جامعة عمار ثليجي الأغواط

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

حاضنة أعمال جامعة الأغواط

مشروع لنيل شهادة مؤسسة ناشئة في إطار القرار الوزاري 1275

السياسة العامة الأمنية الجزائرية في ظل تنامي متغيرات الأمن السيبراني: مشروع CyberGuard Algeria

إعداد وتقديم:

* عمر الجيلالي

تحت إشراف:

* د. ملوكي سفيان

* د. لبرق محمد رياض

الأستاذ	الرتبة	الصفة
قرطي العياشي	أستاذ التعليم العالي	رئيسا
ملوكي سفيان	أستاذ محاضر-أ-	مشرفا
لبرق محمد رياض	أستاذ محاضر-أ-	مشرفا
ميلودي محمد	أستاذ محاضر-أ-	مناقشا
رحماني يوسف زكريا	أستاذ محاضر-أ-	مناقشا

السنة الجامعية 2025-2026

بطاقة المعلومات:

حول فريق الإشراف:

الاسم	المهمة	الكلية
د. ملوكي سفيان	مشرف رئيسي	كلية الحقوق و العلوم السياسية
د. لبرق محمد رياض	مشرف مساعد	كلية العلوم الاقتصادية والتجارية و علوم التسيير

حول فريق العمل:

الاسم	التخصص	الكلية
عمر الجيلالي	العلوم السياسية	كلية الحقوق و العلوم السياسية

﴿ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي
بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ ﴾سورة النمل :الآية19

الـشكـر و الـعـرفـان

الحمد لله حمداً يليق بجلاله، حمداً يسر به البدايات ويُتِم به النهايات، وبه تُبلغ المقاصد وتُنجز الغايات. الحمد لله الذي ما تم جهد إلا بتوفيقه، وما خُتم عمل إلا بفضله وكرمه، فله سبحانه الشكر أولاً وآخراً على نعمة الإتمام والبلوغ.

وبعد إتمام هذا العمل، نسأل الله أن يجعله علماً نافعاً، وأن يرزقنا الانتفاع بما تعلمناه، وأن يزيدنا علماً وعملاً.

كما أتقدم بخالص عبارات الشكر والتقدير إلى كل من أسهم في إنجاز هذا العمل المتواضع، سواء بتوجيه أو دعم أو نصيحة. ويطيب لي أن أخص بالشكر الدكتور ملوكي سفيان و الدكتور محمد رياض لبرق، المشرفان على هذه المذكرة، على ما قدماه لي من توجيهات علمية دقيقة ومتابعة مستمرة ولم يبخلا علينا بالنصح والإرشاد طيلة فترة إعداد هذا العمل، فجزاهما الله عنا خير الجزاء.

كما أتوجه بجزيل الشكر والامتنان إلى أعضاء لجنة المناقشة الموقرين، لتفضلهم بقبول مناقشة هذا العمل وتشريفه بملاحظاتهم القيمة، مع خالص التقدير والاحترام.

ولا يفوتني أن أرفع عبارات الشكر إلى جميع أساتذة قسم العلوم السياسية بجامعة عمار ثليجي، لما لهم من فضل في تكويننا العلمي والمعرفي.

كما أتقدم بعميق الامتنان لكل من قدّم كلمة طيبة، أو نصيحة صادقة، أو فكرة بنّاءة، أو نقداً هادفاً، فكان لذلك الأثر البالغ في إخراج هذا العمل، لهم مني كل التقدير والاحترام.

إ هـد ا ء

إلى من كانت دعواتها سندي، ونورها دليلي، وصبرها سرّ قوتي... إلى والدتي الغالية، التي لا تكفي الكلمات لوصف فضلها، أهديك هذا العمل المتواضع عربون محبة وامتنان لا ينتهي.

إلى والدي العزيز، رمز العطاء والثبات، الذي علّمني أن السعي طريق، وأن النجاح ثمرة صبر وإرادة... لك مني كل التقدير والوفاء.

إلى إخوتي الأعزاء :عمر وإكرام وفتيحة، وإلى زوجها منصور، وإلى أبنائهم الأحبة رتاج وإدريس، أنتم فرح القلب ودفء الروح، وبكم تكتمل معاني العائلة... أهديكم هذا الإنجاز بكل حب.

إلى أمي رحمها الله، التي غابت عن العين ولم تغب عن القلب، أسأل الله أن يجعل هذا العمل صدقة جارية في ميزان حسناتها، وأن يسكنها فسيح جناته.

إلى البرعم سند أبو عبيدة، رمز الأمل والصبر، نسأل الله أن يجعل الشفاء رفيق أيامه، وأن يكتب له مستقبلاً مشرقاً يليق ببراءة طفولته وأحلامه.

إلى كل من ساندني، ووقف إلى جانبي، وقدم لي كلمة طيبة أو دعاء صادقًا من الأصدقاء ... لكم مني خالص المحبة والامتنان.

إليكم جميعًا، أهدي ثمرة هذا الجهد.

الفهرس

فهرس الجداول

فهرس الأشكال:

فهرس المحتوى

مقدمة

أضحت السياسة العامة الأمنية تمثل ركيزة أساسية في منظومات الحوكمة الحديثة، الأمر الذي جعلها محورًا جوهريًا ولاسيما مع تصاعد التحديات السيبرانية التي باتت تهدد استقرار الدول ووظائفها الحيوية. لقد أدى تسارع وتيرة التحول الرقمي وتزايد الهجمات الإلكترونية، التي غالبًا ما تُنفّذ من قبل فواعل غير دولية، إلى إعادة النظر في أسس الحماية الوطنية وآلياتها.

يتجلى ذلك بوضوح في الحالة الجزائرية، بحكم موقعها الجيوستراتيجي واعتمادها المتنامي على البنى التحتية الرقمية في قطاعات إستراتيجية، وخاصة في مجالات الدفاع والطاقة والمالية، حيث تتزايد المخاطر بشكل مركب يستدعي حلولًا استباقية ومرنة، وفي هذا الإطار، استجابت الدولة لهذه التحديات عبر اعتماد إستراتيجيات تقوم على الوقاية، وتحديث الأنظمة التقنية، وبناء كفاءات بشرية متخصصة.

تندرج هذه الدراسة ضمن الجزائر خلال المرحلة الراهنة التي تشهد تسارع التحول الرقمي وتنامي التهديدات السيبرانية على المستويين الداخلي والدولي، لذلك أصبح الأمن السيبراني يشكل خطًّا استراتيجيًا للدفاع ضد التهديدات غير المتماثلة متعددة الأبعاد، وبذلك يمكن القول إن هذه الجهود تعكس وعيًا متناميًا بأهمية حماية الأمن القومي وضمان استدامة استقرار الدولة في ظل البيئة الرقمية المتغيرة. وفي هذا السياق المتسارع الذي تتعاظم فيه التهديدات السيبرانية وتتداخل فيه الأبعاد الأمنية والتكنولوجية، يبرز مشروع CyberGuard Algeria كاستجابة عملية وتجسيد تطبيقي للتوجهات الإستراتيجية التي تبنتها الدولة في مجال الأمن السيبراني.

إذ يُعدّ مشروع CyberGuard Algeria منصةً أكاديمية وتكوينية متخصصة في الأمن السيبراني، تهدف إلى تطوير الكفاءات البشرية وتعزيز الثقافة الرقمية من خلال توفير بيئة تدريبية حديثة قائمة على المقاربات التطبيقية والمحاكاة الواقعية للتهديدات السيبرانية، كما تقدّم المنصة برامج تدريبية متقدمة تشمل حماية الأنظمة والشبكات، وتحليل المخاطر، والاستجابة للحوادث الرقمية، مع توظيف تقنيات الذكاء الاصطناعي في العملية التكوينية. ويسعى المشروع كذلك إلى تأهيل موارد بشرية وفق المعايير الدولية، بما يساهم في دعم التحول الرقمي وتعزيز الوعي الأمني وترسيخ أسس السيادة الرقمية والأمن المعلوماتي للدولة.

الإشكالية:

أدت التحولات الرقمية المتسارعة إلى جعل الفضاء السيبراني مجالاً استراتيجياً يرتبط بالأمن الوطني والتنمية الاقتصادية، وهو ما رافقه تزايد التهديدات والجرائم السيبرانية التي تستهدف الأنظمة المعلوماتية والبنى التحتية الرقمية.

وفي هذا السياق، أصبح تعزيز فعالية السياسات العامة في مجال الأمن السيبراني ضرورة ملحة لضمان حماية البيانات ودعم مسار التحول الرقمي الآمن، حيث سعت الجزائر خلال السنوات الأخيرة إلى تطوير منظومة قانونية ومؤسساتية لمواجهة مختلف المخاطر السيبرانية، غير أن التطور المستمر والمتسارع للتهديدات الرقمية يفرض تحديات متزايدة تستدعي تبني مقاربات أكثر تكاملاً وابتكاراً، قادرة على الاستجابة لطبيعة هذه التهديدات وتعقيداتها المتغيرة.

ومن هذا المنطلق، يبرز مشروع CyberGuard Algeria كمبادرة تطبيقية تهدف إلى دعم الأمن السيبراني من خلال التوعية والاستشارات والخدمات الرقمية، بما يساهم في تعزيز فعالية السياسة العامة ودعم تنافسية الاقتصاد الوطني، وهو ما يقود إلى طرح الإشكالية التالية:

إلى أيّ مدى تتمتع السياسة العامة الجزائرية بالفعالية في مواجهة التهديدات والجرائم السيبرانية في ظلّ التحولات الرقمية المتسارعة خلال المرحلة الراهنة؟ وكيف يمكن لمشروع CyberGuard Algeria أن يُسهم كآلية تطبيقية مبتكرة في تعزيز هذه الفعالية بما يدعم التحول الرقمي الآمن ويعزّز تنافسية الاقتصاد الوطني في الجزائر؟

الأسئلة الفرعية:

- ✓ ما مفهوم السياسة العامة الأمنية؟ الأمن السيبراني؟
- ✓ ما هي أهم النماذج النظرية المفسرة للسياسة العامة الأمنية؟
- ✓ كيف تواجه السياسة العامة الأمنية الجزائرية التهديدات السيبرانية المختلفة؟
- ✓ كيف يمكن لمشروع CyberGuard Algeria أن يعزز فعالية التحول الرقمي الآمن؟

الفرضيات:

- ✓ تزايد التهديدات السيبرانية يفرض على الدولة الجزائرية مراجعة سياستها الأمنية التقليدية.
- ✓ قصور الإطار القانوني والتنظيمي في الجزائر يعيق فعالية الأمن السيبراني.
- ✓ تحقيق حصانة الدولة الرقمية مرهون بمدى قدرة السياسات الأمنية على مواكبة التحولات الرقمية والتكنولوجية.

أهمية الدراسة:

تكتسي دراسة السياسة العامة الأمنية الجزائرية في ظل تنامي المتغيرات السيبرانية الراهنة أهمية علمية وعملية متزايدة، بالنظر إلى الطابع الحيوي الذي تفرضه تحولات الفضاء الرقمي على مفاهيم السيادة والأمن القومي.

فقد أصبحت التهديدات السيبرانية من أبرز المخاطر التي تواجه الدول، بما في ذلك الجزائر، خاصة في ظل تسارع رقمنة المؤسسات الوطنية والاعتماد المتزايد على التكنولوجيات الذكية، وهو ما جعل الفضاء السيبراني مجالًا حيويًا تتقاطع فيه اعتبارات الأمن القومي مع متطلبات التحول الرقمي. وتسعى هذه الدراسة إلى الإسهام في تعميق الفهم لطبيعة التهديدات السيبرانية التي تواجه الأمن القومي الجزائري، وتحليل كيفية تفاعل السياسة العامة الأمنية مع هذه التحديات، بما يتيح تقييم نقاط القوة والقصور في السياسات المعتمدة واقتراح سبل تطويرها بما يواكب تطور البيئة الرقمية.

كما تهدف هذه الدراسة إلى تعزيز الوعي المجتمعي والرسمي بأهمية الأمن السيبراني بوصفه ركيزة أساسية في حماية الاستقرار الوطني وضمان استمرارية الفضاء الرقمي الآمن. ومن جهة أخرى، تتجلى أهميتها في اقتراح سبل تكامل أكثر فعالية بين مختلف الفاعلين الرسميين، مثل الوزارات والمؤسسات الأمنية، وغير الرسميين، كالمجتمع المدني والقطاع الخاص، بما يسمح بصياغة استراتيجيات وطنية تستجيب لمتطلبات العصر الرقمي وتواكب التطورات الدولية في مجال الأمن السيبراني. وتأتي هذه الجهود استجابة لما كشفت عنه الدراسات السابقة من فراغات علمية ومنهجية، مما يجعل هذه الدراسة مساهمة في إثراء النقاش الأكاديمي حول بناء سياسة أمنية رقمية أكثر فعالية واستدامة.

أسباب اختيار الموضوع:

أ – أسباب ذاتية:

- ✓ الرغبة في تقصي وفهم أبعاد السياسة العامة الأمنية.
- ✓ الاهتمام بالسياسة العامة وتطورها.
- ✓ شغف شخصي بكل ما يتعلق بالأمن السيبراني.

ب – أسباب موضوعية:

- ✓ الرغبة في اكتشاف موضوعات بحثية جديدة لا تحظى بالاهتمام الكافي في الجامعات الوطنية.
- ✓ تزايد أهمية القضايا المرتبطة بمستقبل النظام العالمي في ظل تصاعد التهديدات الأمنية خاصة السيبرانية.
- ✓ دراسة هذا الموضوع ضرورية لفهم ديناميكيات القوة في القرن 21 ومستقبل الأمن في الجزائر.

أهداف الدراسة:

- ✓ توضيح مفهوم السياسة العامة الأمنية والأمن السيبراني.
- ✓ معرفة جوانب السياسة العامة الأمنية الجزائرية من محددات وتحديات.

- ✓ التعرف على أهم الإستراتيجيات التي تتبعها الدولة في تعزيز أمن المعلومات والأمن السيبراني.
- ✓ إبراز أهم الفاعلين الرسميين وغير رسميين في السياسة العامة الأمنية.
- ✓ الوقوف على بعض النقائص المسجلة في الدراسات السابقة واقتراح إستراتيجيات جديدة قد تساهم في دعم السياسة العامة الأمنية الجزائرية.

أدبيات الدراسة:

انطلاقًا من الطابع النظري والتطبيقي لموضوع السياسة العامة الأمنية الجزائرية في ظل تنامي متغيرات الأمن السيبراني، فقد استندت هذه الدراسة إلى مجموعة من الأدبيات والمراجع العلمية التي تشكل أساسًا مفاهيميًا ومنهجيًا، من أبرزها:

1- كتاب" صنع السياسة العامة "للمفكر الأمريكي جيمس أندرسون، ترجمة الدكتور عامر الكبيسي، والصادر عن دار المسيرة للنشر والتوزيع عمان، (1998)، يُعد هذا المرجع من الكتب التأسيسية في حقل السياسات العامة، حيث تناول المفاهيم الأساسية للسياسة العامة، وسلط الضوء على مراحل صنعها، إضافة إلى تحليل دور الفواعل الحكومية وغير الحكومية في بلورة السياسات العامة وصياغتها.

2- كتاب" البنية والتحليل في السياسة العامة "للمفكر فهمي خليفة الفهداوي، الصادر عن دار المسرة للنشر والتوزيع عمان،(2001) ، يُعد من المراجع الأساسية في حقل السياسات العامة، حيث يتناول مفهوم السياسة العامة وبيئتها المختلفة، ويحلل الفواعل المتداخلة في صنعها، كما يبرز طبيعة العلاقة التفاعلية بين السياسة العامة والإدارة العامة من حيث الأدوار والوظائف وآليات التنفيذ.

3- كتاب" السياسة الأمنية الجزائرية :المحددات، الميادين، التحديات "للدكتور منصور لخضاري، منشور ضمن مجلة" سياسات عربية"، العدد20 ، مايو (2016)، يُعد هذا المرجع من بين الدراسات التطبيقية الهامة التي تطرقت إلى تبلور السياسة الأمنية في الجزائر، إذ تناول المفاهيم المتعلقة بالأمن الوطني والأمن الاستراتيجي، بالإضافة إلى تحليل محددات هذه السياسة في مواجهة التحديات الأمنية التقليدية وغير التقليدية، لا سيما الإرهاب.

4- كتاب" الدولة العصرية دولة مؤسسات القانون "للمفكر حسن أبشر الطيب، الصادر عن دار الفجر للنشر والتوزيع القاهرة، (2005)، يتناول مفهوم الدولة الحديثة باعتبارها دولة مؤسسات قائمة على سيادة القانون، حيث يبرز دور المؤسسات في تنظيم السلطة وضمان خضوعها للقانون، كما يوضح أهمية توزيع السلطات وتحقيق التوازن بينها بما يعزز الاستقرار السياسي ويكرس مبدأ الشرعية ويحمي

الحقوق والحريات داخل الدولة.

الدراسات السابقة:

1- دراسة عيساوي سفيان (2017)، الموسومة بـ" توظيف المعايير الدولية في صناعة السياسة الأمنية الجزائرية"، والتي نُشرت في المجلة الأفريقية للعلوم السياسية .وقد ركزت الدراسة على تحليل مدى توافق السياسات الأمنية الجزائرية مع المعايير الدولية، مسلطةً الضوء على التأثير المتزايد للفواعل الدولية والمنظمات الإقليمية في توجيه العقيدة الأمنية للدولة .كما تناولت الدراسة أثر التحديات الأمنية في منطقة الساحل الإفريقي على التوجهات الأمنية الجزائرية، واستعرضت الجهود المبذولة لتحقيق المواءمة بين البعد الوطني والضغوط الدولية .وقد اعتمد الباحث على مقاربة تحليلية نظرية، مما يثري الأدبيات المتعلقة بعولمة الأمن الوطني.

2- دراسة سمير بارة (2017)، بعنوان" الأمن السيبراني في الجزائر :السياسات والمؤسسات" ، نشرها في المجلة الجزائرية للأمن الإنساني .تحلل الدراسة بنية المنظومة السيبرانية الجزائرية من منظور مؤسسي، مشيرة إلى دور أجهزة الدولة وخاصة الدفاع الوطني والدرك الوطني في التصدي للتهديدات الرقمية. وقد أشارت إلى أن الجزائر أدركت أهمية الأمن السيبراني ضمن سياستها الأمنية، رغم المعوقات المتعلقة بجمع البيانات، وتطوير التشريعات، وتفعيل بنية مؤسساتية فعالة لمواجهة الجريمة الالكترونية.

منهج الدراسة:

نظرًا للطبيعة المركبة لموضوع هذه الدراسة، التي تتناول السياسة العامة الأمنية الجزائرية في ظل تنامي متغيرات الأمن السيبراني، فقد تم اعتماد مقاربة منهجية متعددة تتيح الإحاطة بالموضوع من مختلف أبعاده القانونية والمؤسساتية والاستشرافية.

فقد تم توظيف المنهج الوصفي لدراسة مكونات السياسة الأمنية الجزائرية من خلال تحليل النصوص القانونية والوثائق الرسمية والاستراتيجيات الوطنية ذات الصلة بالأمن السيبراني، مع إبراز دور المؤسسات الفاعلة في هذا المجال. كما تم الاعتماد على المنهج التاريخي لتتبع نشأة وتطور الاهتمام بالأمن السيبراني دوليا وفي الجزائر، من خلال رصد مراحل التحول من المقاربة الأمنية التقليدية إلى إدماج البعد الرقمي ضمن منظومة الأمن الوطني، وما رافق ذلك من تطور مؤسساتي وتشريعي مرتبط بتزايد التهديدات السيبرانية. إضافة إلى ذلك، تم استخدام المنهج المقارن من خلال مقارنة التجربة الجزائرية ببعض التجارب الدولية الرائدة في مجال الأمن السيبراني، بهدف الوقوف على أوجه التشابه والاختلاف، وتحديد مكامن القوة والنقائص، والاستفادة من الممارسات الدولية الناجحة في بناء منظومات

أمن سيبراني أكثر فعالية. وأخيرًا، تم توظيف المنهج الاستشرافي لاستشراف مسارات تطور السياسة الأمنية الجزائرية في ظل التحولات الرقمية المتسارعة، مع اقتراح تصورات مستقبلية لتعزيز القدرات الوطنية في مواجهة التهديدات السيبرانية وبناء منظومة رقمية أكثر مرونة وأمنًا.

هيكل الدراسة:

تتوزع هذه الدراسة على ثلاثة فصول مترابطة تجمع بين التأصيل النظري والتحليل التطبيقي والاستشراف المستقبلي لموضوع السياسة العامة الأمنية الجزائرية في ظل تنامي التهديدات السيبرانية. وقد خُصص الفصل الأول لدراسة الأسس النظرية والمفاهيمية للسياسة العامة الأمنية والأمن السيبراني، من خلال عرض المفاهيم الأساسية والنظريات المفسرة للسياسات الأمنية، وبيان طبيعة التهديدات السيبرانية وأبعادها المختلفة وأهميتها في البيئة الرقمية المعاصرة.

أما الفصل الثاني فيتناول واقع السياسة العامة الجزائرية في مجال الأمن السيبراني، من خلال تحليل الإطار القانوني والمؤسساتي المنظم لهذا المجال، واستعراض أهم الاستراتيجيات والآليات المعتمدة لمواجهة التهديدات السيبرانية، مع تقييم مستوى فعالية السياسات المتبعة وتحديد أبرز التحديات والصعوبات التي تواجهها في ظل التحولات الرقمية المتسارعة.

في حين خُصص الفصل الثالث للجانب التطبيقي، والمتمثل في مشروع CyberGuard Algeria باعتباره مبادرة رقمية مبتكرة تهدف إلى دعم السياسة العامة للأمن السيبراني في الجزائر، حيث يتناول عرض فكرة المشروع وأهدافه ومكوناته التقنية والتنظيمية، ودراسة جدواه الاقتصادية وآليات تنفيذه، مع إبراز دوره في تعزيز الوعي السيبراني، وتنمية الكفاءات الوطنية، والمساهمة في بناء بيئة رقمية أكثر أمناً ودعماً لمسار التحول الرقمي والتنمية الوطنية.

صعوبات الدراسة:

تتمثل أبرز الصعوبات التي واجهتني في إنجاز هذه الدراسة ومشروع CyberGuard Algeria في الطبيعة المركبة للموضوع الذي يجمع بين السياسة العامة والأمن السيبراني من جهة، وبين الجانب النظري والتطبيقي من جهة أخرى، مما استدعى جهداً معرفياً كبيراً لفهم المفاهيم المتداخلة بين الحقول القانونية والسياسية والتقنية.

واجهت هذه الدراسة عدداً من التحديات العلمية والمنهجية، كان أبرزها ندرة المراجع والدراسات المتخصصة التي تتناول موضوع الأمن السيبراني في السياق الجزائري بشكل مباشر، الأمر الذي فرض الاعتماد على مصادر ومراجع عربية وأجنبية متنوعة من أجل بناء إطار نظري وتحليلي متكامل. كما

برزت صعوبة في التعامل مع الكم الكبير من المعلومات والبيانات ذات الصلة بالموضوع، وما يتطلبه ذلك من جهد في التصنيف والتحليل والتوظيف المنهجي، بما يضمن الحفاظ على الترابط المنطقي بين الأفكار وتسلسلها العلمي وفق متطلبات البحث الأكاديمي.

الفصل الأول: التأصيل المفاهيمي والنظري للسياسة العامة الأمنية والأمن السيبراني.

يمثل الأمن السيبراني أحد أبرز التحولات التي أعادت تشكيل مفهوم الأمن في العصر الرقمي، حيث لم يعد التهديد مقتصراً على الأبعاد العسكرية التقليدية، بل امتد ليشمل الفضاء الإلكتروني باعتباره مجالاً استراتيجياً جديداً تتقاطع فيه المصالح السياسية والاقتصادية والأمنية. وفي ظل هذا التحول، أصبحت الدول مطالبة بإعادة صياغة سياساتها الأمنية بما يستجيب لطبيعة التهديدات السيبرانية التي تتسم بالتعقيد، والسرعة، والعابرية للحدود.

وانطلاقاً من ذلك، يهدف هذا الفصل إلى تحليل الأبعاد المختلفة للأمن السيبراني من خلال مقاربة تجمع بين التأصيل النظري والاستقراء التطبيقي، حيث سيتم التطرق إلى النماذج الدولية الرائدة في هذا المجال، باعتبارها تجارب مرجعية تعكس تنوع المقاربات الاستراتيجية والمؤسساتية. كما يسعى الفصل إلى استثمار هذا التحليل في تقييم واقع السياسة السيبرانية الجزائرية، من خلال الوقوف على محدداتها الأساسية، وتشخيص أبرز التحديات التي تعيق تطويرها، سواء على المستوى المؤسسي أو التشريعي أو التكنولوجي أو البشري. وعليه، فإن هذا الفصل يشكل مدخلاً تحليلياً لفهم كيفية تفاعل الجزائر مع التحولات الرقمية الراهنة، ومدى قدرتها على بناء منظومة سيبرانية فعالة تضمن تحقيق الأمن الوطني في سياق دولي متغير، يتسم بتصاعد حدة التنافس في الفضاء السيبراني.

المبحث الأول: الدراسة المفاهيمية والنظرية للسياسة العامة الأمنية

تُعدّ السياسة العامة الأمنية من أهم السياسات العمومية المعاصرة، نظراً لدورها في تحقيق الاستقرار وحماية الدولة والمجتمع في مواجهة التهديدات التقليدية والحديثة، بما فيها التهديدات المعلوماتية والسيبرانية. وقد اتسع مفهوم الأمن ليشمل أبعاداً سياسية، اجتماعية، اقتصادية وتكنولوجية، مما فرض على الدول تبني سياسات أمنية شاملة ومتكاملة. وفي هذا الإطار، يهتم هذا المبحث بدراسة الأسس المفاهيمية والنظرية للسياسة العامة الأمنية، من خلال تناول مفهوم السياسة العامة، ثم توضيح خصوصية السياسة العامة الأمنية، وأخيراً عرض أبرز النظريات المفسرة لها لفهم آليات صنع القرار الأمني وتطور السياسات الأمنية الحديثة.

المطلب الأول: مفهوم السياسة العامة

يشهد مفهوم السياسة العامة تداخلاً مفاهيمياً واسعاً في حقل العلوم الاجتماعية، إذ يتميز بتعدد التعريفات وتباين زوايا التناول بين مختلف الباحثين والمدارس الفكرية. وقد أدى هذا التباين إلى غياب تعريف موحد أو جامع يمكن الاتفاق عليه، مما جعله موضوعاً لاجتهادات نظرية ومنهجية مستمرة تهدف إلى بلورة حدوده المفاهيمية وتقنين أبعاده العلمية.

وفي هذا الإطار، يُعد ما طرحه الفيلسوف الأمريكي جون ديوي (John Dewey) مساهمة محورية في توضيح طبيعة القضايا العامة التي تشكل جوهر السياسة العامة، حيث بيّن أن النشاطات تتحول إلى شأن عام عندما تنتج عنها آثار أو نتائج تتجاوز نطاق الأفراد أو الجماعات المتورطين فيها بصورة مباشرة، بحيث تمتد تداعياتها لتشمل أطرافاً أخرى داخل المجتمع، وهو ما يستدعي تدخلاً منظماً أو مؤسسياً لتنظيم تلك الآثار.[1]

وعرفها أوستن ريني بأنها علاقة التبعية والطاعة من جانب، والسلطة والسيطرة من جانب آخر[2]، أما ماكس فيبر (Weber) فعرفها من زاوية التأثير على الآخرين بأنها "احتمال قيام شخص ما في علاقة اجتماعية بتنفيذ رغباته رغم مقاومة الآخرين، بغض النظر عن الأساس الذي يقوم عليه هذا الاحتمال" يعكس هذا المنظور قدرة النخبة على الوصول إلى القيم.[3]والموارد المؤثرة داخل المجتمع والتحكم في توزيعها وتوجيهها بما يخدم مصالحهم. كما يبرز مفهوم القوة باعتباره أداة أساسية للتأثير في سلوك الأفراد

[1] John Dewey, **The Public and Its Problems** (New York: Henry Holt and Company,1946). p 13.

[2] حسن أبشر الطيب، **الدولة العصرية دولة مؤسسات القانون**، (القاهرة: دار الفجر للنشر والتوزيع، ط1، 2005)، ص. 295.

[3] نصر محمد مهنا، **علم السياسة**، (القاهرة: دار غريب للطباعة والنشر، 1995)، ص. 120-121.

لقد وصف العديد من علماء السياسة النظام بشكل عام باعتباره مجموعة من الأجزاء تشكل فيما بينها نسقاً من العلاقة المتبادلة في إطار تلك الوحدة الكلية، وعلى هذا الأساس يولي أصحاب هذا الاتجاه أمثال ديفيد إستون (Easton) اهتماماً بالسياسة العامة أي، من وجهة تحليل النظم كنتيجة ومحصلة في حياة المجتمع من منطق تفاعلها الصحيح مع البيئة الشاملة التي تشكل فيها المؤسسات والمرتكزات والسلوكات أصولاً للظاهرة السياسية التي يتعامل معها النظام السياسي فيعرفها بأنها "عملية تخصيص سلطوي للقيم المادية والمعنوية داخل المجتمع في تفاعلية بين المدخلات والمخرجات والتغذية العكسية، من خلال القرارات، والأنشطة الإلزامية الموزعة لتلك القيم.[1]

أما جيمس أندرسون (Anderson) فيعرفها بأنها "برنامجاً موجهاً يتبعه أداء فردي أو جماعي بهدف التصدي لمشكلة معينة أو معالجة قضية محددة، حيث يتم تطوير هذا البرنامج من قبل الهيئات الحكومية ضمن نطاق مسؤولياتها، مع الإشارة إلى أن بعض الفواعل غير الرسمية قد تساهم بدورها في صياغة وتطور هذه السياسات.[2]"

أما عن الكتّاب العرب فقد برزوا أيضاً في تعريف السياسة العامة ونذكر منهم: يعرفها خيري عبد القوي بأنها "تلك العمليات والإجراءات السياسية وغير السياسية التي تتخذها الحكومة بقصد الوصول إلى اتفاق على تعريف المشكلة، والتعرف على بدائل حلها وأسس المفاضلة بينها تمهيداً لاختيار البديل الذي يقترح إقراره في شكل سياسة عامة ملزمة تنطوي على حل مرضٍ للمشكلة[3].

ويعرفها أحمد سعيفان بأنها "تعبير عن الرغبة الحكومية بالعمل، أو الامتناع عن العمل، وهي مجموعة مبنية ومتماسكة من القرارات، والإنجازات يمكن نسبها لسلطة عامة محلية، وطنية أو فوق وطنية، فتضم بذلك أربعة عناصر: الهدف؛ اختيار الأفعال التي تحققه؛ إعلان الفاعلين لهذه السياسة؛ تنفيذ هذه السياسة[4] ، فإنها بذلك تترجم لما تقوله الحكومة وما تفعله إزاء المشاكل الحساسة، لذا، فتعريف السياسة العامة من المنظور الحكومي، يمثل منطلقاً علمياً من خلال دراسة جوانب السياسة وممارساتها المؤثرة في صنع السياسة العامة.

وفي هذا السياق، يبرز تعريف فهمي خليفة الفهداوي بوصفه محاولة تركيبية شاملة، حيث يُعرّف السياسة العامة بأنها: "منظومة فاعلة – مستقلة ومتغيرة ومتكيفة وتابعة – تتفاعل مع بيئتها ومتغيراتها

[1] David Easton,**A Systems Analysis of Political Life** (New York: Wiley, 1965), p.p 134–135.

[2] جيمس اندرسون، **صنع السياسات العامة**، ترجمة عامر الكيسي، (عمان: دار المسيرة، 1999)، ص. 15.

[3] عبد القوي خيري، **دراسة السياسة العامة**، (الكويت: ذات السلاسل للطباعة والنشر والتوزيع، 1988)، ص. 35–36.

[4] أحمد سعيفان، **قاموس المصطلحات السياسية والدستورية والدولية**، (بيروت، مكتبة لبنان،2005)، ص. 213.

ذات الصلة، من خلال استجابة فكرية وعملية تعكس نشاط مؤسسات الدولة وسلطاتها في محيطها الاجتماعي بمختلف مجالاته. وذلك عبر أهداف وبرامج وسلوكيات منظمة تهدف إلى معالجة القضايا والمشكلات الراهنة والمستقبلية، مع الاستعداد لمواجهة تداعياتها، وتحديد الوسائل والموارد البشرية والتقنية والمعنوية الضرورية، وتهيئتها كمنطلقات عملية لغرض التنفيذ والمتابعة والتقويم والتطوير، بما يحقق المصلحة العامة المشتركة بصورة ملموسة في الواقع الاجتماعي."[1]

وتجدر الإشارة إلى أنه، بالنظر إلى تباين الرؤى والاتجاهات الفكرية التي تأسست عليها مختلف التعريفات، يصعب تقديم تعريف إجرائي موحَّد للسياسة العامة. فالتحولات الحديثة المرتبطة بالمفهوم، لاسيما في ظل ما يُعرف بـ "شبكة العمل في السياسة العامة" (Policy Work Net)، تؤكد أن صنع السياسة لم يعد مقتصراً على فاعل رسمي واحد، بل أصبح نتاجاً لمشاركة جماعات متعددة تتغير باختلاف قضايا السياسات العامة وتخضع لمبادئ الشفافية والدقة العلمية في سبيل تحقيق المصلحة العامة.

ورغم ذلك، يمكن صياغة تعريف إجرائي للسياسة العامة بوصفها: تُعرّف السياسة العامة بأنها توجه منظم يتجسد في برامج أو قرارات تتخذها مؤسسات الدولة ضمن نطاق محدد من المجالات – كالتعليم، أو الصحة، أو غيرهما – بغرض معالجة مشكلات وقضايا مجتمعية راهنة أو مستقبلية.

المطلب الثاني: مفهوم السياسة العامة الأمنية

يعرّف سيباستيان روشي (Roché)، في مؤلفه "السوسيولوجيا السياسية للأمن"، السياسة العامة الأمنية بأنها مجموعة من الترتيبات التشريعية والتنظيمية المخصصة لإدارة المجال الأمني، إلى جانب البرامج والأنشطة التي تعمل النخب المحلية والوطنية، إضافة إلى الإدارات العمومية، على تنفيذها سواء بصورة منفردة أو بالشراكة مع فاعلين آخرين، سواء كانوا من المجتمع المدني أو من القطاع التجاري[2]. ويؤكد روشي أن السياسة الأمنية لا تستهدف فقط مرتكبي العنف، بل تشمل أيضاً الضحايا والرأي العام، ما يجعلها ذات طابع شامل ومعقد.

تعريف الباحث بوريش رياض: "هناك سياسات عامة أمنية عندما تحاول سلطة عامة محلية أو وطنية أو إقليمية، من خلال برنامج عمل منسق تعديل البيئة الأمنية لمختلف الفواعل ضمن إطار ضبط

[1] فهمي خليفة الفهداوي، **السياسة العامة: منظور كلي في البنية والتحليل**، (عمان: دار المسرة، ط1، 2001)، ص38.

[2] Roché Sébastian. **Sociologie politique de l'insécurité.** Paris: Presses Universitaires de France, 1998, cité dans: Laurent Mucchielli, Revue française de sociologie, vol. 40, no. 1 (1999), p. 151.

المنطق القطاعي، وتكمن أهمية هذا التعريف في تحديد السياسات العامة الأمنية كقطاع من قطاعات السياسة العامة الغرض منها ضبط القطاع الأمني من خلال سلطة عامة، كما أن هذا التعريف يوسع من دائرة الفواعل المعنيين بالسياسات العامة الأمنية.[1]

تعريف الباحثة سيفيرين جرمن (Severine Germain): السياسات العامة للأمن تهدف إلى مكافحة جنوح التهديدات الفعلية وانعدام الأمن للتهديدات المنظورة، وهذا التعريف يركز في الواقع على الغرض الذي تسعى إليه. السياسات العامة الأمنية والذي يشمل حسب الباحثة شقين الأول يتعلق بمواجهة التهديدات الفعلية التي تواجه الدولة أما الثاني فيتعلق بمواجهة التهديدات المنظورة أو التي يمكن أن تحدث.[2]

تعريف الباحثة ميليوزا راندريما بينينا (Mialisoa Randriama pianina): "جميع السياسات الداخلية لدولة لإنشاء أو إعادة إحلال السلام والحفاظ على أراضيها لضمان الحكم ووسائل للعيش والعمل والاستثمار والقيام بالمشاريع بهدوء"، وقد فرقت الباحثة بين مفهوم السياسات العامة الأمنية الداخلية والخارجية حيث تشير هذه الأخيرة حسب الباحثة: "إلى الاستراتيجيات السياسية والموارد العسكرية لبلد ما لحماية أراضيه وشعبه من العدوان الخارجي، وهذا يعني حماية وحدة أراضيه ضد التهديدات الخارجية.[3]"

وفي ضوء المطلب السابق يمكن القول إن خصائص السياسة العامة تنطبق على السياسات العامة الأمنية لكن مع ملاحظة أساسية وهي أن السياسات العامة المؤسساتية تؤثر على باقي السياسات العامة القطاعية مثل السياسات العامة الاقتصادية فهذه الأخيرة لا يمكن أن تتجسد على أرض الواقع في غياب الأمن وانعدامه، في النهاية، تظل السياسات الأمنية العامة، كسائر السياسات العمومية، في حاجة مستمرة إلى التقييم والتجديد، بما يتناسب مع التحولات الاجتماعية والسياسية. وهذا يفرض إعادة توجيه مستمرة لنشاط أجهزة الأمن العام، مع ضرورة تعزيز التواصل والتكامل بين صناع القرار والمنفذين، بما يضمن تحقيق الاستقرار والتقدم الاجتماعي في إطار مقاربة شاملة للأمن.

[1] Riadh Bouriche, **Approches et conceptions des politiques publiques sécuritaires**, (Forum international "Alger et sécurité en Méditerranée: réalité et perspectives", Université Mentouri Constantine : Faculté de droit et sciences politiques, 29 et 30 avril 2008), p. 17.

[2] Séverine Germain, **Les politiques locales de sécurité en France et en Italie :** une comparaison des villes de Lyon, Grenoble, Bologne et Modène, thèse de doctorat en science politique (Grenoble : Université Pierre Mendès-France, Institut d'études politiques de Grenoble, novembre 2008), p.13.

[3] Mialisoa Randriamampianina,*Sécurité et Défense :* **Nouveaux Défis**, **Nouveaux Acteurs**,(Allemand FRIEDRICH–EBERT–STIFTUNG, 2009), p.9.

المطلب الثالث: النظريات المفسرة للسياسة العامة الأمنية

تمثل النظريات المفسرة للسياسة العامة الأمنية أطراً علمية ومنهجية تساعد على فهم كيفية تشكل القرار الأمني وتفسير ديناميات التفاعل بين الفواعل والمؤسسات، من خلال تقديم تصورات مختلفة لطبيعة القوة، وصنع القرار، وبنية النظام السياسي، والعوامل المؤثرة في توجيه السياسات الأمنية.

أ- المدرسة الواقعية

تُعد الواقعية إحدى أهم النظريات المفسرة للعلاقات الدولية، حيث تركز على القوة والصراع باعتبارهما المحددين الأساسيين للسلوك الدولي، مع اعتبار الدولة الفاعل المركزي في النظام الدولي. تنطلق من فرضية فوضوية النظام الدولي نتيجة غياب سلطة مركزية عليا، مما يفرض على كل دولة الاعتماد على قدراتها الذاتية لضمان أمنها والدفاع عن مصالحها. قدّم كينيث والتز عبر الواقعية البنيوية تصوراً يعتبر الأمن الهدف الأعلى للدول، في حين أكد هانز مورغانثاو أن السياسة الدولية تُختزل في صراع مستمر على القوة. ويرى وولفرز أن مفهوم الأمن يعادل "البقاء"، ويستوجب التسلح واستخدام القوة، خاصة العسكرية. ومع ذلك، واجهت الواقعية انتقادات جوهرية، أبرزها تركيزها المفرط على القوة العسكرية، إغفالها للأبعاد الاجتماعية والإنسانية، والفصل الصارم بين السياسة الداخلية والخارجية، مما يحد من قدرتها التفسيرية للتحولات المعاصرة.[1]

ب/ نظرية النظم السياسية

تُعد نظرية النظم من أبرز الأطر التفسيرية في دراسة صنع السياسة العامة، إذ تنظر إليها باعتبارها: استجابةً من النظام السياسي لمجموعة من المطالب والضغوط الواردة من بيئته الداخلية والخارجية.

يقوم النظام السياسي، وفق هذا المنظور، بوظيفة تحويل المدخلات (Inputs) إلى مخرجات (Outputs)عبر آليات محددة[2].

- ✓ **المدخلات:** تشمل المطالب، وهي مجموع الاحتياجات والمصالح التي يطرحها الأفراد والجماعات على النظام، والتأييد، أي أشكال الدعم السياسي والمؤسسي الذي يمنح للنظام شرعيته.
- ✓ **البيئة:** تمثل السياق الخارجي الذي يؤثر في النظام السياسي ويحدّد طبيعة الضغوط والفرص المتاحة

[1] عبد النور بن عنتر، **البعد المتوسطي للأمن الجزائري: الجزائر، أوروبا و الحلف الأطلسي**، (الجزائر: المكتبة العصرية للطباعة و النشر، ط1، 2005)، ص.19.

[2] جيمس أندرسون، مرجع سابق، ص. 31.

أمامه.

- ✓ **المخرجات:** تتجلى في القرارات والسياسات الرسمية التي يصوغها النظام استجابةً لتلك المطالب.
- ✓ عملية التحويل: آلية معالجة المدخلات عبر المؤسسات السياسية بغرض غربلتها وتحديد الاستجابات الممكنة.
- ✓ **التغذية العكسية:** تشير إلى الأثر الانعكاسي للسياسات العامة على البيئة والمجتمع، وما يترتب عنها من مطالب جديدة.

تتميز هذه النظرية بقدرتها على تنظيم عملية التحليل من خلال التركيز على ديناميكية التفاعل بين المدخلات والمخرجات، غير أنها تفتقر إلى تفسير معمّق لكيفية صناعة القرار داخل "الصندوق الأسود" للنظام السياسي.

ج/ النظرية المؤسساتية

تُعَدّ دراسة المؤسسات الحكومية من أقدم المناهج في العلوم السياسية، إذ تبقى الحياة السياسية في أي مجتمع مرتبطة ارتباطاً وثيقاً بأداء السلطات التنفيذية والتشريعية والقضائية، فالسياسات العامة تُصاغ وتنفذ عبر هذه المؤسسات الرسمية المخوّلة قانونياً.

وقد انصبّ المدخل التقليدي لدراسة المؤسسات على تحليل الهياكل الرسمية والقواعد القانونية والصلاحيات والعلاقات التنظيمية، دون إيلاء اهتمام كافٍ للسلوك الفعلي داخلها أو للسياسات التي تنتج عنها، غير أنّ التطور في حقل العلوم السياسية نقل الاهتمام من الطابع الإجرائي والشكلي إلى دراسة العملية السياسية ذاتها في إطار المؤسسات، مع التركيز على السلوك الواقعي للمشاركين فيها.

وهكذا تحوّل تحليل المؤسسة التشريعية مثلاً من مقاربة ساكنة وإجرائية إلى أخرى ديناميكية تُبرز تفاعلاتها الداخلية، بالرغم من ذلك، يظل البعد المؤسسي بهياكله وإجراءاته وقواعده عنصراً أساسياً في التحليل السياسي، إذ يوجّه سلوك الفاعلين الرسميين ويُؤطّر خياراتهم، ما يجعله مؤثراً في مضمون السياسات العامة وتوجهاتها، وباختصار، فإن فهم صنع السياسات يتطلب الجمع بين تحليل البنية المؤسسية من جهة، ودراسة الديناميات السياسية والسلوكية من جهة أخرى.[1]

[1] جيمس أندرسون، مرجع سابق، ص. 38.

د/ – نظرية النخبة

ترى نظرية النخبة أن السياسة العامة تعكس تفضيلات القلة المسيطرة داخل المجتمع، وليس إرادة الأغلبية، فالمجتمع، وفق هذا التصور، ينقسم إلى نخبة حاكمة تمتلك السلطة والموارد، وجماهير تفتقر إلى أدوات التأثير.

وقد لخص داي (Dye) وزيجلير (Zeigler) في كتابِهما (تجاهل الديمقراطية) النظرية وعلى النحو التالي[1]:

- ✓ السياسات تُصاغ أساسًا لحماية مصالح النخبة وضمان استمرارية النظام الاجتماعي القائم.
- ✓ انضمام أفراد جدد إلى النخبة يخضع لشروط صارمة، تهدف إلى الحفاظ على الاستقرار ومنع التغيير المفاجئ.
- ✓ النخبة تتفق فيما بينها على القيم الأساسية للنظام، مثل حماية الملكية الفردية أو الحد من تدخل الدولة في الاقتصاد.
- ✓ التغيير في السياسات العامة يحدث تدريجيًا عبر مسار تراكمي إصلاحي، لا ثورياً جذرياً، بما يتيح التكيف مع الضغوط دون الإضرار ببنية النظام.
- ✓ العلاقة بين النخبة والجماهير غير متكافئة؛ إذ تمارس النخبة التأثير على القاعدة الشعبية، بينما تخضع لضغوطها في حدود ضيقة.

تُبرز هذه النظرية الطابع الهرمي للعملية السياسية، لكنها تُنتقد بسبب نزعتها الحتمية التي تهمّش دور الجماهير والمؤسسات الوسيطة في صنع السياسة العامة.

هـ/ نظرية السلام الديمقراطي

تعود جذور هذه النظرية إلى إيمانويل كانط، الذي طرح فكرة "السلام الدائم"، مؤكّدًا أن الأنظمة الديمقراطية نادرًا ما تدخل في نزاعات مسلحة مع بعضها، بالنظر إلى اعتمادها على الحوار، التوافق، والعقلانية في حل الخلافات، ويُعزز هذا الطرح ثقافة المشاركة والتعددية داخل الدولة، من خلال آليات مؤسسية تحدّ من احتمالية الانزلاق إلى الحرب.

وعلى الصعيد الدولي، يُنظر إلى التعاون بين الدول باعتباره ضرورة في ظل تشابك العلاقات وتزايد ندرة الموارد، مما يجعل السلام نتاجًا لبنية سياسية تقوم على القيم الديمقراطية والمؤسسات التعاونية.[2]

[1] علي محمود بيومي، **دول الصفوة في اتخاذ القرار السياسي**، (القاهرة: دار الكتاب الحديث، (2004)، ص. 14.

[2] مبروك ساحلي، **نظرية السلام الديمقراطي: كآلية لتحقيق السلام المستدام**، مجلة دراسات وأبحاث، م. 12، ع. 3، (جويلية 2020)، ص.3.

المبحث الثاني: الأمن السيبراني – دراسة مفاهيمية

يُعرَّف الأمن السيبراني بأنه مجموعة من الإجراءات والتدابير الشاملة التي تهدف إلى حماية الأنظمة الرقمية والبنية التحتية المعلوماتية من مختلف التهديدات والهجمات السيبرانية، بما يضمن استمرارية عملها وسلامتها. وتشمل هذه الهجمات محاولات الاختراق، والبرمجيات الخبيثة، والفيروسات، والتصيد الإلكتروني، والاحتيال الرقمي، والتجسس الإلكتروني، إلى جانب غيرها من الأنشطةالعدائية التي قد تُلحق أضرارًا مادية أو تؤثر سلبًا على الأفراد أو المؤسسات أو حتى الحكومات.

ويستند الأمن السيبراني إلى تطبيق مجموعة من التقنيات والسياسات والاستراتيجيات التي تُمكّن من الوقاية من الهجمات، واكتشافها في الوقت المناسب، والتصدي لها بكفاءة، وذلك لضمان السرية، والسلامة، والتوفر، والموثوقية في البيئة الرقمية، بما يعزز الثقة في استخدام النظم المعلوماتية والبنى التحتية الرقمية.

المطلب الأول: تعريف الأمن السيبراني ونشأته

يشكّل الأمن السيبراني مجالًا حديث النشأة نسبيًا يهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات والاختراقات الرقمية، وقد تطور مع توسّع استخدام تكنولوجيا المعلومات والاتصال وتحول الفضاء الرقمي إلى عنصر أساسي في الأمن القومي للدول.

أولًا: تعريف الأمن السيبراني

نظرًا لتعدد وتباين التعريفات المتعلقة بالأمن السيبراني، أصبح من الضروري استعراض أكبر قدر ممكن منها بهدف بناء فهم شامل ومتكامل لهذا المفهوم. وقبل التطرق إلى هذه التعريفات، يستوجب الأمر الوقوف أولًا عند جملة من المفاهيم المرتبطة بالأمن السيبراني، وذلك بغرض مقاربته من زوايا متعددة تسمح بإبراز أبعاده النظرية والوظيفية بشكل أدق وأشمل.

1. السيبرانية لغويًا: تذكر المراجع العلمية بأن عالم الرياضيات نوربرت وينر (Norbert Wiener)، هو أول من استخدم مصطلح السيبرانية وذلك في عام 1948، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكي.[1]

أما فيما يتصل بالبحث عن مصدر كلمة سايبر (Cyber) في المعاجم اللغوية، فيتضح أنها

[1] أحمد عبيس نعمة الفتلاوي، **بحث الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر**، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل،المجلد8، العدد4، السنة الثامنة، 2016. ص.214.

يونانية الأصل وترجع إلى مصطلح(kybernetes) ، الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بعد، وبالرجوع إلى قواميس اللغة، فلم تشر في الغالب إلى مصدر كلمة سايبر (Cyber)، سوى ما وجدناه في قاموس (المورد) إذ يعرفها بالقول: السيبرانية: هي علم الضبط، ومصدرها (Cybernetics)، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها.

وما يؤكد ما طرح سلفاً، إن معظم القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبر إلى مصدرها، بل عرفت في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية الأمريكية إذ يعرفها: أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى. [1]

أما قاموس أكسفورد الإنجليزي، فيُعرف السيبرانية بأنها:

"دراسة فعالية العمل البشري من خلال مقارنتها بفعالية الآلات الحاسبة، وهي مرتبطة بخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي".

وفي السياق الأمني، يُعرف قاموس مصطلحات الأمن المعلوماتي مصطلح "الهجوم السيبراني" بأنه:

"عملية اختراق للفضاء الإلكتروني تستهدف السيطرة على مواقع إلكترونية أو اختراق بنى رقمية محمية، بهدف الإضرار بها أو استغلالها.[2]"

2. السيبرانية اصطلاحًا:

استعمل وينر مصطلح السيبرنطيقا (Cybernetics) لوصف علم جديد يُعنى بدراسة نُظم التغذية الراجعة(Feedback Systems) ، والتي تقوم على استخدام مخرجات النظام (Outputs) في ضبط مدخلاته (Inputs) بهدف التحكم في أدائه وضمان استقراره، وقد رأى وينر أن هذا النموذج لا ينطبق فقط على الآلات، بل يمكن تطبيقه أيضًا على الكائنات الحية، مما جعله أساسًا لعلم جديد يدمج بين مجالات التقنية والبيولوجيا وعلم النفس.

وبحسب وينر، فإن السيبرانية هي "علم القيادة والتحكم في الأحياء والآلات، ودراسة آليات التواصل داخلها"، وقد مثلت أفكاره خطوة نوعية في تصور العلاقة بين الإنسان والآلة، وأسست لمرحلة جديدة في تطوير الأنظمة الذكية و"العقول الإلكترونية"، وقد عبّر وينر عن رؤيته المتوازنة لهذه العلاقة

[1] أحمد عبيس نعمة الفتلاوي، مرجع سابق، ص. 214.

[2] إدريس عطية، **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، مجلة مصداقية، م1، ع1، 2019/12/01، ص. 103.

بقوله: أعطِ ما للإنسان للإنسان، وما للعقل الإلكتروني للعقل الإلكتروني." بهذا المعنى، شدد على أن التكنولوجيا، رغم تطورها المتسارع، يجب أن تظل أداة في يد الإنسان، تُسخَّر لخدمته، وأن القدرات الذكية للآلات لا ينبغي أن تحجب الدور الأخلاقي والقيادي للعنصر البشري.

ومن هنا، جاء ظهور علم السيبرنطيقا كواحد من أبرز ملامح التحول المعرفي في القرن العشرين، حيث ساهمت أبحاث وينر في إرساء الأسس الأولى لتطوير الأنظمة الذكية، التي أصبحت لاحقًا أساسًا لما يُعرف اليوم بالذكاء الاصطناعي والتحكم الآلي،[1]ولقد استند وينر في صياغة هذا العلم إلى دراسته لوظائف الجهاز العصبي البشري، وكيفية استجابته للمثيرات، وتصحيحه لمسارات السلوك بناءً على النتائج.

ومن خلال محاكاة هذه الوظائف، تم تصميم آلات قادرة على ضبط سلوكها ذاتيًا، دون الحاجة إلى إشراف بشري مباشر، مما مهد الطريق لظهور جيل جديد من الآلات الذكية التي تتمتع بقدرات حوسبة وتوجيه ذاتي تفوق الآلات التقليدية كالميكانيكية أو الكهربائية. وهكذا، كانت السيبرانية بمثابة الركيزة الفلسفية والتقنية التي ساهمت لاحقًا في نشأة مفاهيم مثل الفضاء السيبراني، والأمن السيبراني، والأنظمة المستقلة، لتصبح جزءًا من البنية المفاهيمية للعصر الرقمي الحديث.

3. تعريف الأمن السيبراني:

وفقًا لتعريف وزارة الدفاع الأمريكية فيتمحور مفهوم الأمن السيبراني حول "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث". [2]

وبحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول (اتجاهات الإصلاح في الاتصالات للعام) فيشير مصطلح الأمن السيبراني كونه "مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ يمكن استخدامها لحماية البيئة السيبرانية، وتهدف الحماية إلى جعل المعتدين يعدلون عن خططهم أو منعهم من تنفيذها عبر وضع خطة تتلاءم مع المحيط التقني والبشري والتنظيمي والقانوني للأفراد والمؤسسات[3]."

إذا ما تم تعريف الأمن السيبراني إجرائيًا فنجد أنه مجموعة تدابير وإجراءات هدفها حماية أجهزة

[1] إدريس عطية، مرجع سابق ، ص 103

[2] عبد الحميد ميار، عبد الحميد تقى، **دور القيادة السياسية الروسية في تعزيز الأمن السيبراني**، (2012/ 2023)، 22 جوان 2023، تاريخ الاطلاع: (06/04/2025)، نقلا عن الرابط التالي: https://bit.ly/4vt63QK

[3] المرجع نفسه.

الحاسوب وبرمجياته والشبكات والبيانات، وضمان منع الوصول الغير المصرح به إن كان نتيجة إتلاف بيانات أو أجهزة أو أي من الهجمات السيبرانية من خلال اعتماد التشفير، التحكم في الوصول للبيانات والمعلومات بالإضافة إلى اعتماد خطة بغية الاستجابة للحوادث أو استعادتها.

ثانيًا: نشأة الأمن السيبراني

ظهر مفهوم الأمن السيبراني بعد عدة عقود من اختراع الحاسوب، حيث تعود بداياته النظرية إلى أوائل السبعينيات،ففي عام 1971، طور الباحث بوب توماس (Bob Thomas) أول برنامج يُعد من نوع "دودة حاسوبية (Worm) "أطلق عليه اسمCreeper ، كان قادرًا على التنقل بين أجهزة الحاسوب المتصلة بشبكة ARPANET وهي الشبكة السابقة لشبكة الإنترنت الحالية [1].

وبهدف مواجهة هذا التهديد، قام الباحث راي توملينسون (Ray Tomlinson) المعروف أيضًا بابتكاره للبريد الإلكتروني بتطوير برنامج مضاد يُسمىReaper ، والذي كان يتتبع برنامج Creeper ويقوم بحذفه.

يُعد هذا البرنامج أول محاولة في التاريخ لتطوير أداة مضادة للبرمجيات الخبيثة، مما جعله بمثابة أول مضاد فيروسات بدائي، شهدت السبعينيات والسنوات اللاحقة تطورًا متسارعًا في مجال الحوسبة، وهو ما أدى إلى ظهور اختراقات أمنية حقيقية.

ففي عام 1979، ارتبط اسم كيفن ميتنيك(Kevin Mitnick) ، أحد أشهر القراصنة لاحقًا، بأول اختراق مهم لأنظمة التشغيل، وهو لا يزال حينها في سن المراهقة.

في الثمانينيات، ازدادت وتيرة التهديدات السيبرانية. ويُعد إطلاق "دودة موريس Morris) " (Wormفي عام 1988 من قبل روبرت تابان موريس(Robert Tappan Morris) ، أول هجوم واسع الانتشار عبر الإنترنت، حيث أصاب آلاف الأجهزة وأحدث اضطرابًا واسعًا في الشبكة، هذا الهجوم شكّل لحظة فاصلة في تاريخ أمن المعلومات، وساهم في إنشاء أول مركز للاستجابة لطوارئ الحاسوب في الولايات المتحدة،[2] من جهة أخرى، بدأ القطاع الخاص في تطوير حلول لمكافحة البرمجيات الخبيثة، ففي أواخر الثمانينيات، ظهرت شركات مثل McAfee وSymantec، وتبعتها شركات أخرى مثل Avast في بداية التسعينيات، لتقدم برامج مضادة للفيروسات بشكل تجاري.

ومع ذلك، كان ضعف البنية التحتية للشبكات في ذلك الوقت يحدّ من قدرة هذه البرامج على

[1] دحان حيزام القريطي، **الأمن السيبراني وحماية أمن المعلومات**، (الإسكندرية: دار الفكر الجامعي، 2022)، ص. 14.

[2] المرجع نفسه، ص. 16.

التحديث والاستجابة الفورية للتهديدات، وقد تبلورت أهمية الأمن السيبراني تدريجيًا، لاسيما بعد تزايد الهجمات الإلكترونية، وتنامي الاعتماد على الأنظمة الرقمية في مختلف القطاعات الحيوية، مما استدعى تدخل المؤسسات الحكومية والعسكرية لتنظيم المجال ووضع معايير أمنية صارمة.

وقد تسارع هذا التحول مع التزايد الملحوظ في حجم وتعقيد الهجمات الإلكترونية، وتوسع الاعتماد على التقنيات الرقمية في إدارة المرافق والخدمات الحيوية، مثل قطاعات الطاقة والاتصالات والإدارة الحكومية.

ومن أبرز المبادرات في هذا السياق، وضع وزارة الدفاع الأمريكية لمعايير تقييم أنظمة الحوسبة الموثوقة، المعروفة باسم Trusted Computer System Evaluation Criteria (TCSEC) عام 1983، والتي سُميت لاحقًا بـ "الكتاب البرتقالي."

إن تراكم هذه الأحداث والاختراقات والردود التقنية عليها، مهد الطريق نحو تشكيل مفهوم شامل للأمن السيبراني، باعتباره نظامًا متكاملًا لحماية الفضاء الرقمي من الهجمات الإلكترونية، وضمان سلامة البيانات وخصوصيتها واستمرارية الأنظمة.

المطلب الثاني: المفاهيم المرتبطة بالأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:[1]

أ-**الفضاء السيبراني:** عرفته الوكالة الفرنسية لأمن أنظمة الإعلامANSSI ، بأنه فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية كبيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو متسلسلين.

ب- الردع السيبراني: يعرف الردع السيبراني بأنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية.

الهجمات السيبرانية تعرف بأنها فعلًا يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام.

ج- الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو الأجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها وإجمالًا يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى تأمين البرمجيات وأجهزة الحاسوب، وحماية

[1] منى عبد الله السمحان، "**متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**"، مجلة كلية التربية، العدد 111، يوليو 2020، ص.11.

الفضاء السيبراني عمومًا من مختلف الهجمات والاختراقات والتهديدات الإلكترونية التي قد تُعرض الأمن القومي للدول للخطر.

د- أمن المعلومات (Information Security) : حماية بيانات المؤسسة ويعتمد ذلك على ثلاث محاور رئيسية ويرمز لها بـ CIA وهي السريةConfidentiality ،" سلامة المعلومةIntegrity "، "إتاحة المعلومة في أي وقت.

Availability عبارة عن مجموع من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي شكل غير مقصود أو غير مصرح به بالتلاعب أو الاختراق، الاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف.

المبحث الثالث: محددات وفواعل صنع السياسة العامة الأمنية الجزائرية

يمثل موضوع محددات وفواعل صنع السياسة العامة الأمنية في الجزائر أحد المحاور الأساسية لفهم كيفية تشكل القرار الأمني وتوجيهه في ظل بيئة متغيرة تتسم بتعدد التهديدات وتعقدها، خاصة مع بروز التهديدات السيبرانية والتحولات التكنولوجية المتسارعة.

وتتأثر هذه العملية بجملة من المحددات السياسية والمؤسساتية والاقتصادية والتقنية، إلى جانب تدخل فواعل رسمية وغير رسمية تسهم في صياغة وتنفيذ السياسة الأمنية. ويهدف هذا المبحث إلى تحليل أبرز هذه المحددات والفواعل وبيان طبيعة التفاعل بينها، من أجل فهم آليات بناء القرار الأمني في الجزائر في ظل التحديات الراهنة.

المطلب الأول: محددات السياسة العامة الأمنية الجزائرية

تتحدد السياسة العامة الأمنية الجزائرية من خلال مجموعة من العوامل الداخلية والخارجية التي تؤثر في صياغة القرار الأمني وتوجيهه لمواجهة مختلف التهديدات.

أ- المحددات الجيوسياسية:

تحتل الجزائر موقعًا جيوسياسيًا استراتيجيًا بالغ الأهمية، يجعلها نقطة التقاء لعدة فضاءات حيوية متداخلة، وهو ما ينعكس في تشكّل هويتها الاستراتيجية عبر ثلاثة أبعاد رئيسية مترابطة. ويتمثل البعد الأول في المجال المغاربي، الذي يشكل عمقًا تاريخيًا واجتماعيًا مشتركًا ضمن إطار "المغرب العربي

الكبير"، ورغم ما يعتريه من تحديات سياسية تعيق مسار التكامل المؤسسي، فإنه يظل عنصرًا أساسيًا في معادلة الأمن الإقليمي. أما البعد الثاني فيتجلى في الانتماء المتوسطي، حيث تؤدي الجزائر دور الجسر الحضاري والاقتصادي الرابط بين ضفتي المتوسط، بما يعزز موقعها في التفاعلات الأمنية والتجارية بين إفريقيا وأوروبا.

في حين يتمثل البعد الثالث في المجال الإفريقي، لا سيما فضاء الساحل، الذي يُعد امتدادًا جغرافيًا وأمنيًا شديد الحساسية، يتسم بتعقيدات طبيعية وبشرية وتحديات أمنية عابرة للحدود، الأمر الذي دفع الجزائر إلى تبني مقاربة نشطة وفاعلة داخل المنظمات القارية، وعلى رأسها الاتحاد الإفريقي ومبادرة "النيباد"، وبناءً على هذا التعدد في الانتماءات الجيوسياسية، تواجه الدولة الجزائرية ضرورة إدارة توازنات دقيقة تضمن حماية أمنها القومي وتعزيز حضورها ونفوذها في هذه الدوائر الجيو–استراتيجية المتشابكة[1]

ب– المحددات الجيواقتصادية:

تُبرز المحددات الجيواقتصادية في العقيدة الأمنية الجزائرية ارتباط الأمن القومي بالموارد الطاقوية، باعتبارها أحد أهم مصادر القوة والنفوذ الاستراتيجي للدولة، إذ تمتلك الجزائر احتياطيات مؤكدة تُقدَّر بحوالي 12.2 مليار برميل من النفط، ما يضعها في المرتبة 16 عالميًا، مع إنتاج يقارب 1.38 مليون برميل يوميًا، إضافة إلى احتياطيات غاز طبيعي تُقدَّر بنحو 159 تريليون قدم مكعب، لتحتل المرتبة الخامسة عالميًا في الإنتاج، والثانية أفريقيًا في تصدير الغاز، ما يجعلها فاعلًا محوريًا في أسواق الطاقة المتوسطية والأوروبية.

وفي هذا السياق، يشكل الاقتصاد الريعي القائم على المحروقات أحد أهم التحديات البنيوية، حيث يؤدي الاعتماد الكبير على عائدات الطاقة التي تمثل النسبة الأكبر من الصادرات والإيرادات العمومية إلى هشاشة هيكل الاقتصاد الوطني أمام تقلبات الأسعار العالمية، وإلى مخاطر ما يُعرف في الأدبيات الاقتصادية بـ"لعنة الموارد "و"المرض الهولندي"، بما ينعكس على ضعف تنويع القاعدة الإنتاجية واستمرار الفجوة بين الثروة المالية ومؤشرات التنمية الاقتصادية والاجتماعية.

استراتيجيًا، تعتمد الجزائر مقاربة تقوم على توظيف موقعها الجغرافي وإمكاناتها الطاقوية لتعزيز

[1] منصور لخضاري، **السياسة الأمنية الجزائرية: المحددات – الميادين – التحديات**، (الدوحة: المركز العربي للأبحاث و دراسات السياسات، ط1، 2015)، ص ص. 42–49.

أمنها القومي وترسيخ استقلال قرارها الخارجي، من خلال تنويع الشراكات الدولية والانفتاح على قوى صاعدة، وعلى رأسها الصين، التي برزت كشريك اقتصادي رئيسي في مجالات البنية التحتية والطاقة ضمن منطق براغماتي غير مشروط سياسيًا، ويأتي ذلك إطار التحول نحو" الجيواقتصاد "كأداة مركزية في إعادة تشكيل موازين القوى الدولية، حيث أصبحت الموارد الاقتصادية والطاقة عناصر حاسمة في تحديد النفوذ الاستراتيجي للدول.[1]

ج- المحددات الجيواستراتيجية

تُبرز المحددات الجيواستراتيجية الدور الحاسم في تشكيل السياسة العامة الأمنية الجزائرية، إذ يرتبط هذا التشكيل أساسًا بالموقع الجغرافي للجزائر الذي يجعلها همزة وصل بين إفريقيا وأوروبا والعالم العربي، وبامتداد حدودها الطويلة مع دول الساحل الأفريقي التي تتسم بالهشاشة السياسية والأمنية، ما يفرض عليها تحديات معقدة تتعلق بالإرهاب العابر للحدود، والجريمة المنظمة، والهجرة غير الشرعية.

وقد أدت هذه البيئة الجيوأمنية المضطربة إلى إعادة توجيه العقيدة الأمنية الجزائرية نحو مقاربة شاملة تقوم على الاستباقية وحماية الحدود وتعزيز التعاون الإقليمي، بدل الاقتصار على الدفاع التقليدي.

كما ساهم تصاعد التنافس الدولي في منطقة الساحل، خاصة بين الولايات المتحدة عبر قيادة "أفريكوم"، وفرنسا المرتبطة بمصالحها الطاقوية، والصين عبر توغلها الاقتصادي الناعم، في إعادة صياغة أولويات الأمن الجزائري، حيث تبنت الجزائر موقفًا يقوم على رفض الوجود العسكري الأجنبي مع الانخراط الانتقائي في التعاون الدولي.

وضمن هذا السياق، حافظت الجزائر على خصوصية مقاربتها الأمنية القائمة على احترام السيادة الوطنية وعدم التدخل، مع توظيف دبلوماسية أمنية نشطة في محيطها الإقليمي، بما يجعل سياستها الأمنية انعكاسًا مباشرًا لتداخل المحددات الجيوستراتيجية الإقليمية والدولية[2]

المطلب الثاني: فواعل صنع السياسة العامة الأمنية الجزائرية

تتعدد فواعل صنع السياسة العامة الأمنية في الجزائر بين فواعل رسمية وأخرى غير رسمية، والتي تتفاعل فيما بينها في صياغة وتوجيه القرار الأمني.

[1] منصور لخضاري، مرجع سابق، ص ص. 60-80.

[2] المرجع نفسه، ص ص. 82-116.

1. الفواعل الرسمية:

تُعد الفواعل الرسمية الركيزة الأساسية في عملية صنع وتنفيذ السياسات العامة، لما تتمتع به من صلاحيات قانونية ومؤسساتية تخولها التأثير المباشر في القرار العمومي.

أ- السلطة التنفيذية:

تمثل السلطة التنفيذية أحد المكونات المحورية في عملية صنع السياسات العامة، إذ تضطلع بمهمة تنفيذ التشريعات، وضمان حفظ النظام العام، وإدارة الشؤون الوطنية، وتختلف ملامح هذه السلطة باختلاف طبيعة النظام السياسي، حيث تتسم الأنظمة الرئاسية بتركيزها في يد رئيس الدولة، بينما تقوم الأنظمة البرلمانية على ثنائية بين الحكومة ورئيس الدولة، في حين تمارسها هيئة منتخبة في الأنظمة النيابية، وقد أشار دي تانسي إلى أن السلطة التنفيذية تتكون من رئيس الدولة وأعضاء الحكومة والجهاز الإداري المدني.

وتمارس هذه السلطة أدوارًا متعددة تشمل اقتراح السياسات العامة الجديدة، والإشراف على تنفيذها، واتخاذ قرارات حاسمة أثناء الأزمات، وممارسة صلاحيات تعيينية ذات بعد سياسي واستراتيجي، إضافة إلى إدارة قنوات الاتصال السياسي الرسمي عبر المؤتمرات والخطابات. ويظل مدى تأثيرها رهينًا بطبيعة التوازن المؤسسي بين السلطات، إذ يتسع نفوذها في الدول النامية مقارنةً بما هو عليه في الديمقراطيات التي تتميز بتوازن أكبر بين مختلف السلطات.[1]

ب- السلطة التشريعية:

تُعد السلطة التشريعية مؤسسة مركزية في صياغة واعتماد السياسات العامة، ويُناط بها الدور التشريعي الأساسي المتمثل في سن القوانين ومناقشة مشروعات القوانين المقدمة من السلطة التنفيذية، فضلًا عن ممارسة الرقابة على أداء الجهاز التنفيذي.

يشير كنيت بيس ونيكولاس مايس وغيل والت إلى أن السلطة التشريعية تجسد مبدأ السيادة الشعبية باعتبارها الهيئة الأعلى في عملية صنع القرار، وهو يقوم بحسب الباحثين بثلاثة أدوار أساسية: تمثيل الإرادة الشعبية، سن التشريعات، والإشراف على السلطة التنفيذية.[2]

---

[1] غابريال ألموند، بن جيهام باول، **السياسة المقارنة في وقتنا الحاضر**:ترجمة هشام عبد الله، (عمان:الأهلية للنشر والتوزيع، 1999)، ص. 171.

[2] عبد النور زوامبية، **دور السلطة التشريعية في رسم السياسة العامة في الجزائر**، مداخلة في الملتقى الوطني للسياسات العامة ودورها في بناء الدولة وتنمية المجتمع بجامعة مولاي الطاهر، سعيدة، تاريخ الانعقاد 2009، ص ص. 13-14.

كما يُضاف إلى ذلك دورها في موازنة المصالح السياسية، والتشاور مع المجتمع المدني والقطاع الخاص، وضمان الاستمرارية في تنفيذ السياسات. ويؤكد دي تانسي أن وظيفة المشرعين تتجاوز الإطار التشريعي إلى مهام الرقابة والمساءلة، بما في ذلك التحكم في الموازنة العامة، الأمر الذي يعزز من موقعهم ضمن عملية صنع السياسات العامة.

ج /السلطة القضائية

تمثل السلطة القضائية أحد الأعمدة المؤسسية المؤثرة في دورة السياسة العامة، إذ تضمن الالتزام بتطبيق القوانين وتفصل في النزاعات الناشئة عن تفسيرها، كما تضطلع بمهمات أخرى تشمل الرقابة الدستورية على القوانين واللوائح، وصياغة وتفسير النصوص القانونية، والفصل في المنازعات بين الأفراد والدولة، إضافة إلى تحقيق العدالة.[1]

ويُعد استقلالها المؤسسي شرطًا جوهريًا لممارسة هذه المهام، إذ يشكل في الأنظمة الديمقراطية أساسًا لقيامها بدور فاعل في مراجعة شرعية السياسات العامة وضبطها دستوريًا، بينما ينحسر هذا الدور في الدول النامية بفعل هيمنة السلطة التنفيذية، وهو ما يُضعف من فعالية القضاء في عملية صنع السياسة العامة، وعليه فإن مكانة القضاء في الحياة السياسية تبقى مرتبطة بمدى تكريس مبدأ الفصل بين السلطات.

د /الجهاز الإداري

لم يعد الجهاز الإداري مقتصرًا على مهمة التنفيذ، بل أصبح فاعلًا محوريًا في صياغة وتوجيه السياسات العامة بفضل ما يمتلكه من خبرات فنية وموارد معرفية، ويتجسد دوره من خلال مساهمات مباشرة تتمثل في اقتراح مشاريع القوانين أو تعديلها استنادًا إلى تحليلات متخصصة، وأخرى غير مباشرة تتمثل في تفسير السياسات أثناء التنفيذ وتوجيه مساراتها عبر الاستشارات الفنية.[2]

وتعزز مكانة الجهاز الإداري عدة عوامل، من بينها قربه من المواطنين بما يتيح له تقييم فعالية السياسات العامة، والتعقيد المتزايد للقضايا المجتمعية الذي يستدعي الاعتماد على خبراته الفنية، إضافة إلى تفويضه بصلاحيات تشريعية ثانوية من خلال اللوائح التنفيذية، وعليه فإنه يمثل فاعلًا أساسيًا

[1] حسن أبشر الطيب، مرجع سابق، ص – ص 156- 158.

[2] عزيزة ضمبري، **الفواعل السياسية دورها في صنع السياسة العامة في الجزائر**"، رسالة ماجستير غير منشور، جامعة الحاج لخضر، كلية الحقوق، باتنة 2008/2007، ص. 25.

في ضمان الاستمرارية المؤسسية وتكييف السياسات مع المتغيرات التقنية والاجتماعية.

2. الفواعل غير الرسمية

تُعد الفواعل غير الرسمية عنصرًا مكملًا ومؤثرًا في عملية صنع السياسات العامة، حيث تساهم بشكل غير مباشر في توجيه القرار العمومي والتأثير في توجهاته .

أ /الأحزاب السياسية

تُعتبر الأحزاب السياسية تنظيمًا اجتماعيًا وسياسيًا يهدف إلى التعبير عن مصالح فئات محددة، والسعي إلى التأثير في السلطة أو الوصول إليها عبر الانتخابات أو المشاركة في الهيئات المنتخبة.

وتؤثر الأحزاب في صنع السياسات من خلال عدة آليات: ترشيح الممثلين للمناصب العامة، المشاركة في المداولات السياسية، تنظيم الحملات والمظاهرات، بناء التحالفات والائتلافات، تعبئة الرأي العام، وممارسة المنافسة السياسية ضد الأحزاب الأخرى، وبهذا تمثل الأحزاب قناة مؤسسية لتجميع المصالح والتعبير عنها ضمن الإطار السياسي الرسمي.[1]

ب /جماعات الضغط

تُعرف جماعات الضغط بأنها تجمعات ذات مصالح مشتركة، غالبًا مهنية أو اقتصادية، تسعى إلى التأثير على مسار صنع القرار بما يحافظ على مصالحها.

ووفقًا لماري جان ماري دنكان، تمارس هذه الجماعات تأثيرها عبر وسائل متنوعة :استخدام الإعلام للتأثير على البرلمانيين، التشاور المباشر مع الحكومة، التهديد العلني في قضايا محددة، بناء علاقات غير رسمية مع النخب، والتأثير على الرأي العام من خلال الحملات الدعائية أو الإضرابات ،وبذلك، تشكل جماعات الضغط أداة ضغط فعّالة على السياسات العامة، بما فيها السياسات الأمنية.[2]

ج /الرأي العام

يمثل الرأي العام اتجاهًا جماعيًا ناتجًا عن تفاعل آراء الأفراد والجماعات داخل المجتمع، ويُعد مؤشرًا على القبول أو الرفض الشعبي للسياسات العامة، لا يُنظر إليه كمجرد مجموع للآراء الفردية، بل كنتاج ديناميكي لتفاعلها، مما يمنحه وزنًا مؤثرًا على صانعي القرار، سواء من خلال استجابته المباشرة

[1] جيمس أندرسون، مرجع سابق، ص 65.

[2] عبد النور ناجي ومبروك ساحلي، **مقدمة في دراسة السياسة العامة**، (عنابة: دار العلوم للنشر والتوزيع، 2014)، ص. 46.

لمطالب المجتمع أو عبر وسائط كالأحزاب والإعلام.[1]

د /وسائل الإعلام

تشكل وسائل الإعلام فاعلًا غير رسمي مؤثرًا في عملية صنع السياسات العامة، لما تمتلكه من قدرة على تحديد أولويات الأجندة العامة وتوجيه الرأي العام، وقوم بدور الوسيط بين المجتمع وصانع القرار عبر نقل المعلومات، تأطير القضايا، وتوليد الضغوط السياسية.

وبذلك، تمثل الإعلام قوة تأثير غير مباشرة، لكنه حاسم في تشكيل البيئة الاجتماعية والسياسية التي تُصاغ ضمنها السياسات الأمنية.[2]

[1] جيمس أندرسون، مرجع سابق، ص. 67.

[2] حسن أبشر طيب، مرجع سابق، ص. 184 – 186.

خلاصة الفصل الأول:

يتضح أن السياسة العامة الأمنية، في ظل التحولات التكنولوجية المتسارعة، لم تعد مقتصرة على البعد التقليدي لحماية الدولة، بل أصبحت إطارًا مركبًا يتداخل فيه البعد النظري والمؤسساتي مع التطور السيبراني.

وقد أظهر تعدد التعريفات والنظريات المفسرة للسياسة العامة والأمن الأمني اختلاف زوايا التحليل بين القوة، والمؤسسات، وتفاعل الفاعلين داخل النظام السياسي، بينما يبرز الأمن السيبراني كمجال حديث يهدف إلى حماية الفضاء الرقمي عبر أبعاد تقنية وتنظيمية وبشرية تمتد آثارها إلى المجالات العسكرية والاقتصادية والاجتماعية والقانونية والسياسية.

وفي السياق الجزائري، تتشكل السياسة الأمنية من خلال محددات جيوسياسية وجيواقتصادية وجيواستراتيجية، إضافة إلى تعدد الفواعل الرسمية وغير الرسمية، مما يجعل عملية صنع القرار الأمني عملية معقدة وتفاعلية تتطلب مقاربة شاملة ومتكاملة.

الفصل الثاني: السياسة العامة الجزائرية في مجال الأمن السيبراني

– الواقع والتقييم والآفاق–

أدى التوسع المتزايد في استخدام التقنيات الرقمية والاعتماد المتنامي على الأنظمة المعلوماتية في مختلف القطاعات إلى بروز تحديات أمنية جديدة فرضت على الدول إعادة النظر في سياساتها الأمنية وتطوير آليات أكثر فعالية لمواجهة المخاطر السيبرانية، ولم تعد التهديدات السيبرانية تقتصر على استهداف الأفراد أو المؤسسات الخاصة، بل أصبحت تمس الأمن الوطني والسيادة الرقمية للدول، نظراً لقدرتها على التأثير في البنى التحتية الحيوية والأنظمة الاقتصادية والإدارية والعسكرية.

وفي هذا السياق، تسعى الجزائر إلى بناء سياسة عامة أمنية قادرة على مواجهة التحولات التي يشهدها الفضاء السيبراني، من خلال تطوير الأطر القانونية والمؤسساتية وتعزيز القدرات التقنية والبشرية اللازمة للتصدي للجرائم والتهديدات الرقمية، غير أن فعالية هذه السياسة تظل مرتبطة بمدى قدرتها على التكيف مع التطورات المتسارعة للبيئة السيبرانية، فضلًا عن قدرتها على الاستفادة من التجارب الدولية الرائدة في هذا المجال.

المبحث الأول: السياسة العامة الأمنية الجزائرية في مواجهة تهديدات الأمن السيبراني

يمثل الأمن السيبراني أحد أهم أبعاد السياسة العامة الأمنية في الجزائر في ظل التحولات الرقمية المتسارعة وما رافقها من تصاعد في حجم وتعقيد التهديدات الإلكترونية التي مست مختلف القطاعات الحيوية للدولة، وهو ما فرض على صانع القرار الأمني إعادة النظر في أدواته وآلياته التقليدية نحو تبني مقاربة شاملة ومتكاملة تجمع بين الأبعاد القانونية والمؤسساتية والتقنية والبشرية بما يعزز حماية الفضاء السيبراني الوطني.

وفي هذا السياق لم يعد الأمن السيبراني مجرد بعد تقني بل أصبح جزءاً من منظومة الأمن القومي يرتبط بالسيادة الرقمية للدولة وقدرتها على حماية بنيتها التحتية المعلوماتية وبياناتها الاستراتيجية، كما يتأثر بجملة من المحددات الداخلية والخارجية ويعتمد على تفاعل فواعل متعددة على المستويات الوطنية والإقليمية والدولية.

وعليه يهدف هذا المبحث إلى تحليل السياسة العامة الأمنية الجزائرية في مواجهة تهديدات الأمن السيبراني من خلال دراسة تطور الإطار القانوني والمؤسساتي واستعراض أبرز التهديدات السيبرانية وتحليل الإجراءات المعتمدة على المستويات التشريعية والمؤسسية والتقنية والبشرية وصولاً إلى إبراز أهم التحديات التي تعيق تحقيق السيادة السيبرانية في الجزائر.

المطلب الأول: نشأة الأمن السيبراني في الجزائر

شهدت الجزائر، على غرار باقي دول العالم، تحولات رقمية متسارعة أدت إلى بروز الحاجة إلى تبني منظومة متكاملة للأمن السيبراني، وذلك نتيجة تزايد الاعتماد على تكنولوجيات الإعلام والاتصال وما صاحب ذلك من تهديدات إلكترونية متنامية، ويُعرَّف الأمن السيبراني باعتباره مجموعة من الآليات التقنية والقانونية والتنظيمية الهادفة إلى حماية الأنظمة المعلوماتية والشبكات والبيانات من مختلف أشكال الاختراق والاعتداء الرقمي.

وقد مرت نشأة هذا المجال في الجزائر بعدة مراحل متتالية، حيث تميزت المرحلة الأولى، الممتدة إلى ما قبل سنة2004 ، بغياب إطار قانوني واضح نتيجة محدودية استخدام الإنترنت آنذاك، في حين شهدت المرحلة الثانية (2009–2004) بداية التأسيس التشريعي من خلال إصدار قوانين أساسية، على غرار القانون رقم 15–04 المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والقانون رقم–09

04المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مما شكل النواة الأولى لتنظيم المجال.

أما المرحلة الثالثة (2010–2018) فقد عرفت تعزيزًا للإطار القانوني والمؤسساتي، خاصة مع إدراج نصوص تتعلق بحماية البيانات الشخصية والتجارة الإلكترونية، إلى جانب تطوير آليات التحقيق الرقمي، وصولًا إلى المرحلة الحديثة التي اتسمت بتبني مقاربة شاملة للأمن السيبراني في ظل التحول نحو الحكومة الإلكترونية، وإنشاء هيئات مختصة مثل الوكالة الوطنية لأمن الأنظمة المعلوماتية، التي تضطلع بدور محوري في حماية البنية التحتية الرقمية وتعزيز الوعي الأمني.

وقد ساهمت عدة عوامل في تسريع هذا التطور، من بينها تزايد استخدام الإنترنت، وارتفاع معدلات الجرائم الإلكترونية، والحاجة إلى حماية الأمن الوطني والاقتصاد الرقمي، غير أن الجزائر لا تزال تواجه جملة من التحديات، أبرزها نقص الكفاءات المتخصصة، والتطور المستمر لأساليب الهجمات السيبرانية، وصعوبة تتبع الجرائم ذات الطابع العابر للحدود.

وعليه، يمكن القول إن الأمن السيبراني في الجزائر انتقل من مرحلة الغياب إلى مرحلة البناء والتعزيز، ليصبح اليوم عنصرًا أساسيًا في استراتيجية الدولة الرامية إلى تحقيق الأمن والاستقرار في الفضاء الرقمي.[1]

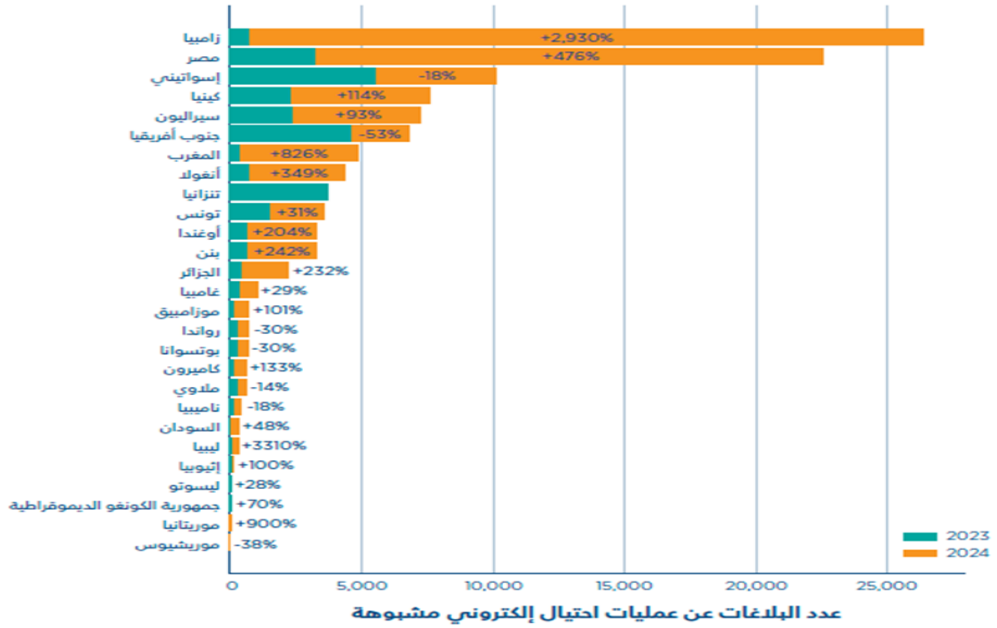
المطلب الثاني: أنواع التهديدات الأمنية السيبرانية في الجزائر

يشهد الفضاء السيبراني في الجزائر تصاعدًا كبيرًا في حجم وتعقيد التهديدات الرقمية، حيث سُجل حوالي 70 مليون هجوم سيبراني سنة 2024، من بينها أكثر من 13 مليون محاولة تصيد احتيالي، ونحو 1,200 حادثة اختراق بيانات، مع معدل سرقة هوية يقدر بـ 3.5 حالة لكل 1,000 نسمة، كما تتصدر البرمجيات الخبيثة قائمة التهديدات بنسبة 31.85%، تليها هجمات التصدي بنسبة 16.38%، وإصابات الهواتف الذكية بنسبة 21.97%، إضافة إلى تنامي هجمات الفدية والاحتيال الرقمي، وهو ما يعكس الطابع البنيوي والمستمر لهذه التهديدات[2].

[1] وهيبة لعور، **الامن السيبراني في الجزائر،سياسات و مؤسسات**، مجلة الفكر الشرطي، ع 28، 2022، ص ص.275–277.

[2] **استراتيجية الأمن السيبراني الوطنية للجزائر 2025-2029:** تحليل معمّق، 15ديسمبر2025، تاريخ الاطلاع: (10جانفي 2026)، نقلا عن الرابط التالي : https://tinyurl.com/2hmuratc

شكل1: الزيادة في تبليغات عن عمليات الاحتيال الإلكتروني في جميع المناطق في إفريقيا بين عامي 2023 و2024



المصدر: بيانات قدمتها شركة كاسبرسكي عبر موقعها الرسمي .

المطلب الثالث: الإجراءات التي تتبناها السياسة العامة الجزائرية في مواجهة الجرائم السيبرانية

تعتمد السياسة العامة الجزائرية في مواجهة الجرائم السيبرانية على مجموعة من الإجراءات، التي تهدف إلى تعزيز الحماية الرقمية، وتطوير قدرات الاستجابة، والحد من مختلف التهديدات السيبرانية.

1.تعريف الجريمة السيبرانية

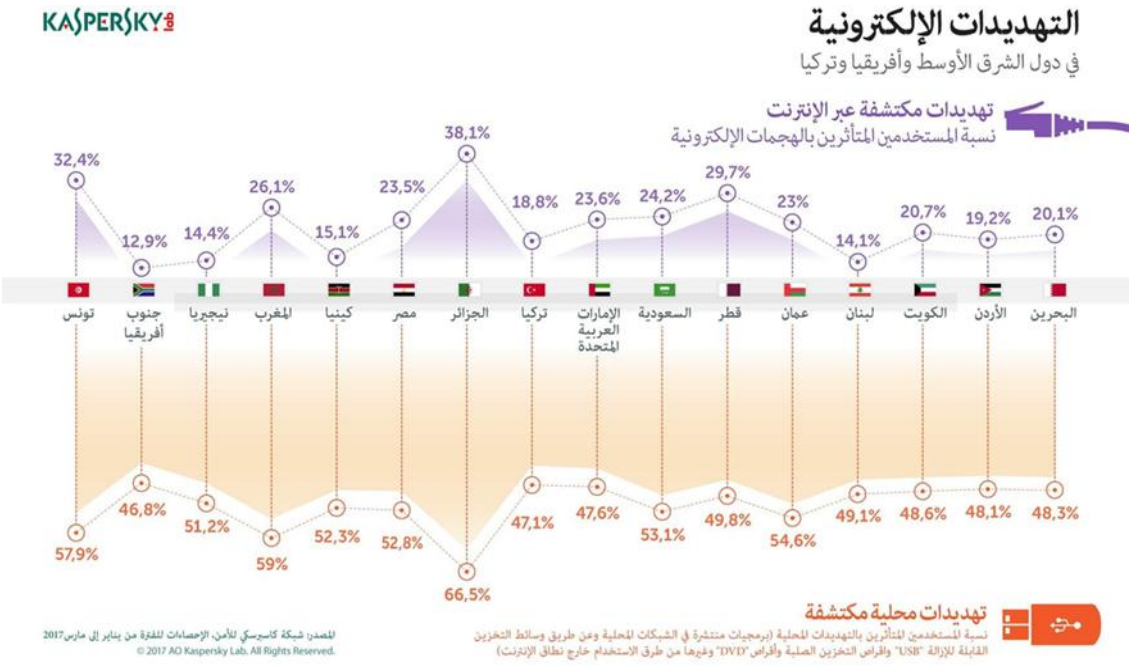
لم يحظَ مفهوم الجريمة السيبرانية بتعريف موحَّد في الأدبيات الفقهية والبحثية، حيث تباينت الرؤى باختلاف المنطلقات التي استند إليها الباحثون، فبينما انصب اهتمام بعضهم على موضوع الجريمة في حد ذاته، ركّز آخرون على الأداة التقنية المستعملة في ارتكابها.

وفي هذا السياق، عُرّفت الجريمة السيبرانية بأنها" :سلوك غير قانوني أو غير أخلاقي يُرتكب عبر الشبكات المعلوماتية العالمية، ويُشكل تهديدًا لمجالات المال والمعرفة والثقة والسمعة، ويتم تنفيذه بالكامل باستخدام الوسائل التقنية الحديثة."[1]

[1] علي قويدري، امال العيش، **الجريمة السيبرانية مفهومها وسبل الوقاية منها**، مجلة نوميرس الاقتصادية، م 03 ، ع 01، 2022، ص194.

أما في التشريع الجزائري، فلم يتبنَّ المشرّع مصطلحًا موحّدًا للتعبير عن هذه الظاهرة، بل استخدم تسميات متعدّدة ضمن نصوصه القانونية، فقد وردت في القانون رقم 04-15 تحت تسمية" الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات"[1]، كما استُخدم تعبير" الجرائم المتصلة بتكنولوجيا الإعلام والاتصال " في القانون رقم 04-09 المتعلق بالوقاية من هذه الجرائم، ويُفهم من خلال هذه المصطلحات أنّ المشرّع الجزائري يُقارب الجريمة السيبرانية على نحو ضمني باعتبارها كل الأفعال الإجرامية التي تستهدف أو تُرتكب عبر الأنظمة المعلوماتية أو وسائل الاتصال الإلكترونية، سواء بشكل مباشر أو غير مباشر.

شكل2: التهديدات الإلكترونية في دول الشرق الأوسط وأفريقيا وتركيا وفق شركة كاسبرسكي للأمن السيبراني.



المصدر :الموقع الرسمي لشركة كاسبرسكي.

2. الإجراءات على المستوى الوطني

تُعد الإجراءات على المستوى الوطني إطارًا عامًا تتداخل فيه مختلف السياسات والتدابير الهادفة إلى تعزيز منظومة الأمن السيبراني، من أبرزها:

[1] القانون رقم 15/04، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، (2004).

1.2. الإجراءات المؤسسية

يتسم البعد المؤسسي بتعدد الهياكل الوطنية ذات الصلة بالأمن السيبراني، حيث تتوزع مهامها بين التخطيط الاستراتيجي والإشراف والتنفيذ والتحقيق، وتتجسد هذه الأبعاد المؤسسية في مجموعة من المؤسسات الوطنية التي تضطلع بأدوار محورية في مجال الأمن السيبران، من أبرزها:

1.1.2. المجلس الأعلى للأمن :هيئة استشارية لرئيس الجمهورية، أُنشئت بموجب دستور 1976، تختص بوضع التوجهات العليا للأمن القومي، بما في ذلك مواجهة التهديدات السيبرانية الكبرى.[1]

2.1.2. وزارة الدفاع الوطني :تضطلع بدور قيادي في صياغة وتنفيذ الاستراتيجيات السيبرانية، وتشرف على هيئات مركزية في هذا المجال، من بينها تنظيم الملتقيات الوطنية.

3.1.2. المجلس الوطني لأمن الأنظمة المعلوماتية :أُنشئ بالمرسوم الرئاسي05–20 ، ويرأسه وزير الدفاع الوطني أو من ينوبه، ويضم ممثلين عن الرئاسة والوزارات السيادية .يتولى اعتماد الاستراتيجيات الوطنية، والإشراف على الوكالة الوطنية، والمصادقة على اتفاقيات التعاون، والتصديق الإلكتروني، وتصنيف الأنظمة المعلوماتية.

4.1.2. الوكالة الوطنية لأمن الأنظمة المعلوماتية :(ANSSI) مؤسسة عمومية إدارية أُنشئت بموجب المرسوم05–20 ، مكلفة بتحضير الاستراتيجيات، والتحقيق في الهجمات، وتنسيق التدابير الوقائية، وتطوير التشريعات والأدوات المرجعية، إضافة إلى أنشطة التدريب واليقظة التكنولوجية. [2]

5.1.2. الدرك الوطني: يضم مركز الوقاية من جرائم الإعلام الآلي أنشئ عام (2008) والمعهد الوطني للأدلة الجنائية أنشئ عام (2009)، ويضطلع بمهام التحقيق، الرصد، والتحليل الجنائي الرقمي.

6.1.2. المديرية العامة للأمن الوطني :(DGSN) تضم المصلحة المركزية لمكافحة الجريمة المعلوماتية أُنشئت عام(2011) ، المكلفة بالتحقيق في الجرائم السيبرانية ضمن الشرطة القضائية.[3]

7.1.2. الهيئة الوطنية للوقاية من الجرائم السيبرانية :(ONPLITIC) سلطة إدارية مستقلة أُنشئت بالمرسوم261–15 ، تتبع وزارة العدل، وتختص بالوقاية من الجرائم المعلوماتية، ودعم السلطات القضائية، والمراقبة الإلكترونية للاتصالات في القضايا الحساسة ذات الصلة بالأمن الوطني[4] .

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، دستور 1976، المادة 125، الجريدة الرسمية للجمهورية الجزائرية، العدد 5، (25 فبراير 1976).

[2] المرجع نفسه.

[3] إلياس شاهد، الحلاج عرابة، عبد النعيم دفرو، **تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر**، المجلة الجزائرية للدراسات المحاسبية والمالية، ع. 3، (ديسمبر 2016)، ص. 130.

[4] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 15–261، المؤرخ في 8 أكتوبر 2015، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، (2015).

2.2. الإجراءات التشريعية

يمثل الإطار القانوني الأساس التنظيمي للسياسة السيبرانية الوطنية، وقد تطور تدريجياً استجابةً للتحولات التكنولوجية:

- ✓ **البدايات** :عالج المشرع بعض القضايا ضمن قوانين قائمة مثل الأمر 03-05 المتعلق بحقوق المؤلف، الذي صنف برامج الحاسوب كمصنفات أدبية محمية.[1]
- ✓ **التجريم الخاص: القانون 15-04** الذي أدخل تعديلات على قانون العقوبات تخص المساس بأنظمة المعالجة الآلية، تلاه القانون 23-06 الذي وسع نطاق التجريم ليشمل الدخول غير المشروع، تعديل البيانات، أو الاتجار غير القانوني بالمعلومات.[2]
- ✓ **الإطار المحوري: القانون 04-09** المتعلق بالوقاية من الجرائم السيبرانية، وضع تعريفاً شاملاً لهذه الجرائم، وأرسى آليات وقائية وإجرائية، أهمها: [3]
- ✓ **المراقبة الإلكترونية:** بإذن قضائي في قضايا الإرهاب والأمن القومي (المادة4).
- ✓ **التعاون مع مزودي الخدمات:** إلزامهم بحفظ بيانات المرور وحجب المحتوى غير القانوني (المادتان 11و.12)
- ✓ **التفتيش والحجز:** بما في ذلك التفتيش عن بعد، والاستعانة بالخبراء (المادتان 3 و.7)
- ✓ **الاختصاص القضائي الموسع:** لمتابعة الجرائم المرتكبة خارج الإقليم ضد مؤسسات الدولة.
- ✓ **التعاون الدولي:** تبادل المساعدة القضائية في جمع الأدلة الإلكترونية.

الإطار التشريعي يتكامل مع قانون العقوبات وقانون الإجراءات الجزائية، ويُظهر توجهاً نحو التجريم والوقاية، مع بروز تحديات في التطبيق العملي تتعلق بالتقنيات الحديثة والتحديث المستمر للقوانين.

وعزز المرسوم الرئاسي رقم 07-26 الصادر بتاريخ 7 يناير 2026، والمنشور في الجريدة الرسمية بتاريخ 21 يناير، ينص على تنظيم وعمل وحدات الأمن السيبراني داخل المؤسسات والإدارات العامة، وتهدف هذه التدابير إلى تحسين الوقاية من مخاطر الهجمات السيبرانية وإدارتها،[4] ويُلزم كل كيان

[1] الأمر رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية،ع04، 2005.

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

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

[4] المرسوم الرئاسي رقم 26-07، المؤرخ في 7 جانفي 2026، المتعلق بإنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في كل مؤسسة وإدارة وهيئة عمومية وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 04، 2026.

عام بإنشاء وحدة متخصصة للأمن السيبراني، منفصلة عن الإدارة المسؤولة عن الإدارة الفنية لأنظمة تقنية المعلومات، ترفع هذه الوحدة تقاريرها مباشرة إلى رئيس المؤسسة، وتتولى تنسيق جميع الإجراءات المتعلقة بحماية البيانات وأمن الأنظمة، بما في ذلك بين الجهات الخاضعة لإشرافها.

وتُكلف الوحدة بوضع سياسة للأمن السيبراني والإشراف على تنفيذها، كما تقوم بإجراء عمليات مسح للمخاطر، وتصميم خطط معالجة مناسبة، وضمان المراقبة المستمرة والتدقيق الدوري، ويجب الإبلاغ عن أي حادث فورًا إلى السلطات المختصة، وينص المرسوم أيضًا على الامتثال لتشريعات حماية البيانات الشخصية، بالتنسيق مع الهيئة الوطنية المختصة بهذا القطاع.

تشجع هذه المبادرة التعاون مع جهات المشتريات العامة وهيئات الأمن الداخلي لضمان إدراج بنود أمنية في عقود التعهيد، وتعزيز حماية الموظفين والمعدات، ولا يعمل القانون 04-09 بمعزل عن باقي التشريعات، بل يتكامل مع قانون العقوبات وقانون الإجراءات الجزائية الذي استحدث بدوره إجراءات خاصة تتناسب مع طبيعة الجرائم السيبرانية، مثل اعتراض المراسلات، والتسرب الإلكتروني.

3.2. الإجراءات التقنية والتكنولوجية

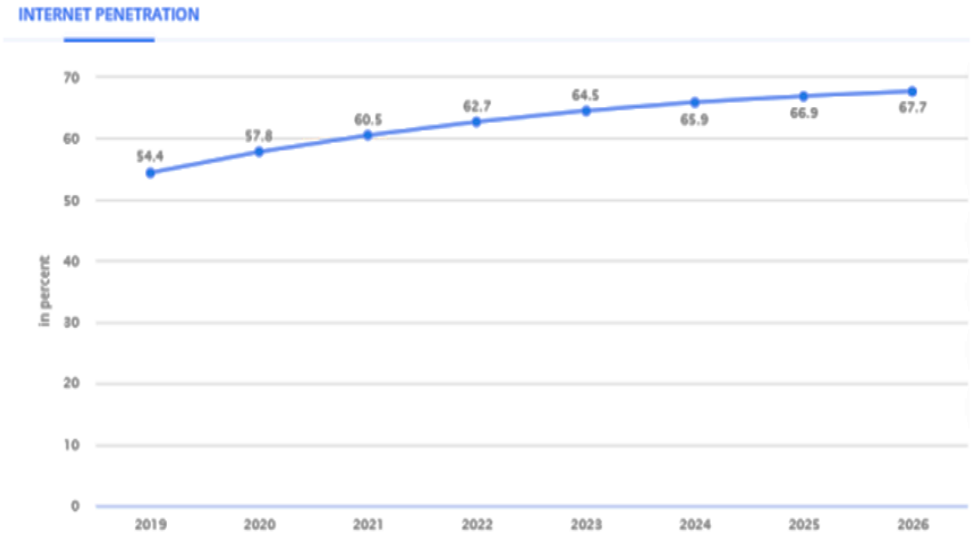
يشهد قطاع الاتصالات والإنترنت في الجزائر تطورًا ملحوظًا يعكس تسارع وتيرة التحول الرقمي، حيث بلغ عدد اشتراكات الهاتف المحمول حوالي 55.6 مليون اشتراك نهاية سنة2025، وهو ما يعادل 117%من إجمالي عدد السكان، في دلالة على انتشار استخدام الشرائح المتعددة وتوسع خدمات الاتصالات، كما تُظهر البيانات أن 94.5% من هذه الاشتراكات تندرج ضمن خدمات النطاق العريض (3G/4G/5G)، مما يعكس تحسن البنية التحتية الرقمية.

وفيما يتعلق باستخدام الإنترنت، فقد بلغ عدد المستخدمين 37.8 مليون مستخدم، بنسبة انتشار قدرت بـ 79.5% من السكان، مع تسجيل نمو سنوي قدره4.8%، غير أن حوالي 20.5% من السكان ما يعادل 9.74 مليون شخص لا يزالون خارج الفضاء الرقمي، ما يعكس استمرار الفجوة الرقمية.

ومن حيث جودة الخدمة، تشير بيانات Ookla إلى أن متوسط سرعة الإنترنت عبر الهاتف بلغ 41.21ميغابت/ثانية، مقابل 37.86 ميغابت/ثانية للإنترنت الثابت، مع تسجيل زيادات سنوية معتبرة بلغت 65.5% و 165%على التوالي، وتعكس هذه المؤشرات مجتمعة تحسنًا تدريجيًا في أداء قطاع الاتصالات، رغم استمرار بعض التحديات المرتبطة بالإدماج الرقمي الشامل[1] .

[1] Kepios, "Digital **Algeria," published by DataReportal**, 08/nov/2025, accessed on: (16/03/2026), Retrieved from the following link: https://tinyurl.com/52nakvtc

شكل3: نسبة انتشار الإنترنت في الجزائر



المصدر : statista, ITU, international telecommunication, internet penetration

ويشكّل الجانب التكنولوجي أحد الركائز الجوهرية للسياسة الأمنية السيبرانية، إذ يتقاطع في إطاره ما تتيحه التحولات الرقمية من فرص استراتيجية مع ما تطرحه التهديدات السيبرانية المتنامية من مخاطر معقدة، وفي هذا السياق، تعي الجزائر الأهمية الحيوية لهذا البعد، وتسعى إلى تعزيز بنيتها التحتية الرقمية وتطوير قدراتها التقنية لمواكبة هذه التحديات، لاسيما في ظل الانخراط في تبنّي تقنيات الجيل الخامس (5G)وما ينجم عنها من تحولات هيكلية عميقة، ويمثّل إدماج هذه التقنيات قفزة نوعية في مسار التحول الرقمي بالجزائر، بما يتيحه من آفاق واسعة في الاتصالات فائقة السرعة، إنترنت الأشياء، والخدمات الذكية، غير أن هذا التطور يثير في الوقت ذاته جملة من التحديات الأمنية البالغة، أبرزها:

تعدد نقاط الهجوم، هشاشة البنى التحتية الحيوية، وتعقيد الشبكات اللامركزية بما يصعّب عمليات المراقبة والاكتشاف.[1]

في هذا السياق، تعمل الجزائر على تعزيز قدراتها التقنية من خلال استراتيجية وطنية للأمن السيبراني تستند إلى مبادئ السيادة الرقمية، بناء أنظمة مرنة، دعم الرقمنة الحكومية، وتهيئة بيئة وطنية مواتية، وفي إطار تعزيز هذا المسار، تسعى الجزائر أيضًا إلى توسيع شراكاتها الدولية، على غرار

[1] مصطفى بن ميرة، **G5 في الجزائر: بين حلم التحول الرقمي وكابوس التهديد السيبراني**"، 06/ 05/ 2025،تاريخ الاطلاع: (2025/05/16)، نقلا عن الرابط التالي: https://bit.ly/3OqJjQu

التعاون الجزائري–الروسي الذي يهدف إلى دعم البنية التحتية السيبرانية وتطوير قدرات الشركة الجزائرية EPE PROXYLAN SPA التابعة لمركز البحث في الإعلام العلمي والتقني.(CERIST)

ويعكس هذا التوجه إدراكًا عميقًا لأهمية البعد التكنولوجي باعتباره ساحة تنافسية بين التطور الدفاعي وتنامي التهديدات، الأمر الذي يستوجب استثمارًا مستدامًا في التقنيات الحديثة، إلى جانب تطوير دائم للقدرات الوطنية لضمان أمن الفضاء السيبراني كجزء لا يتجزأ من عملية التحول الرقمي الشاملة.

4.2. الإجراءات البشرية والمجتمعية

يشكّل العنصر البشري محورًا أساسيًا في أي سياسة فعالة للأمن السيبراني، فهو في آن واحد خط الدفاع الأول ومصدر هشاشة محتمل في حال غياب التأهيل والتوعية، وانطلاقًا من هذا الإدراك تولي الجزائر اهتمامًا متزايدًا لبناء الكفاءات الوطنية وتعزيز الوعي السيبراني على المستويين المؤسسي والمجتمعي، حيث تُعدّ تنمية الموارد البشرية المتخصصة حجر الزاوية في الاستراتيجية الوطنية، ويتجلى هذا التوجه من خلال مبادرات عملية في قطاعات حيوية؛ ففي القطاع الصحي شهد شهر يونيو 2024 تنظيم دورة تكوينية بالشراكة بين وزارة الصحة ومؤسسة "بروكسيلان" التابعة لمركز(CERIST) ، استفاد منها أكثر من 90 مهندسًا في مجال أمن البيانات الصحية، كما شهد القطاع المصرفي في أبريل 2025 شراكة مع شركة "كاسبرسكي" العالمية لتعزيز الثقافة الأمنية وتطوير المهارات المتخصصة، بما يعكس إدراك الجزائر لأهمية الاستثمار في العنصر البشري باعتباره الركيزة الأساسية لتعزيز المناعة السيبرانية الوطنية. [1]

إلى جانب ذلك، تتجه الجهود نحو إدماج الأمن السيبراني في المنظومة التعليمية والتكوينية، سواء عبر مؤسسات أكاديمية متخصصة كـ" المدرسة العسكرية المتعددة التقنيات"، أو من خلال الدورات التدريبية وبرامج التوعية الموجهة للمؤسسات والأفراد ، وتهدف هذه البرامج إلى ترسيخ ثقافة أمنية قائمة على الممارسات السليمة مثل حماية الخصوصية، التصدي للهندسة الاجتماعية، والاستخدام الآمن للبيانات، وبذلك، يتضح أنّ بناء القدرات البشرية وتعميم الوعي يشكّلان بعداً استراتيجياً مكملاً للجهود التقنية والتنظيمية، بما يعزز مرونة الفضاء السيبراني الوطني في مواجهة التهديدات المتصاعدة.[2]

[1] وزارة الصحة الجزائرية، "دورة تكوينية حول أمن البيانات الصحية"، 06جوان 2024، تاريخ الاطلاع: (2025/01/12)، نقلا عن الرابط التالي: https://bit.ly/41eFRLN

[2] وزارة الدفاع الوطني الجزائرية، "المدرسة العسكرية المتعددة التقنيات، تاريخ الاطلاع: (4 جوان 2025)، نقلا عن الرابط التالي https://bit.ly/48hmntG

5.2. الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية في الجزائر (2025–2029)

في ظل التحولات الرقمية المتسارعة وتصاعد التهديدات السيبرانية على المستوى العالمي، برزت الحاجة إلى تبني سياسات وطنية حديثة قادرة على تأمين الفضاء الرقمي وحماية المصالح الاستراتيجية للدولة ، وهذا السياق، أولت الجزائر اهتمامًا متزايدًا بمجال الأمن السيبراني، حيث تم إقرار استراتيجية وطنية لأمن الأنظمة المعلوماتية خلال الفترة الممتدة(2025–2029)، في إطار رؤية شاملة لتعزيز السيادة الرقمية ومرافقة مسار التحول الرقمي.[1]

تندرج هذه الاستراتيجية ضمن التوجهات العليا للدولة الجزائرية الرامية إلى بناء منظومة وطنية متكاملة للأمن السيبراني قادرة على مواجهة التهديدات الرقمية المتنامية والتكيف مع التطورات التكنولوجية المتسارعة، في إطار انتقال نوعي من المقاربات التقليدية إلى مقاربة استباقية قائمة على المرونة السيبرانية وتكامل الأبعاد القانونية والتقنية والبشرية، وتهدف هذه الاستراتيجية (2025–2029) إلى تعزيز القدرات الوطنية وتطوير الإطار التنظيمي وتكوين الموارد البشرية وتوسيع التعاون الوطني والدولي بما يضمن حماية الفضاء السيبراني ودعم السيادة الرقمية.

وتقوم على أربعة أسس رئيسية تتمثل في :رؤية استراتيجية ترتكز على تعزيز المرونة السيبرانية وضمان حماية الفضاء الرقمي؛ وأهداف استراتيجية تهدف إلى بناء نظام وطني متكامل للأمن السيبراني وتطوير الكفاءات وتعزيز الحماية والبنية التحتية، ومبادئ توجيهية تقوم على السيادة الرقمية، والتنسيق بين الفاعلين، وتحديد أهداف قابلة للقياس؛ إضافة إلى أربعة محاور تنفيذية تشمل تطوير القدرات التقنية والعملياتية، وتحديث الإطار القانوني والتنظيمي والمعياري، وتعزيز التكوين والبحث والتحسيس، إلى جانب دعم التعاون الوطني والدولي لمواجهة التهديدات السيبرانية.

3. الإجراءات على المستوى الإقليمي

تعتمد الجزائر على مقاربة إقليمية قائمة على التعاون القانوني والأمني لمواجهة الطابع العابر للحدود للجريمة السيبرانية، خاصة في الفضاء العربي والإفريقي، وفي هذا الإطار، انخرطت في الاتفاقيات العربية، وعلى رأسها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة2010 ، والتي هدفت إلى توحيد التشريعات وتعزيز تبادل المعلومات والتعاون القضائي بين الدول العربية[2]،كما تتفاعل

[1] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 25–321 المؤرخ في 30 ديسمبر 2025 المتعلق بالمصادقة على الاستراتيجية الوطنية لأمن نظم المعلومات 2025–2029، الجريدة الرسمية للجمهورية الجزائرية، العدد 87، الصادر في 30 ديسمبر 2025.

[2] المرسوم الرئاسي رقم 14–252 ،المؤرخ في 08سبتمبر2014 ،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21ديسمبر2010، الجريدة الرسمية الجمهورية االجزائرية الديمقراطية الشعبية، العدد57، صادر بتاريخ 28سبتمبر2014.

الجزائر مع الإطار الإفريقي من خلال اتفاقية مالابو للأمن السيبراني وحماية البيانات(2014) ، التي اعتمدها الاتحاد الإفريقي سنة2014 ، ودخلت حيز التنفيذ في جوان2023 ، حيث تلزم الدول بوضع استراتيجيات وطنية وتعزيز حماية المعطيات الشخصية، إلا أن الجزائر لم تصادق بعد على اتفاقية مالابو، رغم توجهها نحو مواءمة تشريعاتها مع معايير الأمن السيبراني الإفريقية.[1]

ويعكس هذا التوجه الإقليمي إدراك الجزائر أن التهديدات السيبرانية مرتبطة ببيئتها الجيوسياسية المغاربية والإفريقية، مما يفرض تعزيز التنسيق وتبادل الخبرات وبناء قدرات مشتركة لمواجهة الجرائم المرتبطة بالإرهاب والجريمة المنظمة.

4. الإجراءات على المستوى الأوروبي

في إطار التعاون المتوسطي، تتجه الجزائر إلى الاستفادة من التجربة الأوروبية، خاصة من خلال التأثر باتفاقية بودابست لمكافحة الجريمة السيبرانية، التي تم التوقيع عليها في 23 نوفمبر 2001 ودخلت حيز التنفيذ في 1 جويلية 2004، وتعد أول إطار دولي ملزم لتوحيد التشريعات وتعزيز التعاون في التحقيقات الرقمية.

كما تتأثر السياسات الجزائرية بالمقاربات الأوروبية التي ظهرت منذ بداية الألفية، مثل توجه الاتحاد الأوروبي سنة 2002 لإقرار إطار قانوني لحماية الأنظمة المعلوماتية، بهدف توحيد التجريم وتعزيز حماية البنية التحتية الرقمية، وتسعى الجزائر من خلال هذا التعاون إلى[2]:

- ✓ مواءمة تشريعاتها مع المعايير الأوروبية
- ✓ تطوير آليات التحقيق الرقمي
- ✓ الاستفادة من الخبرة التقنية الأوروبية

وذلك بهدف تقليص الفجوة التكنولوجية وتعزيز أمنها في الفضاء المتوسطي الذي يتميز بترابط التهديدات.

5. الإجراءات على المستوى الدولي

على المستوى الدولي، تعتمد الجزائر على التعاون متعدد الأطراف والانخراط في المبادرات الأممية والدولية، حيث ساهمت في التفاعل مع عدد من القرارات والآليات الدولية، أهمها:

---

[1] مريم لوكال، **قراءة في اتفاقية الاتحاد الافريقي حول الامن السيبراني و حماية المعطيات ذات طابع شخصي 2014**، مجلة الدراسات القانونية و الاقتصادية، م 04، ع03، 2021، ص. 670.

[2] محمد سعيد العياش الشها رني،" **أثر العولمة على مفهوم الأمن القومي**"، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية، 2007/2006، ص. 55.

أ/ قرارات الأمم المتحدة المتعلقة بالأمن السيبراني، خاصة:

- ✓ القرار 55/63 لسنة 2001 حول مكافحة إساءة استخدام تكنولوجيا المعلومات. [1]
- ✓ القرار 57/239 لسنة 2002 حول إنشاء ثقافة عالمية للأمن السيبراني. [2]
- ✓ إنشاء مجموعة الخبراء الحكوميين (GGE) سنة 2004 لدراسة التهديدات السيبرانية ووضع قواعد للسلوك الدولي في الفضاء الرقمي.

ب/ التوجه نحو إطار دولي شامل:

شهدت الجهود الدولية لمكافحة الجريمة السيبرانية تطورًا مهمًا منذ سنة 2017، حين بادرت روسيا باقتراح مشروع اتفاقية دولية في هذا المجال، وقد لعبت الجزائر دورًا محوريًا في هذا المسار من خلال توليها رئاسة اللجنة المتخصصة المكلفة بإعداد الاتفاقية وقيادتها للمفاوضات الدولية منذ ماي 2021، وأسفرت هذه الجهود عن اعتماد الاتفاقية رسميًا خلال الدورة التاسعة والسبعين للجمعية العامة للأمم المتحدة في ديسمبر 2024، حيث تم توقيعها من قبل 64 دولة وهيئة إقليمية.

كما فُتحت الاتفاقية للتوقيع أمام الدول في 25 أكتوبر 2025 بالعاصمة الفيتنامية هانوي، في خطوة تعكس التوافق الدولي المتزايد حول ضرورة تعزيز التعاون لمواجهة الجرائم السيبرانية[3].

كما تعتمد الجزائر على:

- ✓ تبادل المعلومات والمساعدة التقنية
- ✓ التعاون مع منظمات مثل الاتحاد الدولي للاتصالات
- ✓ المشاركة في المؤتمرات الدولية

وذلك في إطار ما يسمى بـ الدبلوماسية السيبرانية التي تهدف إلى مواجهة الجرائم العابرة للحدود.

المطلب الرابع: التحديات التي تقف أمام تجسيد السيادة السيبرانية في الجزائر

تواجه الجزائر في سبيل تجسيد سيادتها السيبرانية مجموعة من التحديات المرتبطة بتطور التهديدات الرقمية، تنقسم بين داخلية وخارجية.

الفرع الأول: التحديات الخارجية لتطور الأمن السيبراني في الجزائر

في ظل التوجهات الرسمية الرامية إلى تعزيز الجاهزية السيبرانية ومنح الرقمنة مكانة مركزية

---

[1] United Nations General Assembly, **Resolution 55/63: Combating the Criminal Misuse of Information Technologie**s, 4 December 2000 (adopted 2001), New York: United Nations.

[2] United Nations General Assembly, **Resolution 57/239: Creation of a Global Culture of Cybersecurity**, 20 December 2002, New York: United Nations.

[3] ميتيهان دورماز، **اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الإلكترونية: الأهداف والثغرات**، منصة دعم السلامة الرقمية، 12 ديسمبر 2024، تم الاطلاع عليه بتاريخ 2026/04/10 عبر الرابط التالي: https://tinyurl.com/yrhh5pzx

ضمن أولويات الدولة، برزت مجموعة من التحديات الخارجية ذات الطابع البنيوي والتقني، والتي لا تزال تعيق بناء استراتيجية سيبرانية فعالة ومتكاملة ،ويمكن عرض هذه التحديات كما يلي[1]:

تتسم البيئة السيبرانية العالمية بدرجة عالية من التعقيد والتسارع، نتيجة التداخل المتزايد بين تقنيات حديثة كالذكاء الاصطناعي، والحوسبة السحابية، وإنترنت الأشياء الصناعي، الأمر الذي أدى إلى توسع كبير في سطح الهجوم السيبراني، ويجعل هذا التحول المستمر من الصعب على الدول، بما فيها الجزائر، تطوير استراتيجيات وقائية قادرة على مواكبة نسق التهديدات المتغيرة، كما أن الانتشار الواسع للإنترنت، خاصة عبر الأجهزة المحمولة، أسهم في توسيع نطاق الهجمات السيبرانية، حيث أدى تزايد عدد المستخدمين وارتفاع حجم البيانات المتداولة إلى مضاعفة نقاط الضعف المحتملة، ويزداد هذا الوضع تعقيدا في ظل ضعف ممارسات الأمن السيبراني على المستوى الفردي، مما يهيئ بيئة خصبة لانتشار هجمات معقدة مثل برمجيات الفدية والهجمات المتقدمة المستمرة.

ومن بين أبرز التحديات كذلك تعقيد مسألة الأدلة الرقمية، حيث تتسم الهجمات السيبرانية بقدرتها على إخفاء آثارها أو التلاعب بها، مما يحد من فعالية التحقيقات الجنائية ويصعب عملية الإثبات القضائي، خاصة في ظل محدودية الأطر القانونية والتنظيمية المتعلقة بحفظ الأدلة الرقمية.، وترتبط بذلك إشكالية صعوبة إسناد الهجمات، إذ يعتمد المهاجمون على تقنيات متطورة لإخفاء هوياتهم، مثل: الشبكات الافتراضية الخاصة، والبروكسي، والشبكات المظلمة، مما يعقد عملية تحديد مصدر التهديد ويضعف من فعالية الردع السيبراني.

كما أن الطبيعة اللامادية للفضاء السيبراني، التي تتجاوز الحدود الجغرافية والزمنية، تمثل تحديا إضافيا، حيث يمكن تنفيذ الهجمات من مواقع متعددة وعبر وسطاء تقنيين، وفي أي وقت، مما يستدعي جاهزية دائمة وقدرات استجابة آنية على مدار الساعة، يضاف إلى ذلك اختلال ميزان القوة السيبرانية على المستوى الدولي، حيث تمتلك الدول المتقدمة قدرات هجومية ودفاعية متطورة، ما يمنحها تفوقا استراتيجيا ويجعل الدول النامية أكثر عرضة للاستهداف أو التأثير السيبراني.

وأخيرا، تبرز صعوبة تقييم المخاطر السيبرانية كأحد التحديات الجوهرية، نظرا لتعقيد البيئة الرقمية وتعدد الفاعلين، مما يتطلب بناء نماذج تحليلية متقدمة لفهم التهديدات المحتملة وتقدير آثارها على الأمن الوطني والاقتصاد الرقمي.

[1] إبراهيم عدنان و فايز خضر، **الأدلة الرقمية و اثبات الجرائم السيبرانية: بين التاصيل و التاويل**، المجلة الفلسطنية للأبحاث القانونية، ع 1، اكتوبر 2021، ص. 144.

الفرع الثاني: التحديات الداخلية لتطوير الأمن السيبراني في الجزائر

إلى جانب التحديات الخارجية، تواجه الجزائر مجموعة من التحديات الداخلية ذات الأبعاد البنيوية والمؤسساتية، والتي تؤثر بشكل مباشر على وتيرة تطوير منظومة الأمن السيبراني وفعاليتها، في هذا السياق، يُلاحظ أن الخبرة الوطنية في مجال الأمن السيبراني لا تزال في طور التشكل، رغم الجهود المبذولة لتعزيز هذا القطاع من خلال إنشاء مؤسسات متخصصة وتطوير برامج تكوين أكاديمي ومهني، ويعكس ذلك انتقالا تدريجيا نحو إدماج الأمن السيبراني ضمن أولويات الأمن الوطني.

كما يشهد الاعتماد المؤسساتي على التكنولوجيا الرقمية تزايدا ملحوظا، في إطار مساعي التحول الرقمي، وهو ما يفرض في المقابل تحديات تتعلق بضرورة تأمين الأنظمة المعلوماتية وتعزيز قدرات الكشف المبكر والاستجابة للتهديدات، وفيما يتعلق بالتمويل، ورغم تسجيل تحسن نسبي في حجم الاستثمارات الموجهة للأمن السيبراني، إلا أن الحاجة لا تزال قائمة لتوجيه الموارد نحو مجالات حيوية، مثل تطوير أنظمة كشف التسلل، وتعزيز مراكز الاستجابة للحوادث، واقتناء أدوات التحليل الجنائي الرقمي.

أما على المستوى التشريعي، فلا تزال المنظومة القانونية بحاجة إلى تحديث مستمر لمواكبة التطورات المتسارعة في طبيعة التهديدات السيبرانية، خاصة في ما يتعلق بحماية البيانات الشخصية، ومكافحة الجرائم الإلكترونية المستحدثة، وتنظيم الفضاء الرقمي بشكل أكثر فعالية، كما يمثل الاستثمار في الكفاءات البشرية تحديا محوريا، إذ يتطلب تطوير الأمن السيبراني توفير موارد بشرية مؤهلة ومتخصصة، من خلال تحديث المناهج التعليمية، وتعزيز التكوين التطبيقي، وخلق بيئة محفزة للحد من هجرة الكفاءات.

من خلال ما سبق يتبين أن تجسيد السيادة السيبرانية في الجزائر يواجه تحديات متعددة الأبعاد، تجمع بين ما هو خارجي مرتبط بطبيعة النظام السيبراني العالمي، وما هو داخلي متعلق بالبنية المؤسسية والقدرات الوطنية ، ورغم الجهود المبذولة، فإن تحقيق أمن سيبراني فعال يظل رهينا بتبني مقاربة شاملة ترتكز على تطوير التشريعات، وتعزيز القدرات التقنية والبشرية، وتكريس ثقافة رقمية واعية، فضلا عن دعم الشراكات مع مختلف الفاعلين الوطنيين والدوليين.

المبحث الثاني: الاستراتيجيات الدولية للأمن السيبراني ودلالاتها في تقييم السياسة السيبرانية الجزائرية

يشهد الأمن السيبراني تحوّلًا نوعيًا جعله أحد أهم محددات القوة الوطنية في النظام الدولي المعاصر، حيث أصبحت قدرة الدول على حماية فضائها الرقمي ومواجهة التهديدات السيبرانية عنصرًا مكملًا للأمن التقليدي ، وفي هذا السياق، برزت تجارب دولية متقدمة مثل الولايات المتحدة والصين وروسيا، التي طورت نماذج مختلفة تجمع بين الأبعاد الاستراتيجية والمؤسسية والتكنولوجية وفق رؤى وطنية متباينة.

ويهدف هذا المبحث إلى تحليل هذه التجارب من منظور مقارن لاستجلاء عوامل القوة والفعالية فيها، واستثمار نتائج هذا التحليل في تقييم السياسة السيبرانية الجزائرية من خلال إبراز مكامن القوة والقصور واقتراح سبل تطويرها وتعزيز فعاليتها في مواجهة التهديدات السيبرانية المعاصرة.

المطلب الأول: التجارب الدولية الرائدة

تُعدّ التجارب الدولية الرائدة في مجال الأمن السيبراني نماذج مرجعية طورت مقاربات متقدمة تجمع بين الأبعاد المؤسسية والتقنية والاستراتيجية لمواجهة التهديدات السيبرانية المعاصرة.

1. الاستراتيجية الأمريكية في الأمن السيبراني

تعتمد الولايات المتحدة على مقاربة شاملة تقوم على الردع والهجوم الاستباقي والدفاع المتقدم، حيث لا تكتفي بحماية حدودها الرقمية بل تسعى إلى نقل المواجهة إلى خارجها لضمان التفوق السيبراني.

وترتكز هذه الاستراتيجية على تكامل مؤسساتي قوي تقوده كل من قيادة الأمن السيبراني (USCYBERCOM) ووكالة الأمن القومي (NSA)، مع دمج العمليات السيبرانية ضمن التخطيط العسكري والاستخباراتي، كما تعتمد العقيدة الأمريكية على التكامل مع مجتمع الاستخبارات، بحيث يتم التنسيق بين العمليات السيبرانية والمصالح الاستخباراتية وفق مبدأ الموازنة بين المكاسب والخسائر (Gain/Loss)، وتُستخدم القدرات السيبرانية لتحقيق تأثيرات فورية في العمليات العسكرية، مثل تعطيل الأنظمة الدفاعية أو استهداف البنى التحتية الحيوية، إضافة إلى تنفيذ عمليات سيبرانية استكشافية وهجومية.[1]

ومن أهم مميزات النموذج الأمريكي أيضًا الشراكة الوثيقة بين القطاعين العام والخاص، حيث تلعب

[1] **Cybersecurity and Infrastructure Security Agency** (CISA). "Critical Infrastructure Sectors." accessed on: (01/04/2026), Retrieved from the following link: https://tinyurl.com/3r968dt2

الشركات التكنولوجية الكبرى مثل Microsoft وGoogle وCisco دورًا أساسيًا كخط دفاع أول، مما يعكس طبيعة النظام الليبرالي القائم على توزيع الأدوار بين الدولة والفاعلين الاقتصاديين.[1]

2. الاستراتيجية الصينية في الأمن السيبراني

تقوم الاستراتيجية الصينية على مبدأ السيادة السيبرانية والرقابة المركزية، حيث تسعى الدولة إلى فرض سيطرة كاملة على الفضاء الرقمي الداخلي، من خلال منظومة مؤسساتية تجمع بين البعد الأمني والسياسي والعسكري.

ويبرز في هذا السياق دور مؤسسات رئيسية مثل وزارة أمن الدولة وإدارة الفضاء السيبراني، التي تشرف على تنظيم الأنترنت والرقابة على المحتوى وحماية أمن المعلومات،[2]كما تعتمد الصين على بناء قدرات هجومية ودفاعية متقدمة قادرة على العمل في زمن السلم والحرب، مع دمج الأمن السيبراني ضمن الاستراتيجية الوطنية الشاملة، بما في ذلك الخطط الصناعية والتنموية وتقليل الاعتماد على التكنولوجيا الأجنبية، ويعكس ذلك توجهًا نحو تحقيق الاكتفاء الذاتي التكنولوجي.[3]

إلى جانب ذلك، ترتكز القوة السيبرانية الصينية على التمكين التكنولوجي من خلال الاستثمار في تقنيات متقدمة مثل الذكاء الاصطناعي، شبكات الجيل الخامس (G5)، والحوسبة الكمومية، إضافة إلى توظيفها في تعزيز النفوذ الجيوسياسي عبر مبادرات مثل "طريق الحرير الرقمي"، كما تسعى الصين إلى لعب دور فاعل في صياغة المعايير الدولية للأمن السيبراني بدل الاكتفاء باتباعها.[4]

3. الاستراتيجية الروسية في الأمن السيبراني

تتميز الاستراتيجية الروسية بطرح مختلف يقوم على مفهوم "المواجهة المعلوماتية"، حيث يُنظر إلى الفضاء السيبراني كجزء من صراع استراتيجي شامل يشمل البنية التحتية والمحتوى والإدراك الجماعي، وتهدف هذه المقاربة إلى تحقيق السيطرة الكاملة على المجال المعلوماتي واستخدامه كأداة نفوذ سياسي وعسكري.

ومن الناحية العملياتية، طورت روسيا منذ سنة 2013 قدراتها في إطار الحرب الهجينة، حيث يتم دمج العمليات السيبرانية مع العمليات العسكرية التقليدية، وإنشاء وحدات سيبرانية داخل القوات المسلحة، مع تدريب كوادر متخصصة واستخدام تكنولوجيا المعلومات كأسلحة رقمية، كما تعتمد روسيا على تكامل

[1] Ibid.
[2] "**Xi Jinping Leads China's New Internet Security Group**," The Diplomat, February 28, 2014, accessed on: (16/03/2026), Retrieved from the following link: https://tinyurl.com/425dzxdw
[3] Ibid.
[4] Iibid.

وثيق بين أجهزة الاستخبارات (مثل GRU وSVR) والمؤسسة العسكرية، مع تركيز كبير على جمع المعلومات أكثر من التدمير المباشر.

وتُعد من أبرز خصائص هذه الاستراتيجية توظيف فاعلين غير رسميين (الهاكرز الوطنيين) ضمن إطار غير مباشر يوفر للدولة هامش إنكار (Plausible Deniability)، مما يصعّب عملية التتبع والمساءلة الدولية[1]، وتعكس هذه المقاربة نموذجًا شديد المركزية، حيث يُنظر إلى الفضاء السيبراني ليس كمجال مدني، بل كساحة صراع تعمل فيها أجهزة الأمن والجيش والاستخبارات بشكل متكامل ومنسق.

المطلب الثاني : تقييم السياسة العامة الأمنية السيبرانية الجزائرية

تشير دراسة واقع الأمن السيبراني في الجزائر إلى وجود أربعة جوانب أساسية تحدد فعالية المنظومة الوطنية، وهي: الجانب المؤسسي، الجانب التشريعي، الجانب التكنولوجي، الجانب البشري.

يمكّن تحليل هذه الجوانب من تشخيص مواطن القصور وفهم التحديات التي تعيق بناء استراتيجية سيبرانية متكاملة وفعالة كالتالي:

أ/ الجانب المؤسسي

يمثل الجانب المؤسسي الإطار المنظم للسياسات السيبرانية في الجزائر، إلا أن فعاليته ما تزال محدودة بفعل مجموعة من الاختلالات. فعلى الرغم من إنشاء هياكل متخصصة على غرار*الهيئة الوطنية للأمن السيبراني (ONSC)*و*المركز الجزائري للاستجابة للحوادث السيبرانية (CERT.dz)*، إلا أن التحديات المتعلقة بضعف التنسيق وتداخل الصلاحيات بين مختلف القطاعات (وزارة الدفاع، وزارة الداخلية، وزارة البريد وتكنولوجيات الإعلام والاتصال، وغيرها) تبقى قائمة. هذا التعدد في الفاعلين، في غياب قيادة مركزية وآليات واضحة لتوزيع المسؤوليات، يؤدي إلى تشتت الجهود ويضعف القدرة على صياغة وتنفيذ استراتيجية وطنية متكاملة. كما أن محدودية الموارد البشرية والتقنية والمالية المخصصة لهذه المؤسسات تحدّ من فعاليتها التشغيلية، حيث تعاني من نقص في الكفاءات المؤهلة وصعوبات في الحصول على أحدث التقنيات اللازمة للرصد والتحليل. إضافة إلى ذلك، يبرز قصور في آليات المتابعة والتقييم لمدى تنفيذ الاستراتيجية الوطنية وترجمتها إلى خطط عمل عملية، وهو ما يجعل قدرة المؤسسات على التكيف مع الطبيعة الديناميكية للفضاء السيبراني محدودة، خصوصاً في ظل البيروقراطية التي قد

[1] Giles, Keir. Russia's '**New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. L**ondon: Chatham House, 2016. accessed on: (16/03/2026), Retrieved from the following link: https://tinyurl.com/2vthc6wc

تعيق الاستجابة السريعة للتطورات.

وهو ما يختلف عن نموذج كوريا الجنوبية التي إعتمدت هيئة مركزية عليا (KISA) تشرف بشكل صارم على جميع الأنشطة السيبرانية الوطنية، وتضع خطة عمل موحدة تُترجم الاستراتيجية الوطنية إلى مؤشرات أداء قابلة للقياس (KPIs)، مع آليات محاسبة واضحة. هذا التنظيم المركزي مكّنها من تحقيق استجابة منسقة وفعّالة للهجمات السيبرانية المتطورة. وبالمقارنة، تكشف الحالة الجزائرية عن تشتت مؤسسي يقوض مناعة المنظومة الوطنية ويضعف قدرتها على التكيف مع الديناميكية العالية للفضاء السيبراني.

غير أن هذا العرض ، على أهميته، لا يكفي لفهم عمق الإشكالات التي تعاني منها المنظومة المؤسسية، الأمر الذي يستدعي الانتقال إلى تحليل أكثر تعمقًا يكشف عن الأبعاد البنيوية والحوكمية لهذه الاختلالات.

يمثل الجانب المؤسسي الإطار المنظم للسياسات السيبرانية في الجزائر، غير أن تحليل فعاليته يكشف عن اختلالات بنيوية تتجاوز مجرد تعدد الفاعلين إلى إشكالية أعمق تتعلق بطبيعة الحوكمة السيبرانية ذاتها. فعلى الرغم من إنشاء هياكل متخصصة على غرار الهيئة الوطنية للأمن السيبراني والمركز الجزائري للاستجابة للحوادث السيبرانية(CERT.dz) ، إلا أن غياب مركزية القرار الاستراتيجي يؤدي إلى نمط من "التجزئة المؤسسية(Institutional Fragmentation) "، حيث تعمل هذه الهيئات في إطار شبه مستقل دون تنسيق فعال قائم على منظومة قيادة موحدة.

ولا يقتصر أثر هذا التشتت على ضعف التنسيق، بل يمتد إلى تقليص القدرة على إنتاج سياسات استباقية، إذ تصبح المؤسسات في وضعية ردّ الفعل بدل المبادرة، وهو ما يتعارض مع طبيعة التهديدات السيبرانية التي تتطلب سرعة في اتخاذ القرار وتكاملًا في تبادل المعلومات. كما أن محدودية الموارد البشرية والتقنية لا تعكس فقط نقصًا كمّيًا، بل تعكس أيضًا غياب سياسة وطنية متكاملة لإدارة الكفاءات (Cyber Talent Management)، مما يحدّ من قدرة هذه المؤسسات على استيعاب التكنولوجيات المتقدمة وتوظيفها بكفاءة.

ومن زاوية أخرى، يكشف ضعف آليات التقييم والمتابعة عن غياب ثقافة "الحوكمة القائمة على النتائج(Results-Based Governance) "، حيث لا يتم ربط الاستراتيجيات الوطنية بمؤشرات أداء دقيقة (KPIs) قابلة للقياس، وهو ما يجعل عملية التقييم شكلية أكثر منها عملية. وفي هذا السياق، لا يُعد التحدي مؤسسياً فقط، بل هو تحدٍّ في نموذج الحوكمة ذاته، الذي لا يزال أقرب إلى النمط الإداري

التقليدي منه إلى النماذج الشبكية الحديثة (Network Governance) المعتمدة في الدول المتقدمة.

وبالمقارنة مع تجربة كوريا الجنوبية، التي اعتمدت هيئة مركزية قوية (KISA) تضطلع بوظيفة التنسيق الشامل وتُترجم الاستراتيجية الوطنية إلى خطط تنفيذية دقيقة، يتضح أن الفارق لا يكمن فقط في الإمكانيات، بل في فلسفة التنظيم، حيث تقوم التجربة الكورية على مبدأ "وحدة القيادة وتكامل الفاعلين"، في حين تعاني الحالة الجزائرية من غياب هذا التكامل، مما ينعكس سلباً على مرونة المنظومة وقدرتها على التكيف مع التهديدات المتغيرة.

ب/ الجانب التشريعي

يُشكّل الإطار التشريعي الدعامة القانونية للأمن السيبراني، غير أنّ تحليله في الحالة الجزائرية يكشف عن قصور واضح في مواكبة التطور التكنولوجي. فالقوانين القائمة، مثل القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جاءت في سياقات زمنية وتقنية سابقة، وهو ما يجعلها غير قادرة على الإحاطة بالأشكال الجديدة للجريمة السيبرانية التي استفادت من الذكاء الاصطناعي وانتشار إنترنت الأشياء وتطور برامج الفدية. كما أن التشريع الجزائري ما يزال محدوداً في معالجة قضايا حيوية أخرى مثل حماية البيانات الشخصية، وتأمين البنى التحتية الحيوية، وتحديد التزامات ومسؤوليات القطاع الخاص. هذا فضلاً عن الصعوبات العملية في التطبيق، حيث يتطلب التحقيق في الجرائم السيبرانية خبرات تقنية متخصصة وآليات للتعاون الدولي، وهو ما يظل محدوداً. كذلك فإن العملية التشريعية بطبيعتها بطيئة مقارنة بالسرعة التي تتغير بها التهديدات، مما يستدعي التفكير في اعتماد آليات أكثر مرونة مثل اللوائح التنظيمية المتخصصة التي يمكن تحديثها بسرعة من طرف الهيئات المختصة بناءً على تفويض قانوني.

ومن منظور تحليلي، لا يمكن حصر إشكالات الإطار التشريعي في قدم النصوص فقط، بل ينبغي تفكيكها في ضوء طبيعة المقاربة القانونية وحدود قدرتها على التكيف مع البيئة الرقمية المتغيرة، إذ يُشكّل الإطار التشريعي الركيزة القانونية لتنظيم الأمن السيبراني، غير أن تحليل التجربة الجزائرية يكشف عن فجوة واضحة بين التطور التكنولوجي وتسارع التهديدات من جهة، وبطء التكيف التشريعي من جهة أخرى، فالقوانين الحالية، وعلى رأسها القانون رقم 09-04، صيغت في سياق رقمي أقل تعقيدًا، مما يجعلها اليوم عاجزة عن استيعاب التحولات المرتبطة بظهور تقنيات الذكاء الاصطناعي وإنترنت الأشياء والهجمات المعقدة مثل برامج الفدية والهجمات المتقدمة.

ولا تقتصر الإشكالية على قدم النصوص، بل تمتد إلى طبيعة المقاربة التشريعية ذاتها، التي تميل إلى الطابع الزجري (Punitive Approach) أكثر من كونها مقاربة وقائية أو تنظيمية شاملة. إذ يلاحظ تركيز واضح على تجريم الأفعال، مقابل ضعف في تنظيم مجالات حيوية مثل حماية البيانات الشخصية، أمن البنى التحتية الحيوية، ومسؤوليات الفاعلين الاقتصاديين، خاصة في القطاع الخاص، الذي يُعد شريكًا أساسيًا في الأمن السيبراني.

كما أن فعالية التشريع تصطدم بإشكاليات التطبيق، حيث تتطلب الجرائم السيبرانية قدرات تقنية عالية وآليات تعاون دولي متقدمة، في حين لا تزال هذه الجوانب محدودة، مما يخلق فجوة بين "النص القانوني" و"الواقع العملي". ويُضاف إلى ذلك بطء العملية التشريعية، التي لا تتناسب مع الطبيعة المتسارعة للفضاء الرقمي، مما يجعل القوانين في كثير من الأحيان متأخرة عن التهديدات.

ومن منظور تحليلي أعمق، يمكن القول إن الإشكال لا يكمن فقط في نقص القوانين، بل في غياب "منظومة تشريعية ديناميكية (Adaptive Legal Framework) "قادرة على التكيف المستمر، من خلال آليات مرنة مثل اللوائح التنظيمية والتحديث الدوري للنصوص. وفي هذا السياق، تبرز التجربة الأمريكية كنموذج متقدم، حيث تعتمد على مقاربة تشريعية مرنة ومتكاملة، مدعومة بهيئات مستقلة ، التي تمارس دورًا رقابيًا فعالًا وتضمن التطبيق الصارم للقوانين.

وبالمقارنة، تكشف الحالة الجزائرية عن فجوة مزدوجة: فجوة في تحديث النصوص، وفجوة في تفعيلها، وهو ما يُضعف القدرة على مواكبة التهديدات السيبرانية الحديثة، ويحدّ من فعالية السياسة الأمنية في بعدها القانوني.

ج/ الجانب التكنولوجي

يُعتبر الجانب التكنولوجي الساحة الأساسية للمواجهة، غير أن الجزائر تواجه فيه تحديات استراتيجية عميقة. من أبرزها الاعتماد المفرط على التكنولوجيا المستوردة في بناء البنية التحتية الرقمية واعتماد الحلول الأمنية، وهو ما يثير إشكالات متعلقة بالسيادة الرقمية ويجعل البلاد رهينة لتطورات وسياسات الموردين الأجانب. هذا الوضع يزداد تعقيداً في ظل ضعف منظومة البحث والتطوير الوطنية في مجال الأمن السيبراني، ما يقلل من فرص ابتكار حلول محلية تلبي الخصوصيات الوطنية. على مستوى البنية التحتية، ورغم جهود التحديث، ما تزال بعض المؤسسات تعتمد على أنظمة قديمة وغير مؤمنة بما يكفي، مما يجعلها أهدافاً سهلة للهجمات. كما أن تبني التقنيات الأمنية المتقدمة مثل أنظمة الكشف والاستجابة (EDR/XDR) أو منصات استخبارات التهديدات يبقى محدوداً بسبب ارتفاع التكلفة

ونقص الكفاءات القادرة على تشغيلها. كذلك، يشكل الانتشار المرتقب لتقنيات الجيل الخامس (G5) وإنترنت الأشياء تحدياً مضاعفاً، حيث يزيد من سطح الهجوم ومن تعقيد عملية التأمين، في ظل الحاجة إلى معايير أمنية صارمة واستثمارات كبيرة. وفي هذا السياق، يظل دور CERT.dz أساسياً، إلا أن محدودية الموارد والأدوات التحليلية المتقدمة قد تحد من قدرته على الرصد والاستجابة الفعالة للحوادث المعقدة.

الرصد اللحظي للهجمات والاستجابة الفورية لها. كما شجعت الشركات المحلية على تطوير حلول سيبرانية وطنية، مما عزز استقلاليتها التقنية وخفف من تبعيتها للخارج. مقارنة بذلك، تكشف الحالة الجزائرية عن تأخر ملحوظ في تحديث بنيتها التحتية الرقمية، ونقص حاد في الاعتماد على تقنيات محلية وهو ما يزيد من هشاشتها أمام التهديدات السيبرانية.

د/ الجانب البشري

يمثل العنصر البشري نقطة قوة وضعف في آن واحد ضمن المنظومة السيبرانية الجزائرية. فمن جهة، يُعترف بأهميته كخط دفاع رئيسي، ومن جهة أخرى يكشف الواقع عن فجوة كبيرة في الكفاءات والمهارات المتخصصة. تعاني الجزائر، مثل كثير من الدول النامية، من نقص حاد في الخبرات المؤهلة لتصميم الحلول الأمنية وإدارة الأنظمة وتحليل التهديدات والاستجابة للحوادث، وهو ما يعززه ضعف البرامج الأكاديمية المتخصصة، وهجرة الكفاءات، وضعف جاذبية القطاع للمواهب الشابة. أما على مستوى التدريب، فإن البرامج المتاحة غالباً ما تكون قطاعية ومحدودة النطاق، ولا تواكب التطور السريع للتهديدات. يضاف إلى ذلك قصور في حملات التوعية الوطنية الموجهة للجمهور العام والموظفين في القطاعين العام والخاص، مما يضعف من ترسيخ ثقافة أمنية راسخة. ويُلاحظ كذلك ضعف الاهتمام بالمهارات غير التقنية الضرورية للأمن السيبراني مثل التفكير النقدي، إدارة الأزمات، والوعي بالاعتبارات القانونية والأخلاقية، رغم أن الأمن السيبراني يتجاوز كونه مسألة تقنية ليشكل منظومة شاملة. هذه الفجوة في المهارات والتوعية تجعل الأخطاء البشرية – مثل ضعف كلمات المرور، الوقوع في هجمات التصيد، أو تحميل برمجيات خبيثة – سبباً رئيسياً في نجاح العديد من الاختراقات.

وبالموازاة نرى ان روسيا اعتمدت سياسة وطنية شاملة لبناء القدرات البشرية، بدأت من إصلاح المناهج الأكاديمية وفتح تخصصات دقيقة في الأمن السيبراني، وصولاً إلى برامج تدريبية مستمرة مرتبطة مباشرة بسوق العمل. كما عملت على تحفيز الكفاءات الشابة من خلال منح امتيازات مالية ومهنية، مما ساعدها على بناء كتلة حرجة من الخبراء المحليين القادرين على مواجهة التهديدات. بالمقابل، تكشف

الجزائر عن غياب سياسة متكاملة لبناء القدرات، مما يجعل العنصر البشري عائقاً بنيوياً أمام تطوير الأمن السيبراني الوطني.

هـ/التقييم الاستراتجية الوطنية لأمن الأنظمة المعلوماتية في الجزائر(2025–2029)

تندرج الاستراتيجية الوطنية الجزائرية لأمن الأنظمة المعلوماتية (2025–2029) ضمن سياق دولي يتسم بتصاعد حاد في التهديدات السيبرانية من حيث الحجم والتعقيد، حيث تشير التقديرات إلى أن التكلفة العالمية للجرائم السيبرانية ستصل إلى حوالي 10.5تريليون دولار سنويًا بحلول 2025، مع تسجيل هجوم سيبراني كل 39ثانية تقريبًا. كما بلغ متوسط تكلفة اختراق البيانات عالميًا 4.44مليون دولار، وقد يتجاوز 10ملايين دولار في بعض الاقتصادات المتقدمة، إضافة إلى تسجيل أكثر من 22 ألف حادثة اختراق عبر 139 دولة، وانتشار واسع لهجمات التصيد الاحتيالي التي تجاوزت مليون موقع هجوم خلال فترة قصيرة من سنة 2025 .وفي السياق الوطني، تم تسجيل ما يفوق 70مليون هجوم سيبراني في الجزائر خلال سنة 2024، وهو ما يعكس حجم التهديدات الفعلية التي تواجه البنية الرقمية للدولة. وعليه، فإن تبني الجزائر لمقاربة قائمة على المرونة السيبرانية بدل الاكتفاء بالحماية التقليدية يُعد توجهًا منسجمًا مع التحولات العالمية التي تركز على الاستباقية والقدرة على الاستجابة والتعافي[1].

في حين تعكس الأهداف الاستراتيجية المعلنة، والمتمثلة في بناء نظام وطني متكامل للأمن السيبراني، وتعزيز السيادة الرقمية، وتطوير الموارد البشرية، انسجامًا واضحًا مع المعايير الدولية، لا سيما تلك المعتمدة ضمن مؤشر الأمن السيبراني العالمي الصادر عن الاتحاد الدولي للاتصالات .غير أن تقييم الأداء الفعلي يكشف عن فجوة بين الطموح والواقع، حيث سجلت الجزائر حوالي 33.95نقطة من 100 في هذا المؤشر، وتم تصنيفها ضمن المستوى الثالث(Tier 3) ، وهو ما يعكس مستوى متوسطًا أو دون المتوسط من الجاهزية السيبرانية. وبالتالي، يمكن القول إن الأهداف الاستراتيجية، رغم أهميتها، لا تزال بحاجة إلى آليات تنفيذ فعالة، ومؤشرات قياس دقيقة، لضمان ترجمتها إلى نتائج ملموسة على أرض الواقع[2].

كما تستند الاستراتيجية الوطنية إلى أربعة محاور رئيسية (القدرات التقنية والعملياتية، الإطار القانوني والتنظيمي، التكوين والبحث والتطوير، والتعاون الوطني والدولي)، غير أن تحليلها بشكل مدمج يكشف عن تباين في مستويات القوة والفعالية بينها. فمن جهة، يمثل محور القدرات التقنية والعملياتية عنصرًا

[1] ALGERIATECH Editorial, Kaspersky's Africa Cyberthreat Landscape Report 2025, 06/12/2025, accessed on: (03/01/2026), Retrieved from the following link: http://bit.ly/4duIxMD
[2] Algeria Invest, report by cybersecurity company Kaspersky, 23/03/2025, accessed on: (03/04/2025), Retrieved from the following link: https://bit.ly/4tDW0qh

أساسيًا في مواجهة التهديدات المتزايدة، خاصة في ظل تطور الهجمات السيبرانية مثل: هجمات الفدية التي تكلف ملايين الدولارات لكل حادثة، وتوسع سطح الهجوم نتيجة اعتماد تقنيات الحوسبة السحابية وإنترنت الأشياء، إلا أن محدودية الاستثمارات في الأمن السيبراني مقارنة بالدول المتقدمة تضعف من فعالية هذا المحور.

ومن جهة ثانية، يسعى محور الإطار القانوني والتنظيمي إلى مواكبة التطورات التكنولوجية، غير أن التجارب الدولية تشير إلى أن أكثر من 80% من الدول تمتلك تشريعات سيبرانية، لكن أقل من 50% فقط تطبقها بفعالية،[1] وهو ما يبرز التحدي المرتبط بضعف التنفيذ وليس فقط بغياب النصوص. أما محور التكوين والبحث والتطوير، فيُعد من أهم الركائز الاستراتيجية، خاصة في ظل العجز العالمي الذي يُقدّر بحوالي 3.5 مليون متخصص في الأمن السيبراني، وهو ما يعكس أهمية الاستثمار في العنصر البشري، إلا أن محدودية برامج التكوين في الجزائر قد تعيق تحقيق هذا الهدف. وفيما يتعلق بمحور التعاون الوطني والدولي، فإن طبيعة التهديدات السيبرانية العابرة للحدود تفرض تعزيز الشراكات وتبادل المعلومات، خاصة وأن نسبة معتبرة من الهجمات تتم عبر شبكات دولية منظمة، غير أن مستوى الانخراط الجزائري في آليات التعاون الدولي لا يزال بحاجة إلى تطوير. وعليه، يتضح أن فعالية هذه المحاور تبقى رهينة بمدى تحقيق التكامل بينها، وتعزيز التنسيق المؤسساتي، وتوفير الموارد اللازمة لتنفيذها.

المطلب الثالث: الآفاق المستقبلية للسياسة الأمنية الجزائرية في مجال الأمن السيبراني

بناءً على الاتجاهات العالمية، وتأثير التقنيات الناشئة، والتحديات والفرص الخاصة بالجزائر، يمكن استشراف عدة سيناريوهات محتملة لمسار السياسة الأمنية السيبرانية في البلاد:

1. سيناريو الاستجابة التفاعلية

في هذا المسار، تواصل الجزائر التعامل مع التهديدات السيبرانية بشكل تفاعلي أكثر منه استباقي، حيث يتم تحديث التشريعات والهياكل المؤسسية تدريجيًا استجابة للحوادث الكبرى أو الضغوط الدولية، دون بلورة رؤية استراتيجية شاملة وطويلة المدى، كما يظل التركيز موجهاً نحو حماية البنى التحتية الحيوية، في حين تستمر تحديات فجوة المهارات والاعتماد التكنولوجي في التأثير سلبًا على فعالية المنظومة السيبرانية.

[1] StateGlobe, Identity Theft Rate Statistics in Algeria (2026), March-2026, , accessed on: (01/04/2025), Retrieved from the following link: https://bit.ly/4tyyRp4

2. سيناريو التعزيز الاستراتيجي

يمثل هذا الخيار تبنّي نهج وطني أكثر تكاملاً وفاعلية، حيث تُقرّ استراتيجية وطنية للأمن السيبراني بأهداف واضحة ومؤشرات أداء قابلة للقياس، مع متابعة وتقييم دوري.

يتم تعزيز مكانة الهيئة الوطنية للأمن السيبراني كجهة مركزية للتنسيق، إلى جانب بذل جهود ملموسة لسد فجوة الكفاءات وتطوير المنظومة التشريعية بما يتماشى مع التحولات الرقمية.

3. سيناريو الريادة الإقليمية والابتكار

في هذا التوجه، تتجاوز الجزائر مرحلة التعزيز الدفاعي لتسعى إلى لعب دور ريادي إقليمي في المجال السيبراني، سواء على المستوى المغاربي أو الإفريقي.

يقوم هذا السيناريو على تبنّي سياسة استباقية قائمة على الابتكار المحلي، وتطوير حلول وطنية، وتصدير الخبرات، ويشمل استثمارات كبيرة في البحث والتطوير، وبناء القدرات البشرية، وتعزيز الشراكات الدولية.

خلاصة الفصل الثاني:

تشهد السياسة العامة الجزائرية في مجال الأمن السيبراني تطورًا تدريجيًا في إطار التحول الرقمي المتسارع، حيث عملت الدولة على بناء منظومة قانونية ومؤسساتية وتقنية وبشرية لمواجهة تصاعد التهديدات السيبرانية التي مست مختلف القطاعات الحيوية، غير أن هذه المنظومة ما تزال تعاني من عدة اختلالات تتعلق بتشتت الأدوار المؤسسية، وبطء التحديث التشريعي، والاعتماد على التكنولوجيا المستوردة، وضعف الكفاءات المتخصصة، رغم الجهود المبذولة في مجالات التكوين والتعاون الدولي وتطوير الاستراتيجية الوطنية 2025–2029.

كما يكشف التقييم المقارن مع التجارب الدولية أن الفجوة لا ترتبط فقط بالإمكانات، بل أيضًا بنمط الحوكمة ودرجة التكامل بين الفاعلين، وهو ما يحد من فعالية الاستجابة الوطنية أمام التهديدات السيبرانية المتطورة، ويجعل تعزيز السيادة السيبرانية مرهونًا بتبني مقاربة أكثر شمولية تقوم على التنسيق المؤسسي، وتحديث التشريع، ودعم الابتكار، والاستثمار في العنصر البشري والتقنيات الحديثة.

الفصل الثالث : مشروع CyberGuard Algeria

في هذا السياق المتسارع الذي تتعاظم فيه التهديدات السيبرانية وتتداخل فيه الأبعاد الأمنية والتكنولوجية، يبرز مشروع CyberGuard Algeria كاستجابة عملية وتجسيد تطبيقي للتوجهات الاستراتيجية التي تبنتها الدولة في مجال الأمن السيبراني، إذ يهدف هذا المشروع إلى تعزيز المنظومة الوطنية للحماية الرقمية من خلال تطوير منصة متكاملة تجمع بين التدريب و التكوين قائمة على أحدث التقنيات، بما في ذلك توظيف الذكاء الاصطناعي, بما يتماشى مع متطلبات الحوكمة الحديثة وأسس الأمن القومي.

وعليه، فإن مشروع CyberGuard Algeria لا يمثّل مجرد مبادرة تقنية، بل يعد امتدادًا استراتيجيًا لسياسة أمنية وطنية شاملة، تستهدف تحقيق السيادة الرقمية وضمان استقرار الدولة في ظل التحديات السيبرانية المتزايدة.

المبحث الأول: تقديم المشروع

يُعتبر تقديم المشروع من أهم المراحل الأساسية في إعداد ودراسة أي مؤسسة ناشئة، إذ يسمح بتوضيح الرؤية العامة للمشروع وإبراز مختلف الجوانب المرتبطة بفكرته وأهدافه وآليات تنفيذه، كما يساعد هذا المحور على إعطاء صورة شاملة حول طبيعة المشروع والقيمة التي يقدمها والفئة المستهدفة، إضافة إلى الموارد البشرية والتنظيمية المعتمدة لتحقيق الأهداف المسطرة.

وفي إطار التحول الرقمي الذي تعرفه الجزائر، يندرج مشروع "CyberGuard Algeria" ضمن المشاريع الرقمية المبتكرة التي تهدف إلى تعزيز منظومة الأمن السيبراني الوطني من خلال توفير منصة تعليمية متخصصة تجمع بين التكوين الأكاديمي والتطبيق العملي.

المطلب الأول: التعريف بالمشروع الناشئ CyberGuard Algeria

يُعدّ مشروع CyberGuard Algeria نموذجًا للمشاريع الناشئة المبتكرة في مجال الأمن السيبراني، حيث يهدف إلى تقديم حلول رقمية متخصصة تواكب التحديات والتهديدات السيبرانية المتزايدة في الجزائر.

الفرع الأول: فكرة المشروع

يتمثل مشروع "CyberGuard Algeria" في إنشاء منصة رقمية تعليمية متخصصة في مجال الأمن السيبراني، تهدف إلى توفير تكوين احترافي عالي الجودة لفائدة الطلبة والمهنيين والمؤسسات داخل الجزائر، وذلك من خلال تقديم دورات تدريبية تقنية، مختبرات افتراضية، جلسات مباشرة مع خبراء، وشهادات رقمية قابلة للتحقق.

جاءت فكرة المشروع استجابة للتطور الكبير الذي يشهده العالم في مجال التكنولوجيا الرقمية، وما رافقه من ارتفاع متزايد في حجم التهديدات والهجمات السيبرانية التي أصبحت تستهدف مختلف القطاعات الحيوية، كالمؤسسات الاقتصادية، البنوك، الإدارات العمومية، وشركات الاتصالات.

وفي المقابل تعاني الجزائر من نقص واضح في الكفاءات المتخصصة في الأمن السيبراني، إضافة إلى محدودية المنصات المحلية القادرة على توفير تكوين عملي احترافي يتناسب مع احتياجات السوق الوطنية.

ويعتمد المشروع على إنشاء بيئة تعليمية رقمية متكاملة تجمع بين الجانب النظري والتطبيقي، حيث سيتمكن المستخدم من متابعة الدورات التدريبية عبر الإنترنت، وإنجاز تطبيقات عملية داخل مختبرات افتراضية تحاكي سيناريوهات حقيقية للهجمات الإلكترونية، مما يساعد على اكتساب خبرة ميدانية حقيقية في مجال الحماية المعلوماتية.

كما يهدف المشروع إلى إزالة العوائق التي تواجه المتعلمين الجزائريين عند الولوج إلى المنصات الأجنبية، خاصة ما يتعلق بارتفاع تكاليف الاشتراك وصعوبة الدفع الإلكتروني الدولي، وذلك من خلال توفير نظام دفع محلي يدعم بطاقات "الذهبية" و "CIB"، إضافة إلى توفير محتوى باللغات العربية والفرنسية والإنجليزية لتسهيل الوصول إلى مختلف فئات المستخدمين.

ويُصنف المشروع ضمن المؤسسات الناشئة الرقمية ذات الطابع التكنولوجي والتعليمي، حيث يجمع بين التعليم الإلكتروني (E-Learning) والأمن السيبراني (Cybersecurity) ضمن نموذج اقتصادي مبتكر يستهدف السوق الجزائرية والمغاربية مستقبلاً.

الفرع الثاني: القيم المقترحة للمشروع

تعبر القيم المقترحة عن المزايا والفوائد التي يقدمها المشروع للمستخدمين مقارنة بالحلول المتوفرة في السوق، حيث يسعى مشروع "CyberGuard Algeria" إلى تقديم قيمة حقيقية تتميز بالابتكار والتخصص والملاءمة مع البيئة الجزائرية.

أ/ توفير تكوين متخصص محلي في الأمن السيبراني

يقدم المشروع محتوى تدريبيًا متخصصًا يركز حصريًا على الأمن السيبراني بمختلف فروعه، مثل:

- ✓ الاختراق الأخلاقي (Ethical Hacking)
- ✓ أمن الشبكات
- ✓ التحقيق الرقمي الجنائي (Digital Forensics)
- ✓ حماية تطبيقات الويب
- ✓ أمن الأنظمة والخوادم
- ✓ إدارة المخاطر السيبرانية

وهو ما يسمح ببناء مسار تكويني احترافي متكامل يلبي متطلبات سوق العمل.

ب/ تقليل التكاليف مقارنة بالمنصات الأجنبية

تتميز المنصة بتقديم خدماتها بأسعار مناسبة للقدرة الشرائية المحلية، مع إمكانية الدفع الإلكتروني المحلي، مما يساهم في تقليل الأعباء المالية على الطلبة والمتعلمين مقارنة بالمنصات الأجنبية ذات الأسعار المرتفعة.

ج/ التركيز على الجانب التطبيقي

يعتمد المشروع على مختبرات افتراضية وتمارين عملية تحاكي هجمات إلكترونية حقيقية، مما يسمح للمتعلم باكتساب خبرة عملية بدل الاكتفاء بالمحتوى النظري فقط.

د/ دعم اللغات المحلية

توفر المنصة واجهة استخدام ومحتوى تدريبي بعدة لغات، خاصة اللغة العربية، وهو عنصر مهم يساعد على تسهيل عملية التعلم وتقريب المفاهيم التقنية للمستخدم الجزائري.

هـ/ بناء مجتمع رقمي متخصص

لا يقتصر المشروع على التعليم فقط، بل يهدف إلى إنشاء مجتمع رقمي للأمن السيبراني يضم الطلبة والخبراء والمؤسسات، بما يسمح بتبادل الخبرات ونشر الوعي الأمني داخل الجزائر.

و/ المساهمة في تعزيز السيادة الرقمية

يساهم المشروع في دعم التوجه الوطني نحو تعزيز الأمن الرقمي وتكوين كفاءات محلية قادرة على حماية البنية التحتية الرقمية والمؤسسات الوطنية من التهديدات الإلكترونية.

المطلب الثاني: الهيكل التنظيمي وأهداف المشروع

يشكّل الهيكل التنظيمي وأهداف مشروع CyberGuard Algeria محورًا أساسيًا لفهم طريقة تسييره الداخلية وتوجهاته الاستراتيجية، باعتباره إطارًا يعكس آليات توزيع المهام وتنظيم الوظائف بما يضمن الفعالية في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: فريق العمل

عمر الجيلالي: باحث أكاديمية في العلوم السياسية، متخصّص في سياسات الأمن السيبراني وإدارة الموارد البشرية الأمنية، يمتلك خبرة معتبرة في تحليل السياسات العمومية والتخطيط الاستراتيجي للأمن الرقمي، مع تركيز خاص على تطوير آليات الحوكمة والوقاية من التهديدات السيبرانية، ويجمع في

مسيرته بين الرؤية السياسية والفهم التقني للأمن السيبراني، مما يتيح له مقاربة شمولية لبناء نموذج وطني متكامل لحماية الفضاء الإلكتروني وتعزيز صنع القرار الأمني في الجزائر. كما يسهم في إثراء الإنتاج العلمي من خلال نشر أبحاث محكّمة في مجالات الأمن السيبراني والسياسات العامة وتطوير منظومات الحماية الرقمية، بهدف دعم التحول الرقمي الآمن وتعزيز ثقافة الأمن المعلوماتي على المستويين المؤسسي والوطني.

جدول1: الفريق الأساسي لمشروع CyberGuard Algeria

الوظيفة	نوع التوظيف	المهام الأساسية
مدير المشروع	دائم (دوام كامل)	الإشراف العام على المشروع، إدارة الفريق، متابعة الجدول الزمني، وضمان تحقيق الأهداف الاستراتيجية. إدارة العلاقات والشراكات، تنفيذ خطط التسويق الرقمي، إدارة الحملات عبر الإنترنت، وتحليل بيانات الوصول والمبيعات، تسيير الشؤون الإدارية والمالية، متابعة العقود، وإعداد التقارير المحاسبية والقانونية.
المطور التقني	متعاقد جزئي (دوام جزئي)	تطوير وصيانة المنصة الإلكترونية، إدارة قاعدة البيانات، وضمان الأداء الفني والأمان البرمجي.
الخبير الأمني السيبراني	مستشار خارجي (خبير متعاقد)	إجراء اختبارات الأمان وتحليل الثغرات، إعداد بروتوكولات الحماية، وضمان مطابقة المعايير الأمنية. إعداد الدورات التدريبية ، إنشاء المختبرات الافتراضية تنظيم الحصص المباشرة ، تقييم المتعلمين ومتابعة تقدمهم

الفرع الثاني: أهداف المشروع

يسعى مشروع "CyberGuard Algeria" إلى تحقيق مجموعة من الأهداف الاستراتيجية والاقتصادية والاجتماعية، والتي يمكن تقسيمها إلى أهداف قصيرة ومتوسطة وطويلة المدى.

أولاً: الأهداف قصيرة المدى

- ✓ إطلاق النسخة الأولية للمنصة (MVP)
- ✓ توفير أول مجموعة من الدورات الأساسية
- ✓ استقطاب أول دفعة من المستخدمين
- ✓ بناء الهوية الرقمية والعلامة التجارية
- ✓ توقيع شراكات أولية مع مدربين وخبراء

ثانياً: الأهداف متوسطة المدى

- ✓ توسيع عدد الدورات والمختبرات
- ✓ إدماج تقنيات الذكاء الاصطناعي في التعلم

- ✓ تطوير نظام شهادات رقمية معتمد
- ✓ إنشاء مجتمع إلكتروني متخصص
- ✓ التوسع نحو التكوين المؤسسي B2B

ثالثاً: الأهداف طويلة المدى

- ✓ الريادة في سوق الأمن السيبراني بالجزائر
- ✓ التوسع نحو دول المغرب العربي
- ✓ المساهمة في تكوين كفاءات وطنية عالية المستوى
- ✓ دعم الأمن الرقمي والسيادة السيبرانية
- ✓ التحول إلى مرجع وطني في التكوين الأمني الرقمي

الفرع الثالث: الجدول الزمني لتحقيق المشروع

جدول 1: الجدول الزمني لتحقيق المشروع

المرحلة	المدة الزمنية	الأنشطة الرئيسية	النتائج المتوقعة
المرحلة الأولى: الدراسة والتخطيط	من الشهر 1 إلى الشهر 2	-دراسة السوق وتحليل المنافسين – تحديد احتياجات المستخدمين – إعداد التصور الأولي للمشروع – تحديد المتطلبات التقنية والتنظيمية	-وضع رؤية واضحة للمشروع – إعداد مخطط العمل الأولي – تحديد الموارد المطلوبة
المرحلة الثانية: تطوير النموذج الأولي (MVP)	من الشهر 3 إلى الشهر 5	-تصميم واجهات المستخدم – تطوير قاعدة البيانات – برمجة خصائص المنصة الأساسية – تطوير نظام التسجيل والحجز – اختبار الأداء وإصلاح الأخطاء	-إنشاء نسخة أولية قابلة للاستخدام – جاهزية المنصة للإطلاق التجريبي
المرحلة الثالثة: الإطلاق التجريبي	من الشهر 6 إلى الشهر 7	-إطلاق النسخة التجريبية للمستخدمين – استقبال الملاحظات والتقييمات – تحسين تجربة المستخدم – اختبار الاستقرار وقابلية التوسع	-تحسين جودة المنصة – اكتشاف النقائص التقنية والتنظيمية – بناء قاعدة أولية من المستخدمين
المرحلة الرابعة: التوسع والتطوير	من الشهر 8 إلى الشهر 12	-إضافة دورات ومحتويات جديدة – تطوير المختبرات الافتراضية – إدماج تقنيات الذكاء الاصطناعي – عقد شراكات مع جامعات ومؤسسات – إطلاق حملات تسويقية موسعة	-توسيع قاعدة المستخدمين – رفع جودة الخدمات – تعزيز مكانة المشروع في السوق
المرحلة الخامسة: التوسع الاستراتيجي	بعد السنة الأولى	-التوسع نحو السوق المغاربية – تطوير خدمات B2Bللمؤسسات – إنشاء برامج شهادات احترافية – تحسين البنية السحابية للمنصة	-تحقيق الاستدامة المالية – بناء علامة تجارية وطنية قوية – الريادة في مجال التكوين السيبراني

من خلال هذا المحور، تم التطرق إلى مختلف الجوانب التعريفية الخاصة بمشروع CyberGuard Algeria"، بداية من عرض فكرة المشروع والقيمة المقترحة، وصولًا إلى التعريف بفريق العمل والأهداف الاستراتيجية والخطة الزمنية للتنفيذ، وقد أظهر هذا التحليل أن المشروع يمثل مبادرة رقمية مبتكرة تستجيب لحاجة فعلية داخل السوق الجزائرية، خاصة في ظل تزايد الطلب على خدمات التكوين في مجال الأمن السيبراني، كما يبرز المشروع كحل عملي يساهم في تطوير الكفاءات الوطنية ودعم التحول الرقمي الآمن داخل الجزائر.

المبحث الثاني: الجوانب الابتكارية

أصبحت الابتكارات التكنولوجية في العصر الحديث من أهم العوامل التي تساهم في نجاح المؤسسات الناشئة وتعزيز قدرتها التنافسية داخل الأسواق المحلية والدولية، خاصة في ظل التحولات الرقمية المتسارعة التي يشهدها العالم.

فالمؤسسات الناشئة لم تعد تعتمد فقط على تقديم خدمات تقليدية، بل أصبحت ترتكز على إيجاد حلول مبتكرة تستجيب لمشكلات واقعية وتوفر قيمة مضافة للمستخدمين.

ويُعتبر مجال الأمن السيبراني من أكثر المجالات التي تتطلب الابتكار المستمر، نظرًا للتطور الدائم للهجمات الإلكترونية والتقنيات الرقمية، الأمر الذي يفرض ضرورة تطوير أدوات وأساليب حديثة في التكوين والحماية والتوعية الأمنية.

وفي هذا السياق، يسعى مشروع "CyberGuard Algeria" إلى تقديم نموذج مبتكر في مجال التعليم الرقمي والأمن السيبراني، من خلال الجمع بين التكنولوجيا الحديثة، التكوين التطبيقي، والخدمات الرقمية الموجهة للسوق الجزائرية.

المطلب الأول: طبيعة الابتكارات في مشروع CyberGuard Algeria

يشكّل تحليل طبيعة الابتكارات في مشروع CyberGuard Algeria مدخلًا محوريا لفهم أسسه التقنية والتطبيقية، باعتبارها عناصر تعكس مستوى التطوير والابتكار في مجال الأمن السيبراني ضمن مقاربة علمية وأكاديمية.

الفرع الأول: الابتكار التكنولوجي

يُعد الابتكار التكنولوجي من أبرز العناصر التي يقوم عليها مشروع CyberGuard Algeria، حيث يعتمد المشروع على توظيف أحدث التقنيات الرقمية في تصميم وتطوير المنصة التعليمية، بهدف توفير

تجربة استخدام احترافية وآمنة وفعالة.

ويظهر الابتكار التكنولوجي في المشروع من خلال عدة عناصر أهمها:

أ/ تطوير منصة تعليمية متخصصة في الأمن السيبراني

يعتمد المشروع على إنشاء منصة رقمية متكاملة موجهة حصريًا لتعليم الأمن السيبراني، وهو ما يمثل توجهًا متخصصًا مقارنة بالمنصات التعليمية التقليدية التي تقدم محتوى عامًا في مختلف المجالات، ويسمح هذا التخصص بتوفير بيئة تعليمية أكثر احترافية وتركيزًا على احتياجات المتعلمين في مجال الحماية المعلوماتية.

ب/ اعتماد تقنيات حديثة في البرمجة والتطوير

يعتمد النموذج الأولي للمشروع على مجموعة من التقنيات الحديثة مثل:

- ✓ React.j لتطوير واجهات المستخدم.
- ✓ Node.js و Express لتطوير الخادم الخلفي.
- ✓ SQLite وقواعد بيانات حديثة لتخزين المعلومات.
- ✓ JWT Authentication لتعزيز الحماية والأمان.

ويسمح هذا التوجه ببناء منصة مرنة، سريعة، وقابلة للتوسع مستقبلاً.

الفرع الثاني: الابتكار في نموذج الخدمة

إضافة إلى الابتكار التقني، يعتمد المشروع على نموذج خدمة مبتكر يهدف إلى تحسين تجربة المستخدم وتوفير حلول تتناسب مع البيئة الجزائرية.

أ/ توفير حلول دفع محلية

من أبرز المشكلات التي يواجهها المستخدم الجزائري صعوبة الدفع الإلكتروني الدولي، لذلك يقدم المشروع نظام دفع محلي يدعم:

- ✓ البطاقة الذهبية.
- ✓ بطاقة CIB.
- ✓ وسائل دفع إلكترونية محلية مستقبلية.

ويُعتبر هذا العنصر ابتكارًا مهمًا يساعد على تسهيل الوصول إلى التكوين الرقمي.

ب/ الجمع بين التعليم النظري والتطبيقي

لا تعتمد المنصة على تقديم فيديوهات تعليمية فقط، بل توفر:

- ✓ حصص مباشرة مع خبراء.
- ✓ مختبرات تطبيقية.
- ✓ تمارين واختبارات تفاعلية.
- ✓ متابعة مستمرة للمتعلمين.

وهو ما يجعل تجربة التعلم أكثر فعالية مقارنة بالمنصات التقليدية.

ج/ بناء مجتمع رقمي متخصص

يسعى المشروع إلى إنشاء مجتمع رقمي للأمن السيبراني داخل الجزائر، يسمح بتبادل الخبرات وتنظيم النقاشات التقنية والتعاون بين الطلبة والخبراء والمؤسسات.

د/ نظام الشهادات الرقمية

يعمل المشروع على تطوير نظام شهادات رقمية قابلة للتحقق إلكترونيًا، بما يسمح بإثبات المهارات المكتسبة بطريقة حديثة وموثوقة.

المطلب الثاني: مجالات الابتكار في مشروع CyberGuard Algeria

يشكّل تحليل مجالات الابتكار في مشروع CyberGuard Algeria إطارًا يوضح فهم نطاق تطبيقاته التقنية والتطويرية، باعتبارها تعكس مستويات التحديث والإبداع في مجال الأمن السيبراني ضمن مقاربة علمية وأكاديمية.

الفرع الأول: الابتكار في المجال التعليمي

يُعتبر الجانب التعليمي من أهم مجالات الابتكار في المشروع، حيث يسعى إلى إعادة تصميم مفهوم التعليم الإلكتروني في مجال الأمن السيبراني داخل الجزائر.

أ/ التخصص الحصري في الأمن السيبراني

تفتقر السوق الجزائرية إلى منصات تعليمية متخصصة بالكامل في مجال الأمن السيبراني، لذلك يقدم المشروع محتوى موجهًا بدقة لهذا المجال بمختلف تخصصاته.

ب/ اعتماد التعليم التفاعلي

تعتمد المنصة على التفاعل المستمر بين المدرب والمتعلم من خلال:

- ✓ البث المباشر.
- ✓ الاختبارات التفاعلية.
- ✓ المختبرات التطبيقية.

- ✓ المشاريع العملية.

ج/ دعم اللغات المتعددة

توفر المنصة محتوى بثلاث لغات:

- ✓ العربية.
- ✓ الإنجليزية.
- ✓ الفرنسية.

وهو ما يساهم في تسهيل الوصول إلى مختلف فئات المستخدمين.

د/ ربط التكوين بسوق العمل

يركز المشروع على المهارات المطلوبة فعليًا داخل سوق العمل الجزائري، بما يساعد المتعلمين على تحسين فرص التوظيف.

الفرع الثاني: الابتكار في المجال الاقتصادي والاجتماعي

لا يقتصر الابتكار في المشروع على الجانب التقني فقط، بل يمتد إلى الجوانب الاقتصادية والاجتماعية.

أ/ تقليل التكاليف التعليمية

يسمح المشروع بالحصول على تكوين احترافي بتكلفة منخفضة مقارنة بالمراكز الأجنبية، مما يساهم في دعم الطلبة والشباب.

ب/ بدعم الاقتصاد الرقمي

يساهم المشروع في:

- ✓ تشجيع ريادة الأعمال الرقمية.
- ✓ خلق فرص عمل جديدة.
- ✓ تطوير قطاع التكنولوجيا في الجزائر.

ج/ تعزيز السيادة الرقمية الوطنية

يهدف المشروع إلى تكوين كفاءات محلية قادرة على حماية المؤسسات الوطنية وتقليل الاعتماد على الخبرات الأجنبية.

د/ نشر الثقافة الأمنية

يساهم المشروع في رفع مستوى الوعي بالأمن السيبراني داخل المجتمع، من خلال التكوين والتوعية

الرقمية.

الفرع الثالث: الابتكار في تجربة المستخدم

يركز مشروع "CyberGuard Algeria" على توفير تجربة استخدام حديثة وسهلة وآمنة.

أ/ واجهة استخدام احترافية

تم تصميم المنصة بواجهة عصرية تدعم:

- ✓ سهولة التنقل.
- ✓ الاستجابة لمختلف الأجهزة.
- ✓ دعم الاتجاه RTL للغة العربية.

ب/ تخصيص تجربة التعلم

توفر المنصة مسارات تعليمية مخصصة حسب:

- ✓ مستوى المستخدم.
- ✓ اهتماماته التقنية.
- ✓ تقدمه الدراسي.

ج/ التفاعل الفوري

تتيح المنصة:

- ✓ التواصل المباشر مع المدربين.
- ✓ التقييمات الفورية.
- ✓ الإشعارات الذكية.

د/ الأمان والحماية

نظرًا لطبيعة المشروع، يتم التركيز بشكل كبير على حماية بيانات المستخدمين وتأمين المنصة ضد الاختراقات والهجمات السيبرانية.

من خلال دراسة الجوانب الابتكارية لمشروع "CyberGuard Algeria" يتضح أن المشروع لا يقتصر على كونه منصة تعليمية رقمية تقليدية، بل يمثل نموذجًا مبتكرًا يجمع بين التكنولوجيا الحديثة، التعليم التفاعلي، والخدمات الرقمية المتخصصة في الأمن السيبراني.

كما يبرز المشروع كحل عملي يواكب متطلبات التحول الرقمي في الجزائر ويساهم في تطوير الكفاءات الوطنية وتعزيز السيادة الرقمية، وهو ما يمنحه إمكانيات كبيرة للنجاح والتوسع مستقبلاً داخل

السوق الوطنية والإقليمية.

المبحث الثالث: التحليل الاستراتيجي للسوق

يُعتبر التحليل الاستراتيجي للسوق من أهم المراحل الأساسية في دراسة المشاريع الناشئة، إذ يسمح بفهم البيئة الاقتصادية والتنافسية التي ينشط فيها المشروع، كما يساعد على تحديد الفرص المتاحة والتحديات المحتملة التي قد تؤثر على نجاحه واستمراريته، ويهدف هذا التحليل إلى دراسة مختلف العناصر المرتبطة بالسوق المستهدف، مثل حجم الطلب، طبيعة العملاء، مستوى المنافسة، والاستراتيجيات التسويقية المناسبة. وفي ظل التطور المتسارع للتكنولوجيا الرقمية وزيادة الاعتماد على الأنظمة المعلوماتية، أصبح سوق الأمن السيبراني من أكثر الأسواق نموًا على المستوى العالمي، خاصة مع تزايد الهجمات الإلكترونية والحاجة إلى حماية البيانات والبنية التحتية الرقمية.

كما يشهد السوق الجزائري بدوره اهتمامًا متزايدًا بمجال الرقمنة والأمن المعلوماتي، سواء من طرف المؤسسات العمومية أو الخاصة أو حتى الأفراد، الأمر الذي يفتح المجال أمام ظهور مشاريع رقمية متخصصة قادرة على تلبية هذه الاحتياجات.

وانطلاقًا من ذلك، يسعى مشروع "CyberGuard Algeria" إلى استغلال هذه الفرص من خلال تقديم خدمات تكوين رقمية متخصصة في الأمن السيبراني، تستجيب لمتطلبات السوق الجزائرية وتوفر حلولًا تعليمية حديثة ومبتكرة.

المطلب الأول: تحليل السوق والقطاع المستهدف

يشكّل تحليل السوق والقطاع المستهدف لمشروع CyberGuard Algeria تصورًا يحدد البيئة الاقتصادية والتنافسية التي ينشط فيها المشروع، وتحديد خصائص الطلب والفئات المستهدفة في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: عرض القطاع السوقي

ينتمي مشروع "CyberGuard Algeria" إلى قطاع التكنولوجيا الرقمية والتعليم الإلكتروني، وبشكل أكثر تخصصًا إلى قطاع الأمن السيبراني والتكوين الرقمي، وهو من القطاعات التي تشهد نموًا متزايدًا عالميًا ومحليًا نتيجة التحول الرقمي المتسارع.

*** مفهوم سوق الأمن السيبراني**

يشمل سوق الأمن السيبراني مختلف الخدمات والحلول المرتبطة بحماية الأنظمة والشبكات والبيانات

من الاختراقات والهجمات الإلكترونية، ويضم:

- ✓ خدمات الحماية الرقمية.
- ✓ التكوين والتدريب الأمني.
- ✓ الاستشارات السيبرانية.
- ✓ حلول اكتشاف الثغرات والهجمات.
- ✓ أنظمة إدارة المخاطر الرقمية.

وقد أصبح هذا القطاع من القطاعات الاستراتيجية التي تعتمد عليها الدول والمؤسسات لضمان أمنها الرقمي واستمرارية خدماتها.

*** تطور سوق الأمن السيبراني في الجزائر**

شهدت الجزائر خلال السنوات الأخيرة توسعًا ملحوظًا في مشاريع الرقمنة والخدمات الإلكترونية، مثل:

- ✓ الرقمنة الإدارية.
- ✓ الخدمات البنكية الإلكترونية.
- ✓ التجارة الإلكترونية.
- ✓ التعليم عن بعد.
- ✓ أنظمة الدفع الإلكتروني.

وقد أدى هذا التطور إلى ارتفاع الحاجة إلى مختصين في الأمن السيبراني قادرين على حماية هذه الأنظمة من التهديدات الرقمية، كما ساهمت عدة عوامل في نمو الطلب على التكوين الأمني، من بينها:

- ✓ ارتفاع عدد الهجمات الإلكترونية.
- ✓ نقص الكفاءات المحلية.
- ✓ توجه الدولة نحو الأمن الرقمي.
- ✓ حاجة المؤسسات إلى حماية بياناتها.

جدول 2: الفئات المستهدفة في السوق:

الفئة المستهدفة	الفئات الفرعية	الاحتياجات الرئيسية	القيمة التي يقدمها المشروع
الطلبة الجامعيون	-طلبة الإعلام الآلي – طلبة الشبكات والاتصالات – طلبة الأمن المعلوماتي – طلبة الذكاء الاصطناعي الذي يُقدَّر بحوالي قرابة مليوني طالب جامعي	-اكتساب مهارات تقنية متخصصة – التدريب التطبيقي	-دورات احترافية – مختبرات افتراضية – شهادات رقمية –

		– تحسين فرص التوظيف	محتوى موجه لسوق العمل
المهنيون والتقنيون	–مسؤولو الأنظمة والشبكات – مهندسو الإعلام الآلي – مطورو البرمجيات – موظفو أقسام تكنولوجيا المعلومات	–تطوير المهارات المهنية – مواكبة التهديدات السيبرانية – تحسين الكفاءة الأمنية	–تكوين متخصص – تدريبات متقدمة – تحديث مستمر للمحتوى
المؤسسات والشركات	–المؤسسات الاقتصادية – الشركات الخاصة – البنوك – شركات الاتصالات، حيث يضم الاقتصاد الجزائري أكثر من 1,655,656 مؤسسة اقتصادية مسجلة في السجل التجاري إلى غاية نهاية نوفمبر 2024، من بينها ما يفوق 1.5 مليون شركة ومؤسسة خاصة تمثل أكثر من 95٪ من النسيج الاقتصادي الوطني، إضافة إلى حوالي 30 بنكًا ومؤسسة مالية تنشط في السوق الجزائرية، إلى جانب 4 مؤسسات رئيسية في قطاع الاتصالات	–تدريب الموظفين – رفع الوعي الأمني – حماية الأنظمة والبيانات	–برامج تدريب جماعية – تكوين مؤسساتي B2B –حلول توعوية متخصصة
الهيئات الحكومية والتعليمية	–الإدارات العمومية – الجامعات – مراكز التكوين – المؤسسات التعليمية حيث يُقدَّر عدد الإدارات والهيئات العمومية بأكثر من 5000 إدارة وهيئة عبر مختلف القطاعات، إضافة إلى حوالي 117 مؤسسة للتعليم العالي، وقرابة 1250 مركزًا ومعهدًا للتكوين والتعليم المهنيين، فضلًا عن أكثر من 30 ألف مؤسسة تعليمية	–نشر الثقافة الأمنية – حماية البنية الرقمية – تكوين الكفاءات	–برامج تكوين وتحسيس – دورات موجهة للقطاع الحكومي – محتوى تعليمي متخصص

الفرع الثاني: تحليل الطلب واحتياجات السوق

في الجزائر، يُتوقع أن يصل حجم سوق خدمات "الأمن السيبراني – خدمات الحماية / Security Services" إلى حوالي 51.37 مليون دولار أمريكي بحلول عام 2025.

كذلك سوق "حماية الشبكات / Network Security" في الجزائر يُقدَّر أن يبلغ 48.65 مليون دولار أمريكي في عام 2025، مع معدل نمو سنوي مركب متوقع (CAGR) حوالي 5.36٪ للفترة

2025–2030، ويُتوقع أن يصل إلى نحو 63.15 مليون دولار بحلول 2030.[1]

في أحد القطاعات المتخصصة، "حماية التطبيقات / Application Security" في الجزائر يُتوقع أن تصل إيراداتها إلى 3.33 مليون دولار أمريكي في 2025، مع نمو سنوي مركب تقريبًا 9.59٪ حتى سنة 2030.[2]يشهد سوق الأمن السيبراني في الجزائر تطورًا متسارعًا بفعل التزايد المستمر في حجم التهديدات الرقمية وتعقيدها، الأمر الذي عزز الحاجة إلى حلول وخدمات متخصصة في حماية الأنظمة والشبكات والبيانات. فقد سُجل خلال سنة 2024 ما يقارب 70 مليون هجوم سيبراني، من بينها أكثر من 13 مليون محاولة تصيد احتيالي، إضافة إلى حوالي 1,200 حادثة اختراق بيانات، مع ارتفاع ملحوظ في معدلات سرقة الهوية الرقمية. [3]

نسبة مستخدمي الإنترنت في الجزائر تقدر بـ ≈ 72.9٪ من السكان في أوائل 2024، مما يدلّ على اتساع الفضاء الرقمي الذي تستهدفه خدمات الأمن السيبراني.[4]

وتشير هذه المعطيات إلى أن البيئة الرقمية الجزائرية أصبحت تواجه تحديات أمنية متنامية، خاصة مع انتشار البرمجيات الخبيثة التي تمثل النسبة الأكبر من التهديدات، إلى جانب هجمات التصيد الإلكتروني، وإصابات الهواتف الذكية، فضلًا عن تنامي هجمات الفدية والاحتيال الرقمي، ويعكس هذا الوضع اتساع الطلب على خدمات الأمن السيبراني، بما في ذلك حلول الحماية، وأنظمة المراقبة والاستجابة للحوادث، والتكوين والتوعية الأمنية، مما يجعل القطاع من الأسواق الواعدة والمرشحة للنمو في الجزائر خلال السنوات المقبلة ومنه، يتبين لنا أن سوق الأمن السيبراني في الجزائر واعد وذو طلب متصاعد مدفوعًا بانتشار الإنترنت، ارتفاع التهديدات الإلكترونية، ومبادرات وطنية لتعزيز السيادة الرقمية.حجم السوق الوطني يُقدّر مبدئيًا بعشرات الملايين من الدولارات سنويًا، مع فرص نمو قوية للخدمات المدارَة، التدريب، وحلول الحماية المخصصة.

CyberGuard Algeria في وضع جيد للاستفادة من فجوة العرض المحلي إذا ركّزت على خدمات استشارية وتكوينية وموديلات اشتراك مرنة، وشراكات استراتيجية مع القطاع العام والجامعات.

المطلب الثاني: تحليل المنافسة والاستراتيجية التسويقية

يشكّل تحليل المنافسة والاستراتيجية التسويقية لمشروع CyberGuard Algeria إطارًا لفهم

[1] StateGlobe **,Identity Theft Rate Statistics in Algeria** (2026) ,March-2026 , ,accessed on :(01/04/2025), Retrieved from the following link :https://bit.ly/4tyyRp4
[2] [2] StateGlobe **,**ibid.
[3] StateGlobe **,**ibid.
[4] **Algeria Invest ,ibid.**

موقعه ضمن السوق الديناميكي للأمن السيبراني، من خلال دراسة مستوى المنافسة وآليات التموقع وبناء الاستراتيجية التسويقية وفق مقاربة علمية وأكاديمية.

الفرع الأول: قياس شدة المنافسة

يشهد سوق الأمن السيبراني في الجزائر تطورًا تدريجيًا من حيث الوعي والاستثمار، إلا أنه ما زال في مرحلة النشوء والتشكل، مما يجعل شدة التنافسية متوسطة إلى ضعيفة حاليًا مع تزايد واضح في السنوات القادمة ولفهم موقع CyberGuard Algeria ضمن هذا المشهد، تم اعتماد نموذج قوى بورتر الخمس (Porter's Five Forces) لتحليل البيئة التنافسية:

1- تهديد المنافسين الحاليين

لا توجد شركات محلية كبرى متخصصة حصريًا في الأمن السيبراني، بل مؤسسات تقنية عامة تقدم خدمات جزئية فقط، واللاعبون الدوليون مثل Kaspersky و ESET و Fortinet متواجدون عبر موزعين محليين، دون وجود فروع رسمية.

شدة المنافسة: متوسطة (5/3)، نظرًا لغياب الاحتكار وتنوع الفرص في السوق المحلي.

2- تهديد القادمين الجدد

سهولة الدخول نسبيًا في الجانب الاستشاري والتدريبي، مقابل صعوبة في مجال تطوير الحلول التقنية بسبب نقص الكفاءات والخبرة المحلية، وتزايد عدد الشركات الناشئة التقنية يفتح الباب لمنافسة مستقبلية.

شدة التهديد: مرتفعة (5/4) على المدى المتوسط.

3- قوة الموردين

تعتمد أغلب الشركات على برمجيات وأدوات أجنبية (Open Source أو مرخصة).

الموردون الأجانب يملكون نفوذًا متوسطًا، خاصة في مجال الأدوات الأمنية المتقدمة.

شدة التأثير: متوسطة (5/3).

4- قوة الزبائن والعملاء

الوعي المؤسسي بأهمية الأمن السيبراني لا يزال محدودًا، مما يجعل العملاء حساسِين تجاه الأسعار، ومع تزايد التشريعات الوطنية (مثل قانون حماية البيانات)، يتوقع أن يزداد الطلب تدريجيًا.

قوة التفاوض: متوسطة إلى مرتفعة (5/3.5).

5- تهديد المنتجات البديلة

بعض المؤسسات تعتمد حلولًا مجانية أو داخلية بدلاً من شراء خدمات متخصصة، مع تطور التهديدات، بدأت هذه البدائل تفقد فعاليتها.

جدول 3: شدة التهديد: منخفضة إلى متوسطة (5/2.5).

البند	درجة الشدة (من 5)	التأثير علينا
المنافسون الحاليون	3.0	مجال مفتوح للنمو
القادمين الجدد	4.0	يتطلب بناء ميزة تنافسية قوية
الموردون	3.0	قابل للتقليل بالاعتماد على أدوات محلية
العملاء	3.5	يحتاج لرفع الوعي وبناء الثقة
المنتجات البديلة	2.5	خطر محدود على المدى القصير

شدة التنافسية الإجمالية: متوسطة (5/3.2)

استنتاج: السوق ما زال في طور التشكل، ويمنح CyberGuard Algeria فرصة ممتازة لبناء ريادة محلية مبكرة إذا ركزت على الابتكار، التدريب، والتكوين المتخصص، و الشراكات النوعية.

7- مؤشرات الأداء التسويقي (KPIs)

لمتابعة فعالية الخطة التسويقية، تعتمد منصة CyberGuard Algeria على مؤشرات كمية ونوعية:

جدول 5: مؤشرات الأداء التسويقي

المؤشر	الهدف السنوي (السنة 1)	التبرير والتوافق المالي والمحاسبي
عدد الزوار الشهري للمنصة	1,500إلى 2,000 زائر	حجم زيارات منطقي ومستهدف عبر ميزانية التسويق البالغة 40,000 دج/شهر
معدل التحويل (Conversion Rate)	2% - 2.5%	المعدل العالمي والمحلي الطبيعي لمنصات التعليم الرقمي الناشئة (تحويل 35 إلى 40 زائراً شهرياً إلى عملاء دفع فعليين لتغطية مبيعات الدورات والاشتراكات)
عدد الشراكات	توقيع مذكرات	إعداد الأرضية والشراكات الجامعية دون إيرادات

المؤسسية(B2B)	تفاهم أولية	مدفوعة، تمهيداً لإطلاق أول عقد مؤسساتي مميز في السنة الثانية كما نصت الدراسة المعتمدة.
رضا العملاء (Customer Satisfaction)	85%+	مؤشر نوعي لضمان تجديد الاشتراكات الفردية ورفع معدل الولاء للمنصة الرقمية.
نمو المتابعين على المنصات	25%ربع سنوي	يضمن الانتشار العضوي وبناء الوعي بالعلامة التجارية في قطاع الأمن السيبراني الجزائري.

8- تحليل المنافسين :

جدول 6: تحليل المنافسين

الشركات العالمية (Kaspersky / Cisco / ESET / Fortinet)	منصة 7.77	Cybright Academy	Algérie Télécom – Cyber Security Division	Cyberrian Algeria	Cybears	CyberGuard Algeria منصتي	المعيار
دعم لغوي محصور وغير مناسب للسوق الجزائري	**منصة محلية تدعم العربية**	**منصة جديدة لكن لا تدعم العربية**	**التركيز تقني فقط، دعم لغوي ضعيف**	**خبرة محلية لكن لا يدعم العربية**	**دعم لغوي محصور وغير مناسب للسوق الجزائري**	**يدعم العربية والإنجليزية و الفرنسية وموجه للسوق الجزائري**	**اللغة و الدعم المحلي**
منصات متقدمة لكنها معقدة	**محدود للغاية**	**لا يوجد نظام رقمي متكامل**	**منصات تقنية موجهة للمؤسسات فقط**	**يركز على الشبكات فقط**	**منصات متقدمة مع انعدام الوصول المباشر**	**واجهة سهلة وصول مباشر**	**سهولة الاستخدام**

دعم عالمي لكن غير محلي ومكلف	تدريب محدود وغير منهجي	تدريب غير منهجي	غياب برامج تدريب	تدريب محدود	تدريب محدود يركز على الخدمات اكثر	تدريب احترافي + مسارات تعلم + دعم محلي مستمر	التكيف مع السوق الجزائري
مرتفعة جدًا	مجانية	مقبولة	مرتفعة جدًا	مقبولة	مرتفعة جدًا	تسعير مرن مناسب للمؤسسات الصغيرةوالمتوسطة	التكلفة

9- تحليل SWOT للمشروع

جدول 4: تحليل SWOT للمشروع

العناصر	التفاصيل
نقاط القوة	-التخصص الحصري في مجال الأمن السيبراني. - توفير محتوى تدريبي موجه للسوق الجزائرية. - دعم اللغات العربية والفرنسية والإنجليزية. - توفير نظام دفع محلي (الذهبية و CIB). - التركيز على التطبيق العملي والمختبرات الافتراضية. - إمكانية الوصول إلى التكوين عن بعد من مختلف الولايات. - الاعتماد على تقنيات حديثة في تطوير المنصة.
نقاط الضعف	-محدودية الموارد المالية في المراحل الأولى. - ضعف الشهرة والعلامة التجارية عند الانطلاق. - الحاجة إلى تسويق واسع لبناء الثقة. - صعوبة استقطاب خبراء ومدربين معتمدين بشكل دائم. - الاعتماد الكبير على البنية التحتية الرقمية والإنترنت.
الفرص	-النمو المتزايد لسوق الأمن السيبراني في الجزائر والعالم. - توجه الدولة نحو الرقمنة والتحول الرقمي. - ارتفاع الطلب على الكفاءات السيبرانية. - دعم المؤسسات الناشئة والابتكار الرقمي. - ضعف المنافسة المحلية المتخصصة. - إمكانية التوسع نحو السوق المغاربية والإفريقية.
التهديدات	-المنافسة القوية من المنصات الأجنبية العالمية. - التطور السريع للتكنولوجيا والهجمات الإلكترونية. - احتمال دخول منافسين جدد إلى السوق المحلي. - مخاطر الاختراقات والهجمات على المنصة نفسها. - التغيرات الاقتصادية التي قد تؤثر على القدرة الشرائية للمستخدمين.

الفرع الثاني: الاستراتيجية التسويقية للمشروع

يعتمد مشروع "CyberGuard Algeria" على استراتيجية تسويقية رقمية تهدف إلى الوصول إلى أكبر عدد ممكن من المستخدمين المستهدفين وبناء علامة تجارية قوية في مجال الأمن السيبراني.

1- قنوات التسويق (Marketing Channels)

لضمان وصول فعّال إلى الجمهور، تعتمد CyberGuard على مزيج متكامل من القنوات:

جدول 5: قنوات التسويق (Marketing Channels)

القناة	الوصف	الهدف
المنصة الإلكترونية	موقع تفاعلي يقدم خدمات التدريب والتحليل والاستشارة	جذب المستخدمين وبناء قاعدة بيانات
وسائل التواصل الاجتماعي	حملات توعوية رقمية عبر منصات التواصل الاجتماعي.	نشر الوعي وترويج العلامة
الشراكات المؤسسية	تعاون مع الجامعات والهيئات الحكومية	تعزيز المصداقية وتوسيع الانتشار
الفعاليات والورش	تنظيم أيام تحسيسية وملتقيات تدريبية	تفاعل مباشر مع السوق المحلي
البريد الإلكتروني المهني	نشر نشرات أمنية شهرية وتقارير تحليلية	الحفاظ على التواصل مع العملاء

2- استراتيجية التمركز في السوق

يسعى المشروع إلى التمركز كأول منصة جزائرية متخصصة بشكل احترافي في الأمن السيبراني، مع التركيز على:

- ✓ الجودة التقنية.
- ✓ التكوين التطبيقي.
- ✓ الأسعار المناسبة.
- ✓ القرب من المستخدم الجزائري.

3- استراتيجية التسويق الرقمي يعتمد المشروع على مجموعة من أدوات التسويق الرقمي، منها:

- ✓ التسويق عبر مواقع التواصل الاجتماعي.
- ✓ الإعلانات الممولة.
- ✓ البريد الإلكتروني التسويقي.
- ✓ التسويق بالمحتوى التقني.
- ✓ تحسين الظهور في محركات البحث (SEO).

4- التسويق عبر الشراكات : يسعى المشروع إلى عقد شراكات مع:

- ✓ الجامعات.
- ✓ النوادي العلمية.
- ✓ المؤسسات الاقتصادية.
- ✓ الهيئات الحكومية.

بهدف توسيع قاعدة المستخدمين وتعزيز المصداقية.

5- استراتيجية بناء المجتمع :يركز المشروع على إنشاء مجتمع رقمي متخصص من خلال:

- ✓ تنظيم مسابقات تقنية.
- ✓ إنشاء منتديات ونقاشات.
- ✓ تقديم محتوى مجاني توعوي
- ✓ تنظيم ورشات وندوات رقمية.

6- سياسة التسعير :تعتمد المنصة على أسعار تنافسية تتناسب مع السوق الجزائرية، مع:

- ✓ دورات مجانية مدفوعة.
- ✓ تخفيضات للطلبة.
- ✓ عروض خاصة للمؤسسات.

من خلال التحليل الاستراتيجي للسوق يتضح أن مشروع "CyberGuard Algeria" ينشط داخل قطاع واعد يتميز بنمو متسارع وطلب متزايد على خدمات الأمن السيبراني والتكوين الرقمي، كما أظهر التحليل وجود فجوة حقيقية داخل السوق الجزائرية يمكن للمشروع استغلالها من خلال تقديم خدمات تعليمية متخصصة تجمع بين الجودة، التخصص، والتكلفة المناسبة إضافة إلى ذلك، فإن اعتماد المشروع على استراتيجية تسويقية رقمية وشراكات محلية من شأنه أن يعزز فرص نجاحه وانتشاره داخل السوق الوطنية مستقبلاً.

المبحث الرابع: خطة الإنتاج والتنظيم

تُعتبر خطة الإنتاج والتنظيم من أهم المحاور الأساسية في دراسة المشاريع الناشئة، حيث تهدف إلى توضيح الكيفية التي سيتم من خلالها إنتاج الخدمة أو المنتج، إضافة إلى تحديد الموارد البشرية والتقنية والتنظيمية اللازمة لضمان حسن سير المشروع وتحقيق أهدافه، وتكتسي هذه الخطة أهمية كبيرة بالنسبة للمشاريع الرقمية، نظرًا لاعتمادها على التكنولوجيا والأنظمة المعلوماتية والبنية التحتية الرقمية بدل وسائل الإنتاج التقليدية.

ويختلف مفهوم الإنتاج في المشاريع الرقمية عن المشاريع الصناعية، إذ يرتبط أساسًا بتطوير البرمجيات، إدارة البيانات، تصميم الخدمات الإلكترونية، وتوفير البنية التحتية التقنية اللازمة لتشغيل المنصة وضمان استقرارها وأمانها ،كما يعتمد نجاح المشروع الرقمي على كفاءة التنظيم الداخلي، توزيع المهام، وجود فريق عمل مؤهل قادر على إدارة مختلف العمليات التقنية والإدارية والتسويقية.

وفي هذا الإطار، يعتمد مشروع "CyberGuard Algeria" على نموذج إنتاج رقمي يرتكز على تطوير منصة إلكترونية متخصصة في الأمن السيبراني، مع توفير محتوى تدريبي رقمي، مختبرات افتراضية، وأنظمة تفاعلية حديثة تهدف إلى تقديم تجربة تعليمية احترافية وآمنة للمستخدمين.

المطلب الأول: عملية الإنتاج والتموين

يمثّل تحليل عملية الإنتاج والتموين لمشروع CyberGuard Algeria إطارًا يهدف إلى توضيح كيفية تسيير الموارد وتنظيم مختلف مراحل النشاط داخل المشروع، بما يعكس آليات اشتغال سلسلة القيمة في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: عملية الإنتاج في المشروع الرقمي

نظرًا لكون مشروع "CyberGuard Algeria" مشروعًا رقميًا، فإن عملية الإنتاج لا تعتمد على تصنيع مادي، وإنما ترتكز على إنتاج خدمات ومنتجات رقمية تتمثل أساسًا في تطوير المنصة التعليمية وإعداد المحتوى التدريبي وإدارة الأنظمة الإلكترونية.

1- مراحل عملية الإنتاج الرقمي :

تمر عملية الإنتاج داخل المشروع بعدة مراحل مترابطة تتمثل :

أ/ مرحلة التحليل والتخطيط :تُعتبر هذه المرحلة الأساس الذي يُبنى عليه المشروع، حيث يتم خلالها:

- ✓ دراسة احتياجات السوق والمستخدمين.
- ✓ تحديد خصائص المنصة.

- ✓ إعداد التصاميم الأولية.
- ✓ اختيار التقنيات المناسبة للتطوير.

وتهدف هذه المرحلة إلى وضع تصور شامل لكيفية عمل المنصة والخدمات التي ستوفرها.

ب/ مرحلة التصميم والتطوير : تشمل هذه المرحلة

- ✓ تصميم واجهات المستخدم UI/UX
- ✓ تطوير الواجهة الأمامية للمنصة
- ✓ لابرمجة الأنظمة الأمنية.
- ✓ تطوير الخادم الخلفي وقواعد البيانات
- ✓ تطوير لوحة التحكم الخاصة بالمستخدمين والمدربين.

ويتم الاعتماد على تقنيات حديثة مثل:

- ✓ React.js
- ✓ Node.js
- ✓ Express.js
- ✓ قواعد البيانات الحديثة
- ✓ أنظمة الحماية والتوثيق

ج. مرحلة إنتاج المحتوى التدريبي : تتمثل في:

- ✓ إعداد الدورات التعليمية.
- ✓ تسجيل الشروحات التقنية.
- ✓ تصميم المختبرات الافتراضية.
- ✓ إعداد الاختبارات التطبيقية
- ✓ إنشاء ملفات وموارد تعليمية رقمية.

ويتم ذلك بالتعاون مع مختصين وخبراء في الأمن السيبراني.

د. مرحلة الاختبار وضمان الجودة : قبل إطلاق المنصة يتم:

- ✓ اختبار الأداء والاستقرار.
- ✓ فحص الثغرات الأمنية.
- ✓ تجربة مختلف الخصائص.
- ✓ اختبار تجربة المستخدم.
- ✓ معالجة الأخطاء التقنية.

وتهدف هذه المرحلة إلى ضمان جودة الخدمة الرقمية وحماية بيانات المستخدمين.

هـ. مرحلة التشغيل والصيانة : بعد إطلاق المنصة يتم

- ✓ مراقبة الخوادم والأنظمة.
- ✓ حديث المحتوى.
- ✓ معالجة المشاكل التقنية.
- ✓ تطوير مزايا جديدة.
- ✓ تحسين الأداء والحماية بشكل مستمر.

الفرع الثاني: التموين والموارد التقنية

في المشاريع الرقمية يرتبط التموين أساسًا بتوفير الموارد التقنية والبرمجية اللازمة لتشغيل المنصة وضمان استقرارها.

1- الموارد التقنية الأساسية

يعتمد مشروع "CyberGuard Algeria" على مجموعة من الموارد التقنية، أهمها:

جدول 6: الموارد التقنية الأساسية

المورد التقني	الاستخدام
الخوادم السحابية	استضافة المنصة وقواعد البيانات
قواعد البيانات	تخزين معلومات المستخدمين والدورات
أدوات الحماية السيبرانية	تأمين المنصة ضد الهجمات
أدوات تطوير البرمجيات	برمجة وتحديث النظام
خدمات التخزين السحابي	حفظ الملفات والمحتوى التدريبي
أدوات الاجتماعات المباشرة	تنظيم الحصص التفاعلية

2- التموين البرمجي :

- ✓ شراء أو استخدام البرمجيات الضرورية.
- ✓ الاشتراك في الخدمات السحابية.
- ✓ الحصول على تراخيص بعض الأدوات التقنية.
- ✓ استخدام مكتبات وأطر تطوير حديثة.

3- إدارة البيانات والحماية : نظرًا لطبيعة المشروع، يتم التركيز بشكل كبير على

- ✓ حماية بيانات المستخدمين.
- ✓ تشفير المعلومات الحساسة.
- ✓ إنشاء نسخ احتياطية دورية.
- ✓ مراقبة الأنظمة الأمنية باستمرار.

المطلب الثاني: التنظيم الداخلي والشراكات الرئيسية

يشكّل تحليل التنظيم الداخلي والشراكات الرئيسية لمشروع CyberGuard Algeria إطارًا لفهم أساليب التسيير الداخلي وبنية العلاقات التعاونية التي يعتمدها، بما يبرز مدى تكامل الوظائف وتوسّع مجالات الشراكة في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: اليد العاملة والتنظيم الإداري

يعتمد مشروع "CyberGuard Algeria" على فريق عمل متعدد التخصصات يساهم في تسيير المشروع وضمان استمرارية تطويره.

1- الهيكل التنظيمي للمشروع

يتكون الهيكل التنظيمي من عدة أقسام مترابطة، تتمثل في:

جدول 7: الهيكل التنظيمي للمشروع

القسم	المهام الرئيسية
الإدارة العامة	التخطيط، اتخاذ القرارات، متابعة سير المشروع
القسم التقني	تطوير وصيانة المنصة والأنظمة
قسم الأمن السيبراني	اختبار الحماية وتحليل الثغرات
قسم المحتوى والتكوين	إعداد الدورات والمختبرات التعليمية
قسم التسويق	الترويج وإدارة الحملات الرقمية
قسم الدعم الفني	مساعدة المستخدمين ومعالجة المشاكل

2- الموارد البشرية المطلوبة

يتطلب المشروع مجموعة من الكفاءات، أهمها:

- ✓ مطورو برمجيات.

- ✓ مختصو أمن سيبراني.
- ✓ مصممو واجهات المستخدم.
- ✓ مدربون وخبراء تقنيون.
- ✓ مختصو تسويق رقمي.
- ✓ موظفو دعم فني.

2- نمط العمل المعتمد : يعتمد المشروع على:

- ✓ العمل عن بعد (Remote Work).
- ✓ الاجتماعات الرقمية.
- ✓ أدوات إدارة المشاريع الإلكترونية.
- ✓ بيئة عمل مرنة تعتمد على التكنولوجيا.

ويُساعد هذا النموذج على تقليل التكاليف التشغيلية وتحسين الإنتاجية.

الفرع الثاني: الشراكات الرئيسية

تُعتبر الشراكات عنصرًا أساسيًا في نجاح المشروع، حيث تساعد على توسيع الخدمات وزيادة المصداقية والوصول إلى عدد أكبر من المستخدمين.

1- الشراكات الأكاديمي : يسعى المشروع إلى التعاون مع:

- ✓ الجامعات الجزائرية.
- ✓ مراكز التكوين.
- ✓ النوادي العلمية وذلك بهدف:
- ✓ استقطاب الطلبة.
- ✓ تنظيم دورات وورشات.
- ✓ دعم البحث والتطوير.

2- الشراكات التقنية : تشمل التعاون مع:

- ✓ مزودي الخدمات السحابية.
- ✓ شركات التكنولوجيا.
- ✓ خبراء الأمن السيبراني.
- ✓ مطوري البرمجيات.

3- الشراكات المؤسساتية : يهدف المشروع إلى عقد اتفاقيات مع:

- ✓ المؤسسات الاقتصادية.
- ✓ البنوك.
- ✓ شركات الاتصالات.
- ✓ الهيئات الحكومية

من أجل:

- ✓ تدريب الموظفين.
- ✓ تقديم برامج توعية أمنية.
- ✓ توفير خدمات تكوين احترافية.

4- الشراكات التسويقية : تشمل

- ✓ التعاون مع المؤثرين التقنيين.
- ✓ الشراكة مع المجتمعات الرقمية.
- ✓ المشاركة في الفعاليات التكنولوجية.

الفرع الثالث: سير العمل داخل المنصة الرقمية

يعتمد مشروع "CyberGuard Algeria" على نظام عمل رقمي متكامل يسمح بتقديم الخدمات التعليمية بطريقة منظمة وآمنة.

جدول 8: سير العمل داخل المنصة الرقمية

المرحلة	وصف العملية
التسجيل وإنشاء الحساب	يقوم المستخدم بإنشاء حساب داخل المنصة
اختيار الدورة	تصفح الدورات واختيار البرنامج المناسب
الدفع الإلكتروني	إتمام عملية الدفع عبر وسائل الدفع المحلية
الوصول للمحتوى	متابعة الدروس والمختبرات التفاعلية
التقييم والمتابعة	إجراء الاختبارات وتتبع التقدم
الحصول على الشهادة	منح شهادة رقمية بعد إتمام الدورة

من خلال دراسة خطة الإنتاج والتنظيم يتضح أن مشروع "CyberGuard Algeria" يعتمد على نموذج إنتاج رقمي حديث يرتكز على تطوير الخدمات الإلكترونية والمحتوى التدريبي التفاعلي بدل الإنتاج المادي التقليدي، كما يعتمد المشروع على بنية تنظيمية مرنة وكفاءات متعددة التخصصات

تساهم في ضمان جودة الخدمات واستمرارية التطوير. إضافة إلى ذلك، تلعب الشراكات التقنية والأكاديمية و

المؤسساتية دورًا محوريًا في دعم المشروع وتعزيز فرص نجاحه داخل السوق الجزائرية والمغاربية مستقبلا.

المبحث الخامس: الخطة المالية

تُعتبر الخطة المالية من أهم المحاور الأساسية في دراسة المشاريع الناشئة، حيث تسمح بتحديد الاحتياجات المالية للمشروع وتقييم مدى قدرته على تحقيق الاستدامة والربحية مستقبلاً، كما تساعد على تقدير مختلف التكاليف المرتبطة بمرحلة التأسيس والتشغيل، إضافة إلى دراسة الإيرادات المتوقعة وتحليل الجدوى الاقتصادية للمشروع، وبالنسبة للمشاريع الرقمية، فإن طبيعة التكاليف تختلف عن المشاريع الصناعية أو التجارية التقليدية، إذ تتركز أساسًا على تكاليف التطوير البرمجي، الخدمات السحابية، التسويق الرقمي، الموارد البشرية التقنية، والصيانة المستمرة للأنظمة الإلكترونية، كما تتميز المشاريع الرقمية بإمكانية تقليل التكاليف التشغيلية من خلال الاعتماد على العمل عن بعد والاستعانة بخدمات خارجية (Outsourcing) بدل توظيف عدد كبير من العمال بشكل دائم.

وانطلاقًا من ذلك، يعتمد مشروع "CyberGuard Algeria" على نموذج مالي مرن يتناسب مع طبيعة المؤسسات الناشئة، حيث يتم التركيز على تقليل المصاريف الثابتة والاعتماد على التعاقدات الخارجية في العديد من المهام التقنية والتسويقية، مع تخصيص مكتب صغير لإدارة المشروع واستقبال الاجتماعات والشركاء.

المطلب الأول: نظرة عامة على المشروع

1 تعريف المشروع

مشروع CyberGuard Algeria هو منصة تعليمية رقمية متخصصة في مجال الأمن السيبراني، تهدف إلى توفير تكوين احترافي عالي الجودة لفائدة الطلبة والمهنيين والمؤسسات داخل الجزائر، تقدم المنصة دورات تدريبية تقنية، مختبرات افتراضية، جلسات مباشرة مع خبراء، وشهادات رقمية قابلة للتحقق، وذلك بأسعار مناسبة للقدرة الشرائية المحلية مع دعم وسائل الدفع الإلكترونية الجزائرية.

2 الفرصة السوقية

يُقدَّر حجم سوق الأمن السيبراني في الجزائر بأكثر من 51 مليون دولار سنويًا بحلول عام2025، مع معدل نمو سنوي مركب يناهز 5.4%، سجّلت الجزائر خلال 2024 ما يقارب

70مليون هجوم سيبراني، مع نقص حاد في الكفاءات المحلية المتخصصة، يُتيح هذا الواقع فرصة استثمارية

استثنائية لمشروع CyberGuard Algeria باعتباره المنصة التعليمية الجزائرية الأولى المتخصصة في هذا المجال الحيوي.

3 نموذج الإيرادات

تعتمد المنصة على أربعة مصادر إيراد رئيسية:

- ✓ دورات فردية: 9,000 دج للدورة الواحدة
- ✓ اشتراكات شهرية: 7,000 دج/شهر/مشترك
- ✓ تكوين مؤسساتي (B2B): 150,000 دج/عقد
- ✓ خدمات متنوعة وعمولة خبراء: 10% من الأرباح

المطلب الثاني: الاستثمار الأولي وتكاليف التأسيس

1 تفصيل الاستثمار الأولي

يبلغ إجمالي الاستثمار الأولي اللازم لإطلاق مشروع CyberGuard Algeria مبلغ 931.000 دج، وهو استثمار معقول نسبيًا مقارنة بالمشاريع التقنية الأخرى، نظرًا للطابع الرقمي للمشروع الذي يقلل من الحاجة إلى بنية تحتية مادية كثيفة.

جدول 9: تفصيل الاستثمار الأولي

بند الاستثمار	المبلغ (دج)	النسبة%
ثلاثة مكاتب + ثلاثة كراسي	96.000	10.3%
ثلاثة حواسيب + حاسوب رئيسي	350.000	37.6%
طابعة + هاتف ثابت + مكيف هوائي	135.000	14.5%
إنشاء و تطوير منصة إلكترونية	200.000	21.5%
الرسوم القانونية و الإدارية التأسيسية	50.000	5.4%

احتياطي المالي الأولي	100.000	10.7%
الإجمالي	**931.000**	**100%**

ملاحظة :يمكن تخفيض قيمة الاستثمار الأولي في حال الاعتماد على التمويل الجزئي أو الحصول على دعم من برامج المؤسسات الناشئة، كصندوق دعم المؤسسات الناشئة الجزائرية.

2 هيكل التمويل المقترح

جدول 10: هيكل التمويل المقترح

مصدر التمويل	النسبة%	المبلغ (دج)
تمويل ذاتي (رأس مال شخصي)	40%	372.400
قرض بنكي / صندوقANGEM	35%	325.850
دعم برنامج المؤسسات الناشئة	25%	232.750
الإجمالي	**100%**	**931.000**

1.3 التكاليف الثابتة

التكاليف الثابتة هي النفقات التي يتحملها المشروع بصرف النظر عن حجم المبيعات .تشمل الرواتب والإيجار والاشتراكات الأساسية.

جدول 11: التكاليف الثابتة

بند التكلفة الثابتة	شهري (دج)	سنوي (دج)
إيجار المحل	40.000	480.000
الرواتب والأجور الإجمالية	490.000	5.880.000
الاستضافة السحابية	18.000	216.000
الإنترنت	3.600	43.200
الكهرباء	6.000	72.000
الصيانة والتحديثات	40.000	480.000
التسويق الرقمي	40.000	480.000

إجمالي التكاليف الثابتة	637.600	7.651.200

2.3 التكاليف المتغيرة

تتراوح التكاليف المتغيرة في السنة الأولى بين 15% من الإيرادات، وتنخفض تدريجيًا إلى 9% في السنة السابعة بفضل اقتصاديات الحجم .تشمل :تكاليف إضافة محتوى جديد، عمولات المدربين الخارجيين، تكاليف الخوادم الإضافية عند ارتفاع حركة المرور، ومصاريف التسويق المرتبطة بالإيرادات.

جدول 12: التكاليف المتغيرة

البيان	س1	س2	س3	س4	س5	س6	س7
التكاليف الثابتة(دج)	7.65	7.65	7.65	7.65	7.65	7.65	7.65
التكاليف المتغيرة(دج)	0.54	0.88	1.43	1.99	2.59	3.48	4.12
نسبة التكاليف المتغيرة	15%	13%	12%	11%	10%	10%	9%

المطلب الثالث: توقعات الإيرادات السنوية

يُعدّ تقدير الإيرادات السنوية خطوة أساسية لقياس الجدوى الاقتصادية للمشروع وتوقع أدائه المستقبلي.

1 خطة الإيرادات التفصيلية لكل سنة

بُنيت توقعات الإيرادات على أساس دراسة السوق الجزائري ومعدلات اختراق المنصات الرقمية التعليمية، مع مراعاة مراحل نمو المشروع من الإطلاق إلى النضج.

جدول 13: خطة الإيرادات التفصيلية لكل سنة

مصدر الإيراد	السنة 1	السنة 2	السنة 3	السنة 4	السنة 5	السنة 6	السنة 7
عدد الدورات الفردية/السنة	240	420	720	1.080	1.560	2.100	2.760
إيراد الدورات (دج)	2.160.000	3.780.000	6.480.000	9.720.000	14.040.000	18.900.000	24.840.000
متوسط المشتركين الشهريين	15	30	55	85	120	160	210
إيراد الاشتراكات (دج)	1.260.000	2.520.000	4.620.000	7.140.000	10.080.000	13.440.000	17.640.000
عقود تكوين مؤسساتي	0	1	2	3	5	7	10
إيراد الخدمات المتنوعة+العمولات (دج)	200.000	350.000	540.000	760.000	1.050.000	1.400.000	1.800.000
إجمالي الإيرادات السنوية (دج)	3.620.000	6.800.000	11.940.000	18.070.000	25.920.000	34.790.000	45.780.000
معدل النمو السنوي %	–	87.8%	75.6%	51.3%	43.4%	34.2%	31.6%

2 الأرباح والخسائر السنوية

يوضح هذا الفصل تطور أداء المشروع من الناحية الربحية عبر السنوات السبع، مع تحليل مفصل لكل مكون من مكونات قائمة الدخل.

جدول 14: الأرباح والخسائر السنوية

البيان	السنة1	السنة2	السنة3	السنة4	السنة5	السنة6	السنة7
إجمالي الإيرادات	3.620.000	6.800.000	11.940.000	18.070.000	25.920.000	34.790.000	45.780.000
(-)إجمالي التكاليف	(8.194.200)	(8.535.200)	(9.084.000)	(9.638.900)	(10.243.200)	(11.130.200)	(11.771.400)
EBITDA	-4.574.200	-1.735.200	2.856.000	8.431.100	15.676.800	23.659.800	34.008.600
(-)الاستهلاك والإطفاء	(186.200)	(186.200)	(186.200)	(186.200)	(186.200)	(0)	(0)
الربح التشغيلي EBIT	-4.760.400	-1.921.400	2.669.800	8.244.900	15.490.600	23.659.800	34.008.600
(-)ضريبة الدخل IBS 19%	(0)	(0)	(507.262)	(1.566.531)	(2.943.214)	(4.495.362)	(6.461.634)
صافي الربح / الخسارة	-4.760.400	-1.921.400	2.162.538	6.678.369	12.547.386	19.164.438	27.546.966
هامش الربح الصافي%	-131.5%	-28.3%	18.1%	37.0%	48.4%	55.1%	60.2%

تحليل: يتوقع أن يحقق المشروع أرباحًا إيجابية ابتداءً من السنة الثانية، مع تحسن مستمر في هامش الربح الصافي ليصل إلى مستويات مرتفعة في السنوات الأخيرة، مما يعكس قابلية توسع النموذج التجاري للمنصة الرقمية.

المطلب الرابع: التدفقات النقدية

يُعدّ تحليل التدفقات النقدية من أهم أدوات التقييم المالي، إذ يعكس القدرة الفعلية للمشروع على توليد السيولة وتلبية التزاماته المالية دون الاعتماد على تمويل خارجي.

جدول 15: التدفقات النقدية

بند التدفق النقدي	السنة1	السنة2	السنة3	السنة4	السنة5	السنة6	السنة7
صافي الربح(دج)	-4.760.400	-1.921.400	2.162.538	6.678.369	12.547.386	19.164.438	27.546.966
(+)الاستهلاك والإطفاء	186.200	186.200	186.200	186.200	186.200	0	0
التدفق النقدي التشغيلي(OCF)	-4.574.200	-1.735.200	2.348.738	6.864.569	12.733.586	19.164.438	27.546.966
(-)النفقات الرأسمالية (CAPEX)	-	-	-	(150.000)	-	-	-
التدفق النقدي الحر(FCF)	-4.574.200	-1.735.200	2.348.738	6.714.569	12.733.586	19.164.438	27.546.966
التدفق النقدي التراكمي	-5.505.200	-7.240.400	-4.891.662	1.822.907	14.556.493	33.720.931	61.267.897

ملاحظة: يبدأ التدفق النقدي التراكمي بقيمة سالبة تمثل الاستثمار الأولي البالغ 931.000 دج، ثم يتحول إلى موجب بعد استرداد رأس المال.

2 نقطة التعادل

نقطة التعادل هي مستوى الإيرادات الذي تتساوى فيه إجمالي الإيرادات مع إجمالي التكاليف (لا ربح ولا خسارة).

- ✓ إجمالي التكاليف الثابتة السنوية: 7.651.200 دج
- ✓ معدل التكاليف المتغيرة: 15% من الإيرادات
- ✓ إيرادات نقطة التعادل: 9.001.412 دج
- ✓ الوقت المتوقع للوصول: 30 شهرًا من الإطلاق

3 معدل العائد على الاستثمار ROI

جدول 16: معدل العائد على الاستثمار ROI

المؤشر	س1	س2	س3	س4	س5	س6	س7
صافي الربح(دج)	-4.760.400	-1.921.400	2.162.538	6.678.369	12.547.386	19.164.438	27.546.966
ROI %	-511.3%	-206.4%	232.3%	717.3%	1347.7%	2058.5%	2958.9%

4 صافي القيمة الحالية (NPV) ومعدل العائد الداخلي (IRR)

باستخدام معدل خصم 12% (يعكس تكلفة رأس المال في الجزائر):

- ✓ صافي القيمة الحالية NPV: 28.936.145 دج
- ✓ معدل العائد الداخلي IRR: 64.2%
- ✓ تفسير: طالما أن NPV > 0 وIRR > معدل الخصم (12%)، فإن المشروع مجدي ماليًا ويستحق الاستثمار.

5 فترة استرداد رأس المال

- ✓ فترة الاسترداد البسيطة: 45 شهرًا (3.8 سنة)

هذه الفترة معقولة جدًا لمشاريع التكنولوجيا والتعليم الرقمي، حيث تتراوح عادةً بين 3 و6 سنوات في هذا القطاع.

يعكس ذلك قدرة المشروع على استرداد استثماره الأولي في أقل من نصف عمره الافتراضي.

6 الجدول المالي الموحد (7 سنوات)

يُدرج فيما يلي الجدول المالي الشامل الذي يجمع جميع المؤشرات المالية للسنوات السبع في قراءة موحدة ومنظمة.

جدول 17: الجدول المالي الموحد (7 سنوات)

المؤشر المالي	السنة1	السنة2	السنة3	السنة4	السنة5	السنة6	السنة7
الإيرادات							
إجمالي الإيرادات (دج)	3.620.000	6.800.000	11.940.000	18.070.000	25.920.000	34.790.000	45.780.000
هامش الربح الإجمالي%	-126.4%	-25.5%	23.9%	46.7%	60.5%	68.0%	74.3%
التكاليف							
التكاليف الثابتة(دج)	7.651.200	7.651.200	7.651.200	7.651.200	7.651.200	7.651.200	7.651.200
التكاليف المتغيرة(دج)	543.000	884.000	1.432.800	1.987.700	2.592.000	3.479.000	4.120.200
إجمالي التكاليف	8.194.200	8.535.200	9.084.000	9.638.900	10.243.200	11.130.200	11.771.400
الأرباح والخسائر							
EBITDA(دج)	4.574.200-	1.735.200-	2.856.000	8.431.100	15.676.800	23.659.800	34.008.600
الاستهلاك والإطفاء(دج)	186.200	186.200	186.200	186.200	186.200	0	0
الربح التشغيلي (دج) EBIT	-4.760.400	-1.921.400	2.669.800	8.244.900	15.490.600	23.659.800	34.008.600
الضرائب IBS 19%	0	0	507.262	1.566.531	2.943.214	4.495.362	6.461.634
صافي الربح(دج)	-4.760.400	-1.921.400	2.162.538	6.678.369	12.547.386	19.164.438	27.546.966
هامش الربح الصافي%	-131.5%	-28.3%	18.1%	37.0%	48.4%	55.1%	60.2%
التدفقات النقدية							
التدفق النقدي التشغيلي(دج)	-4.574.200	-1.735.200	2.348.738	6.864.569	12.733.586	19.164.438	27.546.966
النفقات الرأسمالية(دج)	0	0	0	150.000	0	0	0
التدفق النقدي الحر(دج)	-4.574.200	-1.735.200	2.348.738	6.714.569	12.733.586	19.164.438	27.546.966
التدفق النقدي	-5.505.200	-7.240.400	-4.891.662	1.822.907	14.556.493	33.720.931	61.267.897
التراكمي(دج)							
مؤشرات الأداء							
العائد على الاستثمار ROI %	-511.3%	-206.4%	232.3%	717.3%	1347.7%	2058.5%	2958.9%
عدد الدورات المباعة	240	420	720	1.080	1.560	2.100	2.760
عدد المشتركين الشهريين	15	30	55	85	120	160	210
عقود التكوين المؤسساتي	0	1	2	3	5	7	10

المطلب الخامس: الرسوم البيانية وتطور الأداء المالي

1 تطور الإيرادات والأرباح

جدول 18: تطور الإيرادات والأرباح

تطور الإيرادات والأرباح السنوية							
الإيراد	4 م	7م	12م	18م	26م	35م	46م
الربح	-4.760.400	-1.921.400	2.162.538	6.678.369	12.547.386	19.164.438	27.546.966
	س1	س2	س3	س4	س5	س6	س7

2 تطور التدفقات النقدية التراكمية

جدول 19: تطور التدفقات النقدية التراكمية

التدفق التراكمي	سنة1	سنة2	سنة3	سنة4	سنة5	سنة6	سنة7
(م دج)	-5.51	-7.24	-4.89	1.82	14.56	33.72	61.27
الوضع	سالب	سالب	سالب	لاموجب	لاموجب	لاموجب	لاموجب

المطلب السادس: تحليل الحساسية والمخاطر المالية

1 تحليل السيناريوهات

يتضمن تحليل الحساسية دراسة تأثير التغيرات في الإيرادات والتكاليف على المؤشرات المالية الرئيسية، وذلك لتقدير هامش الأمان في المشروع.

جدول 20: تحليل السيناريوهات

السيناريو	NPV (دج)	IRR %	فترة الاسترداد
سيناريو متشائم (−20% إيرادات)	14.658.830	51.3%	56 شهرًا
سيناريو قاعدي (أساسي)	28.936.145	64.2%	45 شهرًا
سيناريو متفائل (+20% إيرادات)	42.855.087	77.0%	37 شهرًا
سيناريو صعود قوي (+35%)	53.301.034	86.6%	31 شهرًا

2 المخاطر الرئيسية وخطط التخفيف

يتضمن هذا المحور تحديد أبرز المخاطر ووضع آليات مناسبة للتخفيف منها.

جدول 21: المخاطر الرئيسية وخطط التخفيف

نوع المخاطرة	خطة التخفيف	احتمالية الحدوث	فعالية التخفيف
بطء اكتساب المستخدمين	حملات تسويقية مكثفة + شراكات جامعية	متوسطة	مرتفعة
المنافسة من منصات أجنبية	التميز بالمحتوى المحلي والأسعار التنافسية	متوسطة	مرتفعة
تقلبات سعر الصرف (نفقات تقنية)	اعتماد أدوات مفتوحة المصدر قدر الإمكان	منخفضة	متوسطة
الهجمات السيبرانية على المنصة	تطبيق أعلى معايير أمان المنصة (JWT)	منخفضة	مرتفعة
تراجع القدرة الشرائية	تقديم خطط تقسيط وعروض مخفضة	متوسطة	متوسطة
صعوبة استقطاب خبراء	عقود شراكة مرنة + نظام العمولات	منخفضة	مرتفعة

3. ملخص المؤشرات المالية الرئيسية

يقدّم هذا القسم أهم المؤشرات المالية الأساسية للمشروع.

جدول 22: ملخص المؤشرات المالية الرئيسية

المؤشر	القيمة
إجمالي الاستثمار الأولي	931.000 دج
إجمالي الإيرادات على 7 سنوات	146.920.000 دج
إجمالي التكاليف على 7 سنوات	68.597.100 دج
إجمالي صافي الأرباح على 7 سنوات	61.417.897 دج
نقطة التعادل السنوية	9.001.412 دج
فترة الوصول لنقطة التعادل	30 شهرًا
صافي القيمة الحالية NPV (12%)	28.936.145 دج
معدل العائد الداخلي IRR	64.2%
فترة استرداد رأس المال	45 شهرًا (3.8 سنة)
العائد على الاستثمار ROI السنة 7	2958.9%
هامش EBITDA السنة 7	74.3%

..

4. توقعات النمو والتوسع

يتناول هذا الجزء توقعات النمو والتوسع المستقبلي للمشروع بناءً على المؤشرات الحالية وفرص التطوير المتاحة.

جدول 23: مراحل تطور المشروع عبر السنوات السبع:

المرحلة	الفترة	الإنجازات المستهدفة	الهدف الاستراتيجي
مرحلة الإطلاق	السنة 1	بناء المنصة، MVP، اكتساب أول 180 مستخدم	التأسيس والتجريب
مرحلة النمو	السنة 2	توسيع المحتوى، 420 مستخدم، أول ربح صافٍ	الربحية الأولى
مرحلة التعزيز	السنة 3	660 مستخدم، دخول قطاع المؤسسات B2B	الاستقرار
مرحلة التوسع	السنة 4	1,020 مستخدم، شراكات جامعية، تجديد تقني	التوسع المحلي
مرحلة النضج	السنة 5	1,440 مستخدم، إطلاق برامج شهادات احترافية	القيادة السوقية
مرحلة الريادة	السنة 6	1,920 مستخدم، استهداف السوق المغاربية	البداية الإقليمية
مرحلة الهيمنة	السنة 7	2,520 مستخدم، 10 عقود B2B، مرجع وطني	الريادة الكاملة

خلاصة الدراسة المالية

تُثبت هذه الدراسة المالية الشاملة أن مشروع CyberGuard Algeria يُعدّ مشروعًا استثماريًا مجديًا ماليًا واقتصاديًا، وذلك استنادًا إلى المؤشرات التالية:

جدول 24: الدراسة المالية الشاملة

صافي القيمة الحالية موجب	NPV = 28.936.145 دج > 0 ← المشروع يولد قيمة فعلية تفوق تكلفة رأس المال
معدل عائد داخلي مرتفع	IRR = 64.2% > معدل الخصم 12% ← المشروع يتجاوز الحد الأدنى المطلوب للاستثمار
فترة استرداد معقولة	45 شهرًا ← أقل من نصف عمر المشروع الافتراضي البالغ 7 سنوات
نمو مستدام في الإيرادات	من 3.620.000 دج (س1) إلى 45.780.000 دج (س7)
هامش ربح متصاعد	هامش EBITDA يصل إلى 74.3% في السنة السابعة
تدفق نقدي حر موجب	ابتداءً من السنة الثانية، مما يضمن الاستدامة المالية

التوصيات المالية

بناءً على نتائج الدراسة المالية، يُوصى بما يلي:

- ✓ الإطلاق الفوري: المشروع جاهز للتطبيق بالحد الأدنى من الاستثمار، مع إمكانية تحقيق ربحية خلال السنة الثانية.
- ✓ إدارة السيولة: الحفاظ على احتياطي نقدي يعادل 3 أشهر من التكاليف الثابتة خلال السنة الأولى.
- ✓ التركيز على الاشتراكات الشهرية: تمثل الإيرادات المتكررة ركيزة استقرار مالي أساسية، وتستحق الأولوية في جهود التسويق.
- ✓ توسيع B2B مبكر: عقد عقود التكوين المؤسساتي من السنة الثانية يُسرّع الوصول لنقطة التعادل ويقلل من المخاطر.
- ✓ استثمار في التسويق: تخصيص 40,000 دج/شهر للتسويق مبدئيًا مع رفعه تدريجيًا بما يتناسب

مع نمو الإيرادات.

- ✓ مراجعة سنوية: إجراء مراجعة مالية دورية كل 6 أشهر لتحديث التوقعات وتعديل الخطة وفق المستجدات.

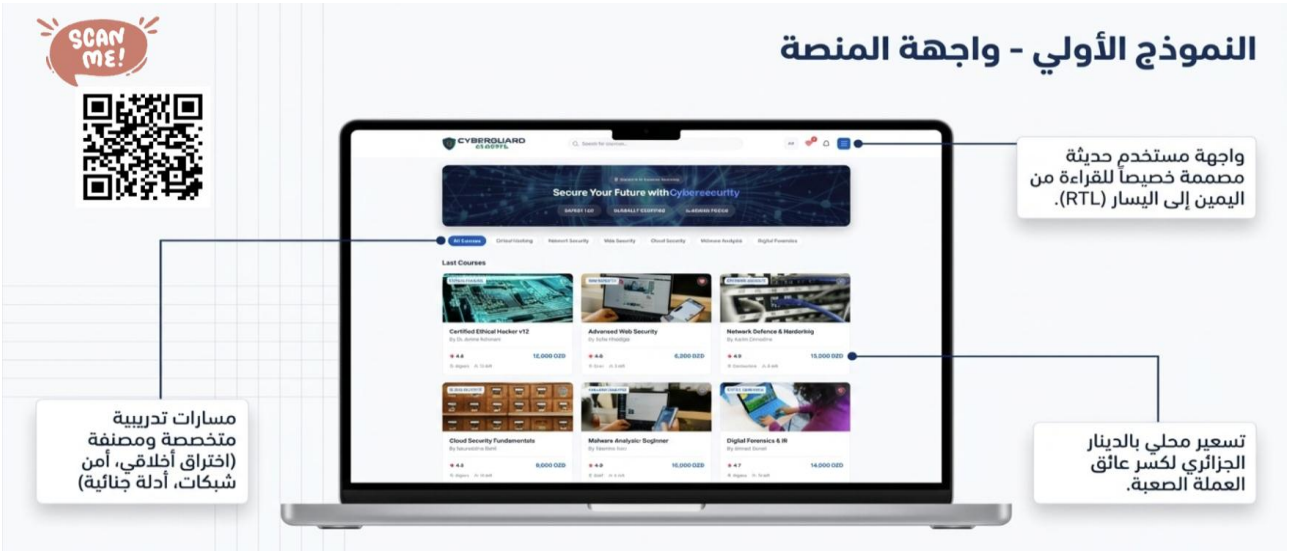
المبحث السادس: النموذج الأولي التجريبي

يُعتبر النموذج الأولي التجريبي (Prototype ou MVP) من أهم المراحل الأساسية في تطوير المؤسسات الناشئة الرقمية، حيث يسمح بتحويل الفكرة النظرية إلى منتج عملي قابل للتجربة والتقييم.

كما يساعد على اختبار مدى قابلية المشروع للتطبيق داخل السوق، وفهم احتياجات المستخدمين بشكل أفضل، إضافة إلى اكتشاف النقائص التقنية والتنظيمية قبل الانتقال إلى مرحلة الإطلاق الكامل.

وانطلاقًا من ذلك، قام مشروع "CyberGuard Algeria" بتطوير نموذج أولي رقمي لمنصة تعليمية متخصصة في الأمن السيبراني، يعتمد على تقنيات حديثة ويوفر مجموعة من الوظائف الأساسية التي تسمح بتقديم تجربة تعليمية تفاعلية وآمنة، ويُشكل هذا النموذج خطوة أولية نحو بناء منصة وطنية متكاملة في مجال التكوين السيبراني الرقمي.

شكل4: رابط تجربة المنصة



المطلب الأول: عرض النموذج الأولي التقني

يشكّل عرض النموذج الأولي التقني لمشروع CyberGuard Algeria مرحلة أساسية لفهم بنيته التقنية وآليات عمله، من خلال إبراز أهم مكوناته الوظيفية والتقنية في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: مفهوم النموذج الأولي في المشروع

يتمثل النموذج الأولي لمشروع "CyberGuard Algeria" في نسخة أولية قابلة للاستخدام من المنصة

الرقمية، تم تطويرها بهدف:

- ✓ اختبار وظائف المنصة الأساسية.
- ✓ تقييم تجربة المستخدم.
- ✓ دراسة قابلية المشروع للتوسع.
- ✓ جمع الملاحظات التقنية والتنظيمية.
- ✓ عرض المشروع على المستثمرين والشركاء.

ويعتمد النموذج الحالي على تقديم مجموعة من الخدمات التعليمية الرقمية المرتبطة بالأمن السيبراني، مع التركيز على سهولة الاستخدام والتفاعل العملي.

الفرع الثاني: التقنيات المستخدمة في تطوير النموذج

تم تطوير النموذج الأولي باستخدام مجموعة من التقنيات الحديثة التي تسمح ببناء منصة مرنة وآمنة وسريعة الأداء.

جدول 25: جدول التقنيات المستخدمة

المجال	التقنية المستخدمة	الوظيفة
الواجهة الأمامية	React.js	تطوير واجهات المستخدم التفاعلية
أداة البناء	Vite	تحسين سرعة التطوير والأداء
التصميم والحركات	Framer Motion	إنشاء واجهات حديثة وحركات ديناميكية
الخادم الخلفي	Node.js + Express.js	إدارة البيانات والخدمات الخلفية
قاعدة البيانات	SQLite	تخزين بيانات المستخدمين والدورات
المصادقة والحماية	JWT Authentication	تأمين تسجيل الدخول والبيانات
إدارة الأكواد	Git & GitHub	تتبع التطوير والتعاون البرمجي
الاستضافة	Cloud Hosting	تشغيل المنصة عبر الإنترنت

المطلب الثاني: خصائص ومكونات النموذج الأولي

يشكّل تحليل خصائص ومكونات النموذج الأولي لمشروع CyberGuard Algeria خطوة أساسية لفهم بنيته التقنية ووظائفه الأساسية، من خلال إبراز مستوى التكامل والفعالية في تصميمه ضمن مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: الوظائف الأساسية للمنصة

يتضمن النموذج الأولي مجموعة من الخصائص الرئيسية التي تسمح بتقديم تجربة استخدام متكاملة.

* **نظام التسجيل وتسجيل الدخول:** يوفر النموذج

- ✓ إنشاء حسابات للمستخدمين.
- ✓ تسجيل الدخول الآمن.
- ✓ استرجاع كلمة المرور.
- ✓ إدارة صلاحيات المستخدمين.

* **لوحة التحكم (Dashboard):** تم تطوير لوحة تحكم خاصة بكل فئة من المستخدمين، حيث تسمح بـ:

- ✓ متابعة الدورات.
- ✓ إدارة الحسابات.
- ✓ تتبع التقدم الدراسي.
- ✓ إدارة المحتوى من طرف المدربين.

* **نظام الدورات التعليمية:** يشمل

- ✓ عرض الدورات المتاحة.
- ✓ تصنيف المحتوى حسب المستوى.
- ✓ تشغيل الفيديوهات التعليمية.
- ✓ تحميل الموارد التعليمية.

* **نظام الحجز والدفع:** يتضمن

- ✓ حجز الدورات.
- ✓ إدارة المقاعد المتاحة.
- ✓ الدفع الإلكتروني المحلي.
- ✓ متابعة العمليات المالية.

* **التقييمات والشهادات:** تسمح المنصة بـ:

- ✓ إجراء اختبارات إلكترونية.
- ✓ تقييم أداء المتعلمين.
- ✓ منح شهادات رقمية قابلة للتحقق.

الفرع الثاني: تصميم وتجربة المستخدم

يركز النموذج الأولي على توفير تجربة استخدام احترافية تتناسب مع طبيعة المنصة التعليمية الحديثة.

* **تصميم الواجهة:** تم تصميم الواجهة وفق المبادئ التالية:

- ✓ البساطة وسهولة الاستخدام.
- ✓ التصميم العصري.
- ✓ دعم اللغة العربية واتجاه RTL.
- ✓ التوافق مع الهواتف والحواسيب.

* **تجربة المستخدم (UX):** يعتمد المشروع على

- ✓ سهولة التنقل داخل المنصة.
- ✓ سرعة الوصول إلى المحتوى.
- ✓ تقليل التعقيد التقني.
- ✓ تحسين التفاعل بين المستخدم والمنصة.

* **الهوية البصرية:** تعتمد المنصة على

- ✓ ألوان مرتبطة بالأمن السيبراني.
- ✓ تصميم احترافي حديث
- ✓ عناصر بصرية تقنية تعكس طبيعة المشروع.

المطلب الثالث: تقييم النموذج الأولي وآفاق التطوير

يشكّل تقييم النموذج الأولي وآفاق تطويره لمشروع CyberGuard Algeria مرحلة تحليلية تهدف إلى الوقوف على مدى فعاليته التقنية الحالية واستشراف إمكانيات تحسينه وتطويره مستقبلًا في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

الفرع الأول: نتائج النموذج الأولي: ساهم النموذج الأولي في تحقيق عدة نتائج إيجابية، أهمها:

- ✓ إثبات قابلية المشروع للتطبيق.
- ✓ اختبار البنية التقنية للمنصة.
- ✓ تحسين تجربة المستخدم.
- ✓ تحديد النقائص التقنية والتنظيمية.
- ✓ تقديم تصور عملي للمستثمرين والشركاء.

كما سمح النموذج بتجربة عدد من الخصائص الأساسية قبل الانتقال إلى مرحلة التطوير الكامل.

الفرع الثاني: التحديات التقنية والتنظيمية: رغم النتائج الإيجابية، واجه المشروع بعض التحديات، من بينها:

- ✓ محدودية الموارد المالية.
- ✓ الحاجة إلى تطوير البنية السحابية.
- ✓ صعوبة إنشاء مختبرات افتراضية متقدمة.
- ✓ الحاجة إلى توسيع فريق العمل.
- ✓ متطلبات الحماية والأمان المرتفعة.

الفرع الثالث: آفاق تطوير النموذج مستقبلاً

يسعى المشروع إلى تطوير النموذج الأولي وتحويله إلى منصة متكاملة من خلال:

- ✓ تطوير المختبرات الافتراضية
- ✓ إنشاء بيئات تدريب أكثر احترافية تسمح بمحاكاة هجمات حقيقية داخل المتصفح.

* دمج تقنيات الذكاء الاصطناعي: مثل

- ✓ المساعد الذكي.
- ✓ تحليل أداء المستخدمين.
- ✓ التوصيات التعليمية الذكية
- ✓ تطوير تطبيقات الهاتف
- ✓ إطلاق تطبيقات Android و iOS لتسهيل الوصول إلى المنصة.

* التوسع في المحتوى التدريبي وإضافة:

- ✓ دورات متقدمة.
- ✓ برامج احترافية.
- ✓ شهادات معتمدة.

التوسع الجغرافي: استهداف

- ✓ السوق المغاربية.
- ✓ الدول العربية.
- ✓ المؤسسات الدولية مستقبلاً.

الفرع الرابع: وصف سير استخدام المنصة

يوضح الجدول التالي طريقة عمل المنصة بداية من تسجيل المستخدم حتى الحصول على الشهادة

جدول 26: عمل المنصة

المرحلة	وصف العملية
إنشاء الحساب	يقوم المستخدم بإنشاء حساب شخصي داخل المنصة
تسجيل الدخول	الدخول الآمن باستخدام البريد الإلكتروني وكلمة المرور
اختيار الدورة	تصفح واختيار الدورة المناسبة
الدفع الإلكتروني	إتمام عملية الدفع عبر وسائل الدفع المحلية
متابعة المحتوى	مشاهدة الدروس وإنجاز التطبيقات
الحصول على الشهادة	استخراج شهادة رقمية بعد إتمام الدورة

الفرع الخامس: شعار المشروع

CYBERGUARD ALGERIA

*** تحليل لشعار ***

الدرع: يرمز إلى الحماية والأمن، وهو العنصر المركزي الذي يعبر عن الدفاع السيبراني.

القفل في الأعلى: يمثل الأمان الرقمي وحماية البيانات.

الدوائر والخطوط المحيطة: ترمز إلى التكنولوجيا، الشبكات، والأنظمة الإلكترونية المتصلة.

الألوان (الأخضر والأحمر) والهلال والنجمة: مستوحاة من العلم الجزائري، ما يعزز الانتماء الوطني والثقة.

النص (Cyberguard Algeria) : الاسم يدمج بين التخصص التكنولوجي الدقيق)الحارس الرقمي) والانتماء الوطني)الجزائر .(ليعكس باختصار هويّة "درع الحماية والدفاع عن الفضاء السيبراني الجزائري."

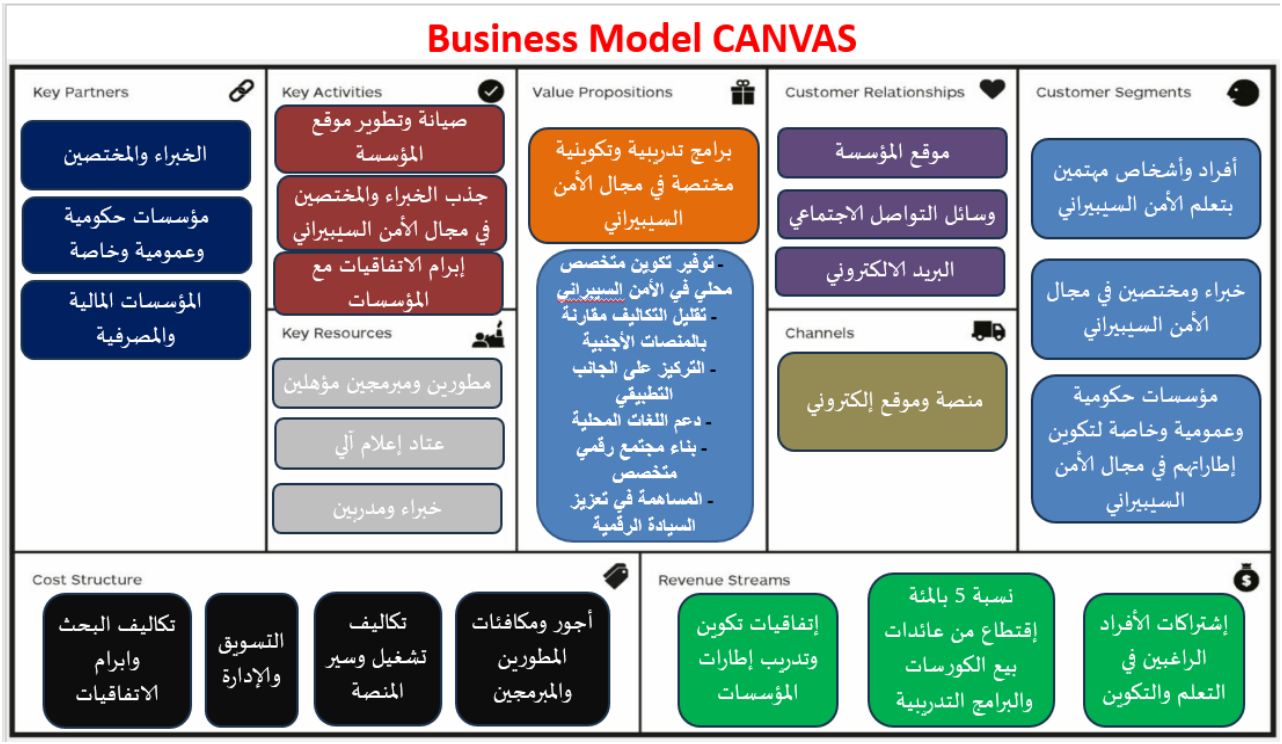
الخلاصة:

الشعار يجمع بين رموز الأمن والتكنولوجيا والانتماء الوطني في تصميم بسيط ومعبّر عن مهمة المنصة في حماية الفضاء السيبراني الجزائري. من خلال دراسة النموذج الأولي التجريبي لمشروع "CyberGuard Algeria" يتضح أن المشروع يمتلك أساسًا تقنيًا قويًا يسمح بتحويل الفكرة إلى منصة تعليمية رقمية قابلة للتطوير والتوسع. كما أظهر النموذج الأولي إمكانية توفير تجربة تعليمية احترافية تجمع بين التكوين النظري والتطبيقي في مجال الأمن السيبراني. ورغم بعض التحديات التقنية والتنظيمية، فإن المشروع يمتلك آفاقًا واعدة للنمو والتوسع، خاصة مع تزايد الحاجة إلى التكوين الأمني الرقمي داخل الجزائر والمنطقة المغاربية.

المطلب الرابع: نموذج العمل التجاري

يمثّل نموذج العمل التجاري لمشروع CyberGuard Algeria إطارًا يوضح كيفية خلق القيمة وتقديمها وتحقيق الإيرادات، من خلال تحديد آليات التشغيل والعلاقات مع مختلف الفاعلين في مجال الأمن السيبراني وفق مقاربة علمية وأكاديمية.

جدول 27: نموذج العمل التجاري



خلاصة الفصل الثالث:

يتمحور هذا الفصل حول تقديم نموذج متكامل لمؤسسة ناشئة تحت اسم"CyberGuard Algeria" ، وهي منصة رقمية تعليمية وتفاعلية متخصصة في التدريب على الأمن السيبراني بالجزائر؛ حيث يغطي الفصل فكرة المشروع وقيمه المقترحة المتمثلة في تقديم محتوى عالي الجودة متعدد اللغات يدعم وسائل الدفع المحلية، معززاً بتحليل استراتيجي دقيق للسوق والمنافسين (SWOT) يبرز الفرص والتحديات، بالإضافة إلى تحديد الهيكل التنظيمي والتشغيلي، والخطط التسويقية والمالية التي تضمن خفض التكاليف واستدامة الإيرادات، وصولاً إلى استعراض النموذج الأولي التجريبي (MVP) وآفاق تطويره المستقبلية لدمج تقنيات الذكاء الاصطناعي والمختبرات الافتراضية لخدمة الأمن الرقمي الوطني.

الخاتمة

الخاتمة

في ضوء ما تم تحليله، تبين أن السياسة العامة الأمنية في الجزائر تعيش مرحلة تحول عميق بفعل تسارع التحولات الرقمية وتزايد التهديدات السيبرانية، التي لم تعد مجرد مخاطر تقنية معزولة، بل أصبحت عنصرًا بنيويًا يعيد تشكيل مفهوم الأمن الوطني ذاته. فقد أضحى الفضاء السيبراني مجالًا استراتيجيًا تتقاطع فيه الأبعاد السياسية والاقتصادية والاجتماعية والقانونية، مما فرض على الدولة الجزائرية إعادة تكييف منظومتها الأمنية بما يضمن الانتقال من المقاربة التقليدية للأمن إلى مقاربة شاملة ومندمجة للأمن السيبراني.

وقد أبرز التحليل أن تطور الإطار المفاهيمي والسياسي للأمن السيبراني في الجزائر جاء تدريجيًا عبر مراحل تشريعية ومؤسساتية متعاقبة، عكست إدراكًا متزايدًا لخطورة التهديدات الرقمية، رغم استمرار وجود تحديات مرتبطة بندرة الكفاءات المتخصصة، وتطور أساليب الهجمات، وضعف التكامل بين الفاعلين المؤسساتيين. كما أظهر الفصل أن فعالية السياسة العامة الأمنية ترتبط ارتباطًا وثيقًا بتفاعل مجموعة من المحددات الجيوسياسية والجيواقتصادية والجيواستراتيجية، إضافة إلى تعدد الفواعل الرسمية وغير الرسمية المشاركة في صنع القرار الأمني.

وعليه، يمكن القول إن الجزائر قطعت شوطًا مهمًا في بناء منظومة للأمن السيبراني، إلا أن تحقيق سيادة سيبرانية فعالة ومستدامة يظل مرهونًا بتعزيز القدرات التقنية والبشرية، وتطوير الإطار القانوني والمؤسساتي، وترسيخ ثقافة الأمن الرقمي، بما يسمح بالانتقال من مرحلة الاستجابة إلى مرحلة الاستباق في مواجهة التهديدات السيبرانية، وبما يضمن حماية الأمن الوطني في سياق دولي يتسم بالتعقيد وعدم الاستقرار المتزايد في الفضاء الرقمي، كذلك يُمثّل مشروع " "CyberGuard Algeriaنموذجاً استراتيجياً مبتكراً في ريادة الأعمال الرقمية الموجهة لخدمة الأمن المعلوماتي في الجزائر، متجاوزاً المفهوم التقليدي للمنصات التعليمية. وقد أثبتت الدراسة الميدانية والتحليل الاستراتيجي والمالي للمشروع مرونة نموذجه الاقتصادي، وقدرته على تحقيق الاستدامة والربحية عبر مواءمته لمتطلبات البيئة المحلية وحلول الدفع المتاحة. إن الانتقال بالفكرة إلى نطاق النموذج الأولي التجريبي (MVP)يعكس جاهزية المشروع الفنية والأكاديمية لسد الفجوة المعرفية وتأهيل كفاءات وطنية متخصصة في الأمن السيبراني. وفي المحصلة، يبرز المشروع كإضافة نوعية تدعم المنظومة الدفاعية الرقمية، وتساهم بفعالية في تعزيز التحول الرقمي الآمن وتحقيق السيادة السيبرانية للجزائر في مواجهة التحديات الراهنة.

الخاتمة

النتائج المتوصل إليها:

- ✓ أظهرت الدراسة أن الأمن السيبراني يشكل بعدًا استراتيجيًا أصيلاً ضمن منظومة الأمن الوطني، ولم يعد عنصرًا ثانويًا أو تكميليًا.
- ✓ تبين أن التحول الرقمي يساهم في تعزيز كفاءة الأداء الحكومي، لكنه في الوقت ذاته يوسع من نطاق المخاطر السيبرانية ويزيد من تعقيدها.
- ✓ أكدت النتائج أن الجرائم السيبرانية تتسم بخصائص نوعية، أبرزها الطابع العابر للحدود، وصعوبة التتبع، والتطور التقني المستمر.
- ✓ كشفت الدراسة عن وجود علاقة ترابط وتأثير متبادل بين مستوى الأمن السيبراني ونجاح سياسات التحول الرقمي.
- ✓ بين التحليل أن حماية البنى التحتية الحيوية أصبحت رهينة بمدى جاهزية الأنظمة السيبرانية وقدرتها على الصمود أمام الهجمات.
- ✓ توصلت الدراسة إلى أن فعالية السياسات الأمنية الحديثة تستدعي تكامل الأبعاد التقنية مع الأطر القانونية والمؤسساتية.
- ✓ أكدت النتائج أن تحقيق السيادة الرقمية يمثل أحد أهم رهانات الأمن الوطني في العصر الرقمي.
- ✓ أظهرت الدراسة أن غياب التنسيق المؤسسي والتشريعي يشكل أحد أبرز التحديات التي تعيق بناء منظومة سيبرانية فعالة.

وبناءً على ما تم التوصل إليه من نتائج في هذه الدراسة، يمكن القول إن الفرضيات الثلاث قد تحققت فعلياً، حيث أظهرت المعطيات أن تزايد التهديدات السيبرانية قد فرض ضرورة مراجعة وتطوير المقاربة الأمنية التقليدية في الجزائر، كما تبين أن وجود بعض القصور على المستوى القانوني والتنظيمي يحدّ من فعالية منظومة الأمن السيبراني ويؤثر على جاهزيتها. إضافة إلى ذلك، فإن تحقيق الحصانة الرقمية للدولة أصبح مرتبطًا بشكل وثيق بمدى قدرة السياسات الأمنية على التكيف مع التحولات الرقمية والتكنولوجية المتسارعة، وهو ما يؤكد وجود علاقة ترابطية واضحة بين الأمن السيبراني ونجاح مسار التحول الرقمي.

ومن هنا يمكننا تقديم بعض الاقتراحات المتواضعة كالتالي:

- ✓ إنشاء قيادة وطنية موحدة للأمن السيبراني.
- ✓ تحديث الإطار التشريعي بشكل دوري ومرن.
- ✓ تعزيز الشراكة مع القطاع الخاص والجامعات.
- ✓ تطوير منظومة استخبارات سيبرانية وطنية.
- ✓ تعزيز التعاون الدولي والإقليمي.

قائمة المصادر و المراجع

أولاً: المصادر والمراجع باللغة العربية

-القرآن الكريم :

1. سورة النمل :الآية 19

- الوثائق الرسمية والتشريعات

1. الأمر رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية، العدد 04، 2005.
2. الجمهورية الجزائرية الديمقراطية الشعبية، دستور 1976، الجريدة الرسمية للجمهورية الجزائرية، العدد 5، (25 فبراير 1976).
3. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 15-261، المؤرخ في 8 أكتوبر 2015، الجريدة الرسمية للجمهورية الجزائرية، العدد 53، (2015).
4. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 25-321 المؤرخ في 30 ديسمبر 2025 المتعلق بالمصادقة على الاستراتيجية الوطنية لأمن نظم المعلومات 2025-2029، الجريدة الرسمية للجمهورية الجزائرية، العدد 87، الصادر في 30 ديسمبر 2025.
5. القانون رقم 15/04، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، (2004).
6. القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والمتعلق بتوسيع التجريم ليشمل أفعال الدخول أو البقاء غير المشروع في نظام معلوماتي والتلاعب بالمعطيات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، 2006.
7. القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 46، 2009.
8. المرسوم الرئاسي رقم 14-252، المؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، صادر بتاريخ 28 سبتمبر 2014.

9. المرسوم الرئاسي رقم 26-07، المؤرخ في 7 جانفي 2026، المتعلق بإنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في كل مؤسسة وإدارة وهيئة عمومية وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 04، 2026.

الكتب:

1. الطيب حسن أبشر، الدولة العصرية دولة مؤسسات القانون، (القاهرة: دار الفجر للنشر والتوزيع، ط1، 2005).
2. الفهداوي فهمي خليفة، السياسة العامة: منظور كلي في البنية والتحليل، (عمان: دار المسرة، ط1، 2001).
3. القريطي دحان حيزام، الأمن السيبراني وحماية أمن المعلومات، (الإسكندرية: دار الفكر الجامعي، 2022).
4. ألموند غابريال، باول بن جيهام، السياسة المقارنة في وقتنا الحاضر: ترجمة هشام عبد الله، (عمان: الأهلية للنشر والتوزيع، 1999).
5. اندرسون جيمس، صنع السياسات العامة، ترجمة عامر الكيسي، (عمان: دار المسيرة، 1999).
6. بن عنتر عبد النور، البعد المتوسطي للأمن الجزائري: الجزائر، أوروبا والحلف الأطلسي، (الجزائر: المكتبة العصرية للطباعة والنشر، ط1، 2005).
7. بيومي علي محمود، دول الصفوة في اتخاذ القرار السياسي، (القاهرة: دار الكتاب الحديث، 2004).
8. خيري عبد القوي، دراسة السياسة العامة، (الكويت: ذات السلاسل للطباعة والنشر والتوزيع، 1988).
9. سعيفان أحمد، قاموس المصطلحات السياسية والدستورية والدولية، (بيروت: مكتبة لبنان، 2005).
10. لخضاري منصور، السياسة الأمنية الجزائرية: المحددات – الميادين – التحديات، (الدوحة: المركز العربي للأبحاث ودراسات السياسات، ط1، 2015).
11. ناجي عبد النور و ساحلي مبروك، مقدمة في دراسة السياسة العامة، (عنابة: دار العلوم للنشر والتوزيع، 2014).
12. مهنا نصر محمد، علم السياسة، (القاهرة: دار غريب للطباعة والنشر، 1995).

المقالات والمجلات العلمية

1. السمحان منى عبد الله، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد 111، (يوليو 2020).
2. الفتلاوي أحمد عبيس نعمة، بحث الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، المجلد 8، العدد 4، 2016.
3. ساحلي مبروك، نظرية السلام الديمقراطي: كآلية لتحقيق السلام المستدام، مجلة دراسات وأبحاث، م12، ع3، (جويلية 2020).
4. شاهد إلياس، عرابة الحلاج، دفرو عبد النعيم، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، ع3، (ديسمبر 2016).
5. عدنان إبراهيم وفايز خضر، الأدلة الرقمية واثبات الجرائم السيبرانية: بين التأصيل والتأويل، المجلة الفلسطينية للأبحاث القانونية، ع1، (اكتوبر 2021).
6. عطية إدريس، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، م1، ع1، 2019.
7. قويدري علي، العيش امال، الجريمة السيبرانية مفهومها وسبل الوقاية منها، مجلة نوميرس الاقتصادية، م03، ع01، 2022.
8. لعور وهيبة، الأمن السيبراني في الجزائر، سياسات ومؤسسات، مجلة الفكر الشرطي، ع28، 2022.
9. لوكال مريم، قراءة في اتفاقية الاتحاد الافريقي حول الامن السيبراني وحماية المعطيات ذات طابع شخصي 2014، مجلة الدراسات القانونية والاقتصادية، م04، ع03، 2021.

الرسائل الجامعية

1. الشهراني محمد سعيد العياش، أثر العولمة على مفهوم الأمن القومي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2007/2006.
2. ضمبري عزيزة، الفواعل السياسية دورها في صنع السياسة العامة في الجزائر، رسالة ماجستير غير منشورة، جامعة الحاج لخضر، كلية الحقوق، باتنة، 2008/2007.

الملتقيات والمؤتمرات

1. زوامبية عبد النور، دور السلطة التشريعية في رسم السياسة العامة في الجزائر، مداخلة في الملتقى الوطني للسياسات العامة ودورها في بناء الدولة وتنمية المجتمع بجامعة مولاي الطاهر، سعيدة، 2009.

المواقع الإلكترونية والتقارير الرقمية

1. استراتيجية الأمن السيبراني الوطنية للجزائر 2025–2029: تحليل معمّق، 15 ديسمبر 2025، نقلاً عن الرابط: https://tinyurl.com/2hmuratc
2. بن ميرة مصطفى ، "G5 في الجزائر: بين حلم التحول الرقمي وكابوس التهديد السيبراني"، 06 ماي 2025، نقلاً عن الرابط: https://bit.ly/3OqJjQu
3. ميار عبد الحميد، تقى عبد الحميد، دور القيادة السياسية الروسية في تعزيز الأمن السيبراني، 22 جوان 2023، نقلاً عن الرابط: https://bit.ly/4vt63QK
4. ميتيهان دورماز، اتفاقية الأمم المتحدة الجديدة لمكافحة الجرائم الإلكترونية: الأهداف والثغرات، منصة دعم السلامة الرقمية، 12 ديسمبر 2024، عبر الرابط: https://tinyurl.com/yrhh5pzx
5. وزارة الدفاع الوطني الجزائرية، المدرسة العسكرية المتعددة التقنيات، نقلاً عن الرابط: https://bit.ly/48hmntG
6. وزارة الصحة الجزائرية، دورة تكوينية حول أمن البيانات الصحية، 06 جوان 2024، نقلاً عن الرابط: https://bit.ly/41eFRLN

ثانياً: المصادر والمراجع باللغات الأجنبية

Official Documents (الوثائق الرسمية)

1. United Nations General Assembly, Resolution 55/63: Combating the Criminal Misuse of Information Technologies, 4 December 2000 (adopted 2001), New York: United Nations.
2. United Nations General Assembly, Resolution 57/239: Creation of a Global Culture of Cybersecurity, 20 December 2002, New York: United Nations.

Books (الكتب)

1. Dewey, John. The Public and Its Problems (New York: Henry Holt and Company, 1946).
2. Easton, David. A Systems Analysis of Political Life (New York: Wiley, 1965).
3. Randriamampianina, Mialisoa. Sécurité et Défense: Nouveaux Défis, Nouveaux Acteurs (Allemand: FRIEDRICH-EBERT-STIFTUNG, 2009).

Journal Articles (المقالات والمجلات العلمية)

1. Sébastian Roché, Sociologie politique de l'insécurité. Paris: Presses Universitaires de France, 1998, cité dans: Laurent Mucchielli, Revue française de sociologie, vol. 40, no. (1999)

Theses (الرسائل الجامعية)

1. Germain, Séverine. Les politiques locales de sécurité en France et en Italie: une comparaison des villes de Lyon, Grenoble, Bologne et Modène, thèse de doctorat en science politique (Grenoble: Université Pierre Mendès-France, Institut d'études politiques de Grenoble, novembre 2008).

Conferences (الملتقيات والمؤتمرات)

1. Bouriche, Riadh. Approches et conceptions des politiques publiques sécuritaires, (Forum international "Alger et sécurité en Méditerranée: réalité et perspectives", Université Mentouri Constantine: Faculté de droit et sciences politiques, 29 et 30 avril 2008).

Reports and Websites (التقارير والمواقع الإلكترونية)

1. Algeria Invest, report by cybersecurity company Kaspersky, 23/03/2025, Retrieved from: https://bit.ly/4tDW0qh
2. AlgeriaTech Editorial, Kaspersky's Africa Cyberthreat Landscape Report 2025 ,06/12/2025, accessed on: (03/01/2026), Retrieved from the following link: http://bit.ly/4duIxMD
3. Cybersecurity and Infrastructure Security Agency (CISA)." Critical Infrastructure Sectors," Retrieved from: https://tinyurl.com/3r968dt2
4. Giles, Keir. Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. London: Chatham House, 2016, Retrieved from: https://tinyurl.com/2vthc6wc
5. Kepios, "Digital Algeria," published by DataReportal, 08/nov/2025, Retrieved from: https://tinyurl.com/52nakvtc
6. StateGlobe, Identity Theft Rate Statistics in Algeria (2026), March-2026, Retrieved from: https://bit.ly/4tyyRp4

7. The Diplomat, "Xi Jinping Leads China's New Internet Security Group," February 28, 2014, Retrieved from: https://tinyurl.com/425dzxdw

ملخص الدراسة:

يعالج موضوع السياسة العامة الأمنية الجزائرية في ظل تنامي متغيرات الأمن السيبراني، عبر مقاربة تحليلية تسعى إلى تأصيل الإطار المفاهيمي لكل من الأمن القومي والسياسة العامة، مع إبراز التحولات التي عرفتها هذه المفاهيم في سياق التغيرات الدولية المتسارعة والتطور التكنولوجي المتنامي. وينطلق الطرح من إبراز الطبيعة المركبة لمفهوم السياسة العامة، من خلال تعدد المقاربات النظرية المفسرة له، لاسيما مقاربة النظم، ونظرية النخبة، والمقاربة المؤسساتية، بما يعكس تعقيد عملية صنع القرار الأمني وتداخل أبعادها السياسية والمؤسساتية والسلوكية. وفي هذا السياق، تُفهم السياسة العامة الأمنية بوصفها منظومة متكاملة من السياسات والاستراتيجيات والتدابير التنظيمية التي تعتمدها الدولة بهدف ضبط المجال الأمني، والتكيف مع مختلف التهديدات، سواء التقليدية منها أو المستجدة، بما يضمن استمرارية الاستقرار وحماية المصالح الحيوية.

وفي إطار التحولات الرقمية، يبرز الأمن السيبراني كأحد المرتكزات الأساسية للأمن الوطني المعاصر، حيث يُنظر إليه كمنظومة شاملة من الإجراءات التقنية والتنظيمية والبشرية الرامية إلى حماية الأنظمة المعلوماتية والبنى التحتية الرقمية، وضمان سرية البيانات وسلامتها وتوافرها، كما يتتبع الطرح التطور التاريخي لمفهوم الأمن السيبراني، مبرزًا ارتباطه بتصاعد وتيرة الهجمات الإلكترونية وتزايد الاعتماد على التكنولوجيات الحديثة في مختلف القطاعات الحيوية. إضافة إلى ذلك، يتم التأكيد على الطابع متعدد الأبعاد للأمن السيبراني، من خلال إبراز أبعاده العسكرية والاقتصادية والاجتماعية والقانونية والسياسية، وما تفرزه من تأثيرات مباشرة وغير مباشرة على استقرار الدولة وأمنها القومي. ويختتم التحليل بتسليط الضوء على محددات صنع السياسة العامة الأمنية في الجزائر، سواء الداخلية أو الخارجية، مع إبراز دور الفواعل الرسمية وغير الرسمية في توجيهها، وذلك في ظل بيئة رقمية ديناميكية تتسم بالتعقيد وتعدد مصادر التهديد.

الكلمات المفتاحية:

السياسة العامة، السياسة العامة الأمنية، الامن القومي، الامن السيبراني، التهديدات السيبرانية.

Abstract:
This study addresses Algerian public security policy in light of the growing dynamics of cybersecurity, through an analytical approach that seeks to establish a conceptual framework for both national security and public policy, while highlighting the transformations these concepts have undergone within the context of rapid international changes and accelerating technological development. It emphasizes the complex nature of public policy by examining various theoretical approaches, notably the systems approach, elite theory, and the institutional approach, reflecting the complexity of the security decision-making process and the interplay of its political, institutional, and behavioral dimensions. Within this framework, public security policy is understood as an integrated system of policies, strategies, and regulatory measures adopted by the state to manage the security domain and adapt to both traditional and emerging threats, ensuring stability and the protection of vital interests.
In the context of digital transformations, cybersecurity emerges as a fundamental pillar of contemporary national security. It is viewed as a comprehensive system of technical, organizational, and human measures aimed at protecting information systems and digital infrastructures, while ensuring the confidentiality, integrity, and availability of data. The study also traces the historical evolution of cybersecurity, highlighting its correlation with the increasing frequency of cyberattacks and the growing reliance on modern technologies across vital sectors. Furthermore, it underscores the multidimensional nature of cybersecurity by examining its military, economic, social, legal, and political dimensions, and their direct and indirect implications for state stability and national security. The analysis concludes by shedding light on the determinants of public security policy-making in Algeria, both internal and external, while emphasizing the role of formal and informal actors in shaping it within a dynamic and complex digital environment characterized by multiple sources of threat.
Keywords:
Public Policy, Security Public Policy, National Security, Cybersecurity, Cyber Threats.