

السيادة الرقمية: تكيف العقيدة الدفاعية الجزائرية مع التهديدات الأمنية الجديدة

Digital Sovereignty: Adaptation of Algeria's Defense Doctrine to Emerging Security Threats

أ. كريمة لعيساوي كلية العلوم السياسية والعلاقات الدولية – جامعة الجزائر 3- الجزائر Loubna-abad@hotmail.fr	الشيماخ مخالفة* كلية العلوم السياسية والعلاقات الدولية – جامعة الجزائر 3- الجزائر Mekhalfiachaima2025@gmail.com
--	---

تاريخ القبول: 2025/12/03

تاريخ الاستلام: 2025/10/06

الملخص

فرصت الثورة الرقمية تحولات عميقة في البيئة الأمنية، حيث أضحت الفضاء السيبراني مجالا تتقاطع فيه التهديدات التقنية مع رهانات السيادة والقدرة الإستراتيجية للدول. وبذلك لم يعد التحول الرقمي مجرد خيار تكنولوجي، بل أصبح عنصرا بنويا يعيد تشكيل مفاهيم الأمن القومي ويدفع نحو صياغة مقاربات جديدة أكثر شمولية، أضحت فيها السيادة الرقمية إطارا مرجعيا لإدارة المخاطر السيبرانية بما يربط بين البعد الوطني ومتطلبات التعاون الدولي في مواجهة التهديدات العابرة للحدود. وقد إنعكست هذه التحولات بشكل واضح على العقيدة الدفاعية الجزائرية، التي تبنت تدريجيا مقاربة تكيفية تدمج الأمن السيبراني كبعد مكمل لباقي أبعاد الأمن القومي، من خلال العمل على بلورة رؤية وطنية قائمة على استيعاب التهديدات الرقمية المستجدة، وتوظيفها ضمن أولوياتها الإستراتيجية لضمان أمنها السيادي في العصر الرقمي.

الكلمات المفتاحية: السيادة الرقمية؛ الفضاء السيبراني؛ الأمن السيبراني؛ التهديدات السيبرانية؛ العقيدة الدفاعية الجزائرية؛

Abstract

The digital revolution has brought about profound transformation in the security environment, as cyberspace has become a domain where technical threats intersect with issues of sovereignty and the strategic capacity of states. Consequently digital transformation is no longer merely a technological option but rather a structural element that reshapes the very notion of national security. It calls for the development of new, more comprehensive approaches, in which digital sovereignty has emerged as a key reference framework for managing cyber risks linking national imperatives with the requirements of international cooperation to confront transnational threats. These transformation have clearly impacted Algeria's defense doctrine, which has gradually adopted an adaptive approach that integrates cybersecurity as complementary dimension to other aspects of national security. This has been pursued through the formulation of a national vision aimed at understanding emerging digital threats and

* المؤلف المرسل: مخالفة الشيماخ، الإيميل: mekhalfiachaima2025@mail.com

incorporation them into its strategic priorities, in order to safeguard sovereign security in the digital age.

Keywords: Digital Sovereignty; Cyberspace; Cybersecurity; Cyber Threats; Algerian Defense Doctrine;

مقدمة:

يتميز النظام الدولي الراهن بتحولات عميقة فرضتها الثورة الرقمية وما رافقها من تطور متسارع في تقنيات الاتصال والمعلوماتية، حيث أضحت التحول الرقمي من بين الركائز الأساسية في العصر الحالي لتعزيز ومضاعفة مكتسبات التطور والإنتاجية، زيادة القدرة التنافسية والتحكم في التكنولوجيا، بل وأكثر من ذلك أصبحت مسألة تقليص الفجوة الرقمية ضرورة إستراتيجية تسعى الدول إلى تحقيقها. هذا التحول أبرز محدودية الوسائل الدفاعية التقليدية في مواجهة التهديدات الجديدة ضمن الفضاء السيبراني، وفي ظل هذه المتغيرات برز مفهوم السيادة الرقمية كأحد المفاهيم المركزية في العلاقات الدولية المعاصرة، يعكس قدرة الدولة على التحكم في فضاءها السيبراني وحماية بنيتها التحتية المعلوماتية من التهديدات الداخلية والخارجية على حد سواء، إضافة إلى استقلاليته في إنتاج وتخزين وتدفق البيانات بما يخدم سيادتها الوطنية. وكاستجابة لمقتضيات الأمن القومي كان إدماج البعد الرقمي في العقيدة الدفاعية الجزائرية حتمياً، نحو انتقالها من التركيز على الردع العسكري التقليدي إلى تبني مقاربة شاملة، تأخذ بعين الاعتبار الرهانات التكنولوجية والأمن السيبراني كأحد ركائز الدفاع الوطني. بناءً على ذلك نطرح الإشكالية التالية:

كيف أعاد التحول الرقمي تعريف مفاهيم الأمن والسيادة داخل العقيدة الدفاعية الجزائرية، وما حدود تكيف هذه العقيدة مع متطلبات السيادة الرقمية في البيئة الإستراتيجية الراهنة؟
تطرح هذه الإشكالية مجموعة من الأسئلة الفرعية :

1. ما المقصود بالتحول الرقمي؟ وما هي انعكاساته على طبيعة التهديدات الأمنية الدولية؟
2. كيف تتجسد السيادة الرقمية كمفهوم جديد في حقل العلاقات الدولية والأمن القومي ؟
3. كيف ساهمت التهديدات السيبرانية في تبني الجزائر لإستراتيجية دفاعية رقمية ضمن عقيدتها الأمنية ؟

فرضية الدراسة:

تنطلق الدراسة من فرضية أن التحول الرقمي أسهم بشكل مباشر في إعادة تكيف العقيدة الدفاعية الجزائرية، بحيث أصبح تكريس السيادة الرقمية ودمج الأمن السيبراني ضمن أولوياتها الإستراتيجية خياراً ضرورياً، لمواجهة التهديدات الأمنية الدولية الجديدة .
أهمية الدراسة:

تتبع أهمية الدراسة من كونها تتناول موضوعا حديثا في حقل العلاقات الدولية والدراسات الأمنية، يتمثل في انعكاسات التحول الرقمي على العقيدة الدفاعية الجزائرية في ظل بيئة أمنية دولية متغيرة تتسم بتصاعد التهديدات السيبرانية، كما تبرز أهمية البحث في أنه يسلط الضوء على مفهوم السيادة الرقمية ودورها في رسم العقيدة الدفاعية الجزائرية وتطوير قدراتها الدفاعية، نحو تكييفها مع متطلبات التطور التكنولوجي للموضع بفاعلية في الأوساط الرقمية.

منهج الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي - التحليلي بوصفه الأداة الأنسب لفهم التحولات المرتبطة بالرقمنة والسيادة الرقمية، وتحليل انعكاساتها على العقيدة الدفاعية الجزائرية، بالإضافة إلى وصف طبيعة التهديدات الأمنية الجديدة التي أضحت تشكل خطراً أمنياً على السياسات الأمنية للدول .

محاور الدراسة:

1. المحور الاول : التحول الرقمي والتهديدات الأمنية الجديدة .
2. المحور الثاني: السيادة الرقمية كإطار لحماية الأمن القومي.
3. المحور الثالث: انعكاسات التحول الرقمي على العقيدة الدفاعية الجزائرية.

1 المحور الاول : التحول الرقمي و التهديدات الأمنية الجديدة:

1.1 التحول الرقمي في العلاقات الدولية من أداة تقنية إلى عنصر استراتيجي:

أدى توجه العالم نحو العصر الرقمي إلى إعادة تشكيل بنية النظام الدولي على مستويات متعددة، بما في ذلك طبيعة القوة، أنماط التفاعلات بين الفواعل وأدوات الصراع. منذ الألفية الثالثة أصبحت التكنولوجيا الرقمية عنصراً أساسياً في صوغ موازين القوى الدولية، ولم يعد التحول الرقمي مجرد عملية تحديث تقني مرتبطة بالاقتصاد والمجتمع بل عنصراً محورياً في إعادة تشكيل العلاقات الدولية، إذ تحول الفضاء السيبراني إلى مجال سيادي وباتت الدول تتنافس على السيطرة عليه باعتباره أحد مصادر القوة والهيمنة، في هذا السياق أصبحت الرقمنة اليوم من أهم أدوات تعزيز النفوذ وفي ذات الوقت هي نقطة ضعف لغير المتحكمين فيها، إذ تمكن الدول من توسيع تأثيرها عبر السيطرة على مسارات المعلومات وتوجيه الخطاب العام (القوة الناعمة)، كما تمنحها قدرات سيبرانية هجومية تستخدم كوسيلة ضغط فعالة (القوة الصلبة) قد تحدث خلافا كبيرا في البنى الدفاعية أو الإقتصادية للدول .

بذلك لم تعد القوة تختزل في عناصرها التقليدية كحجم الترسانة العسكرية أو قوة الاقتصاد الوطني، بل برزت أبعاد جديدة للقوة في مقدمتها القوة الرقمية باعتبارها امتدادا حديثا لمفهوم القوة الناعمة، كما اعتبرت القدرة على التحكم في تدفقات المعلومات والبيانات والتأثير على الفضاء السيبراني معيارا مهما لقياس نفوذ الدول، لذا سارعت الدول نحو تخصيص موارد مالية وبشرية

هائلة لتطوير قدراتها السيبرانية، سواء على مستوى الدفاع أو الهجوم في تحول إستراتيجي يعكس تطور أنماط التسليح وأساليب إدارة الصراع في العصر الرقمي، ما يفسر التزايد التصاعدي لعدد المتصلين بالشبكة العنكبوتية " فحسب آخر تقديرات الاتحاد الدولي للاتصالات فإن 4.9 مليار شخص متصل بالشبكة العنكبوتية مقابل 4.1 مليار سنة 2019 " (غنية، 2023، صفحة 54) تستعمل كلمة الرقمنة ايتيمولوجيا في اللغة الانجليزية بصيغتين متميزتين من حيث المعنى والمجال. تشير الأولى Digitization إلى عملية تحويل المحتوى المادي مثل الوثائق والصور والتسجيلات إلى نسخ رقمية كالمسح الضوئي أو التحويل الرقمي للأشرطة، أما الصياغة الثانية Digitalization فتعبر عن التحول الأوسع نحو استخدام الأدوات والتقنيات الرقمية في تسيير العمليات الإدارية والخدمات عبر منصات الكترونية متطورة، تهدف إلى تجاوز الأساليب التقليدية والعمل وفق نمط رقمي متكامل (بزة، تقييم مسار التحول الرقمي في الجزائر (2020-2023)، 2024، صفحة 46).

- في ذات السياق يمر التحول الرقمي بعدة مراحل مترابطة , يمكن اختصارها فيما يلي :
- **مرحلة النمذجة:** يتم فيها توظيف التقنيات الرقمية لتحويل المعطيات والمعلومات من شكلها الورقي إلى صيغة رقمية قابلة للمعالجة والتخزين، وتبقى هذه المرحلة محصورة في الجانب التقني دون تغيرات جوهرية في نمط العمل أو طبيعة الأنظمة المعتمدة.
 - **مرحلة الرقمنة:** تمثل هذه المرحلة نقلة نوعية تتجاوز مجرد تحويل البيانات إلى رقمنة شاملة تشمل الأنشطة التنظيمية والإدارية، إذ تسمح بدمج التكنولوجيا الرقمية في بيئة العمل من خلال الاعتماد على شبكات الاتصال الحديثة والإنترنت.
 - **مرحلة التحول الرقمي :** تشمل إعادة هيكلة شاملة لطرق العمل ونماذج الأعمال المعتمدة، وفيها يتم الانتقال من مجرد استخدام التقنيات الرقمية إلى تبني نموذج عمل متكامل، يعتمد على الابتكار وتوظيف التكنولوجيا الحديثة في تطوير الخدمات، وتسهيل العمليات الإدارية وتحسين تسيير الموارد المادية و البشرية (معصوم و عزيز، 2024، صفحة 108).

تفاوتت استجابة الدول ومجتمعاتها للتطورات التكنولوجية ضمن هذا التحول الرقمي المتسارع خاصة في تبني الرقمنة بمفهومها السابقين، ففي الوقت الذي اندفعت فيه الدول المتقدمة نحو تبني استراتيجيات رقمية شاملة بتوظيف التكنولوجيا في مختلف العمليات الإدارية والاقتصادية، ما تزال دول أخرى تشق طريقها في هذا المجال بخطى متأنية في تحويل الموارد إلى صيغ رقمية،

متأثرة بتحديات البنية التحتية الرقمية وضعف الوعي العام بضرورة التحول الرقمي وأبعاده الإستراتيجية .

2.1 طبيعة التهديدات الأمنية في العصر الرقمي :

1.2.1 الفضاء السيبراني :

عرف الفضاء السيبراني أنه مجال افتراضي تشكله شبكات الحواسيب والمستخدمين المتصلين بها، حيث يتم تخزين المعلومات وتبادلها والتواصل بشأنها عبر الوسائط الرقمية (Friedman, 2014, p. 13). يوضح هذا التعريف أن الفضاء السيبراني لا يقتصر على البنية التحتية الرقمية، بل يشمل أيضا التفاعلات البشرية والمعلومات المتبادلة عبر الشبكات، وهذا ما يمنحه طابعا مركبا للحدود يجمع بين التكنولوجيا والسلوك الإنساني، ويطرح تحديات أمنية جديدة تتجاوز المفاهيم التقليدية للسيادة والسيطرة نظرا لانفتاحه أمام فواعل متعددة وقدرته على التأثير عن بعد.

2.2.1 التهديدات السيبرانية :

تخفي الجوانب التقنية التي يكتسبها الفضاء السيبراني تأثيره العميق، حيث يشكل قبل كل شيء بيئة إستراتيجية شأنه في ذلك شأن الفضاءات الإستراتيجية العسكرية للدولة (غنية، 2023، صفحة 54)، تحتوي هذه البيئة الإستراتيجية- الفضاء السيبراني- تهديدات سيبرانية والتي تعرف بأنها مجموعة من المخاطر الرقمية تستهدف الأنظمة المعلوماتية والشبكات والبيانات باستخدام تقنيات الحوسبة والاتصال، وغالبا ما تتجسد في أنشطة خبيثة تهدف إلى اختراق الأنظمة، أو سرقة المعلومات، أو الإضرار بالبنية التحتية الرقمية (Samah, 2025, p. 47) وتنبثق هذه التهديدات عادة عندما تسعى جهة معينة لاستغلال ثغرات أمنية للوصول غير المشروع إلى نظم المعلومات، مما يهدد سرية البيانات وسلامتها وتوفرها، كما تتخذ هذه التهديدات عدة أشكال على غرار :

الهجمات السيبرانية : تتمثل أشكال الهجمات السيبرانية في عدد من النشاطات التي يقوم بها فرد أو مجموعة من الأفراد، من خلال:

اختراق الشبكات والتجسس: يتم عبر اختراق الأنظمة والحصول على بيانات حساسة في مجالات متعددة، تستغل لاحقا في تحقيق أهداف اقتصادية وأمنية، وفي حالات أخرى يتم تدمير أو تعديل البيانات المخزنة، من خلال تغييرها بما يخدم الجهة المهاجمة أو محو محتواها بالكامل **تعطيل خدمة الشبكات والبرامج الإلكترونية:** يعد من أكثر الأساليب استخداما في هذا السياق، إذ يعتمد على إغراق الخوادم المستهدفة بكم هائل من الطلبات تفوق طاقتها التشغيلية، ما يؤدي إلى توقفها عن العمل مؤقتا أو كليا (ب.عميور، 2023، صفحة 44) .

الجريمة السيبرانية: تعد من أبرز التهديدات الأمنية المرتبطة بعصر الرقمنة، إذ تشمل مجموعة من الأفعال الإجرامية التي ترتكب باستخدام تكنولوجيا المعلومات وشبكات الاتصال، وتستهدف

الأفراد بشكل خاص بدوافع متعددة سواء كانت لأغراض شخصية، أو لتحقيق مكاسب مالية، أو الإضرار بسمعة الضحية، وتتخذ هذه الجرائم أشكال متنوعة من أبرزها: اختراق الأنظمة، الاحتيال الإلكتروني، استخدام البرمجيات الخبيثة وسرقة الهوية الرقمية، وتتميز هذه الجرائم بقدرتها على إلحاق أضرار بالغة بالضحايا على المستويين المادي والمعنوي، كما يصعب في كثير من الأحيان تتبع مرتكبيها نظرا للطبيعة العابرة للحدود للفضاء السيبراني (Samah، 2025، صفحة 473)

الإرهاب السيبراني Cyberterrorism: يتمثل في استخدام التكنولوجيا الرقمية والوسائل الإلكترونية لتنفيذ أعمال إرهابية تهدف إلى إثارة الفوضى والرعب والذعر، بما في ذلك الهجمات على شبكات المعلومات، الأنظمة الحكومية، البنى التحتية الحيوية أو حتى الأفراد عبر الإنترنت، وتشمل: تجنيد الأفراد، التدريب، الإرشاد والتوجيه، التواصل بين الجماعات الإرهابية، تنفيذ هجمات سيبرانية، التهديدات السيبرانية، نشر الأفكار الإرهابية.

الحرب السيبرانية Cyberwarfare: يركز مفهوم الحرب السيبرانية أساسا على اختراق مواقع الإنترنت أو الأنظمة المعلوماتية المرتبطة بالقضايا الحيوية للدولة المستهدفة، خاصة تلك المرتبطة بالقطاعات الإستراتيجية (الدفاع، الطاقة، الاتصالات)، تختلف الحروب السيبرانية عن الحروب التقليدية من حيث طبيعتها، لأن الصراع في الفضاء السيبراني لا يضمن نتائج متوقعة أو مخططة، بل إنها حروب ديناميكية ومستمرة تتم بشكل خفي وسري يهدد الأمن والنظام العام بشكل مباشر (Samah، 2025، صفحة 474).

تعد الحرب السيبرانية نمطا جديدا من الصراعات يختلف جذريا عن الحروب التقليدية إذ تخوضها الدول أو الفاعلون غير الحكوميين من خلال الفضاء الرقمي، باستخدام أدوات تكنولوجية متطورة بدلا من الأسلحة التقليدية لذا تكون الدول في حالة دائمة من الهجوم أو الدفاع الإلكتروني، دون أن ترتبط العمليات القتالية بميدان مادي أو بوجود قوات نظامية واضحة كما تتميز هذه الحروب بطابعها العملياتي المعقد، حيث يتلاشى الخط الفاصل بين الحرب والسياسة وبين المقاتلين و المدنيين، وتغيب فيها التسلسلات الهرمية التقليدية للأوامر العسكرية، وتهدف هذه الأنشطة أساسا إلى جمع المعلومات الإستخباراتية وتخريب الأنظمة أو التأثير في الرأي العام من خلال الهجمات على الشبكات، سرقة البيانات، الترويج للدعاية الرقمية مما يجعل الحرب السيبرانية ساحة غير متماثلة للصراع تتطلب استراتيجيات أمنية جديدة.

2. المحور الثاني: السيادة الرقمية كإطار لحماية الأمن القومي :

1.2 ماهية السيادة الرقمية و الأمن السيبراني :

1.1.2 السيادة الرقمية:

برزت السيادة الرقمية كأحد الأطر الجديدة لتعزيز الأمن القومي للدول، حيث لم تعد السيادة تقتصر على التحكم في الحدود الجغرافية والقرارات السياسية، بل امتدت لتشمل السيطرة على الفضاء السيبراني والمعلوماتي، فرضت هذه السيادة نفسها كجزء من معادلة الأمن القومي للدول خاصة بعد تصاعد التهديدات السيبرانية، من هذا المنظور أصبحت السيادة الرقمية مطلبًا سياديًا للدول الطامحة إلى تعزيز استقلالها الاستراتيجي وتحسين فضاءها الداخلي ضد التدخلات الخارجية، وتزداد أهمية هذا المفهوم في الدول النامية ومنها الجزائر التي تسعى إلى بناء قدرات رقمية وطنية تؤهلها لاندماج آمن في الاقتصاد العالمي المبني على المعرفة والتكنولوجيا.

استخدم مفهوم السيادة الرقمية لأول مرة في المؤتمر العالمي للاتصالات الدولية سنة 2012، ويقصد به قدرة الدولة على التحكم في التكنولوجيا التي تقوم عليها الأنشطة الاقتصادية والمجتمعية، 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 (غنية، 2023، صفحة 53).

يبرز هذا التعريف السيادة الرقمية كقدرة إستراتيجية تميز بين الدول حسب قدرة تحكمها في مواردها الرقمية الحيوية، من خلال ارتباط السيادة الرقمية بمستوى الاستقلالية التي تمكن الدولة من اتخاذ قراراتها وممارسة أنشطتها السيبرانية بشكل سيادي دون تبعية أو تدخل خارجي، وبين قدرة بعض الفاعلين الدوليين في التأثير وفرض رؤيتهم وشروطهم الرقمية على الدول الأخرى. يعتبر الأمن السيبراني الأداة الأساسية لتحقيق هذه السيادة، إذ يمثل مجموع الإجراءات والسياسات الرامية إلى تحصين المجال الرقمي من الاختراقات والهجمات التي تهدد استقرار الدولة وسيادتها الرقمية ومن ثم أمنها القومي .

2.1.2 الأمن السيبراني :

قدمت وزارة الدفاع الأمريكية تعريفا دقيقا لمصطلح الأمن السيبراني واعتبرته: جميع التدابير التنظيمية اللازمة لضمان حماية المعلومات، سواء كانت في شكلها الفيزيائي أو الإلكتروني من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث (Danial, 2011, p. 103) ويعنى الأمن في المجال السيبراني بإجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام البيئي لتكنولوجيا الاتصال والمعلومات (libicqi, 2007, p. 01).

بناء على ذلك يمكن القول أن الأمن السيبراني مجموعة من الإجراءات والتقنيات والوسائل، التي تهدف إلى حماية الشبكات والأنظمة والمعلومات من التهديدات السيبرانية المحتملة، ويشمل ذلك تأمين الأجهزة والبرمجيات والبنى التحتية الرقمية ضد الهجمات أو الاختراقات .

3.1.2 الأبعاد الإستراتيجية للأمن السيبراني:

البعد العسكري: يتعلق بالحاجة إلى تعزيز نظام الأمن الإلكتروني العسكري، من خلال ربط الوحدات العسكرية ببعضها البعض عبر الفضاء الافتراضي لتسهيل تبادل المعلومات، وينعكس إيجابيا على تحقيق الأهداف العسكرية وعلى حماية القدرات الدفاعية وحتى الهجومية للدولة .

البعد السياسي : وصلت هذه التهديدات السيبرانية إلى مستوى الحروب السيبرانية وسباق تسلح الإلكتروني وتبادل أعمال القرصنة في ملفات وقضايا حساسة، كما أحدث الاعتماد على الفضاء السيبراني ثورة في مفاهيم العلوم السياسية مثل القوى السيبرانية والردع السيبراني

البعد الاقتصادي: يرتبط الأمن السيبراني بالإقتصاد الرقمي ذلك بالاعتماد الكبير على التكنولوجيا الرقمية في المال، الأعمال، والخدمات البنكية والتجارية، مما يجعل الإقتصاد عرضة لهجمات سيبرانية قد تسبب خسائر كبيرة .

البعد الاجتماعي: يظهر في تأثير شبكات التواصل الاجتماعي على تشكيل الرأي العام، نشر الأفكار والمعلومات وأحيانا استغلالها لنشر خطاب الكراهية أو زعزعة الاستقرار .

البعد القانوني: يتعلق بسن تشريعات وطنية لمكافحة الجرائم الإلكترونية وحماية البيانات، إلى جانب محاولات دولية لصوغ قواعد ملزمة رغم صعوبة تحقيق إجماع عالمي (عطية، 2019، الصفحات 105 - 106) ..

رغم تكامل مفهومي الأمن السيبراني والسيادة الرقمية في إطار حماية الأمن القومي للدول، فإن الأمن السيبراني يعنى أساسا بحماية الأنظمة الرقمية والشبكات والبيانات من الهجمات الإلكترونية والاختراقات، ويعتبر أداة تقنية وتدبير دفاعيا في مواجهة التهديدات السيبرانية، أما السيادة الرقمية فهي مفهوم أشمل وأعمق يرتبط بقدرة الدولة على التحكم المستقل في بياناتها وتكنولوجياها الرقمية وصوغ سياستها السيبرانية، بالتالي إذا كان الأمن السيبراني يمثل خط الدفاع التقني، فإن السيادة الرقمية تعكس البعد الاستراتيجي والسيادي في الفضاء الرقمي.

2.2 الجهود الدولية و التكتلات في مجال الأمن السيبراني :

1.2.2 الجهود الدولية في المجال السيبراني:

في ظل تصاعد التهديدات السيبرانية وما تفرزه من مخاطر عابرة للحدود تمس الأمن القومي والسيادة الرقمية للدول، إتجه المجتمع الدولي نحو بلورة أطر قانونية ومؤسسية لمواجهة هذه الظاهرة المعقدة والمتنامية، وقد فرض الطابع اللامادي والهجين للهجمات السيبرانية تحديات حقيقة أمام المنظومات القانونية الوطنية، التي لم تعد كافية بمفردها للتعامل مع هذا النمط الجديد من الجرائم، ونتيجة لذلك برزت الحاجة الملحة إلى تعزيز التعاون الدولي وتنسيق الجهود على المستويين الإقليمي والدولي من خلال وضع تشريعات، توقيع اتفاقيات، وتأسيس مبادرات مؤسسية تهدف إلى تنظيم الفضاء السيبراني وضبط سلوكيات الفاعلين فيه، هذا التوجه يعكس

وعيا عالميا متزايدا بضرورة حماية البنى التحتية الرقمية والمعلوماتية ضمان أمن الفضاء السيبراني كجزء من الأمن القومي .

جاء التحرك الدولي لمكافحة الجرائم السيبرانية، في شكل سلسلة من المبادرات القانونية والمؤسسية أبرزها:

قرار الأمم المتحدة (هافانا أوت 1990): خلال المؤتمر الثامن للأمم المتحدة حول منع الجريمة ومعاملة المجرمين، أقرت توصيات تؤكد على ضرورة تطوير إطار قانوني دولي يتيح التعاون والتنسيق بين الدول للحد من الجرائم السيبرانية .

مؤتمر الجمعية الدولية لقانون العقوبات (ريو دي جانيرو 1994): ناقش المؤتمر الخامس عشر مفهوم جرائم الإعلام الآلي، وقدم قائمة الجرائم التي يجب إدراجها ضمن النصوص الجنائية الوطنية، مثل الدخول غير المشروع والتخريب الرقمي إلى جانب سرقة البيانات (ب. عميور.، 2023، صفحة ص 45) .

إتفاقية بودابست 2001: تعد الاتفاقية الأوروبية بشأن الجريمة السيبرانية المعروفة ب إتفاقية بودابست المعتمدة من طرف مجلس أوروبا، أول صك قانوني دولي شامل في مجال مكافحة الجرائم المعلوماتية . و هدفت هذه الاتفاقية إلى "توفير سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجريمة في الفضاء المعلوماتي، من خلال سن تشريعات ملائمة وتعزيز التعاون الدولي " (Europe 2001, p p1-3) وتعد بذلك المرجع الدولي الأول الذي أرسى قواعد موحدة لتعريف لجريمة السيبرانية وتجريم أفعالها، قسمت الاتفاقية الجرائم المعلوماتية إلى أربع فئات رئيسية، الممتد من المادة 2 إلى المادة 10 كمايلي

- الجرائم الموجهة ضد سرية وسلامة وتوافر البيانات والأنظمة ويتضمنن الولوج غير المشروع (المادة 2)، الاعتراض غير المشروع (المادة 3)، تخريب البيانات وتخريب الأنظمة (المادتان 4-5)، إساءة استخدام الأدوات (المادة 6).

- الجرائم المعلوماتية ذات الطبيعة الاحتيالية ويتضمن التزوير المعلوماتي (المادة 7)، الاحتيال المعلوماتي (المادة 8).

- الجرائم المتعلقة بالمحتوى وتركز على تجريم المواد الإباحية المتعلقة بالأطفال (المادة 9).

- الجرائم المرتبطة بحقوق الملكية الفكرية والتي تجزم انتهاك حقوق الملف عبر النظم المعلوماتية (المادة 10) (Europe 2001, p p 4-9).

يمتاز هذا التصنيف بكونه وظيفيا لا شكليا، إذ لم تُعرّف الاتفاقية " الجريمة السيبرانية" بحد ذاتها، وإنما جرمت الأفعال والسلوكيات التقنية، وهو ما يعرف بالمقاربة القائمة على الأفعال، مما جعل الاتفاقية نموذجا تشريعا مرنا يصلح للتكيف مع التطورات التكنولوجية المتسارعة .

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010: وقعها مجلسا وزراء الداخلية والعدل العرب، والتي تشكل مرجعا إقليميا مهما في تنظيم مكافحة الجريمة الالكترونية داخل الدول العربية.

البيان المشترك 9 جويلية 2018: وقعه كل من الإتحاد الدولي للاتصالات والتحالف السيبراني العالمي، ويهدف إلى توحيد الجهود العالمية لمكافحة التهديدات الرقمية عبر تعزيز التوعية وبناء القدرات وتبادل المعلومات بين الدول والفاعلين غير الحكوميين .

معايير الأمم المتحدة لمواجهة الهجمات السيبرانية عام 2015، تم اعتمادها بالإجماع سنة 2021 في إطار سياسي ملزم يمنع استخدام الانترنت في تهديد الأمن والسلم الدوليين (ب.عمير، 2023، صفحة 45).

2.2.2. التكتلات في المجال السيبراني :

تشير الدراسات الصادرة عن الوكالة الأوروبية لأمن الشبكات والمعلومات إلى وجود ستة فواعل رئيسية وراء التهديدات السيبرانية تشمل: الشركات، مجرمي الانترنت، الموظفين، نشطاء القرصنة، الحكومات، والجماعات المتطرفة، ولتصدي لهذه الفواعل توصي الدراسات بوضع إستراتيجية شاملة تستند إلى محورين :

أولاً: تعزيز التعاون الدولي عبر توفير إطار قانوني وتشريعي موحد .

ثانياً: إرساء حوار استراتيجي بين الدول و شركائها بهدف رفع الجاهزية (ب.عمير، 2023، صفحة 45).

في سياق تعزيز الأمن السيبراني على المستوى الدولي برزت التكتلات السيبرانية كأبرز مظاهر التفاعل الدولي لمواجهة التهديدات الرقمية العابرة للحدود الوطنية، تسعى هذه التكتلات إلى بناء تحالفات إقليمية ودولية لتبادل الخبرات وتطوير استراتيجيات دفاعية مشتركة بما يعزز من قدرات الدول على التصدي للتهديدات السيبرانية الحديثة، نذكر منها: التحالف السيبراني العالمي الذي أنشأه الإتحاد الدولي للاتصالات لتعزيز التعاون الدولي، بالإضافة إلى المركز الأوروبي لمكافحة الجريمة السيبرانية التابعة لوكالة الشرطة الأوروبية والذي ينسق بين الدول الأوروبية لمواجهة الجريمة السيبرانية، كما يعتبر منتدى الإستجابة للحوادث الأمنية والحاسوبية هو الآخر شبكة عالمية تضم فرق الاستجابة للطوارئ السيبرانية في مختلف الدول، تشكل مثل هذه التكتلات أرضية مهمة لتنسيق السياسات وتبادل المعلومات حول التهديدات مما يجعلها أداة مركزية ضمن العقائد الدفاعية الحديثة للدول .

3. المحور الثالث: انعكاسات التحول الرقمي على العقيدة الدفاعية الجزائرية:

عكست الجهود الدولية لمواجهة التهديدات السيبرانية إدراكا عالميا متشركا بخطورة الفضاء السيبراني كجبهة صراع جديدة، مما فرض على الدول ضرورة إعادة النظر في عقائدها الأمنية

والدفاعية التقليدية، إذ لم يعد ممكنا فصل الأمن السيبراني عن منظومة الدفاع الشامل، بل أصبح جزءا بنويا في استراتيجيات الردع والحماية، وبناء على ذلك بدأت العديد من الدول في دمج الأمن السيبراني ضمن عقائدها الدفاعية، سواء عبر تطوير قدرات هجومية رقمية أو من خلال تعزيز البنى التحتية للحماية والتأمين الرقمي، وقد جاء هذا التحول استجابة لمعادلة أمنية جديدة فرضها الواقع الرقمي كما وضحنا من قبل، بظهور مفاهيم جديدة: السيادة، الاستقلال الاستراتيجي، ومفهوم الردع، مفاهيم تقاس بالقدرة على التحكم في الفضاء السيبراني.

في السياق الإقليمي وجدت الجزائر نفسها أمام ضرورة استيعاب هذه المتغيرات ضمن تصورها الدفاعي، في ظل ما يشهده الفضاء السيبراني من تهديدات متزايدة تمس البنى التحتية الحيوية للدولة والمجتمع والاقتصاد، وعليه شرعت في بلورة مقاربة دفاعية تأخذ بعين الاعتبار أهمية السيادة الرقمية كجزء من سيادتها الوطنية .

1.3. العقيدة الدفاعية الجزائرية:

تعرف **العقيدة Doctrine** والتي هي في الأصل كلمة لاتينية **Doctrina** تشمل مجموع العقائد، الآراء، المعتقدات والمبادئ، والأطروحات والمفاهيم النظرية التي تشكل جزءا من التعاليم التي يتبناها الأفراد والمؤسسات، وقد تتخذ هذه العقائد أبعادا متعددة تشمل السياسية، الاقتصادية، الفلسفية، الدينية، أو العلمية، ويكمن هدفها الأساسي في توجيه السلوك أو المساعدة على تفسير الوقائع. (Doctrine, n.d)

لذا يمكن اعتبار العقيدة بمثابة الأداة التي تحدد التوجهات المرجعية للدولة، والتي تبنى عليها المفاهيم النظرية لفهم الوقائع وتوجيه السلوكيات. وبذلك فإن العقيدة الأمنية هي المنهجية التي تعتمدها الدولة لوضع تصور شامل لمقاربتها الأمنية وصياغة الآليات والوسائل اللازمة لتحقيق أهدافها، وهي تستند أساسا إلى ارث تاريخي وتجارب علمية سابقة (عمار، 2017-2018، صفحة 191). تعتمد العقيدة الدفاعية الجزائرية على مقاربة شاملة للأمن القومي، تركز على حماية السيادة الوطنية وضمان الاستقرار الداخلي مع الأخذ بعين الاعتبار التحديات الإقليمية والدولية، خصوصا في منطقة الساحل الإفريقي التي تشهد نشاطا للإرهاب والجريمة المنظمة العابرة للحدود، أصبحت توظف الفضاء السيبراني في دعم هجماتها الإجرامية .

تأخذ العقيدة الدفاعية الجزائرية طبيعة تراكمية تشكل إطارا يمنح توجهاتها الاستقرار والثبات في سياستها الأمنية على المدى الطويل، هذه العقيدة ليست مجرد مجموعة من الإجراءات العسكرية، بل هي نتاج تراكم الخبرات التاريخية والمواقف السياسية والمحددات الجغرافية (زقاغ و منصوري، أمن منطقة الساحل الإفريقي: بين المنظور الأمني الفرنسي والإستراتيجية الأمنية الجزائرية، 2014، صفحة 53)، فضلا عن مسايرة التطورات التقنية ترتبط هذه العناصر بمجموعة من المبادئ الأساسية التي توجه العقيدة الدفاعية، مثل مبدأ عدم التدخل في شؤون الداخلية للدول

وحماية السيادة الوطنية والحفاظ على الاستقلالية في اتخاذ القرارات وكذلك التأكد على الإستعداد الدائم لمواجهة أي تهديد خارجي .

2.3. تكيف العقيدة الدفاعية مع التهديدات السيبرانية :

1.2.3. الجزائر ومواكبة التحول في مجال الرقمنة :

تأتي مواكبة الجزائر للتحول الرقمي في إطار تعزيز سيادتها الرقمية كإمتداد طبيعي للعقيدة الدفاعية الوطنية، من ادراكها بأن الرقمنة كبعد جديد للأمن القومي تسعى لإنشاء بنية تحتية رقمية متينة وتطوير قدرات بشرية وتقنية متخصصة، ووضع اطر قانونية وتشريعية تكفل حماية الأفراد والمؤسسات من التهديدات السيبرانية، يعكس هذا التوجه توازنا بين مبادئ العقيدة الدفاعية التقليدية التي تركز على البعد العسكري والسياسي وبين التحديات الرقمية الجديدة .

أكد السيد رئيس الجمهورية عبد المجيد تبون خلال الملتقى الوطني حول الأمن السيبراني الذي نظم في جوان 2023 أن " التكفل بالأمن الوطني بأبعاده السياسية، العسكرية، الاقتصادية، المجتمعية بل وحتى التكنولوجية ، يستوجب تطوير إستراتيجيتنا الوطنية المتكاملة في المجال الرقمي، والجمع بين الإستباقية والوقاية من التهديدات في الفضاء السيبراني، وحماية المنظومات والمعطيات والسهر على ترقية ثقافة رقمية مواطنيه ووطنية، عمادها التحسيس المستمر واليقظة الإستراتيجية " . (جنادي، 2024، صفحة 35)

سعيها منها في إطار تعزيز التحول الرقمي والانطلاق نحو تحقيق ثورة رقمية، اختارت الجزائر إنشاء هياكل وهيئات مختلفة ضرورية لتسيير وإنجاح هذا التحول:

صادق مجلس الوزراء المنعقد في نوفمبر 2023 على مشروع إنشاء قاعدة لتخزين وحماية البيانات الإلكترونية Data Center، كما ثمن رئيس الجمهورية خلال هذا الإجتماع وضوح الرؤية الخاصة بالتوجه الرقمي في الجزائر حيث تعد مثل هذه القاعدة بنية تحتية حيوية لتخزين البيانات وتسييرها وتحليلها على نطاق واسع (جنادي، 2024، صفحة 34)، إضافة إلى ذلك أنشئت المحافظة السامية للرقمنة في سبتمبر 2023 تحت وصاية رئاسة الجمهورية (يرأسها محافظ سامي للرقمنة برتبة وزير) لضمان توافق مخططات القطاعات المعنية في مجال الرقمنة مع الإستراتيجية الوطنية للرقمنة، مع التقييم واقتراح التدابير، تحديد المشاريع ذات الأولوية والاستثمارات الإستراتيجية، وتعبئة الموارد البشرية والمالية اللازمة.

في سياق عزم الجزائر تسريع وتيرة رقمنة إقتصادها وقطاع الخدمات العمومية، تم إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية في جانفي 2020، وتشمل هذه المنظومة التي وضعت لدى وزارة الدفاع الوطني، مجلسا وطنيا مكلفا بإعداد الإستراتيجية المذكورة والموافقة عليها وتوجيهها بالإضافة إلى وكالة تضطلع بالتنسيق من أجل تنفيذ هذه الإستراتيجية، كما استحدثت مدرسة وطنية عليا للأمن السيبراني بالتنسيق مع وزارة الدفاع .

3.3. الإستراتيجية الوطنية الجزائرية للأمن السيبراني :

تعمل الجزائر منذ بداية توجهها نحو الإدارة الرقمية على حماية أنظمتها المعلوماتية، من خلال تطوير خطط عمل و سن القوانين اللازمة وإشراك جميع الجهات الفاعلة في مقاربة شاملة ومستدامة، تهدف إلى التنسيق بين جميع مؤسسات الدولة ،

قد تجسدت هذه المقاربة في التعليمات الصادرة 1 مارس 2017 التي وضعت آليات لتبادل المعلومات وخلق هيكل لأمن الأنظمة المعلوماتية، في يناير 2020 تم تأسيس منظومة وطنية لأمن الأنظمة المعلوماتية - وكالة أمن أنظمة المعلومات - تحت إشراف وزارة الدفاع الوطني تضم مجلسا ووكالة لتنسيق، إعداد وتنفيذ الإستراتيجية الوطنية للأمن السيبراني بهدف حماية المؤسسات الوطنية من التهديدات السيبرانية وضمان أمن البيانات والمعلومات (جنادي، 2024، صفحة 35)، تشتمل مهامها حسب المادة 20 من المرسوم إدارة لجنة توجيهية تضم مجلسا علميا بالإضافة إلى مركز وطني عملياتي لأمن الأنظمة المعلوماتية، إلى جانب مصالح تقنية وإدارية تحت إشرافها لضمان التنسيق والتنفيذ الفعال للإستراتيجية الوطنية (أ. فضيل و لحمل، 2023، صفحة 47). كما تم إنشاء في 2021 قطب قضائي مختص بالجرائم السيبرانية وهو ما يبرهن على الإهتمام المتزايد الذي توليه السلطات العمومية لمكافحة أشكال الإجرام الرقمي.

تولي المؤسسة العسكرية اهتماما كغيرها من المؤسسات الحيوية للدولة الجزائرية لتطوير قدرتها الدفاعية التقنية والعملياتية ضمن الفضاء السيبراني، وهو ما أكدته السيد الفريق أول السعيد شنقرية، رئيس أركان الجيش الوطني الشعبي: " الجزائر تعي جيدا أهمية الأمن السيبراني الذي أضى ضرورة حتمية، من أجل مواجهة كل أشكال المخاطر والتهديدات التي تستهدف الأنظمة الحساسة والحيوية للدولة بمنطق استباقي" (جنادي، 2024، صفحة 35) في هذا السياق تم إنشاء مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة التابعة لدائرة الاستعمال والتحصين لأركان الجيش الوطني الشعبي في نوفمبر 2015، بهدف تأمين وحماية الأنظمة والمنشآت الحيوية للبلاد ضد تهديدات الإرهاب السيبراني.

أكد السيد رئيس الجمهورية خلال اجتماع مجلس الوزراء المنعقد في 2 جويلية 2023 على " ضرورة إيلاء الأهمية لمسألة الأمن المعلوماتي، والتعاطي معها على أنها مسألة سيادة وطنية" (جنادي، 2024، صفحة 35)، كونها احتلت الجزائر المرتبة التاسعة عشر عالميا في قائمة الدول الأكثر تعرضا للهجمات السيبرانية ومحاولات الاختراق ضد المؤسسات الحساسة، بهدف التجسس وسرقة المعلومات حيث سجل أكثر من 70 مليون هجوم سيبراني في عام 2024، تم إحباطها بواسطة برنامج Kaspersky لمكافحة الفيروسات والإختراقات وحماية الأمن السيبراني (Samah، 2025، صفحة 478)

يظهر بوضوح أن السيادة الرقمية أصبحت عنصراً محورياً في تكيف العقيدة الدفاعية الجزائرية مع متطلبات الأمن السيبراني، فقد أضفت السيادة الرقمية بعداً جديداً لقدرة الدولة على التحكم في أنظمة المعلومات والبنى التحتية الرقمية، ما مكن الجزائر من تطوير آليات دفاعية متكاملة تضم تحديث الأطر القانونية، بناء كفاءات بشرية متخصصة، وتعزيز التعاون بين المؤسسات ما جعل الأمن السيبراني ركيزة أساسية ضمن العقيدة الدفاعية الجزائرية تضمن الحفاظ على استقلالية القرار الوطني، حماية المصالح الإستراتيجية وتعزيز القدرة على مواجهة التهديدات الرقمية المتنامية على الصعيدين الإقليمي و الدولي .

خاتمة:

تُظهر نتائج الدراسة أن التحول الرقمي لم يعد مجرد انتقال تكنولوجي بل تحولاً استراتيجياً أعاد تشكيل طبيعة القوة ومحددات الأمن في النظام الدولي. لقد غيّر هذا التحول من معادلة الصراع التقليدي، وجعل من الفضاء السيبراني ساحة جديدة للمواجهة حيث تتقاطع أدوات التكنولوجيا مع اعتبارات السيادة والأمن القومي. وضمن هذا السياق باتت السيادة الرقمية مفهوماً مؤسساً لإعادة تعريف السلطة والسيطرة في الدولة الحديثة، إذ ترتبط بقدرتها على إدارة بياناتها، التحكم في فضاءها المعلوماتي، وتأمين بنيتها التحتية الحيوية ضد التهديدات العابرة للحدود .

انطلاقاً من الإشكالية المطروحة، بينت الدراسة أن العقيدة الدفاعية الجزائرية استوعبت هذه التحولات البنيوية من خلال تبنيها لمنظور جديد للأمن، يقوم على دمج البعد السيبراني ضمن منظومتها الدفاعية الشاملة، وقد عبرت الاستراتيجية الوطنية للأمن السيبراني عن هذا التوجه بوضوح ، بإعتبارها أداة عملية لتكريس السيادة الرقمية، وتعزيز قدرة الدولة على التفاعل مع التهديدات الرقمية من موقع الفاعل، وبذلك انتقلت الجزائر من مقاربة أمنية تقليدية تركز على الدفاع المادي إلى مقاربة أمنية مركبة تمزج بين الأمن المادي والأمن المعلوماتي بين الردع العسكري والحماية التقنية .

غير أن هذا التطور وإن كان يعكس نضجا في التفكير الدفاعي الجزائري، يثير في المقابل إشكالية التوازن بين التعاون والإنكفاء، فالتعاون الدولي في المجال السيبراني أصبح ضرورة لتبادل المعرفة والتقنيات و مواجهة التهديدات الإرهابية الرقمية، لكنه في الوقت ذاته يطرح مخاطر محتملة تتعلق بسلامة المعلومات الاستراتيجية واحتمال التبعية التقنية، ومن هنا تبرز

الحاجة إلى صوغ معادلة تتعلق بسلامة المعلومات الاستراتيجية واحتمال التبعية التقنية، تحافظ على الإنفتاح التقني الضروري دون التفريط في جوهر السيادة الوطنية .

تأسيسًا على ماسبق يمكن تأكيد فرضية الدراسة التي تقيد بأن التحول الرقمي أسهم بشكل مباشر في إعادة تكييف العقيدة الدفاعية الجزائرية، على نحو يجعل من السيادة الرقمية ركيزة أساسية في تصورهما للأمن القومي، فالأمن السيبراني لم يعد هامشًا في هندسة الدفاع الوطني بل أصبح مكونًا بنيويًا في المنظومة العقائدية للدولة الجزائرية، يستند إلى رؤية شمولية تجعل من السيطرة على المعلومة أساسًا للسيطرة على القرار .

في ضوء هذه المعطيات يمكن إقتراح مجموعة من التوصيات العملية لتعزيز هذا التوجه الإستراتيجي :

1. ترسيخ البعد القانوني للسيادة الرقمية عبر تشريعات حديثة تنظم أمن الفضاء السيبراني وتضمن حماية البيانات ذات الطابع الاستراتيجي .
 2. تطوير القدرات الوطنية الذاتية في مجال البحث والابتكار السيبراني من خلال مراكز متخصصة داخل الجامعات ومؤسسات الدفاع .
 3. إقامة آلية تنسيق وطنية دائمة بين مؤسسات الدولة المعنية بالأمن السيبراني، لتقادي التشتت وضمان سرعة الإستجابة للأزمات الرقمية.
 4. تفعيل الدبلوماسية السيبرانية الجزائرية بما يسمح ببناء شراكات انتقائية تحفظ المصالح الأمنية وتساهم في بلورة قواعد دولية للتحرك في الفضاء السيبراني .
- إن مستقبل العقيدة الدفاعية الجزائرية يتجه نحو الرقمنة كخيار وجودي، يدمج الأمن المعلوماتي في صميم هندسة الأمن القومي، كون السيادة في عصر الشبكات ليست جغرافية فحسب بل رقمية أيضا، وحماية الدولة اليوم تمر عبر تأمين بياناتها ومعطياتها وشبكاتها. بذلك تغدو السيادة الرقمية امتدادا طبيعيا للسيادة الوطنية ورهانا مركزيا في بناء أمن وطني جزائري متجدد يواكب التحولات العالمية في بيئة التهديدات الجديدة .

• مراجع :

• المؤلفات:

1. Danial, V. (2011). *Cyberattaque et Cyberdéfense (Vol. 01)*. Paris: La voisier.

2. Friedman, P. a. (2014). *Cybersecurity and Cyberwar What Everyone Need to Know (01 ed.)*. New York: Oxford University Press.
3. libicqi, C. M. (2007). *Conquest in Cyberspace: National Security and information Warfare*. Cambridge: Cambridge University press.

• الأطروحات:

4. عمار بالة (2017-2018). التهديدات الأمنية في منطقة الساحل الأفريقي وتدابيرها على الأمن القومي الجزائري -مالي نموذجا -. أطروحة مقدمة لنيل شهادة دكتوراه في العلوم السياسية. كلية الحقوق والعلوم السياسية -جامعة باتنة 1-الجزائر, ص 297 .

• المقالات:

العربية:

5. أ فضل شريف , لحمل. أ, (فيفري, 2023) , الاستراتيجية الوطنية للأمن السيبراني ضمان حماية أنظمة معلومات, (715) ص ص 46-48 .
6. أ.جنادي (26 جانفي , 2024) , التحول الرقمي رهان سيادي .مجلة الجيش, (726) ص ص 33-35.
7. إدريس عطية, (ديسمبر 2019) مكانة الأمن السيبراني في منظومة الأمن الجزائري .مجلة المصادقية (01), 01, ص ص 100-123.
8. ب.عميور, (فيفري , 2023) , الدفاع والأمن السيبراني مقارنة متكاملة , مجلة الجيش, (715) ص ص 44-45.
9. عادل زقاغ , سفيان منصوري , (جانفي 2014) , أمن منطقة الساحل الأفريقي :بين المنظور الأمني الفرنسي والإستراتيجية الأمنية الجزائرية .المجلة الجزائرية للأمن والتنمية. (06), ص ص 50-81.
10. غنية حمام. س , (فيفري , 2023) , السيادة الرقمية قدرة الدول على التصدي للتهديدات السيبرانية. مجلة الجيش, (715) ص ص 52-54 .
11. يوسف .بن يزة , (15 ماي 2024) تقييم مسار التحول الرقمي في الجزائر . (2020-2023) , مجلة دراسات وأبحاث. (03) 16, ص ص 44-58

الأجنبية:

12. Samah, S. (2025). *Algeria's Cybersecurity Strategy: Defensive Techniques and Preventive Measures to Counter Cyber Threats*. *Journal of Al Naqad for Political Studies*, 09(01), 465-489.

• الوثائق الرسمية:

13. Council of Europe .(2001) .*Convention on Cybercrime Budapest Convention* Budapest: Council of Europe

• الملتقيات :

14. معصوم ,س & ,عزيب م. (2024) . التحول الرقمي في الجزائر, ضمن كتاب أعمال الملتقى الدولي حول السيادة الرقمية للدولة :سياسات وتجارب مقارنة , الجزائر :جامعة الجزائر 3 كلية العلوم السياسية والعلاقات الدولية, ص ص 105-119 .

• مواقع الأنترنت:

15. Doctrine. (n.d). Retrieved 09 7, 2025, from Toupictionnaire: [Le dictionnaire de politique: https://www.toupie.org/Dictionnaire/Doctrine.htm](https://www.toupie.org/Dictionnaire/Doctrine.htm)