



وزارة التعليم العالي والبحث العلمي

جامعة عباس لغرور - خنشلة -

كلية الحقوق والعلوم السياسية



قسم العلوم السياسية

الأمن السيبراني في الجزائر

دراسة السياسات والمؤسسات

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية
تخصص: دراسات استراتيجية وأمنية

إشراف الدكتورة:

- هاجر خلافة

إعداد الطالبة:

- لينا ندى بن زعيم

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الاصلية	الصفة
عبد الوهاب لوصيف	أستاذ محاضر - أ -	جامعة عباس لغرور خنشلة	رئيسا
هاجر خلافة	أستاذة محاضر - أ -	جامعة عباس لغرور خنشلة	مشرفا ومقررا
عزيز نوري	أستاذ محاضر - أ -	جامعة عباس لغرور خنشلة	عضوا ممتحنا

السنة الجامعية: 2025-2026



شكر وعرفان

بسم الله الرحمن الرحيم والحمد لله رب العالمين الذي بنعمته تتم الصالحات
والذي وفقني وأعانني على إتمام هذا العمل المتواضع.

أتقدم بأسمى عبارات الشكر والتقدير والعرفان إلى أستاذتي المشرفة خالفة
هاجر التي كان لها الفضل الكبير بعد الله تعالى في إنجاز هذه المذكرة فقد
كانت نعم الموجهة والمشرقة لم تبخل علي بتوجيهاتها العلمية الدقيقة ونصائحها
القيمة وملاحظاتها البناءة التي ساعدتني على تصحيح مسار العمل وتطويره في
كل مرحلة.

لقد كانت الأستاذة المشرفة خالفة هاجر مثالاً لأستاذة المخططة في عملها حيث
قدمت لي الدعم العلمي والمعنوي طوال فترة إعداد هذا البحث وكانت
حريصة على أن يظهر هذا العمل في أفضل صورة ممكنة من حيث المنهجية
والمضمون، كما أتقدم لها بجزيل الشكر والعرفان على صبرها وتفهمها
ومتابعاتها المستمرة.

أتقدم بالشكر والاحترام إلى أعضاء اللجنة مناقشة الكرام على قبولهم مناقشة
المذكرة وعلى ملاحظاتهم القيمة التي ستزيد من الجودة العلمية لهذه الدراسة.

ولا يغوتني أن أتقدم بالشكر إلى كافة أساتذة قسم العلوم السياسية الذين
ساهموا في تكويني العلمي والمعرفي طوال سنوات الدراسة.

وفي ختام أسأل الله عز وجل أن يجعل هذا العمل خالصاً لوجهه الكريم وأن ينفع به
كل من يطلع عليه.

الإهداء

الحمد لله حمداً كثيراً طيباً مباركاً فيه الذي وفقني وأعانني على إتمام هذا العمل وفتح لي أبواب العلم والمعرفة فله الحمد والشكر على نعمه التي لا تعد ولا تحصى.

إلى أمي وأبي مصدر الحب والعزاء وسر قوتي في هذه الحياة الذين لم يبخلوا علي يوماً بالدعم والتشجيع والدعاء الصادق وكانا دائماً السند الحقيقي لي في كل مراحل حياتي حفظهما الله وأدامهما تاجاً فوق رأسي.

إلى إخواني عزيزي ومجيد وأختي دعاء الذين كانوا لي الرفيق والداعم في مسيرتي الدراسية وفي حياتي وشاركوني لحظات التعب والنجاح وكان وجودهم مصدر طمأنينة وقوة لي.

إلى عائلتي الكريمة أعمامي وخالاتي الذين كان لهم أثر طيب وتشجيع مستمر في حياتي خاصة خالتي حبيبة التي وقفت بجانبتي في كل اللحظات وكانت أكبر داعمة لي.

إلى جدتي الغالية رحمها الله وأسكنها فسيح جناته التي تبقى ذكرها محفورة في قلبي ودعائها يرافقتني دائماً.

وإلى كل من ساندني ووقف إلى جانبي بكلمة طيبة أو دعاء صادق أو تشجيع لا ينسى.

أهدي هذا العمل لنفسي وإلى عائلتي وكل من دعمني في نجاحه.

حقائق

مقدمة:

يشهد العالم خلال العقود الأخيرة تحولات جذرية بفعل التطور التكنولوجي المتسارع، حيث أصبح التطور التكنولوجي اليوم عنصرا أساسيا في حياة الافراد والمؤسسات، مما أدى إلى بروز الفضاء السيبراني كمجال حيوي جديد تتداخل فيه الأبعاد الاقتصادية والسياسية والأمنية. حيث لم تعد التهديدات الأمنية مقتصرة على أشكالها التقليدية، بل امتدت لتشمل تهديدات سيبرانية حديثة معقدة تستهدف الأنظمة المعلوماتية والبنى التحتية الحيوية، الأمر الذي جعل من الأمن السيبراني قضية استراتيجية تحتل مكانة متقدمة ضمن أولويات الدول.

وفي ظل هذا التحول، سارعت مختلف الدول إلى تبني سياسات واستراتيجيات وطنية تهدف إلى تعزيز أمنها السيبراني، من خلال تطوير الأطر التشريعية والتنظيمية، وإنشاء مؤسسات متخصصة، إلى جانب الاستثمار في القدرات التقنية والبشرية لمواجهة المخاطر الرقمية المتزايدة. وقد أصبح نجاح هذه المقاربات مرتبطا بمدى تكامل عناصرها، خاصة ما يتعلق بالجانب القانوني والمؤسسي، باعتبارهما الأساس في بناء منظومة سيبرانية فعالة ومستدامة.

كما تسعى الجزائر على غرار باقي الدول، إلى مواكبة هذه التحولات من خلال العمل على إرساء منظومة وطنية للأمن السيبراني، تركز على جملة من القوانين والتشريعات، إضافة إلى إنشاء هياكل ومؤسسات معنية بحماية الفضاء الرقمي الوطني. غير أن فعالية هذه المنظومة تبقى محل تساؤل في ظل التحديات المتسارعة التي يفرضها التطور التكنولوجي، وكذا تزايد حدة التهديدات السيبرانية التي تستهدف مختلف القطاعات الحيوية.

2. أسباب إختيار الموضوع

هناك العديد من أسباب إختيار موضوع الأمن السيبراني في الجزائر نظرا لعدة اعتبارات علمية وموضوعية مرتبطة براهنيته وأهميته المتزايدة في ظل التحول الرقمي المتسارع وتنامي

التحديات السيبرانية، لذلك فاختيار هذا الموضوع جاء نتيجة عدة عوامل يتمثل أبرزها فيما يلي:

1. الأسباب الذاتية:

في الاهتمام الشخصي بدراسة قضايا الأمن السيبراني باعتباره مجالا حديثا وحيويا يرتبط بالأمن الوطني والتحول الرقمي، إضافة إلى الرغبة في التعمق في فهم التحديات السيبرانية وآليات مواجهتها في الجزائر.

2. الأسباب الموضوعية:

تتمثل الأسباب الموضوعية في أهمية موضوع الأمن السيبراني في الوقت الراهن، باعتباره أحد أبرز التحديات الأمنية المعاصرة، إضافة إلى تزايد الهجمات السيبرانية التي تستهدف المؤسسات الوطنية، وما يفرضه ذلك من ضرورة تحليل المنظومة التشريعية والمؤسسية في الجزائر وتقييم فعاليتها.

3. أهمية الموضوع

تزداد أهمية دراسة الأمن السيبراني في ظل التحول الرقمي المتسارع، حيث أصبح الفضاء السيبراني مجالا استراتيجيا تبرز فيه تهديدات أمنية جديدة تتجاوز الأشكال التقليدية كما تأتي أهمية هذا الموضوع من خلال تناوله لواقع المنظومة التشريعية والمؤسسية للأمن السيبراني في الجزائر، والسعي إلى تقييم مدى فعاليتها في مواجهة التهديدات الرقمية المتنامية، بما يسهم في فهم هذا المجال واقتراح سبل تطويره.

1. الأهمية العلمية:

تمثل أهمية العلمية لهذه الدراسة في تناولها لموضوع الأمن السيبراني كأحد القضايا الحديثة في الدراسات الأمنية والاستراتيجية، من خلال تقديم تأصيل نظري وتحليل للمنظومة

التشريعية والمؤسسية، بما يسهم في إثراء المعرفة الأكاديمية وفتح المجال لدراسات مستقبلية.

2. الأهمية العملية:

تكمن هذه الدراسة في تقييم منظومة الأمن السيبراني في الجزائر من خلال تحليل التشريعات والمؤسسات، بهدف تحديد مدى فعاليتها في مواجهة التهديدات، وتشخيص نقاط القوة والضعف واقتراح سبل تحسين الأداء.

4. الأهداف الدراسة

تهدف دراستنا للموضوع الى التعرف على مفهوم الامن السيبراني، كما تسعى إلى دراسة واقع المنظومة التشريعية والمؤسسية للأمن السيبراني في الجزائر وتقييم مدى فعاليتها في مواجهة التهديدات السيبرانية إلا أن هذا الهدف يتحقق تدريجيا من خلال أهداف التالية:

- تحديد مفهوم الأمن السيبراني وأبعاده المختلفة.
- تحليل الإطار النظري للأمن السيبراني في الدراسات الأمنية والاستراتيجية.
- دراسة واقع المنظومة التشريعية للأمن السيبراني في الجزائر.
- تقييم مدى فعالية السياسات والمؤسسات في مواجهة التهديدات السيبرانية.
- أبرز التحديات التي تواجه الأمن السيبراني في الجزائر.

5. إشكالية الدراسة

يشهد الفضاء السيبراني تطورا متسارعا جعل منه مجالا استراتيجيا يرتبط بالأمن القومي للدول، في ظل تزايد التهديدات السيبرانية التي تستهدف الأنظمة والبنى التحتية الحيوية حيث

سعت الجزائر إلى تطوير منظومة تشريعية ومؤسسية لمواجهة هذه التحديات، غير أن مدى فعاليتها يبقى محل دراسة.

مما تقدم، يمكن طرح سؤال المركزي التالي:

"كيف تساهم البنية المؤسسية التشريعية في بناء منظومة الأمن السيبراني في الجزائر ومادى فعاليتها؟

ينبثق عن هذه الإشكالية الرئيسية عدد من التساؤلات الفرعية أهمها:

• ما هو الإطار النظري الذي يوطر الأمن السيبراني في الدراسات الأمنية والاستراتيجية؟

• كيف تسهم المنظومة التشريعية والمؤسسية في مواجهة التهديدات السيبرانية في الجزائر؟

• إلى أي مدى تساهم هذه المنظومة في تحقيق الأمن السيبراني في الجزائر؟

• ما هي الآفاق المستقبلية لتطوير الأمن السيبراني في الجزائر؟

6. الفرضيات الدراسة

تنطلق الدراسة في فرضية رئيسية كإجابة مؤقتة على الإشكالية المطروحة.

1. بقدر ما تتعلق التحديات التقنية -البشرية -المؤسسية بالأمن السيبراني في الجزائر، فإن ذلك يفرض ضرورة تطوير السياسات والاستراتيجيات الوطنية في هذا المجال.

7 حدود الدراسة:

حدود الزمانية والمكانية:

البعد الجيو-سياسي: تتمحور الدراسة في حدودها المكانية على الجزائر كفاعل إقليمي محوري في القارة الإفريقية ومنطقة حوض البحر الأبيض المتوسط. ويرتبط هذا البعد بدراسة البيئة الجيو-سياسية الرقمية للجزائر، وكيفية حماية فضاءها السيبراني الوطني من التهديدات العابرة للحدود التي تستهدف سيادتها الرقمية وموقعها الاستراتيجي، لاسيما في ظل التحولات الإقليمية والدولية المتسارعة وتزايد حدة الاستقطاب السيبراني بين الفواعل الدولية .

البعد الاستراتيجي: تنحصر الدراسة في تحليل الاستراتيجية الوطنية للأمن السيبراني بالجزائر وبنيتها المؤسساتية والتشريعية، مع التركيز على كيفية توظيف القدرات السيادية لحماية البنى التحتية الحيوية (كالطاقة والاتصالات) ومواجهة التهديدات الرقمية الحديثة.

البعد القيمي: يتحدد بدراسة التوازن بين متطلبات الأمن الوطني السيبراني كقيمة عليا لحماية الدولة، وبين الحفاظ على الحقوق والحريات الرقمية (كحماية البيانات الشخصية والخصوصية المكفولة دستوريا)، وضبط السلوك الأخلاقي والقانوني داخل الفضاء الرقمي الجزائري.

8. منهجية الدراسة

تعد مناهج البحث العلمي الأدوات الأساسية التي يعتمد عليها الباحث لفهم الظواهر وتحليلها. نظرا للطبيعة الموضوع الامن السيبراني في الجزائر دراسة السياسات والمؤسسات، فقد تم الاعتماد على مجموعة من المناهج المتكاملة منها: المنهج دراسة حالة: تم اعتماده من خلال اختيار الجزائر كنموذج للدراسة، وتحليل منظومتها التشريعية والمؤسساتية في مجال الأمن السيبراني، نظرا لما نشهده من تحولات وتحديات.

- تقنية الاحصائي: تم استخدامه في تحليل المعطيات الكمية من خلال توظيف الجداول والرسوم البيانية (الأعمدة والدوائر) لتوضيح المؤشرات المتعلقة بالأمن السيبراني ودعم النتائج المتوصل إليها.
- الاقتراب القانوني والمؤسسي: تم استخدامها في تحليل الإطار التشريعي المنظم للأمن السيبراني، ودراسة دور المؤسسات والهيكل المكلفة بتأمين الفضاء السيبراني، وتقييم مدى فعاليتها في مواجهة التهديدات.

9. الدراسات السابقة

نقصد بها جميع البحوث والدراسات السابقة العلمية التي تتشابه مع البحث الراهن أو تقترب منه في جانب ما.

- دراسة قام بها سمير بارة بعنوان الدراسة "الأمن السيبراني في الجزائر: السياسات والمؤسسات"، تطرّف فيه تحليل السياسات العامة في الجزائر المتعلقة بالأمن السيبراني، ودور المؤسسات الأمنية والدفاعية في حماية الأنظمة المعلوماتية، مع إبراز التحديات المرتبطة بتزايد الجرائم الإلكترونية وضعف التنسيق بين الهيئات المعنية. ما تم إضافته في هذه الدراسة بتوسيع التحليل ليشمل البناء المؤسسي الكامل والتشريعات والسياسات معاً، إضافة إلى دراسة التحديات والآفاق المستقبلية بشكل أكثر شمولية وحداثة.

- دراسة قامت بها منى الأشقر جبور جاءت على شكل كتاب بعنوان "السيبرانية هاجس العصر"، تطرقت فيه الباحثة الى الدراسة موضوع الأمن السيبراني باعتباره أحد أبرز هواجس العصر في ظل التطور التكنولوجي المتسارع، حيث ركزت على التحولات التي أحدثها الفضاء السيبراني في مختلف المجالات، خاصة على مستوى الأمن القومي والعلاقات الدولية. كما أبرزت الدراسة تزايد التهديدات السيبرانية المرتبطة باستخدام تكنولوجيا المعلومات، وضرورة وضع أطر قانونية وتنظيمية لضبط هذا المجال، إلى

جانب التأكيد على أهمية التعاون الدولي والمؤسساتي لمواجهة المخاطر السيبراني. ما أضافته في دراستنا أن لا تقتصر على الطرح العام لمفهوم الأمن السيبراني، بل تركز بشكل دقيق على الحالة الجزائرية من خلال تحليل المنظومة التشريعية والمؤسساتية وتقييم مدى فعاليتها في مواجهة التهديدات السيبرانية.

- دراسة قام بها جمال بوازدية جاءت بعنوان "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية، تطرق فيها الباحث الى الدراسة تطور الفضاء السيبراني وتأثيره على الأمن القومي، حيث أبرزت أن التحولات التكنولوجية أدت إلى بروز الجرائم السيبرانية كتهديد جديد للدول. كما ركزت على الاستراتيجية الجزائرية في مواجهة هذه الجرائم، من خلال تبني سياسات أمنية تهدف إلى حماية الأنظمة المعلوماتية للمؤسسات والمواطنين، إلى جانب تعزيز آليات المراقبة والتعاون الدولي. كما أكدت الدراسة أن الجزائر تسعى إلى تطوير منظومة أمن سيبراني قادرة على التكيف مع التحديات الناتجة عن التطور التكنولوجي المتسارع. ماتم إضافته عن دراسة جمال بوازدية في كونها لا تركز فقط على الاستراتيجية العامة لمواجهة الجرائم السيبرانية، بل تتجه نحو تحليل معمق للمنظومة التشريعية والمؤسساتية في الجزائر وتقييم مدى فعاليتها، مع دراسة التحديات بشكل تفصيلي واستشراف آفاق تطوير الأمن السيبراني في إطار أكثر شمولاً.

10. صعوبات الدراسة

واجهت الدراسة جملة من الصعوبات المتمثلة في:

واجهنا صعوبة في الوصول لبعض المعلومات الدقيقة المتعلقة بالأمن السيبراني في الجزائر نظرا لطابعها الاستراتيجي والسري.

كما حال ضيق الوقت دون التوسع في دراستنا لمختلف القطاعات الحيوية، مما فرض لدينا التركيز على بعضها.

لاحظنا في دراستنا قلة الإحصائيات الشاملة والموحدة المتعلقة بحجم التهديدات في بعض القطاعات، والاكتفاء بما توفره التقارير الرسمية للمصالح الأمنية.

11. خطة الدراسة

للإحاطة بالموضوع بكل جوانبه ارتأينا تقسيم موضوع الدراسة الى فصلين فضلا عن مقدمة والخاتمة :

يتناول **الفصل الأول** الإطار المفاهيمي والنظري للأمن السيبراني، حيث تم التطرق إلى ماهية الأمن السيبراني من خلال تعريفه وأبعاده وأهدافه، ثم عرض الإطار النظري المرتبط به في حقل الدراسات الأمنية والاستراتيجية، إضافة إلى توظيف بعض النماذج التحليلية المفسرة لتطبيقه.

أما **الفصل الثاني** فقد خُصص لدراسة المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني، من خلال تحليل التشريعات والسياسات المعتمدة، والبناء المؤسسي والتنظيمي، وتقييم فعالية الأداء، إضافة إلى دراسة التحديات والتهديدات التي تواجه هذا المجال، وصولاً إلى استشراف الآفاق المستقبلية لتعزيز الأمن السيبراني في الجزائر.

المفصل الأول

الإطار المفاهيمي والنظري للدراسة

الفصل الأول: الإطار المفاهيمي والنظري للدراسة.

أدى التطور المتسارع في التكنولوجيا المعلومات الى بروز الفضاء السيبراني كبيئة أساسية للتفاعل المؤسسي والفردى، مصحوبا بظهور تهديدات رقمية تستهدف سلامة المعلومات وموثوقية النظم الرقمية. مما جعل الأمن السيبراني ضرورة أكاديمية وميدانية في الدراسات الأمنية واستراتيجية، باعتباره يشمل حماية البيانات والنظم المعلوماتية ويعكس قدرة المؤسسات على مواجهة المخاطر الرقمية والتعامل معها بشكل منهجي.

يتناول هذا الفصل الاطار المفاهيمي والنظري للأمن السيبراني، من خلال استعراض المفاهيم الأساسية، الأبعاد، الأهداف، وربطها بالنظريات والمقاربات المعتمدة في الدراسات الأمنية، مع التعرف على النماذج التحليلية التي تسهم في فهم ودراسة المنظومة السيبرانية.

وعليه ينقسم هذا الفصل الى:

- المبحث الأول: مفهوم الأمن السيبراني.
- المبحث الثاني: الاطار النظري للدراسة.
- المبحث الثالث: النماذج التحليلية مفسرة لتطبيق الأمن السيبراني.

المبحث الأول: مفهوم الأمن السيبراني.

مع التطور السريع لتكنولوجيات المعلومات والاتصال، أصبحت الفضاءات الرقمية جزءاً لا يتجزأ من البنى التحتية الحيوية للدول، مما جعلها عرضة لأنواع جديدة من التهديدات والمخاطر، وعليه سنوضح من خلال هذا المبحث مفهوم الأمن السيبراني، انطلاقاً من عرض أهم المفاهيم المرتبطة به (المطلب الأول)، ثم الانتقال الى دراسة الأهداف وأبعاده (المطلب الثاني)، على نحو يمكننا من بناء قاعدة معرفية جيدة لفهم أبعاد مختلفة للأمن السيبراني.

المطلب الأول: تعريف الأمن السيبراني والمفاهيم ذات الصلة.

يعد الأمن السيبراني من المفاهيم التي نالت اهتمام الباحثين وذلك لدوره الأساسي في حماية المعلومات من التهديدات الرقمية، وتعزيز أمن المؤسسات والأفراد، وقد تعددت التعاريف المحددة للأمن السيبراني، لذا سيتناول هذا المطلب عدداً من الفروع منها لتحديد تعريف الأمن السيبراني (الفرع الأول)، كما سنتطرق من خلال المطلب الى تطور الامن السيبراني (الفرع الثاني)، وبعض المفاهيم المرتبطة (الفرع الثالث).

الفرع الأول: تعريف الأمن السيبراني

أفرز التطور المتسارع لتكنولوجيات المعلومات والاتصال تحديات أمنية جديدة مست الفضاء الرقمي، وأصبح هذا الأخير مجالا حيويًا تتقاطع فيه المصالح السياسية والاقتصادية والأمنية للدول، ففي ظل تزايد التهديدات الرقمية والهجمات السيبرانية، برز مفهوم الأمن السيبراني كأحد الركائز الأساسية لحماية الدول والمؤسسات والأفراد، مما يستدعي الوقوف عند تعريفه.

أولاً: التعريف اللغوي والاصطلاحي

الأمن السيبراني يتكون من لفظتين: "الأمن"، "السيبرانية" وسيتم توضيح معناه من الناحيتين اللغوي والاصطلاحي، كما يلي:

• **الأمن لغة:** في اللغة العربية تدل كلمة الأمن على الطمأنينة وهو نقيض الخوف، أي بمعنى السلامة والأمن مصدر الفعل أمن أمناً وأماناً وأمانة أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه. (السمحان، 2020) كما جاء في قوله تعالى: "الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَآمَنَهُمْ مِنْ خَوْفٍ". سورة قريش

• **الأمن اصطلاحاً:** يعرف باري بوزان الأمن بأنه السعي الى التحرر من التهديد (freedom from threat)، سواء كان هذا التهديد موجهاً الى الدولة أو المجتمع أو الى الأفراد. (Buzan, People, States and Fear: An Agenda for International Security Studies in the Post–Cold War Era, 1991)

• **السيبرانية لغة:** هي مأخوذة من كلمة (سيبر cyber)، وتعني صفة ألي شيء مرتبط بثقافة الحواسيب أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الانترنت)، وهي كلمة مشتقة من لفظة يونانية (kybernetes)، بمعنى الشخص الذي يدير دفة السفينة أو ربان السفينة. وعليه يشير مصطلح (سيبر cyber)، كل ما يتعلق بالتكنولوجيا والفضاء الإلكتروني وتعني القيادة والتحكم. (عطية، 2019)

• **السيبرانية اصطلاحاً:** في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات (نوربرت وينر NORBERT WINTER)، وهو أستاذ الرياضيات في معهد ماساتشوستس التقني MIT الذي أعطاه مفهومها الاصطلاحي الحديث وكان ذلك عام 1948، وبالتالي فالمصدر الاصطلاحي الحديث لكلمة السيبرانية وهو «علم القيادة والتحكم في الاحياء والآلات ودراسة أليات التواصل». (عطية، 2019)

ثانياً: تعريف الأمن السيبراني

قد تعددت التعاريف حول مفهوم الأمن السيبراني، وكل حسب زاوية النظر لهذا النوع من الأمن حيث يعرفه بأنه: نشاط أو عملية وقدرة أو نظم معلومات أو اتصالات الدولة إذ تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المصرح به أو تعديل أو الاستغلال.

ويعرف أيضاً بأنه: حماية الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وهو مجال يركز على اتخاذ إجراءات ومقاييس ومعايير حماية لمواجهة التهديدات ومنعها أو على الأقل التقليل من آثارها.

وقد عرفه أيضاً المشرع الجزائري في نص المادة 2 من المرسوم التنفيذي رقم 05.20 المؤرخ في 25 جويلية 2020 المتعلق بالأمن السيبراني على أنه: " مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقام أحداث مرتبطة بالفضاء السيبراني، وشأنها أن تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلّة، من خدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه. وعليه يركز هذا تعريف مشرع الجزائري للأمن السيبراني على حماية نظم المعلومات من خلال التدابير التقنية والقانونية وضمان السرية والسلامة والتوافر، غير أنه يغفل التهديدات ذات الطابع العسكري. (المرسوم التنفيذي رقم 05/20، 30 جويلية 2020)

كما يعرف الأمن السيبراني: "هو مجموعة من الأدوات والسياسات والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، من الخاطر الحادثة بالمعلومات ومعالجته، والإجراءات والتدريب وأفضل الممارسات، ضمان التقنيات التي يمكن أن يستخدمها لحماية البيئة الالكترونية وتنظيم أصول المستخدم. كما يركز هذا التعريف على الجوانب التقنية

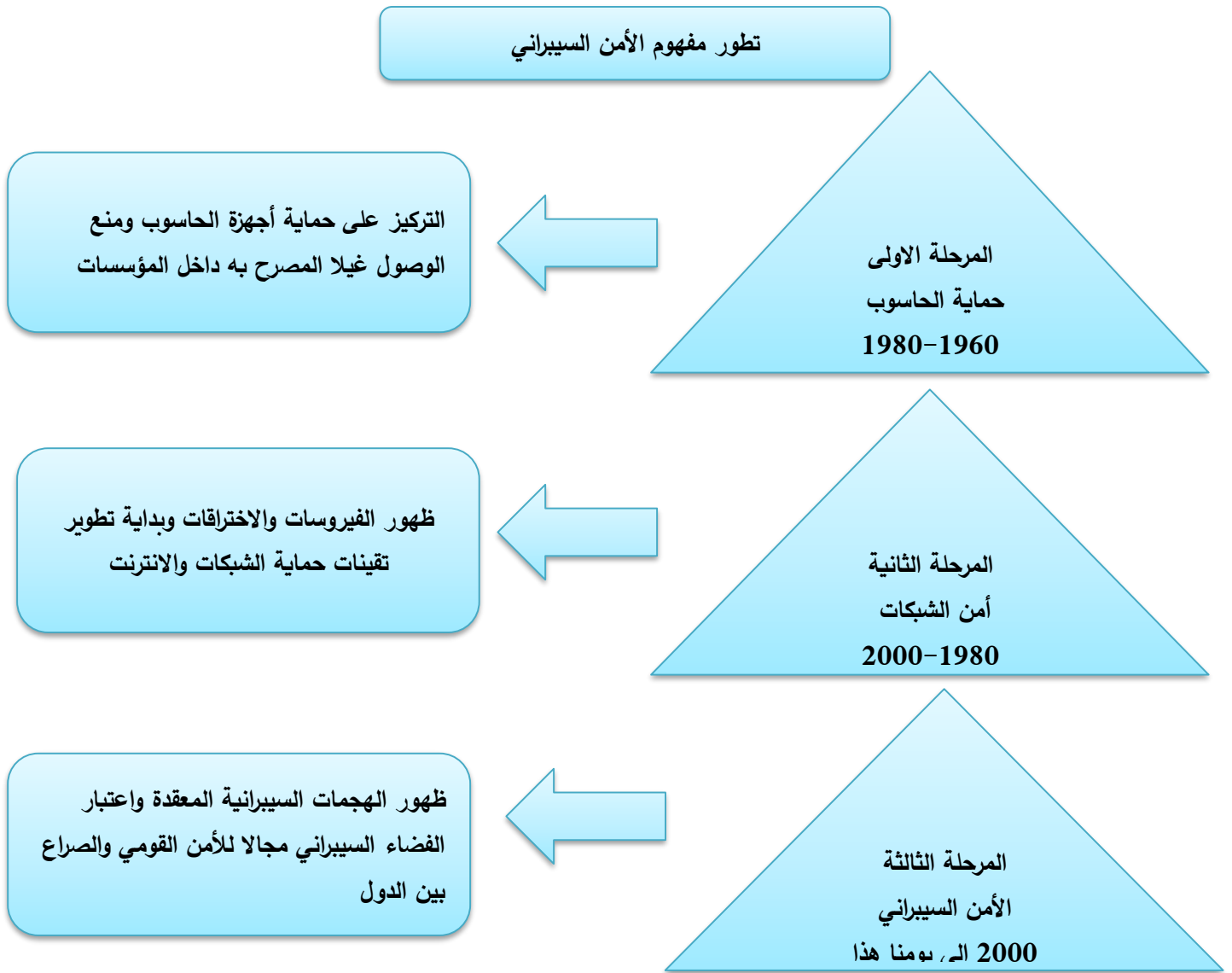
والتنظيمية للأمن السيبراني مع إغفال البعد الاستراتيجي وطبيعة التهديدات السيبرانية. (بارة، 2017)

ومن خلال هذه تعريف يمكن إعطاء تعريف إجرائي للأمن السيبراني: "هو مجموعة من الإجراءات التي تهتم بحماية الفضاء الرقمي من كل التهديدات والهجمات عبر منظومة من الأدوات والسياسات التي تضمن حفظ السرية المعلومات، وسلامتها وتوافرها واستمرارية عمل الأنظمة".

الفرع الثاني: تطور الأمن السيبراني

يوضح هذا المخطط تطور مفهوم الأمن السيبراني عبر عدة مراحل مرتبطة بتطور تكنولوجيا المعلومات والاتصال، فقد ظهر في البداية مفهوم الأمن المعلوماتي الذي ركز على حماية البيانات والمعلومات داخل الأنظمة الحاسوبية من الوصول غير المصرح به أو التلاعب بها. ومع انتشار شبكة الإنترنت وتطور أنظمة الاتصال ظهر مفهوم أمن الشبكات الذي يهتم بحماية الشبكات المعلوماتية من الهجمات الإلكترونية والاختراقات المختلفة. ومع ازدياد الاعتماد على الفضاء الرقمي في مختلف المجالات، برز مفهوم الأمن السيبراني الذي يتجاوز حماية المعلومات والشبكات ليشمل حماية البنية التحتية الرقمية والأنظمة الحيوية للدول. وفي مرحلة لاحقة توسع المفهوم ليشمل ما يعرف بـ الأمن الرقمي الشامل الذي يهتم بحماية البيئة الرقمية بكل مكوناتها، بما في ذلك الأفراد والمؤسسات والأنظمة الرقمية المختلفة.

الشكل رقم 1: تطور الأمن السيبراني



المصدر: من إعداد الطلبة استنادا على: (Keohane & Nye, 2014, p. 24)،

(Moravcsik, 1997, pp. 513-553)، (Nye, 2011)، (Pfleege & Pfleege, 2015, p. 12)، (Stallings, 2019, p. 7)، (Luibecki, 2009, p. 7)

الفرع الثالث: المفاهيم ذات صلة بالأمن السيبراني.

1. الفضاء السيبراني cyberspace:

هو بيئة إلكترونية غير ملموسة معقدة التفاعل يتم فيها بناء نماذج لظواهر أو صورة إلكترونية لظواهر شبه حقيقية في التفاعلات والتعاملات البعيدة فالسيرة عملية انعكاسية نشطة يعكس فيها مدخلات التفاعلات الالكترونية في بيئة لا يستطيع الانسان إدراكها، بصورة أخرى وهي عبارة عن شبكة إلكترونية لمجموعة من الخوادم الالكترونية حيث تتفاعل هذه الشبكات التي تتوفر فيها قاعدة بيانات فيما بينها باستخدام وسيلة تواصل افتراضية متجاوزة كل الحواجز الجغرافية والسياسية، سعياً وراء تحسين قدرة الاتصال والتعامل الالكتروني، كما أنها محاكاة حاسوبية عادة ما تكون في صورة بيئة افتراضية لمستخدمي العالم الافتراضي. (علي ز.، 2020)

وفقاً لوزارة الدفاع الأمريكية، يعرف بأنه: " مجال عالمي داخل بيئة المعلومات يتكون من شبكات معلومات البنية التحتية لتكنولوجيا المعلومات المترابطة، بما في ذلك الانترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر، ومعالجات والضوابط المدمجة. (Mbanaso & Dandaura, 2015)

2. الجريمة السيبرانية cybercrime:

تتكون الجريمة الالكترونية أو الافتراضية " cyber crime " من مقطعين هما الجريمة " crime " و "cyber" أي الالكترونية، ويستخدم مصطلح الالكترونية لوصف فكرة جزء من الحاسب أو للإشارة الى عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة عن القانون، والجرائم الالكترونية: هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد يدافع الجريمة ويقصد إيذاء سمعة الضحية أو إلحاق أي أذى مادي أو عقلي للضحية

سواء كان مباشر أو غير مباشرة، باستخدام شبكات الاتصالات مثل الانترنت غرق الدردشة والبريد الالكتروني. (بن عزوز و هناني، 2022)

3.الهجمات السيبرانية Attacks cyber:

هي أي عمل يستهدف إضعاف قدرات ووظائف شبكة الكمبيوتر لتحقيق الغايات شخصية أو السياسية يتم ذلك عبر استغلال نقاط الضعف في النظام، مما يمكن المهاجم من تلاعب به أو تعطيله. (شلوش، 2018)

4.التحديات السيبرانية cyber threats:

التحديات السيبرانية تمثل المحاولات أو أنشطة ضارة تهدف الى اختراق أو تعطيل أو إتلاف أنظمة المعلومات، أو الوصول غير المصرح به الى البيانات الحساسة، مما يستدعي اتخاذ تدابير أمنية لحماية الأفراد والمؤسسات من الاضرار الرقمية المحتملة. (Saeed & Renas, 2022)

5.الردع السيبراني Deterrence cyber:

يعرف بأنه منع الأعمال الضارة التي تستهدف الأصول الوطنية في الفضاء الرقمي أو الأصول المرتبطة بالعمليات الفضائية، وذلك من خلال اتخاذ إجراءات استباقية ووقائية لحماية البنية التحتية السيبرانية. (إسلام و جمعة، 2022)

6.الأمن المعلوماتي Information security:

حسب اللجنة الوطنية لأنظمة أمن الاتصالات والمعلومات (NSTISSC)، يعرف الأمن المعلومات على أنه: يعني حماية البيانات وأنظمة المعلومات من الوصول أو الاستخدام أو الكشف أو التعديل أو الاتلاف غير المصرح به، وذلك للحفاظ على قيمتها بالنسبة للمؤسسة. ويدفع على أمن المعلومات. (Surwade & Hitendra, 2024)

7. الإرهاب السيبراني Cyber Terrorisme:

يشير إلى الهجمات الإلكترونية تهدف إلى تهديد الحكومات أو العدوان عليها لتحقيق أهداف سياسية أو دينية أو إيديولوجية، يجب أن يكون لهذه الهجمات آثار مدمرة أو تخريبية تعادل الأفعال المادية للإرهاب التقليدي. (كمال، 2022)

8. الذكاء الاصطناعي Artificial intelligence:

يعرف الذكاء الاصطناعي بأنه مجال علمي وتقني يهدف إلى تطوير الأنظمة الحاسوبية القادرة على محاكاة بعض القدرات الذهنية البشرية، مثل التعلم، والتحليل، الاستدلال، واتخاذ القرار، اعتماداً على الخوارزميات ومعالجة البيانات. وقد اكتسب الذكاء الاصطناعي أهمية متزايدة في المجال الأمني، لكونه أداة فعالة في تحليل المخاطر ودعم اتخاذ القرار، خاصة في مجال الأمن السيبراني، حيث يساهم في الكشف المبكر عن التهديدات وتعزيز القدرات الوقائية للدول. (علي، 2019)

المطلب الثاني: أبعاد وأهداف الأمن السيبراني.

يعد الأمن السيبراني من المفاهيم الشاملة التي لا تقتصر على الجانب التقني فقط، بل تمتد لتشمل أبعاداً متعددة تتداخل فيها جوانب العسكرية، الاقتصادية، سياسية، قانونية، إلى جانب بعدها الاستراتيجي. ويهدف الأمن السيبراني من خلال هذه الأبعاد إلى حماية الفضاء الرقمي وضمان أمن المعلومات.

الفرع الأول: أبعاد الأمن السيبراني.

يتسم الأمن السيبراني بطابع شامل ومتعدد الأبعاد، إذ لا يقتصر على الجوانب التقنية فحسب، بل يمتد ليشمل أبعاداً قانونية، عسكرية، سياسية، اجتماعية، اقتصادية واستراتيجية تتكامل فيما بينها لضمان حماية فعالة للفضاء الرقمي.

• البعد العسكري

تكمّن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، مما يسمح بسهولة تبادل المعلومات وتدفقها وكذا السرعة في إعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد ينسب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم التجسس على الأمن العسكري للدول وتعطيل قدرة الدولة على النشر السريع لقواتها وقدراتها أو قطع أنظمة الاقتصاد فيما بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجه الإلكتروني فضلا عن إمكانية وفقدان السيطرة على وحدات القيادة. (عطية، 2019)

• البعد السياسي

يشكل الأمن السيبراني حجر الأساس في الحياة السياسية، حيث أصبح أداة إستراتيجية تؤثر على أمن واستقرار الدول، فهناك العديد من الأمثلة التي تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا على المستوى الدولي، كما أنه لا ينكر الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي. (جيلاني، 2023)

ومن هذا المنطلق، يتضح أن تجسيد الأمن السيبراني كوسيلة فعالة لحماية المعلومات والوثائق الحساسة التي ترتبط بعمل مؤسسات الدولة بات ضرورة ملحة، إذ إن غياب هذا الأمن قد يؤدي إلى نشوء خلافات دبلوماسية بين الدول قد تصل إلى مرحلة النزاعات، وقد شهدت العلاقات الدولية في السنوات الأخيرة تجليات واضحة لهذا الخطر من أبرزها الحرب

الروسية الأوكرانية عام 2022 والتي بدأت بهجمات استهدفت البنى التحتية الحيوية قبل أن تتصاعد الى حرب فعلية مدمرة.

• البعد الاقتصادي

إن الغرض من أمن المعلومات ليس كسب المال، بل حماية الموارد الاقتصادية وتجنب ضياعها أو فقدانها، فتحديد الفوائد المستمدة من المعلومات ليس بالأمر السهل، كما أن تقدير تكلفة الأمن المتمثلة في السمات المرصودة وتكلفة المنتجات الأمنية والتدريب وبناء مراكز التحكم وغيرها من الأمور ذات الصلة أمر صعب للغاية. إن حساب تكلفة أمن المعلومات والخسائر الناجمة عن الأخطاء والأفعال الضارة أمر صعب للغاية، حيث يتم تحديد هذه التكاليف حسب احتياجات المنظمة.

ويرجع ذلك إلى أنه لا يمكن تحديد التكاليف من حيث الأصول التي يتم العمل عليها والتي تحتاج إلى حماية، والأضرار الناجمة عن عدم كفاية الأمن والتعرض المحتمل للهجمات والاختراقات. (العوادي، 2016)

• البعد الاجتماعي

من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل المشاركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة وعُرفت ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول من الضرورة بمكان لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.

وينبغي التشديد على واجب الأمن، والمسؤولية الفردية والتدابير الرادعة، وكذلك التداعيات المحتملة -في إطار القانون الجنائي- التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن، وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات

المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة. إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات.

ينبغي جعل الشبكة الدولية للمعلومات شعاعا مفتوحا للجميع بحيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية زائدة ويحتاج الأمر إلى بلورة مدونة أخلاقيات الأمن، تكون مقبولة ومحترمة من جانب جميع العاملين في الفضاء السيبراني. (جبور، 2017)

البعد القانوني

تتشابك الأبعاد القانونية للأمن السيبراني مع التطور التكنولوجي في علاقة تبادلية، حيث يمثل القانون أداة لضبط المجتمع عن طريق مجموعة القوانين والأوامر، وطبيعي أيضا أن يحمل نفس الوظيفة فيما يتعلق بالفضاء السيبراني، فالجريمة على المستوى الافتراضي تفنقر للصرامة وعليه، باي من الواجب على الدول تكريس منظومة قانونية لتنظيم نشاط الفواعل على مستوى البيئة الافتراضية. (جيلاني، 2023)

لقد أصبح حق النفاذ الى هذه البيئة وما يترتب عنها من حقوق المستحدثة كحق إنشاء المدونات الإلكترونية، الحق في حماية البرامج الإلكترونية من التحديات التي تنتظر التشريع للاجتهاد بخصوصها وإثرائها.

الفرع الثاني: أهداف الأمن السيبراني.

حدد مركز بلفر مجموعة من الأهداف وهي سبعة التي تضطلع بها الدولة، وتتمثل في:

1. مسح ومراقبة المجموعات المحلية من خلال قيام الدولة، من منطلق حماية أمنها القومي بالمراقبة الإلكترونية لرصد واكتشاف وجمع المعلومات الاستخبارية عن التهديدات المحلية والجهات الفاعلة داخل حدودها.

2. تقوية وتعزيز الدفاعات السيبرانية الوطنية: أي تعزيز الدولة ودفاعاتها الوطنية لحماية عن الأصول والأنظمة الحكومية والوطنية، وتحسين السيبرانية الوطنية والنظافة والمرونة.
3. التحكم في بيئة المعلومات ومعالجتها: أي ازدواجية ضوابط المعلومات، وتحكم الدول في المعلومات عبر استخدام الوسائل الإلكترونية وتغيير الروايات في الداخل والخارج وحاولت حماية خصوصية الإنترنت وحرية التعبير لمواطنيها.
4. جمع المعلومات الاستخبارية من دول أخرى لحماية الأمن القومي: من خلال قيام دولة ما بانتزاع أسراراً وطنية من خصم أجنبي كالمعلومات السرية عن الاتفاقيات، والخطط العسكرية السرية والسرقة الملفات والوصول الى اتصالات كبار الشخصيات الحكومية مثل أعضاء البرلمان.
5. تحقيق المكاسب تجارية أو تعزيز نمو الصناعة المحلية، فيمكن للدولة من خلال نشاطها السيبراني تنمية صناعة التكنولوجيا المحلية الخاصة بدولة ما أو استخدام الوسائل التكنولوجية لتطوير صناعات محلية أخرى، عبر وسائل قانونية مشروعة او غير مشروعة كالتجسس الصناعي ضد الشركات الأجنبية لتيسير نقل التكنولوجيا.
6. تعطيل البنية للخصم وقدراته كاستخدام دولة ما تقنيات وتكتيكات وإجراءات إلكترونية مدمرة، لردع أو تآكل أو إضعاف قدرة الخصم على القتال في المجالات الإلكترونية أو التقليدية.
7. تحديد القواعد والمعايير التقنية الإلكترونية الدولية، أي مشاركة الدولة بنشاط في المناقشات القانونية والسياسية والفنية الدولية حول المعايير الإلكترونية.

وعليه بعد دراستنا لهذه الأهداف نجد أنها تتلخص في كالاتي:

يتمثل أهداف الأمن السيبراني في النقاط كالاتي: (للقاني، 2023)

1. حماية أنظمة التقنيات التشغيلية بمختلف مكوناتها، من أجهزة وبرمجيات وخدمات وبيانات، مع سد الثغرات الأمنية والقضاء على نقاط الضعف في الحواسيب والأجهزة المحمولة.
 2. التصدي للهجمات الإلكترونية التي تستهدف المؤسسات الحكومية والقطاعين العام والخاص، وتعزيز قدرة البنى التحتية الحساسة على الصمود أمامها.
 3. مكافحة البرمجيات الخبيثة والتهديدات السيبرانية الى إلحاق الضرر بالمستخدمين أو سرقة بياناتهم، واتخاذ التدابير اللازمة لحماية الأفراد والمستهلكين أثناء استخدام الانترنت.
 4. تعزيز الوعي والتدريب من خلال تزويد الأفراد بآليات وإجراءات فعالة لحماية أجهزتهم ومعلوماتهم الشخصية من الاختراق أو التلف.
- ويمكن القول من خلال هذه الأهداف أن الأمن السيبراني يهدف الحماية الأنظمة والبيانات، وسلامتها، والتصدي للهجمات الإلكترونية، وتوفير بيئة رقمية آمنة، مع تعزيز خصوصية البيانات والوعي، والتدابير الوقائية لمواجهة التهديدات السيبرانية.

المبحث الثاني: الإطار النظري للدراسة.

يعد الأمن السيبراني من القضايا الأمنية الحديثة التي فرضها التطور التكنولوجي المتسارع، مما استدعى مقاربات نظرية جديدة لفهم أبعاده وانعكاساته على أمن الدول. وانطلاقاً من ذلك، يسعى هذا المبحث إلى تناول الأمن السيبراني من منظور نظري، من خلال تحليل إسهامات بعض نظريات والمدارس الفكرية في فهم المجال الأمني المستجد.

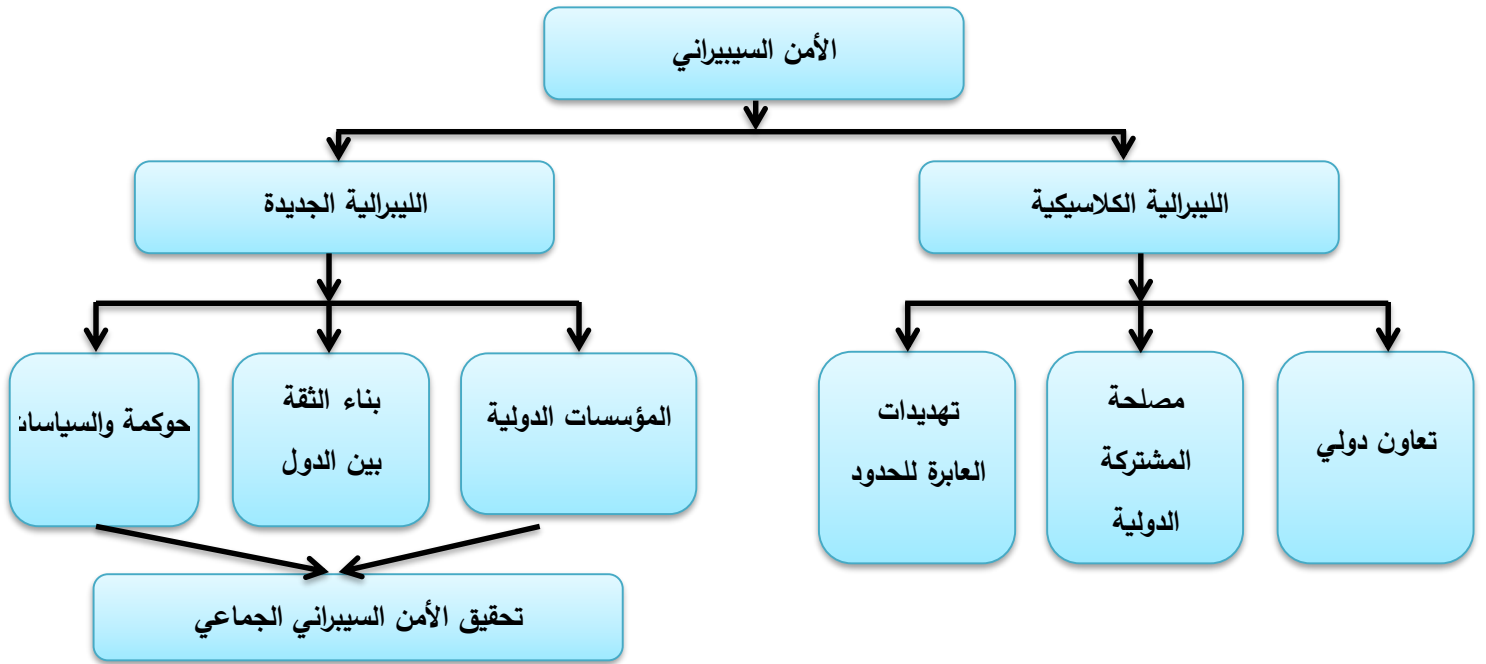
المطلب الأول: الأمن السيبراني من منظورات العلاقات الدولية.

تنطلق النظريات العلاقات الدولية من افتراضات مختلفة في تفسير طبيعة الأمن والتهديدات التي تواجه الدول في النظام الدولي، ومع بروز الفضاء السيبراني كحقل جديد للصراع والتفاعل الدولي، وعليه يتناول هذا المطلب مقارنة الأمن السيبراني من منظور العلاقات الدولية، من خلال إبراز كيفية تفسير بعض النظريات الكبرى، لطبيعة التهديدات السيبرانية وآليات التعامل معها على المستويين الوطني والدولي.

الفرع الأول: الأمن السيبراني من منظور الليبرالية الكلاسيكية والجديدة.

يعد الفكر الليبرالي من أهم المقاربات النظرية في حقل العلاقات الدولية، حيث يركز على دور التعاون بين الدول وأهمية المؤسسات الدولية في تنظيم العلاقات الدولية والحد من الصراعات. وفي ظل التحولات التي يشهدها النظام الدولي وظهور تهديدات جديدة في الفضاء السيبراني، أصبح من ضروري توظيف المنظور الليبرالي لفهم طبيعة التفاعلات الدولية في هذا المجال. وعليه سيتم في هذا الفرع التطرق إلى تفسير الأمن السيبراني منظور الليبرالية الكلاسيكية والجديدة.

الشكل رقم 2: مخطط الأمن السيبراني من منظور الليبرالية الكلاسيكية والجديدة



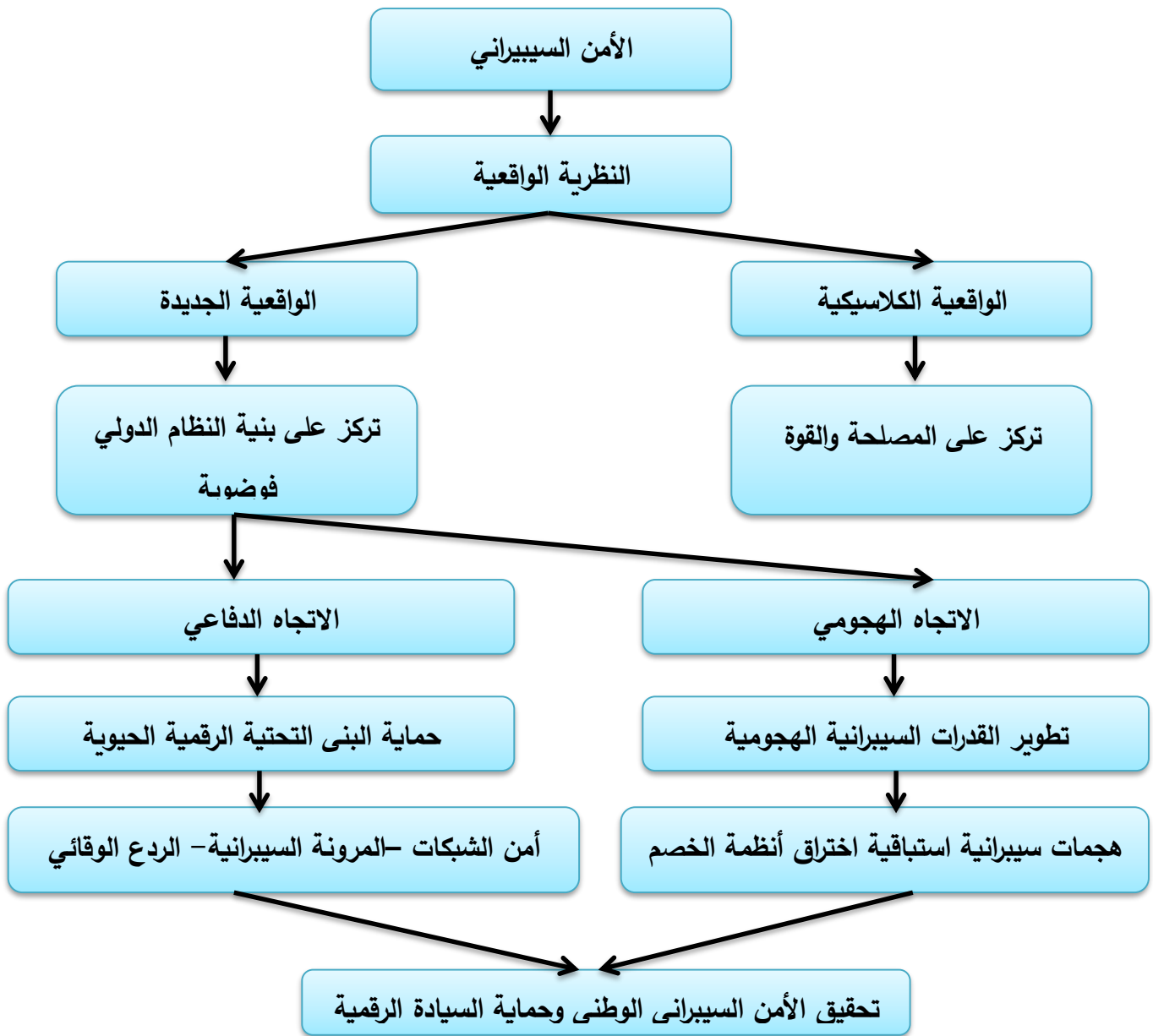
المصدر: من إعداد الطالبة بالاعتماد على (Keohane & Nye, 2014)، (Moravcsik, 1997)، (Nye, 2011)

يوضح هذا المخطط تفسير النظرية الليبرالية للأمن السيبراني من خلال اتجاهين رئيسيين هما الليبرالية الكلاسيكية والليبرالية الجديدة. حيث تؤكد الليبرالية الكلاسيكية على أهمية التعاون بين الدول وحرية تبادل المعلومات كوسيلة للحد من الصراعات وتعزيز الاستقرار الدولي. أما الليبرالية الجديدة تركز على دور المؤسسات الدولية في تنظيم العلاقات بين الدول ووضع قواعد مشتركة لإدارة الفضاء السيبراني. ومن هذا منطلق ينظر إلى الأمن السيبراني باعتباره مجالاً يتطلب تعزيز التعاون الدولي وتطوير أطر تنظيمية مشتركة لمواجهة التهديدات السيبرانية.

الفرع الثاني: الأمن السيبراني من منظور الواقعية الكلاسيكية والجديدة.

تشكل الواقعية أحد أبرز الاتجاهات النظرية في العلاقات الدولية، حيث تركز على مركزية الدولة وطبيعة الصراع في النظام الدولي الذي يتسم بالفوضى وغياب السلطة مركزية. وترى هذه المقاربة أن الدول تسعى باستمرار إلى تعزيز قوتها وقدراتها لضمان أمنها القومي.

الشكل رقم 3: مخطط الأمن السيبراني من منظور الواقعية الكلاسيكية والجديدة



المصدر: من إعداد الطالبة بالاعتماد على (Morgenthau, 2006, p. 102)، (Waltz, 1979)،
(Mearsheimer, 2001, p. 29)، (Nye, 2011, p. 113)

ومواجهة مختلف التهديدات، وفي ظل التحولات التكنولوجية وظهور الفضاء السيبراني كمجال جديد للتنافس بين الدول، أصبح من الممكن توظيف مقاربة الواقعية لفهم طبيعة الصراعات السيبرانية وكيفية سعي الدول لحماية مصالحها الاستراتيجية.

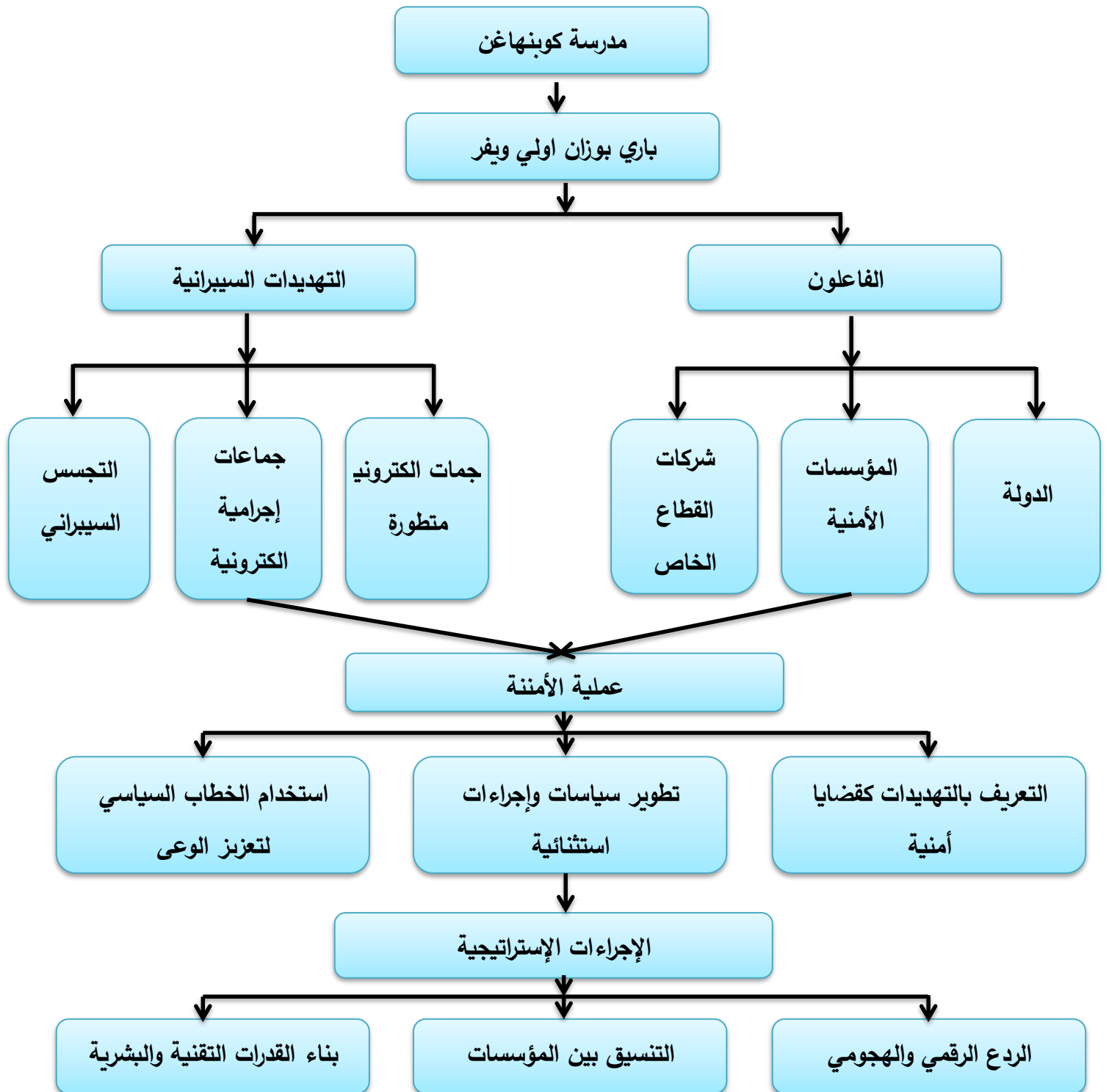
يبين هذا المخطط أن النظرية الواقعية، بشقيها الكلاسيكي والجديد، تنظر إلى الأمن السيبراني باعتباره امتداداً لمنطق القوة والصراع في النظام الدولي الفوضوي. ففي حين تركز الواقعية الكلاسيكية على حماية المصلحة الوطنية وتعظيم القوة، تؤكد الواقعية الجديدة على تأثير بنية النظام الدولي في سلوك الدول.

وضمن هذا الاتجاه تنقسم الواقعية الجديدة إلى اتجاهين في التعامل مع الأمن السيبراني اتجاه دفاعي يركز على حماية البنى التحتية وتحقيق الردع الوقائي، واتجاه هجومي يسعى إلى تطوير القدرات السيبرانية الهجومية واستخدامها كأداة ردع واستباق ضد الخصوم، بهدف حماية السيادة الرقمية وتحقيق الأمن السيبراني الوطني.

الفرع الثالث: الأمن السيبراني من منظور كوبنهاغن

تعد مدرسة كوبنهاغن من أبرز المقاربات المعاصرة في الدراسات الأمنية، حيث قدمت تصوراً موسعاً لمفهوم الأمن من خلال التركيز على عملية الأمنة التي يتم من خلالها تحويل بعض القضايا إلى قضايا أمنية تستدعي اتخاذ إجراءات استثنائية. وعليه يمكن توظيف مقاربة مدرسة كوبنهاغن لفهم كيفية تعامل مع التهديدات الناشئة في الفضاء السيبراني، من خلال اعتبارها تهديدات أمنية تستوجب تبني سياسات واستراتيجيات خاصة لمواجهتها.

الشكل رقم 4: الأمن السيبراني من منظور مدرسة كوبنهاغن



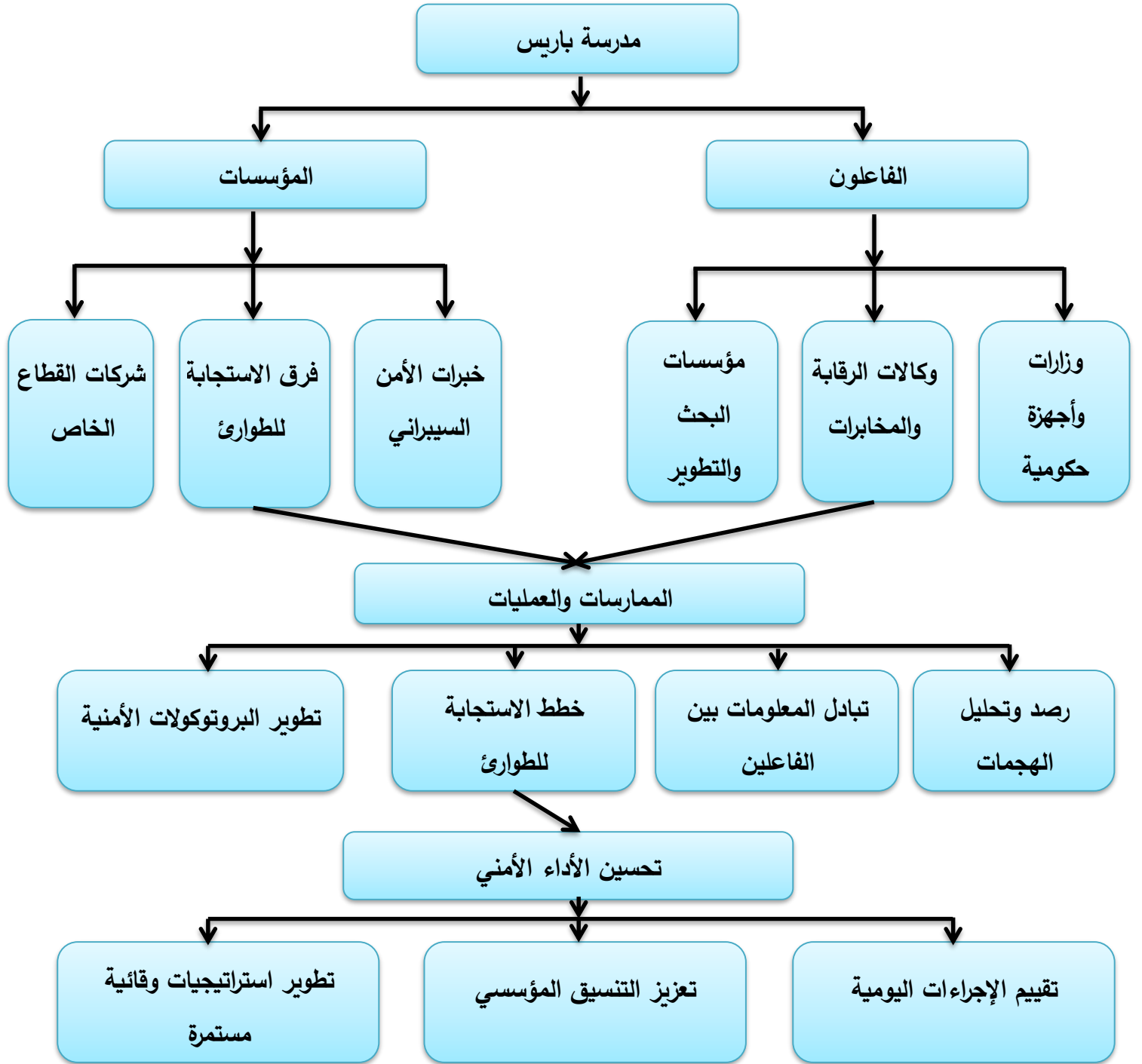
المصدر: من اعداد الطالبة بالاعتماد على (Buzan, 1991, p. 116)، (Buzan & al, 1998, p. 23)

يوضح هذا المخطط تفسير مدرسة كوبنهاغن للأمن السيبراني من خلال مفهوم الأمانة، حيث يتم تحويل بعض القضايا إلى تهديدات أمنية تتطلب اتخاذ إجراءات استثنائية. وفي هذا الإطار يمكن اعتبار الهجمات السيبرانية تهديداً للأمن القومي عندما تقوم الدولة أو الفاعلون الأمنيون بتقديمها على أنها خطر يستوجب استجابة خاصة. وبالتالي يتم تبني سياسات واستراتيجيات أمنية لحماية البنية التحتية الرقمية ومواجهة التهديدات السيبرانية.

الفرع الرابع: مدرسة باريس في منظور الأمن السيبراني.

تركز مدرسة باريس في الدراسات الأمنية على توسيع مفهوم الأمن ليشمل قضايا اجتماعية وسياسية متعددة، بعيداً عن التركيز التقليدي على الأمن العسكري فقط. وتؤكد هذه المدرسة على أن التهديدات لا تقتصر على الدول، بل يمكن أن تنشأ من جماعات غير الحكومية أو من أبعاد اقتصادية واجتماعية، بما في ذلك لفضاء السيبراني. ومن هذا المنطلق، توفر مدرسة باريس إطاراً تحليلياً لفهم كيفية تفسير الأمن السيبراني كقضية متعددة الأبعاد تتطلب استراتيجيات شاملة للتعامل مع التهديدات الرقمية وحماية الأنظمة والمؤسسات.

الشكل رقم 5: الامن السيبراني من منظور مدرسة باريس



المصدر: من اعداد الطالبة بالاعتماد على (Tsoukala ،(Bigo, 2002, pp. 63–92
& Bigo, 2008, p. 45)

يوضح هذا المخطط مقارنة مدرسة باريس في تفسير الأمن السيبراني من خلال التركيز على تعددية الفاعلين والممارسات الأمنية التي تشارك في إدارة التهديدات المعاصرة. فبدل حصر الأمن في البعد العسكري أو في دور الدولة فقط، تؤكد هذه المدرسة على أن إنتاج الأمن يتم عبر شبكة من المؤسسات والجهات المختلفة، مثل الأجهزة الأمنية والهيئات الحكومية والفاعلين غير الحكوميين. وفي هذا الإطار ينظر إلى الفضاء السيبراني باعتباره مجالاً تتقاطع فيه أبعاد سياسية واقتصادية وتقنية متعددة، الأمر الذي يستدعي اعتماد ممارسات أمنية متنوعة تقوم على التنسيق المؤسسي وتبادل المعلومات. ومن ثم فإن تعزيز الأمن غيرالسيبراني وفق هذا المنظور يعتمد على تطوير السياسات واستراتيجيات الوقائية وتكامل جهود مختلف الفاعلين من أجل إدارة المخاطر الرقمية وحماية البنية التحتية المعلوماتية.

المطلب الثاني: موقع الأمن السيبراني ضمن نظريات الفكر الاستراتيجي.

يحتل الفكر الاستراتيجي مكانة مهمة في تحليل القضايا الأمنية المعاصرة، حيث يهتم بدراسة كيفية توظيف الموارد والإمكانات المتاحة لتحقيق الأمن وحماية المصالح الحيوية للدول. ومع بروز الفضاء السيبراني كأحد مجالات التفاعل والصراع في العلاقات الدولية، أصبح الأمن السيبراني جزءاً أساسياً من التفكير الاستراتيجي للدول التي تسعى إلى تطوير استراتيجيات وسياسات تهدف إلى مواجهة التهديدات السيبرانية وتعزيز حماية البنية التحتية الرقمية.

الفرع الأول: الاستراتيجية وأبعادها في الدراسات الأمنية والفكر الاستراتيجي.

أولاً: تعريف الاستراتيجية

الاستراتيجية يعني في الأصل فن القيادة (Art of Generalship) فإن استخداماته المعاصرة قد تعددت وشملت العديد من الميادين. فقد يوصف موقع ما أو جزء من دولة بأنه "استراتيجي" (البحر الأبيض المتوسط، قناة السويس)، ويوصف قرار سياسي أو اقتصادي هام بأنه "استراتيجي" كما يطلق وصف "استراتيجي" على بعض أنظمة الأسلحة التي لها تأثيراً

حاسماً على معبر الحرب وقد يوصف نمط من التفكير أو الدراسات المتخصصة بأنه "تفكير الاستراتيجي" أو "الدراسات الاستراتيجية". (طلاس، 2011)

ثانياً: العلاقة بين الاستراتيجية والدراسات الأمنية

ترتبط الاستراتيجية بالدراسات الأمنية ارتباطاً وثيقاً، إذ تهدف الدراسات الأمنية إلى تحليل طبيعة التهديدات وإدارة المخاطر، بينما توفر الاستراتيجية الإطار العملي لتحديد الوسائل والآليات المناسبة لمواجهتها. ومع ظهور التهديدات السيبرانية، أصبح من الضروري دمج البعد الرقمي ضمن التفكير الاستراتيجي. (Buzan, 1991, p. 27)

ثالثاً: الفكر الاستراتيجي

يشير الفكر الاستراتيجي إلى مجموعة التصورات والمقاربات النظرية التي تهدف إلى فهم البيئة الأمنية وتطوير الاستراتيجيات فعالة لمواجهة التهديدات المعاصرة. وفي ظل التحديات الرقمية المتزايدة، يعد الأمن السيبراني جزءاً أساسياً من هذا التفكير. (Luttwak, 2001, p. 4)

الفرع الثاني: مخطط لنظريات الفكر الاستراتيجي في الأمن السيبراني

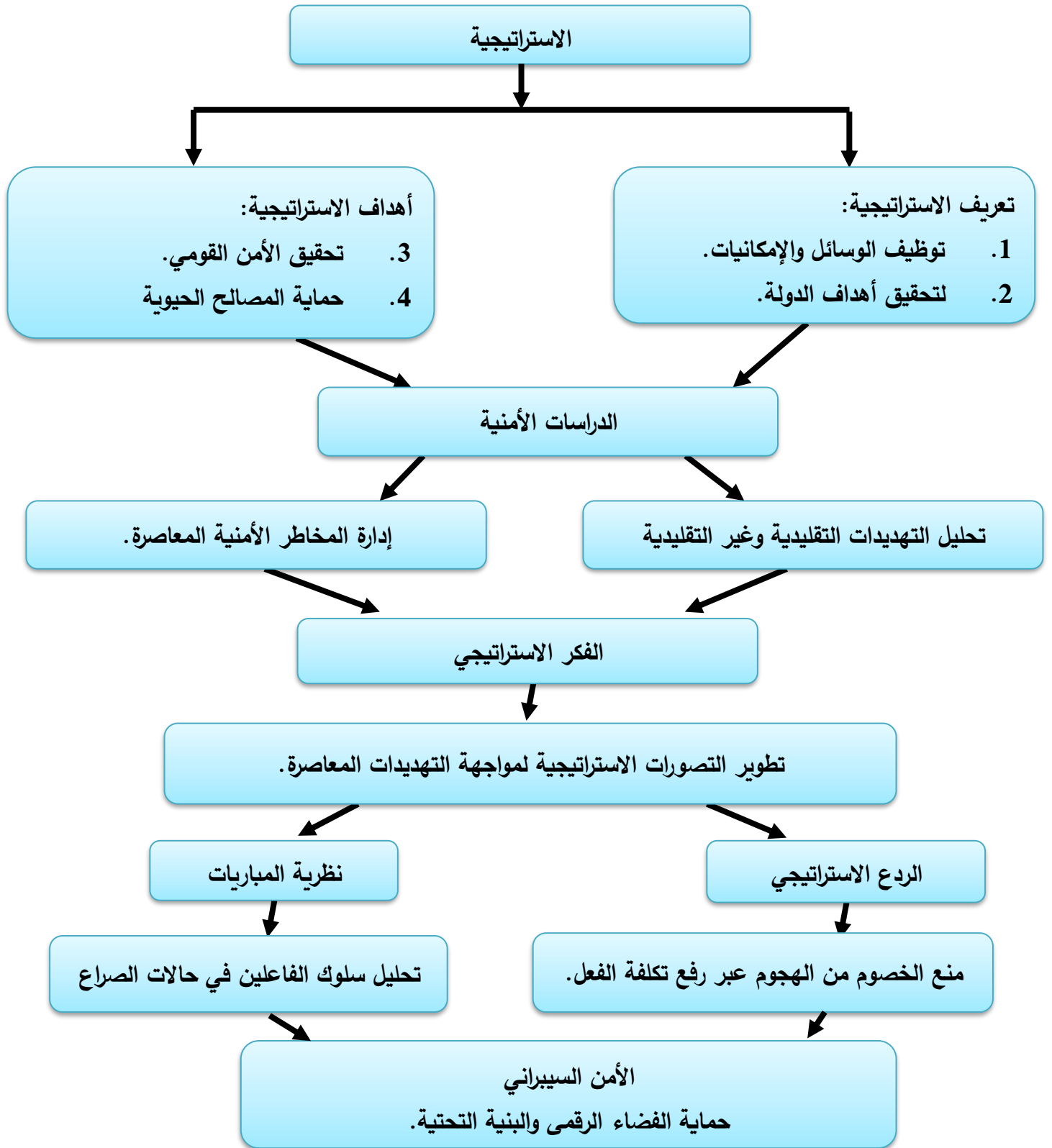
أولاً: الردع الاستراتيجي

يعتمد الردع الاستراتيجي على استخدام القدرات المتاحة لمنع الخصوم من القيام بأعمال عدائية، من خلال إقناعهم بأن تكلفة الهجوم ستكون أعلى من المكاسب المحتملة. وقد توسع مفهوم الردع ليشمل المجال السيبراني، حيث تطور ردع الهجمات الرقمية كأداة لحماية الأمن القومي. (Freedman, 2004, p. 26)

ثانياً: نظرية المباريات

تعد نظرية المباريات أداة تحليلية لفهم سلوك الفاعلين في حالات الصراع والتنافس، من خلال دراسة القرارات التي يتخذها كل طرف لتحقيق أقصى مكاسب ممكنة. وتساعد هذه النظرية في مجال الأمن السيبراني على تفسير تفاعلات الدول والجهات المختلفة فيما يتعلق بالهجوم والدفاع الرقمي. (Schelling, 1960, p. 03)

الشكل رقم 6: موقع الأمن السيبراني ضمن نظريات الفكر الاستراتيجي



المصدر: من اعداد الطالبة بالاعتماد على (Freedman, 2004, p. 26)، (Buzan, 1991, p. 27)

المبحث الثالث: نماذج تحليلية مفسرة لتطبيق الأمن السيبراني.

تمثل النماذج التحليلية أدوات محورية في الدراسات الأمنية والاستراتيجية، حيث تسهم في فهم الظواهر المعقدة وتفسيرها بطريقة منهجية ومنظمة. وفي مجال الأمن السيبراني، ازدادت أهمية هذه النماذج نظراً لتعدد الفاعلين وارتفاع مستوى التهديدات الرقمية وتعقيد التحديات التقنية. ويهدف هذا المبحث الى تقديم مجموعة من النماذج التحليلية، مثل نموذج SWOT ونموذج أندروسكوت، التي تتيح تقييم الهياكل السيبرانية وتحليل نقاط القوة والضعف والفرص والتهديدات، بالإضافة الى فهم تفاعلات المؤسسات والهيئات المسؤولة عن الأمن السيبراني.

المطلب الأول: النموذج التحليلي SWOT في دراسة المنظومة السيبرانية.

تحظى النماذج التحليلية بأهمية متزايدة في الدراسات الأمنية والاستراتيجية، نظراً لما توفره من أدوات منهجية تساعد على تحليل البيانات المعقدة وتفسير مختلف التحديات التي تواجه الأنظمة الحديثة. وفي هذا المطلب يبرز لنا نموذج SWOT كإطار تحليلي يستخدم لتقييم القدرات والإمكانات المتاحة من خلال تحليل نقاط القوة والضعف والفرص والتهديدات. ويسهم توظيف هذا النموذج في مجال الأمن السيبراني في تقديم قراءة تحليلية لواقع المنظومة السيبرانية، بما يسمح بتحديد مواطن القوة والقصور واستشراف التحديات والفرص المرتبطة بتأمين الفضاء الرقمي.

الفرع الأول: تعريف نموذج SWOT

يستخدم نموذج SWOT كأحد الأدوات التحليلية في مجال التخطيط الاستراتيجي، حيث يهدف إلى دراسة البيئة الداخلية والخارجية لأي منظمة أو نظام من خلال تحليل أربعة عناصر أساسية تتمثل في نقاط القوة (Strengths) ونقاط الضعف (Weaknesses) والفرص (Opportunities) والتهديدات (Threats). ويسمح هذا النموذج بتقديم رؤية تحليلية شاملة تساعد على تشخيص الواقع الاستراتيجي للمنظمة أو النظام محل الدراسة، بما

يسهم في تحديد الإمكانيات المتاحة والتحديات المحتملة، ومن ثم دعم عملية اتخاذ القرار ووضع الاستراتيجيات المناسبة لتحقيق الأهداف المرجوة. (الكرخي، 2016)

يعتمد نموذج SWOT على التمييز بين عاملين أساسيين في التحليل الاستراتيجي، يتمثل الأول في **البيئة الداخلية** التي تتضمن نقاط القوة ونقاط الضعف المرتبطة بالموارد البشرية والتقنية والتنظيمية المتاحة داخل المؤسسة أو النظام، في حين يتمثل العامل الثاني في **البيئة الخارجية** التي تشمل الفرص والتهديدات الناتجة عن المتغيرات السياسية والاقتصادية والتكنولوجية في المحيط الخارجي. ويساعد هذا التحليل على تحديد مواطن القوة التي يمكن استثمارها لتعزيز الأداء، إضافة إلى الكشف عن نقاط الضعف التي ينبغي معالجتها من أجل تحسين الكفاءة والقدرة على مواجهة التحديات المختلفة. (قحف، 2002)

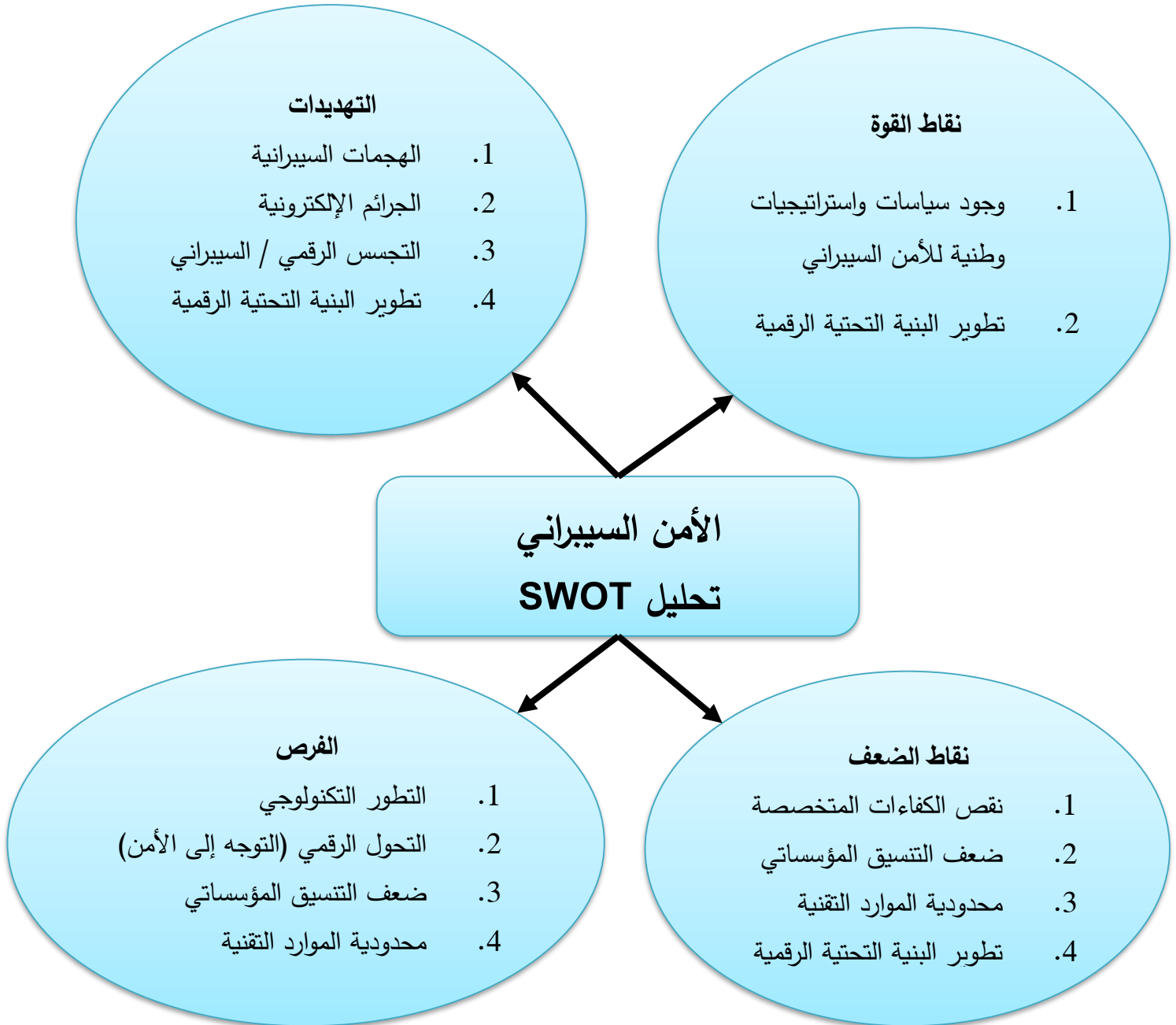
وفي إطار الدراسات الأمنية، يمكن توظيف نموذج SWOT في تحليل مختلف القضايا المرتبطة بالأمن الوطني، ومن بينها **الأمن السيبراني** الذي أصبح أحد المجالات الحيوية المرتبطة بحماية الفضاء الرقمي والبنية التحتية المعلوماتية للدول. ويسمح هذا النموذج بتقييم واقع المنظومة السيبرانية من خلال تحديد القدرات التقنية والمؤسسية التي تمثل نقاط قوة في مواجهة التهديدات الرقمية، إضافة إلى الكشف عن نقاط الضعف التي قد تستغلها الهجمات السيبرانية. كما يساعد على رصد الفرص المتاحة مثل التطور التكنولوجي والتعاون الدولي في مجال الأمن السيبراني، إلى جانب تحديد التهديدات المرتبطة بتزايد الجرائم السيبرانية والهجمات الإلكترونية المتطورة. (العدلوني، 2004)

الفرع الثاني: المخطط التحليلي لتطبيق نموذج SWOT في مجال الأمن السيبراني

يوضح هذا المخطط كيفية تطبيق نموذج SWOT في تحليل واقع الأمن السيبراني، حيث يتم التركيز على تحليل البيئة الداخلية من خلال تحديد نقاط القوة ونقاط الضعف المرتبطة بالقدرات التقنية والمؤسسية، في حين يتم تحليل البيئة الخارجية من خلال رصد الفرص

والتهديدات التي تؤثر في مستوى الأمن السيبراني. ويساهم هذا التحليل في تقديم رؤية استراتيجية تساعد على تعزيز القدرات الدفاعية الرقمية وتطوير السياسات الوطنية لمواجهة التهديدات السيبرانية.

الشكل رقم 7: النموذج التحليلي SWOT في دراسة المنظومة السيبرانية



المصدر: من إعداد الطالبة اعتمادا على: (الكرخي، 2016)، (العدلوني، 2004)،
(قحف، 2002)

المطلب الثاني: نموذج أندرو سكوت لتحليل الهياكل والمؤسسات السيبرانية

يهدف هذا المطلب إلى تقديم نموذج أندروسكوت (Andrew Scott) كأداة تحليلية لفهم كيفية تفاعل المؤسسات والهيئات المسؤولة عن الأمن السيبراني، وتقييم فعاليتها واستجابتها للتهديدات الرقمية.

الفرع الأول: تعريف نموذج أندرو سكوت

يعد نموذج أندروسكوت من النماذج التحليلية المستخدمة في دراسة السياسة الخارجية، حيث يركز على تحليل تفاعل الهياكل المؤسسية وآليات صنع القرار في بيئة دولية معقدة. غير أن تطور التهديدات المعاصرة، خاصة في المجال السيبراني، أتاح إمكانية توظيف هذا النموذج في مجالات تحليلية أخرى، من بينها دراسة الأمن السيبراني. وفي هذا الإطار، يمكن إسقاط نموذج أندروسكوت على تحليل السياسات والمؤسسات السيبرانية، من خلال دراسة البنية المؤسسية، وآليات التنسيق، والقدرات التقنية والبشرية، إضافة إلى السياسات والاستراتيجيات المعتمدة لمواجهة التهديدات الرقمية.

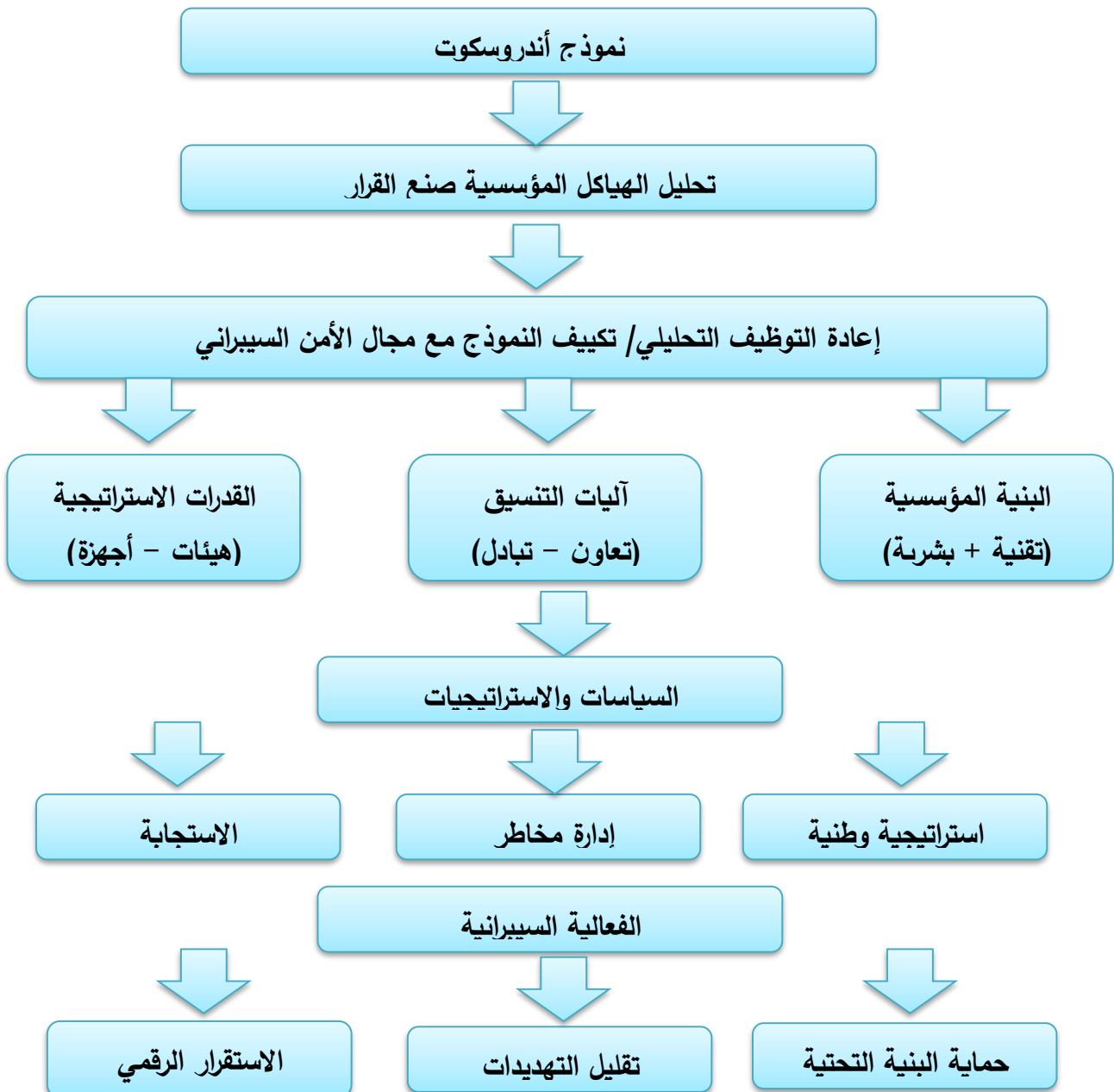
يعتبر نموذج أندروسكوت إطاراً منهجياً لتحليل الهياكل التنظيمية للمؤسسات السيبرانية، ويهدف إلى دراسة تفاعل المؤسسات والهيئات الأمنية والرقمية مع البيئة المحيطة بها. ويركز هذا النموذج على:

1. فهم الهيكل المؤسسي: دراسة تنظيم المهام والمسؤوليات داخل المؤسسات السيبرانية.
2. تقييم آليات التنسيق: تحليل كيفية التعاون بين المؤسسات المختلفة لضمان فعالية الأمن السيبراني.
3. تحديد القدرات التقنية والبشرية: تقييم الموارد المتاحة لمواجهة الهجمات السيبرانية.
4. مراجعة الإجراءات الاستراتيجية: دراسة السياسات والخطط المعتمدة للتصدي للتهديدات الرقمية. (عبد الرحمن، 2020)

ويتيح توظيف هذا النموذج للباحثين وصناع القرار إمكانية تحليل ديناميكية المؤسسات السيبرانية وتحديد نقاط القوة والضعف، بما يساهم في تحسين التنسيق بين الهيئات المختلفة وتعزيز مستوى الأمن السيبراني الوطني.

الفرع الثاني: المخطط التحليلي لنموذج أندرو سكوت

الشكل رقم 8: المخطط التحليلي لنموذج أندرو سكوت



المصدر: من اعداد الطالبة بالاعتمادا على (عبد الرحمن، 2020، صفحة 58)، (سعيد ن.، 2022، صفحة 77)، (يوسف، 2018، صفحة 112)

يوضح هذا المخطط كيفية توظيف نموذج أندروسكوت، المستخدم في تحليل السياسة الخارجية، في دراسة الأمن السيبراني من خلال تكييفه مع طبيعة التهديدات الرقمية المعاصرة. إذ ينطلق النموذج من تحليل الهياكل المؤسسية وآليات صنع القرار، ليتم إسقاطه على تحليل السياسات والمؤسسات السيبرانية عبر دراسة البنية المؤسسية، وآليات التنسيق، والقدرات الاستراتيجية. كما يبرز دور السياسات والاستراتيجيات في إدارة المخاطر والاستجابة للتهديدات، بما يساهم في تحقيق فعالية سيبرانية تتمثل في حماية البنية التحتية الرقمية وتعزيز الاستقرار في الفضاء السيبراني.

خلاصة الفصل الأول:

تناول الفصل الأول الإطار المفاهيمي والنظري للأمن السيبراني، حيث تم التطرق في البداية إلى مفهوم الأمن السيبراني من خلال تعريفه، تم اعتماد على تعريف إجرائي للأمن السيبراني: وبيان أهم المفاهيم المرتبطة به، إضافة إلى إبراز أبعاده وأهدافه المختلفة، سواء التقنية أو الأمنية أو الاستراتيجية، باعتباره مجالاً حديثاً يهدف إلى حماية الأنظمة والشبكات والمعلومات من مختلف التهديدات الرقمية.

كما تطرق الفصل إلى الإطار النظري للأمن السيبراني من خلال ربطه بمجال العلاقات الدولية والفكر الاستراتيجي، حيث أصبح الأمن السيبراني عنصراً أساسياً في تعزيز الأمن القومي وإعادة تشكيل موازين القوة بين الدول في الفضاء الرقمي.

وفي السياق ذاته، تم عرض مجموعة من النماذج التحليلية المفسرة للأمن السيبراني، مثل نموذج SWOT ونماذج تحليل الهياكل والمؤسسات، بهدف فهم نقاط القوة والضعف والفرص والتهديدات داخل المنظومة السيبرانية، إضافة إلى تقييم فعالية المؤسسات والسياسات المرتبطة بها.

وبناءً على ذلك، خلاص الفصل إلى أن الأمن السيبراني لم يعد مجرد جانب تقني فقط، بل أصبح قضية استراتيجية متكاملة ترتبط ارتباطاً وثيقاً بالأمن الدولي وصنع القرار، مما يستدعي اعتماد مقاربات تحليلية شاملة لفهمه وتقييمه.

الفصل الثاني

المقاربة الجزائية لتفعيل منظومة الأمن

السيبراني

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

بعد التطرق في الفصل الأول إلى الإطار المفاهيمي والنظري للأمن السيبراني، يهدف هذا الفصل إلى الانتقال نحو الجانب التطبيقي من خلال دراسة المقاربة الجزائرية في تفعيل منظومة الأمن السيبراني.

وعليه، يتناول هذا الفصل مختلف الجوانب القانونية والمؤسسية المنظمة للأمن السيبراني في الجزائر، كما يسلط الضوء على أبرز التحديات والتهديدات التي تواجه هذا المجال، إضافة إلى تحليل الجهود المبذولة لتعزيزه والآفاق المستقبلية لتطويره، بما في ذلك دور التقنيات الحديثة كالتمولوجيات الرقمية والذكاء الاصطناعي.

ويهدف هذا الطرح إلى تقديم قراءة تحليلية لواقع الأمن السيبراني في الجزائر، واستنتاج مدى فعالية السياسات والمؤسسات في مواجهة التحديات السيبرانية.

- **المبحث الأول: تشريعات وسياسات للأمن السيبراني.**
- **المبحث الثاني: البناء المؤسسي والتنظيمي الخاص بالأمن السيبراني.**
- **المبحث الثالث: التحديات والتهديدات المؤثرة على الأمن السيبراني.**
- **المبحث الرابع: الآفاق المستقبلية لتعزيز الامن السيبراني الوطني.**

المبحث الأول: التشريعات والسياسات للأمن السيبراني.

في ظل التحولات الرقمية المتسارعة، أصبحت التشريعات والسياسات الأساس الذي تركز عليه منظومة الأمن السيبراني، حيث تساهم في ضبط الفضاء السيبراني وحماية الأنظمة، المعلومات من مختلف التهديدات. أين سعت الجزائر إلى تطوير ترسانة قانونية واعتماد سياسات واستراتيجيات وطنية بما يواكب التحديات المتنامية في هذا المجال.

وعليه، سيتم التطرق في هذا المبحث إلى التشريعات المنظم للأمن السيبراني في الجزائر، ثم عرض أهم السياسات والاستراتيجيات الوطنية المعتمدة مع إبراز دور الدولة في مكافحة الجرائم السيبرانية من خلال مختلف الإجراءات الوقائية.

المطلب الأول: التشريعات الخاصة بالأمن السيبراني.

سنتطرق لمختلف القوانين الشاملة في التصدي والمواجهة لمثل هذه الجرائم المستحدثة في الجزائر، وعليه تسعى هذه التشريعات الى دعم الأمن السيبراني من خلال توفير إطار قانوني يواكب التطورات الرقمية.

الفرع الأول: القوانين الوطنية المتعلقة بالجرائم السيبرانية.

تشكل القوانين الوطنية الإطار الأساسي لمكافحة الجرائم السيبرانية، حيث تهدف إلى تنظيم الفضاء الرقمي وتجريم الأفعال التي تستهدف الأنظمة المعلوماتية، بالنسبة للتجربة الجزائرية اعتمدت على مجموعة من القوانين التي يمكن تصنيفها إلى قوانين عامة وأخرى خاصة.

أولاً: القوانين العامة

1. الدستور الجزائري

لقد كفل دستور الجزائر سنة 1996، وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016، حماية الحقوق الأساسية والحريات الفردية، وهذا ما جاء به من أجل تعديل الدستور 2020، على أن تضمن الدولة عدم انتهاك حرمة الإنسان الجزائري. حيث أن هذه الدساتير تخضع لتعديلات كل فترة زمنية لتواكب الاحداث الجارية على مستوى الوطني والدولي.

وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى، والتي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة مايلي:

- **المادة 37:** كل المواطنين سواسية أمام القانون، ولهم الحق في حماية متساوية، ولا يمكن أن يتذرع بأن تمييز يعود سببه إلى المولد أو العرق، الجنس، الرأي، أي شرط، ظرف آخر شخصي أو اجتماعي.
- **المادة 74:** حرية الإبداع الفكري، بما في ذلك أبعاده العلمية والفنية، مضمونة.
- لا يمكن تقييد هذه الحرية إلا عند المساس بكرامة الأشخاص أو بالمصالح العليا للأمة أو القيم والثوابت الوطنية.
- يحمي القانون الحقوق المترتبة على الإبداع الفكري، ففي حالة نقل الحقوق الناجمة عن الإبداع الفكري، يمكن للدولة ممارسة حق الشفعة لحماية المصلحة العامة.
- إذا لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها المضمونة، والقانون يحمي حقوق

المؤلف، ولا يجوز حجز أي مطبوع أو تسجيل أو أي وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي. (عاقلي، 2017، صفحة 127)

2. قانون العقوبات الجزائري

لقد تطرق المشرع الجزائري الى تجريم الأفعال الماسة بأنظمة الحاسوب الآلي، وذلك نتيجة تأثيره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، مما دفع المشرع الجزائري الى تعديل قانون العقوبات بموجب القانون رقم 15 المؤرخ في 10 نوفمبر 2004، المتمم للأمر رقم 15-22 المتضمن قانون العقوبات، تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، ويتضمن هذا القسم ثمانى مواد، من المادة 394 مكرر 7. (عاقلي، 2017)

فبغرض تدارك الفراغ القانوني قام المشرع الجزائري بموجب القانون رقم 04-15. باستحداث جملة من النصوص، حيث جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها ما يقابله من الجزاء، إذ قام المشرع بسن جملة من قوانين القانونية الموضوعية والتي حدد من خلالها كل الأفعال الماسة بنظم المعالجة الآلية للمعطيات وما يقابلها من جزاء أو عقوبة، (القانون رقم 06-22، 2006) والى جانب ذلك فقد قام المشرع الجزائري بسن قواعد إجرائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الإلكترونية، وذلك من خلال تعديل قانون الإجراءات الجزائية بموجب القانون رقم 06-22. (إبراهيم، 2006، صفحة 124)

إذ نصت المادة 394 مكرر منها مايلي: "يعاقب بالحبس من ثلاثة أشهر الى سنة وبغرامة من 50.000 الى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

نصت المادة 394 مكرر 2 على أنه: "يعاقب كل من يقوم عمدا وعن طريق الغش بما يأتي:

1. تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أو ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ونصت المادة 394 مكرر 6 أنه " بالإضافة الى العقوبات الأصلية أي الحبس والغرامة، والاحتفاظ بحقوق الغير حسن النية، بحكم العقوبات التكميلية التالية :

يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محل لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالئها. (نواره، 2017، صفحة 118_119)

2. قانون الإجراءات الجزائية الجزائية

بالنسبة لمتابعة الجريمة الإلكترونية، تتم بنفس الإجراءات التي تتبع بها الجريمة كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة.

نجد أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها أو بالمكان تم الذي دائرته القبض على هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر، ونص التفتيش في المادة 45 الفقرة 7 ومن نفس القانون المعدل إذا جرى تفتيش في مسكن شخص أخرى يشتبه بأنه يحوز أوراقا أو أشياء لها علاقة بالأفعال الاجرامية فإنه يتعين حضوره وقت إجراء التفتيش وإذا تعذر ذلك اتبع الاجراء المنصوص عليه في الفترة السابقة، حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق، قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق

الأحكام الواردة في المادة 44 من القانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية. (ديدان).

ثانيا: القوانين الخاصة

1. القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

صدر القانون رقم 04-09 بتاريخ 5 أوت 2009 ويتضمن 19 مادة موزعة على ستة فصول، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحداث القوانين، قامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية. كما يتضمن هذا القانون أحكاما خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها، وهي الأفعال الموصوفة بجرائم الإرهاب، التخريب، الجرائم الماسة بأمن الدولة أو حالة توفر معلومات عن اعتداء محتمل يهدد منظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام. (نواره، 2017)

يعتبر القانون رقم 04-09 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية، حيث جاء بتجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة، بما في ذلك شبكة الانترنت وعلنكل تقنية مستقبلا. (نايري، 2017، صفحة 39_40)

2. القانون الخاص المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية:

حيث استحدث هذا القانون ووضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الافتراضي، منها استحداث سلطة الضبط، ومن بين مهامها السهر على احترام متعاملي البريد والاتصالات الإلكترونية والأمن السيبراني. (القانون رقم 04-18، 2018)

الفرع الثاني: حماية البيانات والبنية التحتية الحيوية

شكل حماية البيانات والبنية التحتية الحيوية من الركائز الأساسية لتعزيز الأمن السيبراني، لما لها من دور في تأمين الفضاء الرقمي وضمان استمرارية عمل الأنظمة الحيوية، حيث تتجسد هذه الحماية في عدة مجالات مترابطة تشمل حماية البيانات الشخصية، وتأمين الأنظمة المعلوماتية، إضافة إلى حماية القطاعات الحيوية.

أولاً: حماية البيانات الشخصية

وضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الافتراضي والتي جاء إيجازها في عدة نقاط: (القانون رقم 18-07، 2018)

3. استحداث السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ووضع مجموعة التزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات طابع الشخصي.
4. اتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من المسؤول عن المعالجة.
5. تأهيل أعوان الرقابة للقيام ببحث ومعاينة الجرائم المتعلقة بالمعطيات ذات الطابع الشخصي تحت إشراف وكيل الجمهورية.
6. تختص الجهة القضائية الجزائرية بمتابعة الجرائم التي ترتكب خارج إقليم الجمهور من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، كما تختص بمتابعة الجرائم المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية.

ثانيا: حماية الأنظمة المعلوماتية

أصدرت الجزائر مرجعا لأمن المعلومات والذي يعتبر إطارا تنظيميا للأمن السيبراني سنة 2020 يتضمن عشرين مجالا تبعا للنسخة الأولى التي تم إطلاقها سنة 2016 بقيادة وزارة البريد والاتصالات السلكية واللاسلكية والشؤون الرقمية والتي تشمل سبعة محاور فقط. والهدف من وراء إعداد هذا المرجع يكمن في إقامة حوكمة ونهج موحد لأمن المعلومات داخل الهيئات والمؤسسات. هذا المرجع يحدد الحد الأدنى من متطلبات المتعلقة بالأمن وذلك من أجل تسيير ومقاومة والتقليل من أثر التهديدات المتوقعة.

زيادة على ذلك فإن مرجع أمن المعلومات يقدم الضوابط الأمنية وأفضل المؤسسات التي يمكن أن تتبناها الهيئات العمومية، مع التركيز على تدريب المستخدمين بالمخاطر التي تطوي عليها، والتقييم الدوري لضوابط هذا المرجع في: الأمن المادي، أنترنت، المراقبة وتسجيل الوقائع، إدارة الحوادث الأمنية، تسيير استمرارية النشاطات، الموارد البشرية، الأمن المتعلق باستخدام مواقع التواصل الاجتماعي، دمج الأمن خلال دورة حياة تطوير البرمجيات، متطلبات الأمن المشاريع تكنولوجيا الاعلام والاتصال، العلاقة مع الأطراف الثالثة، إدارة الموجودات، حماية البيانات ذات الطابع الشخصي، إدارة ومراقبة النفاذ، أمن أجهزة الموجودات، أمن أجهزة المحمول، أمن الشبكات، أمن أنظمة المعلومات، الأمن المتعلق بالتشغيل، أمن المعلومات بالغ الأهمية، أمن الحوسبة السحابية والتشفير.

ثالثا: حماية القطاعات الحيوية

رغم تزايد الرقمنة، لاتزال العديد من الصناعات تعتمد بشكل كبير على أنظمة الأمان التقليدية، مما يتيح للمهاجمين السيبرانيين فرصة الاستفادة من الثغرات الموجودة في البنية التحتية القديمة. حيث شهدت الجزائر في السنوات الأخيرة تطورا سريعا في مجال تكنولوجيا المعلومات والاتصالات، مما يشكل شرطا ضروريا للتحويل نحو الاقتصاد الرقمي واعتماد

نهج الحكومة الإلكترونية الذي يركز على المواطن. ومع ذلك، فإن هذا التحول يتطلب تأمين وحماية جميع الأنظمة الرقمية وتدفقات المعلومات الخاصة بها.

حيث أدت التهديدات المحتملة للهجمات السيبرانية ضد تكنولوجيا المعلومات والاتصالات إلى خسائر اقتصادية وإلى خلق مناخ من انعدام الأمن وعدم اليقين تجاه الخدمات الرقمية، الأمر الذي يستدعي تطبيق تدابير مضادة تحمي المؤسسات والبنى التحتية الحيوية، وتحافظ على المصالح الحيوية للبلاد وتعزيز الأمن الوطني، والبنوك باعتبارها من أهم المؤسسات المعرضة للهجمات السيبرانية فإنها سعت بدورها إلى البحث عن أساليب وحلول للتقليل من هذه المخاطر، كما أن من أبرز القطاعات الأكثر عرضة لهجمات السيبرانية وهو قطاع الطاقة وذلك نظرا لأهميته البارزة في تشغيل باقي المرافق الحيوية، حيث تؤدي الهجمات إلى تعطيل إمدادات الكهرباء والغاز، وغيرها من القطاعات الحيوية المهمة. (وصديقي و حشروف، 2025)

المطلب الثاني: السياسات والاستراتيجيات الضابطة

لا يقتصر تحقيق الأمن السيبراني على سن التشريعات وتجريم الأفعال المرتبطة بالفضاء الرقمي، بل يتطلب كذلك اعتماد سياسات واستراتيجيات وطنية متكاملة تسهم في توجيه الجهود وتنسيقها بين مختلف الفاعلين، فمع تزايد التهديدات السيبرانية وتعقدها، أصبح من الضروري تبني استراتيجيات فعالة تقوم على التخطيط الاستراتيجي وتحديد الأولويات، بما يضمن الاستجابة السريعة لمختلف المخاطر.

حيث تسعى الجزائر إلى تطوير سياسات واستراتيجيات وطنية تهدف إلى تعزيز حماية الفضاء السيبراني، من خلال دعم القدرات التقنية والبشرية وتكريس التنسيق المؤسسي، بما يتماشى مع متطلبات التحول الرقمي والتحديات الأمنية المعاصرة.

الفرع الأول: الاستراتيجية الوطنية للأمن السيبراني

تعد الاستراتيجية الوطنية للأمن السيبراني في الجزائر إطارا يحدد توجهات الدولة لحماية الفضاء الرقمي، من خلال وضع أهداف وآليات لمواجهة التهديدات السيبرانية، وتعزيز التنسيق بين مختلف الفاعلين، بما يواكب التحول الرقمي المتسارع.

أولا: الإعداد والتخطيط للاستراتيجية الجزائرية في مجال الأمن السيبراني

يبدأ صانع القرار في الجزائر بأهمية سن جملة من التشريعات والنصوص القانونية التي تتلاءم وتتناسب مع مجال الأمن السيبراني، وهو ما تجسد فعلا على أرض الواقع كخطوة أولية، يليها بعد ذلك كخطوة ثانية تعيين الهيئات والمؤسسات الرائدة التي تخول لها مسؤولية إدارة مخاطر التهديدات السيبرانية وبالتالي صياغة وإصدار قوانين وأنظمة، وكذا برامج محددة لعمل هذه الهيئات والمؤسسات كي تأخذ الطابع الرسمي والشرعي.

وعلى باعتبار أن موضوع الأمن السيبراني يأخذ في طياته أساس الطابع الأمني فقد أوكلت المهمة في الجزائر لكل من مؤسسة الجيش الوطني الشعبي، وكذا جهاز الدرك الوطني، وسلك الأمن الوطني ووزارة العدل، وهي المؤسسات الرائدة التي اعتمدت عليها الدولة في هذا الخصوص. حتى تتمكن الهيئات من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السيبراني وفق ما تم رسمه في الاستراتيجية الوطنية، توجهت المؤسسات السيادية (رئاسة الجمهورية، وزارة الدفاع، المؤسسات الأمنية، الوزارات) الى تنظيم دورات تكوينية وسخرت لها كافة الوسائل المادية والبشرية، كما استجذبت الجزائر بخبراء دوليين لتمكين الأطارات الناشطة في المجال من جميع الأسلاك لمعرفة أفضل الممارسات في تكنولوجيا الأمن والسياسات العامة للأعمال الإلكترونية المعمول بها في الخارج، كما تم بعثات للحضور والمشاركة في المؤتمرات الدولية للاستفادة من الخبرات التي تهدف الى إصدار التوصيات المناسبة لأمن وسلامة المعلومات في الفضاء السيبراني. (بوازدية، 2019)

ثانيا: استراتيجية بناء الأمن السيبراني في الجزائر

تبرز جهود الجزائر للحد من مخاطر الحرب السيبرانية التي تستهدف اضعاف مقدراتها في مجال الاعتمادية التقنية، من خلال الاهتمام بوضع سياسات واليات تساهم في تعزيز الأمن السيبراني، وقد عكفت الجزائر منذ سنة 1997 على الاستجابة لهذا الموضوع على مستوى الوسائل والعديد من المؤسسات والهيئات الفاعلة أو المستحدثة في مجال التعاطي مع مانتيجحه مخاطر التهديدات السيبرانية على الأمن القومي للبلاد، ولعل ادراك المخاطر الالكترونية ذات الطابع الاجرامي يستقي خطورته من الهجمات الالكترونية المتعددة والكثيفة التي تتعرض لها الجرائر باستمرار، لاسيما من مناطق ودول تتميز بعداؤها للجزائر.

كما وضع الاتحاد الدولي لاتصالات نموذج لبناء الاستراتيجية الوطنية للأمن السيبراني، ويتضمن هذا النموذج عدة محاور أساسية: الأول يرتبط بالتدابير القانونية والتشريعية، والثاني يتعلق بالتدابير التقنية والبنى التحتية، والثالث خاص بالهياكل التنظيمية المؤسسية للأمن السيبراني في الدولة، الرابع مرتبط ببناء القدرات الفنية في هذا المجال الذي يعاني ندرة المتخصصين، وأخيرا الخامس يتناول التعاون الدولي وتبادل المعلومات بين الدول في مجال الأمن السيبراني، والذي قد يقلل من خطورة الهجمات السيبرانية. (محمودي، 2023)

ثالثا: الاستراتيجية الجزائرية وفق مستويات.

1. على مستوى الوطني:

أدرجت الجزائر الأمن السيبراني كإحدى الأولويات في برنامج المواجهة ضد الالكترونية والإرهاب الالكتروني، بل أصبح يشكل جزء لا يتجزأ من استراتيجيات الدفاع، الدروس المستخلصة من الدول التي لها تجربة في هذا المجال، أثبتت أن النجاعة في تطبيق وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

بين الفاعلين في الميدان، وعليه توجهت الجزائر الى رسم استراتيجيتها مركزة على النقاط التالية: (بوازدية، 2019)

- تحديد المخاطر
- اتخاذ التدابير اللازمة
- تحديد الهيئات المكلفة بإدارة الأمن
- تحديد الهيئات المكلفة بالتنسيق
- تحديد الهيئة الكلفة بالجانب التقني للبحث عن الثغرات وتوجيه التحقيق، ليبقى الهدف الأخير، زيادة قدرات الأمن السيبراني لحماية الأنظمة المعلوماتية وتعزيز سبل المواجهة الوقائية والمواجهة الردعية.

2. على مستوى الإقليمي:

1. على مستوى العربي:

من خلال الدراسات الأكاديمية وتحليل المعطيات المستقاة من المؤسسات المتخصصة في الأمن السيبراني المتضمنة النقائص والثغرات في حماية الأنظمة المعلوماتية للدول العربية، المعلن عليها خلال اللقاءات، يتضح أن المقاومات البشرية والمادية المتوفرة القادرة على تفادي المخاطر لم تجدي نفعا، والدليل أن السلبات التي أصبحت تشكل نسبة كبيرة من المخاطر لا تزال تطرح نفسها ومن بينها نذكر مايلي: (بوازدية، 2019)

- المنظومة التشريعية والتنظيمية العربية تشهد حركة بطيئة، مما يجعلها غير جامعة للعديد من الجوانب الحساسة للفضاء السيبراني.
- عدم توازن المعادلة في الموارد البشرية بين ما هو موجود وما يجب أن يكون.

- عدم جدية التعاون داخليا ومع الأرقام المصرح بها من طرف أجهزة الأمن عن نسبة الاختراقات المتزايدة.

أمام هذه التحديات، لجأت الجزائر في بداية الامر الى التعامل مع هذه الجريمة من خلال تفعيل المبادئ العامة المتعارف عليها عالميا في مجال مكافحة الجريمة (تبادل المعلومات، تبادل الخبرات والمساعدة التقنية).

3. على مستوى الدولي:

مع الانفتاح الذي عرفه العالم بعد الحرب الباردة، أضحت كل المعاملات تخضع الى مبدأ الحرية في التنقل لأي نقطة في العالم (اقتصاد الانترنت) بأقل تكلفة وذلك من خلال ما توفره التكنولوجيا من وسائل اتصال، ومع مرور الزمن أصبحت هذه الوسيلة في متناول الجميع.

من هذا المنطلق وأمام تصاعد الاهتمام العالمي بهذا العالم الافتراضي، توجهت الهيئات المتخصصة سواء على مستوى الدولي (الشركات المتعددة الجنسيات) أو على المستوى الاممي (الاتحاد الدولي للاتصالات) بوضع مقاييس وضوابط لحماية البيانات، سلامة التحويلات الالكترونية في جميع المجالات، (حوكمة الانترنت)، كما تم وضع مناهج وآليات للحماية من الجريمة السيبرانية وتداعياتها المستقبلية. (بوازدية، 2019)

الفرع الثاني: البرامج والمبادرات الحكومية

تجسد الشكل الجزائر استراتيجيتها في الأمن السيبراني من خلال مجموعة من البرامج والمبادرات الحكومية التي تهدف إلى تعزيز الحماية الرقمية وبناء القدرات الوطنية، ومن أبرزها:

1. إطلاق الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية (2025-2029)

قامت الدولة الجزائرية بإطلاق الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة (2025-2029)، والتي تعد إطارا مرجعيا يهدف إلى حماية البنية التحتية الرقمية، وتعزيز المرونة السيبرانية، وضمان السيادة الرقمية الوطنية، خاصة في ظل تسارع التحول الرقمي. (وزارة الدفاع الوطني الجزائرية، 2026)

2. تنظيم ملتقيات وطنية لتعزيز القدرات السيبرانية

عملت الجزائر على تنظيم ملتقيات وطنية لتعزيز القدرات السيبرانية، حيث أن تنظيم هذا الملتقى "يأتي في ظرف يتميز بتسارع غير مسبوق للتحولات التكنولوجية وبروز تهديدات رقمية متزايدة تمس الأنظمة المعلوماتية للمؤسسات الاقتصادية للخدمات الحيوية"، مبرزة الأهمية التي يوليها قطاع التكوين والتعليم المهنيين لهذا الموضوع من خلال "تكوين كفاءات تقنية قادرة على مجابهة التحديات الميدانية والاستجابة لمتطلبات المؤسسات ومرافقة التحول الرقمي الذي يشهده الاقتصاد الوطني".

وأكدت بهذا الخصوص على ضرورة "تحيين برامج التكوين وتعزيز الجانب التطبيقي وإدماج الأدوات التكنولوجية الحديثة بما يضمن مواءمة فعالية بين التكوين ومتطلبات سوق العمل. (وكالة الأنباء الجزائرية، 2026).

3. تنظيم ورشات عمل وتكوين في مجال الأمن السيبراني

تم تنظيم ورشات وطنية من طرف الجهات المختصة، خاصة في إطار الاستراتيجية الوطنية، وقد تناولت مجموعة من محاور الأساسية: (وزارة الدفاع الوطني الجزائري، 2024)

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

- القدرات التقنية العملية وترمي الى تطوير القدرات التقنية-العملية في مجال الحماية ومرونة الأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة الى تزويد بلد الجزائر بوسائل الوقاية والكشف والاستجابة للحوادث السيبرانية.

- التكوين والبحث وتطوير التحسيس وهي تزويد العنصر البشري، بصفته الحلقة الأهم في السلسلة الأمنية، بالكفاءات والمعارف الضرورية التي تسمح له بممارسة مهامه في الفضاء السيبراني بطريقة آمنة وفعالة.

المطلب الثالث: دور الدولة في مكافحة الجرائم السيبرانية

مع التزايد المستمر للتهديدات المرتبطة بالفضاء الرقمي، أصبح تدخل الدولة ضرورة ملحة لشكل لمواجهة الجرائم السيبرانية والحد من آثارها من خلال وضع سياسات والتشريعات، حيث تعمل الدولة الجزائرية على تفعيل مختلف أجهزتها التنفيذية، إلى جانب تبني برامج وقائية وتوعوية، بهدف تعزيز الأمن السيبراني وحماية الأفراد والمؤسسات.

الفرع الأول: جهود الجهاز التنفيذي

تعد الأجهزة التنفيذية في الجزائر بدور أساسي في مكافحة الجرائم السيبرانية، من خلال تتبع الأنشطة الإجرامية في الفضاء الرقمي الذي نشهد عليه تطورا بارزا، انطلاقا من استخدام وسائل وتقنيات حديثة تتماشى مع طبيعة هذه الجرائم. وتشمل هذه الجهود تفعيل دور المصالح الأمنية المختصة في هذا المجال، التي تعمل على رصد التهديدات السيبرانية والتصدي لها بشكل فعال. وذلك عبر ما تعتمد عليه الدولة الآتي:

1. المراقبة الإلكترونية:

استحدثت المشرع الجزائري وبموجب المادة الثالثة 03 من القانون 04-09 المتضمن عدد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها إجراء المراقبة

الإلكترونية حينما أجاز تبعا لمستلزمات التحريات أو التحقيقات القضائية الجارية في إطار هذا النوع من الجرائم، اللجوء الى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، فجاء نص المادة كما يلي: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميعها وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية".

قد أحاط المشرع هذا الإجراء باعتباره وسيلة إجرائية في مجال الجريمة السيبرانية بمجموعة من الحالات التي تستدعي اللجوء للمراقبة الإلكترونية للاتصالات، حددها بموجب 4 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويمكن حصر هذه الحالات في الآتي: (قانون رقم 04-09، 2009)

1. الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

2. في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

3. لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى المراقبة الإلكترونية.

ويبرز دور المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني في دعم جهود مكافحة الجرائم السيبرانية، حيث يتميز بقدرات عالية في محاربة الجريمة بشتى أشكالها.

يحتوي على 11 دائرة متخصصة في عدة مجالات مختلفة، تضمن كلها التكوين والتعليم وكذلك الخبرة، وكذا منح كل المساعدات في المجال التقني، يحتوي على تجهيزات عديدة

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

كالمحطة الثابتة والمحمول للقيام بخبرات في مجال الإعلام الآلي، الشبكات الإعلامية والتجهيزات البنيانية، ومحطة تصليح وترميم مختلف الأجهزة والحوامل غير فعالة.

الفرع الثاني: التدابير الوقائية.

تعتمد الدولة الجزائرية في مكافحة الجرائم السيبرانية على جملة من التدابير الوقائية التي تهدف إلى الحد من المخاطر الرقمية قبل وقوعها، وذلك من خلال تبني مقاربة شاملة تجمع بين الأبعاد القانونية والتقنية والهيكلية، إلى جانب تعزيز التعاون الأمني.

الجدول رقم 1: التدابير الوقائية للأمن السيبراني في الجزائر

الهدف من هذه التدابير القانونية توفير الحماية القانونية للبيانات والأنظمة المعلوماتية، وردع السلوكات الاجرامية.	تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا بتجريم أفعال المساس بأنظمة الحاسوب، مما دفع المشرع بتعديل قانون العقوبات بموجب القانون رقم 04-15 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.	التدابير القانونية
هدف من هذه التدابير التقنية وهو حماية الأنظمة المعلوماتية مثل أنظمة الحماية والمراقبة الالكترونية والتشفير، كما يمنع الاختراقات والكشف المبكر لمختلف التهديدات.	لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للجرائم الإلكترونية لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تتفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها.	التدابير التقنية

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

الهدف من هذه التدابير الهيكلية هو تنظيم فعال للمؤسسات وتحقيق فعالية كبير في مواجهة هذه التهديدات.	انشاء وتنظيم الهيئات والمؤسسات المختصة بالأمن السيبراني منها، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الهيئات القضائية الجزائرية المتخصصة، جهاز الامن الوطني والدرك الوطني.	التدابير الهيكلية
الهدف من هذه التدابير التعاون الدولي تعزيز التعاون بين الأجهزة الأمنية والمؤسسات الوطنية إضافة الى التعاون الدولي في مجال مكافحة الجرائم السيبرانية وخاصة الجرائم العابرة للحدود.	ضرورة التعاون الأمني الدولي لقد أثبت الواقع العملي أي الدولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس في كافة ميادين الحياة. لهذا اصبح من الضروري استحداث لوجود كيان دولي يقوم بالتعاون من اجل مواجهة التهديدات السيبرانية عبر المساعدة القضائية الدولية، تكريس المشرع الجزائري لمبدأ التعاون الدولي.	التدابير التعاون الامني

المصدر: من إعداد الطالبة بالاعتماد على (15-261، 2015)

يوضح الجدول أن التدابير الوقائية في مجال الأمن السيبراني في الجزائر، تتوزع بين أبعاد قانونية، تقنية، هيكلية وتعاونية أمنية، مما يعكس الطابع الشمول لمواجهة هذه التهديدات السيبرانية. كما يوضح أن فعالية هذه التدابير ترتبط بمدى تكاملها مع بعضها البعض بين مختلف المستويات التي تم درستها، بما يقدم من تعزيز القدرة الوقائية وتقليل المخاطر السيبرانية على المؤسسات الوطنية في الجزائر.

المبحث الثاني: البناء المؤسسي والتنظيمي الخاص بالأمن السيبراني

يمثل البناء المؤسسي والتنظيمي أحد الدعائم الأساسية لتجسيد الأمن السيبراني على أرض الواقع، حيث يرتبط نجاح السياسات والاستراتيجيات بمدى توفر هياكل قادرة على تنفيذها بكفاءة، حيث سعت الجزائر إلى إرساء منظومة مؤسسية متكاملة، تقوم على تعدد الفاعلين وتكامل أدوارهم، مع تعزيز آليات التنسيق فيما بينهم، بما على نحو يسمح بمواجهة هذه التهديدات السيبرانية بفعالية وضمان حماية الفضاء الرقمي.

المطلب الأول: المؤسسات والهيئات المتخصصة في تعزيز الامن السيبراني

أدركت الجزائر في ظل التحديات التي تفرضها الجرائم السيبرانية والتهديدات الرقمية المتزايدة، حيث يرتبط نجاح السياسات والاستراتيجيات بمدى توفر هيئات متخصصة قادرة على تجسيدها على أرض الواقع، عملت الجزائر على إرساء مجموعة من المؤسسات والهيئات التي تضطلع بمهام تنظيمية وتقنية وتكوينية، بما يضمن حماية الفضاء الرقمي وتعزيز القدرة على مواجهة التهديدات السيبرانية.

الفرع الثاني: المؤسسات الحكومية

1. مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية للدرك الوطني: أنشئ في 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر ويهدف الى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رابس، هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت. (غازي، 2016، صفحة 43)

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

الجدول رقم 2: يوضح عدد القضايا المعالجة من طرف مركز الوقاية من الجرائم المعلوماتية ومكافحتها

السنة	عدد القضايا المعالجة	طبيعة القضايا
2009	18	• التهديد
2010	22	• جرائم المساس بالنظام العام
2011	24	• الإرهاب
2012	30	• جرائم المساس بأنظمة المعالجة الآلية للمعطيات (الاختراق)
2013	46	• تحريض القسر على الفسق والدعار
2014	102	• إهانة هيئة نظامية
2015	240	• إهانة رموز الدولة
		• النصب والاحتيال

المصدر (عز الدين، 2015)

يوضح الجدول المعطيات المتعلقة بعدد القضايا المعالجة من طرف مركز الوقاية من الجرائم المعلوماتية ومكافحتها خلال الفترة الممتدة من 2009 إلى 2015، حيث يبين لنا عن وجود تزايد في حجم القضايا المسجلة، مما يعكس تصاعد في التهديدات السيبرانية وتوسع نطاق استخدامها. كما يشير ذلك إلى تطور دور المركز الوقاية في التعامل مع هذه القضايا، رغم استمرار الحاجة إلى تعزيز الإمكانيات البشرية والتقنية لمواكبة تهديدات السيبرانية.

2. الوكالة أمن أنظمة المعلوماتية: تم تأسيس منظومة وطنية لأمن الأنظمة المعلوماتية - وكالة أمن أنظمة المعلومات - تحت إشراف وزارة الدفاع الوطني تضم مجلسا ووكالة لتنسيق، إعداد وتنفيذ الإستراتيجية الوطنية للأمن السيبراني بهدف حماية المؤسسات الوطنية من التهديدات السيبرانية وضمان أمن البيانات والمعلومات، (جنادي ، 2024) تشتمل مهامها

حسب المادة 20 من المرسوم إدارة لجنة توجيهية تضم مجلسا علميا بالإضافة الى مركز وطني عملياتي لأمن الأنظمة المعلوماتية، الى جانب مصالح تقنية وإدارية تحت إشرافها لضمان التنسيق والتنفيذ الفعال للإستراتيجية الوطنية. (شريف و لحمل، 2023)

3. وزارة الرقمنة والاحصائيات: ركزت على وضع الأطر التكنولوجية والإدارية المتعلقة بعمل أنظمة المعلومات الحكومية، وهي الجهة المسؤولة عن تنسيق مشاريع الرقمنة على المستوى الوطني، بما في ذلك:

- تطوير منصات الحكومية مؤمنة.
- تشجيع تبني المعايير الدولية في الأمن السيبراني.
- دعم المؤسسات العمومية في عملية التحول الرقمي مع مراعاة الجوانب الأمنية. (غازي، 2016)

3. المدرسة الوطنية العليا للأمن السيبراني:

ضمن الجهود التي تبذلها الجزائر لتعزيز البعد التكويني في منظومة الأمن السيبراني، حيث تمثل مؤسسة تعليمية متخصصة تهدف إلى إعداد كفاءات وطنية عالية التأهيل في مجال حماية الأنظمة المعلوماتية، حيث تسعى هذه المدرسة إلى توفير تكوين أكاديمي وتقني متكامل يجمع بين المعارف النظرية والتطبيقات العملية، بما يسمح بتأهيل إطارات قادرة على مواجهة التهديدات السيبرانية المتزايدة، خاصة في ظل التحول الرقمي الذي يشهده العالم.

كما تركز برامجها على مجالات متعددة، من بينها أمن الشبكات، تحليل الهجمات السيبرانية، وإدارة المخاطر الرقمية. ويعكس إنشاء هذه المؤسسة إدراك الجزائر لأهمية العنصر البشري في تحقيق الأمن السيبراني، حيث لم يعد الاعتماد على الوسائل التقنية كافياً، بل أصبح الاستثمار في تكوين الموارد البشرية المتخصصة ضرورة استراتيجية. كما يبرز هذا التوجه

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

تبنى الدولة لمقاربة استباقية تقوم على بناء القدرات الوطنية وتعزيز الاستقلالية في المجال السيبراني. (وزارة التعليم العالي والبحث العلمي، 2023)

5. المدرسة العليا للذكاء الاصطناعي: من أبرز المؤسسات التكوينية المستحدثة في الجزائر، حيث أنشئت من أجل توجيه الدولة نحو مواكبة التحولات الرقمية وتعزيز استخدام التكنولوجيات الحديثة، وعلى رأسها الذكاء الاصطناعي. كما هدف هذه المدرسة إلى تكوين كفاءات وطنية متخصصة في مجالات تحليل البيانات، التعلم الآلي، والأنظمة الذكية، بما يسمح بتطوير حلول مبتكرة لمختلف التحديات، مثل مانشده الان في الجامعات الجزائرية ودخول للجيل الرابع وذلك عبر تفعيل الذكاء الاصطناعي خاصة في مجال الأمن السيبراني. كما هدفت هذه الدراسة الى جانب سعيها لدعم البحث العلمي والتطبيقي في أرض الواقع، من خلال تشجيع المشاريع المرتبطة باستخدام الذكاء الاصطناعي في الكشف عن التهديدات السيبرانية والتنبؤ بها مستقبلا.

ويعكس إنشاء هذه المؤسسة إدماج الذكاء الاصطناعي ضمن المقاربة الحديثة للأمن السيبراني، حيث أصبح يشكل أداة استراتيجية في تعزيز قدرات الكشف المبكر عن الهجمات وتحليل السلوكيات غير الطبيعية داخل الأنظمة المعلوماتية. كما يُبرز هذا التوجه سعي الجزائر إلى تحقيق التكامل بين التكوين الأكاديمي والتطور التكنولوجي، بما يدعم بناء منظومة سيبرانية متطورة ومستدامة. (منظمة التعاون الاقتصادي والتنمية، 2022) الذكاء الاصطناعي لم يعد مجالا منفصلا، بل أصبح أداة داعمة للأمن السيبراني. (وزارة التعليم العالي والبحث العلمي، 2021)

الفرع الثاني: الهيئات الأمنية والعسكرية

1. وزارة الدفاع الوطني ومركز الاشراف السيبراني: تلعب وزارة الدفاع الوطني دورا محوريا في مجال الأمن السيبراني، لاسيما عبر مديرياتها التقنية والاستخبارتية، التي تعني برصد

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

التحديات الخارجية المحتملة التي تستهدف البنى التحتية الرقمية للدولة، خصوصاً تلك ذات الطابع الاستراتيجي (الطاقة، الاتصالات، النقل...).

كما عملت الوزارة على تطوير مركز إشراف سيبراني يتولى مراقبة الفضاء الرقمي الوطني، واكتشاف محاولات الاختراق والهجمات الإلكترونية في الزمن الحقيقي، مع العمل على تعزيز قدرات الحماية والرد السيبراني. (غازي، 2016)

1. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن السيبراني:

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت تكييف على الشكل الأمني الخاص بمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال بقرار من المدير العام للأمن الوطني واذيف الهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.

الجدول رقم 3: يوضح عدد القضايا المعالجة من طرف المديرية العامة للأمن الوطني

السنة	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	31	31
2008	06	10
2009	29	21
2014	245	/
2015	409	347

المصدر: (حملوي، 2015)

تظهر هذه المعطيات المتعلقة بعدد القضايا المعالجة من طرف المديرية العامة للأمن الوطني انتشار الجرائم المعلوماتية وتنامي استخدامها في الفضاء الرقمي. كما يشير على تطور تصاعدي في تدخلات المصالح الأمنية من حيث المعالجة، مع استمرار في تعزيز الوسائل التقنية والبشرية لمواكبة هذا النوع من الجرائم.

المطلب الثاني: التنسيق المؤسسي وآليات العمل المشترك

التنسيق والتعاون بين مختلف الفاعلين من العناصر الأساسية في بناء منظومة الأمن السيبراني، بالنظر إلى الطبيعة المعقدة والمتداخلة ويحدث من تغيرات للتهديدات الرقمية. كما تسعى الجزائر إلى تطوير آليات التنسيق، سواء على المستوى الداخلي بين المؤسسات الوطنية، أو على المستوى الخارجي من خلال الانخراط في التعاون الدولي.

الفرع الأول: التعاون بين الوزارات والمؤسسات.

أكد المشرع الجزائري من خلال القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أهمية التنسيق والتعاون بين مختلف الهيئات والسلطات المختصة، من أجل تعزيز مكافحة الجرائم الإلكترونية وحماية الأنظمة المعلوماتية. ويظهر ذلك من خلال تبادل المعلومات والتنسيق في إجراءات التحري والمتابعة، بما يساهم في رفع فعالية مواجهة التهديدات السيبرانية داخل الدولة. (قانون رقم 04-09، 2009)

القانون 04-09 لا يهتم فقط بمعاقبة الجرائم المعلوماتية، لكنه يهتم بالعمل بالتعاون بين المؤسسات والوزارات، ويعنى ذلك بأن الدولة تعرف أن الجرائم السيبرانية معقدة جدا ولا تستطيع الجهة واحدة القيام بها بل تحتاج الى التعاون والتنسيق مثال الشرطة، القضاة، الوزارات والمؤسسات التقنية وكل هذه الجهات تعمل عبر تبادل المعلومات فيما بينهم ويتعاونون في التحقيقات كلها تتم عبر التعاون والتنسيق الجيد.

الفرع الثاني: التنسيق مع الهيئات الدولية

ضمن البعد التعاوني، تسعى الجزائر الى الانخراط في أطر إقليمية لمواجهة التهديدات الرقمية، من خلال

- التعاون مع الاتحاد الافريقي في إطار "الاتفاقية النموذجية وحول الأمن السيبراني" (مالابو 2014)

- التنسيق مع الجامعة العربية والأمم المتحدة في إعداد استراتيجيات مشتركة للتصدي للتهديدات العابرة للحدود

- يظهر استعراض دور المؤسسات الحكومية الجزائرية في حماية البنية التحتية السيبرانية أن الجزائر تسير بخطى متسارعة، وإن كانت متفاوتة، نحو ترسيخ ثقافة الأمن السيبراني كأولوية وطنية. ويتضح من خلال الإطار التشريعي والتنظيمي أن الدولة الجزائرية أصبحت واعية بكون الأمن السيبراني لم يعد مسألة تقنية فحسب، بل يمثل بعداً من أبعاد الأمن القومي الشامل، بالنظر الى تهديدات السيبرانية المتزايدة التي تمس استقرار الدولة، وسلامة مؤسساتها، ثقة المواطنين في الخدمات العامة.

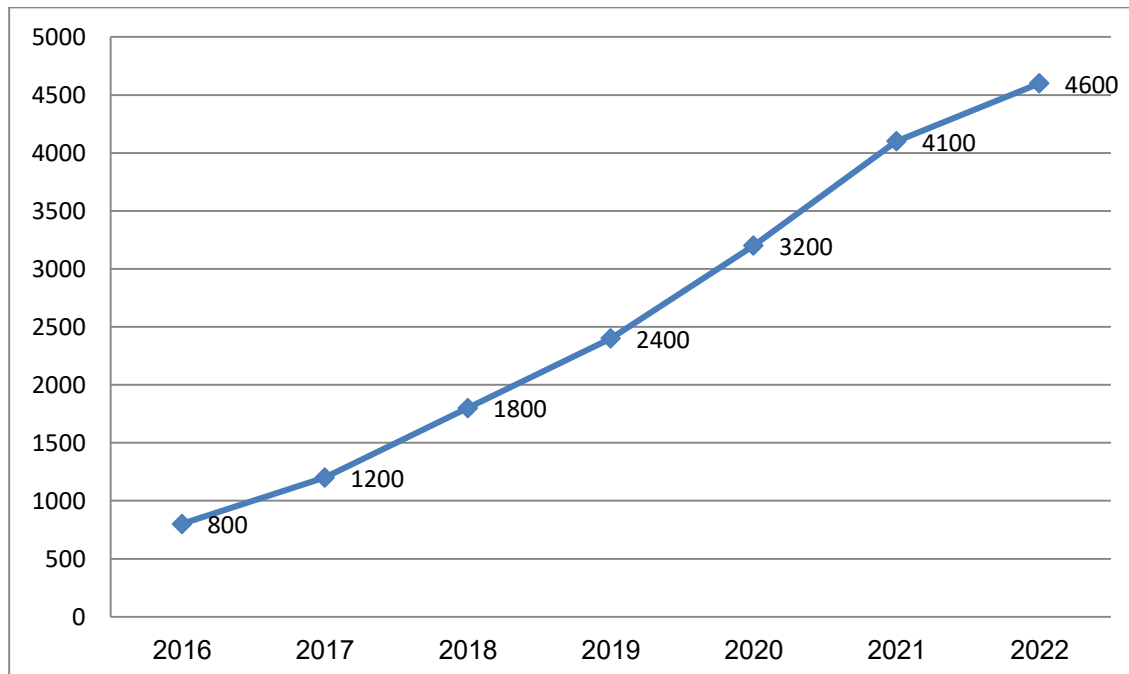
- على الصعيد المؤسسي، يبدو أن الجزائر تتبنى مقاربة أمنية دفاعية تقليدية، حيث لايزال العبء الأكبر في مكافحة التهديدات السيبرانية يقع على عاتق المؤسسات العسكرية وشبه العسكرية، مثل وزارة الدفاع ومديرية الأمن الداخلي، في حين أن المقاربة الشاملة للأمن السيبراني، التي تستند الى إشراك المجتمع المدني، والقطاع الخاص، والمؤسسات البحثية، ما زالت في طور التشكل. هذا يعكس تحدياً في الانتقال من سياسة حماية الى سياسة صمود سيبراني شامل. (شايب، 2024)

المطلب الثالث: فعالية الأداء المؤسسي

فعالية الأداء المؤسسي في مجال الأمن السيبراني عنصرا أساسيا لفهم مدى قدرة منظومة الوطنية على تحقيق حماية فعالة لأنظمة المعلوماتية في مواجهة التهديدات الرقمية. وعليه يتناول هذا المطلب إلى تقديم مؤشرات وإحصائيات وتحليل مستوى فعالية الأداء المؤسسي في الجزائر من خلال إبراز نقاط القوة التي تدعم المنظومة الوطنية، مقابل نقاط الضعف التي تحد من كفاءتها.

الفرع الأول: نقاط القوة

الشكل رقم 9: تطور عدد القضايا السيبرانية المعالجة في الجزائر خلال الفترة 2016-2022.



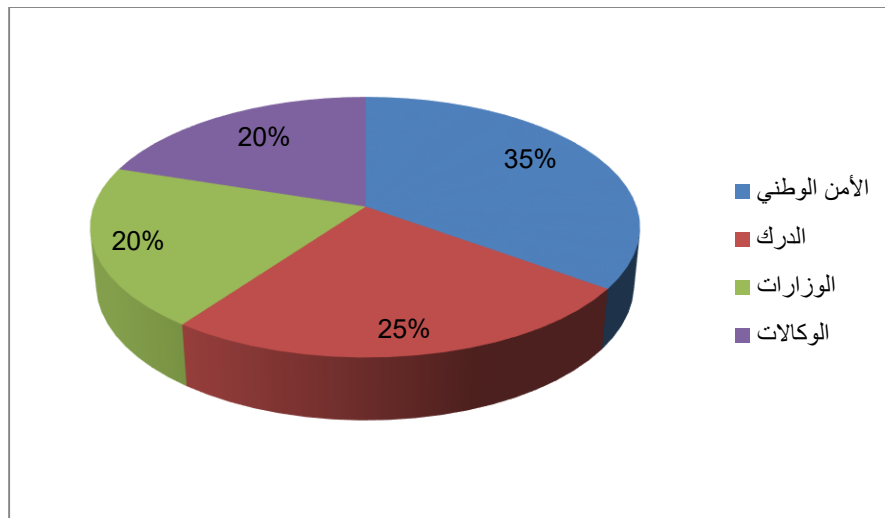
المصدر: من إعداد الطالبة اعتماداً على تقارير المديرية العامة للأمن الوطني، 2022.
اعتماداً على (المديرية العامة للأمن الوطني، 2022)

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

يعكس الشكل (1) منحنى تصاعدي في عدد القضايا السيبرانية المعالجة خلال الفترة 2016-2022، حيث انتقل العدد من مستويات محدودة إلى تسجيل آلاف القضايا سنوياً. ويفسر هذا الارتفاع من جهة بتزايد استخدام الوسائط الرقمية في الجزائر، ومن جهة أخرى بتطور قدرات الأجهزة الأمنية، خاصة التابعة لـ المديرية العامة للأمن الوطني، في كشف وتتبع الجرائم الإلكترونية.

كما يدل هذا التطور على أن المنظومة السيبرانية الوطنية أصبحت أكثر فعالية في رصد التهديدات، رغم أن هذا الارتفاع يعكس أيضاً زيادة في حجم وتعدد الهجمات السيبرانية. وما تتعرضه الجزائر من هجمات وتهديدات

الشكل رقم 10: توزيع المؤسسات الفاعلة في مجال الأمن السيبراني في الجزائر



المصدر: من إعداد الطالبة بالاعتماد على معطيات رسمية لسنة 2022 على تقارير وزارة الدفاع الوطني، وتقارير المديرية العامة للأمن الوطني، وتقارير الدرك الوطني الجزائري.

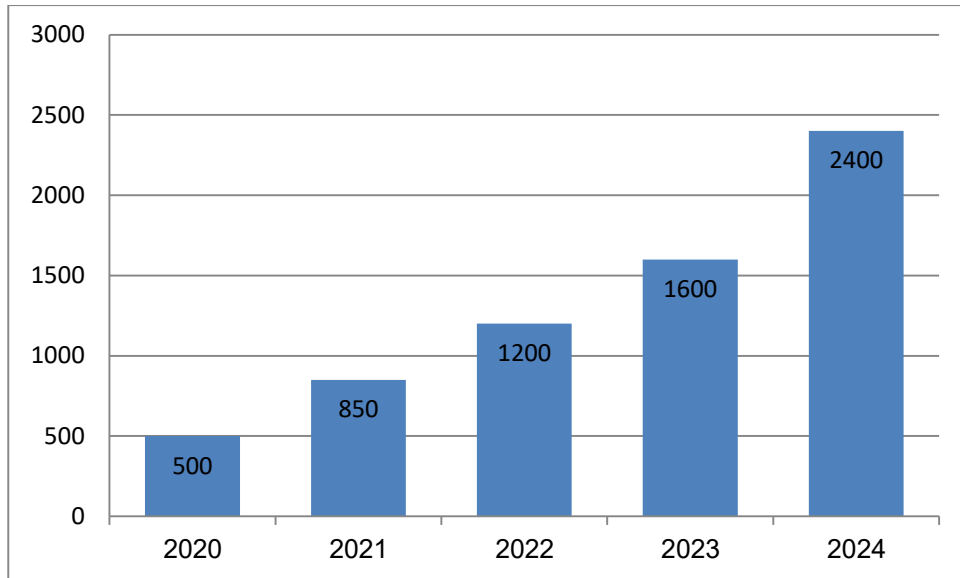
يتميز الشكل (2) توزيعاً مؤسسياً متعدد الأطراف في مجال الأمن السيبراني بالجزائر، حيث يتصدر المديرية العامة للأمن الوطني الدور الأكبر في مكافحة الجرائم الإلكترونية، تليها الدرك الوطني الجزائري، ثم المؤسسات التقنية والوزارية.

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

ويُظهر هذا التوزيع أن منظومة الأمن السيبراني في الجزائر تقوم على مبدأ التكامل الوظيفي بين الفاعلين الأمنيين والتقنيين، بما يسمح بتوزيع الأدوار حسب طبيعة المهام.

كما يدل ذلك على أن الأمن السيبراني لم يعد مقتصرًا على الأجهزة الأمنية فقط، بل أصبح مجالًا تشترك فيه عدة قطاعات حكومية.

الشكل رقم 11: تطور عدد الطلبة في تخصصات الأمن السيبراني والذكاء الاصطناعي في الجزائر 2020 - 2024.



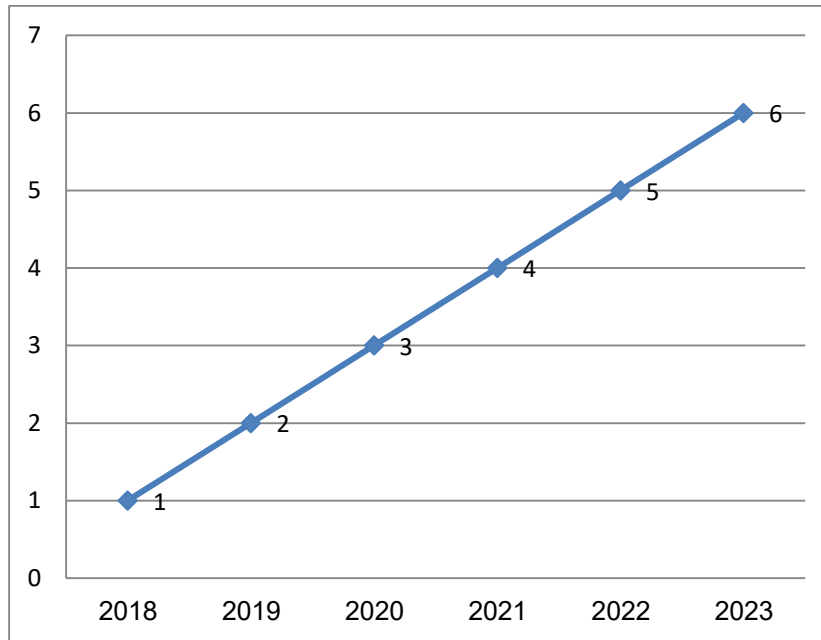
المصدر: من إعداد الطلبة اعتماداً على تقارير وزارة التعليم العالي والبحث العلمي، الجزائر، 2023، ومعطيات حول المدرسة الوطنية العليا للأمن السيبراني والمدرسة العليا للذكاء الاصطناعي.

يبين الشكل (3) تطوراً ملحوظاً في عدد الطلبة المسجلين في تخصصات الأمن السيبراني والذكاء الاصطناعي خلال الفترة 2020-2024، حيث ارتفع العدد بشكل تدريجي من بضع مئات إلى أكثر من ألفي طالب. ويعكس هذا التوجه اهتمام الدولة الجزائرية بتعزيز التكوين في المجالات الرقمية.

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

كما يرتبط هذا التطور بإنشاء مؤسسات متخصصة، مثل المدرسة الوطنية العليا للأمن السيبراني والمدرسة الوطنية العليا للذكاء الاصطناعي، التي تهدف إلى تكوين كفاءات قادرة على مواجهة التهديدات السيبرانية. حيث أصبحت الجزائر تعتمد على الاستثمار في الموارد البشرية كركيزة أساسية لتعزيز أمنها السيبراني، وهو عنصر حاسم في بناء منظومة رقمية فعالة ومستدامة.

الشكل رقم 12: تطور مستوى الاستجابة للحوادث السيبرانية في الجزائر (2018-2023)



المصدر: من إعداد الطالبة اعتماداً على تقارير الاتحاد الدولي للاتصالات، 2021، وتقارير المديرية العامة للأمن الوطني، الجزائر، 2022، ومعطيات وكالة أمن الأنظمة المعلوماتية.

يبين الشكل (4) تحسناً تدريجياً في مستوى الاستجابة للحوادث السيبرانية في الجزائر، حيث انتقل من مستوى ضعيف خلال سنة 2018 إلى مستوى جيد جداً في سنة 2023. ويعكس

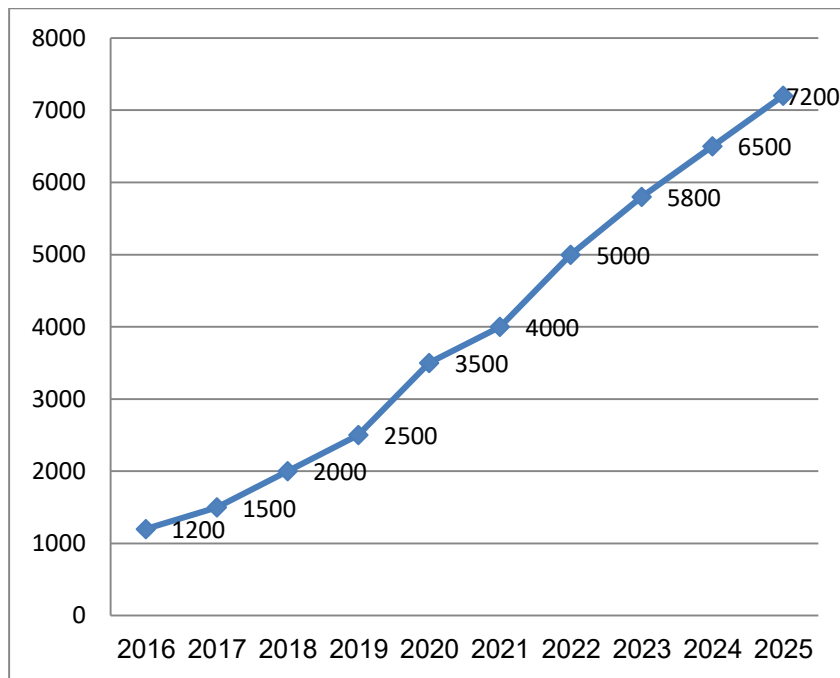
الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

هذا التطور الجهود المبذولة من طرف المؤسسات الأمنية والتقنية لتعزيز جاهزيتها في مواجهة التهديدات الرقمية.

كما يرتبط هذا التحسن بتعزيز التنسيق بين مختلف الفاعلين، مثل المديرية العامة للأمن الوطني ووكالة أمن الأنظمة المعلوماتية، إضافة إلى تطوير آليات الاستجابة للحوادث

الفرع الثاني: نقاط الضعف

الشكل رقم 13: تطور عدد الهجمات السيبرانية في الجزائر خلال الفترة 2016 - 2025.



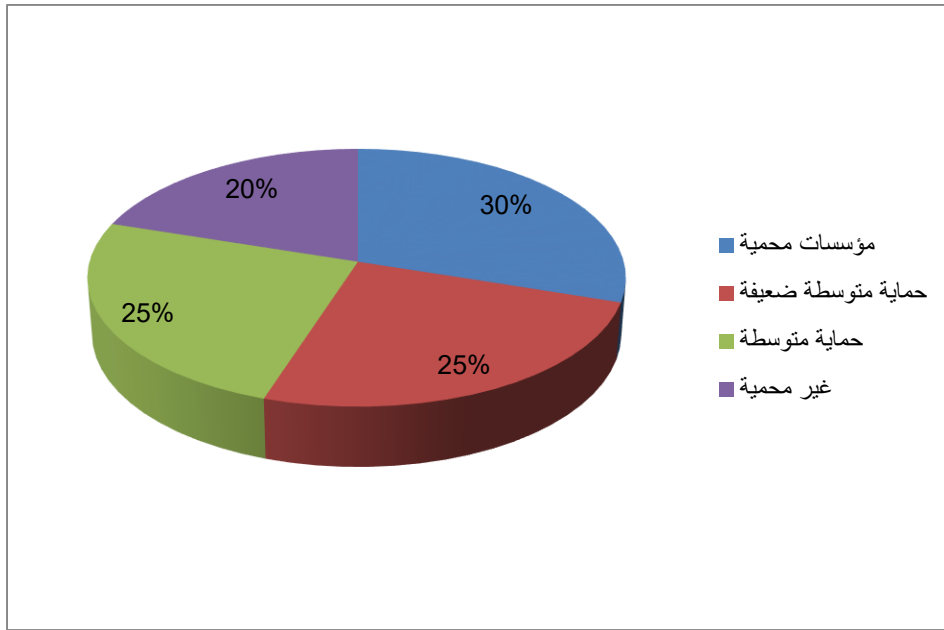
المصدر: من إعداد الطالبة اعتماداً على تقارير المديرية العامة للأمن الوطني، حصيلة الجرائم الإلكترونية، الجزائر، وتقارير الدرك الوطني الجزائري، 2023، مع إسقاطات تقديرية إلى غاية 2025.

يبين الشكل (1) المؤشرات في تزايد مستمر في عدد الهجمات السيبرانية التي تستهدف مختلف القطاعات في الجزائر، بما في ذلك المؤسسات الحكومية والخدمات الرقمية، وهو ما

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

يظهر من خلال المنحنى التصاعدي لعدد القضايا المسجلة (المديرية العامة للأمن الوطني، حصيلة الجرائم الإلكترونية، الجزائر، 2022). وهذا المؤشر يدل على أن وتيرة التهديدات تتجاوز أحياناً قدرة المؤسسات على الاحتواء، مما يعكس فجوة بين تطور الهجمات ومستوى الحماية.

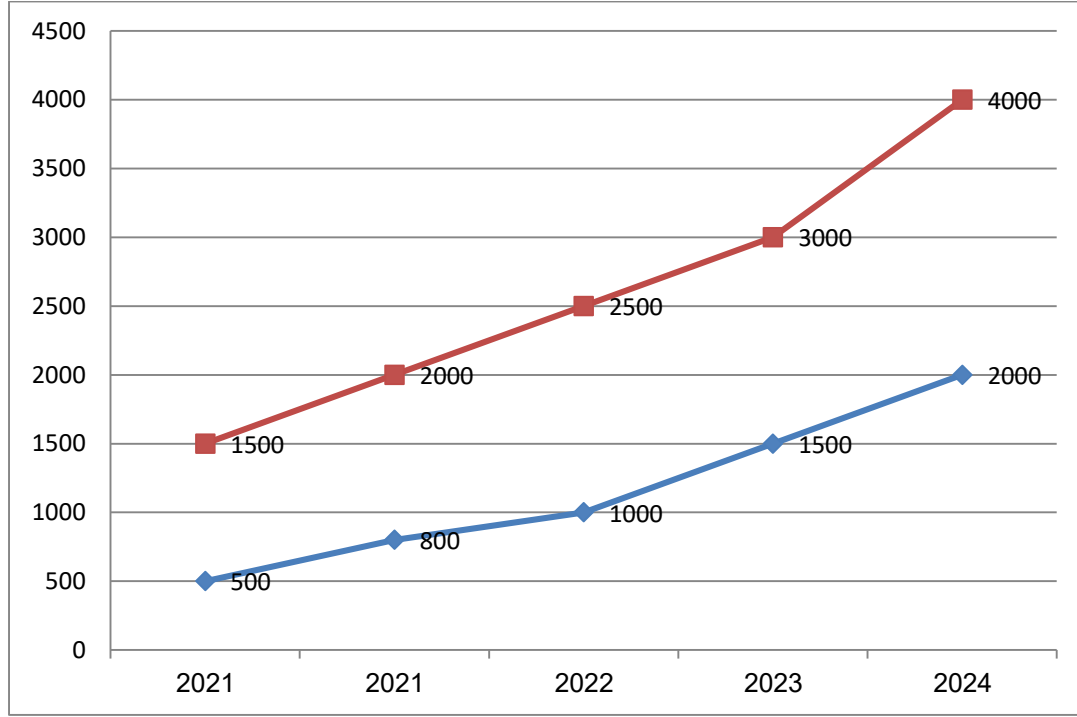
الشكل رقم 14: توزيع المؤسسات في الجزائر حسب مستوى الحماية السيبرانية



المصدر: من إعداد الطالبة اعتماداً على تقارير الاتحاد الدولي للاتصالات، مؤشر الأمن السيبراني العالمي، 2021، ومعطيات وطنية حول الأمن الرقمي في الجزائر.

يبين الشكل (2) رغم وجود مؤسسات متخصصة، إلا أن نسبة المؤسسات التي تعتمد على أنظمة حماية متقدمة لا تزال محدودة، خاصة في بعض القطاعات الحيوية، وهو ما يؤثر على مناعة الفضاء السيبراني الوطني. يعكس هذا التفاوت ضعفاً في تعميم ثقافة الأمن السيبراني، مما يؤدي إلى وجود نقاط ضعف يمكن استغلالها من قبل الجماعات الإجرامية العابرة للحدود الرقمية.

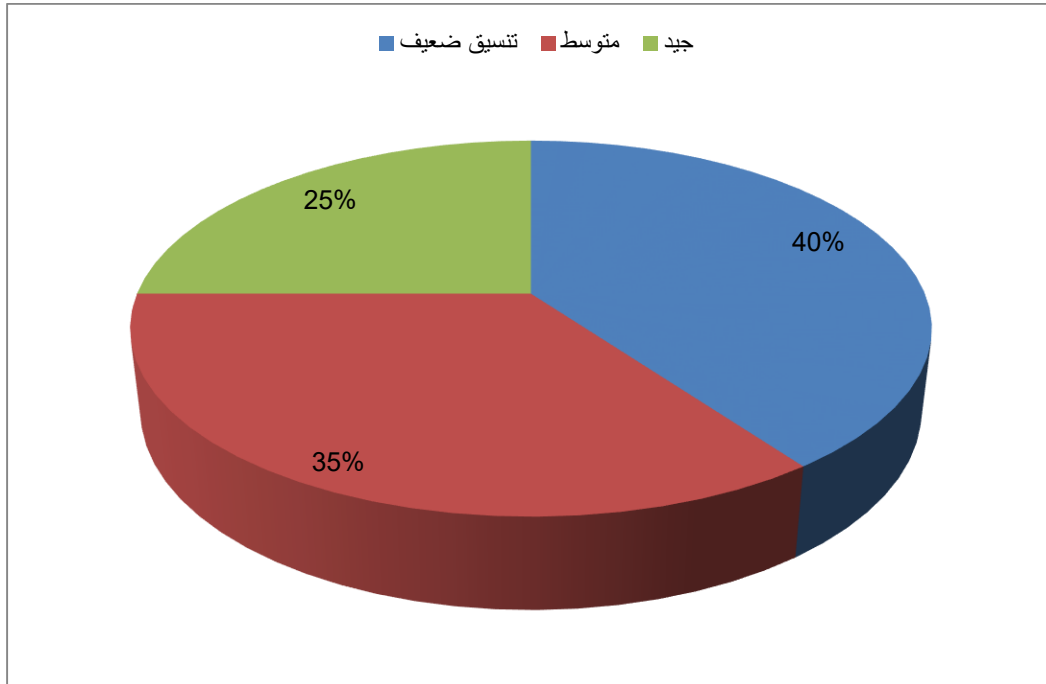
الشكل رقم 15: الفجوة بين احتياجات سوق العمل وعدد المختصين في الأمن السيبراني في الجزائر.



المصدر: من إعداد الطالبة اعتماداً على تقارير وزارة التعليم العالي والبحث العلمي، الجزائر، 2023، ومعطيات حول المدرسة الوطنية العليا للأمن السيبراني.

يبين الشكل (3) الجهود المبذولة في مجال التكوين، إلا أن الطلب المتزايد على الخبرات في الأمن السيبراني يفوق عدد الكفاءات المتخرجة سنوياً خاصة في مجالات متقدمة مثل تحليل الهجمات والاستجابة للحوادث، وهذه الفجوة تشير إلى أن بناء القدرات البشرية لا يزال غير كاف لمواكبة التحديات، مما قد يؤثر على فعالية الأداء المؤسسات.

الشكل رقم 16: مستوى التنسيق بين المؤسسات في مجال الأمن السيبراني في الجزائر.



المصدر: من إعداد الطالبة اعتماداً على تقارير الاتحاد الدولي للاتصالات، 2021، وتقارير حول التنسيق المؤسسي في الجزائر.

يبين الشكل (4) وجود تعددية مؤسساتية، إلا أن التنسيق بين مختلف الهيئات لا يزال يواجه بعض الصعوبات وتحديات عديدة، خاصة فيما يتعلق بسرعة تبادل المعلومات بين مختلف المؤسسات حول التهديدات السيبرانية، وهو ما قد يؤثر على سرعة الاستجابة والتنسيق. إلا أن ضعف التنسيق من أبرز التحديات التي تواجه فعالية الأداء المؤسسي، حيث يؤدي إلى تأخر في اتخاذ القرار الأمني وتقليل فعالية التدخل.

المبحث الثالث: التحديات والتهديدات المؤثرة على الأمن السيبراني.

في ظل التحول الرقمي المتسارع، يشهد الفضاء السيبراني تزايدا ملحوظا في حجم وتعقيد التهديدات السيبرانية، مما يفرض تحديات جديدة على الجزائر في سبيل تأمين أنظمتها المعلوماتية وحماية بنيتها التحتية الرقمية، حيث تواجه جملة من المخاطر السيبرانية التي تتنوع بين الهجمات الإلكترونية، والجرائم المعلوماتية، ومحاولات الاختراق التي تستهدف المؤسسات والبيانات الحساسة.

وعليه، يهدف هذا المبحث إلى تحليل أهم أبرز التحديات والتهديدات التي تؤثر على الأمن السيبراني في الجزائر، من خلال التركيز على طبيعتها ومصادرها، ومدى انعكاسها على فعالية المنظومة السيبرانية الوطنية.

المطلب الأول: التحديات التقنية - القانونية - البشرية.

التحديات التي تواجه الأمن السيبراني متعددة الأبعاد، حيث لا تقتصر على الجانب التقني فقط، بل تشمل أيضًا أبعادًا قانونية وبشرية تؤثر بشكل مباشر على فعالية المنظومة السيبرانية، حيث ان الجزائر تسعى الى مواجهة هذه التحديات من خلال تطوير قدراتها، غير أن طبيعة التهديدات المتغيرة والبيئة تفرض صعوبات مستمرة تتطلب معالجة شاملة ومتكاملة.

الفرع الأول: التحديات التقنية.

تعاني الجزائر من نقص كبير في الاستثمارات الموجهة لتحديث البنية التحتية الرقمية، ما يشكل تحدياً كبيراً أمام تطور الأمن السيبراني في البلاد. على الرغم من الجهود التي تبذلها الحكومة في هذا المجال، فإن حجم الاستثمارات في قطاع التكنولوجيا لا يزال ضئيلاً مقارنة بالدول المجاورة. تشير بيانات "البنك الدولي" الى أن الجزائر أنفقت 0.7 % فقط من ناتجها

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

لمحلي الإجمالي على تطوير التكنولوجيا الرقمية في عام 2022، وهو أقل بكثير من المتوسط العالمي 2.5%. (البنك الدولي، 2023)

قلة الاستثمارات تتجلى في ضعف شبكات الاتصالات وعدم تحديث مراكز البيانات الحكومية، مما يترك المؤسسات الحيوية عرضة للتهديدات السيبرانية. فوفقاً لتقرير "الهيئة الوطنية للأمن السيبراني"، تعتمد العديد من المؤسسات في الجزائر على أنظمة قديمة وغير مؤهلة للتصدي للهجمات الالكترونية الحديثة، ما يجعلها عرضة للاختراقات والقرصنة. (بوعرعار، 2025)

الفرع الثاني: التحديات القانونية

تفعيل القوانين على أرض الواقع وتطبيقها بصرامة: إذ من بين أكبر الإشكالات التي تسهم في انتشار الجريمة الالكترونية، هو الإفلات من العقاب، والتأخر في تفعيل القوانين، وهو يمنح المجرم فرصاً لتكرار جرائمه، ولذلك من الضروري تأكيد على تطبيق القوانين، كما يجب أن تتكيف النصوص القانونية مع التغيرات الحاصلة في هذا المجال، كما يتوجب إنشاء محاكم متخصصة بالجرائم الالكترونية، نظراً للانتشار الواسع لهذا الجرائم. (بارة، الأمن السيبراني في الجزائر: السياسات والمؤسسات، 2017)

غياب التنسيق بين الدول والحكومات: إذ من المعلوم أن الجريمة الالكترونية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ الى أنظمة الحاسوب في أنظمة الحاسوب في أحد الدول، ليتم التلاعب واختراق البيانات في بلد آخر. (بوعرعار، 2025)

التطور التكنولوجي في مجال الانترنت والاتصالات: وهو ما يفرض على الأجهزة الأمنية المختصة بأن تسير هذا التطور، سواء من حيث اكتساب التكنولوجيا والتقنية أو من حيث التمكن من استخدامها واستثمارها بالشكل اللازم، وهذا قد يرهق ميزانياتها المحدودة، ولذلك يتوجب توفير جميع الإمكانيات المادية والبشرية اللازمة للتحقيق الأمن السيبراني.

الفرع الثالث: التحديات البشرية

يعد نقص الوعي والتدريب أحد أبرز التحديات التي تواجه الأمن السيبراني في الجزائر. فمع تصاعد وتيرة الهجمات الإلكترونية، تبين أن العديد من المؤسسات والأفراد ليس لديهم الوعي الكافي بأهمية الأمن السيبراني وطرق الحماية منه. وفقا لدراسة أجرتها "الهيئة الوطنية للأمن السيبراني" في عام 2022، تبين أن حوالي 70% من المؤسسات الجزائرية لا تعتمد برامج تدريبية منتظمة لتوعية الموظفين بأحدث التهديدات السيبرانية وطرق التصدي لها. (الهيئة الوطنية للأمن السيبراني، 2022)

هذا النقص في التدريب لا يقتصر فقط المؤسسات الحكومية، بل يشمل أيضا القطاع الخاص، خاصة الشركات الصغيرة والمتوسطة التي تمثل جزءاً كبيراً من الاقتصاد الوطني. وفقاً لتقرير "منتدى الجزائر للتكنولوجيا"، أظهرت الدراسة أن 80% من الشركات الصغيرة والمتوسطة في الجزائر لا تملك فرقاً متخصصة في الأمن السيبراني، مما يزيد من تعرضها للهجمات الإلكترونية. (منتدى الجزائر للتكنولوجيا، 2021)

المطلب الثاني: التهديدات السيبرانية التي تواجه المؤسسات الوطنية

تتعرض المؤسسات الوطنية في الجزائر، على غرار باقي دول العالم، لمجموعة متزايدة من التهديدات السيبرانية التي تختلف من حيث مصدرها وطبيعتها، حيث يمكن تصنيفها إلى تهديدات داخلية ناتجة عن عوامل بشرية أو تنظيمية داخل المؤسسة، وتهديدات خارجية مصدرها جهات أو أطراف خارجية تسعى لاختراق الأنظمة المعلوماتية أو استهداف البيانات.

الفرع الأول: التهديدات السيبرانية الخارجية

منذ الاستقلال، سعى النظام السياسي الجزائري الى الحفاظ على سيادته واستقلال قراره السياسي، خاصة في ظل الإرث الاستعماري الثقيل والتجاذبات الجيوسياسية الإقليمية

والدولية. إلا أن الجزائر، كغيرها من الدول النامية ذات الأهمية الاستراتيجية، لم تسلم من محاولات التدخل الخارجي المباشر وغير المباشر، سواء عبر الضغوط الدبلوماسية أو الاقتصادية أو من خلال أدوات "القوة الناعمة" والرقمية.

أولاً: اختراق الوكالة الوطنية للأخبار

تعد وكالة الأنباء الجزائرية المنصة الرسمية الأساسية التي تنقل الأخبار والمواقف الرسمية للدولة. ومن هذا المنطلق، فإن محاولة اختراقها لا يعد حدثاً عابراً، بل هو عمل عدائي سيبراني موجه يمس صميم السيادة الوطنية. إذ إن قواعد بيانات الوكالة تحتوي على:

- مراسلات رسمية مع مؤسسات الحكومية وسياسية.
- مواقف دبلوماسية لم تعلن بعد.
- مخططات إعلامية متصلة بالأمن الداخلي والخارجي.

وفي حال تمكن المخترقون من الوصول الى هذه البيانات أو نشر أخبار مزيفة، فإن الضرر قد يمتد الى افتعال أزمات دبلوماسية، كما حدث في أزمة اختراق وكالة الأنباء القطرية "قنا" سنة 2017، حيث أدت تصريحات مفبركة نسبت للأمير قطر الى اندلاع أزمة الخليج، وحصار سياسي واقتصادي لقطر من طرف السعودية والامارات والبحرين.

ثانياً: اختراق حساب وزارة العدل

حادثة اختراق حساب وزارة العدل الجزائرية على "تويتر" من طرف قراصنة مغاربة حملت أبعاداً جيوسياسية خطيرة. فقيام القراصنة بنشر عبارات مؤيدة للحرب الروسية على أوكرانيا اعتبر من طرف السفارة الأوكرانية في الجزائر تصريحاً رسمياً قد يستدعي رداً دبلوماسياً. ومثل هذا التصرف يظهر أن السيطرة على وسائط التواصل الرسمية للدول قد تستخدم

كأدوات استفزاز واستفحال التوترات الدولية، لا سيما عندما يكون البلد المستهدف في موقع الحيادة أو التوازن. (شايب، 2024)

وأكدت فضيحة "بيغاسوس" التي استخدم فيها المخزن وأجهزته الاستخبارية نظام برمجيات NSO الإسرائيلية للتجسس "بيغاسوس (pegasus)" الصهيوني، للتجسس على سياسيين وإعلاميين جزائريين، وغيرهم من السياسيين والناشطين والإعلاميين داخل المغرب أيضا وفي أوروبا، وهو ما كشفت عنه التسريبات التي نشرتها 17 مؤسسة إعلامية دولية بتعاون مع مؤسسة "forbidden stories"، وأكدت أن الجهة الأكثر استهدافا بهذا البرامج الخبيث كانت الجزائر وأجهزتها الرسمية.

وبذلك يشكل المغرب ودولة الكيان أسوأ أنواع التحالفات خاصة في المجال السيبراني، حيث وقعت اتفاقية تعاون في مجال الحرب الالكترونية، والمستهدفة بذلك بطبيعة حال الجزائر بالدرجة الأولى، كما يضاف لهذا الثنائي، طرف الثالث لا يمكن تأمين الجزائر شره، وهو طرف الفرنسي، والذي أثبت مؤخرا من خلال عملية تهريب بوراوي، والتي اعقبها مباشرة الهجوم السيبراني على وكالة الأنباء الجزائرية. وأمام هذه التهديدات المتزايدة في مجال الحرب السيبرانية التي تستهدف الجزائر بضرورة ووحشية، أكدت الدولة الجزائرية عبر عديد من المناسبات إدراكها لحجم التحديات التي يفرضها مثل هذا النوع من الحروب الحديثة، وقد أعدت لها عدتها باعتبارها جزءا أساسيا م استراتيجية الدفاع الوطني الشامل. (شايب، 2024)

ثالثا: اختراق البيانات الحكومية الجزائرية

في العصر الرقمي الذي نعيشه، أصبحت البيانات الحكومية تمثل أحد أعمدة السيادة الوطنية، وأي اختراق لها لم يعد مجرد مسألة أمن معلوماتي، بل تهديد مباشر للنظام السياسي واستقراره. وتشكل الهجمات السيبرانية على قواعد بيانات الوزارات والمؤسسات

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

الرسمية الجزائرية أحد أبرز مظاهر هذا الخطر، إذ تسعى جهات خارجية أو تنظيمات غير شرعية الى زعزعة الثقة بين الدولة والمواطن، أو إحراج السلطات أمام الرأي العام الدولي. أو حتى تعطيل عمل المؤسسات السيادية.

ففي 25 ماي 2025، أعلنت السلطات الجزائرية عن إعفاء المدير العام لشركة "صيدال" الحكومية، عبد الواحد غريمس، وذلك عقب حادثة اختراق سيبراني كبيرة استهدفت قاعدة بيانات وزارة الصناعة الصيدلانية. وتعود هذه الهجمة الى مجموعة قرصنة مغربية تدعى MOR_H4X، والتي تمكنت من الوصول أكثر من 34 جيجابايت من البيانات السرية المتعلقة بالواردات الدوائية والصفقات التجارية الممتدة 2019 وأفريل 2024.

الحادثة التي وصفت بأنها الأخطر في تاريخ البنية السيبرانية لقطاع الصحة والصناعة الدوائية في الجزائر، دفعت الى موجة من ردود الفعل الرسمية، خاصة بعد أن عمدت المجموعة الى نشر الوثائق المسروقة على المنصات الرقمية، مما تسبب في حرج دبلوماسي واقتصادي واسع النطاق. وتسبب في زعزعة الثقة في المؤسسات الرسمية وإقالة المدير العام لصيدال لم تكن مجرد إجراء إداري، بل إشارة سياسية الى تحميل المسؤوليات حول القصور في الحوكمة السيبرانية فالاختراق لم يصب فقط شركة دوائية، بل كشف عن:

- ضعف في منظومة الأمن المعلوماتي بالقطاع الوزاري ككل.
- غياب استراتيجيات استباقية للتعامل مع الهجمات السيبرانية.
- هشاشة التنسيق بين المؤسسات الدولة في إدارة البيانات الحساسة. (شايب، 2024)

ومن هذا المنطلق، إن التهديدات الأمنية التي واجهتها الجزائر مؤخرا، مثل حملات التضليل الإعلامي، اختراق مع وكالة الأنباء الجزائرية، التجسس الرقمي عبر منظومة بيغاسوس، وتدخل في صلب ما يعرف ب التهديدات الهجينة واشكالية التعريف وأنماط المواجهة، أن التصدي لهذه المخاطر يتطلب تجاوز الأساليب الدفاعية التقليدية. وبدلا

من ذلك يدعو الى تبني استراتيجية المرونة الوطنية الشاملة، والتي تقوم على حماية المؤسسات الدولة تكنولوجيا وتوعية الجبهة الداخلية والشعب فكريا لمنع أي محاولة لزعزعة الاستقرار الوطني. (نوري و سليمان، 2021)

الفرع الثاني: التهديدات السيبرانية الداخلية

التهديدات السيبرانية الداخلية من أخطر التحديات التي تواجه المؤسسات في الجزائر، نظرا لارتباطها المباشر بالعنصر البشري داخل التنظيمات الإدارية والاقتصادية. وتتبع خطورة هذا النوع من التهديدات من كونه يصدر عن أفراد يمتلكون صلاحيات قانونية للوصول إلى الأنظمة المعلوماتية، ليس هذا فقط ولديهم خبرة في مجال اختراقات سواء للمؤسسات أو للمواطن وذلك عبر اختراقات بياناتهم شخصية، الأمر الذي يجعل اكتشافه أكثر تعقيدا وتأثيره أكثر عمقا مقارنة بالتهديدات الخارجية.

تعتبر الهجمات الداخلية (Insider Attacks) من أبرز التحديات التي تواجه الأمن السيبراني، تتبع هذه الهجمات من داخل المؤسسة نفسها، وتكون مدفوعة من طرف أفراد يعملون فيها. يتمثل هدف هذه العمليات في تسريب بيانات حساسة لشركات منافسة أو المؤسسات، مما يؤدي الى خسائر مالية كبيرة للشركة المستهدفة. كما لا ننسى من أبرز أمثلة في الجزائر حادثة تسريبات بكالوريا 2016.

كما يعتبر تصيد البيانات والمعلومات عملية احتيالية تعتمد على إرسال رسائل بريد إلكتروني مزيفة تبدو كأنها من مصادر موثوقة، بهدف سرقة بيانات حساسة مثل أرقام بطاقات الائتمان أو بيانات تسجيل الدخول. بمعنى آخر، يتم استغلال ضعف الثقافة الإلكترونية لدى الضحية أو عدم انتباهها للمعلومات المعروضة أمامها، مما يؤدي الى دفعها لمشاركة معلومات حساسة بإرادتها، مثل بيانات بطاقتها الانتمائية أو كلمات المرور الخاصة بالدخول الى المنصات الرقمية أو المواقع المختلفة. وتجدر الإشارة الى أن عمليات تصيد المعلومات

تعد من أكثر الهجمات الإلكترونية شيوعاً، حيث تمثل حوالي 80% من إجمالي الهجمات التي تستهدف الأفراد والمؤسسات. ووفقاً لتقديرات جوجل، يوجد أكثر من 2.1 مليون موقع مخصص لهذه العمليات الاحتيالية. (حبيبتي، 2019)

المبحث الرابع: الآفاق المستقبلية لتعزيز الأمن السيبراني الوطني

يشهد الأمن السيبراني تطورات متسارعة بفعل التحول الرقمي والتقدم التكنولوجي، ما جعله أحد أبرز التحديات الأمنية المعاصرة التي تواجه الدول ومن بينها الجزائر. وفي ظل هذا الواقع الذي نحن فيه، أصبحت الحاجة ملحة لتطوير السياسات الوطنية وتعزيز القدرات المؤسسية لمواكبة التهديدات السيبرانية المتصاعدة.

كما أضحى توظيف التقنيات الحديثة، خاصة الذكاء الاصطناعي، عنصراً أساسياً في دعم منظومات الحماية السيبرانية وتحسين قدرتها على الاستجابة للهجمات الرقمية. حيث يتناول هذا المبحث إلى دراسة الآفاق المستقبلية لتعزيز الأمن السيبراني في الجزائر من خلال تحليل التحولات التكنولوجية والجهود الوطنية، إضافة إلى استشراف مستقبل هذا المجال عبر تقديم توصيات واستراتيجيات قصيرة وطويلة المدى.

المطلب الأول: التحولات التكنولوجية في الأمن السيبراني

يجسد مجال الأمن السيبراني تحولات تكنولوجية متسارعة فرضتها الثورة الرقمية وتطور أنظمة المعلومات والاتصال، حيث أصبحت التهديدات الإلكترونية تتزايد بشكل مستمر، وهو الذي يجعل الأمن السيبراني موضوع مهم جداً في عصرنا الحالي. لهذا تسعى الدول ومن بينها الجزائر على مواكبة هذه التحولات التي نشهدها على مستوى الأفراد والمؤسسات، خاصة مع استخدام التقنيات الحديثة.

الفرع الأول: جهود الدولة الجزائرية في مجال الأمن السيبراني

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

أمام التهديدات والمخاطر المتزايدة التي تخلفها استخدام التكنولوجيا الحديثة في الجزائر فقد بات لزاما اعتماد سياسة أمنية وطنية تضع مسألة توفير الأمن السيبراني على رأس أولوياتها واستراتيجياتها، وذلك من خلال البحث عن آليات وميكانيزمات فعالة يمكن من خلالها إدارة مختلف الحروب السيبرانية سواء باعتماد سياسات وقائية أحيانا أو سياسات علاجية في أحيان أخرى.

قبل التطرق الى مختلف الجهود الجزائرية في مجال تحقيق الأمن السيبراني لا بد بداية من توضيح ترتيب بلدان منطقة الدول العربية من بينهم الجزائر حسب الرقم القياسي العالمي للأمن السيبراني، حيث احتلت الجزائر المرتبة 10 حسب التزامها بتلك التدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني على مستوى العربي مجال تحقيق الأمن السيبراني، كما هو موضح في الجدول التالي: (الاتحاد الدولي للاتصالات، 2015)

الجدول رقم 4: يوضح ترتيب بلدان منطقة الدول العربية حسب الرقم القياسي العالمي

لأمن السيبراني

الترتيب الاقليمي	الرقم القياسي	التعاون	بناء القدرات	تنظيمية	تقنية	قانونية	الدول العربية
1	0.7647	0.6250	0.7500	1.0000	0.6667	0.7500	عمان
2	0.6176	0.5000	0.6250	0.5000	0.8333	0.7500	قطر
3	0.5882	0.5000	1,0000	0.3750	0.5000	0.5000	مصر
4	0.5588	0.3750	0.5000	0.7500	0.6667	0.5000	المغرب
5	0.5294	0.5000	0.2500	0.5000	0.5000	1.0000	تونس
7	0.3529	12,50	0.5000	0.2500	0.3333	0.7500	الامارات العربية المتحدة
8	0.2941	0.2500	0.3750	0.1250	0.1667	0.7500	البحرين
9	0.2059	0.1250	0.0000	0.5000	0.0000	0.5000	الأردن
10	0.1765	0.2500	0.1250	0.0000	0.0000	0.7500	الجزائر
11	0.1471	0.0000	0.1250	0.3750	0.0000	0.2500	دولة فلسطين
12	0.0882	0.1250	0.2500	0.0000	0.0000	0.0000	لبنان

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

13	0.0588	0.1250	0.1250	0.0000	0.0000	0.0000	الكويت
13	0.0588	0.1250	0.0000	0.0000	0.0000	0.2500	اليمن
14	0.0294	0.1250	0.0000	0.0000	0.0000	0.0000	العراق

ومن خلال هذا الجدول يمكن القول أن جهود الجزائرية في مجال تحقيق الأمن السيبراني تبقى ضئيلة، حيث تركزت أساسا في مجال اتخاذ التدابير القانونية الأخرى، ويتضح ذلك من خلال صدور القانون رقم 04-09 المؤرخ في 5 أوت 2009، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم فيه تحديد الحالات التي تسمح باللجوء الى مراقبة الاتصالات الإلكترونية بناء على ما ورد في المادة 4 التي نصت على مايلي:

- للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء الى مراقبة الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، وهذا ما تم من خلال صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن المهام التي تمارسها الهيئة ما ورد في المادة 4 من المرسوم والتي نصت عليها مايلي: (15-261،

(2015)

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع معلومات والتزويد بها ومن خلال الخبرات القضائية.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- إضافة الى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد أنشأت الجزائر هيئات أخرى تضطلع بأدوار جد هامة في مواجهة مختلف الجرائم الالكترونية منها: (بوعلام، 2016)

- مركز الوقاية من الجرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

كما يأتي اهتمام الجزائر بإنشاء مثل هذه المؤسسات الى تزايد معدلات الجرائم الالكترونية التي أصبحت تشكل تهديدا كبيرا على الأمن الوطني، فقد ارتفع معدل الجرائم الإلكترونية في الجزائر بشكل كبير خلال السنوات الأخيرة حسب بعض التقارير الأمنية، حيث عرفت الجزائر تزايد كبير في جريمة الكترونية ويتعلق أبرزها بانتهاك الحريات الشخصية، والتهديد

عبر الانترنت، ونشر صور فاضحة، الابتزاز، والقرصنة الالكترونية وغيرها. (غازي، 2016)

نظرا لخطورة هذه التهديدات فقد أولت الجزائر أهمية كبيرة لمسألة تحقيق الأمن السيبراني، خاصة بعد دخول الجيل الثالث للانترنت وتنامي استخدام شبكات التواصل الاجتماعي، ويظهر ذلك إضافة الى اهتمامها بالجانب القانوني والمؤسسي الذي أشرنا اليه سابقا. (بوعلام، 2016)

الفرع الثاني: تطبيقات الذكاء الاصطناعي في الأمن السيبراني

وفقا لتقرير Capgemini Research Institute سنة 2024 حول تطورات الأمن السيبراني، فإن أهم ميزة رئيسية للذكاء الاصطناعي هي الأمن السيبراني.

• يمكن التعامل مع كميات كبيرة من البيانات

هناك الكثير من الأنشطة الجارية على خوادمنا، هذا يعني أنه يتم نقل كمية كبيرة من البيانات بين عملائنا ومنشأتنا وبين أجهزتنا وشبكاتنا كل يوم، وهذا يعني أن محلي الأمن السيبراني لا يمكنهم التحقق من كل شيء وبيانات عن المخاطر المحتملة، والذكاء الاصطناعي هو الخيار الأفضل لاكتشاف هذه التهديدات التي تمر عبر الأنشطة اليومية.

• توقع تهديدات المستقبلية

إن كمية البيانات التي تمر عبر محلي الأمن السيبراني تجعل من الصعب التنبؤ بالتهديدات المستقبلية، لكن الذكاء الاصطناعي يمكنه معالجة كميات كبيرة من البيانات في وقت واحد، مما يتيح الكشف المبكر عن الأنشطة الضارة، وأخذ تدابير وقائية من أجل حماية المؤسسات.

• تقليل وقت الذكاء الاصطناعي

القدرة على اكتشاف التهديدات بسرعة أمر بالغ الأهمية، حيث أبلغ 42% من المنظمات عن زيادة في التهديدات الحساسة للوقت، والناس بطيئون في تبنيها وهم دون المستوى الأمثل، ومن ناحية أخرى، يمكن للذكاء الاصطناعي فحص كميات كبيرة من البيانات في وقت واحد لاكتشاف التهديدات السيبرانية. (دهماني، 2023)

• التوفير في التكاليف

تتأثر العديد من المؤسسات ماليا بانتهاكات البيانات كل عام، ولا يمكننا تجاهلها ولا يمكننا إيقاف المجرمين، حيث وجدت الدراسة فرقا بنسبة 80% في توفير التكاليف للمنظمات التي تستخدم الذكاء الاصطناعي لأغراض الأمن السيبراني، 2.9 مليون دولار مقارنة بـ 6.71 مليون دولار للمرافق التي لا تستخدم الخدمة.

أهم تقنيات الذكاء الاصطناعي التي لها تأثير فعال نجد ChatGPT، وعلى الرغم من المخاوف بشأن مخاطر الذكاء الاصطناعي التي لها تأثير فعال نجد ChatGPT أداء مفيدة لصناعة الأمن، واستخدام ChatGPT له فوائد عديدة في زيادة الإنتاجية، ومساعدة المهندسين، وتدريب الموظفين، وإنفاذ القانون.

إن تطوير ChatGPT سيعمل على تحسين قدرة الصناعة على اكتشاف الهجمات الإلكترونية والاستجابة لها في الوقت الفعلي، وبالتالي تعزيز مرونة الأمن السيبراني بشكل عام.

كما أبرز التحديات التي تواجه الذكاء الاصطناعي في الأمن السيبراني. (دهماني، 2023)

- يأتي دمج الذكاء الاصطناعي في أنظمة الأمن السيبراني مصحوبا بالعديد من العقبات والقيود الأكثر شيوعا هي الحواجز التي تحول دون استخدام واعتماد الذكاء الاصطناعي من قبل مجرمي الانترنت.

- يعد الذكاء الاصطناعي صناعة جديدة ويجب على المؤسسات استثمار أموال ووقت كبير في قوة الحوسبة والذاكرة ومراكز البيانات لتكون قادرة على بناء أنظمة الذكاء الاصطناعي وصيانتها.
- يزيد استخدام الذكاء الاصطناعي في هذه التقنية من دقة وفعالية الهجمات، مما يخلق تهديدات مدمرة، ويمكن أيضا استخدام الذكاء الاصطناعي في هجمات التصيد الاحتيالي.

المطلب الثاني: مستقبل الأمن السيبراني في الجزائر

في ظل التطورات التكنولوجية المتسارعة، أصبح الأمن السيبراني من أهم القضايا التي تفرض نفسها على الدول، خاصة مع تزايد الاعتماد على الأنظمة الرقمية في مختلف المجالات، حيث تسعى الجزائر إلى تعزيز قدراتها في هذا المجال لمواجهة التهديدات المتزايدة، وضمان حماية مؤسساتها وبنية التحتية الرقمية.

الفرع الأول: توصيات قصيرة المدى

مع تزايد التهديدات السيبرانية التي تشهدها الجزائر وتطور أساليبها، أصبح من الضروري على الجزائر اتخاذ مجموعة من الإجراءات العاجلة التي من شأنها تعزيز مستوى الأمن السيبراني ورفع درجة الجاهزية لمواجهة مختلف المخاطر الرقمية، خاصة مع تسارع الرهيب في وتيرة التحول الرقمي في العديد من القطاعات الحيوية.

تحديث القوانين المتعلقة بالجرائم الالكترونية بما يتماشى مع التطورات التكنولوجية وذلك من خلال سد الثغرات القانونية التي قد تستغل في تنفيذ الهجمات السيبرانية، من أجل حماية أفضل البيانات والمعلومات الحساسة.

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

تعزيز التنسيق بين مختلف الهيئات والمؤسسات المعنية بالأمن السيبراني، من أجل تحقيق استجابة سريعة في حال حدوث هجمات سيبرانية.

ينبغي العمل على أنظمة الحماية داخل المؤسسات، خاصة القطاعات الحساسة مثل شركة سونطرك وسونالغاز....، وذلك من خلال اعتماد على أدوات متطورة لرصد التهديدات والكشف المبكر عنها عبر الذكاء الاصطناعي، مما يساهم في قي الحد من الهجمات واختراقات وتقليل من الخسائر المحتمل حدوثها.

الأخذ بالمسؤولية عن تحقيق الأمن السيبراني، كجزء لا يتجزأ من الوطني.

أما فيما يتعلق من الناحية البشرية، فإنه يمثل أحد أهم عناصر منظومة الأمن السيبراني، الأمر الذي يستدعي كثيف برامج التكوين والتدريب لفائدة الموظفين والمتخصصين وهذا ماتعانيه الجزائر من قلة كفاءات في هذا المجال بتحديد، الى جانب برامج التكوين والتدريب نشر الوعي الأمني لدى المستخدمين، باعتبارهم أحد أبرز نقاط الضعف التي يمكن استهدافها في الفضاء الرقمي.

يمكن القول ان تبني هذه التوصيات على مصر قصير من شأنه أن يساهم في تعزيز قدرات الجزائر في مجال الأمن السيبراني وتحقق إنجازات فيها، ويمهد الطريق نحو بناء منظومة أكثر تطوراً وفعالية في المستقبل.

الفرع الثاني: استراتيجيات طويلة المدى

تعزيز الأمن السيبراني في الجزائر نبني رؤية استراتيجية واضحة تقوم على بناء منظومة وطنية متكاملة، تكون قادرة على أن تتماشى مع التغيرات والتطورات التكنولوجية الحديثة ومواجهة التهديدات السيبرانية.

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

تحديث تشريعات سيبرانية تتماشى مع التطورات الحاصلة في عالم التكنولوجيا، من أجل تسهيل التعاملات في جميع المجالات وتحفيز التكامل مع داخل والخارج.

إنشاء مراكز للسلامة المعلوماتية ولطوارئ الاتصالات تتعاون فيما بينها.

تطوير البنية التحتية الرقمية أمنة، من خلال الاستثمار في تحسين الأنظمة المعلوماتية وتعزيز قدرات الحماية داخل مختلف القطاعات المهمة في الجزائر.

كما أن لا يمكن تحقيق الأمن السيبراني دون وجود كفاءات وطنية مؤهلة قادرة على الابتكار وإيجاد حلول عبر تطوير تتماشى مع خصوصيات البيئة الرقمية في الجزائر.

إدماج التقنيات الحديثة وعلى رأسها الذكاء الاصطناعي في مجال الأمن السيبراني، لما توفره من إمكانيات في تحليل البيانات واكتشاف التهديدات بشكل استباقي، مما يؤدي إلى انتقال من أساليب الدفاع تقليدي إلى أساليب أكثر حداثة وتطورا.

تعزيز التعاون الدولي والإقليمي نظرا للتهديدات العابرة للحدود والقارات وهو ما يستدعي تبادل الخبرات والمعلومات، والاستفادة من التجارب الدولية.

يمكن القول أن هذه الاستراتيجيات على المدى الطويل من شأنه أن يساهم في بناء منظومة أمن سيبراني متكاملة قادرة على مواجهة تحديات المستقبلية، بما يضمن حماية الفضاء الرقمي الوطني وتحقيق الأمن والاستقرار في البيئة الرقمية.

خلاصة الفصل الثاني:

تناول الفصل الثاني المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني من خلال تحليل مختلف الأبعاد القانونية والمؤسسية والتنظيمية، وذلك بهدف إبراز مدى جاهزية الدولة.

فقد تطرق هذا الفصل في شقه الأول إلى الإطار التشريعي والسياساتي الذي تبنته الجزائر في مجال الأمن السيبراني، حيث تم الوقوف على أهم القوانين الوطنية المتعلقة بمكافحة الجرائم السيبرانية وحماية المعطيات ذات الطابع الشخصي، إضافة إلى إبراز الاستراتيجية الوطنية للأمن السيبراني والبرامج الحكومية الداعمة لتعزيز الأمن الرقمي، إلى جانب الجهود المبذولة من طرف الدولة في مواجهة مختلف الجرائم الإلكترونية والحد من آثارها.

أما الشق الثاني فقد ركز على البناء المؤسسي والتنظيمي لمنظومة الأمن السيبراني في الجزائر، من خلال دراسة أهم المؤسسات والهيئات المكلفة بحماية الفضاء السيبراني، سواء ذات الطابع الحكومي أو الأمني والعسكري، مع التطرق إلى آليات التنسيق بين مختلف الفاعلين، وأهمية الشراكات مع القطاع الخاص والمجتمع المدني في تعزيز فعالية المنظومة السيبرانية. كما تم تقييم الأداء المؤسسي من خلال إبراز نقاط القوة التي تتمتع بها هذه المنظومة، مقابل مجموعة من نقاط الضعف التي ما تزال تؤثر على فعاليتها.

كما خلاص الفصل كذلك إلى أن المنظومة السيبرانية في الجزائر تواجه جملة من التحديات المرتبطة بالجوانب التقنية والقانونية والبشرية، إضافة إلى تصاعد التهديدات السيبرانية سواء الداخلية أو الخارجية التي تستهدف المؤسسات الوطنية والبنى التحتية الحيوية.

وفي الأخير أشار الفصل إلى أن تعزيز الأمن السيبراني في الجزائر يتطلب مواكبة التحولات التكنولوجية الحديثة، خاصة في مجال الذكاء الاصطناعي، إلى جانب تطوير استراتيجيات قصيرة وطويلة المدى تضمن بناء منظومة رقمية أكثر أماناً ومرونة في مواجهة المخاطر المستقبلية.

الخاتمة

الخاتمة:

نستخلص من هذه الدراسة التي قمنا بدراستها فيها موضوع الأمن السيبراني في الجزائر من خلال تحليل السياسات والمؤسسات، وأهم الإنجازات المحققة في هذا المجال، يمكن التأكيد على أن الأمن السيبراني أصبح يشكل أحد أهم التحديات الاستراتيجية التي تواجه الدول في ظل التحول الرقمي المتسارع وتزايد الاعتماد على الفضاء السيبراني في مختلف المجالات الحيوية.

أظهرت الدراسة أن الجزائر قطعت خطوات مهمة جدا في سبيل تعزيز منظومة الأمن السيبراني، سواء من خلال تطوير التشريعات وتنظيم القوانين المتعلقة بالجرائم السيبرانية وحماية المعطيات الشخصية، أو من خلال وضع سياسات واستراتيجيات وطنية تهدف إلى تعزيز الأمن الرقمي ومواكبة التهديدات الحديثة.

كما تبين أن هناك بنية مؤسسية قائمة تسعى إلى حماية الفضاء السيبراني الوطني، إلا أنها لا تزال تواجه تحديات تتعلق بالتنسيق بين مختلف الفاعلين وفعالية الأداء المؤسسي.

تعد الجزائر منظومة حديثة المنشأ وهي في طور النمو والتحسين المستمر، فهي عملية ديناميكية تسعى لمواكبة التطور والتحول الرقمي المتسارع والتصدي لأي تهديدات قائمة. وينطبق ذلك بشكل خاص المجال الامن السيبراني، فبينما لاتزال على إنجازاته في طور النمو، استطاعت الدولة مواكبة التطورات والعمل على برامج لحماية معطياتها، ويعود ذلك الى قدرتها الدفاعية (الواقعية الدفاعية) وهنا نقول إن الفكر الاستراتيجي الجزائري يلعب دورا محوريا في استراتيجيات الدولة.

كما خلصت الدراسة إلى أن التهديدات السيبرانية في تزايد مستمر، سواء كانت داخلية أو خارجية، وهو ما يفرض على الجزائر ضرورة تعزيز قدراتها التقنية والبشرية، وتطوير آليات

الاستجابة السريعة، إلى جانب الاستثمار في التكوين والابتكار التكنولوجي، خاصة في مجالات الذكاء الاصطناعي والأمن الرقمي.

يمكن اعتبار أن مستقبل الأمن السيبراني في الجزائر يرتبط بمدى قدرة الدولة على مواكبة التحولات التكنولوجية وتطوير منظومة رقمية مرنة وقادرة على مواجهة التهديدات المستجدة، بما يضمن حماية السيادة الرقمية وتحقيق الأمن الوطني في بعده الشامل.

ويمكن حصر أهم النتائج والتوصيات المتوصل إليها في النقاط التالية:

أولاً: القصور في البنية التشريعية والتنظيمية وعدم إلمام قوانينها بمختلف الأجزاء المكونة للثورة المعلوماتية والتوجه نحو الإجراءات الردعية والتدابير الوقائية للحد من القرصنة.

ثانياً: من خلال الدراسة الميدانية التي قمنا بها أثناء الخرجة العلمية الى أمن ولاية خنشلة، وتحديدًا بمصلحة مكافحة الجرائم الالكترونية تم استخلاص من هذه الخرجة العلمية أن هناك تنسيق بين المؤسسات أي الدعم فيما بينهم، كما أن لها كفاءات وخبراء في مجال الأمن السيبراني والجزائر تواجه تحديات كبيرة.

ثالثاً: المنظومة السيبرانية في الجزائر تواجه مجموعة من التحديات التقنية والبشرية والمؤسسية التي تؤثر بشكل مباشر على مستوى الحماية الرقمية.

التوصيات

أولاً: إنشاء مراكز وطنية متقدمة لمحاكاة الهجمات السيبرانية (Cyber Range) لتدريب الكفاءات ورفع مستوى الجاهزية.

ثانياً: إنشاء مدارس في جميع الاطوار التعليمية من أجل تعليمهم مبادئ الاعلام الآلي والأمن السيبراني.

ثالثاً: ضرورة إنشاء هيئة وطنية موحدة ومستقلة للأمن السيبراني تتولى التنسيق بين مختلف المؤسسات وتوحيد الجهود في مواجهة التهديدات الرقمية.

رابعاً: تعزيز الشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني، خاصة مع شركات التكنولوجيا والاتصالات لتبادل الخبرات والمعلومات.

خامساً: تحديث ترسانة قانونية المتعلقة بمكافحة الجرائم الالكترونية لموكبة التطور الذي نشهده وذلك في أساليب التشفير والهجمات السيبرانية.

سادساً: ضرورة إبرام اتفاقيات تعاون دائمة وبين العلوم السياسية خاصة تخصص دراسات استراتيجية وأمنية ومصالح الأمن الوطني من أجل تبادل الخبرات وتوفير فرص ميدانية للطلبة لفهم الواقع الذي نحن فيه. ولاننسى حملات التوعية وتبدأ من القطاعات الثلاثة التعليمية الى الجامعات.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولاً: المراجع باللغة العربية:

1/- الكتب

1. العماد مصطفى طلاس. (2011). الاستراتيجية السياسية العسكرية. دمشق: دار طلاس للدراسات والترجمة والنشر.
2. أوس مجيد غالب العوادي. (2016). الامن المعلوماتي السيبراني. بيروت: مركز البيان للدراسات والتخطيط.
3. خالد يوسف. (2018). النماذج المؤسسية في الدراسات الأمنية. عمان: دار النهضة العربية.
4. زياد علي علي. (2020). الصراع والامن الجيوسبيبراني في الساحة الدولية، دراسة في استراتيجيات الاشتباك الرقمي. عمان.
5. سامي عبد الرحمن. (2020). تحليل المؤسسات الأمنية وإدارة المخاطر السيبرانية. القاهرة: دار الفكر الجامعي.
6. طارق السويدان ومحمد العدلوني. (2004). التخطيط الاستراتيجي. بيروت: دار ابن حزم.
7. عبد السلام أبو قحف. (2002). الإدارة الاستراتيجية وإدارة الأزمات. الإسكندرية: الدار الجامعية.
8. عبد الكريم بن علي. (2019). الذكاء الاصطناعي: المفاهيم والتطبيقات. عمان: دار المسيرة للنشر و التوزيع.
9. عبد الله للقاني. (2023). دور الأمن السيبراني في تعزيز أمن المعلومات المالية والالكترونية . عمان، الاردن: دار الباروري العلمية للنشر والتوزيع.

10. مجيد عبد جعفر الكرخي. (2016). التخطيط الاستراتيجي باستخدام تحليل SWOT. عمان: دار المناهج للنشر و التوزيع.
11. محمد كمال. (2022). الارهاب الالكتروني. مصر.
12. منى الأشقر جبور. (2017). السيرية هاجس العصر (الإصدار 1). بيروت: المركز العربي للبحوث القانونية والقضائية.
13. مولود ديدان. (بلا تاريخ). قانون الإجراءات الجزائية: المادتان 37 و 45 والأمر 02-05. دار بلقيس.
- 2- المقالات العلمية والدوريات
14. أ جنادي . (2024). التحول الرقمي الرهان سيادي. مجلة الجيش (726).
15. إدريس عطية. (2019). مكانة الأمن السيرياني في منظومة الأمن الوطني الجزائري. مجلة مصداقية، 1(1).
16. إلهام غازي. (2016). الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري. مجلة الجيش، 43(630).
17. ب بوعلام. (2016). الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي. مجلة الجيش (630).
18. بثينة حبيبتي. (2019). معوقات مكافحة الجريمة المعلوماتية. مجلة العلوم الإنسانية، 30(1).
19. جمال إبراهيم. (2006). مكافحة الجريمة الإلكترونية في التشريع الجزائري. المجلة النقدية للقانون والعلوم السياسية، 2(124).
20. جمال بوازدية. (2019). الاستراتيجية في مواجهة الجرائم السيرية: التحديات والآفاق المستقبلية. مجلة العلوم القانونية والسياسية، 1284.

21. حاتم بن عزوز، و حليلة هناني. (2022). الأمن السيبراني والجريمة الإلكترونية في دول ما بعد الحداثة: الولايات المتحدة الأمريكية نموذجاً. مجلة الرسالة للدراسات الإعلامية، 6(2).
22. سعيد محمودي. (2023). الأمن السيبراني في الجزائر بين المعالجة الأمنية والحماية القانونية . مجلة الناقد للدراسات السياسية والقانونية، 7(2).
23. سمير بارة. (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني(40).
24. سمير بارة. (2017). الأمن السيبراني في الجزائر-السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني(4).
25. شوبير جيلاني. (2023). حروب السيبرانية والأمن السيبراني. مجلة الحقوق والحريات، 11(1).
26. عزة شلوش. (2018). القرصنة الإلكترونية في الفضاء السيبراني وأثرها على الأمن القومي للدول. مجلة مركز بابل للدراسات الإنسانية، 8(2).
27. عزيز نوري، و سميرة سليمان. (2021). تهديدات الهجينة بين إشكالية التعريف وأنماط المواجهة. المجلة الجزائرية للأمن والتنمية، 10(1).
28. فضيل شريف، و أ لحمل. (2023). الاستراتيجية الوطنية للأمن سيبراني ضمان حماية أنظمة معلوماتية. (715).
29. محمد دهماني. (2023). الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني. مجلة الفكر القانوني والسياسي، 2(7).
30. مصطفى إسلام، و مصطفى جمعة. (2022). جريمة اختراق الأمن السيبراني واستخدام البيانات والمعلومات في القانون المصري. مجلة القانون والبحوث القانونية، 12(3).

31. منى عبد الله السمحان. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية (118).
32. نادية سعيد. (2022). إدارة الأمن السيبراني: النماذج التحليلية. مجلة العلوم الأمنية.
33. وحيدة وصديقي، و فاطمة الزهراء حشروف. (2025). الأمن السيبراني في البنوك الجزائرية: التحديات والاستراتيجيات. مجلة دفاتر اقتصادية، 1(11).

3- الرسائل الجامعية والمذكرات

34. رانية نابتي، و أميمة نابتي. (بلا تاريخ). إجراءات المثلث الفوري في التشريع الجزائري (مذكرة ماستر). كلية الحقوق والعلوم السياسية.
35. عائشة نايري. (2017). الجريمة الإلكترونية في التشريع الجزائري [رسالة ماجستير غير منشورة]. تخصص قانون إداري. جامعة أدرار.
36. محمد شايب. (2024). تأثيرات التهديدات السيبرانية على الأمن المجتمعي [مذكرة ماستر غير منشورة]. الجزائر: المدرسة الوطنية العليا للعلوم السياسية.

4- الملتقيات والأوراق البحثية

37. حسين نواره. (2017). آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة خاصة إلكترونياً [ورقة بحثية]. الملتقى الوطني حول آليات مكافحة الجرائم الإلكترونية. تيزي وزو: جامعة مولود معمري.
38. عبد الرحمن حملاوي. (2015). دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية [ورقة بحثية]. الملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة. بسكرة: جامعة محمد خيضر.
39. عز الدين. (2015). الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها [ورقة بحثية]. الملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة. بسكرة: جامعة محمد خيضر.

40. فضيلة عاقل. (2017). الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري [ورقة بحثية]. المؤتمر الدولي الرابع عشر للجرائم الإلكترونية. طرابلس.

5/- القوانين والمراسيم

41. القانون رقم 06-22. (20 12, 2006). المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية. الجريدة الرسمية للجمهورية الجزائرية، العدد 84.

42. القانون رقم 18-04. (10 05, 2018). يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. الجريدة الرسمية للجمهورية الجزائرية، العدد 27.

43. القانون رقم 18-07. (10 07, 2018). المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية للجمهورية الجزائرية، العدد 34.

44. المرسوم التنفيذي رقم 05/20. (30 جويلية 2020). الجريدة الرسمية للجمهورية الجزائرية (6904).

45. قانون رقم 09-04. (2009). يتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 47.

46. مرسوم رئاسي رقم 15-261. (2015). يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 53.

6/- التقارير والمنشورات الرسمية

47. الاتحاد الدولي للاتصالات. (2015). تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية. جنيف: مكتبة تنمية.

48. البنك الدولي. (2023). التقرير السنوي للتنمية الرقمية. دار النشر الدولية.

49. الهيئة الوطنية للأمن السيبراني. (2022). التقرير السنوي للأمن السيبراني. دار النشر الوطنية الجزائرية.
50. منتدى الجزائر للتكنولوجيا. (2021). الجاهزية السيبرانية في الشركات الصغيرة والمتوسطة، 2.
51. منظمة التعاون الاقتصادي والتنمية. (2022). الذكاء الاصطناعي والأمن الرقمي. تقرير دولي.
52. وزارة التعليم العالي والبحث العلمي. (2021). إنشاء المدرسة الوطنية العليا للذكاء الاصطناعي. الجزائر.
53. وزارة التعليم العالي والبحث العلمي. (2023). استراتيجية تطوير التكوين في مجالات التكنولوجيات الحديثة. الجزائر.
54. وزارة الدفاع الوطني الجزائري. (2024). ورشة استراتيجية للأمن السيبراني.
55. وزارة الدفاع الوطني الجزائرية. (2026). الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029. الجزائر.
56. وكالة الأنباء الجزائرية. (2026). ملتقى وطني حول تعزيز القدرات في مجال الأمن السيبراني. الجزائر.

ثانيا: المراجع باللغة الأجنبية

1/- books

57. Bigo, D. B. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. Alternatives, 27(1).
58. Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era (2 ed.). Boulder, CO: Lynne Rienner Publishers.
59. Buzan, B., & al. (1998). Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.
60. Freedman, L. (2004). Deterrence. Polity Press.
61. Keohane, R., & Nye, J. (2014). Power and Interdependence. Longman.

62. Luibecki, M. C. (2009). Cyberdeterriene and cyberwar. RAND Corporation.
63. Luttwak, E. N. (2001). Strategy: The Logic of War and Peace. Harvard University Press.
64. Mbanaso, U., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. IOSR Journal of Computer Engineering, (IOSR-JCE), 17(3), 17–24.
65. Mearsheimer, J. J. (2001). The Tragedy of Great Power Politics. Norton: W.W.
66. Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of International Politics. International Organization, 51(4), 513–553.
67. Morgenthau, H. (2006). Politics Among Nations. McGraw-Hill.
68. Nye, J. (2011). The Future of Power. New York: Public Affairs.
69. Pfllege, C. p., & Pfllege, S. L. (2015). Security in computing. Pearson.
70. Saeed, A., & Renas, R. A. (2022). Cybersecurity threats, vulnerability, challenges and proposed solution. Applied Computing Journal, 2(4).
71. Schelling, T. (1960). The Strategy of Conflict. Harvard University Press.
72. Stallings, W. (2019). Effective cybersecurity: A guide to using Best Practices and standers. Wesley: Addison.
73. Surwade, P., & Hitendra, J. P. (2024). Information security. SSRN (Social Science Research Network).
74. Tsoukala, A., & Bigo, D. (2008). Understanding security knowledge. Routledge.
75. Wæver, O. (1995). Securitization and Desecuritization,in On Security. New York: ed. Ronnie D. Lipschutz Columbia University Press.
76. Waltz, K. (1979). Theory of International Politics. McGraw-Hill.

فهرس الأشكال

والجداول

فهرس الأشكال:

- الشكل رقم 1: تطور الأمن السيبراني 15
- الشكل رقم 2: مخطط الامن السيبراني من منظور الليبرالية الكلاسيكية والجديدة 25
- الشكل رقم 3: مخطط الامن السيبراني من منظور الواقعية الكلاسيكية والجديدة 26
- الشكل رقم 4: الأمن السيبراني من منظور مدرسة كوبنهاغن 28
- الشكل رقم 5: الامن السيبراني من منظور مدرسة باريس 30
- الشكل رقم 6: موقع الأمن السيبراني ضمن نظريات الفكر الاستراتيجي 33
- الشكل رقم 7: النموذج التحليلي SWOT في دراسة المنظومة السيبرانية 36
- الشكل رقم 8: المخطط التحليلي لنموذج أندرو سكوت 38
- الشكل رقم 9: تطور عدد القضايا السيبرانية المعالجة في الجزائر خلال الفترة 2016-2022 67
- الشكل رقم 10: توزيع المؤسسات الفاعلة في مجال الأمن السيبراني في الجزائر 68
- الشكل رقم 11: تطور عدد الطلبة في تخصصات الأمن السيبراني والذكاء الاصطناعي في الجزائر 2020 - 2024 69
- الشكل رقم 12: تطور مستوى الاستجابة للحوادث السيبرانية في الجزائر (2018-2023) 70
- الشكل رقم 13: تطور عدد الهجمات السيبرانية في الجزائر خلال الفترة 2016 - 2025 71
- الشكل رقم 14: توزيع المؤسسات في الجزائر حسب مستوى الحماية السيبرانية 72
- الشكل رقم 15: الفجوة بين احتياجات سوق العمل وعدد المختصين في الأمن السيبراني في الجزائر 73
- الشكل رقم 16: مستوى التنسيق بين المؤسسات في مجال الأمن السيبراني في الجزائر 74

فهرس الجداول

- الجدول رقم 1: التدابير الوقائية للأمن السيبراني في الجزائر 58
- الجدول رقم 2: يوضح عدد القضايا المعالجة من طرف مركز الوقاية من الجرائم المعلوماتية ومكافحتها 61
- الجدول رقم 3: يوضح عدد القضايا المعالجة من طرف المديرية العامة للأمن الوطني .. 64
- الجدول رقم 4: يوضح ترتيب بلدان منطقة الدول العربية حسب الرقم القياسي العالمي للأمن السيبراني 83

فهرس الموضوعات

فهرس الموضوعات

الشكر والعرفان

الإهداء

مقدمة: 1.....

الفصل الأول: الإطار المفاهيمي والنظري للدراسة

المبحث الأول: تعريف مفهوم الأمن السيبراني. 11.....

المطلب الأول: تعريف الأمن السيبراني والمفاهيم ذات الصلة. 11.....

الفرع الأول: تعريف الأمن السيبراني. 11.....

الفرع الثاني: تطور الأمن السيبراني. 14.....

الفرع الثالث: المفاهيم ذات صلة بالأمن السيبراني. 16.....

المطلب الثاني: أبعاد وأهداف الأمن السيبراني. 18.....

الفرع الأول: أبعاد الأمن السيبراني. 18.....

الفرع الثاني: أهداف الأمن السيبراني. 21.....

المبحث الثاني: الإطار النظري للدراسة. 24.....

المطلب الأول: الأمن السيبراني من منظور العلاقات الدولية. 24.....

الفرع الأول: الأمن السيبراني من منظور الليبرالية الكلاسيكية والجديدة. 24.....

الفرع الثاني: الأمن السيبراني من منظور الواقعية الكلاسيكية والجديدة. 26.....

الفرع الرابع: مدرسة باريس في منظور الأمن السيبراني. 29.....

المطلب الثاني: موقع الأمن السيبراني ضمن نظريات الفكر الاستراتيجي. 31.....

الفرع الأول: الاستراتيجية وأبعادها في الدراسات الأمنية والفكر الاستراتيجي.	31
الفرع الثاني: مخطط لنظريات الفكر الاستراتيجي في الأمن السيبراني	32
المبحث الثالث: نماذج تحليلية مفسرة لتطبيق الأمن السيبراني.	34
المطلب الأول: النموذج التحليلي SWOT في دراسة المنظومة السيبرانية.	34
الفرع الأول: تعريف نموذج SWOT	34
الفرع الثاني: المخطط التحليلي لتطبيق نموذج SWOT في مجال الامن السيبراني	35
المطلب الثاني: نموذج أندرو سكوت لتحليل الهياكل والمؤسسات السيبرانية.	37
الفرع الأول: تعريف نموذج أندرو سكوت	37
الفرع الثاني: المخطط التحليلي لنموذج اندرو سكوت	38
خلاصة الفصل الأول:	40

الفصل الثاني: المقاربة الجزائرية لتفعيل منظومة الأمن السيبراني

المبحث الأول: التشريعات والسياسات للأمن السيبراني.	43
المطلب الأول: التشريعات الخاصة بالأمن السيبراني.	43
الفرع الأول: القوانين الوطنية المتعلقة بالجرائم السيبرانية.	43
الفرع الثاني: حماية البيانات والبنية التحتية الحيوية.	48
المطلب الثاني: السياسات والاستراتيجيات الضابطة	50
الفرع الأول: الاستراتيجية الوطنية للأمن السيبراني	51
الفرع الثاني: البرامج والمبادرات الحكومية.	54
المطلب الثالث: دور الدولة في مكافحة الجرائم السيبرانية.	56

56	الفرع الأول: جهود الجهاز التنفيذي
58	الفرع الثاني: التدابير الوقائية
60	المبحث الثاني: البناء المؤسساتي والتنظيمي الخاص بالأمن السيبراني
60	المطلب الأول: المؤسسات والهيئات المتخصصة في تعزيز الامن السيبراني
60	الفرع الثاني: المؤسسات الحكومية
63	الفرع الثاني: الهيئات الأمنية والعسكرية
65	المطلب الثاني: التنسيق المؤسساتي وآليات العمل المشترك
65	الفرع الأول: التعاون بين الوزارات والمؤسسات
66	الفرع الثاني: التنسيق مع الهيئات الدولية
67	المطلب الثالث: فعالية الأداء المؤسساتي
67	الفرع الأول: نقاط القوة
71	الفرع الثاني: نقاط الضعف
75	المبحث الثالث: التحديات والتهديدات المؤثرة على الأمن السيبراني
75	المطلب الأول: التحديات التقنية - القانونية - البشرية
75	الفرع الأول: التحديات التقنية
76	الفرع الثاني: التحديات القانونية
77	الفرع الثالث: التحديات البشرية
77	المطلب الثاني: التهديدات السيبرانية التي تواجه المؤسسات الوطنية
77	الفرع الأول: التهديدات السيبرانية الخارجية
81	الفرع الثاني: التهديدات السيبرانية الداخلية

المبحث الرابع: الآفاق المستقبلية لتعزيز الأمن السيبراني الوطني	82
المطلب الأول: التحولات التكنولوجية في الأمن السيبراني	82
الفرع الأول: جهود الدولة الجزائرية في مجال الأمن السيبراني	82
الفرع الثاني: تطبيقات الذكاء الاصطناعي في الأمن السيبراني	86
المطلب الثاني: مستقبل الأمن السيبراني في الجزائر	88
الفرع الأول: توصيات قصيرة المدى	88
الفرع الثاني: استراتيجيات طويلة المدى	89
خلاصة الفصل الثاني:	91
الخاتمة:	93
قائمة المصادر والمراجع:	97
فهرس الأشكال:	105
فهرس الجداول:	106
فهرس الموضوعات	108

المخلص

تتناول هذه المذكرة موضوع الأمن السيبراني في الجزائر، من خلال تحليل المنظومة السيبرانية من حيث السياسات والمؤسسات المعتمدة في هذا المجال، إضافة الى إبراز أهم الجهود المبذولة لحماية الفضاء الرقمي الوطني. كما تتطرق الدراسة الى أبرز التحديات والتهديدات التي تواجه الأمن السيبراني، سواء كانت تقنية أو قانونية أو بشرية، مع التركيز على التهديدات الداخلية والخارجية التي تستهدف المؤسسات الوطنية.

كما تعالج المذكرة فعالية الأداء المؤسسي من خلال تحليل بعض المؤشرات والإحصائيات المتعلقة بالجرائم والهجمات السيبرانية في الجزائر، وفي الأخير تستعرض الدراسة أهم الآفاق المستقبلية لتعزيز الأمن السيبراني الوطني، من خلال دعم التعاون بين مختلف المؤسسات في ظل التحولات الرقمية المتسارعة التي يشهدها العالم اليوم.

Abstract:

This thesis examines cybersecurity in Algeria by analyzing the cyber system in terms of the policies implemented and the institutions involved in this field. It also highlights the main efforts made to protect the national digital space. The study further addresses the key challenges and threats facing cybersecurity, whether technical, legal, or human, with a particular focus on internal and external threats targeting national institution.

In addition, the thesis evaluates the effectiveness of institutional performance through the analysis of certain indicators and statistics related to cybercrimes and cyberattacks in Algeria. Finally, the study outlines future prospects for strengthening national cybersecurity, notably by supporting cooperation between various institutions in the context of rapid digital transformations occurring worldwide.