. The results suggest that effective adoption of security-related artificial intelligence requires a comprehensive strategy based on monitoring and anticipatory measures.

Keywords: artificial intelligence, national security, Algerian national security, cyber security, digital sovereignty.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
“وما توفيقي إلا بالله عليه توكلت وإليه أنيب”
(سورة هود، الآية: 88)

شكر وتقدير

الحمد لله على إحسانه والشكر له على توفيقه لي في إعداد المذكرة يسعدنا أن أتوجه بخالص الشكر والامتنان وفائق الاحترام إلى كل من قدم لي يد العون وساعدني لإتمام العمل، وأخص بالذكر الأستاذ بولعراس فتحي على ما قدمه من نصائح وتوجيهات سديدة وعلى ملاحظاته القيمة وتوصياته الدقيقة لإتمام هذا العمل المتواضع.

أشكر والدي ووالدتي حفظهما لي الله ورعاهما، الذين كانوا عوناً لي خلال مساري الجامعي، فلهم مني كل الشكر والتقدير.

إلى السادة الأفاضل أعضاء اللجنة الموقرة التي تفضلت بمناقشة مذكرتي تحية احترام وتقدير مني لكم.

إلى كل أساتذتي اللذين استنرت بهم في مشواري الجامعي تحية شكر ووفاء وعرفان.

إلى كل من شجعني للمواصلة في درب النجاح شكراً لكم جميعاً.

الطالبة: بن زواش مريم

الإهداء

الحمد لله الذي وفقتني للبدايات بفضلله ووهبني التوفيق والسداد ومنحني الثبات وبلغني
مسك الختام بكرمه بإتمام هذا العمل والخروج به بهذه الصورة المميزة.
أهدي تخرجي إلى من دعماني بدون توقف وعلمانني أن الدنيا كفاح وسلاحها العلم
وعدم الاستسلام الوالدين العزيزين: أبي وأمي، رفيقا دربي وقوتي وبفضلهما
استطعت أن أواجه كل الصعاب وأصل إلى هذه اللحظة، أدامكما الله سندا لي.
إلى من كانا لي بمثابة حافز في خطواتي للوصول إلى مبتغاي أخي وأختي،
إلى جميع أساتذتي الكرام
إلى كل من كان لهم الفضل في وصولي إلى هذه المرحلة من قريب أو من بعيد،
ولو بالدعاء
أهدي هذا العمل إليهم.

مقدمة

مقدمة

شهد مفهوم الأمن الوطني خلال العقود الأخيرة تحولات عميقة تجاوزت التصور التقليدي المرتبط أساساً بالتهديدات العسكرية، ليصبح مفهوماً أكثر اتساعاً وتشابكاً بفعل التحولات التكنولوجية والرقمية المتسارعة التي فرضتها الثورة الصناعية الرابعة. وفي هذا السياق، برز الذكاء الاصطناعي بوصفه أحد أهم المتغيرات المؤثرة في إعادة تشكيل البيئة الأمنية الدولية، ليس فقط باعتباره أداة تقنية، بل باعتباره عاملاً استراتيجياً أصبح يؤثر في طبيعة القوة، وآليات إدارة الصراع، وأنماط الردع، وطرق جمع المعلومات وتحليلها، إضافة إلى دوره المتزايد في مجالات الأمن السيبراني وحماية البنى التحتية الرقمية.

وقد أدى التوسع العالمي في استخدام تطبيقات الذكاء الاصطناعي إلى بروز تحديات أمنية جديدة مرتبطة بالهجمات السيبرانية، والحروب المعلوماتية، والاختراقات الرقمية، واستهداف البيانات والمنظومات الحيوية، الأمر الذي جعل مسألة السيادة الرقمية والأمن السيبراني من القضايا المركزية في السياسات الأمنية المعاصرة. كما أصبحت قدرة الدول على تطوير بنياتها التكنولوجية، وتأهيل مواردها البشرية، وبناء منظومات رقمية آمنة، معياراً أساسياً من معايير القوة والأمن الوطني في البيئة الدولية الراهنة.

ولم تكن الجزائر بمنأى عن هذه التحولات، بحكم موقعها الجيوسياسي وعمقها الاستراتيجي والتحديات الأمنية التي تواجهها في محيط إقليمي ودولي متغير. فقد فرضت التحولات الرقمية المتسارعة على الدولة الجزائرية ضرورة التكيف مع أنماط جديدة من التهديدات، خاصة تلك المرتبطة بالأمن السيبراني، وحماية البيانات، وتأمين البنى التحتية الرقمية، ومواجهة الاستخدامات الأمنية والاستخباراتية المتقدمة للذكاء الاصطناعي. وفي هذا الإطار، شهدت الجزائر خلال السنوات الأخيرة اهتماماً متزايداً بتطوير سياساتها الرقمية والأمنية، من خلال إنشاء مؤسسات متخصصة، وتبني إصلاحات تشريعية، وإطلاق برامج للتحول الرقمي وتعزيز الأمن السيبراني.

وانطلاقاً من ذلك، تسعى هذه الدراسة إلى تحليل تأثير الذكاء الاصطناعي في إعادة تشكيل الأمن الوطني الجزائري خلال الفترة الممتدة بين 2019 و2026، من خلال دراسة التحولات التي فرضتها التقنيات الذكية على البيئة الأمنية الجزائرية، وتحليل الاستجابة المؤسساتية والتشريعية للدولة الجزائرية في هذا المجال. وتنبع أهمية الدراسة من تزايد ارتباط الأمن الوطني بمستوى التطور التكنولوجي والقدرة على بناء سيادة رقمية فعالة، في ظل تصاعد التهديدات السيبرانية والتحولات المرتبطة بالذكاء الاصطناعي على المستويين الإقليمي والدولي.

1- المشكلة البحثية:

أدى التطور المتسارع لتقنيات الذكاء الاصطناعي إلى إحداث تحولات عميقة في طبيعة التهديدات الأمنية وأساليب إدارتها، حيث لم تعد التحديات المرتبطة بالأمن الوطني تقتصر على الأبعاد العسكرية التقليدية، بل امتدت لتشمل الفضاء السيبراني، وحماية البيانات، والسيادة الرقمية، وأمن البنى التحتية المعلوماتية. وفي هذا السياق، أصبح الذكاء الاصطناعي أحد المتغيرات المؤثرة في إعادة تشكيل السياسات الأمنية للدول، من خلال ما يتيح من أدوات جديدة في مجالات الرصد، والتحليل، والاستجابة للتهديدات الرقمية والسيبرانية.

وفي ظل التحولات الرقمية المتسارعة، برزت الحاجة لدى الجزائر إلى تطوير مقاربتها الأمنية بما يتلاءم مع طبيعة التهديدات الجديدة المرتبطة بالفضاء السيبراني والتكنولوجيا الذكية، خاصة في ضوء تزايد أهمية الأمن السيبراني والسيادة الرقمية ضمن منظومة الأمن الوطني المعاصر. وانطلاقاً من ذلك، تتمحور مشكلة الدراسة حول التساؤل الرئيسي الآتي:

إلى أي مدى يساهم توظيف الذكاء الاصطناعي في إعادة تشكيل المقاربة الأمنية

الجزائرية خلال الفترة الممتدة بين 2019 و2026؟

ويتفرع عن هذا التساؤل الرئيسي مجموعة من التساؤلات الفرعية:

• كيف أثرت التحولات الرقمية والتهديدات السيبرانية في توجهات السياسة

الأمنية الجزائرية خلال الفترة 2019-2026؟

- فيما يتمثل واقع جاهزية البنية المؤسسية والتشريعية الجزائرية لتوظيف الذكاء الاصطناعي في المجال الأمني؟
- ما واقع توظيف تقنيات الذكاء الاصطناعي في تعزيز الأمن السيبراني والسيادة الرقمية في الجزائر؟
- كيف تسهم الإستراتيجية الوطنية للذكاء الاصطناعي في تطوير القدرات الأمنية والتكنولوجية للدولة الجزائرية؟

2- الفرضيات:

الفرضية الرئيسية:

كلما توسع توظيف الذكاء الاصطناعي في المنظومة الأمنية للدولة، كلما تعززت قدرة الدولة على الوقاية من التهديدات السيبرانية.

الفرضيات الفرعية:

- العلاقة بين الأمن الوطني والذكاء الاصطناعي تقوم على جدلية التهديد والفرصة.
- تتكيف الهندسة الأمنية مع التحول الرقمي عبر تطوير الأطر التشريعية والمؤسسية، ويرتبط نجاح هذا التكيف بمدى جاهزية واستجابة البنية التحتية التكنولوجية.
- يرتبط تعزيز الأمن الوطني في ظل الإستراتيجية الوطنية للذكاء الاصطناعي، بمدى التركيز على إدماج تطبيقات الذكاء الاصطناعي في القطاعات الحيوية.

3- الإطار المنهجي والنظري للدراسة:

➤ المناهج المستخدمة:

اعتمدت الدراسة على منهج تحليل السياسات العامة باعتباره المنهج الأنسب لفهم كيفية تعامل الدولة الجزائرية مع الذكاء الاصطناعي كخيار أمني واستراتيجي، مدعوماً بالمنهج الوصفي-التحليلي ودراسة الحالة.

منهج تحليل السياسات العامة: يرجع الاعتماد عليه لأن الذكاء الاصطناعي ليس مجرد تقنية، بل خيار سياسي-أمني، تتعامل معه الجزائر عبر: استراتيجيات، تشريعات، مؤسسات، قرارات سيادية. يتم توظيفه في الدراسة بتحليل سياسات الدولة الجزائرية في مجال: الذكاء الاصطناعي، الأمن السيبراني، التحول الرقمي الأمني، صف إلى ذلك

مقدمة

تقييم مدى انسجام هذه السياسات مع متطلبات الأمن الوطني، وبالتالي هذا المنهج يجنبنا الوقوع في الوصف التقني، ويركز على الدولة كفاعل استراتيجي.

المنهج الوصفي-التحليلي: الذي تم استخدامه من أجل ضبط المفاهيم المركزية: الأمن الوطني، الذكاء الاصطناعي، الأمن السيبراني، وكذا وصف واقع إدماج الذكاء الاصطناعي في الجزائر: على المستوى المؤسسي، القانوني، الأمني.

منهج دراسة الحالة: تم الاعتماد عليه لتحليل تجربة وطنية محددة خلال الفترة (2019-2026)، وفهم ديناميات التحول الأمني في الجزائر كحالة مفردة معمقة مع التركيز على الأمن السيبراني، المؤسسات الأمنية، التشريعات الرقمية. وهذا يعزز القيمة العلمية والتطبيقية للدراسة.

➤ الإطار النظري المعتمد:

أولاً: نظرية الأمن الشامل

تُعد نظرية الأمن الشامل من المقاربات الملائمة لفهم التحولات الأمنية المعاصرة، لأنها توسّع مفهوم الأمن ليشمل أبعاداً متعددة تتجاوز المجال العسكري التقليدي، مثل الأمن السيبراني، والأمن المجتمعي، والأمن الاقتصادي، والسيادة الرقمية. وقد ارتبطت هذه المقاربة أساساً بأعمال مدرسة كوبنهاغن، خاصة باري بوزان (Barry Buzan)، وأولي ويفر (Ole Wæver)، وجاب دي وايلد (Jaap de Wilde)، الذين سعوا إلى إعادة تعريف الأمن بوصفه منظومة مركبة تشمل قطاعات متعددة مترابطة.

وقد وردت هذه المقاربة بشكل واضح في كتاب:

Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder: Lynne Rienner Publishers, 1998).

كما تناول باري بوزان فكرة توسيع مفهوم الأمن في كتابه:

Barry Buzan, People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era (Boulder: Lynne Rienner Publishers, 1991).

وتفيد هذه النظرية في دراسة الذكاء الاصطناعي باعتباره محدداً جديداً للأمن الوطني، لما يفرضه من تحولات تمس الأمن السيبراني، والسيادة الرقمية، والبنى المعلوماتية، والقدرات الدفاعية للدولة.

ثانياً: نظرية الأمانة

مقدمة

تُوظف نظرية الأمننة لفهم الكيفية التي يتم من خلالها تقديم الذكاء الاصطناعي داخل الخطاب الأمني باعتباره فرصة استراتيجية أو تهديداً للأمن الوطني. وترجع هذه النظرية إلى مدرسة كوبنهاغن، خاصة أعمال أولي ويفر (Ole Wæver) وباري بوزان (Barry Buzan)، حيث تقوم على فكرة أن التهديدات الأمنية ليست معطيات موضوعية فقط، بل تُبنى أيضاً عبر الخطاب السياسي والمؤسساتي.

وقد ظهرت الأسس الأولى للنظرية في أعمال أولي ويفر، خاصة مقاله:

Ole Wæver, "Securitization and Desecuritization," in *On Security*, ed. Ronnie D. Lipschutz (New York: Columbia University Press, 1995).

كما تم تطويرها بصورة أكثر شمولاً في كتاب:

Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner Publishers, 1998).

وتفيد هذه النظرية في تحليل الكيفية التي يُقدّم بها الذكاء الاصطناعي في الخطاب الأمني الجائري، سواء باعتباره أداة لتعزيز الأمن الوطني، أو باعتباره مصدراً لتهديدات سيبرانية ومعلوماتية جديدة.

ثالثاً: اقتراب حوكمة الأمن

يُعد اقتراب حوكمة الأمن من المقاربات المهمة لفهم إدارة المخاطر الأمنية المعاصرة، خاصة تلك المرتبطة بالفضاء الرقمي والتكنولوجي، حيث يركز على تعدد الفاعلين والمؤسسات وآليات التنسيق والتشريع والتنظيم. وقد ارتبط هذا الاقتراب بعدد من الباحثين في دراسات الأمن والحوكمة، من أبرزهم مارك دوفيلد (Mark Duffield)، وريتا أبراهامسن (Rita Abrahamsen)، ومايكل وليامز (Michael C. Williams).

ومن أبرز الأعمال المرجعية في هذا المجال:

Mark Duffield, *Global Governance and the New Wars: The Merging of Development and Security* (London: Zed Books, 2001).

وكذلك:

Rita Abrahamsen and Michael C. Williams, *Security Beyond the State: Private Security in International Politics* (Cambridge: Cambridge University Press, 2011).

ويُستخدم هذا الاقتراب في تحليل دور الدولة الجائرية والمؤسسات الأمنية والتشريعات الوطنية في تنظيم استخدامات الذكاء الاصطناعي، وضبط مخاطره الأخلاقية والسيبرانية، وفهم مستوى التنسيق المؤسساتي المرتبط بالأمن الرقمي والسيادة الرقمية.

رابعاً: اقتراب صنع القرار الأمني

يفيد اقتراب صنع القرار الأمني في تحليل الكيفية التي تتخذ بها الدولة قراراتها الإستراتيجية المرتبطة بالأمن والتكنولوجيا، خاصة في ظل بيئة دولية وإقليمية متغيرة. ويرتبط هذا الاقتراب بأعمال عدد من الباحثين في دراسات صنع القرار والسياسة الخارجية، من أبرزهم غراهام أليسون (Graham Allison)، وريتشارد سنايدر (Richard Snyder)، وهربرت سايمون (Herbert Simon).

ومن أبرز المراجع المؤسسة لهذا الاقتراب:

Graham Allison and Philip Zelikow, Essence of Decision: Explaining the Cuban Missile Crisis, 2nd ed. (New York: Longman, 1999).

وكذلك:

Richard C. Snyder, H. W. Bruck, and Burton Sapin, Decision-Making as an Approach to the Study of International Politics (Princeton: Princeton University Press, 1954).

أما هربرت سايمون فقد أسس لمفهوم العقلانية المحدودة في كتابه:

Herbert A. Simon, Administrative Behavior (New York: Free Press, 1947).

ويفيد هذا الاقتراب في تفسير توجه الجزائر نحو الاستثمار في الذكاء الاصطناعي باعتباره خياراً استراتيجياً مرتبطاً بقراءة التهديدات الجديدة، والتكيف مع التحولات الإقليمية والدولية، وتعزيز القدرات الأمنية والسيبرانية للدولة.

مفاهيم الدراسة

الذكاء الاصطناعي: يشير إلى الأنظمة أو الأجهزة التي تحاكي الذكاء البشري لأداء المهام، والتي تعتمد على إنشاء وتطبيق الخوارزميات المنفذة في بيئة الحوسبة الديناميكية، وبإمكانها أن تحسن من نفسها استنادا إلى المعلومات التي تجمعها. وهي تتعلق بالقدرة على التفكير الفائق وتحليل البيانات.¹

الأمن الوطني: هو القدرة على توفير أكبر قدر من الحماية والاستقرار لتحقيق التنمية الشاملة للدولة في كافة المجالات السياسية والاقتصادية والاجتماعية والإيديولوجية والعسكرية والمعلوماتية في الدولة ضد كافة أنواع التهديدات الداخلية والخارجية سواء إقليمية أو عالمية.²

الأمن السيبراني: مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.³

السيادة الرقمية: هو قدرة الدولة على التحكم في التكنولوجيا التي تقوم عليها الأنشطة الاقتصادية والاجتماعية، وعلى ممارسة قراراتها السيادية ضمن الفضاء السيبراني دون خضوع لأي تبعية خارجية وهي تتجلى كذلك في امتلاك الدولة القدرة على إدارة فضاءها المعرفي، والتحكم في شبكات الاتصال والبيانات المتداولة عبر الانترنت.⁴

4- مبررات اختيار الموضوع:

ينبع اختيار الموضوع من عدة مبررات موضوعية وذاتية:

1/ **المبررات الموضوعية:** ترتبط بالسياق الوطني والدولي أبرزها: الأهمية الإستراتيجية للموضوع نظرا لحدائته وقلة الدراسات العلمية المحلية حوله، كما أن فترة الدراسة من 2019-2026 ذات دلالة لإعادة تشكيل البيئة الأمنية سواء داخليا أو خارجيا.

¹ منظمة الأمم المتحدة للتربية والعلم والثقافة، *فهرس دليل اليونيسكو في مصطلحات تكنولوجيا المعلومات* (اليونيسكو، 2022) ص 78.

² أحمد محمد فاروق محمو مجاهد، "الأمن الوطني: مفهوم ومهددات الأمن الوطني" *مجلة الدراسات الإفريقية*، م. 42، ع. 2 (يونيو 2021) ص 245.

³ فارس قره، "الأمن السيبراني"، الموسوعة السياسية، 2019-08-28، <https://shorturl.at/2nmah>

⁴ الشيماء مخالفة، كريمة لعبساوي، "السيادة الرقمية: تكيف العقيدة الدفاعية الجزائرية مع التهديدات الأمنية الجزائرية"، *المجلة الجزائرية للعلوم الاجتماعية والانسانية*، م. 12، ع. 02 (2025) ص 396.

2/ المبررات الذاتية: يبرز الاهتمام من الرغبة في استكشاف العلاقة بين الذكاء الاصطناعي والأمن الوطني، خاصة في ظل التحولات المتسارعة للتكنولوجيا. إضافة إلى الطموح الشخصي في التخصص بمجال يجمع بين الدراسات الأمنية والثورة التكنولوجية. فالموضوع يتيح فرصة لفهم أعمق للتحديات والفرص التي يطرحها الذكاء الاصطناعي على مستقبل الدول.

5- أهمية الدراسة:

➤ **الأهمية العلمية للدراسة:** تبرز القيمة العلمية للدراسة في كونها يقدم إطارا تحليليا جديدا يربط بين الأمن الوطني والذكاء الاصطناعي، والذي من شأنه إثراء الدراسات العلمية وفق مقاربة سياسية وأمنية. بهذا الشكل سيساهم في سد الفجوة الأكاديمية، فالموضوع حديث لم يسبق التطرق له، وهو ما يعطي للدراسة قيمة مضافة في هذا المجال الحديث.

➤ **الأهمية العملية للدراسة:** تكمن الأهمية العملية لهذه الدراسة على قدرتها في منح إدراك وجودي لإيجابيات وسلبيات الذكاء الاصطناعي أمنيا ودفاعيا لمساعدة صانع القرار نحو وضع سياسات وآليات فعالة، تعزز من جاهزية الدولة لاعتماد الذكاء الاصطناعي على المستوى الأمني والدفاعي. ضف إلى ذلك المساهمة في تطوير برامج تركز على الابتكار والبحث تنمية للمهارات في هذا المجال، بالشكل الذي يدعم جهود الدولة لتهيئة وتأمين المسار نحو تحول ناجح.

6- أهداف الدراسة:

- يطمح هذا البحث إلى تحقيق مجموعة من الأهداف والغايات، وتتمثل في:
- دراسة العلاقة بين الذكاء الاصطناعي والأمن الوطني الجزائري.
 - تقييم مدى استعداد الجزائر لتبني الذكاء الاصطناعي، وموقعها ضمن مؤشر جاهزية الحكومات للذكاء الاصطناعي.
 - إبراز دور الإستراتيجية الوطنية للذكاء الاصطناعي في تعزيز الأمن الوطني الجزائري.

7- الدراسات السابقة:

أ. كتاب جماعي معنون: **فهم الأمن القومي الجزائري من مدخلي الأمن والدفاع الوطني***، يضم الكتاب مجموعة من المقالات تناولت تعريف الأمن القومي الجزائري وفق مقاربات نظرية مع التركيز على الجانب العسكري، والتهديدات التي تستهدف الدولة الجزائرية والمؤسسات المنوطة بحمايتها. تتفق الدراسة مع الكتاب في اتخاذ الأمن الوطني الجزائري كوحدة تحليل مركزية، أما محور الاختلاف فيكون في كون: الكتاب ينطلق من مقارنة أمنية تقليدية تركز بالأساس على المدخل والتهديدات العسكرية بينما تركز الدراسة على نظرية الأمن الشامل، لأن تطورات الذكاء الاصطناعي أصبحت تمس الأمن العسكري، السياسي، المجتمعي والاقتصادي كمتغير جديد يغير من طبيعة التهديدات.

ب. أطروحة دكتوراه بعنوان: **مستقبل الأمن القومي الجزائري في ظل التطورات التكنولوجية وحروب المعلومات***، حيث تطرق الباحث فيها إلى مفاهيم الأمن القومي الجزائري، التكنولوجيا، حرب المعلومات، من خلال محاور متعددة. ركزت الدراسة على تأثيرات تكنولوجيا المعلومات والاتصالات على الأمن القومي الجزائري مع تسليط الضوء على الإمكانيات التي تملكها الجزائر لمجابهة تهديدات الفضاء الرقمي، واستشراف مستقبل الجزائر الأمني ومدى قدرتها على مواكبة التحولات التكنولوجية. أوجه الشبه: تتفق الدراسة مع الأطروحة في ربط الأمن الوطني بالتحولات التكنولوجية والفضاء الرقمي، والتظر إلى التكنولوجيا كسلاح ذو حدين، إما مصدر تهديد أو عنصر لقوة مضاعفة.

أوجه الاختلاف: ركزت الأطروحة على تكنولوجيا المعلومات والاتصالات ومفهوم حرب المعلومات، في المقابل تركز الدراسة الحالية على الذكاء الاصطناعي باعتباره نقلة نوعية من التعقيد التي تتجاوز مجرد تبادل المعلومات. ومن حيث الحدود الزمنية أخذت الأطروحة طابعا استشرافيا لمستقبل الأمن، أما الدراسة فميزها تأطير زمني

* كتاب فهم الأمن القومي الجزائري من مدخلي الوطني والدفاع الوطني، هو كتاب جماعي لمجموعة من الباحثين من تقديم وليد عبد الحى، وتحرير وإشراف: د. بهلول نسيم، عمان: دار ومكتبة الحامد للنشر والتوزيع، الطبعة الأولى، 2015. يضم مقالات حول الأمن القومي الجزائري، بداية من تأصيل للمفهوم، إلى مختلف الآليات، المؤسسات، الاستراتيجيات المنتهجة في المنظومة الأمنية والدفاعية الجزائرية.

* أطروحة أنجزها الباحث تاهمي مصطفى للسنة الجامعية 2024/2023.

خلال الفترة 2019-2026 وهي الفترة التي شهدت التزايد الحقيقي لتطبيقات الذكاء الاصطناعي والسباق العالمي نحو وضع استراتيجيات وطنية للذكاء الاصطناعي. ج. مقال موسوم: **الذكاء الاصطناعي وتحديات الأمن الوطني: مقارنة تقنية***، تناول المقال مفهوم الذكاء الاصطناعي والفرص التي يتيحها سواء في المجالات الأمنية والعسكرية، وفي ميدان الصحافة والإعلام. كما ركز على مختلف التحديات التي تفرضها تقنيات التعلم العميق على الأمن الوطني. والتي توصلت إلى نتيجة أن الوعي الفردي والمجتمعي يعتبر آلية فعالة لمواجهة المخاطر المرتبطة بتطور تقنيات الذكاء الاصطناعي.

أوجه الشبه: تشترك دراستنا مع المقال في ربط المباشر بين الذكاء الاصطناعي وتأثيراته الحتمية على الأمن الوطني، إضافة إلى النظر لهذه التكنولوجيا كمتغير مزدوج التأثير، يخلق فرصا وتهديدات معقدة غير مسبوقة.

أوجه الاختلاف: المقال انحصر في المقاربة التقنية وآليات عمل التكنولوجيا، في حين الدراسة تركز على مقاربة استراتيجية أمنية تشمل العقيدة الدفاعية وفق الاستجابة المؤسساتية، التشريعية والسيادية لمواكبة الطبيعة الجديدة للتهديدات.

8- حدود الدراسة

➤ الحدود المكانية:

تقتصر هذه الدراسة من الناحية المكانية على الجزائر حيث يتم تحليل الجهود والسياسات التي اتخذت على المستوى الوطني لتبني الذكاء الاصطناعي لتدعيم منظومتها الأمنية، ويهدف ذلك لتوفير إطارا مرجعيا لفهم خصوصية الأمن الوطني الجزائري في مجال الذكاء الاصطناعي.

➤ الحدود الزمانية:

تركز الدراسة على الفترة الممتدة من 2019 إلى غاية 2026، باعتبارها الفترة التي عرفت اهتماما متزايدا مع تكثيف الإجراءات للتوجه نحو الذكاء الاصطناعي. وقد تم اختيار هذه الفترة كونها تمثل الإطار الزمني الأكثر دلالة لتحليل مدى نجاعة كافة التدابير في تعزيز الأمن الوطني.

* المقال من إعداد المهندس محمد بن نجمة الصادر سنة 2023.

9- هيكلة الدراسة:

بناء على المعطيات السابقة وفي إطار الإجابة على نص الإشكالية المطروحة، تم تقسيم العمل إلى ثلاثة فصول:

- **الفصل الأول:** الإطار المفاهيمي والنظري للعلاقة بين الذكاء الاصطناعي والأمن الوطني. يتناول مفهوم متغير الدراسة المستقل: الذكاء الاصطناعي عبر تعريفه من منظور أمني - استراتيجي، وتحديد أهدافه واستخداماته في المجالين الأمني والدفاعي، وينتقل لضبط متغير الدراسة التابع الأمن الوطني الجزائري، مسلطا الضوء على مفهومه ومستوياته، مع إبراز مرتكزاته في ظل التحولات التكنولوجية الراهنة، ورصد طبيعة التهديدات الأمنية الحديثة في البيئة الجزائرية. وفي ختام الفصل تم ربط المتغيرين عبر تحليل طبيعة العلاقة بين الأمن الوطني والذكاء الاصطناعي، من خلال التطرق إلى الذكاء الاصطناعي كمحدد جديد في المنظومة الأمنية ضمن ثنائية: منطق التهديدات التي يفرضها، ومنطق الفرص التي يتيحها.
- **الفصل الثاني:** الهندسة الأمنية الجزائرية في ظل الذكاء الاصطناعي. يعرض الإطار القانوني لأمن السيبراني، ومؤسسات الأمن الوطني، ويحلل موقع الجزائر في مؤشر جاهزية الحكومات للذكاء الاصطناعي.
- **الفصل الثالث:** دور الإستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي (2020-2030) في تعزيز الأمن الوطني. ويقدم الفصل تحليلا لدوافع صياغتها الخارجية والداخلية، محاور الإستراتيجية، انعكاساتها على الأمن الوطني. إلى جانب دراسة نقاط القوة والضعف، التحديات والفرص وفق أداة التحليل SWOT.

الفصل الأول

الإطار المفاهيمي والنظري للعلاقة بين الأمن الوطني والذكاء

الاصطناعي

المبحث الأول: الإطار المفاهيمي للذكاء الاصطناعي.

المبحث الثاني: الإطار المفاهيمي للأمن الوطني الجزائري.

المبحث الثالث: العلاقة بين الأمن الوطني والذكاء الاصطناعي.

المبحث الأول: الإطار المفاهيمي للذكاء الاصطناعي

سعيًا لاستيعاب طبيعة الذكاء الاصطناعي ضمن السياق الأمني، يقدم هذا المبحث تأطيرًا للمفهوم من منظور أمني، استراتيجي، لينتقل إلى تحديد أهدافه الرئيسية، وأبرز تطبيقاته العملية في المجالين الأمني والدفاعي.

المطلب الأول: تعريف الذكاء الاصطناعي من منظور أمني _ استراتيجي

يعد تعريف الذكاء الاصطناعي أمر معقد، لا يوجد تعريف متفق عليه. تعدد التعاريف يعكس طبيعته المتعددة الأبعاد والتنوع الوظيفي لهذه التقنية.¹ هنا سنحدد بعض التعاريف للذكاء الاصطناعي:

التعريف الضيق: يركز على محاكاة الذكاء البشري عبر أجهزة الكمبيوتر. يعرفه البعض بأنه: "تقنية تمكن الآلات من تقليد المهارات البشرية المعقدة، ومع ذلك هذا التعريف يبقى عامًا وغير محدد لتلك المهارات."

التعريف الوظيفي: يولي اهتمامًا بالأداء العملي، يعرفه عالم الحاسوب نيلس جون نيلسون (Nils J. Nilsson) بأنه "تقنية تعمل بشكل مناسب وببصيرة في بيئتها". تعريفًا مشابه قدمته مجموعة الخبراء حول الذكاء الاصطناعي التابعة للمفوضية الأوروبية: "أنظمة تظهر سلوكًا من خلال تحليل بيئتها واتخاذ إجراءات -بدرجة معينة من الاستقلالية -لتحقيق أهداف محددة".²

في سعيًا إيجاد تعريف للذكاء الاصطناعي من منظور أمني -استراتيجي، ننطلق من اعتباره تكنولوجية حيوية، قادرة على محاكاة القدرات البشرية استراتيجيًا لتعزيز الأمن الوطني، على المستوى المعلوماتي والعملياتي. يظهر لنا هنا أن الذكاء الاصطناعي مسألة كسب قوة أمنية ورهان سلطوي ليس مجرد تقنية فقط، لكن كيف ذلك؟ نبرر هذا من خلال:

- ميشال فوكو (Foucault) والسيطرة الخوارزمية: يؤكد ميشال فوكو أن كل إنتاج معرفي مصحوب بعلاقات قوة. تطبق هذه الفكرة على الذكاء الاصطناعي حيث تنتج الخوارزميات

¹ Haroon Sheikh, Corien Prins and Erik Schrijvers, *Mission AI: The New System Technology* (Springer: WRR The Netherlands Scientific Council for Government Policy, 2023), p. 15.

² Ibid.

تصنيفات ومراقبة مستمرة تشكل أشكالاً جديدة من السلطة الأمنية. فالخوارزميات ليست محايدة، إنما تبرمج بأولويات سياسية تعزز هيمنة من يسيطر عليها.¹

- هايدغر (Heidegger) في السؤال حول التقنية، يحذر من أن التكنولوجيا تحول الواقع إلى مخزون جاهز للاستغلال، فهيمنة الذكاء الاصطناعي على السلوك البشري عبر المعلومات والتوصيات الخوارزمية، يخلق استقطاب إدراكي يشكل تهديداً بنيوياً لأمن الاجتماعي.²

الجمع بين الروى المختلفة يقودنا إلى النظر إلى الذكاء الاصطناعي من منظور أمني استراتيجي على أنه أداة للهيمنة والسيطرة:

جدول رقم 01 : يوضح كيف أن الذكاء الاصطناعي يعد أداة للهيمنة والسيطرة.

في أي مستوى؟	كيف؟	بالاتتماد على ماذا؟
الذكاء الاصطناعي الضيق (ANI): يتخصص في مجال واحد، لا يستطيع حل المشكلات في مجالات أخرى بشكل مستقل.	التعلم الآلي (Machine Learning) فرع من الذكاء الاصطناعي يعتمد على البيانات لاتخاذ القرارات والتنبؤ.	الخوارزميات البيانات قوة الحوسبة
الذكاء الاصطناعي العام (AGI): وصل إلى مستوى ذكاء الإنسان، له القدرة على التفكير المنطقي، التخطيط وحل المشكلات.	التعلم العميق: (Deep Learning) تقنية متقدمة يعتمد على شبكات عصبية مشابهة للدماغ البشري، التي تجعله يتوفق في المهام المعقدة، وقراءة الأنماط الخفية.	
الذكاء الاصطناعي الفائق (ASI): الذكاء الذي تفوق على عقل الإنساني في الإبداع، والمعرفة.		

المصدر: من إعداد الطالبة، بالاتتماد على المرجع -بتصرف:-

Introduction to Artificial Intelligence (AI) Technology: Guide for Travel

¹ فادي علي رضا ، الهندسة العكسية للذكاء الاصطناعي في الحروب الحديثة: مقارنة سوسيولوجية عسكرية، مجلة أوراق الثقافة، م. 37 (جولية 2025) ص 188.

²Xinnian Wang, Ao Hu, Xincheng Liu et al, *Intrinsic Security of Artificial Intelligence: System Vulnerabilities, Defense Mechanism, and Theoretical Deepening*(Springer Nature Singapore Pte Ltd, 2026), p. 531.

& Tourism Leaders (Microsoft 2024), pp. 20,21.

يشير الجدول إلى أن تطور الذكاء الاصطناعي ساهم في ظهور نوع جديد من السيطرة التي تجسد في توظيفها خيارات، مصالح أو أولويات قائمة على الخوارزميات، البيانات، وقوة الحوسبة. خاصة في ظل تواجد قوى كبرى مثل: الولايات المتحدة الأمريكية، الصين، روسيا التي تستحوذ وتتحكم في هذه التكنولوجيا الحيوية، في مقابل دول تستورد وتستهلك تلك الأنظمة والبرمجيات، الأمر الذي يجعلها عرضة للتبعية التكنولوجية. وعليه التعريف الإجرائي الذي تتبناه الدراسة للذكاء الاصطناعي بأنه: مجموعة الأنظمة المتقدمة التي تحاكي القدرات البشرية لدعم القرار الأمني وتحقيق الغايات الدفاعية.

المطلب الثاني: أهداف الذكاء الاصطناعي في المجالين الأمني والدفاعي

يعتبر الذكاء الاصطناعي عابر ومتعدد المجالات، ولكن ما يهمنا في إطار هذه الدراسة هو المجالين الأمني والدفاعي. من الناحية التحليلية، نجل الأهداف وفق ثلاثة عناصر أساسية، انطلاقاً من أن كل هدف يعكس استخداماً محدداً، لكن في مجملها هي عناصر متكاملة تشكل أهدافاً إستراتيجية:¹

المواجهة الهجومية المباشرة: يشمل دعم، وتطوير القرار المؤدي إلى استخدام القوة، بتطوير أنظمة الأسلحة المستقلة الفتاكة، وتعزيز القرارات التكتيكية ومساندة الأفراد العسكريين في بيئات القتال، هذا يجعل من الذكاء الاصطناعي قوة قتالية مساندة.

الردع والحماية: وهو هدف عدائي غير حركي، يشمل الدفاع السيبراني وتنفيذ العمليات الهجومية السيبرانية، هنا يتمحور دوره الأساسي كدرع سيبراني ومنسق دفاعي.

الدعم والاستدامة: يركز على الربط بين الهدفين السابقين عبر تعزيز قوة الأنظمة ومرونتها، دعم العمليات الإدارية، اللوجستية والتخطيط العملياتي، تحسين الوعي بالموقف، ودعم العمليات الوطنية الطارئة الذي يعكس رد فعل طويل الأمد يستمر ويتكيف مع المستقبل.²

¹Mariarsaria Taddeo, David McNeish, Alexander Blanchard et al., **Ethical Principles For artificial intelligence in the defence domain**(New York, Routledg: Taylor & Francis Group, 2023), p. 163.

²Loc-cit.

استنادا لأهداف سابقة الذكر، فالربط الإلزامي بينها يشكل تكامل أمني-دفاعي طويل الأمد، فالذكاء الاصطناعي لا يعمل كنظام مستقل، بل وفق شبكة ثلاثية: ميدانية، وقائية ومستديمة.

المطلب الثالث: الاستخدامات الأمنية والدفاعية للذكاء الاصطناعي

يسعى هذا المطلب إلى تسليط الضوء على أبرز الاستخدامات الحيوية للذكاء الاصطناعي في الشقين الأمني والدفاعي. حيث تجمع الأدبيات الحديثة على أن هذه التقنية أصبحت عنصرا جوهريا في تعزيز كفاءة العمليات الأمنية وتطويرها، وهو ما تجسد في التطبيقات التالية:¹

المراقبة: أحدث الذكاء الاصطناعي نقلة نوعية في جمع المعلومات وتحليلها. حيث يمكن للحوارزميات المتقدمة تحديد الأنماط غير المعتادة وتتبع الأشخاص محل الاهتمام، والتنبؤ بالمخاطر الأمنية. لتعزيز جهود مكافحة الإرهاب ومحاربة الجرائم العابرة للحدود. كما أصبحت تقنيات التعرف على الوجه والتتبع البيومتري مكونات رئيسية في أنظمة المراقبة الحديثة.

الأمن السيبراني والدفاع ضد التهديدات: مع تزايد عدد الهجمات الإلكترونية التي تستهدف البنية التحتية، تلعب الأنظمة المدعومة بالذكاء الاصطناعي في كشف التهديدات وتحديدتها من خلال تحليل حركة مرور الشبكة، وتحديد الشذوذ، والتنبؤ بالاختراقات. تتعلم هذه الأنظمة باستمرار من الهجمات السابقة، مما يحسن قدرتها على مواجهة التهديدات الجديدة والمتطورة لحماية قواعد البيانات الحكومية الحساسة، شبكات الدفاع، والأنظمة المالية من المتسللين.²

الأسلحة المستقلة والحروب: توفر الطائرات المسييرة وأنظمة القتال الروبوتية المدعومة بالذكاء الاصطناعي مزايا رئيسية، من خلال تقليل تعرض البشر لمخاطر ساحة المعركة. تساعد هذه التقنيات على تحسين دقة الاستهداف مما يسمح للقوات الدفاعية بتكييف إستراتيجيتها في الوقت الفعلي.

¹Yogita Upadhyat and Rituja Sharma, "Legal Framework for AI in National Security: Balancing Innovation, Ethics, and Regulation," *Journal of Neonatal Sergey*, Vol. 14 (2025), p. 501.

²Loc.cit.

الكوارث والاستجابة للطوارئ: أصبح الذكاء الاصطناعي أداة أساسية في إدارة الكوارث والاستجابة للطوارئ حيث يعزز قدرة الحكومات على التخفيف من الأزمات بفعالية، بشكل أكثر كفاءة أثناء الكوارث الطبيعية أو الهجمات الإرهابية. تسمح التقييمات الفورية المستخلصة من صور الأقمار الصناعية والطائرات بدون طيار، بتحديد أولويات مهام الإنقاذ وتقديم المساعدة.¹

تأمين الحدود: تمكن تطبيقات الذكاء الاصطناعي من مراقبة الحدود ألياً، والكشف عن الأنشطة والوقائع التي يمكن أن تؤثر على السلامة الإقليمية للدولة بمواجهة أعمال التهريب واختراق الحدود والهجرة غير الشرعية.

تقديم الدعم المعلوماتي والاستخباراتي: ويتعلق هذا بحالة الحرب وذلك بتوفير معلومات آلية حول الظروف المحيطة بالقوات على الأرض من خلال صور الأقمار الصناعية ورصد التغريدات والتعليقات في المواقع الاجتماعية والإخبارية وتحليلها عبر الذكاء الاصطناعي وتقديم توصيات فورية للجنود في الميدان العسكري للحصول على المعلومات الضرورية.²

¹*Ibid.*, 502.

² شريف شعبان مبروك، "الاستخدامات العسكرية للذكاء الاصطناعي: الفرص والتحديات"، *مجلة استشراف للدراسات المستقبلية*، م.9، ع.9 (ديسمبر 2024) ص 151، 152.

المبحث الثاني: الإطار المفاهيمي للأمن الوطني الجزائري

المطلب الأول: مفهوم الأمن الوطني و مستوياته

1/ مفهوم الأمن الوطني:

المعنى اللغوي لأمن : هو ضد الخوف ونقيضه، وهو حالة تكتسب نتيجة إجراءات ووسائل متعددة، وليس فعلا واحدا يمكن إنجازة.¹

أ/المفهوم التقليدي للأمن الوطني:

اقتصرت دلالة الأمن الوطني في بداياته حول ضمان حماية السكان والممتلكات داخل حدود الدولة من الأخطار المحتملة، مع تطور العلاقات الدولية، أصبح التركيز على حماية الدولة من تهديدات خارجية، عبر بناء جيوش قوية والدخول في تحالفات عسكرية لضمان سلامة الأراضي. كان مصدر التهديد الأساسي آنذاك هو الدول الأخرى، أي أن الأمن كان يفهم في إطار عسكري بحت.²

ب/ المفهوم المعاصر للأمن الوطني:

شهد المفهوم توسعا تدريجيا استجابة للمتغيرات الزمنية، مكتسبا أبعادا أكثر شمولاً، فلم يعد مقتصرًا على السلاح والتدريب العسكري، بل أصبح يتعامل مع تحديات مثل التضخم السكاني، الفقر، ندرة الموارد، الأمراض، الإرهاب، التطرف، الهجرة غير الشرعية، والحروب الإلكترونية.³

قد تعددت التعريفات في هذا السياق، والتي تتراوح ما بين القيم المجردة أو الاعتبارات الإستراتيجية المحددة أو المفاهيم المجتمعية ذات الطبيعة الشمولية:⁴ وتعرف موسوعة العلوم الاجتماعية الأمن القومي بأنه: قدرة الأمة على حماية قيمها الداخلية من التهديدات الخارجية .

ويرى والتر ليبمان: أن الأمة الآمنة ليست في خطر التضحية بالقيم الأساسية إذا اضطرت الى تجنب حرب ما، وأنها قادرة إذا تم تحديدها على صيانتها بالانتصار في تلك الحرب .

¹ خالد علي محمد الأميري، أحمد فلاح العموش، "الأمن الوطني: المفهوم، الأبعاد والنظريات"، مجلة الآداب، ع. 133 (2020) ص 531.

² رئيسي لعل بعيو، "تطور مفهوم الأمن على الساحة الدولية: نحو توسيع وعميق الأجندة الأمنية"، مجلة الشرطة، ع. 157 (فيفري 2024) ص 29.

³ المكان نفسه.

⁴ رابح لعروسي، "ظاهرة الأمن الوطني: قراءة معرفية في المفهوم والدوافع"، (2017) ص 113.

ويرى ولفرز: أن الأمن يعني حماية القيم التي تم اكتسابها، وغياب الخوف من أي هجوم على تلك القيم .

أما تريجر وكروننبرج في كتاب الأمن القومي والمجتمع الأمريكي يريان أن: القيم القومية الحيوية تشكل جوهر سياسة الأمن القومي، ويتحدد الأمن لديهما بأنه ذلك الجزء من سياسة الحوكمة الذي يستهدف إيجاد شروط سياسية دولية ووطنية ملائمة لحماية أو توسع القيم الحيوية ضد الأعداء الحاليين أو المحتملين .

ويرى كل من بركويتز وبوك في كتاب الأمن القومي الأمريكي أن الأمن يعني: "حماية الدولة من الخطر الخارجي" ¹.

ويرى روبرت مكنمارا وزير الدفاع الأمريكي الأسبق في كتابه جوهر الأمن أن الأمن يعني التنمية .وقد كان هذا التعريف فاتحة الاتجاه وتيار أقوى إلى الربط بين الأمن القومي والرفاهية الاقتصادية والتوازن بالإضافة إلى القدرة العسكرية .

من خلال مختلف التعاريف، نرى أن هناك نقاط تداخل بينهما، بالتركيز على أن: الأمن الوطني يقاس بغياب أي تهديد للدولة، وأساسه يكمن في البقاء والاستمرارية . أما الاختلاف بين التعريفات، فيكمن في الروى والاتجاهات المتبناة من قبل الباحثين والمفكرين: ²

الاتجاه الاستراتيجي: يمثل الاتجاه الواقعي، المدرسة القيمية الإستراتيجية التي تنظر إلى الأمن كقيمة مجردة وتربطه بالحماية من التهديدات الخارجية. يركز هذا الاتجاه على اعتماد القوة العسكرية.

وجهت انتقادات لهذا الاتجاه، أهمها: هو الاهتمام بجانب واحد المتمثل في القوة العسكرية في تعزيز أمن الدولة، في ظل تعدد الظواهر الدولية، وتشابك التفاعلات بين الدول، خاصة مع ظهور تهديدات معقدة ومتشعبة.³

الاتجاه الاقتصادي: يركز أصحاب هذا الاتجاه على ثلاثة مرتكزات رئيسية:

¹ نسيم بهلول، الإطار النظري لدراسة الأمن القومي الجزائري، في فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني، تقديم: وليد عبد الحي (عمان: دار ومكتبة الحامد للنشر والتوزيع، ط. الأولى، 2015) ص 41.

² طه محمد السيد، "مفهوم الأمن القومي"، مجلة الأمن و الإستراتيجية، العدد الأول (يناير 2023) ص 116.

³ بهلول، مرجع سابق، ص 64.

ضرورة تأمين الموارد الاقتصادية، تحقيق الوظيفة الاقتصادية، ضرورة إحداث التنمية كجوهر لتحقيق الأمن القومي.¹

وعليه بحكم الطبيعة الشاملة لمفهوم الأمن الوطني، نركز في الدراسة على الاتجاه التكاملي الذي يجمع بين الاتجاه الاستراتيجي والاقتصادي، ليشمل كافة مكونات وعناصر القوة الشاملة للدولة سياسيا، اقتصاديا، اجتماعيا، عسكريا، أمنيا، ثقافيا.

على ضوء النظرية التي اعتمدتها الدراسة: نظرية الأمن الشامل، نعرف الأمن الوطني إجرائيا على أنه: منظومة شاملة تتفاعل مع المتغيرات الداخلية والخارجية، وتظهر قدرة الدولة على مواجهة التهديدات التقليدية والحديثة، عبر توظيف التكنولوجيا والذكاء الاصطناعي، بما يدعم القرار ويحمي المصالح الحيوية للدولة.

هذا التعريف يعكس الطابع الديناميكي لمفهوم الأمن الوطني الشامل، حيث التكنولوجيا أصبحت جزءا لا يتجزأ من آليات الدولة الأمنية.

2. مستويات الأمن الوطني: يرتبط بمستويات رئيسية تتمثل في :

الأمن الوطني: يركز على حماية البيئة الداخلية للدولة من الأخطار التي تهدد كيانه، ويشمل تعبئة الإمكانيات اللازمة لمواجهة تلك التحديات.

الأمن الإقليمي: يرتبط بأمن مجموعة من الدول ذات حدود مشتركة، ويعكس طبيعة العلاقات بينها سواء كانت قائمة على التعاون أو التهديد.² ويتم ذلك ضمن دائرتين:³ الدائرة المتعلقة بالدول الموجودة في نطاق إقليم معين. وأخرى تتعلق بالدول المتواجدة خارج نطاق إقليم معين.

الأمن الدولي: يمثل المستوى الأوسع، حيث يتناول شبكة من الوحدات السياسية المترابطة وفق أنماط مختلفة من التفاعل.⁴

¹ السيد، مرجع سابق، ص 116.

² عبد القادر زعيم، "الهندسة الإستراتيجية لأمن القومي الجزائري"، *المجلة العربية في العلوم الإنسانية والاجتماعية*، ع.3، م. 17 (15 جويلية 2025) ص 209.

³ علي عباس مراد، *الأمن والأمن القومي: مقاربات نظرية* (لجزائر: ابن نديم للنشر والتوزيع، الطبعة الأولى، 2017) ص ص 57، 58.

⁴ المكان نفسه .

يوضح تعدد مستويات الأمن الوطني الطبيعة التداخلية والتكاملية للعلاقات بين الدول، حيث لا يمكن فصل الأمن الداخلي عن الإقليمي والدولي، بل هي حلقات مترابطة تؤثر في بعضها البعض.

المطلب الثاني: مرتكزات الأمن الوطني الجزائري في ظل التحولات التكنولوجية

يقوم الأمن الوطني الجزائري على مجموعة من الدعامات العملية والبنائية التي ترتبط بطبيعة تكوين الدولة الجزائرية، والتي على أساسها يتم تحقيق الأمن فعليا. نظرا للطبيعة التحليلية للدراسة سنحدد لكل مرتكز الهدف الأساسي له، والمخرجات التي تضمن تحقيقها.

الجدول رقم 02: يبين المرتكزات الأساسية لأمن الوطني الجزائري في ظل التحولات التكنولوجية.

المرتكزات	الأهداف	المخرجات
المرتكز السيادي-المؤسساتي	تعزيز استقلالية وعقلانية القرار الوطني لضمان استقرار وسيادة النظام السياسي، بناء مؤسسات قوية سواء من الناحية التنظيمية أو من الناحية العملية لتكون كقوى مساندة للخطط والبرامج، المشاريع الوطنية	تحديث النصوص التشريعية بما يتلاءم مع الواقع وتعزيز آليات الحوكمة بما يضمن الشفافية والكفاءة المؤسسية.
المرتكز العسكري-الدفاعي	تأمين وحماية أراضي الوطن ووحدتها، وسلامة المواطنين من كافة التهديدات الهجينة.	الاستثمار في التقنيات التكنولوجية الجديدة في الأنظمة الأمنية والعسكرية، لتعزيز اليقظة الدفاعية، تدريب وحدات متخصصة في الأمن السيبراني
المرتكز الاقتصادي-الطاقوي	تنويع مصادر الاقتصاد، مواكبة التحول نحو اقتصاد المعرفة، تعزيز الاستخدام للموارد	دعم الصناعات المحلية، تعزيز الانتقال السلس للطاقات المتجددة مع دمج

الطاقوية.	التقنيات الحديثة مثل: الزراعة الذكية	
المرتکز الاجتماعي	الحفاظ على التماسك الجبهة الداخلية، تقليص كافة الفوارق تحسين جودة الحياة . ترسيخ وعي جمعي مدرك لإيجابيات والمخاطر التقنيات الحديثة.	تشجيع التكوين والتدريب في المجال التكنولوجي.
المرتکز السيبراني-التكنولوجي.	تعزيز الابتكار في مجال البحث العلمي، إنشاء كفاءات ومختصين في المجال الرقمي، حماية الأنظمة المعلوماتية، وتحقيق الأمن السيبراني.	تطوير البنية التحتية لشبكات للتكنولوجيا والمعلومات والاتصالات، إنشاء مراكز وطنية أمنية لمحاربة الجرائم الإلكترونية، وضع أطر تشريعية مناسبة، إشراك كافة الفاعلين.

المصدر: الجدول من إعداد الطالبة بناء على التزامات 54 للرئيس الجمهورية- بتصرف.

يشير الجدول إلى أن هذه المرتكزات هي أسس مترابطة لمفهوم الأمن الوطني الشامل، التي تتفاعل فيما بينها. فالاستقلالية المؤسسية لا تتحقق دون حماية عسكرية قوية، ولا تستمر دون قاعدة اقتصادية فعالة، وتماسك اجتماعي الذي يمثل شرطا أساسيا لنجاح أي سياسة أمنية.

مع التحولات التكنولوجية، يصبح المرتکز السيبراني- التكنولوجي بمثابة الرابط الذي يصل بين جميع المرتكزات، إذ يوفر الاستمرارية والمرونة في بيئة عالمية متغيرة.

المطلب الثالث: التهديدات الأمنية الحديثة في البيئة الجزائرية .

الحديث عن مفهوم التهديدات في السياق الجزائري يرتبط بشكل وثيق بالتطورات التي طرأت على مفهوم الأمن الوطني. ليشمل تساؤلات حول الأنماط الجديدة من التهديدات اللاتماثلية، لاسيما ما تعلق منها بالسيادة الرقمية، هذا ما سنتعرف عليه ضمن المطلب.

الجدول رقم 03: يوضح التهديدات الأمنية الحديثة في السياق الجزائري.

التهديد	لماذا يعتبر تهديدا؟	الارتباط بالبيئة والعمق الاستراتيجي الجزائري
الارهاب الإلكتروني	الإرهاب ظاهرة ديناميكية عابرة للحدود، فهو نتاج نسقي لعدم الاستقرار الإقليمي للدول. ينقسم خطره إلى شقين: ميداني يعتمد على استغلال الصدعات المجتمعية. سيبراني يوظف الفضاء الرقمي وشبكات التواصل للدعاية والتجنيد ونشر الفكر المتطرف.	الجزائر تواجه تحدي تأمين حدود شاسعة ومحاذية لبنيات اقليمية غير مستقرة: مالي وليبيا، مما يجعلها عرضة لمحاولات اختراق عبر ممرات لوجستية، فضلا عن مجابهة الأفكار الهدامة رقميا لضمان الوحدة الوطنية.
التجسس السيبراني (برنامج بيغاسوس)	تهديد غير مرئي، يستهدف السيادة المعلوماتية للدولة من خلال برمجيات اختراق متطورة مثل: (pegasus) الذي يخترق أجهزة تعمل بأنظمة تشغيل (IOS) أو (Android)، إضافة إلى اعتماده على تقنيات الهجمات خالية من النقر (zero-click)	واجهت الجزائر محاولات اختراق وتجسس سيبراني ممنهجة، استهدفت آلاف الهواتف والشخصيات الحيوية، مما يشكل تهديدا مباشرا لأمن الوطني ويفرض تبني مقاربة الدفاع السيبراني الاستباقي لحماية البيانات السيادية.
تداعيات عدم الاستقرار في مالي	تراجع البيئة الأمنية في الساحل الإفريقي بعد انسحاب مالي في يناير 2024 من اتفاق الجزائر لسلام والمصالح 2015، وتنامي استقطاب الدولي عبر فواعل غير دولية مثل مجموعة فاغنر الروسية	يمثل هذا التحول تقويضا للدور الدبلوماسي الجزائري كوسيط اقليمي، ويفرض بيئة عدائية على طول الحدود الجنوبية.
الأزمة السياسية	أحدث الانقلاب العسكري عام	بالنسبة للجزائر، يثير هذا

والجيوستراتيجية في النيجر	2023 فراغا عمق من الأزمة السياسية في النيجر، حولها إلى ساحة صراع وتنافس بين القوى الدولية الكبرى والجماعات المتמרدة المحلية	الوضع مخاوف أمنية على مستويين: الأول عسكري يتمثل في خطر تسلل العناصر الإرهابية عبر جبال الطاسيلي والهقار. الثاني مرتبط بتوسع نشاط شبكات الهجرة غير الشرعية والاتجار بالبشر.
الجريمة المنظمة	نشاط تقوده شبكات عابرة للحدود مرتبطة بجوانب خارجية تهدف إلى ضرب الاستقرار المجتمعي والاقتصادي للدول	هذا التهديد يستهدف الجزائر بشكل منهج والتي شملت تدفقات قياسية من القتل الهندي، حيث توضح مؤشرات تقرير المخدرات العالمي لعام 2024 حجم المحجوزات الضخم الذي يعكس حجم التهديد على الحدود الغربية.
الهجرة غير النظامية	تهديد اجتماعي ديمغرافي واقتصادي مرتبط بنيويا بشبكات الجريمة المنظمة العابرة للحدود، التي تشكل ضغطا على البنى التحتية والنسيج الاجتماعي للدول المستقبلية	بالنظر إلى الموقع الاستراتيجي للجزائر كبوابة شمالية نحو القارة الأوروبية، تحولت إلى وجهة للتدفقات المهاجرين، خاصة عبر المحور الجنوبي
التحالفات والمخاطر الإقليمية التطويق	أدى إلى إعادة صياغة التوازنات العسكرية والاستقرار في المنطقة، نظرا لتواجد عسكري أجنبي مباشر ذات أجناس مع الحدود الجزائرية.	يمثل هذا التحول تهديدا مباشرا للعمق الاستراتيجي والسيادة الوطنية، تزامنا مع استمرار التوترات المحيطة

بفضية الصحراء الغربية، الأمر الذي جعل الجزائر تتخذ مواقف حازمة شملت قطع العلاقات الدبلوماسية والرفع من درجة الجاهزية والردع في الجهة الغربية	الجيوستراتيجي (التطبيع المغربي- الإسرائيلي)
---	--

المصدر: من إعداد الطالبة بالاعتماد على عدة مراجع.**

يشير الجدول إلى أن الجزائر بحكم ثقلها الاستراتيجي المكتسب من موقعها الحيوي، قوة قراراتها السيادية، دورها على المستوى الإقليمي والدولي، جعلها عرضة لمختلف التهديدات الأمنية غير النمطية التي تجاوزت الطابع التقليدي إلى تهديدات قائمة على التكنولوجيات الحديثة.

* Lynda Maizi, "Regional and Internal Security challenges and Their Implications on the Algerian National Security", *Annals of Algiers University* 1, vol.39,N.3 (2025) p. 151.

* Abde Samed Bouregba and Manel Ismahan Rebbah, " Algeria's National Security Doctrine: Sovereignty, Resilience, and Regional Challenges", *Annals of Algiers University* 1, Vol.39, N.4 (2025) p. 251.

* عنتر بن مرزوق، محي الدين حرشاوي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، 15 فيفري 2025،

<https://shorturl.at/v3lcj>.

المبحث الثالث: العلاقة بين الأمن الوطني والذكاء الاصطناعي

تزايد استخدامات الذكاء الاصطناعي في المنظومة الأمنية والدفاعية في الوقت الراهن، جعل منه أداة حيوية شكلت طابع علائقي مزدوج. هذا ما سنتعرف عليه في هذا المبحث.

المطلب الأول: الذكاء الاصطناعي كمحدد جديد في المنظومة الأمنية.

أحدث انتقال الذكاء الاصطناعي من فكرة إلى التطبيق العملي، إلى إعادة هيكلة جذرية للسياسات الأمنية والتصورات الوطنية. من الناحية التحليلية نركز على النقاط التالية: ¹ **الذكاء الاصطناعي وصنع القرار الأمني:** مع التغير الذي أحدثه الذكاء الاصطناعي في مدركات الصراع، من كونه صراع قوة مادية إلى صراع خوارزميات وبيانات وسرعة القرار، هنا يبرز اتجاهين بخصوص صناعة القرار لاسيما في حالة الحرب: الأول يتمثل في سرعة الاستجابة واتخاذ القرارات لإدارة الصراعات بدقة عالية، الثانية مع الكميات الضخمة للبيانات التي يعالجها الذكاء الاصطناعي، تزيد احتمالية عدم اليقين في وضع تقديرات بخصوص نوايا وقدرات الخصم، وفي تقدير الموقف، بالشكل الذي يؤثر على عملية اتخاذ القرار برفع من احتمالية الوقوع في الخطأ ².

الذكاء الاصطناعي والسيادة الرقمية: لم يعد مفهوم السيادة يقتصر على الحدود الجغرافية، بل أصبحت تعرف بالسيادة الرقمية التي تشمل الفضاء الرقمي، الذي ساهم في بسط الهيمنة على الوسائل التكنولوجية، وصار بمثابة ساحة تنافس وصراع جديد لممارسة الردع والهجوم. ³

البيانات كأصل استراتيجي: تعد البيانات العمود الاستراتيجي للقوة الدولة، فالاستحواذ عليها وتأمينها، يعكس مدى قدرة الدول على توجيه قراراتها السيادية، وتخصيص إمكانياتها،

¹ عمار صالح العاقل سليمان، "تأثير الذكاء الاصطناعي على سياسات الأمن القومي"، *مجلة العلوم الشاملة*، م.10، ع.39 (مارس 2026) ص 3330.

² فتحي بولعراس، "محددات الأمن القومي في عصر الذكاء الاصطناعي"، *مجلة الديمقراطية*، ع.100 (أكتوبر 2025) ص 66.

³ مصطفى تاهمي، "مستقبل الأمن القومي الجزائري في ظل التطورات التكنولوجية وحروب المعلومات"، أطروحة مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه في علوم سياسية وعلاقات دولية (جامعة الجزائر 03: كلية العلوم السياسية والعلاقات الدولية، 2024/2023) ص 16، 15.

وفعالية سياساتها في تعزيز الأمن الوطني، لاسيما ما تعلق بالمسائل الأخلاقية والقانونية في استغلال تلك البيانات وتنظيم استخدامها.

التحول في بنية المؤسسات الأمنية، وذلك وفق ثلاث مدخلات: 1

1- تطوير أجهزة الأمن والاستخبارات :

يساهم الذكاء الاصطناعي في تحويل منطق الأجهزة الأمنية والاستخباراتية القائم على رد الفعل إلى منطق الاستباق الذي يتيح الرصد والتنبيه التهديدات الهجينة من خلال السرعة القدرة على الاستجابة باتخاذ قرارات عقلانية تجنب الوقوع في الأخطاء.

2- إنشاء وحدات الأمن السيبراني:

شكل التحول نحو الذكاء الاصطناعي خطوة أساسية في تطوير الهياكل الرقمية المتخصصة في الأمن السيبراني في إطار توجه شامل لترسيخ ثقافة وقائية قبل وقوع الهجمات، وذلك تماشيا مع التطورات المتلاحقة لنظم الذكاء الاصطناعي.

3- تحديث التشريعات الأمنية:

يعد تحديث الأطر القانونية خطوة محورية لضمان الاستخدام المسؤول للتقنيات الذكاء الاصطناعي، والمرونة في التكيف مع متطلبات الأمن الوطني في حماية البيانات والخصوصية المجتمعية للدول، من سوء الاستغلال التكنولوجي، وهذا من شأنه إرساء الثقة في المنظومة الأمنية وتكريس آليات الحوكمة فعالة ومستدامة.²

المطلب الثاني: الذكاء الاصطناعي بين منطق التهديد و منطق الفرص.

توظيف الذكاء الاصطناعي في الميدان الأمني طرح معادلة مزدوجة، فمن جهة يعزز قدرة الدولة على حماية مصالحها الحيوية، ومن جهة أخرى، يفتح المجال أمام مخاطر انتهاك السيادة الرقمية، وتقوض استقلالية الدولة.³

أ/ **التقنية ذات الاستخدام المزدوج (Dual-Use Technology):** يعود تركيزنا على هذا المفهوم، كونه يعطي إطارا لاعتبار الذكاء الاصطناعي ثنائي الاستخدام. ويشير المصطلح

¹ سليمان، مرجع سابق، ص ص 3330، 3331.

² المكان نفسه.

³Kenza Belhocine, Loubna Hachouf and Tahar Zouagri, "Uses of Artificial Intelligence in The Security and Military Fields: Between The Demands of Innovation and The Limits of Criminal Liability", *LEX LOCALIS- Journal of Local Self-Government*, Vol.23, No.8(2025),p. 6

إلى إمكانية استغلال الذكاء الاصطناعي مدنيا وعسكريا، ما يعيد تشكيل مشهد التحدي الأمني بشكل أساسي.

الجدول رقم 04: يوضح مقارنة بين مشهد التحدي الأمني الكلاسيكي والتحدي الأمني في ظل الذكاء الاصطناعي.

البعد	التحدي الأمني الكلاسيكي	التحدي الأمني ذي الاستخدام المزدوج
مصادر القدرات	مستقلة	متداخلة بسبب العولمة
المحفز	زيادة في القدرات العسكرية.	زيادة في القدرات التكنولوجية
أنواع اليقين	عدم التمييز ما إذا كانت القدرات تستخدم بهدف هجومي أو دفاعي	صعوبة التمييز ما إذا كانت التكنولوجيات تستخدم مدنيا أو عسكريا.
الإجراء المتبع	زيادة التسليح العسكري.	زيادة القدرات التكنولوجية عبر إجراءات جيو اقتصادية.

المصدر: الجدول من إعداد الطالبة، استنادا إلى المرجع الآتي بالتصرف:

Chun Hey, Brain Kot, " Dual-Use Security Dilemma and the U.S-china AI Technology Race", thesis submitted in partial fulfillment of the requirements for the degree of MPhil (University of Oxford, May 2025) p 20.

يتبين من الجدول، أن العلاقة بين الأمن الوطني والذكاء الاصطناعي قائمة على علاقة بنيوية مزدوجة، فتعاضد قدرة الدولة في دمج هذه التقنية، يرفع من مرونتها في حماية أنظمتها وبرامجها الأمنية. في حين ضعف بنيتها التحتية، يجعلها بيئة هشة معرضة لمختلف الهجمات السيبرانية.

ب/ التهديدات والفرص التي يطرحها الذكاء الاصطناعي:

- التهديدات:

1. التزييف العميق: تستخدم تقنيات الذكاء الاصطناعي في إنتاج محتويات مزيفة تبدو واقعية لنشر الشائعات والتأثير على الرأي العام، ضمن ما يعرف بحروب الجيل الخامس، وتعد منصات التواصل بيئة مناسبة لانتشار هذه الأخبار المضللة، نظرا لقدرتها الواسعة على تجاوز الحدود السياسية والاجتماعية.¹

¹ محمد بن نجمة، "الذكاء الاصطناعي وتحديات الأمن الوطني: مقارنة تقنية"، مجلة مصداقية، م.5، ع. 2 (2023) ص 60.

2. انتهاك خصوصيات الأفراد التلاعب الاجتماعي: تساهم خوارزميات الذكاء الاصطناعي في انتهاك خصوصية الأفراد عبر تحليل اهتماماتهم والتنبيه بسلوكهم تحت غطاء تحسين الخدمات، إضافة إلى استخدام الروبوتات في توجيه الرأي العام ونشر التطرف.¹

3. قدرة التنظيمات الإرهابية على استخدام الذكاء الاصطناعي: ويتم ذلك بتحليل بيانات المستخدمين بدقة لتحديد الأفراد المتفاعلين بشكل متكرر مع محتوى متطرف، أو من لديهم القابلية لاعتناق إيديولوجيات معينة. بعد ذلك يتم استهداف هؤلاء الأفراد برسائل مخصصة وتوجيههم تدريجياً نحو التطرف.²

4. قضية التحيز: اعتماد الذكاء الاصطناعي على البيانات التي تقدم له، والتي لا تنفصل عن معتقدات ورؤية ومنطلقات أصحابها، يكرس تحيزات موجودة في العالم الحقيقي، فالخوارزميات المستخدمة قد تكون متحيزة بطبيعتها، التي تمكن من تسلي الأخطاء لنماذج التعلم الآلي، وفي المنطق المدمج.³

5. التمييز بين الأهداف: غياب ضوابط تقنين استخدام الذكاء الاصطناعي في المجال العسكري من ناحية، واحتدام التنافس الدولي على تقنياته المختلفة من ناحية ثانية، يتولد مخاوف من فشل الروبوتات المقاتلة والأسلحة الذاتية التشغيل في استشعار الفرق بين الأهداف العسكرية والأهداف المدنية التي لا يجب المساس بها.⁴

- الفرص:

على الرغم من التحديات المرتبطة باستخدامه، فإن هناك فرصاً إستراتيجية يمكن استثمارها لتطوير قدرات الدولة في مواجهة التهديدات المعقدة والمتغيرة:⁵

1. معالجة البيانات الضخمة: تتمثل إحدى المزايا الجوهرية للذكاء الاصطناعي في قدرته على تحليل كميات هائلة من البيانات بسرعة.

¹ المكان نفسه.

² فتحي بولعراس، مرجع سابق، ص 65.

³ محمد الأمين دبار، جمال الدين بابو، تداعيات الذكاء الاصطناعي على الأمن القومي، مجلة القانون الخاص، م. 02، ع. 01 (جوان 2024) ص 104.

⁴ المرجع نفسه، ص 106.

⁵ "Institut des Sciences Stratégiques, "L'impact de l'AI sur la sécurité nationale, accessed April 30, 2026, <https://shorturl.at/7oFlg>

2. **التنبؤ بالأزمات والتهديدات:** يمكن لأنظمة المعتمدة على الذكاء الاصطناعي أن تعتمد على تحليل الاتجاهات التاريخية ورصد الأنماط السلوكية للتنبؤ بالأزمات قبل وقوعها. هذا النهج الاستباقي يساهم في تقليل المخاطر من خلال تعزيز القدرة على الاستعداد المبكر.

3. **تعزيز مرونة المؤسسات الأمنية:** يساعد الذكاء الاصطناعي في بناء منظومات أكثر مرونة في مواجهة التهديدات الناشئة، من خلال دعم عمليات المحاكاة والتخطيط الاستراتيجي، وتوفير أدوات للتكيف مع بيئات أمنية وديناميكية.¹

يظهر تحليل الدور الوظيفي لإدماج الذكاء الاصطناعي ضمن المنظومة الأمنية مسارين مختلفين، الأمر الذي جعل من هذه التكنولوجيا الحديثة هي خط الهجوم والدفاع الأول ضمن واقعا سيبرانيا معقدا.

فمن جهة يعيد تشكيل مفهوم التهديد، ليشمل هندسة الرأي العام عبر التزييف العميق والتحكم بالخوارزميات التي قد تحمل تحيزات مبرمجها، كذلك تمكين التنظيمات المتطرفة من نشر لأفكارها، إضافة إلى أتمتة الحرب بأسلحة ذاتية التشغيل ومخاطر التي قد تدفع الروبوتات لارتكاب أخطاء لعدم التمييز بين المدنيين والعسكريين. أما المسار الآخر، فيحمل فرصا واعدة إذا أحسن استغلاله والتي تكمن في قدرته الفائقة على معالجة البيانات الضخمة، والتنبؤ بالأزمات بناء على الأنماط السلوكية والتاريخية، هذا النهج الذي من شأنه أن يمنح مرونة وكفاءة دفاعية بناء على مدى دمج هذه الخوارزميات في شبكات صنع القرار الأمني.

¹Ibid.

الفصل الثاني

الهندسة الأمنية الجزائرية في ظل الذكاء الاصطناعي (2019-2026)

المبحث الأول: تكييف العقيدة الأمنية مع التحول الرقمي.

المبحث الثاني: الأطر التشريعية والمؤسسية للأمن في عصر الذكاء الاصطناعي.

المبحث الثالث: تقييم جاهزية الجزائر لتبني الذكاء الاصطناعي.

المبحث الأول: تكيف العقيدة الأمنية الجزائرية مع التحول الرقمي

يعالج هذا المبحث مسار تكيف العقيدة الأمنية الجزائرية في خضم الواقع المعقد، بتسليط الضوء على مسارين يعكسان التوجه الحديث للدولة الجزائرية كاستجابة مؤسسية واستراتيجية لمواكبة متطلبات التحول الرقمي.

المطلب الأول: الأمن السيبراني كأولوية وطنية

أعاد الذكاء الاصطناعي صياغة مفاهيم أمنية جديدة، متخطيا الحدود الجغرافية، ليجعل من الأمن السيبراني ركيزة محورية. الأمر الذي دفع الدول إلى إعادة النظر في ترتيب أولوياتها، وهيكله عقائدها الأمنية لمجابهة التحديات الناشئة في الفضاء السيبراني. لقد سعت الجزائر على غرار العديد من الدول، لتكييف تصوراتها الأمنية للتوافق مع مقتضيات الوضع التكنولوجي الراهن، وذلك وفق ثلاث مراحل رئيسية:

مرحلة صياغة الرؤية: ركزت فيها الجزائر على تحديد الدوافع السيادية لتبني الأمن السيبراني، بداية بالمنحى التصاعدي في معادلات الجريمة السيبرانية. والتي أصبحت تمثل التهديد الأبرز في الجزائر. ففي سياق متصل، وفقا لإحصائيات كاسبرسكي، تم تسجيل 140,000 هجوم سيبراني يوميا في جانفي 2024.¹

الشكل رقم 01 : يبين إحصائيات حول التهديدات التي تم اكتشافها ضد مستخدمي الكمبيوتر في الجزائر خلال شهري افريل وماي 2024.



المصدر: EL Hirsti and Abderrahmane, *loc. cit.*

¹Hayet Sereir EL Hirsti and Abderrahmane, "Cybersecurity as a Fundamental Element of The Digital Economy in Algeria", *Abaad Iktissadia Review*, 14, no. 1 (2024), p. 382.

يمكن إرجاع الارتفاع في مستوى الهجمات، من جهة إلى تواجد بيئة رقمية هشة أتاحت لاستغلال الثغرات في الجوانب التشريعية، ما فتح المجال لجرائم المساس بأشخاص والابتزاز. ومن جهة أخرى، اعتبار الجزائر هدفا استراتيجي ضمن حروب الجيل الخامس التي استهدفت البنى التحتية والمنظومات السيادية. وعليه، قد ترجمت الجزائر توجهاتها، من خلال مفهوم الأمن الشامل ككل غير متجزئ، بإدراج الأمن السيبراني كبعد جيواستراتيجي مكمل لمختلف أبعاد الأمن الوطني(الداخلي، الاقتصادي، الاجتماعي، الفكري والثقافي)، هنا يكمن الهدف الجوهرى في حماية المصالح الحيوية للدولة في سياق حروب الجيل الجديد.¹ وفيما يخص المقاربة: انتهجت الدولة الجزائرية المقاربة الشاملة لتحقيق التنسيق الوظيفي بين مختلف مؤسسات الدولة لضمان أمن الفضاء السيبراني الوطني.²

فاستناد لنظرية الأمانة التي اعتمدت عليها الدراسة، تم إضفاء في هذه المرحلة الطابع الوجودي للتهديدات السيبرانية.

2. مرحلة الإدراك الاستراتيجي: جسدت الترجمة الفعلية للتصورات أعلى المستوى الحكومي، تتميز هذه المرحلة بتحول جذري في الخطاب الرسمي لصناع القرار بزيادة الإدراك أن الفضاء السيبراني هو ساحة صراع دولي لا مفر منه. وتجسد هذا التحول في المستويات التالية:

أولاً: مستوى القيادة العليا للبلاد (رئيس الجمهورية): التأكيد على أن الرصد والجاهزية الاستباقية للتهديدات السيبرانية هما شرطان أساسيان لحماية المنشآت والمصالح الحيوية للبلاد.³

ثانياً على المستوى العسكري: اعتبار الأمن السيبراني ضرورة حتمية للدفاع عن الأنظمة الحساسة للدولة مع التركيز على منطق الوقاية والردع.⁴

¹ "الافتتاحية: الأمن لا يقبل التجزئة"، مجلة الجيش الوطني الشعبي، العدد 719 (جوان 2023) ص 1.

² فضيل شريف، "الإستراتيجية الوطنية للأمن السيبراني"، ترجمة: أ.لحمل، مجلة الجيش، العدد 715 (فيفري 2023) ص ص 47، 48.

³ ن. بوكراع، "من أجل جزائر صامدة سيبرانيا"، مجلة الجيش، ع. 719 (جوان 2023) ص 8.

⁴ المرجع نفسه، 9.

3. مرحلة التجسيد الفعلي لإستراتيجية الدفاع السيبراني: تمثل هذه المرحلة المأسسة الفعلية لأمن السيبراني عبر هيكله القوى الدفاعية للدولة، وبناء القدرات لاستجابة الفورية، والإدارة المستمرة للمخاطر. وفق هندسة ثلاثية قائمة على:

الرصد والاستباق: بإنشاء مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، في نوفمبر 2015 التابعة لدائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي. مهمتها تتمثل في: التخطيط الاستراتيجي ومتابعة تجسيد السياسة الشاملة للدفاع السيبراني ضد التهديدات السيبرانية المستهدفة لأنظمة المعلومات.¹

إنشاء المركز الوطني للإشارة والحروب الإلكترونية سنة 2019، وهو تابع لدائرة الإشارة و أنظمة المعلومات والحرب لإلكترونية بوزارة الدفاع الوطني.²

الإعلان عن صدور الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029، في نسختها الأولى يوم 3 مارس 2026، التي تعد بمثابة إطار شامل لضمان المرونة السيبرانية الوطنية وحماية البنية التحتية الرقمية للدولة وبياناتها، وحماية المواطنين.³

الردع القانوني: باستحداث قطب جزائي مكلف بالجرائم السيبرانية في شهر أوت 2021، وهو ما يعكس الأهمية التي توليها السلطات العمومية للتكيف مع طبيعة التهديدات العابرة للحدود ومكافحة الأنماط غير التقليدية للجريمة.⁴

الاستثمار في المورد البشري: من خلال إنشاء المدرسة الوطنية العليا لأمن السيبراني بموجب مرسوم رقم 24-181 في 5 يونيو 2024، وتتولى مهمة ضمان تكوين مهندسين وحاملي شهادة دكتوراه ذوي كفاءات علمية وتقنية ذات مستوى عال، المساهمة في المجهود

¹ سلمة بورباح، "السياسة العامة الجزائرية في مجال السيبرانية: الواقع والتحديات"، *مجلة دفاتر السياسة والقانون*، م. 15، ع. 1 (2023)، ص 282.

² المكان نفسه.

³ "وكالة أمن الأنظمة المعلوماتية: عرض الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029"، *مجلة الجيش*، ع. 752 (مارس 2026)، ص 17.

⁴ شريف، مرجع سابق، ص 47.

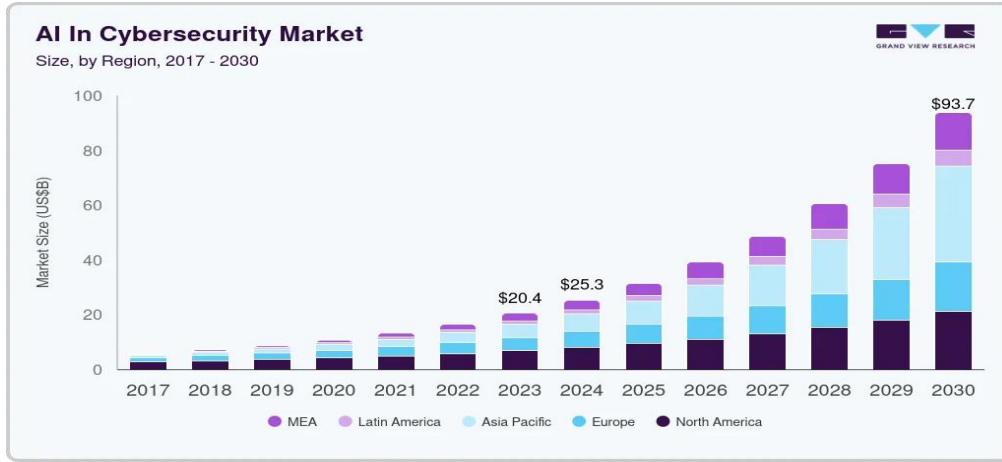
الفصل الثاني

الوطني للبحث العلمي والتطوير التكنولوجي في مجال أمن الأنظمة المعلوماتية، تعزيز تطوير العلوم والتقنيات في مجال الأمن السيبراني.¹

المطلب الثاني: الذكاء الاصطناعي كرهان استراتيجي للدولة الجزائرية

استنادا إلى نظريات الدراسة الأمن الشامل ونظرية الأمانة، لم يعد الأمن السيبراني مجرد تقنية، بل أصبح قضية سيادية مركزية تتصدر اهتمامات الحكومات والشركات والمجتمعات.² وهذا ما يتضح في الشكل الآتي:

الشكل رقم 02: يبين تطور الذكاء الاصطناعي في سوق الأمن السيبراني



المصدر: <https://shorturl.at/HjtxD>

يشير الارتفاع المتزايد لاعتماد الذكاء الاصطناعي في مجال الأمن السيبراني، بنحو 25.3 مليار دولار أمريكي عام 2024، مقارنة بعام 2023 بقيمة 20.4 مليار دولار أمريكي، ومن المتوقع أن يصل إلى 93.75 مليار دولار أمريكي بحلول عام 2030، بنمو سنوي مركب قدره 24.4% من عام 2025 إلى 2030.³

يعكس هذا التنافس التكنولوجي، فهما للطبيعة الحروب المستقبلية، الذي يستوجب على الدول تطوير الأنظمة الدفاعية والهجومية. الأمر الذي وسع دوائر التسليح بين القوى

¹ مرسوم رئاسي رقم 24-181 مؤرخ في 28 ذي القعدة عام 1445 الموافق 5 يونيو سنة 2024، يتضمن إنشاء مدرسة وطنية عليا في الأمن السيبراني، الجريدة الرسمية للجمهورية الجزائرية، ع. 39، ص 6.

² Global Cybersecurity Outlook 2026: Insight Report January 2026(World Economic Forum, 2026), p.9.

³"AI in Cybersecurity Market (2025-2030)", accessed May 01,2026, <https://shorturl.at/HjtxD>

الفصل الثاني

الكبرى، مثل الولايات المتحدة والصين وروسيا، إلى تسخير الإمكانيات لإعادة صياغة استراتيجية الحروب وآليات الردع .

لكن الاعتماد على تقنية الذكاء الاصطناعي، في ظل تواجد قوى تتحكم وتستحوذ عليه. يجعل الدول مثل: الجزائر تواجه إشكاليات بنيوية مركبة عند هندسته ضمن منظومتها الوطنية. وبالتالي وفقا لنظرية الأمن الشامل، لا يمكن حصر الرهانات المطروحة في العقيدة الأمنية الجزائرية في البعد التقني، بل تمتد لتشكل تهديدا سياديا مركبا:¹

السيادة التكنولوجية:

تشكل الاستقلالية التكنولوجية طرعا محوريا في الجزائر، خاصة مع تزايد الاعتماد على الذكاء الاصطناعي ضمن طبيعة تنافسية معقدة، الأمر الذي كرس لنمط جديد من التبعية القائمة على اكتساب التقنيات الحديثة. وهو ما ينعكس سلبا على استقلالية عملية اتخاذ القرار، لاسيما في إدارة البيانات الحساسة. ومن هذا المنطلق، تبرز الحاجة الملحة لصياغة رؤية سياسية متكاملة تركز على الاستثمار والابتكار لبناء قدرات محلية .²

الردع الإقليمي: يعد تأمين الأمن والحماية للسيادة الوطنية مبدأ أساسيا في العقيدة الأمنية الجزائرية. فالجزائر بحكم ثقلها الإقليمي وموقعها الإستراتيجي تسعى جاهدة لمواجهة كافة التهديدات التي تمس باستقرارها، فمع دمج الذكاء الاصطناعي أصبح مفهوم الردع أكثر ديناميكية يستند على الرصد الاستباقي والاستجابة السريعة.³

التكيف الثقافي:

من بين الإشكاليات التي يطرحها الذكاء الاصطناعي هي مسألة الهوية الثقافية، كونه هو مصدر ومورد لثقافة مكتسبة من توجهات غربية للمنطق، الكفاءة والسيطرة القائمة على

¹ Tewfik Hamel, *Impact de l'intelligence artificielle sur la doctrine militaire : le cas de l'Algerie. Modernisation continue sans rupture*(Rosa Luxemburg Stiftung, 7 octobre 2025), accessed May 03, 2026, <https://shorturl.at/RpyLv>.

² عبد الرحمان هادف، "الذكاء الاصطناعي في الجزائر: رهان السيادة في زمن الثورة التكنولوجية"، *الأخبار التلفزيون*، 16 ديسمبر 2025، تاريخ الدخول 12 مارس 2026، <https://shorturl.at/UeRO>

³ Hamel, *op.cit.*

البيانات، الأمر الذي شكل اصطدام بين الأنساق الثقافية المختلفة في ظل تعدد وتنوع المجتمعات، وبين منطق خوارزمي مبرمج.¹

وهنا يكمن التحدي بالنسبة للجزائر في إدخال الذكاء الاصطناعي في العقيدة الأمنية دون المساس بالقيم الأساسية للدولة الجزائرية. فالخوارزميات ليست محايدة بل تحمل في طياتها قيم وتوجهات مصمميها.

¹ هادف، مرجع سابق.

المبحث الثاني: الأطر التشريعية والمؤسسية للأمن في عصر الذكاء الاصطناعي.

نستعرض في هذا المبحث الإطار القانوني والمؤسسي للأمن، إلى جانب السياسات المنتهجة، ضمن رؤية طموحة وواضحة لإرساء معالم الذكاء الاصطناعي بشكل يعزز الأمن الوطني الجزائري.

المطلب الأول: الإطار التشريعي للأمن السيبراني.

تتبنى الدولة الجزائرية مقاربة تشريعية متكاملة تستهدف تحصين الفضاء السيبراني وتكريس السيادة الرقمية، وذلك عبر منظومة قانونية توازن بين متطلبات الالتزام بالمعايير الدولية والحفاظ على المصالح العليا للدولة. لإعداد الأرضية لتعزيز الأمن السيبراني في الجزائر نذكرها على النحو الآتي:¹

-قانون العقوبات رقم 66-156 المؤرخ في 8 يونيو 1966(كما عدل لاحقا): يعد النواة الأولية لمكافحة الجرائم السيبرانية، حيث يجرم أفعالا مثل القرصنة، والوصول غير المشروع إلى البيانات، سرقة الهوية، والاحتياز عبر الأنظمة الرقمية .

-القانون رقم 09-04 المؤرخ في 5 أغسطس 2009: الذي وضع إطار وقائي للتعامل مع الجرائم المعلوماتية، عبر إدخال تعريفات جديدة، وتحديد ميكانيزمات خاصة بما يسمح يقظة أكبر لمعالجة الجرائم.²

-القانون رقم 15-04 المؤرخ في 1 فبراير 2015: فتح المجال لمبدأ الثقة من خلال تنظيم التوقيع والتصديق الإلكترونيين، ومنح الطابع القانوني الإثباتي بما يضمن سلامة التعاملات الإلكترونية.

-القانون رقم 18-04 المؤرخ في 10 مايو 2018: الذي كرس قواعد لضبط قطاع الاتصالات، التي توازن بين مبدأ السيادة الوطنية وحماية البنية التحتية لاتصالات.

¹Salah Ghechir, "Digital Sovereignty and Cyber security: Legal and Strategic Implications for Algeria," *Herodotus' Journal of Human and Social Sciences*, Vol. 9, No .5 (2025) pp364,365.

² Ibid.

-القانون رقم 07-18 المؤرخ في 10 يونيو 2018 (دخل حيز التنفيذ في 10 أغسطس 2023): يكرس حماية الأشخاص الطبيعيين في معالجة البيانات الشخصية، ويستند إلى معايير دولية مثل: (GDPR) اللائحة الأوروبية العامة لحماية البيانات مع التركيز على ضمان الرقابة الوطنية. كما أنشأ السلطة الوطنية لحماية البيانات الشخصية المخولة بإصدار التراخيص، ومعالجة الشكاوى، إجراء التحقيقات، وضمان امتثال الهيئات العامة والخاصة.¹

أكدت مختلف هذه التشريعات مدى اهتمام الجزائر بتنظيم فضاءها السيبراني، بداية بتحديد الجرائم السيبرانية والعقوبات المترتبة عنها، وتنظيم الخدمات الرقمية المتعلقة بشبكة الاتصالات، وخصوصية البيانات تعزيزا لرقابة قانونية بما يضمن الثقة لدى المستخدمين وحماية المصالح الوطنية.

تطور الجوانب التشريعية ذات العلاقة بالأمن السيبراني:

مع التحولات المتسارعة، اتجهت الجزائر إلى تطوير التشريعات، نظرا لتغير في المعطيات على المستوى العالمي خاصة مع تزايد استخدام تقنيات الذكاء الاصطناعي، وتشمل:²

الحماية الدستورية: قد قدم الدستور الجزائر المعتمد في نوفمبر 2020 بعض الحقوق لحماية سرية المعلومات والمراسلات والاتصالات الخاصة، من خلال المادة 47 التي نصت على:

لكل شخص حق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى و الثانية إلا بأمر معلن في السلطة القضائية.

كما نصت ذات المادة على حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. ويعاقب القانون على كل انتهاك لهذه الحقوق.³

¹ Ibid.

² عبد الرزاق لعريوي، "متطلبات حوكمة الذكاء الاصطناعي في الجزائر-الواقع والمأمول"، مجلة اقتصاد المال والأعمال، م. 9، ع. 2 (أكتوبر 2024)، ص 234.

³ دستور 2020، الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية للجمهورية الجزائرية، ع. 82، 15 جمادى الأولى عام 1442هـ، الموافق 30 ديسمبر سنة 2020، ص 13.

الجوانب التشريعية المتعلقة بالخدمات الإلكترونية: المرسوم التنفيذي رقم 21-44 المؤرخ في 17 جانفي 2021 الذي يحدد نظام الاستغلال المطبق على كل أنواع الشبكات المفتوحة للجمهور وعلى مختلف خدمات الاتصالات الإلكترونية.

- مرسوم تنفيذي رقم 22-39 ماضي في 10 يناير 2022، يحدد شروط منح الترخيص العام لإنشاء واستغلال وتوفير خدمات الاتصالات الإلكترونية للجمهور، وقد عدل لاحقا بالمرسوم التنفيذي رقم 22-369 ماضي في 27 أكتوبر 2022.¹

- قرار ماضي في 27 يوليو 2022، الجريدة الرسمية عدد 66 المؤرخ في 02 أكتوبر 2022، الذي يحدد دفاتر الشروط النموذجية المتعلقة بخدمات الاتصالات الإلكترونية للجمهور الخاضعة لنظام الترخيص العام.²

- قانون رقم 26-02 مؤرخ في 29 شعبان عام 1447 الموافق 17 فبراير سنة 2026: الذي يهدف إلى تحديد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني.

التشريعات المتعلقة بتنظيم الهياكل الرقمية:

- مرسوم رئاسي رقم 23-314 ماضي في 06 سبتمبر 2023، يتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها. معدل بالمرسوم الرئاسي رقم 24-63 ماضي في 01 فبراير 2024.

- مرسوم رئاسي رقم 24-64 ماضي في 03 فبراير 2024، يحدد التنظيم الداخلي للمحافظة السامية للرقمنة.

- مرسوم رئاسي رقم 24-181 مؤرخ في 28 ذي القعدة عام 1445 الموافق 5 يونيو سنة 2024، يتضمن إنشاء مدرسة وطنية عليا في الأمن السيبراني.³

التشريعات المتعلقة بحماية البيانات والخصوصية: إلى جانب القانونين رقم 09-04، 15-04 الذي سبق الإشارة إليهما، تم إصدار المرسوم التنفيذي رقم 19-271 المؤرخ في 7 أكتوبر 2019، المتعلق بالمرجع الوطني لتوافقية الأنظمة المعلوماتية.

¹ لعريوي، مرجع سابق، ص 235.

² المكان نفسه.

³ مرسوم رئاسي رقم 24-181، مرجع سابق، ص 5.

- المرسوم الرئاسي رقم 05-20 المؤرخ في 20 يناير 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.
- الأمر رقم 09-21 المؤرخ في 8 يونيو 2021 والمتعلق بحماية المعلومات والوثائق الإدارية.¹
- المرسوم الرئاسي رقم 350-25 المؤرخ في 30 ديسمبر 2025، الذي أنشأ المنظومة الوطنية لحوكمة البيانات، التي تضمن وضوح القواعد واستقرار التشريعات، وحماية المعطيات، بما يعزز ثقة الفاعلين الاقتصاديين والمستثمرين الوطنيين والدوليين بتحسين الولوج إلى بيانات موثوقة وقابلة للاستغلال.²
- قانون رقم 11-25 لسنة 2025: الذي يهدف إلى تعديل وتتميم القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.³
- مرسوم رئاسي رقم 07-26 مؤرخ في 18 رجب عام 1447 الموافق 7 جانفي سنة 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره.⁴
- تعكس هذه التطورات التشريعية الحاجة إلى بناء إطار قانوني شامل، لاسيما مع غياب قوانين خاصة تحدد وتنظم استخدام الذكاء الاصطناعي، ما يشكل فجوة أخلاقية وتشريعية.
- المطلب الثاني: الإطار المؤسسي للأمن الوطني.**

¹ المكان نفسه.

² كلمة الوزير الأول خلال إشرافه على وضع المنظومة الوطنية لحوكمة البيانات حيز الخدمة"، مصالح الوزير الأول، 09 فبراير 2026، <https://shorturl.at/RWUVK>

³ قانون رقم 11-25 مؤرخ في 28 محرم عام 1447 الموافق 24 يوليو سنة 2025، يعدل ويتم القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، ع. 48، ص 15.

⁴ مرسوم رئاسي رقم 07-26 مؤرخ في 18 رجب 1447 الموافق 7 جانفي سنة 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية للجمهورية الجزائرية، ع. 4، ص 21.

تجسيدا لإدراك الدولة الجزائرية للتهديدات السيبرانية، واستنادا لمقاربة حوكمة الأمن، عملت السلطات على تطوير منظومة وطنية لأمن السيبراني من خلال استحداث وتفعيل شبكة مؤسساتية متخصصة، يمكن ذكرها كالآتي:¹

رئيس الجمهورية: هو أعلى هرم السلطة، وتعد وظيفة ضمان الأمن من صلاحياته وهذا ما أوضحه الدستور الجزائري لسنة 2022، فحسب المادة 84: يجسد رئيس الجمهورية، رئيس الدولة، وحدة الأمة، ويسهر في كل الظروف على وحدة التراب الوطني والسيادة الوطنية.

ضف إلى ذلك ما نصت عليه المادة 91 من الدستور: يضطلع رئيس الجمهورية، بالإضافة إلى السلطات التي تخولها إياه صراحة أحكام أخرى في الدستور، بالسلطات والصلاحيات الآتية:

القائد الأعلى للقوات المسلحة للجمهورية، ويتولى مسؤولية الدفاع الوطني. كما يقرر إرسال وحدات من الجيش الوطني الشعبي إلى خارج الوطن بعد مصادقة البرلمان بأغلبية ثلثي (3/2) أعضاء كل غرفة من غرفتي البرلمان.²

المجلس الأعلى للأمن: يعد هيئة استشارية عليا حسب ما نص عليه دستور 2020 في المادة 208: يرأس رئيس الجمهورية المجلس الأعلى للأمن، ويقدم المجلس الأعلى للأمن لرئيس الجمهورية آراء في المسائل المتعلقة بالأمن الوطني، يحدد رئيس الجمهورية كفاءات تنظيم المجلس الأعلى للأمن وسيره.³

وزارة الدفاع الوطني: تضطلع بدور مركزي وقيادي في جهود الأمن السيبراني الوطنية. وتشرف على هيئات تقنية عليا رئيسية، تتمثل في:

المجلس الوطني لأمن الأنظمة المعلوماتية: أنشئ بموجب المرسوم الرئاسي 05-20، برئاسة وزير الدفاع الوطني أو ممثله. ويضم في تشكيلته ممثلين عن رئاسة الجمهورية،

¹ سفيان ملوكي، عمر جيلالي، "السياسة العامة الأمنية في ضوء التحديات السيبرانية المعاصرة"، مجلة الفكر القانوني والسياسي، م. التاسع، ع. الثاني (2025)، ص 218.

² دستور 2020، الجريدة الرسمية للجمهورية الجزائرية، ع. 82، 15 جمادى الأولى عام 1442هـ، الموافق 30 ديسمبر سنة 2020، ص ص 22-20.

³ المرجع نفسه، ص 44.

الفصل الثاني

والوزير الأول والوزارات الرئيسية الخارجية، والداخلية، العدل والمالية والطاقة، الاتصالات والتعليم العالي.

يختص المجلس: بإقرار الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والإشراف على مخطط عمل الوكالة الوطنية، وتقارير نشاطها والموافقة على اتفاقية التعاون الدولي، وإقرار سياسات التصديق الإلكتروني، وتصنيف الأنظمة المعلوماتية، واقتراح تكييف الأطر الهيكلية والتنظيمية، وإبداء الرأي الملزم في المشاريع القوانين ذات الصلة.¹

الوكالة الوطنية لأمن الأنظمة المعلوماتية (ANSSI Algérie): أنشئت بمقتضى مرسوم رئاسي رقم 05-20، وهي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية، مقرها في مدينة الجزائر. تكمن مهامها في:

تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، العمل على تنسيقها وتنفيذها، اقتراح كفاءات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية، إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية، متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية، وضمان اليقظة التكنولوجية.²

الدرك الوطني: يشارك الدرك الوطني في مهمة الدفاع الوطني طبقا للخطة المقررة من قبل وزير الدفاع الوطني وفي محاربة الإرهاب،³ يضم وحدتين متخصصتين:

مركز الوقاية من جرائم الإعلام الآلي: أنشئ عام 2008، يركز على تحليل بيانات الجرائم المعلوماتية، وتحديد هوية مرتكبيها، وتأمين الأنظمة المعلوماتية، كما يقوم بحملات توعية.

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 الضارة.⁴

المديرية العامة للأمن الوطني (DGSN) تضم:

¹ ملوكي، جيلالي، مرجع سابق، ص 219.

² مرسوم رئاسي رقم 05-20 مؤرخ في 24 جمادى الأولى عام 1441هـ، الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، ع. 64، ص 7.

³ وزارة الدفاع الوطني، "الدرك الوطني: التنظيم و المهام"، تاريخ الدخول 14 مارس 2026، <https://shorturl.at/bCcaQ>

⁴ المرجع نفسه.

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

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (ONPLITIC): أنشئت بموجب المرسوم الرئاسي 15-261، وكان قد نص على إنشائها سابقا القانون 04-09. وهي سلطة إدارية مستقلة لدى وزير العدل، من المهام الرئيسية اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، تنشيط وتنسيق عمليات الوقاية، ومساعدة السلطات القضائية، ومصالح الشرطة القضائية في مكافحة هذه الجرائم، إجراء مراقبة وقائية للاتصالات الإلكترونية لكشف الجرائم المتعلقة بالإرهاب، التخريب والمساس بأمن الدولة.¹

يعكس هذا التحول ما تشير إليه أدبيات حوكمة الأمن، حيث لم يعد الأمن نتاجا حصريا للمؤسسة العسكرية، بل نتيجة تفاعل منظومات قانونية وتكنولوجية ومؤسسية.

المطلب الثالث: السياسات الوطنية في مجال الذكاء الاصطناعي.

في إطار تحديث عقيدتها الدفاعية والأمنية، كثفت الجزائر جهودها لتدعيم أمنها الوطني في الفضاء السيبراني. وهذا ما سنتطرق له في هذا المطلب.

مركز الذكاء الاصطناعي (SKAILAB) يعد أول مركز وطني للذكاء الاصطناعي في الجزائر تم إنشائه بجامعة أوت 1955 بولاية سكيكدة ، وانطلق في فيفري 2020 بتكوين طلبة في الماستر والدكتوراه، بالتنسيق مع (INTEL) الشركة الأمريكية.² يضطلع بتقديم حلول للقطاعات الاقتصادية والصناعية، وفق منطق تعاوني قائم على بناء شراكات، وتكوين قدرات وطنية في مجال جمع ومعالجة البيانات وتطوير نماذج للذكاء الاصطناعي.³

المدرسة الوطنية العليا للذكاء الاصطناعي (ENSIA):

¹ سمير قلاع الضروس، "الأمن السيبراني الوطني: قراءة في أهم الإستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر"، مجلة الرواق للدراسات الاجتماعية والإنسانية، م. 8، ع. 2 (2022)، ص 260.

² "مخبر الذكاء الاصطناعي (جامعة 20 أوت 1955 - سكيكدة) SKAILAB"، الصفحة الرسمية لجامعة 20 أوت 1955 سكيكدة، فيسبوك، تاريخ الدخول 20 مارس 2026،

<https://shorturl.at/P2I1>

³Mohamed Fayza Sari, "Artificial Intelligence in Algeria: A Diagnostic Assessment," *Journal of Law, Society and Authority*, Vol.14, No.2 (September 2025), p. 111.

أنشئت عام 2021، بموجب مرسوم رئاسي رقم 21-323، تهتم بتكوين وتدريب كفاءات عالية في الذكاء الاصطناعي وعلوم البيانات، تعني بتقديم قيمة مضافة للمنظومة التقنية الوطنية، لضمان الاستقلالية الرقمية.¹

المدرسة العليا للرياضيات (ENSM):

تأسست في 12 أكتوبر 2021، هدفها يكمن في تكوين مهندسين متخصصين في الرياضيات، وفي مجالات: النمذجة والمحاكاة، الإحصاء والتشفير والأمن السيبراني، وتضم أكثر من 700 طالب.²

المجلس العلمي للذكاء الاصطناعي:

تم إنشائه بموجب قرار مشترك بين وزارتي التعليم العالي والبحث العلمي، واقتصاد المعرفة والمؤسسات الناشئة والمؤسسات المصغرة. يناط بمهمة وضع الخطط الإستراتيجية القطاعية من خلال:³

تهيئة بيئة تقنية وقانونية متكاملة، تضمن دمج الذكاء الاصطناعي في مختلف القطاعات، وضع مخططات تعليمية متخصصة، وتحديد محتوى وعروض التكوين، بالإضافة إلى تعيين مراكز التدريب المؤهلة. بحث فرص التعاون العالمي وتوظيفها لخدمة مؤسسات البحث العلمي والمجتمع الاقتصادي.⁴

الإستراتيجية الوطنية للذكاء الاصطناعي:

تعد خطة وطنية شاملة، في مجال البحث والابتكار في الذكاء الاصطناعي. صيغت بمساهمة 150 خبير. وترتكز وفق رؤية استشرافية (2020-2030) على الاستثمار في المورد البشري، من خلال التعليم والتدريب لتشجيع توظيف الذكاء الاصطناعي في القطاعات الحيوية.⁵ قد أفردنا فصلا كاملا من هذه الدراسة لهذه الإستراتيجية بشكل مفصل.

¹ أحمد دقعة، أحمد حنيش، "استخدام التقنيات الحديثة للذكاء الاصطناعي في الدول العربية (دراسة حالة الجزائر)" مجلة الدراسات الاقتصادية والمالية، م. 17 (ديسمبر 2024)، ص243.

² "المدرسة الوطنية العليا في الرياضيات، معلومات عن المدرسة ENSM"، <https://shorturl.at/cN4AE>

³ "المجلس العلمي للذكاء الاصطناعي"، المدرسة الوطنية العليا للذكاء الاصطناعي ENSIA، 27 يونيو 2023، تاريخ الدخول 30 مارس 2026، <https://shorturl.at/COeGP>

⁴ المرجع نفسه.

⁵ سمير بركات، "تقييم جاهزية الذكاء الاصطناعي في ضوء المؤشرات العالمية- مؤشر جاهزية الحكومات للذكاء الاصطناعي نموذجا"، مجلة الدراسات الاقتصادية المعاصرة، م. 9، ع. 2 (2024)، ص218.

الصندوق الاستثماري المخصص للذكاء الاصطناعي:

خصّصت الجزائر صندوقا استثماريا بقيمة 1.5 مليار دينار جزائري عبر مجمع اتصالات الجزائر. لدعم المشاريع المبتكرة في مجالات الذكاء الاصطناعي، الأمن السيبراني، والروبوتات.

يعد هذا الصندوق خطوة مهمة لتمكين المؤسسات الناشئة من تطوير تقنيات محلية، والمساهمة ب 7% من الناتج المحلي الإجمالي الجزائري بحلول عام 2027، الوصول إلى عتبة 20.000 وحدة.¹

مراكز تطوير المهارات (Skills Centers):

تتماشياً مع متطلبات عصر الذكاء الاصطناعي، توجه قطاع البريد والمواصلات السلكية واللاسلكية من أجل تطوير المهارات إلى توفير برامج تدريبية قصيرة المدى، في التقنيات الحديثة. وتأتي هذه المبادرة لتحويل البحوث العلمية إلى حلول تكنولوجية تلبي احتياجات السوق المحلية والإقليمية.²

شبكات الجيل الخامس (5G):

تعتبر تحولاً نوعياً في البنية التحتية الرقمية، والتي تتماشى والأولوية الوطنية للذكاء الاصطناعي، بتبني إنترنت الأشياء والحوسبة السحابية في مجالات الصحة، والتعليم، والتنقل الذكي. فمن المتوقع أن يتم رفع مساهمة الشبكة في الناتج المحلي إلى 13 مليار دولار بحلول عام 2030، من خلال خلق القيمة المضافة وجذب الاستثمارات المباشرة.³

الشراكة بين اتصالات الجزائر وشركة هواوي:

¹ السيد الوزير يشرف على افتتاح فعاليات الطبعة الثالثة لمندى تكنولوجيات الإعلام والاتصال (CTO FORUM ALGERIA)، وزارة البريد والمواصلات السلكية واللاسلكية، 19 فبراير 2025، تاريخ الدخول 14 مارس 2026، <https://shorturl.at/ISMfY>

² السيد الوزير يشرف على تدشين أول مركز للمهارات (SKILLS CENTER) للتكوين المجاني قصير المدى في التكنولوجيات المتقدمة، وزارة البريد والمواصلات السلكية واللاسلكية، 23 فبراير 2025، تاريخ الدخول 14 مارس 2026، <https://shorturl.at/L9gBB>

³ اتصالات: إطلاق شبكة الجيل الخامس رسمياً في الجزائر"، الموقع الرسمي للتلفزيون الجزائري، 4 ديسمبر 2025، تاريخ الدخول 14 مارس 2026،

الفصل الثاني

تمثل إطار تعاوني بين اتصالات الجزائر وشركة هواوي، لتوسيع شبكة نقل بصرية بسعة 400 جيجابت في الثانية. والتي صممت لاستيعاب تطبيقات الذكاء الاصطناعي وانترنت الأشياء (IoT). وفي إطار رؤيتها الإستراتيجية 2024-2028، تهدف اتصالات الجزائر إلى تنويع الخدمات الرقمية، مع تفعيل شراكة تقنية مع شركة جازي لإطلاق منصات مدمجة مثل Twinbox المخصصة للتعليم الإلكتروني.¹

المفارقة أن الاعتماد على الشراكات في مجال التقنيات الحديثة يساعد على نقل الخبرات، في حين اقتناء برمجيات جاهزة يشكل تهديد يمس بخصوصية وأمن المعلومات الوطنية من خطر التجسس والقرصنة.

التعاون الإفريقي في التحول الرقمي و الذكاء الاصطناعي:

تبنت الجزائر سياسة واضحة خلال مؤتمر الشركات الناشئة الإفريقية المنعقدة في ديسمبر 2024، القائمة على فرص تعاون إفريقية ذو توجه استراتيجي لتعزيز مكانة الجزائر على المستوى القاري. والتي تركز على تبادل الخبرات وتطوير قدرات رقمية مشتركة.²

¹Lazhari Zouaoud, "Assessing the Reality of Algeria's Digital Transformation Strategy: Achievements and Prospects", *Journal of Management and Economic Sciences Prospects*, Vol. 9, No. 1(2025), p. 434.

²Ibid., p.435.

المبحث الثالث: تقييم جاهزية الجزائر لتبني الذكاء الاصطناعي

للتعرف على مدى جاهزية الجزائر في مجال الذكاء الاصطناعي، وكذا فعالية السياسات التي انتهجتها الدولة سيتم الاعتماد على مؤشر جاهزية الحكومات في الذكاء الاصطناعي*، لتقييم مبادراتها في تبني التكنولوجيات الحديثة الداعمة لأمنها الوطني. لكون أن هذا المؤشر يحتوي على ثلاث ركائز: الحكومة، قطاع التكنولوجيا، البيانات والبنية التحتية، وهذا ما سنركز عليه خلال هذا المبحث.

المطلب الأول: جاهزية الحكومة

تتمحور ركيزة الحكومة حول وجود رؤية واضحة لتطوير وحوكمة الذكاء الاصطناعي، مع مراعاة الضوابط التنظيمية والمعايير الأخلاقية. والتي تتطلب قدرات رقمية مؤسسية، تشمل الكوادر البشرية والمنظومات الإجرائية التي تضمن مرونة الحكومة في استيعاب التقنيات الناشئة¹.

جدول رقم 05: يبين جاهزية ركيزة الحكومة للجزائر خلال الفترة (2021-2024).

السنوات	2021	2022	2023	2024
قيمة المؤشر	32.96	30.17	30.10	31.68
الترتيب العالمي	99	111	120	107

المصدر: من إعداد الطالبة، بتصرف بالاعتماد على: صبرين بوعزة، هدى بصاشي، انعكاسات تطبيق الذكاء الاصطناعي كثورة صناعية رابعة على اقتصاديات الدول-مؤشرات الجاهزية الحكومية للذكاء الاصطناعي في الدول العربية نموذجا-، ص743.

يظهر الجدول تفاوت في قيمة المؤشر، بين التراجع الكبير والتحسين النسبي في سنة 2024 بقيمة 31.68 . ويمكن إرجاع ذلك إلى:

* التعريف والمنهجية: يصدر المؤشر سنويا عن مؤسسة أكسفورد إنسايت، تأسست عام 2017، ويقع مقرها الرئيسي في لندن، ويعتمد هذا المؤشر على تقييم جاهزية الذكاء الاصطناعي ل188 دولة. وذلك لدعم الحكومات في جهودها للاستفادة من الذكاء الاصطناعي وفي تقديم خدمات أفضل ومواجهة التحديات العامة، ويشتمل المؤشر على 3 ركائز أساسية، مكونة من 10 أبعاد، 40 مؤشرا فرعيا. مأخوذة من مرجع: إيمان عبد القادر، "رؤية نقدية لمؤشر جاهزية الحكومة للذكاء الاصطناعي لعام 2024"، مجلة الأمن القومي والاستراتيجية، ع. 6 (يوليو 2025)، ص 148.

¹Oxford Insights, Government AI Readiness Index 2023 (London: Oxford Insights,2023), p. 5.

الرؤية: رغم إطلاق مشروع الإستراتيجية الوطنية للذكاء الاصطناعي منذ عام 2020، إلا أنها لم تعرض إلا في ديسمبر 2024 في نسختها الأولى، خلال ندوة نظمت ضمن فعاليات الطبعة الثالثة للمؤتمر الإفريقي للمؤسسات الناشئة، لذا لا تزال تفتقر إلى الوضوح¹.

الحوكمة: في ظل القوانين الموضوعية سابقا، فإن المشرع الجزائري لم يتطرق سواء بشكل صريح أو ضمني، إلى الذكاء الاصطناعي واستخداماته. فهي تعاني من تأخر في تطوير نصوص تنظيمية محددة تهدف إلى حوكمة وأخلاقيات الذكاء الاصطناعي².

الأمر الذي جعل الجزائر ضمن المخرجات الرسمية في الدورة الثمانين للجمعية العامة للأمم المتحدة تدعو إلى صياغة أطر قانونية لضبط الاستخدامات العسكرية للذكاء الاصطناعي، بهدف كبح سباق تسلح نوعي الذي يفتقر إلى ضوابط ومنع وصول التقنيات المتقدمة إلى الفواعل من غير الدول³.

القدرة الرقمية: يشير هذا المؤشر إلى القدرة الرقمية الموجودة لدى الحكومة من حيث الخدمات الحكومية المقدمة عبر الانترنت.

لا تزال مختلف الأنشطة في الجزائر، بما في ذلك القطاعات الاقتصادية والصناعية والمالية، تعاني من بطء وتيرة التحول الرقمي، على الرغم من مرور أكثر من خمس سنوات على الإعلان عن ضرورة تبني التكنولوجيا والرقمنة، وهذا التحول تشهده قطاعات قليلة، مثل التعليم العالي والتربية الوطنية⁴.

القدرة على التكيف لمواكبة التغيير والابتكار بفعالية: صنفت الجزائر من حيث الترويج للاستثمار في التقنيات الناشئة في المرتبة 85 سنتي 2021 و2022، والمرتبة 86 لسنة 2023 من أصل 134 دولة وهي مرتبة متوسطة على العموم⁵.

المطلب الثاني: جاهزية قطاع التكنولوجيا

¹ أسماء زينات، "واقع جاهزية الدول العربية في استخدام الذكاء الاصطناعي"، *مجلة الاستراتيجية والتنمية*، م. 15، ع. 2 (جويلية 2025)، ص 417.

² Sari, op.cit., pp. 114,115.

³ Mounir Benhah and Hamza Ouassaa, "Artificial Intelligence in Algeria: Between Reality and Ambition", *Journal of Economic Growth and Entrepreneurship*, Vol. 8, No. 4 (2025), p. 57

⁴ Sari, op.cit., p. 114.

⁵ بركات، مرجع سابق، ص 221.

الفصل الثاني

يعتمد قطاع التكنولوجيا على الابتكار، مدعوم ببيئة أعمال محفزة لريادة الأعمال واستثمارات مستدامة في البحث والتطوير، والرأس المال البشري، لتوفير كفاءات متخصصة لتطوير حلول متقدمة تواكب المتطلبات الحكومية المتغيرة.¹

الجدول رقم 06: يشير جاهزية قطاع التكنولوجيا للجزائر خلال الفترة (2021-2024).

السنوات	2021	2022	2023	2024
قيمة المؤشر	29.57	29.93	30.56	33.26
الترتيب العالمي	99	111	120	107

المصدر: بوعزة، بصاشي، مرجع سابق ، ص 744.

يشير الجدول إلى وجود تحسن طفيف في قيمة المؤشر من 29.57 سنة 2021 إلى 33.26 سنة 2024. في مقابل تراجع الترتيب العالمي ما يعني سرعة التطور العالمي الهائلة التي تشهدها قطاع التكنولوجيا، وهذا يعكس فعالية جهود الدولة في تطوير البنية التكنولوجية، لكنها تبقى محدودة من حيث الأثر الكمي، ويعود السبب في ذلك: القدرة على الابتكار: يشير إلى مدى امتلاك قطاع التكنولوجيا الظروف المناسبة لدعم الابتكار.²

الجدول رقم 07: يبين أداء الجزائر وفقا لمؤشر الابتكار العالمي خلال الفترة (2020-2025).

السنة	الترتيب العام	مدخلات الابتكار	مخرجات الابتكار
2021	120	109	128
2022	115	110	118
2023	119	118	116

¹ Oxford Insights, *Government AI Readiness Index 2023*, p. 5. <https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-1.pdf>

² Ibid., p. 39.

الفصل الثاني

115	113	115	2024
111	112	115	2025

المصدر: من إعداد الطالبة، بالاعتماد على المرجع: <https://shorturl.at/0A1S4>

يظهر الجدول تحسنا تدريجيا في ترتيب من حيث مؤشر الابتكار العالمي، ففي عام 2025 قد سجلت الجزائر نتائج في مخرجات الابتكار أفضل من المدخلات، حيث احتلت المرتبة 112 في المدخلات والمرتبة 111 من ناحية مخرجاتها، وذلك مقارنة مما كانت عليه في السنوات الماضية.

بالرغم من التحسن الطفيف، إلا أنها لا تزال تعاني من ضعف الابتكار، يرجع ذلك إلى العوامل لآتية:

التمويل: في عام 2025، تم توجيه ما يقارب 1.5 مليار دينار جزائري، أي حوالي 11 مليون دولار أمريكي نحو مجالات: الذكاء الاصطناعي والأمن السيبراني، والروبوتات. مما ساهم في استثمار تراكمي بلغ حوالي 50 مليار دينار، أي حوالي 370 مليون دولار أمريكي بين عامي 2020 و2024.

يمثل هذا زيادة سنوية كبيرة بنسبة 25%، حيث تستهدف هذه المخصصات المالية إلى إطلاق أكثر من 500 مشروع بحلول عام 2026.¹

ونخلص إلى القول، أن الجزائر تواجه تحديات في توفير التمويل الكافي الموجه لدعم البحث و التطوير، لاعتماد على القطاع العام كممول وحيد، فنقص التمويل الموجه لتمويل المشاريع البحث و التطوير لدعم مشاريع الذكاء الاصطناعي، من شأنه أن يضعف البنية التحتية الرقمية.²

رأس المال البشري: تعاني الجزائر من نقص الكفاءات المتخصصة في مجال الذكاء الاصطناعي ويعود ذلك إلى حداثة تطبيق هذا المجال في الجزائر.

¹ Benhah, Ouassaa, op. cit., p. 52.

² بركات، مرجع سابق، ص 221.

الفصل الثاني

حيث يرتقب تخرج الدفعة الأولى من حاملي شهادة مهندس في الذكاء الاصطناعي عام 2026. كما عملت وزارة التعليم العالي على إدراج مفاهيم الذكاء الاصطناعي ضمن مختلف التخصصات الأكاديمية، سعياً منها لتعميم المعرفة الرقمية¹.

المطلب الثالث: جاهزية البيانات والبنية التحتية.

الجدول رقم 08: جاهزية ركيزة البيانات و البنية التحتية للجزائر خلال الفترة (2021-2024)

السنوات	2021	2022	2023	2024
الجزائر	51.24	45.88	47.30	52.24
قيمة المؤشر	99	111	120	107
الترتيب العالمي				

المصدر: بوعزة، بصاشي، مرجع سابق، ص745.

تبين الأرقام انخفاض في قيمة المؤشر من 51.24 سنة 2021 إلى 45.88 سنة 2022، يمكن إرجاع ذلك إلى محدودية الاستثمار في البنية التحتية الرقمية الشبكات ومراكز البيانات، ليشهد ارتفاعا ملحوظا سنة 2024 وهذا يعكس الجهود والمحاولات لإصلاح الوضع ووصلت قيمة المؤشر 52.24.

البيانات: انطلاقا من أن الذكاء الاصطناعي، يتطلب تدفقات ضخمة من البيانات عالية الجودة. فهي تظل دون فاعلية ما لم تدعم ببنية تحتية قادرة على معالجة البيانات وتشغيل التطبيقات وإيصالها للمستفيدين².

هنا تبرز إشكالية، جودة وتوافر البيانات كعائق أمام الاستفادة من البيانات، فالوصول إلى بيانات عالية الجودة في الجزائر غالبا ما يكون مقيدا³.

البنية التحتية: تشير البنية التحتية في سياق الذكاء الاصطناعي إلى الأنظمة والتقنيات الضرورية لربط الأجهزة والتي تمكن من تبادل البيانات بين الأجهزة المختلفة بشكل فعال

¹ زينات، مرجع سابق، ص 410.

²Oxford Insights, *loc. cit.*

³Fatima Zohra Gharbi, "Artificial intelligence in higher education and scientific research: concerns, difficulties, and opportunities for economic sciences in Algeria's current situation", *Revue Algérienne d'Economie de gestion*, Vol. 19, No. 1 (2025), p.98.

الفصل الثاني

وآمن، مما يسمح بتواصل الأنظمة وتبادل المعلومات بسلاسة.¹ وعليه تشمل البنية التحتية في الجزائر على:

1/ سوق الإنترنت والهاتف (النقل والثابت):

جدول 09: يبين تطور إجمالي المشتركين في الهاتف و الإنترنت في الجزائر خلال الفترة (2021-2025).

السنوات	2021	2022	2023	2024	2025 ثلاثي ثاني
تطور الهاتف النقل	47.016	49.016	51.522	54.051	54.874
تطور الهاتف الثابت	5.097 مليون	5.576 مليون	6.324 مليون	6.931 مليون	7.375 مليون
تطور شبكة الانترنت (الثابت والنقل)	45.945 مليون	49.454 مليون	53.620 مليون	57.54 مليون	59.01 مليون

المصدر: من إعداد الطلبة بالاعتماد على مؤشرات سوق الهاتف النقل والثابت وسوق الأترنت من

سلطة ضبط البريد والاتصالات الإلكترونية، <https://shorturl.at/KiSGL>

يكشف الجدول التطور التصاعدي للمؤشرات، قد تم تسجيل نمو عدد المشتركين في الهاتف النقل بنسبة 54.874 مليون مشترك في الثلاثي الثاني لسنة 2025، أما الهاتف الثابت فقدّر 7.375 مليون مشترك في ذات السنة، وعدد مشرركي الانترنت وصل إلى 59.01 مليون مشترك.

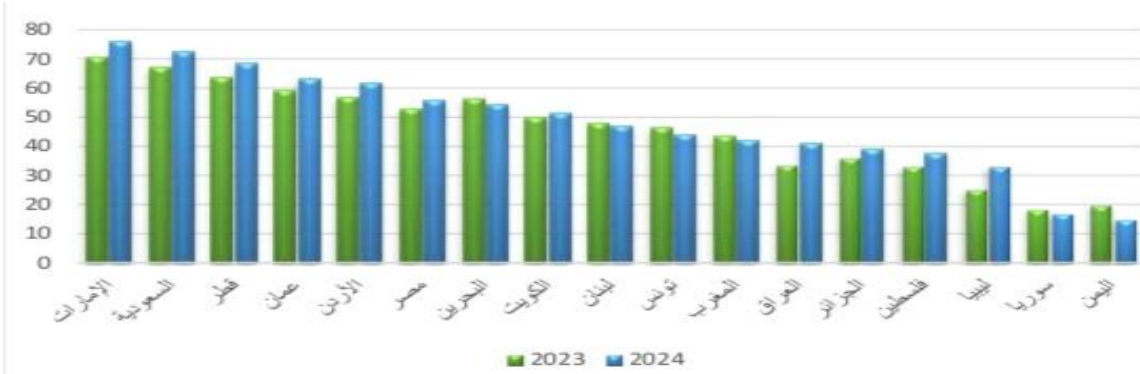
وفي ذات التوجه، قد ارتفع عدد الأسر الموصولة بشبكة الألياف البصرية من 53394 بداية 2020 إلى 2,2 مليون شهر جوان 2025.² وهذا راجع إلى مدى الالتزام بتحسين جودة الخدمات الرقمية المقدمة للمشركين.

¹ لعريوي، مرجع سابق، ص 230.

² وزارة البريد والمواصلات السلكية واللاسلكية، "الجزائر تتخطى عتبة 2.2 مليون أسرة موصولة بشبكة الألياف البصرية إلى غاية المنزل (FTTH)"، 19 جوان 2025، <https://shorturl.at/Xhco>

الفصل الثاني

الشكل رقم 03: مؤشر جاهزية الحكومات للذكاء الاصطناعي لعامي 2023-2024 لدول الشرق الأوسط وشمال إفريقيا.



المصدر: ريمة يونس، "واقع جاهزية بعض الدول الشرق الأوسط وشمال إفريقيا في استخدام الذكاء الاصطناعي خلال الفترة 2024-2022"، ص 156.

وعليه، هذا التفاوت في الأداء جعل الجزائر تبقى دون المستوى المطلوب، ففي سنة 2024 احتلت الجزائر المرتبة 107 من أصل 181 دولة، بلغت القيمة الإجمالية للمؤشر 39.06 ، أما على المستوى العربي فتمركزت في المرتبة 13.

فبالرغم من الجهود المبذولة، لم تتمكن من تقليص الفجوة بينها وبين دول أخرى التي تشهد تقدما ملحوظا في هذا المؤشر، على سبيل المثال: قطر (68.22، المرتبة 54 عالميا) مصر (سنة 2024: قيمة المؤشر 55.63 المرتبة 65 عالميا)، المغرب (41.78، المرتبة 88 عالميا)، وهذا يظهر الوتيرة البطيئة لتبني الذكاء الاصطناعي، وتعميم الخدمات الرقمية، لاسيما في ظل غياب عنصر الحوكمة .¹

¹Oxford Insights, Government AI Readiness Index 2024

الفصل الثالث

الاستراتيجية الوطنية للبحث والابتكار في الذكاء

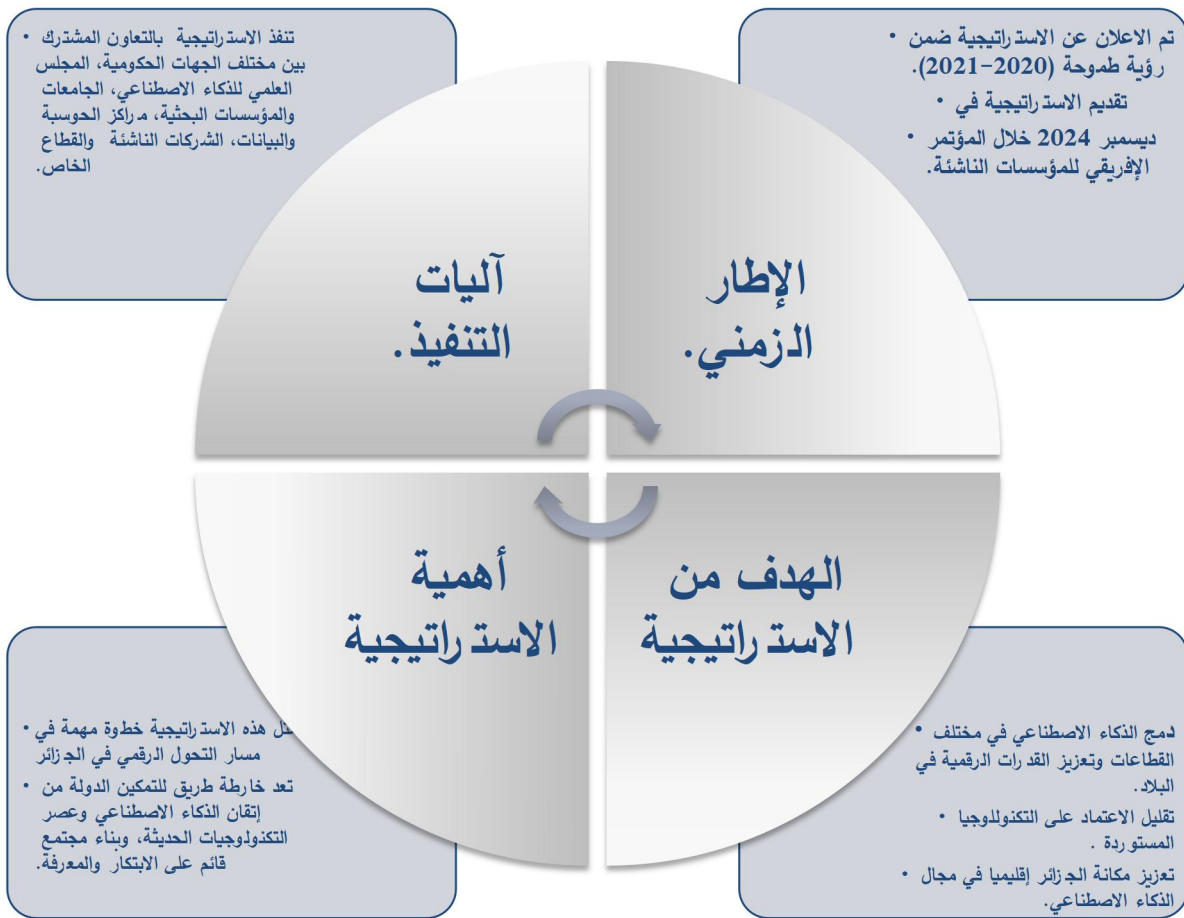
الاصطناعي (2030-2020)

- المبحث الأول: تحليل الإستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي (2030-2020)
- المبحث الثاني: تقييم الإستراتيجية الوطنية في ضوء تحليل

SWOT

المبحث الأول: تحليل الإستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي (2020-2030)

الشكل رقم 04: يشير إلى الإطار العام لإستراتيجية الوطنية للذكاء الاصطناعي.



المصدر: من إعداد الطالبة، بناء مرجعين:

<https://shorturl.at/ytdWA> ، <https://shorturl.at/7ljtY>

المطلب الأول: دوافع الصياغة والسياق الأمني

لم تصنع الإستراتيجية الوطنية للذكاء الاصطناعي في الجزائر بمعزل عن التحولات الجيوسياسية والأمنية التي ميزت الفترة (2019-2026). والسؤال المركزي هنا هو: لماذا اتجهت الجزائر إلى اعتماد هذه الإستراتيجية؟ تكمن الإجابة في مجموعة دوافع خارجية وداخلية جعلت من الذكاء الاصطناعي درع دفاعي يعزز الأمن الوطني.

أولاً: الدوافع الخارجية:

الحرب الأوكرانية- الروسية (2022): تحولت هذه الحرب إلى مختبر مفتوح لتجريب أنظمة التشغيل الذاتية المعززة بالذكاء الاصطناعي. فقد استخدم الطرفان الطائرات المسييرة والدرونات ذاتية التشغيل.¹ كما اعتمدت أوكرانيا على برامج لتوظيف صور "Palantir" لتحليل متقدمة، مثل: الأقمار الاصطناعية، البيانات المفتوحة في عمليات الاستهداف العسكري.

لعبت شركات التكنولوجيا العالمية "مايكروسوفت"، و"أمازون"، و"جوجل"، و"ستارلينك" دوراً محورياً في حماية أوكرانيا من الهجمات الإلكترونية عبر ترحيل البيانات إلى الخوادم السحابية وضمان الاتصال المستمر.²

في المقابل، استخدمت روسيا الذخائر ذكية "ZALA Aero KUB-BLA"، بينما اعتمدت أوكرانيا على طائرات من دون طيار "Bayraktar TB2" تركية المستقلة جزئياً.³

الحرب على غزة (2023): كشفت هذه الحرب عن مستوى متقدم من الأتمتة العسكرية، حيث وظف الكيان الصهيوني أنظمة مثل لافندر والإنجيل لتحديد آلاف الأهداف عبر

¹ بلال فكاني، "أثر توظيف أنظمة التحكم الذاتي المعزز بالذكاء الاصطناعي في الحروب الجديدة وإشكالية الموازنة بين الكفاءة الميدانية ومعايير القانون الدولي الإنساني"، *المجلة الجزائرية للعلوم الاجتماعية والإنسانية*، م. 13، ع. 2 (2025)، ص 98.

² المكان نفسه.

³ "كيف يدير الذكاء الاصطناعي دفة الحروب الحديثة؟"، *مركز المستقبل لأبحاث والدراسات المتقدمة*، 20 مايو 2024،

<https://futureuae.com/ar-AE/Mainpage/Item>

خوارزميات تعتمد على قواعد بيانات ضخمة¹. كما استخدمت منظومات حماية ذاتية (Trophy) لحماية المدرعات².

أبرزت هذه الممارسات أن التهديدات الحديثة امتدت إلى الفضاء الرقمي والمعلوماتي. وهو ما يفسر توجه الجزائر نحو تعزيز أمنها السيبراني، ومواكبة التحولات التي فرضتها البيئة الدولية الجديدة.

ثانيا: الدوافع الداخلية: إلى جانب السياق الخارجي، تواجه الجزائر سياق أمني داخلي مرتبط بضرورة حماية حدودها الطويلة، وضمان أمن البنى التحتية الحيوية، هذه العوامل التي تضافرت مع السياق الخارجي، جعلت من صياغة إستراتيجية وطنية للذكاء الاصطناعي خيارا ضروريا لتعزيز الأمن الوطني، وتشمل:

الحراك الشعبي 2019: في سياق الحراك الشعبي الذي اندلع في الجزائر في فبراير 2019، لم يعد الفضاء الرقمي مجرد أداة للتواصل والتعبئة، بل تحول إلى ساحة معارك معلوماتية وسياسية، تم توظيف فيها الأخبار الزائفة، الصور المفبركة، ومقاطع الفيديو المختلفة لتشويه أحداث المسيرات، وتأجيج المشاعر، وتشثيت الحراك من الداخل³.

حادثة إختراق المجال الجوي الجزائري (أبريل 2025): في خطوة تبرز التطور النوعي في آليات الدفاع، أسقطت القوات الجزائرية طائرة الدرون مسيرة تركية مسلحة اخترقت المجال الجوي لمسافة 2 كيلومتر، قرب حدود مالي، فقد أظهر الحدث أن التهديدات تتجاوز الحدود التقليدية إلى الفضاء الرقمي والطائرات ذاتية التشغيل⁴. تؤكد هذه الواقعة سرعة الدولة لاعتماد تقنيات اليقظة المتقدمة في مجال الدفاع الجوي وأمن الحدود.

¹ المكان نفسه.

² فكاني، مرجع سابق، ص 100.

³ خديجة يحيى، نصيرة صبيات، "الأخبار المفبركة في شبكات التواصل الاجتماعي بين التعقيم الإعلامي والرد في الفيسبوك: دراسة تحليلية لأزمة الحراك الشعبي الجزائري 2019 صفحة (FAKE NEWS DZ نموذجاً"، مجلة الرواق للدراسات الاجتماعية والإنسانية، م. 11، ع. 1

(2025)، ص311.

⁴ بيان لوزارة الدفاع الوطني، تأمين الحدود.. إسقاط مسيرة استطلاع مسلحة، وزارة الدفاع الوطني، 01 أبريل 2025،

<https://shorturl.at/WyDHT>

يشير هذا الميدان الجديد للصراع الجيوسياسي، استنادا إلى نظرية الأمنة في الدراسة إلى ضرورة وجودية لبلورة إستراتيجية تجمع بين حماية السيادة ومواكبة التطور التكنولوجي العالمي.

المطلب الثاني: محاور الإستراتيجية.

اعتمدت الجزائر في إستراتيجيتها الوطنية للذكاء الاصطناعي على ستة محاور رئيسية، التي صيغت استجابة لاحتياجات أمنية وتنموية محددة. سنركز في هذا المطلب على السؤال الآتي: لماذا هذه الخيارات دون أخرى؟.

تعتمد الإستراتيجية على ستة محاور أساسية:¹

1. **محور البحث والابتكار:** يحتل هذا المحور مكانة أساسية في بناء قدرات علمية وتقنية متميزة، عبر تشجيع التعاون بين الجامعات والمؤسسات الصناعية، إضافة إلى العمل على تعزيز الشراكات الدولية لاستقطاب مشاريع بحثية طويلة الأمد.²

ففي سياق الأمن السيبراني، تعمل الجزائر باعتماد على فريق بحثي من جامعة العلوم والتكنولوجيا بوهران (USTO) على تطوير نماذج ذكية للتنبؤ والكشف عن التهديدات، لأجل حماية البنى التحتية المعلوماتية وتوفير قاعدة معرفية قوية لاتخاذ قرارات فعالة.³

2. **محور تطوير المهارات:** تشكل المهارات والإبداع عنصرا أساسيا في الانتقال من النقل التكنولوجي إلى إنتاج المعرفة محليا، ومن السياسات البارزة في هذا الإطار هو إنشاء المدرسة الوطنية العليا للذكاء الاصطناعي كخطوة لتقليل التبعية من خلال تكوين كوادر لإدارة الخوارزميات بشكل آمن داخل الحدود الوطنية، وبما يسمح بمنح استقلالية في اتخاذ القرارات الإستراتيجية.

محور الاستثمار في البنية التحتية: يجسد تركيز الدولة على البعد السيادي في إدارة البيانات عبر إنشاء مراكز بيانات وطنية كقضية إستراتيجية في تعزيز الأمن وحماية خصوصية المواطنين والمؤسسات.

¹ "الإستراتيجية الوطنية للذكاء الاصطناعي في الجزائر"، مكتبة الابتكار، <https://shorturl.at/X2kZU>

² المكان نفسه.

³ "E- Governance en Algérie 2025: Perspectives et défis", Centre d' Etude Africaines de l'Université HSE, Moscou, 2025, p. 18.

وتماشيا مع هذا الاتجاه، اعتمدت الحكومة في مارس 2025 مشروع إنشاء مركز بيانات للذكاء الاصطناعي بوهران، لخلق بيئة موثوقة تدعم الباحثين والشركات الناشئة والمؤسسات الأكاديمية.¹

3. **محور الإطار التنظيمي:** يعالج هذا المحور مدى الوعي بتطوير أطر لحوكمة البيانات، وتأسيس منظومة قانونية وأخلاقية لضمان الاستخدام المسؤول للتقنيات الحديثة، فغياب سياسات رقابية وتشريعات واضحة يفتح المجال لاستغلال هذه البرمجيات للتجسس على المستخدمين، والتأثير على الرأي العام.

4. **محور الاستثمار في الشركات الناشئة:**

تسعى الجزائر من خلال هذا المحور إلى ضمان التكامل بين البعد الاقتصادي والسيادي عبر تحويل المهارات إلى مشاريع تسهم في تحقيق السيادة التكنولوجية. تجدر الإشارة إلى النمو الملحوظ في عدد المؤسسات الناشئة من 200 سنة 2019 إلى أكثر من 13.000 حاليا، مع هدف الوصول إلى 20.000 مؤسسة ناشئة في آفاق 2029.²

إضافة إلى تشجيع إدراج شركات ناشئة وسريعة النمو في البورصة، خصوصا في مجالات التكنولوجيا، الزراعية، الصحية والتجارة الإلكترونية، الذكاء الاصطناعي، بهدف تمويل توسعاتها وتأمين اختراعاتها على المستوى المحلي.³

5. **محور التركيز على القطاعات الحيوية:** ويعكس أولويات الدولة نحو المجالات ذات الأثر الاقتصادي، الاجتماعي والأمني المباشر.

ويشمل الزراعة من خلال إدارة الموارد المائية والمحاصيل بتقنيات ذكية لتحقيق الأمن الغذائي، الصحة بتحسين جودة الخدمات، ومراقبة الوضع الصحي لضمان الأمن الصحي،

¹ "وهران تحتضن أول مركز بيانات متطور لدعم الذكاء الاصطناعي في الجزائر"، *أنتر نيوز*، 16 مارس 2025، تاريخ الدخول 25 مارس 2026، <https://shorturl.at/5psB6>

² "ريادة الأعمال مؤسسات ناشئة: بروز المنظومة الوطنية دوليا يعكس التزام الدولة بمرافقة الشباب المقاول"، وكالة الأنباء الجزائرية، 07 ديسمبر 2025، تاريخ الدخول 25 مارس 2026، <https://shorturl.at/RCJwA>

³ "دخول مرتقب لخمس مؤسسات ناشئة على الأقل في بورصة الجزائر سنة 2026"، وكالة الأنباء الجزائرية، 12 فيفري 2026، تاريخ الدخول 25 مارس 2026، <https://shorturl.at/LbU2O>

أما في قطاع الطاقة فيركز على تحقيق الأمن الطاقوي في إدارة مصادر الطاقة المختلفة والتننبؤ بالطلب. وأخيرا الأمن السيبراني، حماية للبنى التحتية الحيوية والبيانات الحساسة.¹ يدل اهتمام الدولة الجزائرية بالمحاور الستة السابقة، إلى الرغبة في بناء قاعدة متينة تتمركز كلها حول بقاء واستمرارية الاستقرار الوطني، في ضوء التطورات التكنولوجية الراهنة.

المطلب الثالث: انعكاسات الإستراتيجية على الأمن الوطني.

لا تزال الإستراتيجية الوطنية للذكاء الاصطناعي في الجزائر في مراحلها الأولى، وهو ما يثير سؤالا جوهريا: كيف يمكن لهذه الإستراتيجية أن تعزز الأمن الوطني الجزائري؟ في هذا المطلب، سنناقش الانعكاسات المتوقعة على الأمن الوطني.

يمكن تلخيص الانعكاسات المتوقعة في خمسة مسارات رئيسية:

المسار الأول: تدعيم المقاربة الدفاعية بتوفر الإستراتيجية قاعدة بحثية، وتقنية وتدريبية لدعم الباحثين والمهندسين في الذكاء الاصطناعي على تطوير أنظمة مراقبة دقيقة، وتحسين القدرة على اتخاذ قرارات رشيدة، ورفع من نجاعة العمليات الدفاعية على المدى المتوسط والبعيد.

المسار الثاني: تعزيز السيادة الرقمية تهدف الإستراتيجية إلى دمج هذه التكنولوجيا في القطاعات الحيوية لاقتصاد والمجتمع، مع التركيز على خلق فرص لأجيال القادمة. تكريس الاستقلال التكنولوجي، وهو ما يحمي الجزائر من التبعية التكنولوجية ويعزز مكانتها كقطب تكنولوجي مبتكر.²

المسار الثالث: التكامل بين الأمن والتنمية وضعت الإستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي 2020-2030، إطارا يجمع بين التنمية الاقتصادية، والتعليم والابتكار من جهة، والأمن والدفاع، الحدود من جهة أخرى.³

¹ Djallal Bouabdallah, "L'Algérie à l'ère de L'AI: Une vision Stratégique pour 2035," *LinkedIn*, 12 décembre 2024, <https://shorturl.at/4jUzS>

² Ibid.

³ " الإستراتيجية الوطنية للذكاء الاصطناعي في الجزائر"، مكتبة الابتكار، مرجع سابق.

المسار الرابع: تعزيز دور الجزائر في إفريقيا بتبني رؤية طموحة لتسريع اعتماد الذكاء الاصطناعي في القارة الإفريقية، بما يخدم أهداف التنمية المستدامة، في إطار تأمين السيادة الإفريقية ضد التبعية التكنولوجية، مما يساهم في بيئة رقمية مستقرة تدعم المصالح الأمنية والإستراتيجية للدولة الجزائرية في عمقها الإفريقي.

المسار الخامس: ترسيخ الأطر الأخلاقية والتنظيمية تتحدث الإستراتيجية عن بناء منظومة إستراتيجية للذكاء الاصطناعي المسؤول، بهدف الحد من مخاطر استغلال التكنولوجيا في التزييف والمراقبة، بما يساهم في تقوية الشرعية القانونية الأمن الرقمي.¹

¹Amir Nour, "Intelligence artificielle: L'Algérie adopte une stratégie nationale", *L'écho D'Algerie*, 8 décembre 2024, <https://shorturl.at/sinh2>

المبحث الثاني: تقييم الإستراتيجية الوطنية في ضوء تحليل SWOT

يعد تحليل SWOT (نقاط القوة *Strenghts*، الضعف *Weaknesses*، الفرص *Opportunities*، التهديدات *Threats*) أداة فعالة لتقييم الإستراتيجية الوطنية للذكاء الاصطناعي في الجزائر (2020-2030)، خاصة في الجانب الأمني الدفاعي لتحديد العوامل الداخلية والخارجية لرفع قدرات الاستعداد الدفاعي.

من شأن هذه الأداة تقديم تقييم استراتيجي حول إمكانيات الجزائر للقيادة في الذكاء الاصطناعي.

المطلب الأول: نقاط القوة والضعف.

نقاط القوة: تتميز الإستراتيجية بقاعدة داخلية قوية تدعم السيادة الرقمية، كما يلي:¹

1. **دعم سياسي قوي:** ويركز على وجود رؤية وطنية طموحة، وقد انعكس هذا الالتزام السياسي القوي بإنشاء مجلس مخصص لإشراف على تنفيذها، إلى جانب تقديم دعم مالي حكومي للشركات التكنولوجية ومبادرات البحث العلمي كركيزة لضمان استمرارية المشروع. حيث بلغت ميزانية البحث العلمي والتطوير التكنولوجي لسنة 2026 بقيمة 43 مليار دينار كرخص الالتزام،² وهو زيادة واضحة مقارنة بالسنوات الماضية، وهذا يدل على إرادة سياسية في بناء قاعدة بحثية وتقنية قوية.

2. رؤية شاملة ومتكاملة للإستراتيجية:

- تغطي الإستراتيجية 6 محاور مندمجة، مما يعكس طابعاً متكاملًا، قائم على التفاعل بين الدولة والمجلس الوطني للذكاء الاصطناعي، الجامعات، والشركات الناشئة في تنفيذ الإستراتيجية.

3. **التركيز على تطوير رأس المال البشري:** بدعم بناء كفاءات رقمية محلية عبر تطوير منظومة البحث والتطوير بشكل متواصل.

فعلى الصعيد الأكاديمي والبحثي: يتم حالياً تخصيص ما بين 10 إلى 15% من ميزانية البحث والتطوير للذكاء الاصطناعي. يدعم هذا الاستثمار شبكة متنامية من 12 مركز بحث

¹ اتجاهات التكنولوجيات الناشئة: الذكاء الاصطناعي والبيانات الضخمة لأغراض التنمية 4.0، الاتحاد الدولي للاتصالات: قطاع التنمية، منشورات ITU، ص 55.

² قانون رقم 17-25 مؤرخ في 23 جمادى الثانية عام 1447هـ، الموافق 14 ديسمبر سنة 2025، يتضمن قانون المالية لسنة 2026، الجريدة الرسمية للجمهورية الجزائرية، ع. 88، ص 6.

متخصص، والتي أنتجت مجتمعة 859 منشورا علميا محكما في مجال الذكاء الاصطناعي خلال عام 2024، وهي زيادة ملحوظة بنسبة 40%¹.

4. **الحرص على السيادة الرقمية:** ويتضح ذلك في دمج مطلب الأمن السيبراني ضمن الإستراتيجية، وهذا يتبين في المحور السادس بالسعي لإدماج الذكاء الاصطناعي في القطاعات الحيوية، وهذا من شأنه يضمن حماية البيانات والمصالح الحيوية للدولة.²

5. **دور دبلوماسي مسؤول دوليا:** تلعب الجزائر دورا سياسيا ودبلوماسيا في المحافل الدولية للدعوة إلى وضع أطر ملزمة تمنع سوء استخدام الذكاء الاصطناعي العسكري، مما يحافظ على السلم العالمي، ويعزز صورتها كدولة ملتزمة بالضوابط الأمنية وفي تنظيم التقنيات العسكرية الذكية.

نقاط الضعف (Weaknesses): تواجه الإستراتيجية نقائص داخلية تعيق التنفيذ الكامل:

1. بنية تحتية محدودة للابتكار المحلي:

ما تزال البنية التحتية التكنولوجية غير مكتملة تقنيا، مع تأخر في تعميم أنظمة ذكاء اصطناعي متقدمة.³

حيث احتلت الجزائر المرتبة 17 بقيمة بنقطة 27.75 في مجال البيانات والبنية التحتية، متأخرة عن دول إفريقيا مثل: تونس التي تصدرت الترتيب بقيمة 30.75، جنوب إفريقيا المرتبة الثانية بقيمة 30.56، كينيا: المرتبة الثالثة، 29.45 نقطة، أما مصر المرتبة الرابعة بقيمة 27.75 نقطة، فقد أظهرت أداء أفضل بفضل أنظمة اتصال أكثر تطورا.⁴

يمكن تحليل ضعف موقع الجزائر في الترتيب الإفريقي إلى وجود فجوة بين الطموح السياسي والقدرات التقنية المتوفرة، ما يجعلها عرضة للتبعية التكنولوجية.

4. **غياب الإطار التنظيمي:** تأخر وضع إطار تشريعي لضبط استخدام الذكاء الاصطناعي.

¹ Benhah, Ouassaa, *op.cit.*, p. 52.

² ثامري بلقاسم، شرفاوي العابد، "التحول الرقمي في الجزائر: دراسة تحليلية الاستراتيجية الوطنية للتحول الرقمي في الجزائر (من أجل جزائر رقمية 2030) حسب تقرير المحافظة السامية للرقمنة نسخة أوت 2024"، *مجلة إدارة الأعمال والدراسات الاقتصادية*، م. 11، ع. 1 (2025)، ص 678.

³ المكان نفسه.

⁴ Qhala, Qubit Hub, *AI Talent Readiness Index for Africa* (02 April 2025), pp. 79-82.

المطلب الثاني: الفرص والتحديات الأمنية

يعد تقييم الفرص والتحديات الأمنية لإستراتيجية الوطنية للذكاء الاصطناعي خطوة مهمة، للوقوف عند الفرص التي يمكن استثمارها، والتحديات التي تعيق مسار نجاحها.

الفرص (Opportunities): توفر الإستراتيجية فرصا خارجية لتعزيز الأمن الوطني:¹

1. دعم منظومة الشركات الناشئة والاستثمارات: خاصة ببروز شركات مثل:²

الشركة الناشئة الجزائرية Farm AI في القطاع الزراعي، والتي تحصلت على المرتبة الثانية في المسابقة العالمية نظمتها شركة هواوي سنة 2023، وشركة Smart Factory التي تعمل على تحسين الإنتاج الصناعي في الجزائر مدعومة بالذكاء الاصطناعي، لتحسين الكفاءة والإنتاجية في المصانع.

يوضح هذا التوجه قدرة الابتكار المحلي على المنافسة الدولية، حيث تقوم جامعة العلوم والتكنولوجيا هواري بومدين بتكوين أكثر من 500 موهبة محلية سنويا في مجال الذكاء الاصطناعي.³

2. إمكانيات القيادة الإقليمية في إفريقيا:

تدل استثمارات الجزائر في الشركات الناشئة في مجالات الذكاء الاصطناعي والأمن السيبراني بقيمة 1.5 مليار دينار، إلى جانب تفوقها الأكاديمي بوجود أكثر من 57 ألف طالب في 74 برنامج ماجستير، حيث تصنف الجزائر ضمن أفضل خمس دول إفريقية في مجال النشر العلمي المعترف به، ووجود باحثين ضمن أفضل 2% عالميا، على قدرتها في التحول إلى قطب تكنولوجي إقليمي.⁴

التحديات الأمنية:

1. مخاطر الأمن السيبراني التهديدات المتزايدة على أنظمة المعلومات، قد تؤثر على ثقة المستخدمين. ما يهدد استقرار الأمن الداخلي ويصعب التمييز بين المحتوى الحقيقي والمزيف.⁵ إذ يظهر تقرير كاسبيرسكي حول مشهد التهديدات السيبرانية في إفريقيا لسنة

¹ ثامري، شرفاوي، مرجع سابق، ص 679.

² E-Governance en Algérie 2025: Perspectives et défis, op. cit.

³ Ibid.

⁴ Ty Davila, "why Algeria is positioned to become North Africa's AI leader", New Lines Institute for Strategy and Policy, January 26, 2026, <https://shorturl.at/2gkcw>

⁵ ثامري، شرفاوي، مرجع سابق، ص 679.

2025 أن الجزائر تحتل المرتبة الأولى إفريقيا بأكثر من 13.6 مليون محاولة للتصيد الإلكتروني، وهو يفوق بكثير أنغولا (7.5 مليون) والكاميرون (6.4 مليون) وجنوب إفريقيا (1.2 مليون).¹

تظهر هذه المؤشرات إلى حجم التهديدات السيبرانية الموجهة ضد الجزائر مقارنة بدول أخرى، الأمر الذي يؤثر على تنفيذ الإستراتيجية الوطنية للذكاء الاصطناعي ويجعلها بحاجة إلى تعزيز قدراتها الدفاعية في الأمن السيبراني.

2. **المنافسة الإقليمية:** تواجه الجزائر منافسة كبيرة من الدول الإفريقية في استقطاب الاستثمارات الرقمية التي تؤثر على مكانتها كواجهة رقمية.

فحسب تقرير مؤشر جاهزية المواهب في مجال الذكاء الاصطناعي، تحتل الجزائر المرتبة الثامنة إفريقيا في الجاهزية الحكومية بقيمة 40.25، مقارنة ببعض الدول مثل: رواندا في المرتبة الأولى 51.6 وغانا المرتبة الثالثة 49.05، وحتى مصر المرتبة الرابعة بقيمة 46.9 وتونس المرتبة السادسة بنقطة 2.43.

هذا الترتيب يظهر أن المنافسة الإقليمية قوية، وأن العديد من الدول الإفريقية استطاعت تحقيق مؤشرات أعلى في الحكومة الرقمية والبنية التحتية، ما يعزز قدرتها على جذب الاستثمارات التكنولوجية.

فإن التحدي أمام إستراتيجية الوطنية للذكاء الاصطناعي في الجزائر يتمثل في تقليل هذه الفجوة وتحسين موقعها التنافسي لضمان مكانتها كواجهة تكنولوجية إقليمية.

الذكاء الاصطناعي العسكري غير الخاضع لضوابط: يمثل تحدياً أساسياً لأمن الوطني والسيادة الرقمية لاسيما في ظل التهديدات العابرة للحدود، لذا حذرت الجزائر في الأمم المتحدة من سوء استخدام التقنية الذي قد يؤدي إلى تفاقم الصراعات وانتهاك القوانين الدولية والإنسانية.³

¹Africa Cyberthreat Landscape Report (Kaspersky, 2025), p. 5.

²Qhala, Qubit Hub, op. cit., p. 85.

³ "مجلس الأمن: الجزائر تطالب بمنع سوء استخدام الذكاء الاصطناعي العسكري"، الإذاعة الجزائرية، 19 ديسمبر 2024، تاريخ الدخول 25

مارس 2026، <https://shorturl.at/yKOcL>

الفصل الثالث

من خلال دمج العوامل الداخلية: نقاط القوة والضعف، مع العوامل الخارجية: الفرص والتهديدات. يمكن صياغة بدائل إستراتيجية تتعلق بالجانب الدفاعي، تضم أربعة مجموعات:¹

الجدول رقم 10: يوضح البدائل الإستراتيجية لأداة التحليل **SWOT**.

نقاط القوة - فرص (SO)	نقاط القوة - التهديدات (ST)
دعم سياسي + استثمارات دفاعية = تطوير تقنيات الذكاء الاصطناعي محليا.	رؤية استشرافية شاملة 2030+ المنافسة العالمية = تعزيز المواجهة في إطار التنافس العالمي.
نقاط الضعف - فرص (WO)	نقاط الضعف - التهديدات (WT)
نقص كفاءات + تعاون دولي = جلب الخبرات وتوفير تدريب مشترك.	بنية تحتية محدودة + هجمات ومخاطر سيبرانية = استثمار فوري في الأمن السيبراني.

المصدر: من إعداد الطالبة بناء على معطيات سابقة.

يبرز من صياغة هذه البدائل أن نجاح الإستراتيجية الوطنية للذكاء الاصطناعي مرهون بمدى قدرة الدولة في تحويل محاورها إلى منظومة دفاعية متكاملة، تتفاعل وتتحكم في العوامل الداخلية والخارجية السائدة، بالشكل الذي يجعلها تنتقل من مجرد طموح سياسي إلى مرحلة التنفيذ الفعلي بتوظيف نقاط القوة المؤسسية، والاستثمار في الفرص المتاحة لتعزيز الأمن السيبراني ومواجهة التهديدات العالمية.

¹Syarif Hidayatullah et al., "Reformulating National Defense Policy Through Artificial Intelligence: Enhancing Strategic Decision Making and Ethical Governance," **Journal of Social Work and Science Education**, Vol. 6(2025), p. 195.

الخاتمة

نستنتج من خلال هذه الدراسة التي تناولت محددات الأمن الوطني الجزائري خلال الفترة من 2019-2026، أن الذكاء الاصطناعي لم يعد مجرد تقنية، فقد شكل نقطة تحول مفصلية كشف عن مصادر للتهديدات جديدة وإمكانيات للفرص على حد سواء. فمن خلال تحليل الإطار التشريعي والمؤسسي، ورصد جهود الدولة الجزائري. أمكن الوقوف على مدى جاهزية الدولة والتفاعل مع التطورات المتلاحقة، وعلى فاعلية السياسات المتبعة لتعزيز الأمن الوطني.

لقد أظهرت الدراسة أن الجزائر تبنت مقاربة استباقية قائمة على الوقاية، لاسيما مع تزايد مستوى الهجمات السيبرانية، غير أن هذه التدابير بقيت محدودة لتحقيق أمن وطني شامل ومستدام، بسبب جملة من التحديات البنيوية والتنظيمية التي انعكست على موقع الجزائر في المستوى دون المتوسط في مؤشر جاهزية الحكومات للذكاء الاصطناعي.

1- اختبار صحة الفرضيات:

الفرضية الرئيسية: كلما توسع توظيف الذكاء الاصطناعي في المنظومة الأمنية، كلما تعززت قدرة الدولة على الوقاية من التهديدات السيبرانية.

تعد هذه الفرضية صحيحة، فالواقع الجزائري أكد ذلك من خلال توجه الدولة إلى اعتماد مفاهيم جديدة ضمن عقيدتها الأمنية الأمن السيبراني، السيادة الرقمية، مع استحداث هياكل متخصصة في المجال وتفعيل تشريعات واتخاذ تدابير، تتلاءم مع متطلبات عصر الذكاء الاصطناعي القائم على النهج الرصد، الوقاية، والاستجابة السريعة.

الفرضيات الفرعية:

1. العلاقة بين الأمن الوطني والذكاء الاصطناعي تقوم على جدلية التهديد والفرصة.

الفرضية صحيحة، نتيجة لاتساع دائرة الفاعلين لتشمل فواعل من غير الدول، خاصة التنظيمات الإرهابية التي اتخذت من مختلف البرمجيات والأنظمة الذكية ملاذ لاستهداف استقرار الدول وتهديد مصالحها السيادية، وفي المقابل تتسارع الدول لتوظيفها كآلية ردع وجدار حماية ضد مستهدفاتها.

2. تتكيف الهندسة الأمنية مع التحول الرقمي عبر تطوير الأطر التشريعية والمؤسسية، ويرتبط نجاح هذا التكيف بمدى جاهزية واستجابة البنية التحتية التكنولوجية.

الفرضية صحيحة، نظرا لتواجد جهود تشريعية ومؤسسية واضحة من قبل الدولة الجزائرية، لكن محدودية البنية التحتية، يجعلها هدفا مباشرا لمختلف الهجمات وفي المراتب متأخرة ضمن المؤشرات العالمية. والأمر لا يفهم من هذه الزاوية فقط، بل يرتبط كذلك بغياب إطار تشريعي واضح يضبط أخلاقيات استخدام الذكاء الاصطناعي.

3. يرتبط تعزيز الأمن الوطني في ظل الإستراتيجية الوطنية للذكاء الاصطناعي، بمدى التركيز على إدماج تطبيقات الذكاء الاصطناعي في القطاعات الحيوية.

الفرضية غير مؤكدة، لكون أن التركيز على إدماج الذكاء الاصطناعي في القطاعات الحيوية ما هو إلا هدف، في حين جعل الإستراتيجية كإجراء لتعزيز الأمن الوطني يركز بشكل أكبر على نهج أمني تكاملي، يشمل الأمن الخوارزمي، تحقيق التنمية مستدامة، تكوين المورد البشري، والحوكمة، الاستثمار في البنية التحتية الرقمية، التفاعل والتنسيق بين مختلف الهيئات، مع تعزيز التعاون الدولي.

ويمكن حصر أهم النتائج المتوصل إليها في النقاط التالية:

أولاً: الذكاء الاصطناعي أصبح محددًا بنيويًا للمنظومة الأمنية الشاملة، بالشكل الذي أعاد تعريف العديد من المفاهيم الجديدة، مشكلة بذلك طفرة في تحول العلاقة بين اكتساب القوة وامتلاك المعرفة، في ظل التحديات الراهنة القائمة على ثلاثية: ضرورة التكيف العقيدة الأمنية مع التحولات التكنولوجية بدمج التقنيات المتقدمة مع القدرات العسكرية التقليدية، تعزيز الأمن السيبراني وحماية الأنظمة الحيوية، وأخيرا تطوير الكفاءات المتخصصة في مجال الذكاء الاصطناعي.

ثانياً: أصبحت العلاقة بين الذكاء الاصطناعي والأمن الوطني علاقة مبنية على ازدواجية الاستخدام، فمن جهة يساهم الذكاء الاصطناعي في رصد التهديدات وتحليل البيانات الضخمة، تعزيز القدرة على التنبؤ بالمخاطر والتعامل معها بفعالية. ومن ناحية أخرى، يتيح المجال لفاعلين جدد لاستغلال هذه التقنية في شن هجمات سيبرانية واسعة النطاق.

ثالثاً: منطق تكييف العقيدة الأمنية الجزائرية مع التهديدات السيبرانية، تجاوز المفاهيم التقليدية، ليشمل الفضاء السيبراني الذي أصبح مجالاً سيادي، وعليه ارتكزت هندستها على إدماج البعد السيبراني ضمن منظومتها التشريعية، واستحداث هيئات أمنية متخصصة، هذا التحول أدى إلى مأسسة فعلية ومنظمة لأمن السيبراني في إطار تشريعي، مؤسساتي، وسيادي. وقد تبين أن الجزائر خُطت خطوات مهمة في بناء هذه الأطر، إلا أن الحاجة إلى تحديث التشريعات والتنسيق بين مختلف الأطراف أصبح ضرورة لمواكبة التطورات في مجال الذكاء الاصطناعي.

رابعاً: لعبت السياقات الأمنية الداخلية والخارجية دوراً في الاهتمام بتأطير الذكاء الاصطناعي ضمن إستراتيجية تتبنى رؤية شاملة طويلة الأمد، والتي لا تقتصر على الأمن بالمفهوم الضيق، بل تمتد لتشمل التنمية، البحث والتطوير، التعاون الدولي، وهذا يبرز أن الذكاء الاصطناعي لم يعد مجرد أداة تقنية، بل ركن أساسي لأمن الوطني الجزائري.

التوصيات:

أولاً: ضرورة تطوير إطار تشريعي واضح وشامل يضبط الاستخدامات الأمنية للذكاء الاصطناعي.

ثانياً: تطوير البنية التحتية الرقمية بما يسمح بتعميم استعمال تقنيات الذكاء الاصطناعي بكفاءة وفعالية، وإتاحة الوصول السلس للبيانات.

ثالثاً: التنسيق بين مختلف الهيئات الوطنية، المؤسسات، الخبراء مع بناء شراكات والانفتاح على التعاون الدولي والإقليمي، بما يسمح من وضع رؤى متكاملة تحقق نجاعة أكبر في المجالات التكنولوجية ويكرس السيادة الرقمية.

قائمة المراجع والمصادر

أولاً: باللغة العربية:

أ/ الوثائق الرسمية:

1. دستور 2020 ، الجريدة الرسمية للجمهورية الجزائرية، ع.82، 15 جمادى الأولى عام 1442، 30 ديسمبر سنة 2020.
2. مرسوم رئاسي رقم 24-181 مؤرخ في 28 ذي القعدة عام 1445 الموافق 5 يونيو سنة 2024، يتضمن إنشاء مدرسة وطنية عليا في الأمن السيبراني.
3. مرسوم رئاسي رقم 20-05، مؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية للجمهورية الجزائرية، ع.64.
4. مرسوم رئاسي رقم 26-07 مؤرخ في 18 رجب 1447 الموافق 7 جانفي سنة 2026، يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية، وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية للجمهورية الجزائرية، ع.04.
5. قانون رقم 25-11 مؤرخ في 28 محرم عام 1447 الموافق 24 يوليو سنة 2025، يعدل ويتم القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية للجمهورية الجزائرية.
6. قانون رقم 25-17 مؤرخ في 23 جمادى الثانية عام 1447 الموافق 14 ديسمبر سنة 2025، يتضمن قانون المالية لسنة 2026، الجريدة الرسمية للجمهورية الجزائرية، العدد 88.

ب/ الكتب:

1. سليخ، أسامة. الاتجاهات الإستراتيجية لمواجهة التهديدات الأمنية اللاتماثلية: مدخل مفاهيمي نظري. منشورات ألفا للوثائق، الطبعة الأولى، 2022.
2. مراد، علي عباس. "الأمن والأمن القومي: مقاربات نظرية". الجزائر: دار الروافد الثقافية-ناشرون، الطبعة الأولى، 2017.

3. وليد، عبد الحي. فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني. عمان: دار ومكتبة الحامد للنشر والتوزيع، الطبعة الأولى، 2015.

ج/ المقالات العلمية:

1. "الافتتاحية: الأمن لا يقبل التجزئة". مجلة الجيش الوطني الشعبي، ع. 719، جوان 2023، ص 1، <https://shorturl.at/Sknz9>

2. عبد القادر، إيمان. "رؤية نقدية لمؤشر جاهزية الحكومة للذكاء الاصطناعي لعام 2024". مجلة الأمن القومي والاستراتيجية، ع. 6، يوليو 2025، ص ص 148-153.

3. الأميري، خالد علي محمد. العموش، أحمد فلاح. "الأمن الوطني: المفهوم، الأبعاد والنظريات". مجلة الآداب، ع. 133، 2020، ص ص 529-548.

4. بركات، سمير. "تقييم جاهزية للذكاء الاصطناعي في ضوء المؤشرات العالمية- مؤشر جاهزية الحكومات للذكاء الاصطناعي نموذجاً". مجلة الدراسات الاقتصادية المعاصرة، م. 9، ع. 2، 2024، ص ص 213-228.

5. بعيو، رئيسي لعل. "تطور مفهوم الأمن على الساحة الدولية: نحو توسيع وتعميق الأجندة الأمنية". مجلة الشرطة، ع. 157، فيفري 2024، ص ص 29-31

6. بن نجمة، محمد. "الذكاء الاصطناعي وتحديات الأمن الوطني: مقاربة تقنية". مجلة مصداقية، م. 5، ع. 2، 2023، ص ص 49-64.

7. بورباح، سلمة، "السياسة العامة الجزائرية في مجال السيبرانية: الواقع والتحديات". مجلة دفاتر السياسة والقانون، م. 15، ع. 1، 2023، ص ص 273-291.

8. بوعزة، صبرين. بصاشي، هدى. "انعكاسات تطبيق الذكاء الاصطناعي كثورة صناعية رابعة على اقتصاديات الدول-مؤشرات الجاهزية الحكومية للذكاء الاصطناعي في الدول العربية نموذجاً-". مجلة المنهل الاقتصادي، م. 8، ع. 1، جوان 2025، ص ص 733-750.

9. بوكراع، ن. من أجل جزائر صامدة سيبرانيا. مجلة الجيش، ع. 719، جوان 2023، ص ص 8-10.

10. بولعراس، فتحي. "محددات الأمن في عصر الذكاء الاصطناعي". *الديمقراطية*، ع. 100، أكتوبر 2025، ص ص 64-67.
11. ثامري، بلقاسم. شرفاوي، العابد. "التحول الرقمي في الجزائر: دراسة تحليلية لإستراتيجية الوطنية للتحول الرقمي في الجزائر (من أجل جزائر رقمية 2030) حسب تقرير المحافظة السامية للرقمنة نسخة أوت 2024". *مجلة إدارة الأعمال والدراسات الاقتصادية*، م. 11، ع. 1، 2025، ص ص 663-682.
12. دقعة، أحمد. حنيش، أحمد. "استخدام التقنيات الحديثة للذكاء الاصطناعي في الدول العربية (دراسة حالة الجزائر)". *مجلة الدراسات الاقتصادية والمالية*، م. 17، ديسمبر 2024، ص ص 231-249.
13. دبار، محمد الأمين. بابو، جمال الدين. "تداعيات الذكاء الاصطناعي على الأمن القومي". *مجلة القانون*، م. 2، ع. 1، 2024، ص ص 100-122.
14. زيغم، عبد القادر. "الهندسة الاستراتيجية لأمن القومي الجزائري". *المجلة العربية في العلوم الإنسانية والاجتماعية*، ع. 3 م. 17، جويلية 2025، ص ص 206-213.
15. زينات، أسماء. "واقع جاهزية الدول العربية في استخدام الذكاء الاصطناعي". *مجلة الاستراتيجية والتنمية*، م. 15، ع. 2، جويلية 2025، ص ص 401-423.
16. السيد، طه محمد. "مفهوم الأمن القومي". *مجلة الأمن والاستراتيجية*، ع. 1، يناير 2023، ص ص 128، 129.
17. شريف، فضيل. "الإستراتيجية الوطنية للأمن السيبراني". ترجمة: أ. لحمل. *مجلة الجيش*، ع. 715، فيفري 2023، ص ص 8-10.
18. علي رضا، فادي. "الهندسة العكسية للذكاء الاصطناعي في الحروب الحديثة: مقاربة سوسيولوجية عسكرية". *مجلة أوراق الثقافة*، م. 37، جويلية 2025، ص ص 177-190.
19. فكاني، بلال. "أثر توظيف أنظمة التحكم الذاتي المعزز بالذكاء الاصطناعي في الحروب الجديدة وإشكالية الموازنة بين الكفاءة الميدانية ومعايير القانون الدولي الإنساني". *المجلة الجزائرية للعلوم الاجتماعية والإنسانية*، م. 13، ع. 2، 2025، ص ص 87-108.

20. قلاع الضروس، سمير. "الأمن السيبراني الوطني: قراءة في أهم الإستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر". *مجلة الرواق للدراسات الاجتماعية والإنسانية*، م. 8 ، ع. 2 ، 2022، ص ص 249-267.

21. لعريوي، عبد الرزاق. "متطلبات حوكمة الذكاء الاصطناعي في الجزائر-الواقع والمأمول". *مجلة إقتصاد المال والأعمال*، م. 9 ، ع. 2، أكتوبر 2024، ص ص 213-240.

22. مجاهد، أحمد محمد فاروق. "الأمن الوطني: مفهوم ومهددات الأمن الوطني". *مجلة الدراسات الإفريقية*، م. 42، ع. 2، يونيو 2021، ص ص 238-261.

23. مخالفة، الشيماء. لعيساوي، كريمة. "السيادة الرقمية: كيف العقيدة الدفاعية الجزائرية مع التهديدات الأمنية الجزائرية". *المجلة الجزائرية للعلوم الاجتماعية والإنسانية*، م. 12، ع. 2، 2025، ص ص 390-405.

24. نموشي، نسرين. "الذكاء الاصطناعي والثورة في الشؤون العسكرية: تأثير التقنيات الذكية على استراتيجيات الحروب وميزان القوى الدولي". *مجلة السياسة العالمية*، م. 9، ع. 1، 2025، ص ص 331-355.

25. يحيى، خديجة. صبيات، نصيرة. "الأخبار المفبركة في شبكات التواصل الاجتماعي بين التعطيم الإعلامي والرد في الفايسبوك: دراسة تحليلية لأزمة الحراك الشعبي الجزائري 2019 صفحة "FAKE NEWS DZ" نموذجاً". *مجلة الرواق للدراسات الاجتماعية والإنسانية*، م. 11، ع. 1، 2025، ص ص 304-319.

26. يونس، ريمة. "واقع جاهزية بعض دول الشرق الأوسط وشمال إفريقيا في استخدام الذكاء الاصطناعي خلال الفترة 2022-2024". *مجلة الامتياز لبحوث الاقتصاد والإدارة*، م. 9، ع. 2، 2025، ص ص 147-166.

ج/ الرسائل الجامعية:

أ. أطروحات الدكتوراه:

1. تاهمي، مصطفى. "مستقبل الأمن القومي الجزائري في ظل التطورات التكنولوجية وحروب المعلومات". أطروحة مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه، الطور

الثالث علوم سياسية وعلاقات الدولية. جامعة الجزائر 03: كلية العلوم السياسية والعلاقات الدولية. 2024/2023.

2. شريط، سمية. "دور البعد الجيوسياسي في بناء الإستراتيجية الأمنية للدول -دراسة حالة الجزائر". أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم السياسية، المدرسة الوطنية العليا للعلوم السياسية، 2025/2024.

ب. مذكرات الماستر:

1. بوطمين، وائل خليل الرحمان. "البعد السبيرياني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة". مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في ميدان الحقوق والعلوم السياسية، المدرسة الوطنية العليا للعلوم السياسية، 2025/2024.

د/ مواقع الإلكترونية:

1. الإستراتيجية الوطنية للذكاء الاصطناعي في الجزائر، مكتبة الابتكار،

<https://shorturl.at/X2kZU>

2. بيان لوزارة الدفاع الوطني، تأمين الحدود.. إسقاط مسيرة استطلاع مسلحة، وزارة

الدفاع الوطني، 01 أفريل 2025، <https://shorturl.at/WyDHt>

3. قره، فارس. الأمن السبيرياني. الموسوعة السياسية، 28 أوت 2019،

<https://shorturl.at/2nmah>

4. كيف يدير الذكاء الاصطناعي دفة الحروب الحديثة؟. مركز المستقبل لأبحاث

والدراسات المتقدمة، 20 مايو 2024، <https://shorturl.at/INQI7>

5. لعروسي، رابح. ظاهرة الأمن الوطني: قراءة معرفية في المفهوم والدوافع. 2017،

<https://shorturl.at/KB2rs>

6. مؤشرات سوق الهاتف النقال والثابت وسوق الإنترنت من سلطة ضبط البريد

والاتصالات الإلكترونية: <https://shorturl.at/KiSGL>

7. وزارة البريد والمواصلات السلكية و اللاسلكية، الجزائر تتخطى عتبة 2.2 مليون أسرة

موصولة بشبكة الألياف البصرية إلى غاية المنزل (FTTH)، 19 جوان 2025،

<https://shorturl.at/Xhcoy>

4. "دخول مرتقب لخمس مؤسسات ناشئة على الأقل في بورصة الجزائر سنة 2026"،

وكالة الأنباء الجزائرية، الخميس 12 فيفري 2026، <https://shorturl.at/xsyBW>

5. "ريادة الأعمال مؤسسات ناشئة: بروز المنظومة الوطنية دوليا يعكس التزام الدولة
بمرافقة الشباب المقلول" وكالة الأنباء الجزائرية، ديسمبر 2025،

<https://shorturl.at/dQaxc>

6. المدرسة الوطنية العليا في الرياضيات، معلومات عن المدرسة NHSM،

<https://shorturl.at/u0wBc>

7. المجلس العلمي للذكاء الاصطناعي، المدرسة الوطنية العليا للذكاء الاصطناعي

ENSIA، 27 يونيو 2023، <https://shorturl.at/aBFeb>

8. وزارة الدفاع الوطني. الدرك الوطني: التنظيم و المهام،

<https://shorturl.at/EaLmE>

9. عبد الرحمان هادف، الذكاء الاصطناعي في الجزائر: رهان السيادة في زمن الثورة

التكنولوجية، الأخبار التلفزيون، 16 ديسمبر 2025، <https://shorturl.at/deIYO>

10. وزارة البريد والمواصلات السلكية واللاسلكية: الجزائر، صفحة الفايسبوك، 19 جوان

2025، <https://shorturl.at/h6Cy6>

11. "السيد الوزير يشرف على تدشين أول مركز للمهارات SKILLS CENTER

للتكوين المجاني قصير المدى في التكنولوجيات المتقدمة"، وزارة البريد والمواصلات

السلكية واللاسلكية، 23 فبراير 2025، <https://shorturl.at/L9gBB>

12. "مجلس الأمن: الجزائر تطالب بمنع سوء استخدام الذكاء الاصطناعي العسكري،

الإذاعة الجزائرية، 19 ديسمبر 2024، <https://shorturl.at/yKOcL>

ثانيا: باللغة الأجنبية:

1/ books:

1. Taddeo, Mariarsaria. McNeish, David. Blanchard, Alexander, and Others. Ethical Principles For Artificial Intelligence in The

Defence Domain. In: ***Artificial Intelligence and International Conflict in Cyberspace***. New York : Routledge Taylor & Francis Group, 2023.

2. Epasto, Simona. Artificial Intelligence in Compromised Geographies: Redefining Power and Territorial Challenges. In: ***Compromised Geography: Spreading a New world***. Springer Nature, 2026.

3. Sheikh, Haroon. Prins, Corien. Schrijvers, Erik. ***Mission AI: The New System Technology***. Springer: WRR The Netherlands Scientific Council For Government Policy, 2023.

4. Wang, Xinnian. Hu, Ao. Liu, Xincheng and Others. *Intrinsic Security of Artificial Intelligence: System Vulnerabilities, Defense Mechanism, and Theoretical Deepening*. In : ***Computer Applications***. Springer Nature Singapore Pte Ltd, 2026.

2/ Articles:

1. Benhah, Mounir. Ouassaa, Hamza. "Artificial Intelligence in Algeria: Between Reality and Ambition". *Journal of Economic Growth and Entrepreneurship*, Vol.8, No.4, 2025, p p 46-59.

2. Belhocine, Kenza. Hachouf, Loubna. Tahar, Zouagri. "Uses of Artificial Intelligence in The Security and Millitary Fields: Between The Demands of Innovation and The Limits of Criminal Liability". *LEX LOCALIS- Jouranl of Local Self-Government*, Vol.23, No.8, 2025: <https://shorturl.at/tGHwl>

3. Gharbi, Fatima Zohra. "Artificial intelligence in higher education and scientific research: concerns, difficulties, and opportunities for economic sciences in Algeria's current situation". *Revue Algérienne d'Economie de gestion*, Vol.19, No. 1, 2025, pp. 85-100.
4. Ghechir, Salah. "Digital Sovereignty and Cyber security: Legal and Strategic Implications for Algeria." *Herodotus' Journal of Human and Social Sciences*, Vol. 9, No .5 (2025) pp. 361-370.
5. Hidayatullah, Syarif. Supriyadi, Asep Adang. Purwanto, Ignatius Eko Djoko and Other. "Reformulating National Defense Policy Through Artificial Intelligence: Enhancing Strategic Decision Making and Ethical Governance". *Journal of Social Work and Science Education*, Vol. 6, 2025, pp 180-200.
6. Sari Mohamed, Fayza, "Artificial Intelligence in Algeria: A Diagnostic Assessment". *Journal of Law, Society and Authority*, Vol. 14, No. 2, September 2025, pp. 101-118.
7. Sereir EL Hirsti, Hayet. Benine, Abderrahmane. "Cybersecurity as a Fundamental Element of The Digital Economy in Algeria". *Abaad Iktissadia Review*, Vol. 14, No. 1, 2024, pp. 368-390.
8. Maizi, Lynda. "Regional and Internal Security challenges and Their Implications on the Algerian National Security". *Annals of Algiers University 1*, vol.39,N.03, 2025, p.p 147,160.

9. Abde Ssamed Bouregba, Manel Ismahan Rebbah, "Algeria's National Security Doctrine: Sovereignty, Resilience, and Regional Challenges". *Annals of Algiers University 1*, Vol. 39, N. 4, 2025, pp. 239-255.

10. Yogita Upadhyat, Rituja Sharma. "Lagal Framework for AI in National Security: Balancing Innovation, Ethics, and Regulation". *Journal of Neonatal Surgey*, Vol. 14, 2025, pp. 500-508.

3/ Thesis:

Chun Hey, Brain Kot, "Dual-Use Security Dilemma and the U.S-china AI Technology Race." thesis submitted in partial fulfilment of the requirements for the degree of MPhil .University of Oxford, May 2025.

4/ Reports:

1. L'impact de l'AI sur la sécurité national. Institut des Sciences Stratégiques(ISS): <https://shorturl.at/23OnG>

2. Mirjana Stankovic, Aminata Amadou Garba, Nikola Neftenov, Nouvelles tendance technologiques: l'intelligence artificielle et les mégadonnées au service du développement 4.0. ITU publication: Union internationale des télécommunications Secteur du développement, 2021.

3. Oxford Insights. Government AI Readiness Index 2023.

4. Introduction to Artificial Intelligence (AI) Technology, guide for travel & tourism leaders: Microsoft, January 2024.

5. Oxford Insights. Government AI Readiness Index 2023

6. Oxford Insights. Government AI Readiness Index 2025.
 7. Africa Cyberthreat Landscape Report. Kaspersky, 2025.
 8. *AI Talent Readiness Index for Africa*. Qhala, Qubit Hub, 02 April 2025.
 9. "E- Governance en Algérie 2025: Perspectives et défis", Centre d' Etude Africaines de l'Université HSE, Moscou, 2025.
 10. Ty Davila, "why Algeria is positioned to become North Africa's AI leader", *New Lines Institute for Strategy and Policy*, 26/01/2026, <https://shorturl.at/2gkcw>
- Global Cybersecurity Outlook 2026: Insight Report, January 2026. World Economic Forum, 2026

5/ web sites:

1. Algeria ranking in the Global Innovation Index 2025, wipo, <https://shorturl.at/0A1S4>
2. Amir Nour, Intelligence artificielle: L'Algérie adopte une stratégie nationale, L'écho D'Algérie, 8 décembre 2024, <https://shorturl.at/3aOKJ>
3. Présentation de la stratégie national de l'intelligence artificielle 2020-2030, Algérie press service, Lundi, 18 Janvier 2021, 17:36: <https://shorturl.at/ytdWA>
4. Djallal Bouabdallah, L'Algérie à l'ère de L'AI: Une vision Stratégique pour 2035. Linked in, Le 12 déc 2024, <https://shorturl.at/4jUzS>
5. Tewfik Hamel, Impact de l' intelligence artificielle sur la doctrine militaire : le cas de l' Algerie. Modernisation continue

sans rupture, Rosa Luxemburg Stiftung, 7 octobre 2025,
<https://shorturl.at/RpyLv>.

قائمة الجداول

الرقم	العنوان	الصفحة
01	جدول يوضح كيف أن الذكاء الاصطناعي يعد أداة للهيمنة والسيطرة.	14
02	مرتكزات الأمن الوطني الجزائري في ظل التحولات التكنولوجية.	21-22
03	التحديات الأمنية الحديثة في السياق الجزائري.	25-23
04	مقارنة بين مشهد التحدي الأمني الكلاسيكي والتحدي الأمني في ظل الذكاء الاصطناعي.	28
05	جاهزية ركيزة الحكومة للجزائر خلال الفترة (2024-2021).	48
06	جاهزية قطاع التكنولوجيا للجزائر خلال الفترة (2024-2021).	50
07	أداء الجزائر وفقا لمؤشر الابتكار العالمي خلال الفترة (2025-2021)	50-51
08	جاهزية ركيزة البيانات و البنية التحتية للجزائر خلال الفترة (2021-2024)	52
09	تطور إجمالي المشتركين في الهاتف والإنترنت في الجزائر خلال الفترة (2025-2021)	53
10	البدائل الإستراتيجية لأداة التحليل <i>SWOT</i> .	67

جدول الأشكال

الصفحة	العنوان	الرقم
32	منحنى بياني يبين التهديدات التي تم اكتشافها ضد مستخدمي الكمبيوتر في الجزائر خلال شهر أفريل وماي 2024	01
35	أعمد بيانية تبين سوق الذكاء الاصطناعي في الأمن السيبراني .	02
54	أعمدة بيانية تبين تطور مؤشر جاهزية الحكومات للذكاء الاصطناعي لعامي 2023-2024 لدول الشرق الأوسط وشمال إفريقيا	03
56	مخطط يظهر الإطار العام لإستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي (2020-2030)	04

الفهرس	
الصفحات	العناوين
أ	الملخص
11-1	مقدمة
12	الفصل الأول: الإطار المفاهيمي والنظري للعلاقة بين الأمن الوطني والذكاء الاصطناعي.
13	المبحث الأول: الإطار المفاهيمي للذكاء الاصطناعي.
15-13	المطلب الأول: تعريف الذكاء الاصطناعي من منظور أمني _ استراتيجي.
16-15	المطلب الثاني: أهداف الذكاء الاصطناعي في المجالين الأمني والدفاعي.
17-16	المطلب الثالث: الاستخدامات الأمنية و الدفاعية للذكاء الاصطناعي.
18	المبحث الثاني: الإطار المفاهيمي للأمن الوطني الجزائري.
21-18	المطلب الأول: مفهوم الأمن الوطني ومستوياته .
22-21	المطلب الثاني: مرتكزات الأمن الوطني الجزائري في ظل التحولات التكنولوجية .
25-22	المطلب الثالث: التهديدات الأمنية الحديثة في البيئة الجزائرية.
26	المبحث الثالث: العلاقة بين الأمن الوطني والذكاء الاصطناعي.
27-26	المطلب الأول: الذكاء الاصطناعي كمحدد جديد في المنظومة الأمنية
30-27	المطلب الثاني: الذكاء الاصطناعي بين منطق التهديد و منطق الفرص
31	الفصل الثاني: الهندسة الأمنية الجزائرية في ظل الذكاء الاصطناعي (2026-2019).
32	المبحث الأول: تكييف العقيدة الأمنية مع التحول الرقمي.
35-32	المطلب الأول: الأمن السيبراني كأولوية وطنية.
37-35	المطلب الثاني: الذكاء الاصطناعي كرهان استراتيجي.
38	المبحث الثاني: الأطر التشريعية والمؤسسية للأمن في عصر الذكاء الاصطناعي.
41-38	المطلب الأول: الإطار التشريعي للأمن السيبراني.
44-41	المطلب الثاني: الإطار المؤسسي للأمن الوطني.

47-44	المطلب الثالث: السياسات الوطنية في مجال الذكاء الاصطناعي.
48	المبحث الثالث: تقييم جاهزية الجزائر لتبني الذكاء الاصطناعي.
49-48	المطلب الأول: جاهزية الحكومة.
52-50	المطلب الثاني: جاهزية قطاع التكنولوجيا.
54-52	المطلب الثالث: جاهزية البيانات و البنية التحتية.
55	الفصل الثالث: الاستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي (2030-2020)
56	المبحث الأول: تحليل الإستراتيجية الوطنية للبحث والابتكار في الذكاء الاصطناعي(2030-2020).
58-57	المطلب الأول: دوافع الصياغة والسياق الأمني.
61-59	المطلب الثاني: محاور الإستراتيجية.
62-61	المطلب الثالث: انعكاسات الإستراتيجية على الأمن الوطني.
63	المبحث الثاني: تقييم الإستراتيجية الوطنية في ضوء تحليل SWOT.
64-63	المطلب الأول: نقاط القوة ونقاط الضعف.
67-65	المطلب الثاني: الفرص والتحديات الأمنية.
71-68	الخاتمة.
83-72	قائمة المراجع والمصدر.
84	قائمة الجداول
85	قائمة الأشكال
87-86	الفهرس