

المناعة الرقمية كآلية لتعزيز سيادة الدولة في سياق القوة الحادة: الجزائر أنموذجا

Digital Immunity as a Mechanism for strengthening State Sovereignty in the Context of Sharp Power: Algeria as a Model

سرنيج جميلة^{*1}

المدرسة الوطنية العليا للصحافة وعلوم الاعلام، (الجزائر)،

djamsernih16@outlook.fr

<https://orcid.org/0009-0008-4803-7570>

تاريخ الاستلام: 31-08-2025 تاريخ القبول: 21-03-2026 تاريخ النشر: 2026-05-19

ملخص:

يهدف هذا البحث إلى تسليط الضوء على المناعة الرقمية كركيزة أساسية لتعزيز سيادة الدول في عالم يعرف تحديات وتهديدات متنامية من: تضليل إعلامي، هجمات سيبرانية وحروب نفسية عبر الفضاء الرقمي. والجزائر من الدول المستهدفة بهذه الممارسات في سياق القوة الحادة الرقمية، وتم استخدام المنهج الوصفي التحليلي لوصف جهود الجزائر وحرصها على بناء استراتيجية وطنية متكاملة لتعزيز مناعتها الرقمية وحماية أمنها السيبراني والحفاظ على حقها الكامل في ممارسة سلطتها على إقليمها وفضائها الرقمي وحرية اتخاذ قراراتها. تحققت من خلال الدراسة النتائج التالية: المناعة الرقمية تصون سيادة الدولة وتعدّ أداة استراتيجية للتصدّ لتهديدات القوة الحادة في الفضاء الرقمي عبر تكثيف الجهود المؤسسية، التقنية، القانونية، بالإضافة إلى نشر الوعي والتثقيف الرقمي بين أفراد المجتمع.

كلمات مفتاحية: المناعة الرقمية؛ السيادة؛ القوة الحادة؛ الفضاء الرقمي؛ الجزائر.

Abstract :

This research aims to shed light on Digital Immunity as a key pillar to strengthen the Sovereignty of States in a world that is known for its growing challenges and threats: disinformation, cyberattacks, and psychological warfare through the digital space. Algeria is one of the countries targeted by these practices in the context of Digital Sharp Sower, and by using the descriptive-analytical approach we describe Algeria's efforts to build an integrated national strategy to enhance its Digital Immunity, protect its cybersecurity, and preserve its full right to exercise its authority over its territory, its digital space and its freedom to make decisions. The study achieved the following results: Digital Immunity preserves the Sovereignty of the State and is considered a strategic tool to address the threats of Sharp Power in the digital space by intensifying institutional, technical, legal efforts, and digital education.

Keywords: Digital Immunity; Sovereignty; Sharp Power; Digital Space; Algeria.

* المؤلف المرسل.

مقدمة:

لا جدال في أنّ العولمة قد فرضت واقعا جديدا، تمّ من خلاله مراجعة العديد من المفاهيم في العلاقات الدولية وعلى رأسها كل ما يتعلق بالسلطة، النفوذ والسيادة، وذلك ارتباطا بتعدد وتنوع الفواعل على الساحة الدولية؛ فبعدما كانت الدولة الفاعل الوحيد والموحد في النظام الدولي، أصبح هناك فواعل غير دولية تعتبر هي الأخرى من أشخاص القانون الدولي والتي تؤثر في رسم السياسة الدولية؛ كذلك فيما يتعلق بمفهوم السيادة الذي لم يبق هو الآخر ثابتا أمام التغيرات التي عرفها النظام الدولي والتوجّه نحو التكتل والتعاون بين مختلف الفواعل مما خلق مصالح متشابكة عابرة للحدود.

فبعدما كنا نتكلم عن السيادة المطلقة وفق المنطق الواسطاني 1648، أصبحنا نتكلم عن السيادة المرنة ومن ثمّ الحديث عن السيادة الرقمية، خاصة امام التطور التكنولوجي السريع والهيمنة التكنولوجية التي باتت تفرض نفسها انطلاقا من اتصال العالم ككل بهذا الفضاء الرقمي المعقّد الذي أصبح ساحة للمواجهة الخفية وسبيل لإضعاف المناعة الرقمية للدول، بالتالي أصبح هذا الفضاء ساحة يتم من خلالها استهداف الخصم من خلال اختراق سيادته الرقمية، انتهاك خصوصيته وهويته السيبرانية، تتبّعه والمساس ببياناته الحساسة.

فبذلك يصبح " من يمتلك السيطرة على الفضاء الرقمي، يمتلك مفاتيح السيادة في القرن الراهن" ... ومن هذا المنطلق، لم يعد كافيا التوقّف عند حدود المنطق الواسطاني القائم على السيادة المطلقة للدولة في ادارة شأنها الداخلي (أي داخل إقليمها وحدودها السياسية والتي لا تخضع لإرادة أي دولة أخرى في الخارج) كافيا، لأنّ سيادة الدولة لا تنحصر في إقليمها المادي فحسب (الجوي، البري، البحري) بل تمتد إلى الفضاء الرقمي خاصة أمام الاختراقات الالكترونية والضغط الرقمي الذي تتعرض له الدول وعلى رأسها الجزائر في سياق ما يعرف اليوم بـ "القوة الحادة" واستغلال التطور التكنولوجي للتلاعب واختراق منظومتها السيادية. ومن هذا المنطلق، تحرص الجزائر كباقي الدول وتولّي أهمية كبيرة للأمن السيبراني وتعزيز المناعة الرقمية للدفاع عن سيادتها الرقمية والوطنية والتصدّ للهجمات السيبرانية.

وانطلاقا من أهمية تعزيز الجزائر لقدراتها ومناعتها الرقمية للدفاع عن سيادتها وحماية فضائها السيبراني من الاختراق المتعدد الأبعاد، نطرح اشكالياتنا كالآتي:

- كيف تساهم المناعة الرقمية في تعزيز سيادة الجزائر الرقمية، بالتالي حماية سيادتها الوطنية في ظل تنامي تهديدات القوة الحادة في الفضاء الرقمي؟

الأسئلة الفرعية:

- ما مدى تأثير تعزيز المناعة الرقمية في الجزائر على مستوى حماية سيادتها الرقمية؟
- ماهي أشكال القوة الحادة الرقمية المعتمدة ضد الجزائر؟
- هل تعدّ الجهود الجزائرية في بناء مناعتها الرقمية كافية لصون سيادتها الوطنية وفرض سيادتها الرقمية؟

فرضيات الدراسة:

- كلما تعززت المناعة الرقمية في الجزائر، ارتفع مستوى حماية سيادتها الرقمية.
 - تمّ الاعتماد على منصات التواصل الاجتماعي لاستهداف ثقة المواطنين الجزائريين في حكومتهم كأحد أشكال القوة الحادة الرقمية ضد الجزائر.
 - تساهم الجهود الجزائرية في تعزيز مناعتها الرقمية لحماية سيادتها الوطنية والرقمية، مع ضرورة الاستمرار في تطويرها لمواجهة تهديدات القوة الحادة المستقبلية.
- يهدف هذا البحث إلى طرح العلاقة بين المناعة الرقمية والسيادة الوطنية في ظل تهديدات القوة الحادة في الفضاء الرقمي لما لها من انعكاس على أمن واستقرار الدول واستقلالها في اتخاذ قراراتها السياسية؛ قمنا بتسليط الضوء على التجربة الجزائرية وجهودها المبذولة في مواجهة تهديدات القوة الحادة لبناء مناعة رقمية تعزّز سيادتها الرقمية وتصون سيادتها الوطنية. وكان ذلك باتباع المنهجية التالية:

1. السيادة والمناعة الرقمية: تأصيل مفاهيمي.
2. القوة الحادة في السياق الرقمي.
3. الجهود الجزائرية في بناء المناعة الرقمية كدرع واق للسيادة الرقمية والوطنية.

1.. السيادة والمناعة الرقمية: تأصيل مفاهيمي:

إن الدولة السيّدة هي ذلك الكيان السياسي الاجتماعي الذي يتمتّع دون غيره بحق احتكار القوة واستخدامها للحفاظ على النظام العام والاستقرار الداخلي للدولة وحماية سيادتها وتجانسها وتماسكها كوحدة واحدة وموحّدة من أي تهديدات أو أطماع خارجية.

الفرنسي جون بودان (Jean Bodin) يعدّ من المنظرين الذين لعبت اسهاماتهم دورا هاما في بلورة مبدأ السيادة الوطنية وفق المنطق الواسطالي، حيث عرّف السيادة عبر كتابه "Les Six Livres de la République": "السيادة هي السلطة العليا التي يخضع لها المواطنون ولا يحدّ منها القانون." (حمياز، 2017، ص.3)؛ أي السيادة مطلقة لأن الدولة تمارسها دون أي حدود أو قيود؛ وفي تيار السيادة المطلقة نجد توماس هوبز (Thomas Hobbes) الذي يدعوا إلى سلطة مطلقة للحاكم (فلاح، 2022، ص.166) غير قابلة للتجزئة، كما ينادي بالاستحواذ على المزيد من القوة. أما عن جون لوك (Jean Luc) وجون جاك روسو (Jean Jacques Rousseau) فيختلفان عنه؛ حيث أنّ لوك يرى أنّ السلطة ليست مطلقة بيد

الحاكم لأنّ الشعب هو الذي يختار من يمثله (سيادة الشعب) وله الحق في عزله وتغييره إذا لم يحترم القانون وحريات الأفراد وحقوقهم؛ بينما روسو يعتبرها كتعبير عن الإرادة العامة للشعب.

بعدما تطرقنا الى البعد القانوني للسيادة وكذلك البعد الفلسفي الاجتماعي الخاص بها، نقول أنّ السيادة هي حق الدولة الكامل في ممارسة سلطتها على اقليمها وشعبها وتعدّ ركنا أساسيا من أركان الدولة (إلى جانب الاعتراف المتبادل بالسيادة)؛ من المهم تسليط الضوء عن السيادة في العصر الحديث (عصر الثورة الرقمية) الذي يحمل أبعادا ومتغيرات جديدة خلقت عالما متشابكا ومختزلا للحدود بفعل العولمة، فلم يعد الحديث عن السيادة انطلاقا من الحدود السياسية المادية، بل امتدت إلى المجال الرقمي وهو ما فرض بروز اطار يضمن التحكم في الموارد والبنى التحتية المعلوماتية وحماية المعطيات الوطنية لضمان استقلال قرارات الدولة وقدرتها على التحكم في فضاءها السيبراني الذي يعتبر ساحة جديدة للحروب .

يعرّف تقرير لجنة التحقيق التابعة لمجلس الشيوخ الأمريكي السيادة الرقمية (Digital Sovereignty) بأنها: "قدرة الدولة على التصرف في الفضاء الإلكتروني، وهو شرط ضروري للحفاظ على قيمها التي تنطوي من ناحية على قدرة مستقلة على التقييم واتخاذ القرار والعمل في الفضاء الإلكتروني" (سنوسي، 2024، ص.4)؛ كما تشير إلى قدرة دولة أو كيان على ممارسة السيطرة على بياناتها وبنيتها التحتية وتقنياتها الرقمية الضرورية لحماية مصالحها الوطنية في الأمن والاقتصاد والقيم الثقافية والتمتع بالاستقلالية في مواجهة الفاعلين الأجانب في المجال الرقمي (سنوسي، 2024، ص.5)؛ كما تعبّر عن صلاحيات الدولة والتي تتمثل في الحفاظ على الاستقلالية والسيادة التكنولوجية بالإضافة إلى ضرورة حماية البيانات من أي سيطرة ورقابة. وعليه يمكن تقديم تعريف شامل للسيادة الرقمية بأنها: "قدرة الدولة وحققها في التحكم والسيطرة على فضاءها ومصيرها الرقمي (البيانات، البرامج، الأجهزة) الذي تعتمد عليه بطريقة مستقلة ودون هيمنة أجنبية" (ايجر، 2024، ص.75)؛ لأنّه في حال عدم تمكّن الدولة من التحكم في هذا الفضاء المعقّد وعجزها عن بناء مناعة رقمية لحمايته فستعرف أزمات متشابكة: كأزمة الهوية الوطنية بسبب سياسة التئيس التي تؤثر على روح الانتماء والولاء للوطن، أزمة الأمن والاستقرار بفعل الإرهاب الرقمي، أزمة الشرعية... الخ.

إنّ العمل على ايجاد سبل جديدة لتعزيز أمن تكنولوجيا المعلومات يمكّن الدول من بناء مناعة رقمية (Cyber Immunity) قادرة على مواجهة الهجمات السيبرانية، التضليل الإعلامي واختراق الفضاء الإلكتروني؛ أي بناء نهج أمني استباقي تلتجئ اليه الدول، المؤسسات والأفراد، قائم على حماية الأنظمة الرقمية، وبناء أنظمة مقاومة قبلية لتعزيز الصلابة الرقمية وفي نفس الوقت التصدي لمختلف التهديدات والهجمات السيبرانية دون الحاجة إلى التوقف عن العمل (العربية، 2023)، لأنّ مستوى الحماية عال بشكل يجعل من تكلفة الهجوم على الأنظمة الرقمية للدولة أكبر من تكلفة الضرر الذي يمكن أن تسببه، بالإضافة إلى ردع مجرمي الإنترنت بشكل يجعل الهجوم غير مربح على الأقل. (Pankov, 2019).

2.. القوة الحادة في السياق الرقمي:

القوة في العلاقات الدولية تعني القدرة على التأثير في سلوك الطرف الآخر للحصول على النتائج المرجوة؛ فهي وسيلة لممارسة النفوذ وتحقيق المصلحة الوطنية، كما تعدّ معياراً أساسياً لقياس مدى إمكانية الدول على التأثير في السياسة الدولية؛ فإذا سلطنا الضوء على القوة العسكرية نجد أن السعي الكبير للدول كان متمركزاً حول كسب القوة والمزيد من القوة للتفوق على الخصم (خاصة دول الجوار التي كانت تعتبر أول عدو لبعضها)، أو العمل على الحفاظ على وضعها القائم واللجوء إلى التعاون والتحالف الدولي في إطار السياسة الدفاعية؛ فمفهوم القوة تطوّر مع المدرسة الواقعية، والتي تبلور معها مفهوم القوة الصلبة (Hard Power) التي تركز على الأداة العسكرية، الإكراه، الضغط، والتي أضافت -الواقعية الجديدة- فيما بعد محددات أخرى للقوة كالاقتصاد والثروة. (حسن، 2024). وفي إطار التعاون والتكامل بين مختلف الفواعل الذي يعكس الجاذبية والاقناع بعيداً عن منطق القوة الصلبة والإكراه، نشير إلى ما يعرف بالقوة الناعمة (Soft Power) حيث يؤكد جوزاف ناي (Joseph Nye) عبر بحث قام بكتابته في مجلة "Foreign Affairs" تحت عنوان "كيف تشكّل القوة الحادة تهديداً ضد القوة الناعمة" عن صمود القوة الناعمة في السياسة الدولية، باعتبارها تشير إلى قابلية التأثير على الآخرين بجذبهم وإقناعهم بشكل أفضل مما يحدث عن طريق استخدام الإكراه والابتزاز (كات، 2018). أما عن القوة الذكية (Smart Power) فتكون بالجمع بين القوتين الصلبة والناعمة لكي تحقق الدولة أهدافها بكفاءة عالية.

اليوم أصبحنا نتكلم عن القوة الحادة (Sharp Power) والتأثير عبر التلاعب والاختراق -إعلامياً، ثقافياً، رقمياً- بدلاً من الاقناع أو الإكراه، وإحداث خلل في الجهة المستهدفة، وذلك من خلال عدة أدوات:

- التضليل الإعلامي ونشر الأخبار الكاذبة.
- الضغط الرقمي والابتزاز الإلكتروني.
- التجسس الرقمي وحرب المعلومات.
- التدخل في الانتخابات وتوجيهها (التي تعدّ مسألة داخلية تخص الدولة فقط).
- التسبّب في أزمات داخلية عن طريق التشكيك في مصداقية الحكام؛ استهداف العقول وخلق الانقسامات داخل المجتمع وإثارة النعرات الطائفية والقبلية؛ فالقوة الحادة كما يعرفها ناي؛ "تشير إلى الخداع في استخدام المعلومات لأغراض عدوانية" (كات، 2024).

فاذا كان سعي الدول نحو كسب القوة والمزيد من القوة لفرض نفوذها على الصعيد الدولي، فهي اليوم تستخدم القوة الحادة في سبيل تحقيق ذلك؛ كما تستخدمها بغية تشويه البيئة السياسية للدول (Walker, 2018). ففي نوفمبر 2017 ظهر مصطلح القوة الحادة عبر دراسة أكاديمية للباحثان كريستوفر وولكر وجيسكا... في مجلة "foreign affairs" بعنوان: "The meaning of Sharp Power ; How Authoritarian States Project Influence"، حيث تم تعريف القوة الحادة بأنها: "الاعتماد على الوعيّة، التهيب والضغط لاختراق الداخل (استخدام الأداة السياسية، الاقتصاد، الاعلام)، التأثير على القوى المؤثرة وعلى عملية صنع القرار" (Hoshang, 2021,p.3)؛ وهذه الدراسة كانت تركز بالأساس على

روسيا والصين ودورهما الدولي المتنامي ثقافيا وإعلاميا وقدرتهما على التأثير وتشكيل الرأي العام الدولي وأن ذلك ليس بقوة ناعمة بل هو قوة حادة.

بما أننا نعيش اليوم في عصر الأنترنت وعصر التطور التكنولوجي، فإنه من المهم الحديث عن القوة الحادة في السياق الرقمي واستغلال أدوات الإعلام الرقمي والمعلوماتي للتأثير الخفي على باقي المجتمعات، نظرا للتغيير الذي طرأ على العالم برمته ارتباطا بظهور الفضاء الإلكتروني والشبكة العنكبوتية وما لهم من تأثير في الحياة البشرية، ففرضوا وجودهم "كقوة إلكترونية" تقوم بتسيير العالم من خلال آحاد وأصفار مجهرية، وأصبح من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة هو الأكثر قدرة على التأثير في سلوك الفاعلين المستخدمين لهذه البيئة (خليفة، 2017). وهو الأكثر قدرة على إلحاق الضرر بالآخر؛ فالقوى الاستبدادية اليوم تعمل على التكيف مع الأساليب القمعية للعصر الرقمي لتمارس نفوذا أكبر في الخارج لإضعاف الدول، وتقويض سلامة مساحة المعلومات. وانطلاقا من منصة البحث «Sharp Power» لدينا خريطتان توضحان ذلك؛

خريطة رقم 1.

تبين نفوذ القوة الحادة خارج الحدود الوطنية، عبر قطاع الإعلام، التكنولوجيا.



المصدر: International forum for democratic studies (2025)

خريطة رقم 2

تبيين نفوذ القوة الحادة لكل من: الصين، روسيا، إيران، السعودية، الامارات العربية المتحدة في 143 دولة عبر العالم.



المصدر: (International forum for democratic studies (2025)

فانتشار مفهوم "القوة الحادة" (Sharp Power) في الدول الغربية وجد لوصف محاولات الاختراق الخارجي لمؤسسات صنع القرار والمجتمعات، وهو ما اعتبره بعض الخبراء "عودة لأجواء الحرب الباردة" والعداء بين القوى الكبرى (حمدون، 2018) بوسائل أخرى من ضمنها الوسيلة الإعلامية الرقمية؛ فالإعلام كوسيلة للقوة الحادة أصبح سلاح الدول ومختلف الفواعل الأخرى لنجاح قضيتها خاصة الاعلام الرقمي؛ حيث يقول جوزاف ناي (Joseph Nye) في هذا السياق: "المعارك لا تريح فقط في ميادين القتال، بل الراجح في الحرب هو ذلك الذي تريح قصته إعلاميا" وريح الحرب في هذا السياق يكون باللجوء الى التضليل الاعلامي، البروباغندا و الحروب النفسية والتلاعب بالمعلومة عبر الفضاء السيبراني وشبكات التواصل الاجتماعي، الاعتماد على الذباب الالكتروني لتضخيم الأمور، التلاعب بالمحتوى والاستغلال السلبي للذكاء الاصطناعي بنشر فيديوهات وصور مفبركة لتشويه الخصم. حيث انتقل فضاء الصراع من شكله التقليدي إلى الفضاء الرقمي الذي أصبح ذو ثقل جيوسراتيجي يتعلق بتدفق البيانات والمعلومات الهامة عبر العالم بشكل سريع، منخفض التكلفة وبتأثير كبير مع صعوبة الوصول الى مصدر التأثير؛ بالتالي أصبح هناك تكالب وصراع بين مختلف القوى الدولية من أجل السيطرة عليه لإلحاق الضرر بالطرف الآخر؛ حيث يعتبر التجسس، الهجمات السيبرانية، الدعاية الرقمية، الحرب النفسية للمعلومات، نشر الاخبار الزائفة والمضللة... الخ من أولويات الفواعل على الساحة الدولية من منطق "من يسيطر على الفضاء الرقمي يمتلك مفاتيح السيادة في العصر الحالي"؛ وكما يقول البروفيسور (Jaques Barrat): "في القرن الواحد والعشرين... أصبح هنالك تنافس من أجل السيطرة على المعابر الاستراتيجية، مصادر المعلومات والمعلومات ذاتها"؛ بالتالي السيطرة على محركات نقل المعلومة والبيانات - التي تمثل العالم الرقمي والفضاء السيبراني- من أوليات هذه الفواعل لريح الحرب السيبرانية.

3.. الجهود الجزائرية في بناء المناعة الرقمية كدرع واق للسيادة الرقمية والوطنية:

أمام التهديدات المتعددة والمتنوعة التي بات يحملها الفضاء الرقمي، ونظرا لتداعياتها على أمن وسيادة الدول؛ سارعت الجزائر كغيرها من الدول الى حماية فضاءها السيبراني Cyberspace⁽¹⁾ الذي يرتبط ارتباطا وثيقا بسيادتها الوطنية؛ فعملت على تعزيز مناعتها الرقمية وتقويتها لمواجهة أي شكل من أشكال التهديدات السيبرانية التي تستهدف أمنها واستقرارها الداخلي؛ وانطلاقا من ذلك، حرصت الدولة الجزائرية على تعزيز حضورها السيادي في عصر القوة الحادة "لجزائر صامدة سيبرانيا"، وذلك من خلال العمل على تطوير استراتيجية وطنية متكاملة في المجال الرقمي والجمع بين الاستباقية والوقائية؛ ويكون ذلك من خلال:

1.3.. حديد التهديدات السيبرانية:

التعرف على المخاطر التي تستهدف أنظمة الجزائر، أفرادها ومؤسساتها، والتي تختلف باختلاف مصدرها (من الداخل أو الخارج)، هدفها (اقتصاد الدولة، تجانسها المجتمعي، أفرادها)، وطبيعتها.

1.1.3.. الإرهاب السيبراني:

للإرهاب السيبراني تعاريف عديدة ومتنوعة، حيث يعرفه باري كولن (Barry Collin) بأنه يشير إلى استخدام الفضاء الإلكتروني كأداة لإلحاق الضرر بالبنية التحتية، والذي تكون أهدافه غالبا سياسية، وهو ذو طابع دولي عابر للحدود والقارات، وهجماته تتسم بالدقة والسرعة في ضرب الأهداف. أما مكتب التحقيقات الفدرالي الأمريكي فيعرفه: "بكونه هجوما متعمدا ضد أنظمة وبيانات الكمبيوتر بهدف التسبب في الضرر والدمار" (كواشي، 2023، ص.208).

كما يشير الإرهاب السيبراني الى استخدام الانترنت والفضاء الرقمي لنشر الفكر المتطرف والتحريض على العنف، وهو من أخطر التحديات الأمنية اليوم خصوصا وأنه في يد الجماعات المتطرفة والفواعل غير القانونية، لذلك تضعه الجزائر في مقدمة أولوياتها الأمنية، خصوصا وأن موقعها المحاط بدول تشهد نشاطا متناميا للتنظيمات الإرهابية على رأسها تنظيم "الدولة الإسلامية"، بوكو حرام وغيرها من التنظيمات والجماعات المتطرفة التي تعمل بالتنسيق مع بعضها في مختلف الدول الأفريقية على وجه الخصوص، والتي استغلت منصات التواصل الاجتماعي لزرع الفكر المتطرف واستقطاب الشباب -بما فيه الشباب الجزائري- وحثه على التجنيد عن بعد؛ كما تستغل هذه المنصات لإيقاظ الخلايا الإرهابية النائمة في المنطقة ككل. كما تعرضت الجزائر الى الإرهاب السيبراني في شكل هجمات سيبرانية من أجل شل القطاعات الحساسة فيها وتسريب البيانات وتعطيل الخدمات وزعزعة الثقة الداخلية؛ ففي سنة 2022 تم احباط ما لا يقل عن 29.7

* (1) يعرفه عبد القادر محمد فهي بأنه: «مجموع شبكات الحاسوب في العالم، وكل ما ترتبط به وتتحكم فيه هذه الشبكات، وهو لا يقتصر على شبكة الانترنت فقط وإنما يشمل العديد من شبكات الحاسوب الأخرى، فالفضاء الإلكتروني يشمل كل شبكات الحاسوب التي تدير نشاطات الدول ومؤسساتها ومرافقها وكل ما يتعلق ببيئتها الحيوية، وفي القطاعات المدنية والعسكرية" (زواوي، 2023، ص. 150)

مليون هجمة ضد الجزائر، منها أكثر من 19 مليون تهديد طال عناوين بريد إلكتروني جزائرية، كما منعت أكثر من 400 ألف هجوم ضار استهدف عناوين URL ، و34 ألف مسّ مضيفي عناوين URL ، إلى جانب تحديد وإيقاف أكثر من نصف مليون هجوم باستعمال برمجيات خبيثة (حويشة، 2022). وفي أبريل 2025 نشرت مجموعة للقرصنة من دولة مجاورة استهدافها لـ MGPTT الجزائر بغية سرقة بيانات حساسة؛ وامتد ذلك إلى غاية الجامعات الجزائرية؛ وكل محاولات الحاق الضرر بالجزائر سواء بتعطيل أنظمتها ومؤسساتها، أو عن طريق التجسس الإلكتروني لسرقة المعلومات، أو التهريب ونشر الفكر المتطرف... الخ يمكن تأويلها بالموقع المحوري للجزائر ومكانتها الهامة في المنطقة؛ والجزائر دائما في وضع الدفاع والتأهب.

2.1.3.. الحرب النفسية-الإعلامية-المجتمعية في الفضاء الرقمي السيبراني:

التي تستهدف التلاعب بالرأي العام وإضعاف تماسك النسيج الاجتماعي، بالإضافة إلى نشر خطاب الكراهية للمساس بوحدة الوطن والتسبب في أزمات داخلية (كما أشرنا في النقطة السابقة)؛ فإذا قدمنا أمثلة من الواقع فتكون حول الإشاعات وتضخيم الأحداث لنشر الهلع بين الجزائريين: كندرة المواد الغذائية وغيرها؛ كذلك السعي إلى أحداث الانقسامات الداخلية بين المناطق المختلفة بلهجاتها وعاداتها وثقافتها والتي تندرج ضمن غنى الجزائر في تنوعها ، والسعي نحو أحداث البلبلة عبر منصات التواصل الاجتماعي باستخدام الذكاء الاصطناعي للتلاعب بالرأي العام واستغلال الأحداث الحساسة، لكن تجانس المجتمع الجزائري وتفطنه لمثل هذه التلاعبات بالإضافة إلى حنكة صانع القرار منعت من حدوث ما كان مخطط له من قبل الأيدي الخارجية. بالإضافة إلى التشويش على المعلومة الصحيحة، تئيس الشباب الجزائري بهدف إضعاف الشعور بالانتماء للوطن وبالتالي ضرب الوحدة الوطنية، ناهيك عن حالات الاختراق وسرقة الهوية الرقمية وانتهاك الخصوصية الرقمية للمواطن الجزائري.

2.3.. وضع آليات الرقابة والرصد الناجعة لمواجهة التهديدات السيبرانية وضمان أمن فضائها الرقمي:

تكون من خلال:

أولا: المعالجة القانونية: نذكر منها:

- إصدار القانون 09-04 بتاريخ 5 أوت 2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها (حراي، 2022، ص.12). حق المراقبة الالكترونية والتدخل القضائي والتحقيق الرقمي، وضع آليات قانونية لمواجهة الجرائم السيبرانية.
- مرسوم رئاسي رقم 21-439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: اعتماد الجزائر على مجموعة من الأجهزة والهيئات لمكافحة الهجمات السيبرانية، منها:

- مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية للدرك الوطني (2008)

- المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني (2004)
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني
- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (قلاع الضروس، 2022).

ثالثا: الاستثمار في العنصر البشري: بتكوين خبراء أمن معلومات، تحليل وتشفير البيانات...

رابعا: حسن استغلال الأداة الاعلامية الرقمية في بناء الوعي وخلق ثقافة أمنية رقمية لدى الأفراد؛ فمثلا يمكن أن يكون الاعلام أداة القوة الحادة لتحطيم الطرف المستهدف، يمكن أن يلعب دورا إيجابيا بكونه خط دفاع أول ضد هذا النوع من الحروب التي تستهدف علاقة المواطنين بدولتهم، فيقوم الاعلام الرقمي بمحاربة جميع الاخبار المضللة، وكشف الهجمات الرقمية...الخ.

خامسا: التعاون الدولي والمحلي مع حرص الجزائر على اشراك المجتمع المدني بمختلف مؤسساته للتخفيف من المخاطر السيبرانية (حرابي، 2022، ص.10) في كل ما يتعلق برفع الوعي القانوني لدى مستخدمي الفضاء السيبراني بالجرائم السيبرانية.

خاتمة:

لأن الدولة التي لا تحمي فضاءها الرقمي تبقى عرضة للاختراق والتأثير الخارجي؛ ولأن الجزائر تؤمن بأنه كلما تعززت المناعة الرقمية ارتفع مستوى حماية سيادتها الرقمية، نجدها تركز اليوم على الاستثمار في كل هيئة رقابية أو بنية تحتية تكنولوجية من شأنها أن تقوّي هذه المناعة حرصا منها على ضمان أمنها واستقلالها في صنع واتخاذ قراراتها؛ ففي عالم يعرف تنوّع الحروب المعلوماتية (من حيث الفاعلين أو الأدوات المستخدمة) وتعدّد التهديدات السيبرانية (التضليل الإعلامي الممنهج عبر المنصات الرقمية للتأثير في الرأي العام وفي توجهاته وقناعاته، الهجمات السيبرانية لشل القطاعات الحساسة وتسريب البيانات وتعطيل الخدمات وزعزعة الثقة الداخلية، التجسس الإلكتروني...الخ)، تعمل الجزائر على مضاعفة جهودها لبناء مناعة رقمية قوية في مواجهة التهديدات الناجمة عن القوة الحادة الرقمية، حماية لسيادتها الوطنية وفرضا لسيادتها الرقمية.

يمكن تعداد النتائج التي خلصت إليها دراستنا كالاتي:

- ضرورة تكثيف التوعية والتثقيف الرقمي، مع الحرص على اشراك المجتمع المدني بمختلف مؤسساته للتخفيف من المخاطر السيبرانية.
- التحسيس بأهمية استخدام برامج حماية موثوقة والتحذير من البرامج الخبيثة كخطوة أساسية لتعزيز المناعة الرقمية وحماية السيادة الوطنية.
- أهمية تكوين خبراء أمن معلومات، محللو بيانات...إلخ

- الحاجة إلى تكثيف الندوات والملتقيات العلمية على مستوى الجامعات من أجل التوعية بمخاطر التهديدات في الفضاء السيبراني.
- يعدّ الاستناد إلى القانون وتجريم الهجمات الرقمية أولية قصوى لردع المعتدين على الفضاء الرقمي للدولة.
- وفي إطار هذه النتائج نوصي بتكثيف جهود الدول -وعلى رأسها الجزائر- في مجال الأمن الرقمي والعمل على بناء مناعة رقمية قوية التي تعتبر أساسا لضمان حماية السيادة الوطنية للدولة.

قائمة المصادر والمراجع:

1. المؤلفات / الكتب:

- حراي، الخطاب، (2022). حوكمة الامن السيبراني في الجزائر: نحو استراتيجية تعاونية للوقاية من المخاطر السيبرانية، كتاب جماعي، نسخة رقمية، على الرابط:
https://www.researchgate.net/publication/359511657_hwkmt_alamn_alsybrany_fy_aljza_yr_nhw_astratyjt_tawnyt_llwqayt_mn_almkhatr_alsybranyt
- خليفة، إيهاب، (2017). القوة الإلكترونية... كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت (ط1). العربي للنشر والتوزيع، مصر؛
- 2. الأبحاث في المجالات العلمية / المقالات:
- ايجر، أمينة. (2024). السيادة الرقمية في العالم المعلوم: التحديات والرهانات، مجلة الدراسات القانونية والسياسية، الجزائر، المجلد 10، العدد 2، ص.ص 71-83؛
- حسن، فاضل. (2024). القوة واستخداماتها في العلاقات الدولية: دراسة مستقبلية، مجلة الدراسات الاستراتيجية والعسكرية، برلين، العدد 25، ص.ص 68-101؛
- حمياز، سمير. (2017). إشكالية مفهوم السيادة الوطنية في ظل المتغيرات الدولية الراهنة، مجلة الآداب والعلوم الاجتماعية، الجزائر، المجلد 14، العدد 1، ص.ص 11-22؛
- زاوي، لمياء، رملي، فهم. (2023). التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر، المجلة الجزائرية للأمن والتنمية، الجزائر، المجلد 12، العدد 2، ص.ص 148-160؛
- سنوسي، علي. (2024). السيادة الرقمية والاستقلال التكنولوجي بين تحديات الظروف الوطنية والدولية، المجلة الجزائرية للحقوق والعلوم السياسية، الجزائر، المجلد 09، العدد 02، ص.ص 842-862؛
- فلاح، عبد الزهرة لازم. (2022). توماس هوبز رائد الفكر السياسي في الفلسفة الحديثة، مجلة كلية التربية، العراق، العدد 3، ص.ص 157-170؛
- قلاع الضروس، سمير. (2022). الأمن السيبراني الوطني: قراءة في أهم الإستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والإنسانية، الجزائر، المجلد 8، العدد 2، ص.ص 249-267؛
- كواشي، عتيقة. (2023). تداعيات الإرهاب السيبراني على الامن القومي الجزائري، المجلة الجزائرية للأمن والتنمية، الجزائر، المجلد 12، العدد 3، ص.ص 205-214؛

3. مواقع إلكترونية:

- العربية (28/3/2023)، هل تعرف ما هي "المناعة الرقمية"؟ إليك معلومات من ذهب عنها يوغين كاسبرسكي يدلي بمعلومات حول الأمن السيبراني ومستقبله، <https://www.alarabiya.net/technology/2023/03/28/%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D9%85%D9%86-%D8%B0%D9%87%D8%A8%D8%B9%D9%86%D8%A7%D9%84%D9%85%D9%86%D8%A7%D8%B9%D8%A9%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9> (15/8/2025، تاريخ التصفح)؛
- حمدون أحمد (16/8/2018)، تزايد ممارسات "القوة الحادة" في التفاعلات الدولية، المستقبل للأبحاث والدراسات المتقدمة، <https://futureuae.com/ar/Release/ReleaseArticle/596/sharp-power-%D8%AA%D8%B2%D8%A7%D9%8A%D8%AF%D9%85%D9%85%D8%A7%D8%B1%D8%B3%D8%A7%D8%AA-%D8%A7%D9%84%D9%82%D9%88%D8%A9-%D8%A7%D9%84%D8%AD%D8%A7%D8%AF%D8%A9-%D9%81%D9%8A-%D8%A7%D9%84%D8%AA%D9%81%D8%A7%D8%B9%D9%84%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9> (14/8/2025، تاريخ التصفح)؛
- كات عمار (29/1/2018)، العالم بين فكي تهديدات "القوة الحادة" و"القوة الناعمة"، <https://arabic.euronews.com/2018/01/29/soft-sharp-power-russia-china> (12/8/2025 تاريخ التصفح)؛
- Hoshang A. (2021). Sharp Power Theory in International Relations and its Employment in Countries' Foreign Policies, *Qalaai Zanist Scientific Journal*, p.p.696-734 ;
<https://sharppower.org/#map> (Consulté le, 15/8/2025) ;
- International forum for democratic studies(2025), Sharp Power RP,
- Pankov N. (26/9/2019). *Cyber-immunité appliquée : de quoi s'agit-il ?*, <https://www.kaspersky.fr/blog/applied-cyberimmunity/12361/> (Consulté le, 16/8/2025) ;
- Walker C.(07/2018). "What is Sharp Power?", *Journal of Democracy*, <https://www.journalofdemocracy.org/articles/what-is-sharp-power/>(Consulté le,16/8/2025)