مجلة القانون والعلوم البينية
ASJP Algerian Scientific Journal Platform
e ISSN 0744 – 2992 - ISSN2830-9804
المجلد : 05 -العـدد: 01(2026) ،ص11-34
https://www.asjp.cerist.dz/en/PresentationRevue/908

الأمن السيبراني كآلية لتعزيز الأمن القومي وحماية الخصوصية المعلوماتية

Cybersecurity as a mechanism for enhancing national security and protecting information privacy

شويحة إسراء سمية*[1]، كوفي هديل[2]، شلالي رضا[3]

[1] قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الجلفة (الجزائر)، issraachouiha@gmail.com

[2] قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الجلفة (الجزائر)، kofihadil@gmail.com

[3]قسم القانون العام، كلية الحقوق والعلوم السياسية، جامعة الجلفة (الجزائر)، chelali175@gmail.com

تاريخ الاستلام: 2025/10/18 تاريخ القبول 2025/12/15

ملخص:

تهدف هذه الدراسة إلى تحليل دور الأمن السيبراني كآلية لتعزيز الأمن القومي وحماية الخصوصية المعلوماتية، وذلك في ظل تزايد التهديدات الرقمية وتعقيداتها. اعتمدت الدراسة على المنهج الوصفي التحليلي لتوضيح المفاهيم الأساسية للأمن السيبراني وخصائصه، ثم إبراز أبعاده المتعددة السياسية والاقتصادية والعسكرية والثقافية، إضافة إلى استعراض التدابير التقنية والتنظيمية لتحقيقه. وقد خلصت النتائج إلى أن الجزائر تواجه تحديات بارزة في هذا المجال، أهمها ضعف التشريعات، نقص الكفاءات، وقصور البنية التحتية، مما يعيق فعالية منظومتها السيبرانية. ومن هنا توصي الدراسة بضرورة صياغة استراتيجية وطنية شاملة ترتكز على التكوين والتشريع والتعاون الدولي، بما يجعل الأمن السيبراني أداة لضمان السيادة الرقمية وتعزيز مسار التنمية المستدامة.

كلمات مفتاحية: الأمن السيبراني، الأمن المعلوماتي، التهديدات السيبرانية، الأمن القومي.

Abstract:

This study aims to analyze the role of cybersecurity as a mechanism for strengthening national security and protecting information privacy in light of the growing complexity of digital threats. The study adopts a descriptive-analytical approach to clarify the fundamental concepts and characteristics of cybersecurity, highlight its multidimensional aspects—political, economic, military, and cultural—and review the technical and organizational measures necessary to achieve it. The findings reveal that Algeria faces significant challenges in this field, most notably weak legislation, a shortage of expertise, and infrastructure deficiencies, which hinder the effectiveness of its cybersecurity framework. Accordingly, the study recommends the formulation of a comprehensive national strategy based on capacity building, legislative development,

CC BY NC

* المؤلف المرسل

and international cooperation, making cybersecurity an essential tool for safeguarding digital sovereignty and promoting sustainable development.
Keywords: Cybersecurity, Information Security, Cyber Threats, National Security.

1 مقدمة:

يشكّل الأمن السيبراني اليوم أحد المرتكزات الجوهرية لحماية سيادة الدول وضمان استقرارها في عالمٍ تتسارع فيه التحولات التكنولوجية وتتصاعد معه موجات التهديدات الرقمية. فقد انتقلت الهجمات الإلكترونية من كونها أعمالًا فردية معزولة إلى ظاهرة معولمة، تتجاوز الحدود الجغرافية والسياسية، مستهدفةً البنى التحتية الحيوية، والمؤسسات الرسمية، والمجتمعات على حد سواء. ولم يعد الأمن محصوراً في أبعاده العسكرية أو التقنية فحسب، بل أصبح فضاءً مركّبًا تتقاطع فيه الاعتبارات السياسية، والاقتصادية، والاجتماعية، والثقافية، وحتى القيمية، الأمر الذي يجعل بناء منظومة سيبرانية متكاملة وفعّالة ضرورةً استراتيجية لا غنى عنها.

وتنبع أهمية تناول هذا الموضوع من كون الأمن السيبراني أصبح عنصراً استراتيجيًا لا يقل أهمية عن الدفاع العسكري أو الاقتصادي، باعتباره خط الدفاع الأول في مواجهة التهديدات الرقمية المعقدة والعابرة للحدود. وتتجلى هذه الأهمية بوضوح عند النظر إلى واقع الأمن السيبراني في الجزائر، حيث يشكّل ركيزة أساسية لحماية الخصوصية المعلوماتية وضمان السيادة الرقمية في زمن تزايدت فيه المخاطر عالميًا. ومن هنا تبرز الإشكالية الجوهرية التي يسعى هذا المقال لمعالجتها والمتمثلة في التساؤل: ما هو الدور الأساسي والفعّال الذي يلعبه الأمن السيبراني في الحفاظ على خصوصيات الأمن القومي للدولة؟ وما هي الوسائل المتاحة لتحقيق ذلك في ظل تزايد التهديدات الرقمية وتعقيداتها؟

ومن هذه الإشكالية تنبثق عدة **تساؤلات فرعية** تسعى هذه الدراسة لمعالجتها، وهي:

1) ما مفهوم الأمن السيبراني وما أبرز خصائصه وأنواعه؟
2) كيف يساهم الأمن السيبراني في حماية الأمن القومي وتأمين البنية الرقمية للدولة؟
3) ما أهم التدابير التقنية والتنظيمية والتنموية اللازمة لتحقيق أمن سيبراني فعّال؟
4) ما أبرز التحديات والمعوقات التي تواجه الجزائر في تطبيق منظومة الأمن السيبراني وحماية الخصوصية المعلوماتية؟

المنهج المتبع:

تم الاعتماد على المنهج **الوصفي التحليلي**، باعتباره الأداة الأنسب لدراسة موضوع الأمن السيبراني، إذ يتيح توصيف المفاهيم المرتبطة به من جهة، وتحليل أبعاده، وتفسير علاقته بحماية الخصوصية المعلوماتية والأمن القومي من

جهة أخرى. كما ساعد هذا المنهج في استقراء الواقع الجزائري من خلال إبراز التحديات الراهنة والفرص المتاحة لبناء منظومة سيبرانية فعّالة.

استنادًا إلى الإشكالية المطروحة، سيتم تناول الموضوع وفق الخطة التالية:

1. مقدمة.

2. ماهية الأمن السيبراني.

نعريف الأمن السيبراني.

المفاهيم المرتبطة بالأمن السيبراني.

انواع وخصائص الأمن السيبراني.

4.2 عناصر وأهداف الأمن السيبراني.

3. أبعاد الأمن السيبراني والتدابير المتبعة لتحقيقه.

ابعاد الأمن السيبراني.

التدابير الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني وفق التشريع الجزائري.

4 التحديات المواجهة للأمن السيبراني في الجزائر.

2.1 عوائق بلوغ الأمن السيبراني في الجزائر.

2.1 تحديات الأمن السيبراني.

5. الخاتمة.

ماهية الأمن السيبراني.

1.2 تعريف الأمن السيبراني[1].

- **التعريف اللغوي والاصطلاحي:**

التعريف اللغوي: كلمة "السيبرانية" مأخوذة من كلمة "سايبر" (Cyber)، وهي صفة تُطلق على كل ما يرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي. فـــ"السيبرانية" تعني "فضاء الإنترنت"، وهي كلمة مشتقة من الكلمة اليونانية kybernetes، والتي ظهرت بداية في مؤلفات الخيال العلمي، وكان يُقصد بها "قيادة ربان السفينة".

التعريف الاصطلاحي: استُعملت كلمة "السيبرانية" (Cybernetics) بمفهومها الحديث لأول مرة من قِبل عالم الرياضيات الأمريكي Norbert Wiener (نوربرت وينر)، أستاذ الرياضيات في معهد ماساتشوستس للتكنولوجيا (MIT)، حيث أعطاها مفهومها الاصطلاحي الحديث عام 1948.

وقد استخدمها لوصف نظام "التغذية الراجعة" (Feedback) بهدف الاستفادة من مخرجات الأنظمة في ضبط مدخلاتها والتحكم فيها واستقرار أدائها.

- **التعريف القانوني والفقهي:**

- **التعريف القانوني الدولي للأمن السيبراني:**

يُعرف الأمن السيبراني في القانون الدولي كمجموعة من الوسائل والسياسات والإجراءات التي تهدف إلى حماية الأنظمة المعلوماتية والاتصالات الإلكترونية من التهديدات والاختراقات.

تعريف المشرّع الجزائري للأمن السيبراني: جاء في الفقرة الثالثة من المادة العاشرة من القانون رقم 18-04 أن الأمن السيبراني هو: "مجموع الأدوات والسياسات ومفاهيم الأمن، والآليات الأمنية، والمبادئ التوجيهية، وطرق تسيير المخاطر، والأعمال، والتكوين، والممارسات الجيدة، والضمانات، والتكنولوجيات، التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضد أي حدث من شأنه المساس بتوافر وسلامة البيانات المخزنة أو المعالجة أو المُرسلة."

- **التعريف الفقهي للأمن السيبراني:**

الأمن السيبراني هو مجموعة من الوسائل التقنية والتنظيمية والإدارية التي تُستخدم لمنع الوصول أو الاستخدام غير المصرح به، وسوء الاستغلال، وسرقة أو استرجاع المعلومات الإلكترونية، وأنظمة الاتصالات والمعلومات.

كما يهدف الأمن السيبراني إلى تعزيز حماية و سرية خصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

وبناءً عليه، يمكن تعريف الأمن السيبراني فقهيًا بأنه: "مجموعة من الإجراءات التقنية والتنظيمية والإدارية التي يتم استخدامها لمنه الدخول أو الاستخدام غير المصرح به، وسوء استغلال واسترجاع المعلومات الإلكترونية، وأنظمة الاتصالات والمعلومات، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، إضافة إلى اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من التهديدات والمخاطر في الفضاء السيبراني."

2.2 المفاهيم المرتبطة بالأمن السيبراني.

- **الفضاء السيبراني (Cyberspace):**

الفضاء السيبراني هو مجال افتراضي من صنع الإنسان، يقوم على استخدام أنظمة الحواسيب، وشبكات الإنترنت، وكمّ هائل من البيانات والمعلومات والأجهزة.

وقد عرّف بعض الباحثين الفضاء السيبراني بأنه "الذراع الرابعة للجيوش الحديثة"، إلى جانب البرّ والبحر والجو، نظرًا لما له من أهمية استراتيجية في الحروب الحديثة[2].

- **الجريمة السيبرانية (Cybercrime):**

هي فعل غير مشروع يصدر عن شخص أو مجموعة، ويستهدف أو يمس مصلحة أو حقًا متعلقًا بالمكونات المادية أو غير المادية للوسائل السيبرانية.

وقد اعتبر المشرّع هذا النوع من الأفعال جريمة يُعاقب عليها بموجب نصوص قانونية جنائية، باعتبار أن الاعتداء على تلك المكونات جريمة تشكّل تهديدًا للأمن العام والمجتمعي[3].

- **الهجمات السيبرانية:**

عرفها Michael-N-Schmir بأنها مجموعة من الإجراءات التي تتخذها الدولة من أجل مهاجمة نظم معلومات العدو، بهدف التأثير عليها وإلحاق الضرر بها، والدفاع عن أنظمة المعلومات الخاصة بالدولة المهاجِمة.

وقد عرّفها عبد القادر محمد فهيمي (Abdelkader Mohamed Fehimi) بأنها:"هجمات تُستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة أو من قبل فاعلين من غير الدول، لتعطيل كفاءة السيطرة والقدرة على

التحكم في منظومة شبكات الحاسوب، وما تتضمنه من بيانات ومعلومات للخصم، أو حتى تدميرها، سواء كان ذلك على مستوى منظومات القوة العسكرية، مما يشكل تهديداً جسيماً للأمن القومي للدولة"[4].

- **أمن المعلومات:** ينقسم أمن المعلومات إلى عدة زوايا رئيسية، نعرضها كما يلي[5]:

- **الزاوية الأكاديمية:**

أمن المعلومات، من المنظور الأكاديمي، هو علم يبحث في نظريات واستراتيجيات حماية المعلومات من المخاطر التي تهددها، ومنع الاعتداء عليها، أو الوصول غير المصرح به إليها، أو إهدارها. ويشمل هذا المفهوم الأدوات والإجراءات الضرورية لضمان حماية المعلومات من التهديدات الخارجية والداخلية.

- **الزاوية التقنية:**

في هذا الإطار، يُعنى أمن المعلومات بالبحث عن الوسائل والأدوات والإجراءات اللازمة لحماية المعلومات من المخاطر الداخلية والخارجية. ويعمل المختصون في هذا المجال على تطوير أفضل الطرق لضمان أمن المعلومات وتأمينها من مختلف أنواع التهديدات.

- **الزاوية القانونية:**

تتمثل في مجموعة الدراسات والتشريعات التي تهدف إلى حماية سرية وسلامة وتوافر المعلومات، ومكافحة الأنشطة الإجرامية التي تستهدف البيانات أو تستغلها في ارتكاب الجرائم. ويتجلى هذا البعد القانوني عملياً من خلال سن قوانين تجرّم الأفعال غير المشروعة التي تستهدف نظم المعلومات، وتحدد العقوبات المناسبة لها، كجرائم الحاسوب والإنترنت، بما يوفر الردع القانوني اللازم.

- **الحروب السيبرانية:**

الحروب السيبرانية هي سلسلة من الهجمات الإلكترونية التي تقوم بها دولة ما، أو مجموعة من الأفراد المدعومين من جهة معينة، لاختراق البنية التحتية المعلوماتية لدولة أخرى.

وتستهدف هذه الهجمات قطاعات استراتيجية مثل: الطاقة، الاتصالات، التجارة الإلكترونية، النقل، الخدمات الحكومية، والمالية، بغرض تحقيق أهداف سياسية، إجرامية، أو اقتصادية.

وقد أثبتت المستجدات والمتغيرات في موازين القوى ببعض المناطق التي تعرف أزمات أمنية، خاصة في منطقة الشرق الأوسط، أن هذه الهجمات غالباً ما توجه نحو المساس بالتطبيقات العسكرية في الفضاء السيبراني، كالتشويش

على أنظمة الرادار، وأجهزة الإنذار، وتعطيل شبكات الاتصال والمعلومات الرقمية، بين "دولة أ" و"دولة ب"، سواء بهدف التجسس أو إضعاف القدرات العسكرية أو التحضير لهجوم فعلي.وقد تكون هذه الهجمات أيضًا من طرف واحد فقط[6].

- **الإرهاب السيبراني:**

عرف جيمس لويس (James Lewiss)، الباحث في مركز الدراسات الاستراتيجية والدولية (CSIS)، الإرهاب السيبراني بأنه: "استخدام أدوات شبكات الحاسوب لتدمير أو تعطيل البنية التحتية الوطنية الحيوية، مثل الطاقة والنقل، أو بغرض ترهيب الحكومة أو المدنيين، ودفع الأمن نحو ارتكاب أعمال إرهابية باستخدام تقنيات تكنولوجيا المعلومات".وبهذا المعنى، يُعد الإرهاب السيبراني أداة تكنولوجية جديدة ضمن أدوات الإرهاب التقليدي.

وتكمن خطورته في قدرته على تجاوز الحدود الجغرافية والوطنية، والتأثير على الدول والمجتمعات دون الحاجة لوجود الإرهابيين فعليًا في نفس الدولة المستهدفة.

ويهدف الإرهاب السيبراني بشكل أساسي إلى: جذب الانتباه،

إثارة الفزع والخوف بين السكان المدنيين،

وإجبار الحكومات على تغيير سياساتها وفقًا لمطالب الإرهابيين[7].

- **العقيدة الأمنية:**

تمثل تصورًا شاملًا يحدد المنهجية التي تعتمدها الدولة في مقاربة أمنها، كما تحدد أفضل السبل والوسائل لتحقيق هذا الأمن. وتُعد مرجعية هذه العقيدة في العادة عبارة عن أطروحات نظرية صادرة عن الدول وصنّاع القرار فيها.

وقد تتخذ العقيدة الأمنية طابعًا أيديولوجيًا، إذا كانت نابعة من نظام فكري متجانس ومتناغم، يقدّم تفسيرات محددة للواقع.

ويترتب على ذلك أن تتبنى القوى النافذة في المجال الأمني هذه التفسيرات والرؤى، مما يوجّه السياسات الأمنية للدولة وفقًا لذلك[8].

3.2 أنواع وخصائص الأمن السيبراني.

- **أنواع الأمن السيبراني[9]:**

_ **أمن الشبكات** (Network Security): يوفر هذا النوع من الأمن السيبراني الحماية لأنواع شبكات الحاسوب المختلفة، سواء من التهديدات الداخلية أو الخارجية.

ويتم ذلك من خلال استخدام تقنيات متطورة لمنع الفيروسات والبرمجيات الخبيثة وسرقة البيانات.

كما يعتمد أمن الشبكات على مجموعة من البروتوكولات الأمنية التي تسمح فقط للمستخدمين المصرّح لهم بالوصول إلى الشبكات، مما يعزز من حمايتها.

_ **الأمن السحابي** (Cloud Security): يعتمد الأمن السحابي على تقنيات حماية البيانات المخزنة عبر الحوسبة السحابية، وهو جزء لا يتجزأ من الأمن السيبراني.

ويُعرّف الأمن السحابي بأنه: "مجموعة من السياسات، والتقنيات، والضوابط التي تعمل معًا لحماية البيانات والتطبيقات والخدمات التي تشكّل بيئة الحوسبة السحابية".

تشمل مهام الأمن السحابي:

- حماية البيانات.
- الفصل بين المهام والصلاحيات.
- حماية التطبيقات والأنظمة الحساسة.
- تمكين المستخدمين من مراقبة وتخزين بياناتهم بشكل آمن عبر حلول متقدمة.

_ **أمن التطبيقات** (Application Security): يقوم هذا النوع من الأمن على وضع التدابير والإجراءات اللازمة لحماية البرمجيات من الفيروسات ومحاولات الاختراق وسرقة المعلومات السرية.

ويهدف إلى إفشال أي نوع من الهجمات التي تستهدف التطبيقات البرمجية، وذلك باستخدام أدوات وبرامج حماية متعددة أثناء مراحل تطوير البرمجيات.

وفي السياق الجزائري، تسعى المؤسسات من خلال هذا النوع إلى حماية البيانات الحساسة، وخاصة في ظل التحول الرقمي المتسارع الذي تشهده الدولة.

4.2 عناصر وأهداف الأمن السيبراني

1.4.2 عناصر الأمن السيبراني

لتحقيق الأمن السيبراني بفعالية، لا بد من توفر مجموعة من الركائز والعناصر الأساسية التي تعمل بانسجام وتناسق، ويمكن تصنيف هذه العناصر إلى ما يلي:

- **العنصر التقني** (Technical Element):

تلعب التكنولوجيا دوراً بالغ الأهمية في حماية الأفراد والمنظمات من الهجمات السيبرانية. وتشمل الجوانب التقنية ما يلي:

- حماية الأجهزة الذكية والحواسيب.
- تأمين الشبكات باستخدام جدران الحماية.
- استخدام برامج مكافحة الفيروسات.

- **العنصر البشري** (Human Element):

يُعد العنصر البشري من أهم مكونات الأمن السيبراني، حيث تقع على عاتق مستخدمي البيانات والأنظمة في أي منشأة مسؤولية تطبيق مبادئ حماية البيانات الأساسية.

ويجب على الأفراد الالتزام بالتدابير التالية:

- استخدام كلمات مرور قوية ومعقدة يصعب اختراقها.
- تجنّب فتح الروابط والمرفقات المشبوهة الواردة عبر البريد الإلكتروني.
- إجراء نسخ احتياطية منتظمة للبيانات، لضمان استعادتها في حال وقوع أي هجوم سيبراني أو فقدان للمعلومات[10].

- **الأنشطة والعمليات** (Operations and Activities):

تُوظَّف الأفراد والتقنيات لتنفيذ أنشطة تهدف إلى تطبيق مبادئ الأمن السيبراني والتصدي للهجمات الإلكترونية بفعالية. وتشمل هذه الأنشطة ما يلي:

- **أمن الشبكات** (Network Security): حماية شبكات الاتصال من الاختراقات والهجمات باستخدام أنظمة دفاعية متطورة.

- **أمن التطبيقات** (Application Security): تأمين البرمجيات من الفيروسات والثغرات من خلال التحديثات والفحص المستمر.

- **أمن البيانات والمعلومات** (Data and Information Security): الحفاظ على سرية وسلامة البيانات ومنع التلاعب أو التسريب.

- **الأمن التشغيلي** (Operational Security): تأمين العمليات اليومية وضمان استمرارية الأداء دون انقطاع.

- **التعافي من الكوارث** (Disaster Recovery): وضع خطط مسبقة للاستجابة للأزمات واستعادة الأنظمة بسرعة.

- **استمرارية العمل** (Business Continuity): اعتماد تدابير لضمان استمرار الخدمات الحيوية أثناء الأزمات[11].

2.4.2 أهداف الأمن السيبراني:

تهدف استراتيجيات الأمن السيبراني إلى تحقيق جملة من الأهداف التي تُسهم في تعزيز الحماية الرقمية، وضمان سلامة واستمرارية الأنظمة والخدمات الرقمية. وفيما يلي أبرز هذه الأهداف[12]:

- **ترسيخ منظومة أمنية متكاملة:** لحماية البنية الرقمية بمختلف مكوناتها من أجهزة، وبرمجيات، وخدمات، وصون البيانات من أي تهديد أو اختراق، بما يضمن استمرارية الأداء وثقة المستخدم في الفضاء السيبراني.

- **تعزيز قدرات الحماية الرقمية:** لمواجهة الهجمات والحوادث السيبرانية التي تستهدف الأجهزة الحكومية ومؤسسات القطاعين العام والخاص، ويُعد ذلك ضرورة أمنية وطنية؛ إذ إن مثل هذه التهديدات قد تُخلّ باستقرار الأنظمة وتُعرض المعلومات الحساسة للخطر، مما يستدعي تطوير آليات دفاع متقدمة واستجابات مدروسة، بالاعتماد على بنى تحتية مؤمّنة وكفاءات متخصصة لضمان استمرارية الخدمات وسلامة البيانات.

- **تأمين بيئة رقمية موثوقة:** يُعد شرطًا أساسيًا لنجاح التعاملات في مجتمع المعلومات، حيث إن كل تبادل إلكتروني يتطلب حماية خصوصية البيانات وضمان سلامة المحتوى. ويُحقق ذلك عبر معايير أمنية دقيقة تُعزز الثقة بين الأطراف المتعاملة، وتمثل هذه الثقة دعامة رئيسية للتطور الرقمي المستدام.

- **صمود البنية التحتية الحساسة:** أمام الهجمات السيبرانية، يمثل عنصراً جوهرياً في حماية الأمن الوطني؛ فالقطاعات الحيوية مثل الطاقة، الصحة، النقل تعتمد على أنظمة رقمية معرضة للاستهداف. ومن الضروري اعتماد تقنيات متقدمة تمنح هذه البُنى القدرة على مقاومة الأعطال واستيعاب الصدمات الرقمية دون انهيار، مما يُسهم في استمرار الخدمات الأساسية دون انقطاع أو خلل.

- **الحد من الجرائم الإلكترونية:** من خلال توفير المتطلبات القانونية والتقنية الضرورية لحماية المستخدمين في البيئة الرقمية، وتقليل مخاطر الاختراق والاستغلال، بالإضافة إلى تحسين وعي الأفراد ضمن منظومة أمن معلومات شاملة ومتماسكة.

- **معالجة الثغرات الأمنية:** في أنظمة الحواسيب والأجهزة المحمولة تُعد أولوية، بهدف كشف الخلل البرمجي والنقاط الحساسة التي قد تُستغل في تنفيذ هجمات رقمية أو التسبب بخلل وظيفي. ويشمل ذلك التحديث المستمر للأنظمة وتطبيق اختبارات أمان ضرورية، مما يُسهم في بناء بيئة رقمية أكثر صلابة واستقراراً.

- **سد الثغرات في أنظمة أمن المعلومات:** وهو محور أساسي لحماية البنية الرقمية من الاستغلال والاختراق، ويُركّز على تحديد الفجوات الأمنية في البنية التحتية المعلوماتية والعمل على معالجتها قبل أن تتحول إلى تهديد فعلي. ويعتمد ذلك على أدوات فحص وتحليل متقدمة، تضمن الوصول إلى نظام معلوماتي متماسك من خلال يقظة تقنية مستمرة.

- **مواجهة البرمجيات الخبيثة:** من الركائز الأساسية لحماية البيئة الرقمية، حيث يُركّز هذا الهدف على كشف البرامج الضارة التي تهدف إلى التخريب أو سرقة المعلومات. ويتم استخدام تقنيات متقدمة لمنع تنفيذها وتقليل آثارها على المستخدمين، بما يضمن سلامة البيانات واستقرار الأداء.

- **توفير مستوى عالٍ من الأمان الرقمي:** بما يُراعي حقوق المستخدمين ويُقلل من المخاطر التي قد يتعرض لها المواطنون والمستهلكون أثناء التصفح أو تنفيذ معاملاتهم عبر الإنترنت، وذلك من خلال آليات حماية فعالة تغطي مختلف الاستخدامات الرقمية.

- **الارتقاء بوعي الأفراد وتطوير كفاءاتهم:** يُركّز هذا الهدف على رفع مستوى الوعي الرقمي وتطوير المهارات في التعامل مع التهديدات الإلكترونية، عبر تدريب الأفراد على أحدث الآليات والإجراءات التي تمكنهم من حماية أجهزتهم وبياناتهم من محاولات التلاعب أو الاستخدام غير المشروع.

2 أبعاد الأمن السيبراني والتدابير المتبعة لتحقيقه

1.3 أبعاد الأمن السيبراني

للأمن السيبراني أبعاد متعددة تمس السياسة والجيش والاقتصاد والمجتمع والقانون، وكل بُعد له أهميته في حماية الفضاء الرقمي.

- **البُعد السياسي:**

لم يسلم المجال السياسي من التهديدات والهجمات السيبرانية، والتي وصلت إلى حدّ الحروب السيبرانية وسباق التسلّح السيبراني وتبادل القرصنة في الملفات والقضايا الحساسة.

لقد أحدث الاعتماد على الفضاء السيبراني ثورةً في المفاهيم السياسية، مثل مفهوم القوة السيبرانية والردع السيبراني، كما أثّر في آليات التجسس بين الدول، حيث أصبحت تعتمد بشكل أكبر على القرصنة.

تُعتبر القرصنة اليوم من أهم الأدوات التي تستخدمها الدول للتجسس، وغالبًا ما تصل هذه الدول إلى المعلومات من خلال الثغرات الرقمية التي تسعى الحكومات والشركات لحمايتها.

إضافة إلى ذلك، تحاول بعض الجهات التأثير على الرأي العام عبر نشر الأخبار الكاذبة، وفي بعض الحالات، تحدث اختراقات لمواقع حكومية بالتزامن مع حملات ترويج إعلامية مغرضة.

- **البُعد العسكري:**

يُعد من أكثر الأبعاد التي تسعى الدول إلى تأمينها من خطر التهديدات السيبرانية؛ فقد أصبح الجناح العسكري يعتمد بشكل كبير على تقنيات الثورة التكنولوجية، سواء من حيث التواصل عبر الشبكات العسكرية، أو تبادل المعلومات والأوامر، أو إصابة الأهداف عن بُعد، أو إعداد الخطط الاستراتيجية.

تحقيق الأمن السيبراني في الجانب العسكري أصبح ضرورة ملحّة نظرًا لحجم الخطر الذي يمكن أن يُحدثه أي اختراق، مثل تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، أو حتى التحكم في بعض الأسلحة كالصواريخ الموجهة والطائرات دون طيار، وهو ما يُشكل تهديدًا خطيرًا للأمن القومي[13].

- **البُعد الاقتصادي:**

يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد، حيث يوجد تلازم واضح بين اقتصاد المعرفة وتوسيع استخدام تقنية المعلومات والاتصالات، إضافة إلى القيمة الكبيرة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كافة المستويات.

تلعب تقنيات المعلومات والاتصالات دورًا كبيرًا في تعزيز التنمية الاقتصادية للعديد من الدول، من خلال الاستفادة من الفرص التي توفرها الشركات الدولية والمؤسسات الكبرى، خاصة فيما يتعلق بإدارة تكلفة الإنتاج وتحقيق الكفاءة.

كما دخل العالم عصر المال الإلكتروني في بيئة متحركة بعد إطلاق الخدمات الإلكترونية، وأصبحت المصارف والمؤسسات المالية تستثمر بشكل متزايد في القطاع المالي الرقمي، وتتنافس الشركات في إصدار تطبيقات تتيح آليات دفع آمنة.

وقد دفعت هذه التطورات بعض الدول إلى سنّ تشريعات خاصة لحماية الأموال الرقمية، في ظل ما قد تثيره من تحديات مثل الجرائم المالية العابرة للحدود، كغسيل الأموال والتهرب الضريبي. فالأمن السيبراني يُسهم في ضمان تقديم الخدمات الإلكترونية بفعالية، ويعزز الإقبال عليها، مما يُترجم عمليًا إلى تطوير أسس اقتصاد سليم ومستدام.

- **البُعد الاجتماعي:**

تُساهم شبكات التواصل الاجتماعي، بشكل خاص، في فتح المجال أمام الأفراد للتعبير عن تطلعاتهم وطموحاتهم الاجتماعية، كما تُمكّن مختلف شرائح المجتمع من المشاركة في تطويره.

وتُتيح هذه الشبكات الفرصة للاطلاع على الأفكار والمعلومات، بما يُشكل حاجة لدى المجتمع للحفاظ على استقلال الفضاء الإلكتروني والمجتمع الذي يُبنى عليه.

كما أن انفتاح المجتمع على المجتمعات الأخرى يُؤسس لتبادل الخبرات وفتح آفاق جديدة للتعاون والتكامل.

- **البُعد القانوني:**

تُعد العلاقة بين القانون والتكنولوجيا علاقة تبادلية؛ فالتطورات التكنولوجية المتسارعة تفرض على التشريعات القانونية أن تواكب هذه التحولات عبر تنظيم الأعمال القانونية وغير القانونية في هذا المجال.لكن، وبصورة عامة، ما زالت الجريمة السيبرانية تفتقر إلى الأطر القانونية الصارمة للتعامل معها، ويرجع ذلك إلى عدة عوامل، من أبرزها:

- طبيعة الجريمة الإلكترونية نفسها.
- صعوبة تحديد هوية مرتكبي هذه الجرائم.
- مرونة التعريفات المرتبطة بتقنية المعلومات.

إضافة إلى ذلك، فإن الجرائم السيبرانية غير مقيدة بحدود جغرافية، مما يتطلب تفعيل التعاون الدولي المشترك لمكافحتها بفعالية[14].

2.3 التدابير الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني وفق التشريع الجزائري

سعى المشرّع الجزائري إلى مواجهة الإجرام الإلكتروني ومعالجة تطوراته الخطيرة من خلال سنّ مجموعة من القوانين، بدأها بتعديل قانون العقوبات بموجب القانون رقم 04-15، والذي تضمن أحكاماً خاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ثم تلاه القانون رقم 06-22، المعدل لقانون الإجراءات الجزائية، إضافة إلى القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وقد تم اتخاذ عدة تدابير يمكن تصنيفها على النحو الآتي[15]:

1.2.3 التدابير الموضوعية والتقنية للأمن السيبراني

اتبع المشرّع الجزائري نهج الدول المتقدمة، وخاصة فرنسا، حيث سنّ قوانين خاصة بتجريم السلوكيات الماسة بأنظمة المعالجة الآلية للمعلومات، مستهدفًا بذلك إجراءات محددة كما ورد في القانون 06-22، الذي تضمّن تدابير قانونية، ثم تلاه العمل على تدابير تقنية وإجرائية.

- **التدابير القانونية للأمن السيبراني:**

تأثر المشرّع الجزائري بما أفرزته ثورة المعلوماتية من أنماط إجرامية مستحدثة، مما استدعى تعديل قانون العقوبات بموجب القانون رقم 04-15، المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، حيث أُدرج القسم "السابع مكرر" تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، من المادة 394 مكرر إلى 394 مكرر 7، والتي تضمنت عدة جرائم.

وفي عام 2006، أُدخل تعديل آخر بموجب القانون رقم 06-23، حيث جُددت العقوبات المقررة لهذه الأفعال دون المساس بالنصوص التجريمية الواردة في القسم نفسه من قانون 04-15. ويُعزى هذا التعديل إلى تزايد الوعي بخطورة هذا النوع من الإجرام، بالنظر إلى تأثيره المباشر على الاقتصاد الوطني وانتشاره المتسارع.

كما أدرج المشرّع، بموجب القانون رقم16-02 المعدل والمتمم لقانون العقوبات، مادتين جديدتين هما:

- المادة 87 مكرر 11 التي استعملت عبارة "تكنولوجيات الإعلام والاتصال".
- المادة 394 مكرر 8 التي تضمنت مصطلحات مثل "مقدّم خدمات الإنترنت".

- **التدابير التقنية والإجرائية للأمن السيبراني**

أدرك المشرّع الجزائري أن مواجهة الإجرام الإلكتروني لا تكون فقط بوضع قواعد قانونية موضوعية ذات طبيعة ردعية، بل يجب أن تُرافقها تدابير وقائية وتحفظية، تسمح بتفادي وقوع الجريمة أو على الأقل كشفها في وقت مبكر للحد من آثارها. لذلك، تضمّن القانون رقم 06-22 عدة إجراءات منها:

- التحري في الجرائم المتلبس بها.
- التحقيق في الجرائم الإلكترونية.
- اللجوء إلى إجراءات اعتراض المراسلات السلكية واللاسلكية.
- تسجيل المحادثات والأصوات والتقاط الصور.
- الاستعانة بكافة الترتيبات التقنية اللازمة لكشف ملابسات الجريمة وإثباتها.

كل هذه الإجراءات لا تخضع بالضرورة لقواعد التفتيش والضبط التقليدية، إلا أن المشرّع لم يُطلق العنان لاستعمالها دون قيود، بل أحيطت بمجموعة من الضمانات القانونية التي تهدف إلى الحد من تعسف السلطات وضمان حماية الحقوق والحريات العامة، لاسيما الحياة الخاصة للأفراد.

2.2.3 التعاون الدولي والتدابير الهيكلية لفاعلية الأمن السيبراني

- **التعاون الأمني الدولي:**

يُعد التعاون الأمني الدولي ضرورة حتمية لمواجهة الجرائم الإلكترونية، حيث أثبت الواقع العملي أن أي دولة بمفردها لا تستطيع التصدي لهذا النوع من الإجرام بالنظر إلى تطوره السريع والعابر للحدود.

لذا، أصبحت الحاجة ماسة إلى وجود كيان دولي يُشرف على التنسيق والتعاون بين أجهزة الشرطة في مختلف الدول، خاصة في ما يتعلق بـــ:

- تبادل المعلومات حول الجرائم والمجرمين بأقصى سرعة.

- تعقب المجرمين الفارين من وجه العدالة.

- دعم التحقيقات المشتركة في القضايا السيبرانية.

هذا التعاون الدولي يُعدّ ركيزة أساسية لتعزيز فعالية الأمن السيبراني ومكافحة الجرائم الإلكترونية على المستوى العالمي.

- **المساعدة القضائية الدولية وتحديث آليات التعاون الدولي في المادة الجنائية:**

يبدأ تحديث آليات التعاون القضائي الدولي في المادة الجنائية بخطوة أولى تتمثل في ضرورة تطوير القوانين الوطنية لتكون أكثر شمولية ومرونة، حتى تواكب الحركة التشريعية الدولية في مجال مكافحة الجريمة، وتعزز التعاون بين الأجهزة التنفيذية للدول، وإنشاء هيئات متخصصة لمواجهة الجريمة المنظمة.

كما يجب بناء نظرية متكاملة تستفيد من التطور التكنولوجي في إجراءات جمع الأدلة وتبادل المعلومات، بهدف التصدي للمنظمات الإجرامية التي تعتمد على أساليب علمية ومنهجية لإخفاء الأدلة والتخلص منها.

وهذا يستدعي تطوير التعاون القضائي في مختلف مراحله، بما في ذلك مرحلة تنفيذ الأحكام.

- **تكريس المشرع الجزائري لمبدأ التعاون الدولي في مكافحة الأمن السيبراني:**

أكد المشرّع الجزائري التزامه بالتعاون الدولي في هذا المجال، حيث نصّت المادة 16 من القانون 09-04 على أنه:> "يمكن للسلطات القضائية المختصة تبادل المساعدة القضائية على المستوى الدولي في إدارة التحقيقات والتحريات المتعلقة بالجرائم الإلكترونية، وذلك لجمع الأدلة المتعلقة بها".

ويأتي هذا النص في ضوء الصعوبات التقنية البالغة التي تطرحها هذه الجرائم المستحدثة من حيث كشفها، إثباتها، وملاحقة مرتكبيها، حيث لا يمكن لدولة واحدة بمفردها التصدي لها.

ونظرًا لحالة الاستعجال التي تتطلبها إجراءات التحقيق لجمع الأدلة في مثل هذه القضايا، أقر المشرّع قبول طلبات المساعدة القضائية حتى وإن وردت عبر وسائل الاتصال السريعة، مثل البريد الإلكتروني أو الفاكس، شريطة التأكد من صحتها فقط، وذلك احترامًا لمبدأ سيادة الدول، وبناءً على مبدأ المعاملة بالمثل، كما نصت عليه المادة 17 من نفس القانون.

من الثابت أنه لا يمكن لأي دولة، مهما بلغت من تقدم في مجال الأمن السيبراني، أن تواجه بمفردها الإجرام السيبراني. ولذلك، فإن السبيل الفعّال لمكافحة هذا النوع من الإجرام هو انتهاج التعاون الدولي، وخاصة القضائي. وقد نصت على هذا التعاون عدة اتفاقيات دولية وإقليمية، من أبرزها:

- اتفاقية بودابست لمكافحة الجريمة السيبرانية لسنة 2001، التي تُعتبر ذات طابع دولي رغم أنها إقليمية، وتُعدّ مرجعًا رئيسًا للدول في صياغة سياسات التصدي للتهديدات السيبرانية.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، والتي أكدت بدورها على أهمية التعاون الدولي في هذا المجال.

3.2.3 التدابير الهيكلية لفعالية الأمن السيبراني:

انطلاقًا من حرصه على مكافحة الجريمة السيبرانية، أنشأ المشرّع الجزائري عدة هياكل مؤسساتية متخصصة، من أبرزها:

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:** تم تأسيس هذه الهيئة بموجب المادة 13 من القانون 04-09 المؤرخ في 5 أوت 2009، وقد حدّد المرسوم الرئاسي رقم 21-439 تشكيلتها وتنظيمها وكيفيات سيرها، كما أُلحق الإشراف عليها برئاسة الجمهورية.

  أهم اختصاصاتها كما وردت في المادة 4 من المرسوم:

  - الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
  - مكافحة هذه الجرائم بكافة أشكالها.
  - تبادل المعلومات مع الدول الأخرى من أجل تعزيز التعاون الدولي والمساعدة القضائية.

- **الهيئات القضائية الجزائية المتخصصة:** وُجدت هذه الهيئات بموجب القانون رقم 14-04 المؤرخ في 10 نوفمبر 2014، ويُقصد بها الأقطاب الجزائية المتخصصة.

وقد خُصصت بموجب المواد 37، 40 و327 من قانون الإجراءات الجزائية للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى المخولة لها بموجب القانون.

- **جهازي الأمن الوطني والدرك الوطني:** قامت مديرية الأمن الوطني وجهاز الدرك الوطني بإنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، كما تم تكوين عناصر متخصصة في هذا المجال، سواء داخل الوطن أو خارجه.

ويتوفر كلا الجهازين على مخبرين علميين تابعين للشرطة العلمية والتقنية، مزودين بأحدث الأجهزة والتكنولوجيات اللازمة لكشف هذا النوع من الإجرام.

- **المعهد الوطني للأدلة الجنائية وعلم الإجرام:** يتكون المعهد من 11 دائرة متخصصة في مجالات متعددة، وتُعنى هذه الدوائر بإنجاز الخبرات وتقديم الدعم الفني والتقني. وتتولى دائرة الإعلام الآلي والإلكتروني تحديداً مسؤولية:

  - معالجة وتحليل الأدلة الرقمية.
  - تقديم المساعدة الفنية للمحققين أثناء المعاينات الميدانية.
  - دعم العدالة بكافة الأدلة التقنية اللازمة في مجال الجرائم السيبرانية.

يتضح من خلال ما سبق أن الجزائر، بتشريعاتها الموضوعية، الإجرائية، والإجرامية، تسعى جدياً إلى مواجهة هذا النوع المستحدث من الإجرام بمختلف الوسائل والأساليب، دون المساس بحقوق الإنسان التي كرسها دستور 2020، خاصة في ما يتعلق بحماية الحياة الخاصة وضمان كرامة الفرد، بما يضمن تكفلًا فعّالًا بحياة كريمة ومصونة لكل المواطنين.

3 التحديات المواجهة للأمن السيبراني في الجزائر

1.4 عوائق بلوغ الأمن السيبراني في الجزائر

تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن الإلكتروني، ويمكن ذكر أهمها فيما يلي[16]:

- **زيادة عدد المشتركين في شبكة الإنترنت:** تجاوز عدد المشتركين في شبكة الإنترنت في الجزائر أكثر من 10 ملايين مشترك، ومع زيادة عدد مستخدمي الشبكة، تتضاعف المخاطر، مما يجعل عملية اكتشاف هوية مرتكبي الجرائم الإلكترونية تحدياً حقيقياً، بسبب صعوبة البحث والتحري وسط هذا العدد الهائل والمتزايد باستمرار.

- **انتشار تكنولوجيا الإنترنت فائقة السرعة والتدفق:** أدى التطور التكنولوجي السريع إلى تسهيل تنفيذ الجرائم الإلكترونية في وقت وجيز، ما يضع الجهات الأمنية المختصة أمام تحدي سرعة مباشرة التحقيقات، ومتابعة الجناة، والتسلح بالأجهزة المتطورة والبرامج الحديثة ذات الأداء العالي.

- **ظهور الإنترنت اللاسلكي (Wi-Fi، G3، G4):** لم يعد المجرم بحاجة إلى الجلوس خلف حاسوب موصول سلكيًا بشبكة الإنترنت لارتكاب جريمته، مما يستدعي من الجهات الأمنية الاستعداد بأحدث التقنيات لمواجهة هذه التطورات.

- **الاستخدام الواسع لوسائل التواصل الاجتماعي:** بلغ عدد مستخدمي مواقع التواصل الاجتماعي في الجزائر أكثر من سبعة ملايين مستخدم، ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الإلكترونية، مثل القذف، التحرش الجنسي، واستغلال القُصّر، وغيرها.

وهذا يتطلب وضع استراتيجيات محكمة لضمان الأمن السيبراني عند استخدام هذه المنصات.

- **عملية التخفي أثناء استخدام خدمات الإنترنت** (مثل: Proxy): تُعد من أكبر الإشكاليات التي تواجه الجهات المختصة بالتحقيق، وتتطلب تعاون جهات متعددة، والتزود بوسائل متطورة قادرة على رصد التفاصيل الدقيقة، وفك الشيفرات، وتطوير البنية التحتية المعلوماتية، وتحديثها باستمرار، وتصميم برامج عالية الكفاءة.

- **غياب التنسيق بين الدول والحكومات:** الجريمة الإلكترونية جريمة عابرة للحدود والقارات، حيث يمكن لمرتكب الجريمة النفاذ إلى أنظمة الحواسيب في دولة ما، لتنفيذ التلاعب أو اختراق البيانات في بلد آخر، وتسجيل النتائج في بلد ثالث، بل وتخزين الأدلة في بلد رابع.

هذا التوزيع يساعد المجرم الإلكتروني على إخفاء هويته واستغلال الموارد من خلال قنوات موجودة في دول مختلفة.

وبفضل قدرته على التنقل إلكترونيًا بين الشبكات والنفاذ إلى قواعد البيانات في قارات مختلفة، تتعدد الجهات القضائية والقوانين التي يجب التعامل معها، مما يشكل تحديًا كبيرًا.

لذلك فإن مكافحة الجريمة الإلكترونية بشكل فعّال، تقتضي تعاونًا دوليًا سريعًا، فعّالًا، وعلى أعلى درجات التنسيق.

- **التطور التكنولوجي المستمر في مجالي الإنترنت والاتصال:** يفرض هذا التطور المتسارع على الأجهزة الأمنية المختصة مواكبته، سواء من حيث اقتناء التكنولوجيا المناسبة أو من حيث التمكن من استخدامها واستثمارها بالشكل الأمثل.

غير أن هذا قد يُرهق الميزانيات المحدودة، ولذلك يتوجب توفير كل الإمكانيات المادية، المالية، والبشرية اللازمة لضمان أمن سيبراني فعّال.

– **نقص الوعي بمفهوم الأمن السيبراني:** يُعد نشر الوعي لدى مستخدمي شبكة الإنترنت أمراً بالغ الأهمية، ويتطلب القيام بحملات توعوية تدعو المستخدمين إلى اتخاذ التدابير اللازمة لضمان الحد الأدنى من الأمان، وتعليمهم آليات التشفير والاحتياطات الواجب اتخاذها عند استخدام وسائل التواصل الاجتماعي.

كما ينبغي تعزيز ثقافة التبليغ عن الجرائم الإلكترونية في الوقت المناسب، لتمكين الجهات المعنية من القيام بدورها بفعالية وكشف مرتكبي الجرائم.

– **ضعف تفعيل القوانين على أرض الواقع:** من أبرز الإشكالات التي تُسهم في انتشار الجريمة الإلكترونية هو الإفلات من العقاب، والتأخر في تطبيق القوانين.

كما يجب أن تتكيف النصوص القانونية مع المستجدات التقنية في هذا المجال، وينبغي إنشاء محاكم متخصصة في الجرائم الإلكترونية نظراً للانتشار الواسع لهذا النوع من الجرائم.

2.4 تحديات الأمن السيبراني

لقد واجه الأمن السيبراني العديد من التحديات المتنوعة، ما يؤكد أن الخطر السيبراني لا يساوي صفراً، ولا يمكن تحقيق أمن سيبراني بنسبة 100%. ومن بين هذه التحديات[17]:

– **العنصر البشري:** يُعتبر العنصر البشري من أخطر التحديات في مجال الأمن السيبراني، ويتجلى ذلك فيما يلي:

- صعوبة التحكم في ردود الفعل العاطفية.
- تعقيد السياسة الأمنية لاعتمادها على قرارات بشرية.
- أنظمة الأمن تُصمم وتدار من قبل الإنسان، وبالتالي فهي عرضة للأخطاء أو لسوء الاستخدام.
- حتى الأنظمة أو التطبيقات الموثوقة يمكن أن تتعرض لهجوم من قِبل مستخدمين ينتهكون الحقوق.

– **نقص الكفاءات البشرية المتخصصة:** يُعد نقص المتخصصين في مجال أمن المنظومات تحدياً حقيقياً للشركات والمؤسسات، إذ تُخاطر هذه الأخيرة باستخدام أدوات وأشخاص غير مؤهلين بشكل كافٍ.

– **ثغرات التشفير وكلمات المرور:** رغم اعتماد أنظمة التشفير، إلا أن لها نقاط ضعف، وقد يتم اختراقها باستخدام كلمات مرور قابلة للكسر.

– **الابتكار في خدمة الهجمات السيبرانية:** تستغل بعض الأطراف الابتكارات التقنية في تطوير هجماتها، ولهذا يجب أن تتكيف أساليب المراقبة التقليدية مع التهديدات الحالية والمستقبلية.

– **ظهور تقنيات جديدة = نقاط ضعف جديدة:** كل تقنية جديدة قد تُنتج ثغرات أمنية جديدة. وحتى الشركات التي تمتلك موارد جيدة تجد نفسها مُجبرة على تطوير دفاعاتها باستمرار.

– **توسع رقعة الهجوم السيبراني:** يعود ذلك إلى الارتفاع الكبير في عدد الأجهزة المتصلة بالإنترنت، وكذا عدد مستخدمي الشبكة من جهة، بالإضافة إلى التهديدات المتبادلة بين الدول، مما أدى إلى تصاعد عدد الحروب السيبرانية والتجسس السيبراني من جهة أخرى.

الخاتمة:

لقد تناولت هذه الدراسة موضوع الأمن السيبراني من خلال التطرق إلى مفهومه ومقوماته، ثم تحليل أبعاده والتدابير المتبعة لتحقيقه، وصولًا إلى رصد أبرز التحديات التي تواجه الجزائر في هذا المجال. ومن خلال هذا المسار، تبيّن أن الأمن السيبراني لم يعد مجرد خيار تقني، بل أصبح ركيزة أساسية لضمان استقرار الدول وتعزيز أمنها القومي في عالم تتزايد فيه المخاطر الرقمية تعقيدًا وتطورًا. فهو يمس مختلف الأبعاد السياسية والاقتصادية والعسكرية والثقافية، مما يجعله حاضرًا في صميم السياسات الوطنية.

وقد خلصت الدراسة إلى أن واقع الأمن السيبراني في الجزائر يكشف عن تحديات متشابكة، أبرزها ضعف البنية التحتية، نقص الكفاءات، والقصور التشريعي، على الرغم من وجود بعض التدابير التقنية والتنظيمية التي تسعى الدولة لاعتمادها. وبذلك يمكن القول إن الأهداف المسطرة لهذه الدراسة – والمتمثلة في توضيح المفاهيم الأساسية للأمن السيبراني، إبراز دوره في حماية الأمن القومي، وتحليل التحديات التي تواجه الجزائر – قد تحققت من خلال ما تم عرضه.

وفي ضوء ذلك، يتضح أن الأمن السيبراني يشكّل خط الدفاع الأول عن السيادة الوطنية والخصوصية المعلوماتية، وأن تحقيق منظومة سيبرانية فعّالة يتطلب صياغة استراتيجية وطنية شاملة ترتكز على التكوين والتشريع والتعاون الدولي، بما يجعل الاستثمار فيه خيارًا استراتيجيًا لضمان التنمية والاستقرار في عصر الرقمنة.

التوصيات:

1. بلورة إستراتيجية وطنية متكاملة للأمن السيبراني، تستند إلى رؤية استشرافية تأخذ بعين الاعتبار التحولات الجيوسياسية والرقمية.

2. إرساء منظومة تشريعية متطورة قادرة على ضبط الفضاء السيبراني، وحماية المعطيات الشخصية، ومكافحة الجرائم الإلكترونية.

3. تعزيز القدرات البشرية من خلال تكوين نخب متخصصة في الأمن المعلوماتي، وتطوير كفاءات تقنية قادرة على مجابهة التهديدات المستحدثة.

4. تحديث البنية التحتية الرقمية وتزويدها بالوسائل التكنولوجية المتقدمة، بما يضمن صمودها أمام الهجمات السيبرانية المعقدة.

5. توسيع مجالات البحث العلمي والابتكار في ميدان الأمن السيبراني، مع ربطه بالتنمية الوطنية وبناء اقتصاد معرفي تنافسي.

6. تطوير الوعي المجتمعي الرقمي عبر برامج توعوية وتربوية، لترسيخ ثقافة الاستخدام الآمن والمسؤول للتكنولوجيا.

7. تعزيز التعاون الإقليمي والدولي من خلال اتفاقيات وشراكات استراتيجية لتبادل الخبرات وبناء آليات مشتركة للتصدي للمخاطر العابرة للحدود.

5. قائمة المراجع:

- **البحوث الجامعية:**

1. بوزادية جمال ، "الأمن السيبراني"، محاضرات مقدمة لطلبة ماستر2،تخصص دراسات أمنية وإستراتجية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2021.
2. شاري خيرة ، صادقي إيمان، "الأمن السيبراني وأثره في تحقيق الأمن القومي"، مذكرة ماستر غير منشورة، جامعة محمد البشير الابراهيمي-برج بوعريريج، 2023.
3. الدام محمد ، "الأمن السيبراني"، مذكرة ماستر غير منشورة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه محمد لخير-الوادي-، 2023.

- **المقال المنشور:**

1. بارة سمير، "الأمن السيبراني في الجزائر: السياسات والمؤسسات"، المجلة الجزائرية السيبراني، جامعة قاصدي مرباح، ورقلة، العدد 04، 2017.
2. بوقرص ساعد، "الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات استراتيجية خاصة"، مجلة الأبحاث في الحماية الاجتماعية، جامعة العلوم والتكنولوجيا هواري بومدين، الجزائر، المجلد 03، العدد 03، 2022.

3. جعواد أمير عبد العظيم محمد عبد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، كلية الدّراسات الإسلامية والعربية بنات، القاهرة، العدد 35، الجزء 3، 2020.
4. شريط نجمة، "الأمن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والعقود"، المجلة الجزائرية للسياسة والأمن، جامعة وهران 02، المجلد 02، العدد 02، 2023.
5. عطية إدريس، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مجلة مصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، المجلد 1، العدد 1، 2019.
6. طالة لامية، "الإرهاب السيبراني والأمن القومي: قراءة في تحولات الإستراتيجية الدفاعية"، مجلة حوليات جامعة الجزائر 01، كلية علوم الإعلام والاتصال، جامعة الجزائر 03، المجلد 35، العدد 04، 2021.
7. عبده الله السمحان منى، "متطلبات تحقيق الأمن لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة منصورة، المملكة العربية السعودية، العدد 191، 2020.
8. ڤطاف سليمان، "الأليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني (الجزائر نموذجا)"، مجلة الحوكمة والقانون الإقتصادي، مخبر البحث كلية الحقوق والعلوم السياسية، عمار ثليجي-بالأغواط-الجزائر، المجلد 03، العدد 02،023.
9. مسيكة محمد، "الفضاء السيبراني وتحديات الأمن القومي للدول"، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور الجلفة، المجلد 07، العدد 04، 2022.

زروقة إسماعيل، "الفضاء السيبراني والتحول في مفاهيم القوة وصراع"، مجلة العلوم القانونية والعلوم السياسية، جامعة محمد بوضياف-المسيلة-، المجلد 10، العدد 01، 2019.

الهوامش

[1] ڤطاف سليمان. "الأليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني (الجزائر نموذجا)" **مجلة الحوكمة والقانون الإقتصادي**، مخبر البحث كلية الحقوق والعلوم السياسية، عمار ثليجي-بالأغواط-الجزائر، المجلد (03)، العدد (02)، 2023، ص ص 82-83.

[2] إسماعيل زروقة، "الفضاء السيبراني والتحول في مفاهيم القوة وصراع"، **مجلة العلوم القانونية والعلوم السياسية**، جامعة محمد بوضياف-المسيلة-، المجلد 10،العدد 01، 2019، ص 1017.

[3] أمير عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، **مجلة الشريعة والقانون**، كلية الدّراسات الإسلامية والعربية بنات، القاهرة، العدد 35، الجزء 3، ، 2020ص 391.

[4] خيرة شاري، صادقي إيمان، **"الأمن السيبراني وأثره في تحقيق الأمن القومي"**، مذكرة ماستر غير منشورة، جامعة محمد البشير الابراهيمي-برج بوعريريج، 2023، ص 23.

[5] جمال بوزادية، **"الأمن السيبراني"**، محاضرات مقدمة لطلبة ماستر2،تخصص دراسات أمنية وإستراتجية، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 03، 2021، ص 27.

[6] نفس المرجع، ص 52.

[7] لامية طالة ، "الإرهاب السيبراني والأمن القومي: قراءة في تحولات الإستراتيجية الدفاعية"، **مجلة حوليات جامعة الجزائر 01**، كلية علوم الإعلام والاتصال، جامعة الجزائر 03، المجلد 35، العدد 04، 2021 ،ص 361.

[8] نجمة شريط، "الأمن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والعقود"، **المجلة الجزائرية للسياسة والأمن**، جامعة وهران 02، المجلد 02،العدد 02، 2023، ص 81.

[9] محمد الدام، **"الأمن السيبراني"**، مذكرة ماستر غير منشورة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه محمد لخير-الوادي-، 2023، ص 10.

[10] نفس المرجع، ص 12.

[11] محمد مسيكة، "الفضاء السيبراني وتحديات الأمن القومي للدول"، **مجلة العلوم القانونية والاجتماعية**، جامعة زيان عاشور الجلفة، المجلد 07، العدد 04، 2022، ص 458.

[12] منى عبد الله السمحان، "متطلبات تحقيق الأمن لأنظمة المعلومات الإدارية بجامعة الملك سعود"، **مجلة كلية التربية**، جامعة منصورة، المملكة العربية السعودية، العدد191، 2020، ص 12.

[13] نجمة شريط، مرجع سبق ذكره، ص 78.

[14] إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، **مجلة مجلة مصداقية**، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، المجلد 1،العدد 1، 2019، ص ص 105-106.

[15] ق‌طاف سليمان، مرجع سبق ذكره، ص ص 85-88.

[16] سمير بارة، "الأمن السيبراني في الجزائر: السياسات والمؤسسات "، **المجلة الجزائرية اللامن الانساني**، جامعة قاصدي مرباح، ورقلة، العدد 04، 2017، ص ص 275-277.

[17] ساعد بوقرص، "الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات استراتيجية خاصة، **مجلة الأبحاث في الحماية الاجتماعية**، جامعة العلوم والتكنولوجيا هواري يومين، الجزائر، المجلد 03، العدد 03، 2022، ص 73.