المدرسة الوطنية العليا للعلوم السياسية

الاستراتيجية الوطنية الجزائرية في مواجهة التهديدات السيبرانية: تحديات ورهانات منذ سنة 2020

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في العلوم السياسية

تخصص سياسات عامة

اعداد الطالبة:

تيميزار صوفيا

اشراف الأستاذ:

خننو فاتح

لجنة المناقشة:

اسم ولقب الاستاذ	الصفة
أوعشرين ابتسام	رئيسا
خننو فاتح	مشرفا ومقررا
كعبش سامي	عضو مناقشا

السنة الجامعية : 2025/ 2026

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

{يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ واللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ}

سورة المجادلة الآية 11

إهـــــــــداء

أهدي عملي هذا إلى من قال فيهما الله:

﴿وَاخْفِضْ لَهُمَا جَنَاحَ الذُّلِّ مِنَ الرَّحْمَةِ وَقُلْ رَبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا﴾

سورة الإسراء الآية 24

إلى والديَّ الكريمين حفظهما الله وأطال في عمرهما.

إلى إخوتي الأعزاء ولكل الأهل.

إلى أصدقائي.

وإلى من رفعوا رايات العلم والتعليم أساتذتي الأفاضل.

وإلى كل من ساهم في إنجاح هذه المذكرة.

الشكر والعرفان

الحمد لله الذي وفّقني وأعانني على إنجاز هذا العمل وإتمامه.

أتقدم بخالص الشكر إلى الأستاذ المشرف خننو فاتح على توجيهاته ونصائحه القيمة طيلة فترة إنجاز هذه المذكرة.

كما أتوجه بجزيل الشكر إلى كافة الأساتذة الذين أشرفوا على تكويني الجامعي وأسهموا في إثراء رصيدي المعرفي والعلمي.

وأخيراً، أشكر كل من مدّ لي يد العون والدعم، من قريب أو بعيد، وأسهم في إنجاح هذا العمل.

الملخص

في ظل تزايد وتيرة الهجمات السيبرانية عالميا وتوجه الدولة نحو التحول الرقمي الشامل، تهدف هذه الدراسة إلى تحليل الاستراتيجية الوطنية الجزائرية في مواجهة التهديدات السيبرانية، من خلال التطرق إلى مفاهيم الأمن السيبراني والتهديدات الرقمية، ودراسة الإطار القانوني والمؤسساتي المعتمد في الجزائر لتعزيز حماية الفضاء السيبراني. كما تسعى الدراسة إلى إبراز أهم التحديات التي تواجه الاستراتيجية الوطنية للأمن السيبراني، إضافة إلى الرهانات المستقبلية المرتبطة بالسيادة الرقمية والتحول الرقمي.

اعتمدت الدراسة على المنهج الوصفي، منهج تحليل المضمون ومنهج دراسة الحالة، من خلال وصف الإطار المفاهيمي والنظري للأمن السيبراني وتحليل النصوص القانونية والاستراتيجيات الوطنية المتعلقة بالأمن السيبراني، مع التركيز على الحالة الجزائرية.

وقد خلصت الدراسة إلى أن الجزائر تسعى إلى تعزيز أمنها السيبراني عبر تطوير التشريعات وإنشاء هيئات متخصصة، رغم استمرار بعض التحديات التقنية والبشرية. كما أظهرت الدراسة أن تحقيق السيادة الرقمية أصبح رهانًا أساسيًا لدعم الأمن الوطني والتحول الرقمي.

الكلمات المفتاحية

الأمن السيبراني، الفضاء السيبراني، الاستراتيجية الوطنية، السيادة الرقمية، التهديدات السيبرانية، الجزائر.

ABSTRACT

In light of the increasing frequency of cyberattacks globally and the state's move toward comprehensive digital transformation, this study aims to analyze Algeria's national strategy in addressing cyber threats by delving into the concepts of cybersecurity and digital threats, and examining the legal and institutional framework adopted in Algeria to enhance the protection of the cyber space. The study also aims to highlight the main challenges facing the national cybersecurity strategy, in addition to the future stakes related to digital sovereignty and digital transformation.

The study relied on the descriptive method, content analysis method, and case study method, by describing the conceptual and theoretical framework of cybersecurity, analyzing legal texts and national strategies related to cybersecurity, with a focus on the Algerian case.

The study concluded that Algeria is striving to enhance its cybersecurity by developing legislation and establishing specialized bodies, despite the persistence of some technical and human challenges. The study also showed that achieving digital sovereignty has become a key bet to support national security and digital transformation.

Keywords: Cybersecurity, cyberspace, national strategy, digital sovereignty, cyber threats, Algeria.

خطة الدراسة

مقدمة

الفصل الأول: الإطار المفاهيمي والنظري للأمن السيبراني

المبحث الأول: مقاربة مفاهيمية للفضاء السيبراني والأمن السيبراني

المطلب الأول: مفهوم السيبرانية، الفضاء السيبراني والأمن السيبراني

المطلب الثاني: الفواعل في الفضاء السيبراني

المطلب الثالث: أبعاد الأمن السيبراني

المبحث الثاني: التهديدات الأمنية السيبرانية

المطلب الأول: مفهوم التهديد السيبراني

المطلب الثاني: أساليب تنفيذ الهجمات السيبرانية

المطلب الثالث: أنواع التهديدات السيبرانية

المبحث الثالث: استراتيجيات الدول الرائدة للأمن السيبراني

المطلب الأول: الإستراتيجية الصينية للأمن السيبراني

المطلب الثاني: الإستراتيجية الامريكية للأمن السيبراني

المطلب الثالث: الإستراتيجية الروسية للأمن السيبراني

الفصل الثاني: آليات مواجهة التهديدات السيبرانية في الجزائر

المبحث الأول: الإطار القانوني والمؤسساتي للأمن السيبراني في الجزائر

المطلب الأول: الإطار القانوني والتنظيمي للفضاء الرقمي في الجزائر

المطلب الثاني: الهيئات المسؤولة عن الأمن السيبراني في الجزائر

المبحث الثاني: محاور الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية

المطلب الأول: حماية البنى التحتية الحيوية

المطلب الثاني: التكوين والتحسيس في المجال السيبراني

المطلب الثالث: التعاون الوطني والدولي في المجال السيبراني

المبحث الثالث: تأثير التهديدات السيبرانية على الأمن الوطني الجزائري

المطلب الأول: أشكال التهديدات السيبرانية التي تواجه الجزائر

المطلب الثاني: تداعيات التهديدات السيبرانية على الجزائر

الفصل الثالث: تحديات ورهانات مواجهة التهديدات السيبرانية في الجزائر

المبحث الأول: التحديات التي تواجه الاستراتيجية الوطنية للأمن السيبراني

المطلب الأول :التحديات التقنية والتكنولوجية

المطلب الثاني :التحديات البشرية والتكوينية

المطلب الثالث :التحديات القانونية والتنظيمية

المبحث الثاني: الرهانات المستقبلية لتعزيز الأمن السيبراني في الجزائر

المطلب الأول :السيادة الرقمية وحماية المعطيات

المطلب الثاني :الأمن السيبراني كشرط للتنمية الاقتصادية والتحول الرقمي

المطلب الثالث :تموقع الجزائر في الحوكمة السيبرانية الدولية

الخاتمة

مقدمة

شهد العالم خلال العقود الأخيرة تطورا تكنولوجيا متسارعا وثورة معلوماتية غير مسبوقة مست مختلف مجالات الحياة السياسية والاقتصادية والاجتماعية والأمنية، حيث أصبحت تكنولوجيات الإعلام والاتصال والرقمنة ركيزة أساسية في بناء الدول الحديثة وتسيير مؤسساتها. وقد أدى هذا الاعتماد المتزايد على التكنولوجيا إلى بروز فضاء جديد يعرف بالفضاء السيبراني، الذي أتاح فرصاً واسعة لتبادل المعلومات، تطوير الخدمات، وتحقيق التنمية.

لكن، وفي المقابل، أفرز هذا الفضاء المفتوح والمترابط تهديدات ومخاطر بالغة التعقيد تمس بشكل جوهري أمن الدول واستقرارها. فلم يعد مفهوم الأمن الوطني مقتصرا على حماية الحدود البرية والبحرية والجوية، بل امتد ليشمل تأمين المجال الرقمي، حيث أضحى الفضاء السيبراني أحد الأبعاد الجديدة للحروب والصراعات الحديثة. ومع تزايد الاعتماد على الأنظمة المعلوماتية والشبكات الرقمية، برزت التهديدات السيبرانية كأحد أخطر التحديات الأمنية المعاصرة، نظرا لما تتسم به من سرعة في الانتشار، وصعوبة في تحديد هوية المهاجمين، وتعدد مصادرها بين دول وجماعات منظمة وأفراد.

ولم تعد هذه التهديدات تقتصر على الجرائم الإلكترونية البسيطة، بل تطورت لتشمل اختراق الأنظمة الحساسة، التجسس، سرقة المعطيات الاستراتيجية، وتعطيل البنى التحتية الحيوية، إضافة إلى توظيفها في حروب الجيل الرابع لنشر الشائعات والمساس بالتماسك المجتمعي، وهو ما يشكل تهديدا مباشرا للسيادة الوطنية بمفهومها الرقمي الحديث. الأمر الذي فرض على مختلف الدول تسريع وتيرة تحديث منظوماتها الدفاعية، وتبني استراتيجيات وطنية شاملة تعنى بالأمن السيبراني.

وفي هذا السياق الجيوسياسي والأمني المعقد، أدركت الجزائر باعتبارها دولة ذات موقع استراتيجي وموارد حيوية مهمة، حتمية الانخراط في مسار التحول الرقمي وتعزيز أمنها السيبراني لحماية مقدراتها الوطنية. وقد تجسد هذا التوجه من خلال تبني مجموعة من القوانين والتشريعات، وإنشاء هيئات ومؤسسات متخصصة، إلى جانب وضع استراتيجية وطنية تهدف إلى تأمين الفضاء السيبراني الوطني وتعزيز الأمن الرقمي.

غير أن تحقيق هذه الحماية المنشودة يواجه مجموعة من التحديات، خاصة في ظل التطور السريع والمستمر لأساليب الهجوم السيبراني، الأمر الذي يجعل من حماية المعطيات وتأمين البنى التحتية الحيوية وتحقيق السيادة الرقمية رهانات أساسية أمام دولة الجزائر.

تسعى هذه الدراسة إلى تحليل الاستراتيجية الوطنية الجزائرية في مجال الأمن السيبراني خلال الفترة(2020-2026) ، وبيان مختلف الآليات القانونية والمؤسساتية المعتمدة لمواجهة التهديدات السيبرانية، مع إبراز أهم التحديات والرهانات المرتبطة بتحقيق السيادة الرقمية في الجزائر.

الإطار المنهجي والنظري للدراسة:

1/ المشكلة البحثية

اعتمدت الجزائر مقاربة وطنية للأمن السيبراني تقوم على وضع إطار استراتيجي ومؤسساتي وقانوني يهدف إلى حماية فضائها الرقمي وتعزيز قدرتها على مواجهة هذه التهديدات. غير أن فعالية هذه المقاربة تبقى مرتبطة بمدى قدرتها على تجاوز مختلف التحديات التقنية والبشرية والتنظيمية التي تواجه تطبيقها على أرض الواقع. وانطلاقاً من ذلك، تتبلور الإشكالية الرئيسية لهذه الدراسة في التساؤل الآتي:

ما هي معالم الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية بين التحديات والرهانات المستقبلية منذ سنة 2020؟

وللإجابة على هذا التساؤل الرئيسي، تم تفكيكه إلى التساؤلات الفرعية الآتية:

1. ما هي طبيعة التهديدات السيبرانية المعاصرة، وكيف تنعكس تداعياتها على الأمن الوطني الجزائري؟
2. ما هو الإطار القانوني والمؤسساتي الذي تعتمده الجزائر لتأمين فضائها الرقمي وحماية البنى التحتية الحيوية؟

3. ما هي أبرز التحديات التي تعيق فاعلية هذه الاستراتيجية، وكيف يمكن تجاوزها لكسب رهانات السيادة الرقمية والتنمية؟

2/ الفروض العلمية

كإجابة أولية عن تساؤلات الدراسة ننطلق من الفرضيات التالية:

1. تعتمد فعالية الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية على مدى تكامل أبعادها القانونية والمؤسساتية والتقنية، وعلى قدرتها على مواكبة التطور المتسارع للتهديدات السيبرانية.
2. يمثل التكوين والتحسيس عنصرا أساسيا في فعالية الأمن السيبراني داخل المؤسسات الجزائرية.
3. تواجه الاستراتيجية الوطنية الجزائرية للأمن السيبراني مجموعة من التحديات التقنية والبشرية والقانونية التي تؤثر على فعاليتها .

3/ مجالات الدراسة

أ. المجال المكاني

تنحصر الدراسة في الجزائر، الواقعة في شمال إفريقيا والمطلة على البحر الأبيض المتوسط، باعتبارها مجالا جغرافيا للدراسة.

ب. المجال الزماني

تتزامن هذه الدراسة مع الفترة الممتدة منذ سنة 2020، باعتبارها مرحلة شهدت تزايد الاهتمام الرسمي بالأمن السيبراني وتعزيز مسار التحول الرقمي، إضافة إلى صدور الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029.

ج. المجال الموضوعي

تتناول هذه الدراسة موضوع الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية، من خلال دراسة مفاهيم الأمن السيبراني والتهديدات الرقمية، وتحليل الإطار القانوني

والمؤسساتي المعتمد في الجزائر، إضافة إلى التحديات والرهانات المرتبطة بتعزيز الأمن السيبراني والسيادة الرقمية.

4/ الأهمية العلمية والعملية للدراسة:

1. الأهمية العلمية:

تكمن الأهمية العلمية لهذا البحث في:

- الإسهام في إثراء الدراسات الأكاديمية المتعلقة بالأمن السيبراني والاستراتيجيات الوطنية الرقمية، خاصة في البيئة الجزائرية .
- تحليل الإطار القانوني والمؤسساتي الذي تعتمد عليه الجزائر في مواجهة التهديدات السيبرانية .
- توفير مرجع علمي يمكن للباحثين والطلبة الاستفادة منه في الدراسات المستقبلية المتعلقة بالأمن السيبراني والتحول الرقمي .

2. الأهمية العملية:

تتجلى الأهمية العملية للبحث فيما يلي:

- إبراز واقع الأمن السيبراني في الجزائر والتحديات التي تواجه الاستراتيجية الوطنية في هذا المجال.
- دعم الجهود الرامية إلى تعزيز الوعي السيبراني داخل المؤسسات والمجتمع .
- إبراز أهمية الأمن السيبراني كعامل أساسي لحماية البنية التحتية الرقمية وتحقيق التنمية الاقتصادية والسيادة الرقمية.

5/ أهداف الدراسة

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف، أهمها:

- التعرف على مفهوم الأمن السيبراني والتهديدات السيبرانية وأبعادها المختلفة .
- رصد وتحليل أبرز التهديدات والهجمات السيبرانية التي تستهدف الجزائر، مع إبراز انعكاساتها على المؤسسات الحيوية والسيادة الرقمية.

- دراسة الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية وتحليل محاورها واهدافها الأساسية .
- تحديد أبرز التحديات التي تواجه الجزائر في مجال الأمن السيبراني .
- إبراز الرهانات المستقبلية المرتبطة بالسيادة الرقمية والتحول الرقمي في الجزائر .

6/ أسباب اختيار الموضوع

1. الأسباب الموضوعية:

- تنامي التهديدات والهجمات السيبرانية على المستوى الدولي، وما تشكله من خطر على أمن الدول والمؤسسات والبنى التحتية الحيوية .
- توجه الجزائر نحو الرقمنة وتطوير الخدمات الإلكترونية، الأمر الذي يستوجب تعزيز الحماية السيبرانية وتأمين الفضاء الرقمي الوطني .
- أهمية الأمن السيبراني باعتباره جزءاً أساسياً من منظومة الأمن الوطني وحماية المعطيات والأنظمة المعلوماتية .

2. الأسباب الذاتية:

- الاهتمام الشخصي بمجال الأمن السيبراني والتطورات التكنولوجية الحديثة، باعتباره من أكثر المواضيع ارتباطاً بمستقبل الدول والمجتمعات .
- السعي إلى اكتساب معرفة أكاديمية وبحثية في مجال الأمن السيبراني، باعتباره من المجالات الحديثة والمتجددة.
- الرغبة في التعمق في دراسة التهديدات السيبرانية وآثارها على الأمن الوطني والسيادة الرقمية، خاصة في ظل التحول الرقمي المتسارع .

7/ مناهج الدراسة

اعتمدت هذه الدراسة على مجموعة من المناهج العلمية التي تتناسب مع طبيعة الموضوع وأهدافه، والمتمثلة في:

- **المنهج الوصفي:** تم الاعتماد عليه لوصف الإطار المفاهيمي والنظري للأمن السيبراني، وتحديد مختلف المفاهيم المرتبطة به، إضافة إلى وصف الإطار القانوني والمؤسساتي المنظم للأمن السيبراني في الجزائر.
- **المنهج التحليلي:** اعتمدت هذه الدراسة على المنهج التحليلي، من خلال تحليل الإطار المفاهيمي والقانوني والمؤسساتي للأمن السيبراني، ودراسة مكونات الاستراتيجية الوطنية الجزائرية وتقييم فعاليتها في مواجهة التهديدات السيبرانية.

8/ الاقترابات المعتمدة:

اعتمدت هذه الدراسة على مجموعة من النظريات والاقترابات العلمية لفهم وتحليل موضوع الأمن السيبراني في الجزائر،

- **اقتراب السياسات العامة**

يعتمد هذا الاقتراب على تحليل كيفية صياغة وتنفيذ وتقييم السياسات العمومية في مجال الأمن السيبراني، من خلال دراسة دور الدولة ومختلف الفاعلين المؤسساتيين في وضع الاستراتيجيات الوطنية لحماية الفضاء السيبراني.

- **الاقتراب المؤسسي**

اعتمدت الدراسة على الاقتراب المؤسسي لتحليل دور المؤسسات والهيئات الرسمية المكلفة بالأمن السيبراني في الجزائر، ودراسة مدى مساهمتها في حماية الفضاء السيبراني وتعزيز الأمن الوطني.

- **الاقتراب القانوني**

تم الاعتماد على الاقتراب القانوني لدراسة مختلف النصوص التشريعية والتنظيمية المتعلقة بالأمن السيبراني، وتحليل الإطار القانوني الذي اعتمدته الجزائر لمواجهة التهديدات السيبرانية.

9/ أدوات جمع البيانات

اعتمدت هذه الدراسة على مجموعة من أدوات جمع البيانات التي تتناسب مع طبيعة الموضوع وأهدافه، وتتمثل فيما يلي:

1. **الملاحظة الميدانية**

من خلال التربص داخل وكالة الأنباء الجزائرية، وما أتاحه من معاينة مباشرة للتهديدات السيبرانية التي تستهدف المؤسسات العمومية والاقتصادية، والاطلاع على بعض آليات الحماية والاستجابة للهجمات الإلكترونية .

2. **المقابلة الميدانية**

من خلال إجراء مقابلات مع إطارات ومختصين في المصالح العملياتية لمكافحة الجرائم السيبرانية التابعة لأمن ولاية الجزائر، بهدف جمع معطيات واقعية حول طبيعة التهديدات السيبرانية وأساليب مواجهتها .

3. **تحليل الوثائق والنصوص القانونية**

من خلال جمع وتحليل البيانات من مصادرها المكتوبة والرقمية، وشملت النصوص القانونية والتشريعية المكونة للإطار القانوني للأمن السيبراني في الجزائر والوثائق والاستراتيجيات الرسمية لاستخلاص التوجهات، الأهداف، والآليات المؤسساتية.

10/ الدراسات السابقة:

- **دراسة بدرين سيد علي بعنوان: "الإستراتيجية الأمنية الجزائرية لمواجهة التهديدات السيبرانية" مذكرة ماستر (2023)، المدرسة الوطنية العليا للعلوم السياسية:**

تناولت هذه الدراسة موضوع الأمن السيبراني في الجزائر من خلال التركيز على الاستراتيجيات والآليات القانونية والمؤسساتية المعتمدة لمواجهة التهديدات السيبرانية، كما تطرقت إلى دور الهيئات الأمنية ومختلف الأجهزة المختصة في حماية الأمن الوطني. غير أن هذه الدراسة لم تتناول بشكل معمق التحديات والرهانات المستقبلية التي تواجه الجزائر في المجال السيبراني، خاصة في ظل التطورات التكنولوجية المتسارعة وتنامي أشكال التهديدات السيبرانية.

- **دراسة إدريس عطية بعنوان "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، كلية الحقوق والعلوم السياسية بجامعة العربي التبسي (2019):**

عالجت هذه الدراسة مسألة التغير في مفهوم التهديدات الأمنية الحاصلة بسبب التطورات في مجال التكنولوجيا، حيث أصبحت قضية الأمن السيبراني من التحديات الكبرى التي تواجهها الدول على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد حجم التهديدات السيبرانية التي تصيب أمن معلومات الدول وتؤدي إلى اختراق أمنها الوطني. وتم التركيز من خلال هذه الدراسة على التصورات الجزائرية في مجابهة المخاطر والتحديات السيبرانية، والتعاطي مع هذه التهديدات وفق منطق التوقع والاحتمال .غير أنها حصرت التحليل في "الردع الأمني" ومكافحة الجريمة، دون بلوغ رهان "تحقيق السيادة الرقمية"، وهو الجانب الذي ستعمل الدراسة الحالية على استكماله.

11/ صعوبات الدراسة

واجهت هذه الدراسة جملة من الصعوبات المنهجية والموضوعية، ويمكن إجمالها فيما يأتي:

1. **الطابع السري للمعلومات:** نظراً لارتباط موضوع الأمن السيبراني بالأمن القومي والدفاع الوطني، واجهت الدراسة صعوبة في الحصول على بعض الإحصائيات الدقيقة والتقارير التقنية المتعلقة بالهجمات السيبرانية، لكون جزء معتبر منها يندرج ضمن المعلومات ذات الطابع السري المرتبطة بالمصالح العليا للدولة.
2. **نقص المراجع المتخصصة:** على الرغم من توفر عدد من الدراسات والمراجع المتعلقة بالجريمة الإلكترونية بصفة عامة، إلا أن هناك نقصاً ملحوظاً في الأدبيات الأكاديمية التي تتناول التهديدات السيبرانية من منظور استراتيجي وأمني مرتبط بحماية السيادة الوطنية الجزائرية.

3. حداثة الموضوع وتسارع تطوره: يعد الأمن السيبراني من المواضيع الحديثة والمتجددة باستمرار، حيث تشهد التهديدات السيبرانية وأساليب الهجوم تطورا متسارعا، بالتوازي مع تحديث التشريعات والاستراتيجيات الوطنية والدولية، الأمر الذي استدعى بذل جهد إضافي لمواكبة المستجدات ومتابعة التطورات المرتبطة بموضوع الدراسة طوال فترة إنجاز البحث.

الفصل الأول: الإطار المفاهيمي والنظري للأمن السيبراني.

تمهيد:

يعد الفضاء السيبراني من أبرز مظاهر التحول التكنولوجي الذي يشهده العالم المعاصر، حيث تجاوز كونه مجرد وسيلة تقنية ليصبح بيئة رقمية متكاملة تتقاطع فيها المصالح السياسية والاقتصادية والأمنية للدول .ومع هذا الاعتماد المتزايد على الأنظمة الرقمية، برزت جملة من التهديدات والمخاطر السيبرانية التي تستهدف البنى التحتية الحيوية، مما جعل من "الأمن السيبراني" ركيزة أساسية ضمن أولويات السيادة الوطنية والأمن القومي .

إن فهم طبيعة المواجهة في هذا الفضاء الافتراضي يستوجب بالضرورة بناء أرضية نظرية ومعرفية صلبة، تبدأ بتحديد ماهية الفضاء السيبراني وفواعله وأبعاد أمنه، ثم الانتقال إلى تشخيص أنماط التهديدات السيبرانية والآليات التقنية والبشرية المستخدمة في تنفيذها .ولا يكتمل هذا الإطار النظري دون الإسقاط على الواقع الدولي عبر استعراض استراتيجيات القوى الكبرى التي صاغت نماذج رائدة في الدفاع والهجوم السيبراني .

وعليه، يسعى هذا الفصل إلى تقديم مقاربة شاملة للأمن السيبراني من خلال ثلاثة مباحث أساسية: يتناول المبحث الأول المقاربة المفاهيمية للفضاء السيبراني وفواعله وأبعاده، بينما يخصص المبحث الثاني لدراسة التهديدات الأمنية السيبرانية وآليات تنفيذها وأنماطها، لينتهي الفصل في المبحث الثالث باستعراض وتحليل تجارب دولية رائدة في صياغة استراتيجيات الأمن السيبراني .

المبحث الأول: مقاربة مفاهيمية للفضاء السيبراني والامن السيبراني

المطلب الأول: مفهوم السيبرانية، الفضاء السيبراني والامن السيبراني

الفرع الأول: تعريف السيبرانية

قاموس المورد يعرف كلمة سايبر (Cyber) بانها علم الضبط ومصدرها (Cyberrnetics)، وبمعنى ادق ضبط الأشياء عن بعد والسيطرة عليها.[1]

وتشُير كلمة "سيبراني" إلى الأنشطة الإلكترونية والحاسوبية.[2]

كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي نوربرت وينر norbert winer وهو أستاذ الرياضيات في معهد ماساشوستس التقني MIM الذي أعطاها مفهومها الاصطلاحي الحديث وكان ذلك عام 1948، اثناء دراسته لموضوع القيادة والسيطرة والاتصال. [3]

وهي مأخوذة من كلمة سيبر وتعني صفة لأي شيء مرتبط بثقافة الحواسيب او تقنية المعلومات او الواقع الافتراضي، فالسيبرانية تعني فضاء الانترنت وهي كلمة مشتقة من الكلمة اليونانية kybernetes التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها القيادة والتحكم عن بعد.[4]

---

[1] منير البعلبكي، قاموس المورد: عربي–إنجليزي (بيروت: دار الملايين، 2004)، ص. 243، تم الاطلاع عليه في 10 مارس 2026
file:///C:/Users/mmmm/Downloads/Noor- Book.com%202%20.pdf

[2] Joseph Ney S, “Cyber power”, Harvard Kennedy School, (2010): p03, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf

[3] بلفرد لطفي لمين، امحند برقوق، "الفضاء السيبراني فواعل وتهديدات"، مجلة افاق للعلوم، مجلد.9، عدد.03، (2024)، ص 622.

[4] احمد عبسي نعمة الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، **مجلة المحقق للعلوم القانونية والسياسية**، ص 214.

يعرف قاموس لاروس الفرنسي كلمة السيبرانية انها علم يدرس آليات الاتصال والتحكم في الآلات وعند الكائنات الحية.[1]

نقول ان السيبرانية هي التحكم او التحكم عن بعد، فعندما تأتي مع كلمة أخرى تعني التحكم بها او ادارتها كما في الامن السيبراني، تعني كيفية التحكم والسيطرة على الجريمة الالكترونية. [2]

أما القوة السيبرانية عرفها جوزيف ناي القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي انها القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في بيئات تشغيلية أخرى وعبر أدوات القوة".[3]

وحسب جوزيف ناي، يمكن استخدام القوة السيبرانية لتحقيق نتائج مرغوبة داخل الفضاء الإلكتروني، أو يمكنه استخدام الأدوات الإلكترونية لتحقيق نتائج مرغوبة في مجالات أخرى خارج الفضاء الإلكتروني.[4]

الفرع الثاني: تعريف الفضاء السيبراني

ظهر مصطلح الفضاء السيبراني في ثمانينيات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الامريكي الكندي ويليام جيبسون، حيث يعتمد هذا المجال الافتراضي على نظم الكمبيوتر وشبكات الأنترنت ومخزون هائل من المعلومات والبيانات، فيتم التواصل بالشبكات عبر الهواتف وأجهزة الحواسيب، وغيرها من دون التقيد بالحدود الجغرافية.[5]

---

[1] Larousse Dictionnaire de français (Malesherbes: Imprimerie Maury, mars 2010) ،p 104 .

[2] فراس جمال شاكر، السيبرانية وتحولات القوة في النظام الدولي (دار أمجد للنشر والتوزيع، 2023)، ص 25.

[3] Joseph Ney, op.cit, p04

[4] Ibid

[5] يوسف بوغرارة، "الامن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني"، **مجلة الدراسات الافريقية وحوض النيل**، المركز الديمقراطي العربي، مجلد.1، عدد.3، (2018)، ص 103.

عرفته الوكالة الفرنسية لأمن أنظمة الاعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي بأنه: مساحة اتصال تتكون من الربط العالمي لمعدات المعالجة الآلية للبيانات الرقمية.[1]

وحسب المفهوم الأمريكي فان الفضاء السيبراني هو مجال عالمي ضمن بيئة المعلومات، ويتألف من شبكات مترابطة من البنى التحتية المترابطة وتكنولوجيات المعلومات، بما في ذلك الانترنت، وشبكات الاتصالات السلكية واللاسلكية، وأنظمة الحاسوب، والعمليات المدمجة، وأجهزة التحكم.[2]

الفضاء السيبراني هو مجال او فضاء تتم داخله عمليات التفاعل عبر شبكات من الحواسيب المترابطة. ولا يقتصر الفضاء الإلكتروني على شبكة الإنترنت وأجهزة الحاسوب فحسب، بل يشمل كذلك جميع الشبكات الخاصة بالحواسيب التي لا يتم الولوج إليها عبر الإنترنت، إضافة إلى ما تحتويه هذه الأجهزة من بيانات ومعلومات. كما أنه مجال لا يشترط وجود الأطراف المتفاعلة ضمن نطاق جغرافي واحد في وقت محدد، إذ يمكن أن تتم التفاعلات فيه بصورة متزامنة أو غير متزامنة، مع إمكانية تواجد الأطراف في أي موقع جغرافي. [3]

"الفضاء السيبراني هو مجال تشغيلي مؤطر باستخدام الإلكترونيات لاستغلال المعلومات عبر أنظمة مترابطة وبنيتها التحتية المرتبطة بها". تعتمد القوة على السياق، وتعتمد القوة السيبرانية على الموارد التي تميز مجال الفضاء السيبراني [4]

الفرع الثالث: تعريف الامن السيبراني

عند تحليل مفهوم الامن السيبراني نجده يتكون من كلمتين "الامن " و "السيبراني"

الأمن لغة:

[1] Agence nationale de la sécurité des systèmes d'information (ANSSI), CyberDico, p 9. Consulté le 5 Avril2026. https://www.info.gouv.fr/upload/media/content/0001/11/a5fcaf7ccf1f6058d70e3a17570037569b979d84.pdf

[2] بلفرد لطفي لمين، المرجع السابق، ص 623.

[3] شفيق نوران، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في ابعاد الامن الالكتروني (المكتب العربي للمعارف، 2016)، ص 23.

[4] Joseph, op.cit, p04.

تناولت الدراسات كلمة الامن مرادفا للطمأنينة وتحقيق حالة من انعدام الشعور بالخوف، واحلال شعور الأمان ببعديه النفسي والجسدي محل الشعور بالخوف. [1]

الامن اصطلاحا:

تعددت الآراء واختلفت حول مفهوم الأمن، رغم شيوع استخدامه، إذ لا يبتعد في جوهره عن معناه اللغوي، غير أنه اكتسب أبعادًا جديدة بفعل تطور العلاقات الدولية وما شهدته من مستجدات.

يقدم هنري كسنجر تعريف للأمن بأنه أي تصرف يسعى المجتمع عن طريقه لتحقيق حقه في البقاء. [2]

عرفه البعض بانه الشعور بالطمأنينة الذي يتحقق من خلال رعاية الفرد والجماعة ووقايتهما من الخروج على قواعد الضبط الاجتماعي من خلال ممارسة الدور الوقائي والقمعي والعلاجي الكفيل بتحقيق هذه المشاعر.[3]

كما يعرف بأنه– الجهد اليومي الذي يصدر من الدولة لتنمية أنشطتها الرئيسية السياسية والعسكرية والاقتصادية والاجتماعية ودفع أي تهديد او تعويق تو اضرار بتلك الأنشطة. [4]

اما باري بوزان barry buzan وهو أحد المختصين في الدراسات الأمنية يعرف الامن على انه –غياب التهديد على القيم الأساسية في المجتمع– ويعتبر تعريف باري بوزان من أحدث تعريفات الامن الأكثر تداولا في الادبيات الأمنية ويراه أيضا انه العمل على التحرر من التهديد، وفي سياق النظام الدولي فهو قدرة الدولة والمجتمعات على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي اعتبرها معادية في سعيها للأمن.[5]

يمكن تعريف الامن السيبراني بأنه امن الشبكات، والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالأنترنت. وعليه فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير

[1] دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، (الإسكندرية: دار الفكر الجامعي، ط.1، 2021)، ص11.
[2] محمد طه السيد، مفهوم الأمن القومي، **مجلة الأمن القومي والاستراتيجية أكاديمية ناصر العسكرية للدراسات العليا**، (2023)، ص 128.
[3] عماد حسين عبد الله، إدارة الامن في المدن الكبرى، (المركز العربي للدراسات الأمنية والتدريب، الرياض 1991)، ص32.
[4] أشرف السعيد احمد، تكنولوجيا المعلومات وحروب الجيل السادس، (2019)، ص51.
[5] عمار بالة، "اسهامات مدرسة كوبنهاغن في توسيع مفهوم الأمن: من الأمن العسكري الى الأمن المجتمعي"، **مجلة الحقوق والحريات**، خنشلة الجزائر، المجلد10، العدد 02 (2022)، ص. 15.

الحماية المفروض اتخاذها او الالتزام بها لمواجهة التهديدات ومنع التعديات او للحد من اثارها في أقسى واسوء الأحوال.[1]

وقد قدمت وزارة الدفاع للولايات المتحدة الأمريكية تعريفا دقيقا لمصطلح الامن السيبراني، فاعتبرته:" جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث. [2]

واعتبرت وكالة الامن الرقمي الاوروبية ان معنى الامن السيبراني هو قدرة النظام المعلوماتي على مقاومة محاولات اختراق التي تستهدف البيانات.[3]

يعرف كل من **Neittaanmäki Pekka,Lehto Martti** الامن السيبراني "على أنه مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة."[4]

التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول" اتجاهات الاصلاح في الاتصالات للعام 2011-2010"، "هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادئ توجيهية، ومقاربات إدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".[5]

لأمن السيبراني هو مجموعة القوانين والإجراءات والتقنيات والآليات التنظيمية التي تعتمدها الدولة أو المؤسسة بهدف حماية الأنظمة المعلوماتية والشبكات والبيانات من التهديدات والهجمات السيبرانية، وضمان سرية المعلومات وسلامتها وتوافرها، بما يحقق استمرارية العمل وتقليل المخاطر في الفضاء السيبراني.

---

[1] منى الأشقر جبور: السيبرانية هاجس العصر، (المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية)، ص.25.

[2] جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والافاق المستقبلية، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد 1، (2019)، ص.5.

[3] يوسف بوغرارة، المرجع السابق، ص 107.

[4] جمال بوازدية، المرجع السابق، ص5.

[5] المرجع نفسه، ص 6.

المطلب الثاني: الفواعل في الفضاء السيبراني

الفضاء السيبراني هو مسرح للتفاعل بين مختلف الفواعل، يحدد جوزيف ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبرانية:

الفرع الأول: الفواعل الدولاتية

تمثل الدول الفاعل المحوري والأكثر قوة في مجال الفضاء السيبراني رغم انتشار القوة للأفراد والمؤسسات الجماعات الارهابية في هذا المجال الا ان الدولة حافظت على مكانتها على رأس هذه الفواعل بحكم تفوقها التكنولوجي وامتلاكها الموارد والإمكانات البشرية والمؤسسية التي تمكنها من بسط النفوذ وإحكام السيطرة في هذا المجال. كما تتمتع الدول بالقدرة على وضع وصياغة السياسات الوطنية والدولية المرتبطة بالأمن السيبراني، وتوظف هذا الفضاء ضمن استراتيجياتها الأمنية والدفاعية لتحقيق مصالحها وحماية أمنها القومي[1].

ففي نهاية 2008 استطاعت حوالي 180 دولة ان تمتلك ترسانة من الأسلحة الالكترونية. وتسعى عديد من الدول الى تطوير قدرتها في هذا المجال نتيجة لما يقدمه الفضاء الالكتروني من فرص للفواعل لتحقيق مصالحهم. وهنا وجب التأكيد على قدرة الدولة على السيطرة على المجال البري والبحري والجوي، وكذا الفضاء الإلكتروني لما تملكه من مقومات وأمن ومرافق وتنظيم ومنشئات الدالة على المفهوم الصلب للسيادة.[2]

الفرع الثاني: الفواعل الغير الدولاتية

حيث يلعب الفواعل من غير الدول دورا كبيرا في مجال الفضاء الالكتروني سواء من حيث التفاعل أومن حيث التأثير، ويمكن رصد الفواعل التالية:

1. المنظمات الغير حكومية:

لا تقتصر مصادر الهجمات الالكترونية على الدول فقط، بل قد تصدر أيضا من الفواعل من غير الدول كالمنظمات غير الحكومية، وان كانت لا تمتلك القدرات ذاتها التي تمتلكها

[1] دحان حزام القريطي، المرجع السابق، ص 21.
[2] شفيق نوران، المرجع السابق، ص 40.

الدول والحكومات للقيام بهجمات الكترونية معقدة، فإن أنشطتها قد تقتصر غالبا على استهداف مواقع إلكترونية، بغرض تحقيق مكاسب سريعة قبل أن تتمكن السلطات المختصة من اكتشافها واتخاذ الإجراءات القانونية اللازمة بحقها. ويعتبر أخطر أنواع هذه المنظمات هي المنظمات الاجرامية حيث بدأت هذه هذه الاخيرة التي تتخذ الفضاء الالكتروني لها كمجال وحيد فقط مثل منظمة"Yakuza "اليابانية، او منظمة" Asian Triads " التي تمتهن غسيل الاموال والابتزاز والاحتيال المالي، القرصنة، والتجسس الصناعي لتحقيق مكاسب هائلة.[1]

2. الشركات المتعددة الجنسيات:

تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكرا على الدول، فخوادم شركات مثل: جوجل Google وفيسبوك Facebookوميكروسوفت Microsoft وآبل AppleوأمازونAmazon، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها، وهذا ما حدث في فضيحة تسريب بيانات مستخدمي فايسبوك لصالح شركة "كامبردج أناليتيكا" التي تم الاستعانة بها لصالح حملة الرئيس الأمريكي ترامب.[2]

3. الجماعات الإرهابية:

تعد من أبرز الفواعل الدولية، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.[3]

الفرع الثالث: الأفراد

---

[1] المرجع نفسه، ص ص. 44، 45 .

[2] إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، **مجلة العلوم القانونية والسياسية**، المجلد 10، العدد1 (2019)، ص. 4.

[3] إسماعيل زروقة، المرجع السابق، ص .5.

أصبح الافراد، بفضل تطور الفضاء السيبراني، فواعل مؤثرين في العلاقات الدولية، وعموما يمتلكون مهارات عالية وقد ساعدت تكنولوجيا المعلومات والاتصالات والانترنت الأفرد على امتلاك القوة السيبرانية.[1]

المطلب الثالث: ابعاد الامن السيبراني

1. **البعد العسكري:** يوفر الامن السيبراني للقوات المسلحة تسهيل تبادل المعلومات وسرعة إصدار الأوامر، مما يعزز تحقيق الأهداف العسكرية عم ضرورة امتلاك القدرة على التصدي لأي محاولة اختراق للشبكات التي تستهدف قواعد البيانات العسكرية.[2]

2. **البعد الاقتصادي:** تظهر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الاقتصادي لان الفضاء الإلكتروني أصبح أساسا للتعاملات التجارية والمالية والاقتصادية وأصبح الحاسوب أداة لتسيير الصناعة والاقتصاد وهذا يستدعي الحرص على تحقيقه.[3]

3. **البعد الاجتماعي:** تعتبر الشبكة الدولية للمعلومات مجالا مفتوحا لجميع الأفراد، حيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية، وهنا يجب التنويه إلى ضرورة التحسيس بأخلاقيات الامن السيبراني.[4]

4. **البعد السياسي:** للدولة الحق في حماية نظامها السياسي ومصالحها، وتجدر الإشارة الى ان موازين القوى تغيرت حيث اصبح بإمكان المواطن ان يتحول الى لاعب أساسي واصبح بإمكانه الاطلاع على خلفيات القرارات السياسية عبر الكم الهائل من المعلومات التي سهل عليه الوصول لها عن طريق الانترنت، و هنا نشير إلى التسريبات للوثائق الحساسة مثلا والتي تثير مشكلات عويصة، و أيضا دور شبكات التواصل الاجتماعي

[1] فراس جمال شاكر، المرجع السابق، ص. 185.

[2] جيلالي شويرب، فائزة مراد، مفهوم الحروب السيبرانية والامن السيبراني، **مجلة الحقوق والحريات**، المجلد 11، العدد 1، (2023)، ص 10.

[3] المرجع نفسه.

[4] يوسف بوغرارة، المرجع السابق، ص. 108.

في تنظيم الدعايات السياسية و الانتخابية ، و تنظيم التظاهرات الافتراضية و افتعال الاحتجاجات الإلكترونية ، وأصبح الفضاء السيبراني ملاذا للتجنيد مم طرف التنظيمات الإرهابية و العديد من الايديولوجيات و الدعايات الدينية مما أصبح يهدد تماسك المجتمع.[1]

5. **البعد القانوني** :يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية لحل النزاعات التي يمكن أن تنشأ عنها. وهو ما يستدعي مواكبة

التحولات التي رافقت ظهور مجتمع المعلومات. فظهرت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الأنترنت، والحق في حماية ملكية البرامج المعلوماتية. كما ظهرت موجبات جديدة، ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الابلاغ عن مخالفات وجرائم خاصة بالمحتوى .كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات.[2]

[1] المرجع نفسه، ص. 109.

[2] سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، جامعة قاصدي مرباح ورقلة، ص. 6.

المبحث الثاني: التهديدات الأمنية السيبرانية

المطلب الأول: مفهوم التهديد السيبراني

التهديد السيبراني هو برنامج ضار آت من الفضاء السيبراني يهدف إلى المساس بأمن الميكروكمبيوتورات والهواتف الذكية والأجهزة اللوحية والشبكات وغيرها من الأشياء المتصلة بالأنترنت. يمكن أن يكون مرتكب التهديد السيبراني شخصا أو دولة أو مجموعة او قراصنة أو منظمة ذات أهداف جيوسياسية.[1]

"أي ظرف أو حدث ينطوي على إمكانية التأثير سلبا على العمليات التنظيمية أو الأفراد من خلال نظام معلومات عن طريق الدخول غير المصرح به أو التدمير أو الكشف أو تعديل الحكومات والخدمات" [2]

التهديدات السيبرانية هي تلك التهديدات التي تواجه النظم المعلوماتية وإمكانية ممارسة اعمال القرصنة المعلوماتية بأبعادها المختلفة، فإمكانية اختراق تلك النظم من شأنه ان يخلق تهديدات امنية خطيرة كالتأثير على حركة الطيران والمعاملات والتجارة الالكترونية والاعمال البنكية والمؤسسات وغيرها، التي تستخدم الأساليب الالية الحديثة في المعاملات، هذا إضافة الى إمكانية اختراق منظومات الاتصال والتحكم في إدارة العمليات.[3]

المطلب الثاني: أساليب تنفيذ الهجمات السيبرانية

اليات تنفيذ التهديدات او الهجمات السيبرانية هي تلك الأدوات والطرق والأساليب لتنفيذ الهجوم السيبراني، وقد شهدت تطورا كبيرا في السنوات الأخيرة، وتتميز بالتعقيد بما يمكنها من اختراق الأنظمة واحداث اضرار بالغة، ومن اهم اليات تنفيذ الهجمات السيبرانية ما يلي:

---

[1] ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، **مجلة الأبحاث في الحماية الاجتماعية**، المدرسة العليا للضمان الاجتماعي محمد الصالح منتوري، (2022)، ص. 5.

[2] NIST, Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1, 2012, p. 4.

[3] سيد علي بدرين، "الاستراتيجية الأمنية الجزائرية لمواجهة التهديدات السيبرانية"(مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2023)، ص. 42.

1. **هجمات التصيد Phishing:** يعتمد هذا الأسلوب على الهندسة الاجتماعية Social Engineering من خلال تحفيز الضحية لفتح رابط يحتوي على برمجية خبيثة تصيب الجهاز، وذلك من خلال ارسال رسائل تحتوي على موضوعات قد تكون من اهتمام الضحية، او استخدام أسماء قد تكون مألوفة بالنسبة لها، مع ارفاق احدى البرمجيات الخبيثة بهذه الرسائل. وبمجرد قيام الضحية بفتح الرسالة تبدأ عملية القرصنة. ويعتبر البريد الالكتروني والرسائل الشخصية والتطبيقات التي يتم تنصيبها على مواقع التواصل الاجتماعي من أكثر الاشكال شيوعا.[1]

2. **هجمات وقف الخدمة DDOS:** هي أحد أخطر اشكال الهجمات السيبرانية، حيث يتم استخدام برامج كمبيوتر مخصصة لهذا الغرض، او السيطرة على عدد كبير من أجهزة الكمبيوتر وتكوين شبكة روبوتية، يستخدمها الهاكرز في إطلاق هجمة الكترونية ضخمة على الضحية، واغراقها بالآلاف من الرسائل والطلبات التي تؤدي في النهاية الى انقطاع الخدمة ووقفها، سواء كان ذلك موقع انترنت، او خدمة الكترونية خاصة او حكومية. [2]

3. **البرمجيات الخبيثة:** البرمجيات الخبيثة هي برامج أو شيفرات تصمم عمدا لإلحاق الضرر بالأنظمة الحاسوبية أو للقيام بأنشطة غير مشروعة على الجهاز المصاب. يشمل هذا المصطلح أنواعا متعددة من التهديدات الرقمية، أبرزها: الفيروسات التي تصيب الملفات وتنتشر بينها، وأحصنة طروادة التي تبدو كبرامج شرعية لكنها تخفي وظائف ضارة، والديدان القادرة على التكاثر والانتشار عبر الشبكات، وبرامج التجسس التي تراقب نشاط المستخدم لجمع المعلومات، إضافة إلى البرامج الإعلانية الضارة. تصل هذه البرمجيات إلى الأجهزة بطرق مختلفة مثل مرفقات البريد الإلكتروني الخبيثة، تحميل برامج مجهولة أو مزيفة من الإنترنت، أو استغلال الثغرات الأمنية أثناء تصفح المواقع. وبعد الإصابة، تنفذ مهاماً ضارة كسرقة البيانات الحساسة (ككلمات المرور)، تسجيل ضغطات لوحة المفاتيح، فتح أبواب خلفية

[1] فراس جمال شاكر، المرجع السابق، ص ص. 223-224.
[2] المرجع نفسه.

للمهاجمين، أو تعطيل النظام وإتلاف الملفات. تُعد البرمجيات الخبيثة خطراً رئيسياً في مجال الأمن السيبراني بسبب تنوعها وتطور أساليبها، مما يستوجب الحذر عند التعامل مع الملفات والبرامج غير الموثوقة[1].

4. **الهندسة الاجتماعية:** هي أسلوب اختراق لا يعتمد على وسائل تقنية معقدة، بل يستهدف العنصر البشري من خلال خداع الأفراد والتلاعب بهم لدفعهم إلى كشف معلومات سرية أو تنفيذ إجراءات تخدم المهاجم. فهي تستغل نقاط الضعف النفسية بدلاً من استهداف الأجهزة أو البرمجيات مباشرة.

تتنوع أساليبها، مثل انتحال صفة شخص موثوق (كموظف دعم فني)، إرسال رسائل تبدو رسمية، الادعاء بوجود مشكلة تتطلب كلمة مرور، أو طلب إذن دخول معين. ومن خلال هذه السيناريوهات الكاذبة، ينجح المهاجم في كسب ثقة الضحية ودفعها للإفصاح عن معلومات حساسة أو القيام بإجراء يخدم الهجوم، كالنقر على رابط ضار أو تشغيل ملف مرفق.[2]

المطلب الثالث: أشكال التهديدات السيبرانية

تتعدد أنماط التهديدات او الهجمات السيبرانية التي يتم فيها استخدام الأسلحة السابق ذكرها نذكر ما يلي:

1. **التجسس السيبراني:**

التجسس السيبراني Cyber espionage هو القيام باختراق شبكة او جهاز الكتروني بهدف الحصول على المعلومات السرية الموجودة عليه والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء كانت معلومات عسكرية او اقتصادية او تجارية او صناعية او غيرها. [3]

[1] فهد قطينة، الهجمات السيبرانية دليل أشهر أنواع الهجمات السيبرانية الشامل، أكاديمية الامن السيبراني، ص 6.
[2] المرجع نفسه، ص ص. 5، 6.
[3] شفيق نوران، المرجع السابق، ص 30.

2. الجريمة السيبرانية:

الجريمة السيبرانية هي فعل يتسبب بضرر جسيم للأفراد او الجماعات المؤسسات بهدف ابتزاز الضحية وتشويه سمعتها من اجل تحقيق مكاسب مادية او خدمية، واهداف سياسية باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الانترنت. [1]

يعرفها الفقيه الفرنسي **Masse** بأنها الاعتداءات غير القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح. [2]

هذا النوع من الجرائم يستهدف نقاط الضعف في الشبكات والبنى التحتية عبر الانترنت للدول والمؤسسات او الافراد، حيث يستخدم خلاله المجرمون برمجيات خبيثة.

3. الإرهاب السيبراني:

هو عمل اجرامي الكتروني، يستخدم فيه وسائل اتصال كسلاح ينتج عنه عنف وتدمير او بث الخوف تجاه المستهدف سواء كان فردا او مؤسسة او دولة، والهدف التأثير على الحكومات او السكان، عادة ما يمثل اجندة سياسية او اجتماعية او فكرية معينة. [3]

يعرف الإرهاب السيبراني بأنه هجمات غير مشروعة أو تهديدات تستهدف الحواسيب أو الشبكات أو البيانات المخزنة إلكترونيا، ويكون الهدف منها الانتقام أو الابتزاز أو الإكراه أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي لتحقيق اهداف سياسية أو دينية أو اجتماعية معينة. كما ان الإرهاب السيبراني يتخذ شكل التخويف أو التهديد، سواء كان ماديا أم معنويا، عبر الوسائل الإلكترونية، مما يؤدي إلى إلحاق أضرار نفسية أو عقلية أو مالية بالأفراد أو الجماعات أو الدول.[4]

كما يعد الإرهاب السيبراني نشاطا أو هجوما منظما تحركه دوافع سياسية، ويستهدف إثارة الرعب لدى الرأي العام، مستفيدا من الفضاء الإلكتروني كوسيلة لتنفيذ عملياته. ويتم ذلك من

[1] فراس جمال شاكر، المرجع السابق، ص 42.
[2] المرجع نفسه، ص. 37.
[3] المرجع نفسه، ص. 48.
[4] سيد غلي بدرين، المرجع السابق، ص 50.

خلال توظيف التقنيات الرقمية الحديثة التي قد تلحق أضرارا بالبنية التحتية الحيوية للدول والشعوب، وما يترتب عليها من خسائر اقتصادية وبشرية جسيمة. [1]

ومن خلال ما سبق، يتضح أن الإرهاب السيبراني لا يختلف في جوهره عن إرهاب الجماعات المسلحة، بل قد يكون أشد خطرا نظرا لصعوبة التصدي له وتحديد مرتكبيه، خاصة وأنهم غالبا ما ينفذون هجماتهم من خارج حدود الدول المستهدفة، مما يؤدي إلى أضرار بالغة بتلك الدول.

4. الحرب السيبرانية:

تعرف الحرب السيبرانية في الادبيات الاستراتيجية على انها استخدام مقصود ومنظم لقدرات رقمية هجومية من اجل احداث ضرر او شلل او اختراق في أنظمة حيوية تابعة لخصم سياسي او عسكري ضمن سياق صراع بين الدول او الجهات السياسية المتنافسة، ويشمل ذلك الهجمات التي نهدف الى التأثير في القرار السياسي او تعطيل البنية التحتية او حتى المساس بالاستقرار الاجتماعي من خلال التشويش على المعلومات ونشر الفوضى الإعلامية. [2]

وتعد الحرب السيبرانية من أبرز مظاهر الصراعات الحديثة، حيث تتميز بعدة خصائص تجعلها مختلفة عن الحروب التقليدية. فهي لا تقتصر على الدول والجيوش فقط، بل يشارك فيها أيضا فاعلون غير حكوميين كالقراصنة والجماعات الإجرامية، كما يصعب في كثير من الأحيان تحديد مصدر الهجمات بسبب إمكانية إخفاء الهوية الرقمية. إضافة إلى ذلك، لا تميز الحرب السيبرانية بين الأهداف العسكرية والمدنية، إذ قد تستهدف البنى التحتية الحيوية مثل المستشفيات وشبكات النقل والمؤسسات الحكومية ووسائل الإعلام، بل قد تُستعمل أجهزة المدنيين نفسها في تنفيذ الهجمات دون علمهم، كما هو الحال في هجمات حجب الخدمة الموزعة (DDoS). وتتميز هذه الحرب كذلك بسرعة تنفيذ الهجمات وطابعها الخفي، حيث يمكن أن تُحدث خسائر كبيرة خلال وقت قصير أو تبقى البرمجيات الخبيثة كامنة لفترات

[1] عتيقة كواشي، "تداعيات الإرهاب السيبراني على الامن القومي الجزائري"، المجلة الجزائرية للأمن والتنمية، المجلد 12، العدد (2023) ص 208.

[2] علاء الدين حسين خماس، الحرب السيبرانية مستقبل الحروب في عالم ما وراء الجغرافيا دراسة استراتيجية في طبيعة حروب القرن الحادي والعشرين في العصر الرقمي، (الأردن عمان: شركة دار الأكاديميون للنشر والتوزيع، 2025)، ص ص. 24،25.

طويلة قبل تفعيلها. ومن ثمّ، فإن الحرب السيبرانية لا تمثل مجرد تطور تقني، بل تعكس تحولا عميقًا في طبيعة الصراعات الحديثة، لما تفرضه من تحديات على مفاهيم السيادة والأمن الوطني والاستقرار الدولي. [1]

[1] علاء الدين حسين مكي خماس، المرجع السابق، ص ص 25-27.

المبحث الثالث: استراتيجيات الدول الرائدة للأمن السيبراني

المطلب الأول: الإستراتيجية الصينية للأمن السيبراني

أصبح الأمن السيبراني يمثل أولوية رئيسية لدى القيادة الصينية، حيث أعلن الرئيس الصيني شي جين بينغ أن بلاده تسعى لتصبح "قوة إلكترونية"، وهو هدف يتضمن جوانب اقتصادية وتكنولوجية متنوعة .يُعتبر الأمن السيبراني ركيزة أساسية لدعم هذا الاتجاه وتحقيق تلك الأهداف. وبنهاية عام 2017، أصدرت الصين مجموعة من الوثائق الأساسية التي تضمنت الاستراتيجية الوطنية للأمن السيبراني، واستراتيجية التعاون الدولي في المجال السيبراني، بالإضافة إلى قانون الأمن السيبراني. شكلت هذه الوثائق ركائز الإطار التنظيمي للفضاء السيبراني في الصين، حيث رسمت ملامحه ووضحت مسؤوليات العديد من الفاعلين في هذا المجال[1].

في البداية، كان تركيز الصين الرئيسي داخليا يهدف الى منع انتشار الأفكار الليبرالية الغربية عبر الإنترنت، وقد تبنت مفهوم "السيادة السيبرانية" الذي يسمح للدول بالسيطرة على جزء الإنترنت الذي يقع ضمن سيادتها. ولتفعيل هذا المفهوم، نفذت الصين مشروع "الدرع الذهبي Golden Project Shield" أو"الجدار الناري العظيم[2]" للرقابة والتصفية وبدأت حظر بعض التطبيقات الأمريكية مثل فيسبوك وتويتر ويوتيوب بسبب تعارضها مع قوانين الرقابة الصينية. [3]

---

[1] هيشام داود الغنجة، جيوبوليتيكا الأمن السيبراني؛ دراسة حالة الصراع الصيني الأمريكي في الفضاء السيبراني، **مجلة الفكر القانوني والسياسي**، م.9، ص ص. 8،9.

[2] **مشروع الدرع الذهبي، أو "جدار الحماية العظيم للصين"**، مبادرة تديرها وزارة الأمن العام التابعة للحكومة الصينية. يركز هذا المشروع على مراقبة وحجب ما يمكن وما لا يمكن الاطلاع عليه عبر شبكة الإنترنت في الصين. بدأ هذا المشروع سنة 1998، ولا يزال يشهد تطويرًا مستمرًا في تقنيات التقييد من خلال عدة أساليب.

[3] وائل خليل الرحمان بوطمين، "البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة"،(مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2025)، ص 77.

وفي هذا السياق، يزعم المسؤولون الصينيون أن العقيدة العسكرية للصين تتميز بالطابع الدفاعي، والنقاط الأساسية للاستراتيجية الصينية من خلال المبادئ التالية:[1]

أولاً :التصدي ومواجهة أي شكل من أشكال العدوان؛

ثانيا: حماية الأمن الوطني السياسي والسيادة الوطنية والوحدة والسلامة الإقليمية؛

ثالثا: حماية حقوق الصين ومصالحها البحرية، والدفاع عن مصالح الصين في الخارج؛

رابعا :تعزيز التنمية المستدامة للدولة.

من خلال دراسة الاستراتيجية الصينية للأمن السيبراني التي صدرت في عام2017 عن إدارة الفضاء السيبراني، يمكن استنتاج عدة نقاط أساسية:

تؤكد الصين أولًا أن الفضاء السيبراني يتساوى مع غيره من المجالات فيما يتعلق بمبدأ السيادة، حيث تعتبر السيادة السيبرانية جزءا أساسيًا من سيادتها الفعلية.

ثانيا: تؤكد الصين أنها لا تهدف الى السيطرة على الفضاء السيبراني، لكنها في الوقت نفسه تعلن جاهزيتها لمواجهة أي تهديد قد يتعرض لأمنها في هذا السياق.

ثالثًا، اعتماد الصين لاستراتيجية الأمن السيبراني لا يعني إغلاق السوق المحلية أمام الشركات او الأطراف الأجنبية، بل يتعلق أساسا بخضوع جميع الفاعلين، سواء كانوا محليين أو دوليين، لرقابة تتماشى مع توجهاتها الاستراتيجية والسياسات التي تسعى لتنفيذها.[2]

لذا، يمكن الإشارة إلى أن طموحات الصين في الأمن السيبراني تتماشى مع استراتيجيتها العامة للأمن الوطني، حيث تهدف من خلالها الى تعزيز أهدافها الاقتصادية وتوسيع نفوذها الناعم في الفضاء السيبراني ويعتبر ذلك من أبرز علامات التنافس السيبراني.

[1] هيشام داود الغنجة، المرجع السابق، ص .8.

[2] هيشام داود الغنجة، المرجع السابق، ص 9.

المطلب الثاني: الإستراتيجية الامريكية للأمن السيبراني.

تعود البدايات الفعلية للسياسات السيبرانية الامريكية الى عام 1998، حين أصدر الرئيس بين كلينتون التوجيه الرئاسي رقم 63 بشأن حماية البنية التحتية الحيوية، ويعتبر اعتراف رسمي بان الامن القومي لم يعد مرتبطا فقط بالقواعد العسكرية والجيوش، بل أصبح يشمل أيضا أنظمة الكهرباء والاتصالات والمصارف التي اصبحت تعتمد على تقنيات رقمية متصلة. وتلا ذلك تشكيل أولى الفرق الفيدرالية المعنية بأمن الفضاء الرقمي، بالتنسيق بين وزارة الدفاع ووكالة الأمن القومي وهيئات الاستخبارات. [1]

وفي عام 2009 تم تأسيس القيادة السيبرانية الامريكية (US Cyber Command) وهي وحدة مستقلة داخل القيادة الاستراتيجية للقوات المسلحة، تتولى مسؤولية الدفاع عن أنظمة وزارة الدفاع، وتنفيذ عمليات هجومية عند الضرورة. وبتأسيس هذه القيادة أوضحت الولايات المتحدة الامريكية ان الفضاء السيبراني هو ميدانا للحرب ولا يقل أهمية عن البر والبحر والجو والفضاء الخارجي وأن العمليات الرقمية أصبحت جزءا من أدوات القوة الصلبة في العقيدة الامريكية.[2]

تمت صياغة في مارس 2026 وثيقة تحت عنوان "الاستراتيجية السيبرانية للرئيس ترامب من أجل أمريكا" وتعتبر رؤية شاملة لتعزيز التفوق الأمريكي في الفضاء الإلكتروني، وتركز على حماية البنية التحتية، وتعزيز الابتكار، وردع الخصوم. وتحظى الاستراتيجية باهتمام بالغ بالنظر إلى تصاعد أهمية القوة السيبرانية في التفاعلات الدولية.

جاءت الأولوية في الاستراتيجية لاستعادة الردع، والدفاع الاستباقي السيبراني، مع تأكيد توظيف واشنطن لكل الامكانات المتاحة في عملياتها السيبرانية الدفاعية والهجومية.[3] يؤشر ذلك إلى حجم التهديدات التي تواجه الولايات المتحدة عبر الفضاء السيبراني، حيث أن على

[1] علاء الدين حسين خماس، المرجع السابق، ص. 165.

[2] المرجع نفسه، ص 166.

[3] President Trump's CYBER STRATEGY for America, March 2026, P.3. Accessed April 20, 2026 https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf

مدار عام 2025 سجلت الولايات المتحدة 31,020 حادثة إلكترونية تم الإبلاغ عنها، وهي أعلى نسبة على مستوى العالم ما جعلها تتصدر قائمة الدول الأكثر تعرضاً للهجمات السيبرانية.[1]

تمنح الاستراتيجية أولوية قصوى لتشكيل سلوك الخصوم عبر استخدام كافة القدرات الدفاعية والهجومية في الفضاء السيبراني، وشن هجمات سيبرانية استباقية انطلاقاً من أن الهجوم وسيلة للدفاع، وتوسيع نطاق التعاون مع القطاع الخاص لتعطيل شبكات التهديد او الخصوم. [2]

وتأكد أن ضمان الأمن السيبراني يتطلب جهد جماعي، حيث تتكامل جهود الحكومة الأمريكية والأفراد والشركات لمواجهة الهجمات السيبرانية، وأن على كل أمريكي اتخاذ تدابير فعلية لحماية نفسه وأسرته في الفضاء السيبراني.[3]

بالإضافة الى تحديث وتأمين شبكات الحكومة وأنظمة المعلومات الفيدرالية لضمان الأمن السيبراني من خلال الانتقال الحوسبة السحابية وتعزيز أمن العملات المشفرة وتقنيات سلسلة الكتل (البلوك تشين)، واعتماد التشفير ما بعد الكمي (Post-Quantum Cryptography)، وتطبيق نموذج الثقة الصفرية (zero-trust architecture) مع تطوير البحث والابتكار في هذه المجالات التقنية لاسيما الحوسبة الكمومية والذكاء الاصطناعي.[4]

أما العنصر السادس من الاستراتيجية يركز على العنصر البشري كرصيد استراتيجي "يحمي الشعب الأمريكي والوطن وأسلوب الحياة الأمريكي". من خلال تبني مسار لتطوير ودعم المواهب والمهارات السيبرانية عبر المؤسسات التعليمية والشركات "لبناء قوى عاملة سيبرانية عالية الكفاءة". [5]

---

[1] تهديدات الجرائم الإلكترونية: أهم 10 دول مستهدفة في عام 2025، موقع CloudSEK، 13 فيفري 2026، تاريخ التصفح 29 مارس 2026. https://www.cloudsek.com/ar/knowledge-base/countries-most-targeted-by-cyberattacks

[2] President Trump's CYBER STRATEGY for America, op.cit, P. 4

[3] Ibid, P. 5.

[4] Ibid.

[5] Ibid, P. 6.

تنتقل هذه الاستراتيجية من الموقف الدفاعي إلى موقف أكثر هجومية واستباقية، حيث تجمع بين القوة العسكرية التقنية، والابتكار الاقتصادي، وبناء المواهب لضمان بقاء الولايات المتحدة القوة السيبرانية المهيمنة عالمياً.

المطلب الثالث: الاستراتيجية الروسية للأمن السيبراني

تعد روسيا من أوائل الدول التي أولت اهتماماً كبيراً بقضايا الأمن السيبراني وأمن المعلومات على المستوى الدولي، حيث بادرت سنة 1998 بطرح أول مشروع قرار أمام الجمعية العامة للأمم المتحدة يتعلق بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي. وقد تبنت روسيا رؤية استراتيجية تربط الأمن السيبراني بشكل مباشر بمفهوم السيادة الوطنية والأمن القومي، إذ تسعى إلى تعزيز "السيادة التكنولوجية" من خلال تقليل التبعية للتكنولوجيا الغربية وتطوير بدائل وطنية في مجالات البرمجيات والمعدات الرقمية الحساسة. كما لا تقتصر المقاربة الروسية على الجوانب التقنية فقط، بل تمتد إلى مفهوم "أمن المعلومات" بمفهومه الواسع، الذي يشمل حماية الفضاء المعلوماتي والفكري والمجتمعي من التأثيرات الخارجية والحملات الإعلامية المضللة[1].

وقد تعزز هذا التوجه مع تحديث عقيدة أمن المعلومات الروسية، خاصة نسخة سنة 2016، التي وضعت الأمن السيبراني ضمن أولويات الدفاع الوطني، واعتبرت الهجمات الإلكترونية من أبرز التهديدات التي تستهدف استقرار الدولة وبنيتها التحتية الحيوية[2]. كما قامت روسيا بإنشاء عدة مؤسسات متخصصة في الأمن الإلكتروني، من بينها مجلس الأمن الروسي، وجهاز الأمن الفيدرالي، والجهاز الفيدرالي للتحكم التقني، ووزارة الاتصالات وتكنولوجيا

[1] وائل خليل الرحمان بوطمين، المرجع السابق، ص ص. 89،90.

[2] المرجع نفسه، 93،94.

المعلومات، إضافة إلى إنشاء قيادة سيبرانية مستقلة داخل الجيش الروسي لتعزيز قدرات الردع والدفاع الإلكتروني[1].

وتقوم الاستراتيجية الروسية كذلك على توظيف القدرات السيبرانية الهجومية في إطار الحروب الإلكترونية، من خلال استهداف البنية التحتية المعلوماتية للخصوم والتأثير على أنظمتهم المدنية والعسكرية، إضافة إلى استخدام حملات التضليل الإعلامي والتأثير في الرأي العام لخدمة المصالح الروسية. وقد ظهر ذلك بوضوح في الهجمات الإلكترونية التي نسبت إلى روسيا ضد Georgiaسنة 2008 قبل التدخل العسكري الروسي. كما تؤكد العقيدة العسكرية الروسية لسنة 2010 على التكامل بين الوسائل العسكرية وغير العسكرية، مع إعطاء أهمية متزايدة لحرب المعلومات والفضاء الإلكتروني. [2]

[1] عصام محمد أمانى، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، **مجلة كلية الاقتصاد والعلوم السياسية**، (2021)، ص. 173.

[2] عصام محمد أمانى، المرجع السابق، ص 172.

خلاصة الفصل الأول:

نخلص في نهاية هذا الفصل إلى أن الأمن السيبراني لم يعد ترفاً تقنياً، بل أصبح ضرورة وجودية للدولة الحديثة في ظل تعاظم الفضاء السيبراني وتداخل فواعله. فمن خلال المقاربة المفاهيمية والنظرية، يتضح أن هذا الفضاء يتميز بخصائص فريدة تجعل من التهديدات السيبرانية خطراً عابراً للحدود، يصعب التنبؤ به أو احتواؤه بالوسائل الأمنية التقليدية، مما يفرض تبني استراتيجيات دفاعية وهجومية متطورة.

لقد كشفت دراسة التجارب الدولية الرائدة (الصين، الولايات المتحدة، وروسيا) عن وجود تباين في المنطلقات الاستراتيجية، حيث تتراوح بين التركيز على السيادة الرقمية والتحكم في المحتوى، وبين التفوق التكنولوجي والردع السيبراني. ورغم هذا التباين، فإن القاسم المشترك بين هذه القوى هو الإدراك العميق بأن الفضاء السيبراني هو "المجال الخامس" للحروب، وأن الاستثمار في العنصر البشري والبنية التحتية المعلوماتية هو الضمان الوحيد للأمن القومي.

الفصل الثاني: آليات مواجهة التهديدات السيبرانية في الجزائر

تمهيد

في ظل التزايد المستمر للتهديدات السيبرانية وما قد تسببه من مخاطر على أمن الدول واستقرارها، أصبحت مسألة تعزيز الأمن السيبراني من الأولويات الأساسية للسياسات الوطنية. وفي هذا الإطار، عملت الجزائر على تبني مجموعة من التدابير القانونية والمؤسساتية بهدف حماية فضائها السيبراني والتصدي لمختلف الهجمات والجرائم الإلكترونية، من خلال سنّ تشريعات متخصصة وإنشاء هيئات ومؤسسات مكلفة بتأمين الأنظمة المعلوماتية.

ويهدف هذا الفصل إلى دراسة الاستراتيجية الجزائرية لمواجهة التهديدات السيبرانية، من خلال التطرق إلى الإطار القانوني والمؤسساتي للأمن السيبراني في الجزائر، ثم إبراز أهم محاور الاستراتيجية الوطنية، خاصة ما يتعلق بحماية البنى التحتية الحيوية، وتعزيز التكوين والتحسيس، وتطوير التعاون الوطني والدولي في المجال السيبراني. كما يتناول الفصل تأثير التهديدات السيبرانية على الأمن الوطني الجزائري، من خلال تحليل أشكال هذه التهديدات وانعكاساتها المختلفة على الجوانب الأمنية والاقتصادية والسياسية للدولة.

يُصادق المرسوم الرئاسي رقم 25–321، الموقع في 30 ديسمبر 2025، على الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025–2029، بهدف تعزيز حماية الإدارات العمومية والبنى التحتية الرقمية للدولة. تتضمن الاستراتيجية اربعة محاور: [1]

1. القدرات التقنية–العملياتية.
2. الإطار القانوني والتنظيمي والمعياري.
3. التكوين والبحث والتطوير والتحسيس .
4. التعاون الوطني والدولي

[1] وكالة أمن الأنظمة المعلوماتية. الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025–2029.

المبحث الأول: الإطار القانوني والمؤسساتي للأمن السيبراني في الجزائر

المطلب الأول: الإطار القانوني والتنظيمي للفضاء الرقمي في الجزائر

الفرع الأول: التكريس الدستوري لحماية الفضاء الرقمي والبيانات

تظهر المراجعات الدستورية المتتالية تطورا تدريجيا في تكريس الحماية القانونية للفضاء الخاص، استجابة للتحولات التكنولوجية وازدياد الاعتماد على الوسائط الرقمية :

1. دستور1996

يشكل الإطار القانوني أحد الركائز الأساسية لضمان الأمن السيبراني وحماية الفضاء الرقمي الوطني، وقد عملت الجزائر على تطوير مجموعة من النصوص القانونية المنظمة لهذا المجال.

يندرج نص المادة 39 من دستور 1996 الجزائري ضمن باب الحقوق والحريات الأساسية، ويعد من أهم الضمانات الدستورية لحماية الحياة الخاصة للأفراد في الجزائر حيث تنص المادة 39 على أن " **لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة يكل اشكالها مضمونة**". [1]

وتنص المادة 63 من نفس الدستور على أن "**يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة، وحماية الاسرة والشبيبة والطفولة**". [2]

2. دستور 2016

[1] دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996، الجريدة الرسمية العدد 76، صادر في 8 ديسمبر 1996، ص12.

[2] المرجع نفسه، ص 14.

أكدت المادة 46 على نفس حقوق المادة 39 من دستور 1996، مع إضافة دستورية هامة تعتبر حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حقاً أساسياً يضمنه القانون[1] .

كما تنص المادة 44 من نفس الدستور على حرية الابتكار الفكري والفني والعلمي وحقوق المؤلف يحميها القانون. [2]

3. دستور 2020

في دستور 2020، الفصل الرابع المتعلق بالحقوق والحريات، تنص المادة 47 على حق كل فرد في حماية خصوصيته وكرامته، كما يضمن له التمتع بسرية مراسلاته واتصالاته الخاصة مهما كان شكلها، مقيدة أي مساس بها بقرار قضائي مسبب، مع ترتيب عقوبات قانونية على المنتهكين. [3]

وتشكل هذه النصوص الأساس القانوني لحماية الفضاء الرقمي من التهديدات المرتبطة باختراق الخصوصية، والتنصت غير المشروع، وتسريب البيانات الشخصية. وبالتالي، فإن هذه المواد مجتمعة تشكل الإطار الدستوري الذي يستند إليه الأمن السيبراني في الجزائر لحماية الخصوصية وضمان أمن المعلومات.

الفرع الثاني: الترسانة القانونية المنظمة للمجال السيبراني

اعتمد المشرع الجزائري مجموعة من القوانين المتخصصة لتنظيم النشاط الرقمي ومكافحة التهديدات :

---

[1] دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2016، الجريدة الرسمية العدد 14، صادر في 7 مارس 2016، ص. 11.

[2] المرجع نفسه، ص11

[3] دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020، الجريدة الرسمية العدد 82، صادر في 30 ديسمبر 2020، ص. 13.

1. مكافحة الجرائم المعلوماتية:

يعد قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (القانون رقم 09-04 لسنة 2009) من أبرز القوانين، حيث يحدد الجرائم المعلوماتية ويضع العقوبات المقررة لكل من يعتدي على الأنظمة الرقمية أو يسعى لاختراقها أو المساس بسلامة المعطيات. وقد أنشأ هيئة خاصة للوقاية من هذه الجرائم ومكافحتها وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بموجب المادة 13 منه. [1]

صدر هذا القانون في إطار مواجهة تزايد الجرائم الإلكترونية في الجزائر ومكافحتها، ويعد من أوائل النصوص التشريعية في الجزائر لمواجهة التهديدات الرقمية.

صدر المرسوم الرئاسي رقم 15 -261 مؤرخ في 8 أكتوبر 2015 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها ويحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها. [2]

2. التوقيع والتصديق الإلكتروني :

مع تطور المعاملات الإلكترونية وعولمة الاقتصاد الرقمي ظهرت تهديدات جديدة تتمحور حول الثقة والأمان في التعاملات داخل الفضاء السيبراني، حيث أصبح مجرمو المعلوماتية قادرون على إيجاد نقاط ضعف في الفضاء الرقمي تسمح لهم بتنفيذ اعمال إجرامية باستعمال برمجيات خبيثة خاصة ان التبادلات الالكترونية تكون خالية من أي حضور جسدي مما يصعب التعرف على هوية الأشخاص الذين يتعامل معهم[3]، هذا الأمر جعل المشرع الجزائري يصدر القانون 15-04 المؤرخ في 1 فيفري 2015 المحدد للقواعد العامة

---

[1] قانون رقم 09-04 مؤرخ في 5 اوت لسنة 2009، الجريدة الرسمية العدد 47، **مؤرخة في 16 اوت 2009**.ص ص. 5-8.

[2] مرسوم رئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015، الجريدة الرسمية العدد 53، ص16

[3] شلحة رشيد، " اليات مواجهة التهديدات السبرانية في الجزائر"(مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2019) ص 88.

المتعلقة بالتوقيع والتصديق الالكترونين، ويعد إطارا قانونيا ينظم استخدام التوقيع الإلكتروني وشهادات التصديق في المعاملات الرقمية، بهدف ضمان موثوقية الوثائق الإلكترونية وحجيتها القانونية. [1]

والتصديق الإلكتروني، هو عملية تهدف إلى ضمان قانونية وسلامة وأمان المعلومات المرسلة أو المخزنة إلكترونيا. تعتمد على استخدام المفاتيح المشفرة (المفتاح العام والمفتاح الخاص) لتأمين البيانات والصفقات عبر الإنترنت. يستخدم التصديق الإلكتروني بشكل شائع لضمان هوية الأطراف المشاركة في معاملة إلكترونية وضمان عدم تغيير البيانات أثناء النقل. [2]

بموجب أحكام القانون رقم 15-04- تعتمد هيكلة النظام الوطني للتصديق والتوقيع الإلكترونيين على ثلاث جهات مكملة وهي: [3]

- **السلطة الوطنية للتصديق الإلكتروني (ANCE)**، التابعة لمصالح الوزير الأول، تلعب دورا مركزيا في ترقية استعمال التوقيع والتصديق الإلكترونيين وتطويرهما وضمان موثوقية استعمالهما.
- **السلطة الحكومية للتصديق الإلكتروني (AGCE)**، الخاضعة لإشراف وزير البريد والمواصلات السلكية واللاسلكية مسؤولة عن متابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة الموثوقة وكذلك توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي.
- **السلطة الاقتصادية للتصديق الإلكتروني (AECE)**، التابعة لسلطة ضبط البريد والاتصالات الالكترونية (ARPCE)، مسؤولة عن متابعة ومراقبة مؤديي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكتروني لصالح الجمهور.

[1] القانون رقم 15-04 المؤرخ في 1 فيفري 2015، الجريدة الرسمية العدد 6، ص. 6.

[2] موقع وزارة البريد والمواصلات السلكية واللاسلكية، تاريخ تصفح الموقع 15 فيفري 2026 https://www.mpt.gov.dz/

[3] المرجع نفسه.

يعزز هذا القانون أمن المعاملات الإلكترونية، ويحد من مخاطر التزوير والاختراق، كما يدعم الثقة في الفضاء الرقمي من خلال آليات التشفير والتوثيق الإلكتروني.

3. الاتصالات والتجارة الالكترونية:

حدد القانون 18-04 مؤرخ في 10 ماي 2018 القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية ويعد إطارا قانونيا ينظم قطاع الاتصالات الإلكترونية في الجزائر ويهدف إلى ضبط تقديم خدمات الإنترنت والاتصالات وضمان استمراريتها وجودتها في إطار قانوني منظم مع حماية حقوق المستخدمين في الفضاء الرقمي. [1]

ينص القانون على تجريم انتهاك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الالكترونية أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها، وتجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة وسنت مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون. [2]

وينظم القانون البنية التحتية للاتصالات الإلكترونية، التي تعد المجال الأساسي لتبادل البيانات والمعلومات. كما يساهم في تعزيز أمن الشبكات والحد من المخاطر التقنية مثل الاختراقات والهجمات السيبرانية، من خلال فرض قواعد تنظيمية على متعاملي الاتصالات وضبط نشاطهم في هذا المجال. [3]

---

[1] القانون رقم 18-04 المؤرخ في 10 ماي سنة 2018، الجريدة الرسمية العدد 27، ص ص.3-5.

[2] مهدي رضا، الجرائم السيبرانية واليات مكافحتها في التشريع الجزائري، **مجلة ايليزا للبحوث والدراسات**، م.6، ع.2، (2021) ص. 121.

[3] قانون رقم 18-04، المرجع السابق، ص ص. 3-9

أما قانون 18-05 مؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالتجارة الالكترونية للسلع والخدمات، ويهدف إلى تأطير المعاملات التجارية التي تتم عبر الوسائط الرقمية وضمان حماية مختلف الأطراف. [1]

تنص المادة الثانية منه انه يطبق هذا القانون في حالة ما إذا كان أحد أطراف العقد الالكتروني متمتعا بالجنسية الجزائرية او مقيم شرعي في الجزائر، أو شخص معنوي خاضع للقانون الجزائري، او في حالة ما إذا كان محل العقد أو تنفيذه في الجزائر. كما حدد هذا القانون شروط ممارسة التجارة الإلكترونية، التزامات المستهلك الالكتروني، وواجبات المورد الالكتروني. [2]

ومن جهة أخرى، اعترف القانون بحجية العقود الإلكترونية ووسائل الإثبات الرقمية، وشجع على اعتماد وسائل الدفع الإلكتروني مع فرض تدابير أمنية لحماية المعاملات المالية. وفي نفس السياق، نص على حظر تسويق بعض المنتجات عبر الإنترنت، وفرض عقوبات على المخالفين لضمان احترام القواعد القانونية. [3]

4. حماية المعطيات الشخصية:

أصدر المشرع الجزائري القانون 18- 07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والذي يهدف في المقام الأول إلى تحديد قواعد قانونية تعنى بحماية حقوق الشخص الطبيعي في شرفه وسمعته وحياته الخاصة في مجال المعالجة الشخصية للمعطيات، [4]والذي أنشأ ما يسمى بـ

[1] قانون 18-05 مؤرخ في 10 ماي سنة 2018، الجريدة الرسمية العدد 28، ص. 4.

[2] المرجع نفسه، ص. 5.

[3] المرجع نفسه، ص ص. 5-9

[4] القانون 18- 07 المؤرخ في 10 جوان 2018، الجريدة الرسمية عدد 34، ص ص. 11-14

"السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي" التي تشكل آلية مهمة لحماية المعطيات ذات الطابع الشخصي في إطار احترام الحياة الخاصة للأشخاص. [1]

وقد عرف المشرع الجزائري" المعطيات ذات الطابع الشخصي "في القانون 18-07 انها: **كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه،" الشخص المعني "بصفة مباشرة وغير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.**

"الشخص المعني" : كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة. [2]

5. حماية المعطيات في المؤسسات والإدارات والهيئات العمومية:

يتضمن المرسوم الرئاسي رقم 26-07 مؤرخ في 7جانفي 2026 انشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية حماية المعطيات في المؤسسات والإدارات والهيئات العمومية، حيث تنص المادة الثانية من المرسوم على الزامية المؤسسات والادارات والهيئات العمومية بوضع هيكل يكلف بأمن الأنظمة المعلوماتية والذي يجب أن يكون مستقلا عن الهيكل المكلف بالأنظمة المعلوماتية. [3]

يتولى الهيكل مسؤولية امن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والإدارات والهيئات العمومية بكيفية دائمة وفي كل الظروف. ويكلف ب: [4]

---

[1] المرجع نفسه، المادة 22، ص 16.

[2] القانون 18- 07، المرجع السابق، المادة 3، ص 12.

[3] المرسوم الرئاسي رقم 26-07 مؤرخ في 7 جانفي 2026، الجريدة الرسمية العدد04، المادة 02، ص 21.

[4] المرجع نفسه، المادة 04.

- تصميم والإشراف على تنفيذ سياسة الأمن السيبراني للمؤسسة.
- تحديد المخاطر من خلال رسم خرائط مخصصة ووضع خطط معالجة.
- المراقبة المستمرة لأنظمة معلومات المؤسسة للكشف عن التهديدات والحوادث.
- التنسيق مع وكالة أمن الأنظمة المعلوماتية بشأن الحوادث الهامة والإبلاغ الفوري للسلطات المعنية.
- إجراء أو الإشراف على تقييمات أمنية لأنظمة المعلومات.
- ضمان الامتثال لمعايير الأمن السيبراني الوطنية وتشريعات حماية البيانات الشخصية. [1]

الفرع الثالث: الآليات الجنائية وتقنيات التحري الخاصة

1. قانون العقوبات (تعديل 04-15)

ينص القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل لقانون العقوبات الجزائري على تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات ضمن المواد من 394 مكرر إلى 394 مكرر7، حيث يهدف إلى حماية الأنظمة المعلوماتية والبيانات الرقمية من مختلف أشكال الاعتداء فقد جرم المشرع الدخول أو البقاء غير المشروع في نظام معلوماتي، كما عاقب على عرقلة سيره أو التشويش عليه، إضافة إلى إدخال أو حذف أو تعديل المعطيات بطريقة غير مشروعة. وامتد التجريم ليشمل التزوير المعلوماتي واستعمال المعطيات المزورة مع العلم بذلك، فضلا عن معاقبة كل من يساهم أو يشارك في ارتكاب هذه الجرائم. كما شدد العقوبات في حال استهداف أنظمة الدولة أو الهيئات العمومية أو إذا ترتبت عن الأفعال أضرار جسيمة مع النص على إمكانية مصادرة الوسائل والأدوات المستعملة في

[1] المرسوم الرئاسي رقم 26-07، المادة 04.

ارتكاب الجريمة. ويعكس هذا الإطار القانوني حرص المشرع الجزائري على مواكبة تطور الجريمة الإلكترونية وتعزيز الحماية القانونية للفضاء الرقمي. [1]

2. قانون الإجراءات الجزائية

القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 هو قانون عدل وأكمل بعض أحكام قانون الإجراءات الجزائية، خاصة في مجال مكافحة الجريمة المنظمة والجرائم الخطيرة. وقد سمح هذا القانون في إطار قانوني مضبوط وتحت رقابة قضائية، باللجوء إلى وسائل التحري الخاصة مثل اعتراض المراسلات الإلكترونية والهاتفية، وتسجيل الأصوات والتقاط الصور، وذلك في حالات محددة كالإرهاب والجريمة المنظمة وتبييض الأموال. ويهدف هذا النص القانوني إلى تعزيز فعالية أجهزة إنفاذ القانون في مواجهة الجرائم المعقدة مع ضمان احترام الحقوق والحريات الفردية من خلال اشتراط الحصول على إذن مسبق من الجهات القضائية المختصة. [2]

القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدّل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، نص في فصله الرابع المعنون بـ اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، من خلال المواد 65 مكرر 7 إلى 65 مكرر 10 على جواز لجوء السلطات القضائية، في إطار التحري والتحقيق في بعض الجرائم الخطيرة، إلى هذه الوسائل وفق شروط قانونية محددة. ويتم ذلك بإذن من وكيل الجمهورية أو قاضي التحقيق، مع إمكانية تكليف ضباط الشرطة القضائية أو أعوان مختصين بتنفيذ هذه العمليات باستخدام الوسائل التقنية المناسبة. كما تحرر محاضر مفصلة تتضمن جميع

[1] القانون رقم 04-15 المرخ في 10 نوفمبر 2004 يعدل ويتمم الامر 66-156المؤرخ في 8 جوان سنة 1966، الجريدة الرسمية العدد 71، ص ص. 11،12.

[2] القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 يعدل ويتمم الامر 66-156المؤرخ في 8 جوان سنة 1966، الجريدة الرسمية العدد 84، ص ص. 11-22.

الإجراءات المنجزة، وترفق بملف القضية مع الحفاظ على سريتها، وتتم هذه التدابير تحت رقابة القضاء وضمن أجال محددة. [1]

وانطلاقا من هذه الأحكام، يتضح أن المشرع الجزائري قد تبنى سياسة جنائية تقوم على توسيع وسائل البحث والتحري لمواجهة الجرائم الخطيرة، من خلال إقرار تقنيات حديثة تمس بالحياة الخاصة للأفراد. غير أن هذا التوسع لم يكن مطلقا، بل قيد بجملة من الضمانات القانونية، أبرزها الإذن القضائي المسبق، وتحديد نطاق ومدة هذه الإجراءات، إضافة إلى إخضاعها لرقابة القضاء وتوثيقها بمحاضر رسمية. وهو ما يعكس سعيا إلى تحقيق توازن بين فعالية العدالة الجزائية وحماية الحقوق والحريات الفردية.

المطلب الثاني: الهيئات المسؤولة عن الأمن السيبراني في الجزائر

الفرع الأول: وكالة أمن الأنظمة المعلوماتية ASSI

أصدر المشرع الجزائري في 20 جانفي سنة 2020 المرسوم الرئاسي رقم 05-20 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية هدفها وضع استراتيجية شاملة ومتكاملة للأمن المعلوماتي بواسطة أجهزة عليا في الدولة من خلال المادة الثالثة التي تضمنت تشكيلة المنظومة من مجلس وطني لأمن الأنظمة المعلوماتية والذي يدعى في صلب النص "المجلس"، ووكالة أمن الأنظمة المعلوماتية تدعى في صلب النص " وكالة".[2]

وتعتبر المنظومة خطوة هامة نحو بناء هيكل تنظيمي يعنى بالتهديدات والجرائم المعلوماتية.

[1] القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدّل والمتمم للأمر رقم 66-155، الجريدة الرسمية العدد 84، ص ص.8،9.

[2] المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي2020، الجريدة الرسمية العدد 04، المواد 1، 2، 3، ص. 6.

1. المجلس الوطني لأمن الأنظمة المعلوماتية:

- **تشكيلة المجلس وطني لأمن الأنظمة المعلوماتية:**

يعد المجلس وطني لأمن الأنظمة المعلوماتية أحد مكونات المنظومة الوطنية يترأسه وزير الدفاع الوطني أو ممثله ويتكون من ممثل عن: رئاسة الجمهورية، الوزير الأول، وتشكيلة وزارية متنوعة تضم الشؤون الخارجية، الشؤون الداخلية، العدل، الطاقة، المالية، الاتصالات، التعليم العالي، ويستعين المجلس بأي مؤسسة أو شخص من شأنه أن يساعده في أعماله[1] . ويتوفر المجلس على أمانة تقنية يسيرها أمين عام توضع تحت تصرف سلطة رئيس المجلس تقوم بعدة مهام من بينها: العمل على إعداد مشروع النظام الداخلي للمجلس والتنسيق مع الوكالة، كما تقوم بجمع الوثائق والمعلومات لتحضير أشغال المجلس الوطني من أي ادارة أو مؤسسة أو هيئة.[2]

- **مهام المجلس وطني لأمن الأنظمة المعلوماتية:**

يتولى المجلس الوطني عدة مهام تضمنها المرسوم التنفيذي رقم 05-20 في المادة 04 كالبت في الاستراتيجية التي تم اقتراحها من قبل الوكالة، كما يدرس المجلس مخطط عمل الوكالة ويقرر في نشاطاتها ويوافق عليها. كما يتولى الموافقة على اتفاقيات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال الانظمة المعلوماتية.[3]

كذلك من مهام المجلس الموافقة على تصنيف الأنظمة المعلوماتية، والتي تتعدد فعلى سبيل المثال نجد نظم المعلومات الإدارية وتتعلق بالأنظمة المسؤولة عن تقديم المعلومات الضرورية للإدارة حتى تتمكن من تحديد المشكل وحله، كما أن هناك أنظمة دعم القرار وهي التي تسمح باتخاذ القرار المناسب لحل الاشكال المطروح وخلق فرص للتطوير والابتكار من

[1] المرجع نفسه، المادة 5، ص. 6.

[2] المرسوم الرئاسي رقم 20-05، المرجع السابق، المواد 7، 8، 9، ص.6.

[3] المرجع نفسه، المادة 4، ص. 6.

أجل الحصول على أفضل النتائج[1] .كما يقترح المجلس مدى ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، ويبدي رأيه في أي مشروع نص تشريعي أو تنظيمي له علاقة بأمن الأنظمة المعلوماتية.[2]

2. وكالة أمن الأنظمة المعلوماتية:

أنشأت هذه الوكالة بموجب المرسوم الرئاسي رقم 20-05، اذ نصت المادة 17 على أنها مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية مقرها بالجزائر.[3]

- **مهام وكالة أمن الأنظمة المعلوماتية:**

حسب المادة 18 من المرسوم الرئاسي رقم 05-20 وكل للوكالة مهام تتعلق بتحضير، تنسيق وتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، كما أنها تقترح طريقة اعتماد مزودي التدقيق ضمن نفس المجال إضافة إلى إجراء التحقيقات الرقمية عند وقوع الهجمات أو الحوادث السيبرانية وجمع وتحليل الأدلة المرتبطة بها. كما تسهر على جمع وتبادل المعلومات المتعلقة بالحوادث مع مختلف المؤسسات، وتقديم الدعم والمساعدة للإدارات والهيئات العمومية والخاصة في مجال تدبير المخاطر وتعزيز الأمن المعلوماتي، مع ضمان اليقظة التكنولوجية المستمرة. وتشمل مهامها أيضا مراقبة ومواكبة الأنظمة الحساسة، وإعداد الدراسات والتقارير، وتحيين خريطة الأنظمة المعلوماتية المصنفة، واقتراح المعايير والإجراءات الملائمة وفق أفضل الممارسات الدولية، فضلًا عن اعتماد الحلول والمنتجات

[1] صونيا مقري، وليد بن لعامر، المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم 20-05، مجلة البحوث في العقود وقانون الاعمال، (الجزائر: م.10، ع.2، 2025)، ص. 138.

[2] المرسوم الرئاسي رقم 20-05، المرجع السابق، المادة 4، ص. 6.

[3] المرجع نفسه، المادة 17، ص. 7.

الأمنية ومقدمي خدمات الثقة الرقمية، وأخيرًا تنظيم أنشطة التكوين والتحسيس لنشر ثقافة الأمن المعلوماتي.[1]

- **تنظيم وكالة أمن الأنظمة المعلوماتية:**

تتولى لجنة توجيه إدارة وكالة أمن الأنظمة المعلوماتية، كما يسريها مدير عام ويعمل تحت سلطته مديريات ومصالح تقنية وإدارية بالإضافة إلى مركز وطني عملياتي لأمن الأنظمة المعلوماتية. [2]

1. لجنة التوجيه:

يعين رئيس لجنة التوجيه في وزارة الدفاع الوطني طبقا للتنظيم المعمول به[3].

وتتكون لجنة التوجيه من ممثلين من مختلف الوزارات: وزارة الدفاع، الوزارة المكلفة بالشؤون الخارجية، الوزارة المكلفة بالداخلية، الوزارة الكلفة بالعدل والمالية والطاقة، الوزارة المكلفة بالتعليم العالي، الوزارة المكلفة بالصناعة والتجارة، الوزارة المكلفة بالاتصالات، بالإضافة إلى عدة سلطات كسلطة ضبط البريد والاتصالات الإلكترونية، السلطة الوطنية للتصديق الإلكتروني، السلطة الحكومية للتصديق الإلكتروني، الهيئة الوطنية لحماية المعطيات ذات الطابع الشخصي، مصالح الأمن. والمدير العام على سبيل الاستشارة.[4]

2.**المدير العام للوكالة:**

يعين طبقا للتنظيم المعمول به في وزارة الدفاع الوطني.

يتولى التسيير اليومي والعملياتي للوكالة، يمثلها أمام القضاء وفي جميع أعمال الحياة المدنية، يسهر على تنفيذ قرارات "مجلس التوجيه"، ويُشرف على إدارة الموارد البشرية وتنسيق عمل المديريات الداخلية. [5]

---

[1] المرسوم الرئاسي رقم 20-05، المرجع السابق، المادة 18، ص.7.

[2] المرجع نفسه، المادة 20، ص. 8.

[3] المرجع نفسه، المادة 21، ص. 8.

[4] المرجع نفسه، المادة 22، ص. 8.

[5] المرجع نفسه، المادة 28، ص. 9.

3.اللجنة العلمية للوكالة:

تعد اللجنة العلمية هيئة استشارية تتكون من عشرة (10) أعضاء تعينهم لجنة التوجيه لمدة ثلاث (3) سنوات قابلة للتجديد. وتتمثل مهمتها في إبداء الرأي والمشورة للمدير العام للوكالة في كافة المسائل ذات الطابع العلمي المرتبطة بنشاطات البحث والتطوير، حيث تتولى تقييم تجانس البرامج والمشاريع المقترحة وكيفيات تنفيذها، وتوجيه نشاطات التكوين العلمي والإتقان لفائدة مستخدمي الوكالة والهيئات العمومية، فضلًا عن تقديم توصياتها بشأن تنظيم التظاهرات العلمية واقتناء المراجع ذات الصلة. [1]

الفرع الثاني: الهيئات التابعة لوزارة الدفاع الوطني

1.المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

تم انشاءه بموجب المرسوم رئاسي رقم 04-183، وهو مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يوضع تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، وضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة.[2]

ودخل حيز الخدمة ابتداء من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة.[3]

---

[1] المرسوم الرئاسي رقم 20-05، المرجع السابق، المادة 31، ص. 9.

[2] المرسوم رئاسي رقم 04-183، المؤرخ في 8جوان 2004، الجريدة الرسمية العدد 41، ص. 18

[3] ادريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، **مجلة مصداقية**، م1.، ع.1، (2019)، ص. 113.

يحتوي المعهد على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات، مصلحة البيئة، أما فيما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي، على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية.[1]

يعتبر المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني مكسبا يدعم قدرات الدرك الوطني في مكافحة الجريمة بجميع أشكالها وذلك بإدراج العلوم في العدالة الجزائية، كما أن التحكم في التقنيات الحديثة من شأنه أن يدعم قدرات المؤسسة لمكافحة الإجرام المتطور باستمرار والذي يعتمد على التكنولوجيات الجديدة.[2]

- **مهام المعهد الوطني للأدلة الجنائية وعلم الاجرام:**

- الإسهام في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- إنجاز الخبرات والتحاليل بناء على طلبات القضاة، المحققين والسلطات المؤهلة.
- تصميم بنوك معطيات وإنجازها وفقا للقانون.
- الدعم التقني للوحدات أثناء التحقيقات المعقدة.
- العمل على ترقية البحث التطبيقي وأساليب التحريات التي ثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.
- المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيات الدقيقة.
- المشاركة في الدراسات والبحوث المتعلقة بالوقاية والتقليل من كل أشكال الإجرام.
- المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية. [3]

2. مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية للدرك الوطني:

[1] المرجع نفسه، ص. 113.

[2] الموقع الرسمي لوزارة الدفاع الوطني الجزائري، تاريخ الاطلاع 1 أفريل 2026.
https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

[3] المرجع نفسه.

نشأ هذا المركز في سنة 2008 وهو جهاز مختص في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية، ويهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي. يتواجد المركز ببئر مراد رايس، ويعكف 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 وللبنوك. [1]

كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها، واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها والملتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها. [2]

- **مهام مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية للدرك الوطني:**
  - ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.
  - القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.
  - مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة.
  - المشاركة في عمليات التحري عبر شبكة الإنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.
  - المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.[3]

الفرع الثالث: المصلحة المركزية لمكافحة الجرائم السيبرانية:

[1] ادريس عطية، المرجع السابق، ص ص. 112،113.

[2] سمير بارة، المرجع السابق، ص ص. 435،436.

[3] سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، **مجلة القانون الجزائري العام والمقارن**، م.7، ع.1، (جوان 2021)، ص. 281.

وهي مصلحة تابعة لمديرية الأمن الوطني، والتي أنشأت سنة 2011 وتعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة – أنتربول، أفريكوم– أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الاجرام. [1]

الفرع الرابع: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

أنشأت بمقتضى القانون رقم 09–04 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، حيث تنص المادة 13 من هذا القانون على انه " تنشأ هيئة وطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم". [2]

وأحال بخصوص تشكيلتها، تنظيمها وكيفيات سيرها الى التنظيم. وقد صدر تباعا المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر 2015 في الجزائر، وهو النص الذي يحدد تنظيم وسير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وقد نصت المادة02 من المرسوم على ان" الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل". [3]

وصدر المرسوم الرئاسي رقم 21– 439 المؤرخ في 07 نوفمبر 2021 والذي يتضمن إعادة تنظيم هذه الهيئة تحت سلطة رئيس الجمهورية، حيث تنص المادة 02 من هذا المرسوم على أن " الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى رئيس الجمهورية". [4]

---

[1] جمال بوزادية، المرجع السابق، ص. 1280.

[2] القانون رقم 09-04، المرجع السابق، المادة 13، ص. 8.

[3] المرسوم الرئاسي رقم 15-261، المرجع السابق، المادة 02، ص. 16.

[4] المرسوم الرئاسي رقم 21– 439 المؤرخ في 07 نوفمبر 2021، الجريدة الرسمية عدد 86، المادة 02، ص.5.

تكلف الهيئة باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إضافة إلى تنشيط وتنسيق الجهود الوطنية في هذا المجال. كما تضطلع بدور مهم في مساعدة السلطات القضائية ومصالح الشرطة القضائية في مكافحة هذه الجرائم، وذلك من خلال جمع المعلومات وتزويد الجهات المختصة بها، وتقديم الخبرات القضائية والتقنية. بما في ذلك تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.[1]

وتتكفل أيضًا بضمان المراقبة الوقائية للاتصالات الإلكترونية، بهدف الكشف عن الجرائم المرتبطة بالأعمال الإرهابية والتخريبية وكل ما من شأنه المساس بأمن الدولة.[2]

الفرع الخامس: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

أصدر المشرع الجزائري القانون 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي والذي أنشأ بموجبه السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي حيث تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، مقرها بالجزائر العاصمة بموجب المادة 22 من القانون 18-07.[3]

- **تشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:**

تتكون السلطة الوطنية من ستة عشرة (16) عضوا يعينون حسب اختصاصهم القانوني و/أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي بموجب مرسوم رئاسي لمدة خمسة (5) سنوات قابلة للتجديد، وذلك كما يلي:[4]

- ممثل عن وزير الشؤون الخارجية

[1] القانون رقم 09-04، المرجع السابق، المادة 14، ص.8.

[2] المرسوم الرئاسي رقم 21- 439، المرجع السابق، المادة 4، ص. 5.

[3] القانون رقم 18- 07، المرجع السابق، المادة22، ص 16.

[4] المرجع نفسه، المادة 23، ص 16

- ممثل عن الوزير المكلف بالبريد والمواصلات السلكية ولاسلكية والتكنولوجيات والرقمنة.
- ممثل عن الوزير المكلف بالداخلية.
- ممثل عن الوزير المكلف بالصحة.
- ممثل عن وزير الدفاع الوطني.
- ممثل عن وزير العدل حافظ الأختام.
- ممثل عن وزير العمل والتشغيل والضمان الاجتماعي.
- ثلاث شخصيات، من بينهم الرئيس، يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية .
- ثلاثة قضاة يقترحون من قبل المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة.
- عضو من كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية.
- ممثل عن المجلس الوطني لحقوق الإنسان.

ويمكن للسلطة الوطنية أن تستعين بأي شخص مؤهل لمساعدتها في أشغالها، بالإضافة إلى تزويدها بأمانة تنفيذية، يسيرها أمين تنفيذي يساعده في تأدية مهامه مستخدمون.[1]

- **مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:**

تعنى السلطة بعدة مهام تسند إليها في إطار حماية حق الشخص الطبيعي في حرمة حياته الخاصة، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاهه مما جعلها آلية لصون وحماية هذا الحق في إطار القانون، وتتمثل مهامها في: [2]

[1] القانون 07-18، المرجع السابق، المادة 27، ص. 18.

[2] المرجع نفسه، المادة 25، ص. 17.

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي،
- اعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم
- تتولى السلطة الوطنية تقديم الاستشارات للأشخاص والكيانات التي تلجا لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة، بالإضافة إلى تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون،
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي المعالجة
- الأمر بإغلاق معطيات أو سحبها أو إتلافها .
- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي
- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل .
- اصدار عقوبات إدارية، حيث تتخذ في حق المسؤول عن المعالجة الذي يخرق أحكام هذا القانون الإجراءات الإدارية الآتية حسب المادة46 من هذا القانون: الإنذار، الأعذار، السحب المؤقت لمدة لا تتجاوز سنة، أو السحب النهائي لوصل التصريح أو الترخيص، فرض الغرامة المالية، وتكون قرارات السلطة الوطنية قابلة للطعن أمام مجلس الدولة.[1]
- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.
- وضع قواعد السلوك والاخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي. [2]

[1] القانون رقم 07-18، المرجع السابق، المادة 46، ص.21.

[2] المرجع نفسه، المادة 25، ص. 17.

اسندت إليها عديد المهام تصب في إطار حماية حق الشخص الطبيعي في حرمة حياته الخاصة، مما جعلها آلية لصون وحماية هذا الحق في إطار القانون.

الفرع السادس: المحافظة السامية للرقمنة

أنشئت المحافظة السامية للرقمنة تحت وصاية رئاسة الجمهورية بموجب المرسوم الرئاسي رقم 23-314 المؤرخ في 6 سبتمبر 2023 [1]، المعدل بالمرسوم الرئاسي رقم 24-63 المؤرخ في 01 فيفري 2024، الذي حدد هيكلتها الداخلية وآليات عملها التنظيمية، بما يشمل توزيع الاختصاصات على هياكلها التنفيذية وتحديد مهام لجنتها العلمية والتقنية [2]. ما منحها مكانة محورية تؤهلها لقيادة التحول الرقمي الوطني بصفة شاملة وأفقية لتوحيد الجهود نحو تجسيد الإرادة السياسية للدولة في جعل الرقمنة رافعة استراتيجية للتنمية الاقتصادية والاجتماعية وأداة أساسية لتحديث الإدارة العمومية وعصرنتها وبناء اقتصاد رقمي مستدام.[3]

حسب المادة 4 من المرسوم الرئاسي رقم 23-314 أسندت إلى المحافظة السامية للرقمنة المهام الأساسية التالية : [4]

- تصميم وإعداد الاستراتيجية الوطنية للتحول الرقمي، بالتشاور مع القطاعات المعنية والمؤسسات والقطاع الاقتصادي والمجتمع المدني وكل الأطراف الفاعلة .
- متابعة تنفيذ الاستراتيجية الوطنية للتحول الرقمي.
- السهر على توافق المخططات القطاعية في مجال الرقمنة مع الاستراتيجية الوطنية للتحول الرقمي.
- تقييم إنجازات كل القطاعات واقتراح التصحيحات اللازمة وفق مؤشرات الأداء ذات الصلة بالرقمنة.

---

[1] المرسوم الرئاسي رقم 23-314 المؤرخ في 6 سبتمبر 2023، الجريدة الرسمية العدد 59، ص. 9.

[2] المرسوم الرئاسي رقم 24-63 المؤرخ في 01 فيفري 2024 الجريدة الرسمية العدد 8 ، ص. 4.

[3] الموقع الرسمي للمحافظة السامية للرقمنة، تاريخ الاطلاع 17 أفريل 2026. https://www.hcn.dz/pres-HCN/Haut-Commissariat-%C3%A0-la-Num%C3%A9risation

[4] المرجع نفسه.

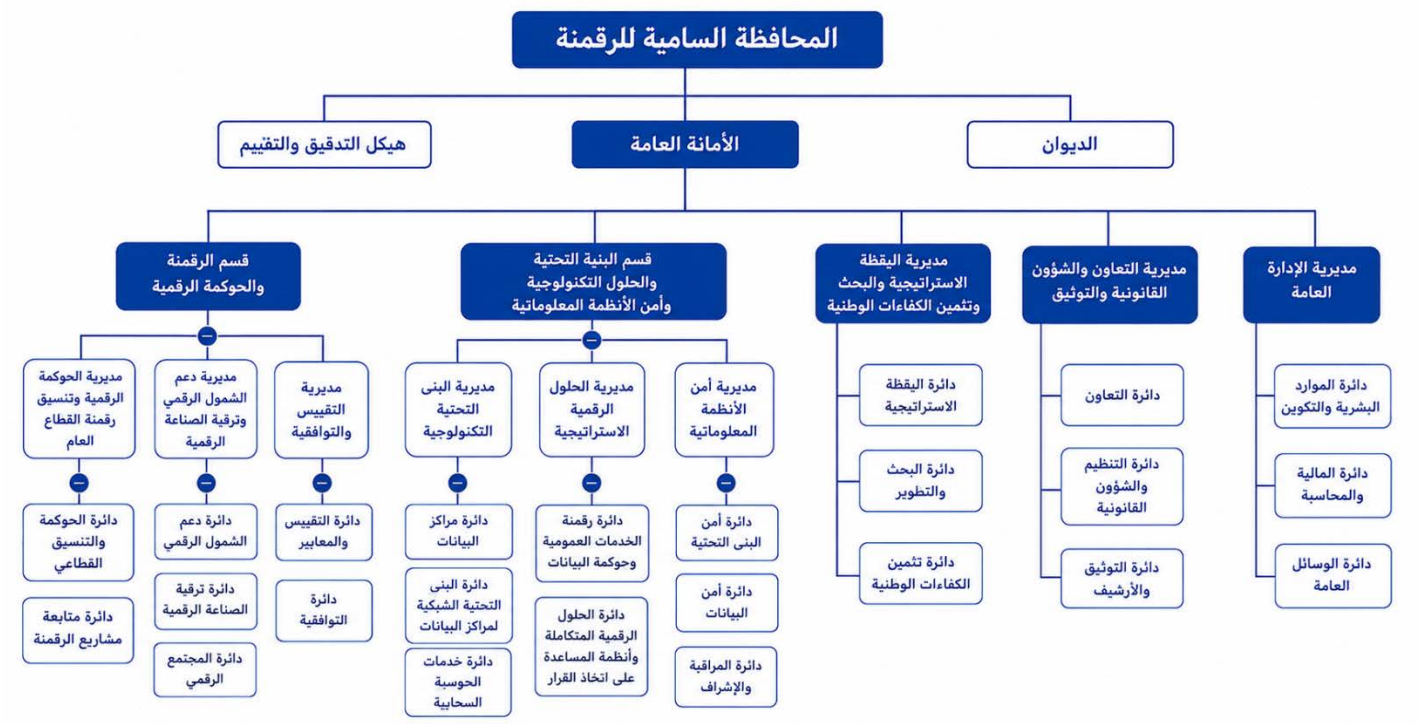
- ضمان توافق الاستراتيجية الوطنية للتحول الرقمي مع متطلبات أمن الأنظمة المعلوماتية، بالتنسيق مع الجهات المختصة .
- تحديد المشاريع ذات الأولوية والاستثمارات الاستراتيجية وكيفيات تعبئة الموارد البشرية وأدوات التمويل الخاصة بها .
- اقتراح الأدوات القانونية والتنظيمية و/أو الحلول التقنية الكفيلة بضمان الفعالية والتحسين المستمر لمحاور التحول الرقمي .
- اقتراح كل تدبير من شأنه تعزيز السيادة الرقمية وتطوير المنتوج الوطني، وتنمية الموارد البشرية والكفاءات الوطنية المطلوبة في مجال الرقمنة.
- إنجاز وتشجيع الدراسات الاستشرافية حول تطوير الرقمنة وضمان اليقظة التكنولوجية، مع اقتراح إنجاز مشاريع بحث في مجال اختصاصها.
- التعاون مع المؤسسات والمنظمات الدولية المماثلة في مجال الرقمنة، طبقا للتشريع والتنظيم المعمول بهما. [1]

وبفضل هذه الصلاحيات، تضطلع المحافظة السامية للرقمنة بدور محوري في الانتقال من إدارة تقليدية إلى إدارة ذكية، قائمة على البيانات الدقيقة، بما يسهم في تحسين جودة الخدمة العمومية، وترقية الأداء المؤسساتي، وترسيخ الشفافية في التسيير والحفاظ على المال العام، بما يخدم المصالح العليا للدولة والمواطن على حد سواء.[2]

- **الهيكل التنظيمي للمحافظة السامية للرقمنة:**

[1] المرسوم الرئاسي رقم 23-314، المرجع السابق، ص ص.9،10.

[2] الموقع الرسمي للمحافظة السامية للرقمنة. المرجع السابق. https://www.hcn.dz/pres-HCN/Haut-Commissariat-%C3%A0-la-Num%C3%A9risation



الشكل رقم (1): الهيكل التنظيمي للمحافظة السامية للرقمنة:

المصدر: الموقع الرسمي للمحافظة السامية للرقمنة، تاريخ تصفح الموقع 17 أفريل 2026.

https://www.hcn.dz/pres-HCN/Haut-Commissariat-%C3%A0-la-Num%C3%A9risation

الفرع السابع: المرجع الوطني لأمن نظم المعلومات (RNSI)

يعد المرجع الوطني لأمن المعلومات (RNSI 2020) إطارا شاملا يهدف إلى تقديم مجموعة من المتطلبات الأساسية لتطوير وتنفيذ سياسة أمن أنظمة المعلومات داخل المؤسسات العمومية في الجزائر. ويوفر هذا المرجع نهجا لتأمين المعلومات يعتمد على إدارة المخاطر فيما يتعلق بضمان السرية، السلامة، والتوافر.[1]

ينطبق هذا المرجع على الإدارات، القطاعات العمومية، والبنى التحتية التي تعالج معلومات حساسة، حيث يتضمن 20 مجالا أساسيا في الأمن المعلوماتي، من بينها إدارة الأصول،

[1] Référentiel National de Sécurité de l'Information, Ministère de la Poste des Télécommunications (MPTI), L06-Version Finale du RNSI 2020, P.13. https://www.mpt.gov.dz/wp-content/uploads/2023/12/Referentiel-National-de-la-Securite-de-lInformation-2020-VERSION-FINALE-1-1.pdf

حماية البيانات ذات الطابع الشخصي، التحكم في الوصول، أمن الشبكات، أمن الحوسبة السحابية والتشفير [1] . كما يحدد إطارا واضحا للحوكمة من خلال إلزام كل مؤسسة بتعيين مسؤول عن أمن أنظمة المعلومات (RSSI) يتولى تحليل المخاطر وإعداد التقارير الدورية، إلى جانب إنشاء لجنة توجيه (CD) لضمان توافق أهداف أمن المعلومات مع أهداف المؤسسة، ولجنة أمن المعلومات (CSI) لمتابعة تنفيذ الاستراتيجية الأمنية.[2]

وقد تم إعداد هذا المرجع بالاستناد إلى معايير دولية مثل ISO 27001 و ISO 27002، إضافة إلى القوانين الجزائرية ذات الصلة، على غرار القانون رقم 18-07 المتعلق بحماية المعطيات الشخصية والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال. [3]

ويركز أيضا على ضرورة إدارة الأصول المعلوماتية من خلال جرد دقيق وتصنيفها حسب حساسيتها، فضلا عن وضع ضوابط لأمن الأجهزة المحمولة والعمل عن بعد، بما في ذلك سياسات استخدام الأجهزة الشخصية (BYOD) وآليات حماية البيانات في حال الفقدان أو السرقة.[4]

ويخضع المرجع لعملية متابعة وتحسين مستمرين لمواكبة التطورات التشريعية والتهديدات السيبرانية، مع توفير أدوات تقييم لقياس مدى التزام المؤسسات بتطبيق متطلباته، كما تتضمن ملاحقه نموذج "ميثاق المعلوماتية" الذي يحدد حقوق وواجبات المستخدمين، مثل منع استخدام البريد الإلكتروني الشخصي لأغراض مهنية وضرورة الإبلاغ الفوري عن أي حادث أمني. [5]

[1] Référentiel National de Sécurité de l'Information, Ministère de la Poste des Télécommunications (MPTI),op.cit, P.25

[2] Ibid, P. P 14- 19.

[3] Ibid, P.P 11, 12

[4] Ibid, P14 .

[5] Ibid, P79.

المبحث الثالث: تأثير التهديدات السيبرانية على الأمن الوطني الجزائري

المطلب الأول: أشكال التهديدات السيبرانية التي تواجه الجزائر

الفرع الأول: احصائيات شركة كاسبرسكي

نبذة عن شركة كاسبرسكي: تأسست شركة Kaspersky عام 1997 بناء على مجموعة من وحدات مكافحة الفيروسات التي وضعها "يوجين كاسبيرسكي(Eugene Kaspersky) "، وهو خبير في الأمن السيبراني والرئيس التنفيذي للشركة منذ 2007.
وهي الان أكبر شركة خاصة في العالم تقدم حلول الأمن السيبراني، وتلتزم بمحاربة الجريمة الإلكترونية وفي الوقت نفسه تحافظ على أعلى معايير النزاهة الاحترافية والشفافية.[1]

تشير المعطيات الحديثة إلى تزايد حدة التهديدات الأمنية السيبرانية على المستويين العالمي والوطني، حيث أفادت تقارير شركة Kaspersky أنه خلال سنة 2025 تم رصد ما معدله 500 ألف برمجية خبيثة يوميا، وهو ما يمثل ارتفاعا بنسبة 7% مقارنة بسنة 2024. ويعود هذا التصاعد إلى تنامي عدة أنواع من التهديدات، من بينها برامج سرقة كلمات المرور التي ارتفعت بنسبة 59%، وبرامج التجسس بنسبة 51%، إضافة إلى أبواب الخلفية بنسبة 6%، وذلك وفقا للتقرير السنوي "Security Bulletin" الذي يرصد أبرز تطورات الأمن السيبراني عالميا.[2]

[1] Site officiel de Kaspersky, Consulté le 27 Avril 2026. https://www.kaspersky.fr/about

[2] Site officiel de Kaspersky, Consulté le 27 Avril 2026. https://www.kaspersky.fr/about/press-releases/le-chiffre-de-lannee-kaspersky-a-detecte-quotidiennement-un-demi-million-de-malwares-en-2025

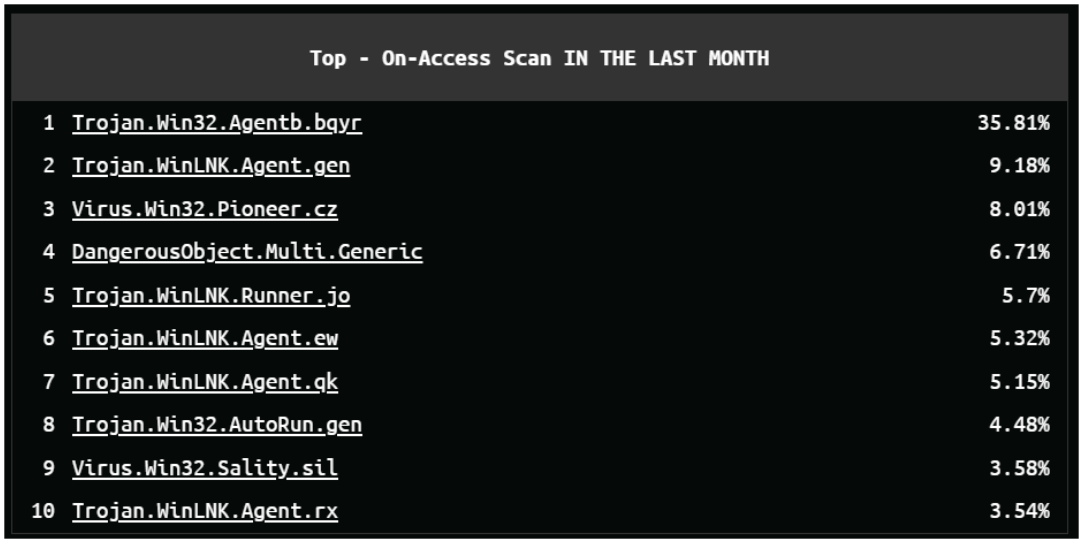
WORLD		
1	Turkmenistan	22.84%
2	Afghanistan	12.64%
3	Burundi	12.29%
4	Central African Republic	11.48%
5	Mongolia	11.34%
6	Mali	10.4%
7	Chad	10.35%
8	Cameroon	10.28%
9	Uzbekistan	10.09%
10	Algeria	9.95%
11	Kazakhstan	9.79%
12	Congo Republic	9.75%
13	Congo Democratic Republic	9.72%
14	Benin	9.5%

الشكل رقم (2): ترتيب الدول حسب نسبة التعرض للهجمات السيبرانية عالميًا خلال الفترة الممتدة من 27مارس الى 27 افريل 2026

المصدر: موقع شركة كاسبرسكي **CYBERTHREAT** LIVE MAP

https://cybermap.kaspersky.com/

يظهر الشكل رقم 1 الخاص بتوزيع نسب التعرض للهجمات السيبرانية عالميا خلال الفترة الممتدة من 27 مارس الى 27 أفريل2026، أن الجزائر احتلت المرتبة العاشرة عالميا بنسبة تقارب 9.95%، وهو ما يعكس مستوى معتبرا من التهديدات السيبرانية التي تستهدف الفضاء الرقمي الوطني. وتؤكد هذه المعطيات أن الجزائر تعد من بين الدول الأكثر عرضة للهجمات السيبرانية خلال هذه الفترة، مما يستدعي تعزيز آليات الحماية والتصدي لهذه التهديدات.



Top - On-Access Scan IN THE LAST MONTH		
1	Trojan.Win32.Agentb.bqyr	35.81%
2	Trojan.WinLNK.Agent.gen	9.18%
3	Virus.Win32.Pioneer.cz	8.01%
4	DangerousObject.Multi.Generic	6.71%
5	Trojan.WinLNK.Runner.jo	5.7%
6	Trojan.WinLNK.Agent.ew	5.32%
7	Trojan.WinLNK.Agent.qk	5.15%
8	Trojan.Win32.AutoRun.gen	4.48%
9	Virus.Win32.Sality.sil	3.58%
10	Trojan.WinLNK.Agent.rx	3.54%

الشكل رقم (3): أبرز أنواع البرمجيات الخبيثة المكتشفة في الجزائر خلال الفترة الممتدة من 27 مارس الى 27 أفريل 2026.

المصدر: موقع شركة كاسبرسكي **CYBERTHREAT** LIVE MAP

https://cybermap.kaspersky.com/

وتُظهر بيانات شركة Kaspersky المتعلقة بالجزائر انتشارا ملحوظا لعدة أنواع من البرمجيات الخبيثة، حيث تتصدر أحصنة طروادة [1] (Trojan Horses) قائمة التهديدات، إلى جانب أنواع أخرى من الفيروسات والبرمجيات الضارة، وهو ما يعكس تنوع وتعقيد الهجمات السيبرانية التي تستهدف الأنظمة والمستخدمين داخل البيئة الرقمية الجزائرية.[2]

وعلى الصعيد الوطني، تكشف نفس المصادر (كاسبرسكي) أن الجزائر تعرضت لحوالي 70 مليون هجوم سيبراني خلال الفترة الممتدة من جانفي إلى أكتوبر 2024، مما وضعها في المرتبة التاسعة عشرة عالميا من حيث الدول الأكثر تعرضا للهجمات السيبرانية. كما تبرز هذه المؤشرات تصاعد استهداف المؤسسات الاقتصادية، حيث تمثل نسبة 15.5% من

[1] **أحصنة طروادة(Trojan Horses)** : هو برنامج خبيث يتخفى في هيئة ملف أو تطبيق شرعي لخداع المستخدمين. بمجرد تحميله، يمنح المخترقين وصولاً للتحكم عن بُعد، أو يسرق البيانات، أو يُنزل برمجيات ضارة أخرى دون علم المستخدم.

[2] بيانات موقع شركةKaspersky ، تاريخ الاطلاع 27 أفريل 2026، https://cybermap.kaspersky.com/

الهجمات المسجلة في منطقة شمال وغرب ووسط إفريقيا هجمات تستهدف الشركات الصغيرة والمتوسطة، التي أصبحت هدفا رئيسيا للمجرمين الإلكترونيين[1].

الفرع الثاني: احصائيات الجرائم السيبرانية في الجزائر من سنة 2020 الى سنة 2025

1.احصائيات الجرائم السيبرانية خلال سنتين 2020-2021

السنة	2020	2021
عدد الجرائم المسجلة	5200	2838

الجدول رقم (1): احصائيات القضايا المتصلة بتكنولوجيات الاعلام والاتصال المسجلة على المستوى الوطني خلال سنة 2020 وسنة 2021.

المصدر: الإذاعة الجزائرية (تصريح كل من الملازم الأول مطمط أمين وفريد درامشية الرائد المختص في الاجرام السيبراني بقيادة الدرك الوطني)
https://news.radioalgerie.dz/ar/node/21741

وهذه الجرائم الإلكترونية تشمل محاذير الابتزاز والتهديد والتشهير والمساس بالحريات الشخصية والحياة الخاصة عبر شبكات التواصل الاجتماعي، فضلا عن جرائم نشر المعلومات الزائفة والمضللة، القرصنة والتشهير والتحرش الإلكتروني والنصب والاحتيال. [2]

[1] موقع شركةKaspersky ، المرجع السابق.

[2] الإذاعة الجزائرية، تصريح قدمه وفريد درامشية الرائد المختص في الاجرام السيبراني بقيادة الدرك الوطني، تاريخ الاطلاع 29 أفريل 2026. https://news.radioalgerie.dz/ar/node/21741

2. احصائيات الجرائم السيبرانية خلال السنتين 2022-2023

الجرائم	عدد القضايا المسجلة		عدد الأشخاص المتورطين	
	2023	2022	2023	2022
المساس بالأشخاص عبر شبكة الأنترنت	1999	2046	1796	1905
المساس بأنظمة المعالجة الآلية للمعطيات	323	331	217	202
النصب والإحتيال عبر شبكة الأنترنت	1130	801	1958	1318
المساس بالأطفال عبر شبكة الأنترنت	113	56	124	78
نشر محتويات مخالفة للنظام عبر شبكة الأنترنت	1066	1083	1332	1427
بيع السلع المحظورة عبر شبكة الأنترنت	110	115	181	159
جرائم أخرى	395	286	538	496
المجموع	**5136**	**4718**	**6146**	**5567**

الجدول رقم (2): إحصائيات الجرائم السيبرانية في الجزائر خلال سنة 2022 وسنة 2023.

المصدر: الحصيلة السنوية لنشاطات المصالح العملياتية للأمن الوطني لسنة 2023
https://www.algeriepolice.dz/IMG/pdf/dpj.pdf

يكشف ارتفاع العدد الإجمالي للقضايا من 4718 سنة 2022 إلى 5136 سنة 2023، وارتفاع عدد المتورطين من 5567 إلى 6146، عن منحى تصاعدي للجرائم السيبرانية في الجزائر، مما يعكس تنوع وتطور أشكال التهديدات الأمنية في البيئة الرقمية.

4. احصائيات الجرائم السيبرانية خلال السنتين 2024-2025

الجرائم	عدد القضايا المسجلة		عدد القضايا المعالجة	
	2024	2025	2024	2025
المساس وإلحاق الضرر بالأنظمة الالية لمعالجة المعطيات	89	72	34	27
جرائم المساس بالأشخاص عبر شبكة الأنترنت	420	616	197	239
الشذوذ في الأنترنت	04	04	04	04
استعمال الأنترنت لأغراض لها علاقة بأفعال إرهابية	07	04	07	04
النصب عبر شبكة الأنترنت	239	441	68	144
التحريض على الكراهية بين المواطنين والسكان	14	37	13	12
نشر محتويات مخالفة للنظام العام عبر شبكة الانترنت	18	61	15	47
بيع سلع محضورة عبر الانترنت	10	06	06	06
جرائم اخرى	176	460	76	192
المجموع	**977**	**1701**	**411**	**674**

الجدول رقم (3): إحصائيات الجرائم السيبرانية المسجلة من طرف أمن ولاية الجزائر خلال السنتين 2024-2025

المصدر: مقابلة مع إطار عن المصلحة الولائية للشرطة القضائية بأمن ولاية الجزائر في تاريخ 10 ماي 2026. أنظر الملحق رقم 2 صفحة 108.

بناء على البيانات الواردة، شهدت الجريمة الإلكترونية طفرة كبيرة بنسبة نمو تجاوزت 74% في إجمالي القضايا المسجلة بين عامي 2024 و2025. ويلاحظ أن جرائم المساس بالأشخاص والنصب عبر الإنترنت، هي الأكثر انتشارا وتصاعدا. وبالتوازي مع هذا الارتفاع، كثفت المصالح المختصة جهودها حيث ارتفع عدد القضايا المعالجة من 411إلى 674قضية معالجة، مما يعكس استجابة أمنية نشطة لمواجهة هذه التهديدات الرقمية المتزايدة.

كما سجلت الجزائر عموما سنة 2025 ما مجموعه 13,204 قضية متعلقة بالجريمة السيبرانية، تورط فيها 7,815 شخصًا، ويعد هذا الرقم منحى تصاعديا لهذه الظاهرة، مما يعكس تزايد حجمها بشكل متسارع. [1]

وتتعلق أبرز هذه الجرائم بالاحتيال الإلكتروني، والاعتداءات على حقوق الأطفال، وكذا الاتجار غير المشروع عبر الإنترنت. وقد ساهم الانتشار الواسع لوسائل التواصل الاجتماعي والتجارة الإلكترونية غير الرسمية في ظهور أنماط جديدة من الإجرام، تعتمد أساسا على انتحال الهوية وتقنيات الهندسة الاجتماعية، مما يزيد من صعوبة كشفها وتتبعها[2].

وفي إطار مكافحة الجرائم السيبرانية، نفذت المصلحة المركزية لمكافحة الجرائم السيبرانية للأمن الوطني (SCLC) خلال شهر ديسمبر 2025، بالتنسيق مع فرقها المتخصصة، عمليات أمنية واسعة النطاق شملت مختلف ولايات الوطن، وذلك بهدف تعزيز الأمن الرقمي وحماية المواطنين وممتلكاتهم. وقد اسفرت عن تفكيك 32 شبكة إجرامية منظمة متخصصة في النصب عبر الإنترنت، من بينها شبكة ذات امتداد دولي، مع توقيف 197 شخصًا متورطًا في عمليات التصيد الاحتيالي. كما كشفت التحليلات الجنائية أن هذه الشبكات

[1] الشرطة الجزائرية، "الحصيلة السنوية لنشاطات المصالح العملياتية للأمن الوطني خلال سنة 2025"، YouTube، تاريخ الاطلاع 8 أفريل 2026، https://www.youtube.com/watch?v=ByAbWkRnTcc

[2] الشرطة الجزائرية،"دور مصالح الأمن الوطني في محاربة الجرائم الإلكترونية"، YouTube، تاريخ الاطلاع 8 أفريل2026، https://www.youtube.com/watch?v=nJw1M6Lsm-U

تعتمد على أساليب متطورة لجمع معلومات الضحايا، مثل الهندسة الاجتماعية والتصيد الاحتيالي، وانتحال هوية مؤسسات عمومية وخاصة، على غرار تطبيق "بريدي موب"، وهو ما تسبب في خسائر مالية تجاوزت 52 مليار سنتيم. [1]

يتضح من خلال المعطيات السابقة أن التهديدات الأمنية السيبرانية في الجزائر تشهد تطورا ملحوظا من حيث الحجم والتنوع والتعقيد. فالمؤشرات العالمية، على غرار ارتفاع عدد البرمجيات الخبيثة وتزايد نشاط برامج سرقة البيانات والتجسس، تعكس بيئة رقمية دولية متوترة تنعكس بدورها على الواقع الوطني.

وعلى المستوى المحلي، تؤكد الأرقام المسجلة من طرف الجهات الأمنية، إلى جانب البيانات الإحصائية للفترة الممتدة بين 2020 و2025، وجود منحى تصاعدي واضح للجرائم السيبرانية، سواء من حيث عدد القضايا أو عدد المتورطين، مع بروز خاص لجرائم النصب والاحتيال عبر الإنترنت، والاعتداءات المرتبطة بالمحتوى الرقمي، فضلا عن جرائم المساس بالحياة الخاصة للأشخاص، بما في ذلك الابتزاز الإلكتروني، إضافة إلى استهداف الأفراد والمؤسسات على حد سواء.

كما تبرز العمليات الأمنية المنفذة ميدانيا، أن هذه التهديدات لم تعد تقتصر على ممارسات فردية معزولة، بل أصبحت تعتمد على تنظيمات إجرامية تستغل تقنيات متطورة، مثل الهندسة الاجتماعية، والتصيد الاحتيالي، وانتحال الهوية، لتحقيق أهدافها، فضلا عن استغلال الفضاء الرقمي في أنشطة غير مشروعة مثل بيع السلع المحظورة عبر الإنترنت.

وبناء على ذلك، تتخذ التهديدات السيبرانية في الجزائر أشكالاً متعددة، تجمع بين تهديدات تقنية، كالهجمات بالبرمجيات الخبيثة واختراق الأنظمة، وتهديدات سلوكية قائمة على الخداع والتلاعب بالمستخدمين، إضافة إلى جرائم تمس بالنظام العام والحقوق الفردية، الأمر الذي

[1] الموقع الرسمي للشرطة الجزائرية، تاريخ الاطلاع 10 أفريل2026،
https://www.algeriepolice.dz/?%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A-%D8%AA%D9%88%D9%82%D9%8A%D9%81-197-%D9%85%D8%AD%D8%AA%D8%A7%D9%84-%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%8A%D9%86%D8%B4%D8%B7%D9%88%D9%86

يزيد من صعوبة مكافحتها، ويستدعي اعتماد مقاربة شاملة ترتكز على التكامل بين الحلول التقنية، والتدابير القانونية، وتعزيز الوعي الرقمي لدى مختلف الفاعلين.

كما تم الاستفادة من المعطيات الميدانية المتحصل عليها خلال فترة التربص على مستوى وكالة الأنباء الجزائرية، والتي أتاحت الاطلاع على طبيعة التهديدات السيبرانية التي تستهدف المؤسسات العمومية والاقتصادية في الجزائر. وفي هذا الإطار، سجل خلال شهر أفريل 2025 تعرض الموقع الإلكتروني لوكالة الأنباء الجزائرية لأربع هجمات من نوع حجب الخدمة الموزعة (DDoS) خلال أسبوع واحد، وهو ما يعكس تصاعد الهجمات الموجهة ضد المؤسسات الوطنية الحساسة. كما تبين أن البريد الإلكتروني المهني للمؤسسة يتعرض يومياً لأكثر من 500 محاولة هجوم إلكتروني يتم التصدي لها وحجبها بواسطة أنظمة الحماية، الأمر الذي يبرز الحجم المتزايد للتهديدات السيبرانية ومحاولات الاختراق والاستهداف الرقمي التي تواجهها المؤسسات الجزائرية. [1]

المطلب الثاني: تداعيات التهديدات الأمنية السيبرانية على الجزائر

بعد التطرق إلى أشكال التهديدات السيبرانية التي تواجه الجزائر، يجدر تحليل انعكاساتها على الأمن الوطني، باعتبارها لم تعد تقتصر على الجانب التقني، بل امتدت لتشمل مختلف الأبعاد الحيوية للدولة، وذلك في ظل تزايد الاعتماد على التكنولوجيات الرقمية.

فعلى الصعيد الأمني، تساهم الجرائم السيبرانية في زعزعة الاستقرار الداخلي، من خلال انتشار جرائم النصب والاحتيال الإلكتروني، وانتحال الهوية، والتصيد الاحتيالي، وهي الجرائم التي شهدت تزايدا ملحوظا خلال السنوات الأخيرة. كما يعكس تفكيك شبكات إجرامية منظمة تنشط عبر الإنترنت تطور هذه الظاهرة وتحولها إلى نشاط إجرامي ممنهج، مما يصعب من عملية مكافحتها نظرا لطابعها العابر للحدود.

[1] مقابلة ميدانية مع إطار بمصلحة الأمن السيبراني بوكالة الأنباء الجزائرية، الجزائر العاصمة، 12 ماي 2026. أنظر الملحق رقم 3 صفحة 110.

أما على الصعيد الاقتصادي، فتبرز انعكاسات هذه التهديدات من خلال الخسائر المالية التي يتعرض لها الأفراد والمؤسسات نتيجة عمليات الاحتيال الإلكتروني، إضافة إلى استهداف الشركات، خاصة الصغيرة والمتوسطة، الأمر الذي يؤثر سلبا على الثقة في المعاملات الرقمية ويعيق مسار التحول الرقمي.

وفيما يتعلق بالبعد الاجتماعي، تؤدي التهديدات السيبرانية إلى المساس بالحياة الخاصة للأفراد، من خلال جرائم الابتزاز الإلكتروني وانتهاك الخصوصية، فضلا عن استهداف فئة الأطفال عبر الإنترنت، وهو ما يشكل خطرا على القيم الاجتماعية ويؤثر على تماسك المجتمع.

كما تمتد هذه الانعكاسات إلى البعد السيادي والاستراتيجي، حيث يمكن أن تؤدي الهجمات السيبرانية إلى استهداف الأنظمة المعلوماتية والبنى التحتية الحيوية، وهو ما يشكل تهديدا مباشرا لأمن الدولة وسيادتها الرقمية، خاصة في ظل الاعتماد المتزايد على الأنظمة الرقمية في تسيير المرافق العمومية.

ومن الناحية القانونية، ورغم الجهود المبذولة في مجال سن التشريعات المتعلقة بمكافحة الجرائم السيبرانية، إلا أن التطور السريع لهذه التهديدات يفرض تحديات مستمرة على فعالية هذه الأطر القانونية، مما يستدعي مواكبتها للتطورات التكنولوجية. [1]

في ضوء ما سبق، يتبين أن التهديدات السيبرانية في الجزائر تتسم بتعدد أشكالها وتزايد انعكاساتها على مختلف المستويات، مما يجعلها من أبرز التحديات الأمنية المعاصرة. وبينما تكشف المعطيات عن تصاعد هذه الظاهرة، فإن مواجهتها تستدعي تطوير استراتيجيات وطنية فعالة ترتكز على الوقاية والاستباق، وتعزيز القدرات التقنية والبشرية، بما يضمن تحقيق الأمن السيبراني كأحد مكونات الأمن الوطني الشامل.

[1] مصطفى جمعي، التهديدات الأمنية السيبرانية وأثرها على الأمن الوطني الجزائري 2018-2020. مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2021، ص.48-51.

المبحث الثالث: محاور وأهداف الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية

المطلب الأول: حماية البنى التحتية الحيوية

تسعى الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية إلى تعزيز البنية التحتية الرقمية والقدرات التقنية باعتبارها أساس الأمن السيبراني الوطني. حيث أولت الدولة اهتماما كبيرا بتطوير شبكات الاتصال، ومراكز البيانات، والحوسبة السحابية الوطنية، بما يسمح بتأمين وحماية المعطيات الحساسة وضمان استمرارية الخدمات الرقمية. كما نصت الاستراتيجية الوطنية لأمن نظم المعلومات 2025–2029 على ضرورة تعزيز السيادة الرقمية من خلال بناء بنية تحتية قوية قادرة على مواجهة التهديدات السيبرانية المتزايدة.[1]

وفي هذا السياق، تؤكد المرجعية الوطنية لأمن نظم المعلومات (RNSI 2020) على ضرورة تطوير بنية تحتية رقمية مرنة وآمنة، تعتمد على الحوكمة الأمنية وتحديد المسؤوليات داخل المؤسسات، بما يضمن حماية الأنظمة المعلوماتية الحيوية من التهديدات السيبرانية.[2]

ومن الناحية التطبيقية، شرعت الجزائر في تنفيذ مشاريع استراتيجية كبرى، من أبرزها إنشاء مراكز بيانات وطنية متطورة، على غرار مركز البيانات بولاية وهران، الذي يعد من المشاريع المحورية في دعم الحوسبة السحابية الوطنية وتخزين المعطيات الحساسة داخل التراب الوطني، بما يعزز السيادة الرقمية ويحد من المخاطر المرتبطة بالاعتماد على الخوادم الخارجية.[3]

---

[1] وكالة أمن الأنظمة المعلوماتية. الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025–2029. تاريخ الاطلاع 20 أفريل 2026. https://www.mdn.dz/assi/nsiss_ar.pdf

[2] Référentiel National de Sécurité de l'Information, Ministère de la Poste des Télécommunications (MPTI), op.cit .P. 25.

[3] الموقع الرسمي لوزارة البريد والمواصلات السلكية واللاسلكية، تاريخ الاطلاع 1 أفريل2026. https://www.mpt.gov.dz

كما تم تطوير الشبكة السيادية للاتصالات الحكومية بموجب المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر 2025، المتضمن وضع منظومة وطنية لحوكمة البيانات، حيث تم تكريس هذه الشبكة كبنية تحتية داخلية مغلقة وآمنة لتبادل البيانات بين المؤسسات والإدارات العمومية، ومعزولة عن شبكة الإنترنت، بما يقلل من مخاطر الهجمات السيبرانية ويضمن حماية البيانات ذات الطابع الحساس. كما تم ربط مختلف القطاعات الوزارية والهيئات العمومية ومراكز البيانات الوطنية ضمن هذه المنظومة، بما يسمح بتبادل المعلومات في بيئة موحدة وآمنة تدعم التكامل بين المؤسسات وتسهل التحول الرقمي[1].

وفي السياق نفسه، تم تعزيز آليات الحماية السيبرانية من خلال إنشاء مراكز الاستجابة للحوادث الأمنية(CERT) ، التي تتولى مهام مراقبة الأنظمة المعلوماتية، ورصد الهجمات الإلكترونية، وتحليلها، والتدخل السريع للحد من آثارها، وهو ما يمثل عنصرا جوهريا في تعزيز القدرات التقنية للدولة.[2]

كما تعتمد المؤسسات العمومية على حلول تقنية متقدمة مثل جدران الحماية[3] (Firewalls) وأنظمة كشف ومنع التسلل[4] (IDS/IPS) بهدف تأمين الشبكات الداخلية وحماية البيانات من التهديدات الداخلية والخارجية. [5]

---

[1] المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر 2025، الجريدة الرسمية العدد 87.

[2] Référentiel National de Sécurité de l'Information, Ministère de la Poste des Télécommunications (MPTI), op.cit. P.30.

[3] **جدران الحماية (Firewalls): هي أنظمة أو برامج أمنية تستخدم لمراقبة حركة البيانات الواردة والصادرة عبر الشبكات، بهدف حماية الأنظمة المعلوماتية والبرامج والملفات من الاختراق والسرقة والهجمات الإلكترونية التي قد تنفذها جهات خارجية غير مصرح لها.**

[4] **أنظمة كشف ومنع التسلل (IDS/IPS) هي أدوات أمنية سيبرانية تراقب الشبكات والأنظمة .بينما يكتفي نظام كشف التسلل (IDS) بمراقبة حركة البيانات وإرسال تنبيهات عند اكتشاف نشاط مشبوه، يقوم نظام منع التسلل (IPS)باتخاذ إجراءات تلقائية (مثل حظر حركة المرور) لإيقاف التهديدات في الوقت الفعلي قبل حدوث الضرر**

[5] مقابلة ميدانية مع إطار بمصلحة الأمن السيبراني بوكالة الأنباء الجزائرية، الجزائر العاصمة، 12ماي 2026.أنظر الملحق رقم 3 ص 110.

يتضح من خلال ما سبق أن الجزائر تتبنى مقاربة شاملة لحماية البنى التحتية الحيوية، تقوم على الجمع بين تطوير البنية التحتية الرقمية وتعزيز آليات الحماية التقنية والمؤسساتية. فمشاريع مراكز البيانات الوطنية والشبكات السيادية للاتصالات تعكس توجها واضحا نحو ترسيخ السيادة الرقمية وتقليص التبعية التكنولوجية للخارج، في حين تساهم مراكز الاستجابة للحوادث الأمنية والأنظمة التقنية المتخصصة في رفع مستوى الجاهزية السيبرانية للدولة. وعليه، فإن حماية البنى التحتية الحيوية أصبحت تمثل أحد المرتكزات الأساسية للاستراتيجية الوطنية الجزائرية للأمن السيبراني، باعتبارها شرطا ضروريا لضمان استمرارية الخدمات الحيوية وحماية المصالح الوطنية في الفضاء السيبراني.

المطلب الثاني: التكوين والتحسيس في المجال السيبراني

إن كسب رهان الأمن السيبراني لا يرتكز فقط على تطوير البنية التحتية التقنية، بل يقوم أساسا على تثمين العنصر البشري باعتباره الركيزة الجوهرية في منظومة الحماية الرقمية. ففعالية الأمن السيبراني ترتبط بمدى توفر كفاءات مؤهلة، قادرة على فهم التهديدات الرقمية والتعامل معها، وهو ما يجعل من التكوين والتحسيس عنصرين استراتيجيين في بناء أمن سيبراني وطني فعال.

الفرع الأول: التكوين في المجال السيبراني

وفي هذا الإطار، تعتمد الجزائر مقاربة متعددة الأبعاد تقوم على الجمع بين التكوين المتخصص والتأهيل المستمر للإطارات. حيث نظمت وكالة أمن الأنظمة المعلوماتية لوزارة الدفاع الوطني، بالتعاون مع وزارة التعليم العالي والبحث العلمي، دورات تكوينية على مستوى المدرسة الوطنية العليا في الأمن السيبراني، بهدف رفع مستوى الكفاءات التقنية وتحديث معارف الإطارات وفق المعايير الدولية في مجال الأمن السيبراني.[1]

[1] الموقع الرسمي لوكالة الانباء الجزائرية، تاريخ الاطلاع 15 أفريل 2026. https://www.aps.dz/

كما عززت المديرية العامة للأمن الوطني هذا التوجه من خلال تنظيم دورات تكوينية وطنية في الأمن السيبراني والذكاء الاصطناعي لفائدة الإطارات الأمنية المختصة في مكافحة الجرائم السيبرانية، بما يساهم في تطوير قدراتهم في مواجهة التهديدات الرقمية المتزايدة. [1]

ويُلاحظ في هذا السياق أن الجزائر تتجه نحو إدماج الأمن السيبراني داخل المنظومة الأكاديمية بشكل هيكلي، من خلال إنشاء أقطاب علمية متخصصة، أبرزها القطب العلمي والتكنولوجي بسيدي عبد الله، الذي يضم مؤسسات تكوينية متقدمة من بينها المدرسة الوطنية العليا للذكاء الاصطناعي(ENSIA) ، والتي تهدف إلى تكوين مهندسين متخصصين في الذكاء الاصطناعي وعلوم البيانات وفق مقاربات حديثة تتماشى مع التحول الرقمي العالمي[2].

وفي الإطار ذاته، أطلقت المدرسة العليا الجزائرية للأعمال (ESAA) برنامج ماجستير في إدارة الأمن السيبراني، الذي يهدف إلى تكوين كفاءات قادرة على إدارة المخاطر الرقمية والاستجابة الفعّالة للحوادث السيبرانية وفق المعايير الدولية، مما يعكس توجه الدولة نحو بناء نخبة متخصصة في هذا المجال الاستراتيجي. [3]

ويتعزز دور التكوين في مجال الأمن السيبراني في الجزائر من خلال برامج وطنية تهدف إلى إعداد كفاءات قادرة على مواكبة التحولات التكنولوجية، حيث تم إطلاق برنامج وطني للتكوين في مجال الذكاء الاصطناعي من طرف وزارة التكوين والتعليم المهنيين بالتنسيق مع وزارة اقتصاد المعرفة والمؤسسات الناشئة، والذي يعتمد على مقاربة تطبيقية قائمة على المشاريع الواقعية، بهدف تمكين المتكونين من اكتساب مهارات رقمية متقدمة تساهم في دعم البيئة الرقمية الوطنية.[4]

---

[1] الموقع الرسمي للشرطة الجزائرية، تاريخ الاطلاع 15 أفريل 2026. https://www.algeriepolice.dz/

[2] الموقع الرسمي للمدرسة الوطنية العليا للذكاء الاصطناعي، تاريخ الاطلاع 15 أفريل 2026. https://www.ensia.edu.dz/ar/

[3] الموقع الرسمي للمدرسة العليا الجزائرية للأعمال، تاريخ الاطلاع 15 أفريل2026. .https://www.esaa.dz/ar/

[4] الموقع الرسمي لوزارة التكوين والتعليم المهنيين، تاريخ الاطلاع 15 أفريل 2026. https://mvet.gov.dz/

كما أطلقت وزارة البريد والمواصلات السلكية واللاسلكية في 16 ماي 2026 البرنامج الوطني للتمكين الرقمي "77،7" تحت شعار " من سن 7 الى 77 – مسار وطني نحو المهارات الرقمية" ويهدف هذا البرنامج إلى تكوين مختلف فئات المجتمع الجزائري في المهارات الرقمية الأساسية والمتقدمة، من خلال سبع مسارات تعليمية موجهة لمختلف الأعمار، تبدأ بالأطفال وتصل إلى كبار السن.

وتبرز أهمية هذا البرنامج في إدماجه الوعي بالأمن السيبراني كمكوّن إلزامي ضمن جميع المسارات التكوينية، حيث يشمل التوعية بمخاطر التصيد الاحتيالي، وحماية البيانات الشخصية، ومكافحة المعلومات المضللة والاحتيال الرقمي. [1]

وتعكس هذه المبادرة توجهاً استراتيجياً نحو تعزيز الثقافة السيبرانية لدى المواطنين وتقليص الفجوة الرقمية مع رفع الوعي المجتمعي بالمخاطر السيبرانية، بما يساهم في بناء رأس مال بشري قادر على مواكبة متطلبات التحول الرقمي ومواجهة التهديدات السيبرانية المتزايدة في الجزائر.

ويُظهر هذا البرنامج إدراك السلطات الجزائرية بأن الأمن السيبراني لا يرتبط فقط بالبنية التقنية، بل يعتمد أيضاً على العنصر البشري والتكوين المستمر باعتبارهما خط الدفاع الأول ضد التهديدات السيبرانية.

الفرع الثاني: التحسيس في المجال السيبراني

أما على مستوى التحسيس، فإن الجامعات الجزائرية تلعب دورا محوريا في نشر الثقافة السيبرانية، حيث نظمت العديد من الجامعات ندوات علمية وأيام دراسية حول الأمن

[1] فيسبوك وزارة البريد والمواصلات السلكية واللاسلكية، تاريخ الاطلاع 18 ماي2026.
https://web.facebook.com/mpt.gov.dz

السيبراني، بهدف تعزيز وعي الطلبة والباحثين بمخاطر الفضاء الرقمي من بينها جامعة الجزائر 1 بن يوسف بن خدة وجامعة عبد الحميد مهري قسنطينة 02. [1]

وفي هذا السياق، تم إطلاق برامج وطنية لتعزيز دور الشباب في الأمن السيبراني، من خلال المجلس الأعلى للشباب[2]، إضافة إلى تنظيم المسابقة الوطنية للأمن السيبراني CTF) (El-Djazair، التي تهدف إلى اكتشاف الكفاءات الشابة وتطوير مهاراتها في مجال الاختراق الأخلاقي وحماية الأنظمة المعلوماتية، بما يعكس توجها وطنيا نحو إشراك الشباب في بناء السيادة الرقمية. [3]

كما يبرز البعد المؤسساتي من خلال تنظيم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ليوم دراسي حول حماية البيانات في ظل التحول الرقمي والأمن السيبراني والذكاء الاصطناعي، حيث تم التأكيد على أهمية التوازن بين التحول الرقمي وحماية الخصوصية، وتوحيد ممارسات معالجة المعطيات وفق القانون 18-07. كما شدد المشاركون على أن حماية البيانات أصبحت ضرورة قانونية ومجتمعية في ظل الاعتماد المتزايد على المعطيات الرقمية. وفي هذا الإطار، تم التوقيع على اتفاقيات تعاون مع المدرسة الوطنية العليا للذكاء الاصطناعي والمدرسة الوطنية العليا للإعلام الآلي، بهدف تعزيز التكوين والبحث وتطوير حلول رقمية تدعم الأمن السيبراني وحماية المعطيات. [4]

كما تتعزز الجهود التحسيسية من خلال الأجهزة الأمنية التي تعتمد مقاربة وقائية تشمل الحملات الإعلامية، والمشاركة في البرامج التلفزيونية والإذاعية، إضافة إلى حملات موجهة داخل المؤسسات التربوية، بهدف نشر ثقافة الاستخدام الآمن للإنترنت لدى مختلف الفئات.

---

[1] الموقع الرسمي لجامعة الجزائر 1 بن يوسف بن خدة، تاريخ الاطلاع 16 أفريل 2026. https://www.univ-alger.dz/?p=7138&lang=fr

[2] الموقع الرسمي للمجلس الأعلى للشباب، تاريخ الاطلاع 16 أفريل 2026. https://www.csj.gov.dz/detail-article/369

[3] المرجع السابق.

[4] الموقع الرسمي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، تاريخ الاطلاع الاطلاع 16 أفريل 2026. https://anpdp.dz/ar/?page_id=1878

أما أطلقت اتصالات الجزائر فقد أطلقت برنامج"SHIRUDO" ، القائم على أسلوب الألعاب الجادة، والذي يهدف إلى تبسيط مفاهيم الأمن السيبراني وتعزيز السلوك الوقائي لدى المستخدمين بطريقة تفاعلية ومبسطة.[1]

كما تم توسيع نطاق التحسيس ليشمل الفئات الناشئة، من خلال تنظيم أيام إعلامية توعوية لفائدة الأطفال المتمدرسين ، بهدف غرس ثقافة الأمن السيبراني منذ المراحل الأولى للتعليم، وتعزيز قدرتهم على التعامل الآمن مع الوسائط الرقمية حيث تنظم وكالة أمن الأنظمة المعلوماتية لدائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، أياما إعلامية توعوية حول الأمن السيبراني لفائدة الأطفال المتمدرسين من الطور الابتدائي، في إطار مخطط العمل الخاص بالحملات التحسيسية الموجهة لمختلف فئات المجتمع، حيث تم التأكيد على أهمية تعزيز الوعي الرقمي لدى الأطفال، وتمكينهم من التعرف على المخاطر السيبرانية و الوقاية منها، بما يساهم في بناء جيل رقمي واع وآمن. [2]

وفي إطار تعزيز حماية الفئات الهشة داخل الفضاء السيبراني، ولا سيما الأطفال والقصر، شهدت الجزائر تنسيقا متزايدا بين الهيئات المكلفة بحماية الطفولة والأجهزة المختصة بمكافحة الجرائم السيبرانية. ويهدف هذا التعاون إلى تطوير آليات فعالة لرصد التهديدات الرقمية التي قد تستهدف الأطفال، ومتابعة المحتويات الإلكترونية التي تمس بحقوقهم أو تعرضهم لمختلف أشكال الاستغلال والإساءة عبر الإنترنت. كما يندرج ضمن هذا التوجه العمل على إنشاء خلية يقظة سيبرانية تابعة للهيئة الوطنية لحماية وترقية الطفولة، تتولى

[1] الموقع الرسمي لاتصالات الجزائر، تاريخ الاطلاع 16 أفريل 2026.
https://www.algerietelecom.dz/ar/produits/shirudo-formation-en-cyber-securite-en-ligne-prod179

[2] الموقع الرسمي لوزارة الدفاع الوطني، تاريخ الاطلاع الاطلاع 16 أفريل2026.
https://www.mdn.dz/site_principal/sommaire/actualites/ar/2025/avril/cyber12042025ar.php

مهام المتابعة والإنذار المبكر بشأن المخاطر الرقمية التي تهدد سلامة الأطفال في البيئة الإلكترونية.[1]

وفي السياق ذاته، تولي السلطات العمومية أهمية متزايدة للجانب الوقائي من خلال نشر الوعي الرقمي وتعزيز ثقافة الاستخدام الآمن للإنترنت لدى الأطفال والأسر. وتجسد ذلك في إطلاق برامج وحملات تحسيسية تهدف إلى التعريف بمخاطر الاحتيال الإلكتروني وسوء استعمال الوسائط الرقمية، إلى جانب تنظيم أنشطة توعوية موجهة للتلاميذ والأولياء من أجل ترسيخ الممارسات الرقمية الآمنة. كما تسهم الوسائط الإعلامية والرقمية في دعم هذه الجهود عبر نشر محتويات توعوية تساعد على رفع مستوى الوعي بالمخاطر السيبرانية والحد من انعكاساتها على الفئات الناشئة[2].

من خلال مختلف برامج التكوين والتحسيس المعتمدة، يتبين أن الجزائر تسعى إلى بناء مقاربة وقائية للأمن السيبراني ترتكز على تنمية الموارد البشرية إلى جانب تطوير الوسائل التقنية. فإدماج الأمن السيبراني في المؤسسات الجامعية والتكوينية، وتنظيم الدورات المتخصصة لفائدة الإطارات، وإطلاق برامج وطنية للتمكين الرقمي، كلها مؤشرات على إدراك الدولة لأهمية العنصر البشري في مواجهة التهديدات السيبرانية. كما تعكس هذه الجهود انتقال السياسة الوطنية من التركيز على الحماية التقنية فقط إلى تبني مفهوم أكثر شمولا للأمن السيبراني، يقوم على نشر الثقافة السيبرانية وتعزيز الوعي الرقمي لدى مختلف فئات المجتمع، بما يسهم في بناء بيئة رقمية أكثر أمنا وقدرة على مواجهة المخاطر المستقبلية.

[1] الموقع الرسمي للشرطة الجزائرية، تاريخ الاطلاع 17 أفريل2026. https://www.algeriepolice.dz/

[2] الموقع الرسمي لوزارة وزارة البريد والمواصلات السلكية واللاسلكية، الأسرة والطفل عبر الأنترنت بأمان من أجل فضاء أنترنت آمن، تاريخ الاطلاع 17 أفريل2026. https://www.mpt.gov.dz/

المطلب الثالث: التعاون الوطني والدولي في المجال السيبراني.

يعد التعاون في المجال السيبراني من الركائز الأساسية لتعزيز الأمن الرقمي، نظرا للطبيعة المعقدة والعابرة للحدود التي تميز التهديدات السيبرانية، مما يستوجب تنسيقا فعالا بين مختلف الفاعلين على المستويين الوطني والدولي.

الفرع الأول: التعاون الوطني

على الصعيد الوطني، تعتمد الجزائر على مقاربة تشاركية تقوم على تنسيق الجهود بين مختلف المؤسسات والهيئات، لاسيما الأجهزة الأمنية، والقطاعات الوزارية، والمؤسسات الأكاديمية، بهدف تعزيز الجاهزية السيبرانية وتحسين آليات الوقاية والاستجابة للتهديدات الرقمية.

ويتجسد هذا التعاون من خلال التكامل بين الهيئات الأمنية والمؤسسات الجامعية في مجالات التكوين وتبادل الخبرات، إضافة إلى التنسيق مع مختلف القطاعات الحكومية لضمان حماية الأنظمة المعلوماتية والبيانات الحساسة.

كما يمتد هذا التعاون ليشمل التنسيق بين الأجهزة الأمنية والهيئات القضائية، مما يسمح بتحسين آليات مكافحة الجرائم السيبرانية وتعزيز فعالية المتابعة والتحقيق، إلى جانب دعم بناء القدرات الوطنية من خلال الشراكات مع المؤسسات الأكاديمية ومراكز البحث.

الفرع الثاني: التعاون الدولي

على الصعيد الدولي، تعمل الجزائر على تعزيز حضورها في الجهود العالمية لمكافحة الجرائم السيبرانية من خلال الانخراط في الاتفاقيات الدولية وتطوير شراكات تقنية مع مختلف الدول والمنظمات.

وفي هذا الإطار، يعد توقيع الجزائر على اتفاقية الأمم المتحدة لمكافحة الجرائم السيبرانية تجسيدا لالتزامها بالعمل متعدد الأطراف، حيث تهدف هذه الاتفاقية إلى وضع إطار قانوني

دولي يعزز التعاون بين الدول، خاصة في مجالات تبادل الأدلة الإلكترونية وتكييف آليات التحقيق مع البيئة الرقمية.[1]

كما يبرز التعاون الدولي من خلال الشراكات التقنية، لاسيما التعاون بين AFRIPOL وشركة Kaspersky، القائم على تبادل المعلومات حول التهديدات السيبرانية وتحليلها ودعم القدرات التقنية لأجهزة إنفاذ القانون، بما يعزز الجهود الإفريقية في مواجهة الجرائم السيبرانية. [2]

وفي السياق ذاته، تعمل الجزائر على تطوير تعاون ثنائي مع دول رائدة في المجال الرقمي، كما هو الحال في التعاون الجزائري–الكوري في مجال الأمن السيبراني، والذي يتجسد من خلال تنظيم منتديات مشتركة تهدف إلى تبادل الخبرات وبناء القدرات التقنية ودعم التحول الرقمي الآمن.[3]

[1] الموقع الرسمي لوزارة الشؤون الخارجية، تاريخ الاطلاع 30 أفريل 2026. https://www.mfa.gov.dz/ar

[2] Site officiel de l'Afripol, Consulté le 30 Avril 2026. https://afripol.africa-union.org/fr

[3] الموقع الرسمي ل وزارة البريد والمواصلات السلكية واللاسلكية، تاريخ الاطلاع 30 مارس 2026. https://www.mpt.gov.dz/

خلاصة الفصل الثاني

إن دراسة الاستراتيجية الجزائرية لمواجهة التهديدات السيبرانية تبرز الاهتمام المتزايد الذي توليه الجزائر لمجال الأمن السيبراني باعتباره عنصرا أساسيا في حماية الأمن الوطني ومواكبة التحول الرقمي. وقد تجسد ذلك من خلال وضع إطار قانوني وتنظيمي يهدف إلى مكافحة الجرائم الإلكترونية وتعزيز حماية الأنظمة المعلوماتية، إلى جانب إنشاء هيئات ومؤسسات متخصصة تتولى مهمة الوقاية من التهديدات السيبرانية والتصدي لها.

كما بينت الدراسة أن الاستراتيجية الوطنية الجزائرية ترتكز على مجموعة من المحاور الأساسية، أبرزها حماية البنى التحتية الحيوية، وتطوير التكوين والتحسيس في المجال السيبراني، وتعزيز التعاون الوطني والدولي لمواجهة المخاطر الرقمية المتزايدة. وتظهر هذه الجهود سعي الجزائر إلى بناء منظومة سيبرانية متكاملة قادرة على تعزيز الأمن الرقمي ودعم استقرار مؤسسات الدولة في ظل التحولات التكنولوجية المتسارعة.

الفصل الثالث: تحديات ورهانات مواجهة التهديدات السيبرانية في الجزائر

تمهيد

أصبح الأمن السيبراني في الوقت الراهن من أبرز التحديات التي تواجه الدول في ظل التوسع المتزايد في استخدام تكنولوجيات الإعلام والاتصال وتسارع وتيرة التحول الرقمي، حيث لم تعد التهديدات السيبرانية تقتصر على الجوانب التقنية فقط، بل أصبحت تمس مختلف الأبعاد الأمنية والاقتصادية والسياسية. وفي هذا الإطار، تسعى الجزائر إلى تعزيز استراتيجيتها الوطنية للأمن السيبراني لمواجهة المخاطر الرقمية المتنامية وحماية فضائها السيبراني.

غير أن تحقيق فعالية هذه الاستراتيجية يواجه عدة تحديات تقنية وبشرية وقانونية، تفرض ضرورة تطوير القدرات الوطنية وتعزيز الجاهزية لمواجهة التهديدات السيبرانية المتطورة. وفي المقابل، يمثل الأمن السيبراني رهانًا استراتيجيًا بالنسبة للجزائر، باعتباره مرتبطًا بتحقيق السيادة الرقمية، وحماية المعطيات، ودعم التنمية الاقتصادية والتحول الرقمي، إضافة إلى تعزيز مكانة الدولة ضمن منظومة الحوكمة السيبرانية الدولية.

وعليه، يهدف هذا الفصل إلى دراسة أبرز التحديات التي تواجه الاستراتيجية الوطنية للأمن السيبراني في الجزائر، ثم التطرق إلى الرهانات المستقبلية المرتبطة بتعزيز الأمن السيبراني ودوره في دعم الأمن الوطني والتنمية الشاملة.

المبحث الأول: التحديات التي تواجه الاستراتيجية الوطنية للأمن السيبراني

المطلب الأول :التحديات التقنية والتكنولوجية

يتسم الفضاء السيبراني اليوم بتعقيد متزايد وغير مسبوق، يتجاوز الأطر الدفاعية التقليدية، نتيجة التداخل العميق بين التقنيات الناشئة والأنظمة الحيوية للمؤسسات والدول ويعود هذا التعقيد أساسا إلى التسارع الكبير في اعتماد التقنيات الحديثة، بما في ذلك الذكاء الاصطناعي، وما يرافقه من تحولات في طبيعة التهديدات والهجمات السيبرانية، التي أصبحت أكثر تطورا ودقة واتساعا في نطاق تأثيرها. كما أن التطور المستمر في التقنيات الناشئة يعزز من صعوبة ضبط المجال السيبراني ويزيد من مستويات المخاطر المرتبطة به. [1]

إضافة إلى ذلك، أدى الاعتماد المتزايد على سلاسل التوريد الرقمية المترابطة والخدمات السحابية إلى خلق بيئة تقنية معقدة تتسم بضعف الشفافية وصعوبة تتبع الثغرات الأمنية، خصوصا تلك الناتجة عن أطراف ثالثة، مما ينعكس سلبا على مرونة الأنظمة المعلوماتية وقدرتها على الصمود أمام الهجمات. [2]

تشهد الجزائر جملة من التحديات التقنية المرتبطة بتطور البيئة الرقمية، حيث أدى الانتشار الواسع لتكنولوجيات الاتصال الحديثة، مثل شبكات الأنترنت اللاسلكي (WiFi) وتقنيات الجيل الرابع والخامس(4G,5G) التي ساهمت في توسيع نطاق الفضاء السيبراني وزيادة تعقيده، الأمر الذي أدى الى صعوبة مراقبة الشبكات وتعقب الهجمات الالكترونية، خاصة مع إمكانية تنفيذها عن بعد دون قيود مكانية.

كما ساهمت تكنولوجيا الإنترنت عالي التدفق(FTTH) في تسريع تنفيذ الهجمات والجرائم الإلكترونية وتوسيع نطاقها، مما يفرض على الجهات المختصة ضرورة امتلاك أنظمة متطورة لاستجابة سريعة وفعالة.

---

[1] World Economic Forum. Global Cybersecurity Outlook 2025: Navigating through rising cyber complexities. Geneva, 2025, P.P.3-16. Accessed April 23,2026. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[2] Ibid, PP.7-25.

ومن جهة أخرى، يشكل استخدام تقنيات إخفاء الهوية، مثل الخوادم الوسيطة (Proxy)، تحديا تقنيا كبيرًا، حيث تعقد عمليات التحقيق الرقمي وتستدعي توظيف أدوات متقدمة في التحليل الجنائي المعلوماتي.[1]

ويشكل التطور المتسارع لتقنيات الذكاء الاصطناعي أحد أبرز التحديات التي تواجه الأمن السيبراني في الوقت الراهن، نظراً لما تتيحه هذه التقنيات من إمكانات متقدمة يمكن توظيفها لأغراض مشروعة أو استغلالها في أنشطة سيبرانية ضارة. فقد أصبحت أدوات الذكاء الاصطناعي قادرة على القيام بهجمات الإلكترونية، وتحليل الثغرات الأمنية بسرعة كبيرة، وإنتاج محتويات رقمية مزيفة ذات درجة عالية من الإقناع، مثل تقنيات التزييف العميق (Deepfake)، مما يزيد من صعوبة اكتشاف التهديدات والتصدي لها. [2]

وعند إسقاط هذه التحديات على الواقع الميداني الجزائري، تبرز الحاجة الملحة لتحديث البنية التحتية الرقمية؛ إذ تشير المعطيات التي تم الحصول عليها من أمن ولاية الجزائر (2026) إلى أن الثغرات المرتبطة بكيان الأنظمة (الأجهزة والبرمجيات) كانت مسؤولة عن جزء كبير من القضايا السيبرانية المعالجة التي مست المؤسسات، وهو ما يؤكد أن الجانب التقني يمثل الركيزة الأساسية في الاستراتيجية الوطنية للمواجهة، ويفرض تحديثاً مستمراً للمنظومات الدفاعية لمواكبة التهديدات المتطورة. [3]

---

[1] عادل بوعرعار، الاليات المسخرة لمواجهة تحديات الامن السيبراني في الجزائر، **مجلة سوسيولوجيا الجريمة للبحوث والدراسات في الظواهر الاجرامية**، م.6، (2025)، ص ص. 97،98.

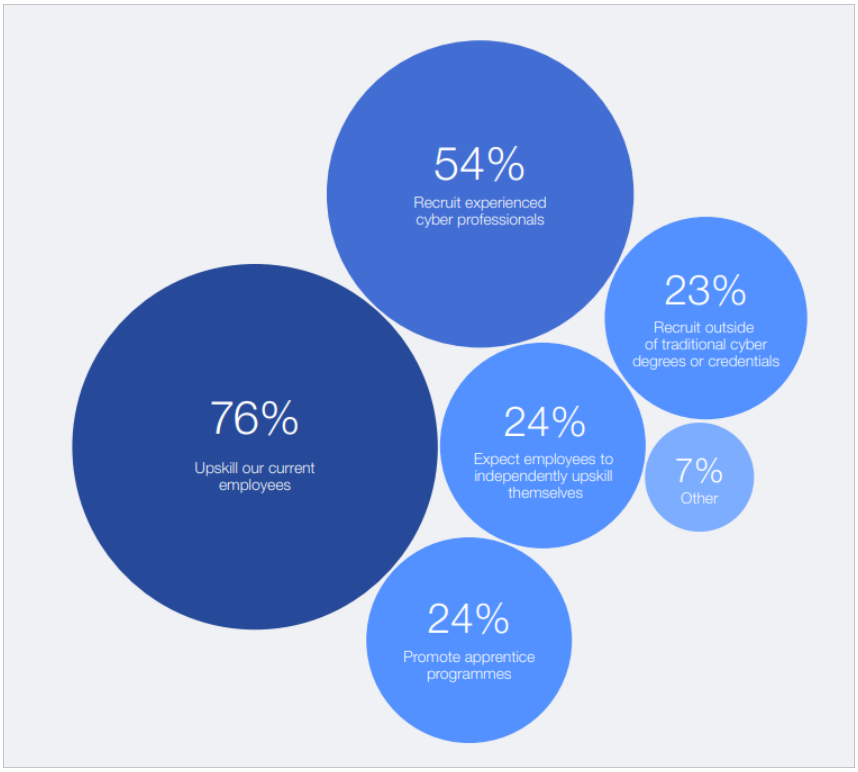
[2] مراد أحداد، حكيمة جاب الله، "استخدامات الذكاء الاصطناعي في تعزيز الأمن السيبراني: دراسة في الفرص والتحديات"، **مجلة هيرودوت للعلوم الإنسانية والاجتماعية**، المجلد 9، العدد 5، 2025، ص ص 371–386.

[3] مقابلة ميدانية مع إطار عن المصلحة الولائية للشرطة القضائية بأمن ولاية الجزائر في تاريخ 10 ماي 2026. أنظر الملحق رقم 1 صفحة 106.

المطلب الثاني :التحديات البشرية والتكوينية

يتناول تقرير المنتدى الاقتصادي العالمي التحديات البشرية والتكوينية باعتبارها أحد العوامل الرئيسية التي تزيد من تعقيد المشهد السيبراني العالمي، حيث يشير إلى اتساع فجوة المهارات في مجال الأمن السيبراني بنسبة 8% منذ عام 2024، مع تأكيد أن منظمتين من كل ثلاث منظمات تعانيان من نقص في المهارات يتراوح بين المتوسط والحرج. [1]

وفي هذا السياق، يبرز نقص المواهب والكفاءات المتخصصة كأحد أبرز التحديات، إذ لا تتجاوز نسبة المنظمات التي تبدي ثقة في امتلاكها للموارد البشرية المؤهلة لمواجهة المتطلبات الأمنية الحالية14% فقط، بينما يعد القطاع العام الأكثر تأثرا، حيث صرحت 49% من مؤسساته بوجود نقص في الكفاءات، مع تسجيل ارتفاع ملحوظ مقارنة بالسنوات السابقة ويؤدي هذا النقص إلى زيادة هشاشة الأنظمة، حيث تصبح أكثر من ثلثي المنظمات عرضة للهجمات السيبرانية المتقدمة نتيجة غياب المهارات الحيوية.[2]



[1] World Economic Forum. op.cit, P. 36.

[2] Ibid.

الشكل رقم (4): كيف تتعامل المنظمات مع فجوة المهارات في مجال الأمن السيبراني

المصدر: World Economic Forum. Global Cybersecurity Outlook 2025: Navigating through rising cyber complexities. Geneva, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

من خلال الشكل رقم 4، تعتمد 76% من المنظمات على إعادة تأهيل وصقل مهارات موظفيها الحاليين، في حين تلجأ 54% إلى توظيف خبرات جاهزة، و24% إلى برامج التكوين المهني، بينما تسعى 23% إلى استقطاب كفاءات من تخصصات غير تقنية لسد الفجوة بين البعد التقني وتأثيراته التنظيمية. ومع ذلك، لا يزال الاستثمار في مهارات الذكاء الاصطناعي محدودًا، حيث أشار 67% من القادة الى وجود فجوة واضحة في هذا المجال.[1]

بالرجوع الى الحالة الجزائرية، تواجه الجزائر تحديات بشرية وتكوينية في مجال الأمن السيبراني، تتمثل أساسا في نقص الكفاءات المتخصصة وضعف التكوين التقني والتطبيقي، إضافة إلى محدودية برامج التأهيل والتدريب المستمر، الأمر الذي يؤثر على فعالية المؤسسات في التصدي للتهديدات السيبرانية وضمان حماية البنية التحتية الرقمية.[2]

كما أن بعض النقاشات المهنية وتجارب العاملين في المجال تشير إلى وجود طلب متزايد على خبراء الأمن السيبراني في الجزائر، مقابل استمرار مشكلة نقص الخبرة العملية والتكوين المتخصص[3].

وعلى صعيد الواقع العملي، أظهرت المعطيات الميدانية المتحصل عليها خلال فترة التربص بوكالة الأنباء الجزائرية أن العامل البشري يمثل ثغرة أمنية تضاهي في خطورتها الثغرات التقنية، حيث تعود نسبة 70% من الاختراقات المسجلة ضد المؤسسات إلى أخطاء

[1] World Economic Forum. op.cit, PP. 36,37.
[2] Ibid, P .40.
[3] Ibid.

الموظفين الناتجة عن ضعف الوعي الرقمي أو الوقوع في فخاخ الهندسة الاجتماعية، وهو ما يفرض ضرورة الاستثمار في الرأس المال البشري وتعزيز الوعي السيبراني الوطني.[1]

ولا يتوقف تحدي العامل البشري عند حدود البيئة المهنية داخل المؤسسات، بل يمتد ليشمل المواطن كحلقة جوهرية في الفضاء السيبراني، حيث تبرز الفجوة في الثقافة الرقمية والوعي السيبراني لدى شريحة واسعة من أفراد المجتمع كعائق أمام التحول الرقمي الآمن. ويظهر ذلك جليا في سهولة وقوع المواطنين في فخاخ النصب والاحتيال الإلكتروني عبر تقنيات بسيطة ولكنها مؤثرة، مما يعكس الحاجة الملحة لتكثيف الحملات التحسيسية الوطنية.

إن رفع مستوى الإدراك الأمني لدى المواطن لم يعد مجرد خيار، بل أصبح ضرورة أمنية لتحصين الفضاء العام من الهجمات التي تستغل العواطف أو نقص الخبرة التقنية، وهو ما يجعل من 'التوعية المجتمعية الشاملة' رهاناً لا يقل أهمية عن بناء الأنظمة الدفاعية.

المطلب الثالث :التحديات القانونية والتنظيمية

تواجه الدول في مجال الأمن السيبراني جملة من التحديات القانونية والتنظيمية التي ازدادت تعقيدا مع التطور السريع للفضاء الرقمي وتنامي التهديدات العابرة للحدود، حيث يشير تقرير Global Cybersecurity Outlook 2025إلى أن تعدد التشريعات واختلافها بين الدول أدى إلى حالة من "التجزئة التنظيمية"، الأمر الذي يعيق بناء منظومة دولية منسجمة. كما تواجه الدول صعوبة في تحقيق التوازن بين تعزيز الحماية الرقمية وضمان مرونة الأنظمة القانونية لمواكبة التقنيات الناشئة كالحوسبة السحابية والذكاء الاصطناعي، خاصة في ظل تزايد القوانين المتعلقة بحماية البيانات وأمن البنى التحتية الحيوية، وهو ما يضعف فعالية التعاون الدولي ويزيد من تعقيد إدارة المخاطر الرقمية في ظل التوترات الجيوسياسية العالمية . [2]

[1] مقابلة ميدانية مع إطار بمصلحة الأمن السيبراني بوكالة الأنباء الجزائرية، الجزائر العاصمة، 12 ماي 2026. أنظر الملحق رقم 3 صفحة 110.

[2] World Economic Forum, op.cit, p p. 5- 25.

وفي إطار المنظومة القانونية والإجرائية الجزائرية، تبرز هذه التحديات بشكل جلي من خلال محورين أساسيين:

الفرع الأول: تحدي البيئة التشريعية الداخلية

تتسم الاستراتيجية الجزائرية بتعدد النصوص التشريعية المنظمة للمجال وغياب قانون موحد وشامل للأمن السيبراني،ض إذ يعتمد الإطار القانوني الحالي على مجموعة من القوانين والمراسيم المتفرقة مثل قانون مكافحة الجرائم المعلوماتية (09-04)، وقانون حماية المعطيات الشخصية (18-07)، وقانون البريد والاتصالات الإلكترونية (18-04).
ويضاف إلى هذا التشتت تحدي "الفجوة الزمنية" بين التشريع والتنفيذ، وهو ما تجسد في تأخر تفعيل قانون حماية المعطيات الشخصية لسنوات قبل دخوله حيز التطبيق الفعلي عام 2023. [1]

الفرع الثاني: تحديات الملاحقة الدولية والسيادة الرقمية

تبرز عقبات ملموسة عند التعامل مع الجرائم التي يكون مصدرها خارج الحدود الإقليمية، إذ أكدت التجربة الميدانية لـ أمن ولاية الجزائر أن نجاح الملاحقة القضائية الدولية وإجراءات التحقيق الرقمي يرتكز بشكل أساسي على مدى تفعيل "مبدأ المعاملة بالمثل "في إطار الاتفاقيات الثنائية. فبينما يسير التعاون بسلاسة مع الدول التي تربطها بالجزائر اتفاقيات تعاون مشترك، تظل الصعوبات الإجرائية قائمة في حالات غياب هذه الأطر، مما يؤدي إلى بطء في تتبع الأثر الرقمي للمجرمين[2] .

[1] Data protection and cybersecurity laws in Algeria, **27 Jan 2026, https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria2?utm**

[2]مقابلة ميدانية مع إطار عن المصلحة الولائية للشرطة القضائية بأمن ولاية الجزائر في تاريخ 10 ماي 2026. انظر الملحق رقم 1 صفحة 106.

يظل تحديث الترسانة القانونية وتوحيدها، وتطوير الآليات المنظمة للتعاون القضائي الدولي، رهانا حتميا لضمان انسيابية تبادل الأدلة الرقمية وملاحقة الجناة، بما يخدم مصلحة الأمن الوطني ويجسد مفهوم السيادة الرقمية الكاملة في مواجهة تهديدات عابرة للحدود بطبيعتها.

المبحث الثاني: الرهانات المستقبلية لتعزيز الأمن السيبراني في الجزائر

المطلب الأول: السيادة الرقمية وحماية المعطيات

تعد السيادة الرقمية مبدأ توجيهيا استراتيجيا يهدف إلى حماية الفضاء السيبراني الوطني . وتتمثل رهاناته في :

1. **توطين البيانات والبنية التحتية** :الرهان على امتلاك أكثر من5 مراكز بيانات وطنية متوافقة مع المعايير الدولية لضمان معالجة وتخزين البيانات داخل الحدود الوطنية وتعزيز الاستقلالية التكنولوجية. [1]
2. **الاستقلالية التكنولوجية** :تطوير الصناعة الرقمية المحلية وتقليل التبعية للخارج من خلال تعزيز البنى التحتية الرقمية الأساسية . [2]
3. **حماية الخصوصية** :الالتزام بضمان حماية البيانات الشخصية وإدارتها بطريقة مؤمنة وفق التشريعات والقواعد الأخلاقية، وهو رهان أساسي لبناء الثقة مع المواطنين . [3]
4. **الهوية الرقمية الوطنية** :ومن بين الأهداف المسطرة ضمن الاستراتيجية الوصول إلى نصف مليون اسم نطاق وطني (dz.) لتعزيز التمثيل والسيادة الرقمية عبر الإنترنت[4] .

يتضح من خلال هذه الرهانات أن الجزائر تسعى إلى تعزيز سيادتها الرقمية باعتبارها أحد مقومات الأمن الوطني في العصر الرقمي. فحماية البيانات وتوطينها داخل الحدود الوطنية

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، رئاسة الجمهورية، المحافظة السامية للرقمنة، "الاستراتيجية الوطنية للتحول الرقمي في الجزائر 2025–2030"، نسخة أوت 2024، ص.15 https://www.hcn.dz/SNTN-Ar.pdf

[2] المرجع نفسه، ص ص. 8- 12.

[3] المرجع نفسه.

[4] المرجع نفسه، ص. 15.

من شأنه أن يقلل من مخاطر التبعية التكنولوجية والاختراقات الخارجية، كما يساهم في تعزيز الثقة في الخدمات الرقمية. غير أن تحقيق هذه الأهداف يبقى مرتبطاً بمدى قدرة الدولة على تطوير بنية تحتية رقمية متطورة، وتوفير الكفاءات اللازمة لإدارتها وتأمينها.

المطلب الثاني: الأمن السيبراني كشرط للتنمية الاقتصادية والتحول الرقمي

يمثل الأمن الرقمي دعامة أساسية وبالغة الأهمية يرتكز عليها أمن محاور التحول الرقمي. وتبرز الرهانات الاقتصادية كالتالي :

1. **تحصين الاقتصاد الرقمي** :مرافقة التحول الرقمي للقطاع الاقتصادي ومؤسسات الدولة، وحماية التراث المعلوماتي الوطني كأداة للتنمية الاجتماعية والاقتصادية . [1]
2. **أمن المعاملات المالية** :توفير بيئة آمنة لترقية الشمول المالي، خاصة مع التوجه نحو إلغاء الدفع النقدي للمعاملات التي تتجاوز 500,000 دج . [2]
3. **حماية البنى التحتية الحساسة** :ضمان أمن ومرونة الأنظمة في قطاعات الطاقة، الصحة، الاتصالات، والنقل، حيث أن أي تعطيل لعملها ينجر عنه آثار سلبية كبيرة على الأمن الوطني ورفاهية السكان . [3]
4. **جذب الاستثمارات:** توفير بيئة سيبرانية آمنة من شأنها تعزيز جاذبية الجزائر للاستثمارات الأجنبية في مجال الاقتصاد الرقمي . [4]
5. **دعم المؤسسات الناشئة** :دعم المؤسسات الناشئة العاملة في مجال الرقمنة وتعزيز مساهمتها في الاقتصاد الوطني. [5]

---

[1] الجمهورية الجزائرية الديمقراطية الشعبية، وكالة أمن الأنظمة المعلوماتية، "الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025–2029، ص ص. 2-5.

[2] الاستراتيجية الوطنية للتحول الرقمي في الجزائر2025–2030، المرجع السابق، ص 18.

[3] الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029 ، المرجع السابق، ص 3-5

[4] الاستراتيجية الوطنية للتحول الرقمي في الجزائر2025–2030، المرجع السابق، ص 19.

[5] المرجع نفسه، ص 18.

تبرز هذه الرهانات العلاقة الوثيقة بين الأمن السيبراني والتنمية الاقتصادية، حيث أصبح نجاح مشاريع التحول الرقمي مرهوناً بتوفير بيئة رقمية آمنة تضمن حماية المعطيات والأنظمة الحيوية. فكلما ارتفع مستوى الأمن السيبراني، ازدادت ثقة الأفراد والمؤسسات في الخدمات الرقمية، وهو ما ينعكس إيجاباً على الاستثمار والابتكار ونمو الاقتصاد الرقمي.

المطلب الثالث: تموقع الجزائر في الحوكمة السيبرانية الدولية

تطمح الجزائر الى التموقع كفاعل إقليمي في مجال التحول الرقمي بحلول عام 2030.[1]

ويتمثل هذا التموقع في :

1. **تصدير الخدمات الرقمية** :استغلال قدرات الربط الوطنية لتصدير خدمات الحوسبة السحابية والإنترنت نحو بلدان الجوار ومنطقة الساحل الإفريقي، مما يعزز التعاون الإقليمي . [2]
2. **المساهمة في التشريع الدولي** :الرهان على المساهمة بفعالية في إعداد الإطار القانوني والمعياري على المستوى الدولي في مجال الأمن السيبراني[3] .
3. **تأطير التعاون الدولي** :إقامة روابط عملياتية فعالة لمجابهة التهديدات السيبرانية بصفة جماعية وتأطير التعاون الدولي على المستويين الاستراتيجي والتقني . [4]
4. **الحفاظ على الكفاءات** :الرهان على تقليص هجرة الكفاءات المتخصصة في تكنولوجيات الإعلام والاتصال بنسبة40% لضمان وجود مورد بشري مؤهل يقود التموقع الدولي للجزائر . [5]

تعكس هذه الرهانات إدراك الجزائر للطبيعة العابرة للحدود للتهديدات السيبرانية، والتي تجعل من التعاون الدولي والتنسيق الإقليمي ضرورة استراتيجية لمواجهتها. كما أن تعزيز حضور الجزائر في مجال الحوكمة السيبرانية الدولية يساهم في دعم مكانتها الإقليمية والدولية، ويمنحها فرصة

[1] الاستراتيجية الوطنية للتحول الرقمي في الجزائر 2025–2030، المرجع السابق، ص 10.

[2] المرجع نفسه، ص. 14-15.

[3] الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025-2029، المرجع السايق، ص10

[4] المرجع نفسه، ص. 10.

[5] الاستراتيجية الوطنية للتحول الرقمي في الجزائر، المرجع السابق، ص. 16.

للمشاركة في صياغة القواعد والمعايير المنظمة للفضاء السيبراني. غير أن تحقيق هذا التموقع يبقى رهينا بتطوير القدرات الوطنية، والاستثمار في الموارد البشرية المؤهلة، وتعزيز الشراكات الدولية في المجالات التقنية والأمنية ذات الصلة.

خلاصة الفصل الثالث

من خلال دراسة تحديات ورهانات مواجهة التهديدات السيبرانية، يتضح أن الجزائر تسعى إلى تطوير منظومتها الوطنية للأمن السيبراني لمواجهة المخاطر الرقمية المتزايدة، رغم وجود تحديات تقنية وبشرية وقانونية تؤثر على فعالية هذه الاستراتيجية. وفي المقابل، يشكل الأمن السيبراني رهانا أساسيا لحماية السيادة الرقمية، وتأمين المعطيات، ودعم التنمية الاقتصادية والتحول الرقمي، إضافة إلى تعزيز مكانة الجزائر في مجال الحوكمة السيبرانية الدولية.

الخاتمـــة

توصلت هذه الدراسة إلى أن الأمن السيبراني أصبح يشكل أحد الركائز الأساسية لحماية الأمن الوطني في ظل التحولات الرقمية المتسارعة وما صاحبها من تنامي التهديدات السيبرانية التي تستهدف الدول ومؤسساتها وبناها التحتية الحيوية. فقد أفرز الفضاء السيبراني أنماطا جديدة من المخاطر الأمنية تجاوزت الحدود الجغرافية التقليدية، وأصبحت قادرة على التأثير في مختلف الأبعاد السياسية والاقتصادية والعسكرية والاجتماعية للدولة.

ومن خلال دراسة واقع الأمن السيبراني في الجزائر، تبين أن الدولة الجزائرية أولت اهتماما متزايدا بهذا المجال من خلال تطوير ترسانة قانونية متخصصة، وإنشاء مؤسسات وهيئات مكلفة بحماية الأنظمة المعلوماتية ومكافحة الجرائم والتهديدات السيبرانية، فضلا عن تبني استراتيجيات وطنية تهدف إلى تعزيز أمن الفضاء الرقمي الوطني وحماية المصالح الحيوية للدولة.

كما أظهرت الدراسة أن التهديدات السيبرانية لم تعد تقتصر على الجرائم الإلكترونية البسيطة، بل امتدت لتشمل التجسس السيبراني والإرهاب السيبراني والحروب السيبرانية، الأمر الذي يفرض على الدول تعزيز جاهزيتها وقدراتها التقنية والبشرية لمواجهة هذه المخاطر المتزايدة. وفي هذا الإطار، تسعى الجزائر إلى تعزيز منظومتها الوطنية للأمن السيبراني من خلال تطوير آليات الحماية والوقاية والاستجابة، وتكثيف التعاون بين مختلف المؤسسات والهيئات المعنية.

وعلى ضوء ما سبق، أصبح الأمن السيبراني يمثل ضرورة استراتيجية لحماية الأمن الوطني الجزائري، وأن فعالية الجهود المبذولة في هذا المجال تظل مرتبطة بمدى مواكبة التطورات التكنولوجية المتسارعة، وتعزيز الكفاءات البشرية المتخصصة، وترسيخ ثقافة الأمن السيبراني، بما يساهم في بناء فضاء رقمي آمن يدعم استقرار الدولة ويحافظ على سيادتها ومصالحها الوطنية.

أهم الاستنتاجات:

- الأمن السيبراني أصبح جزءا أساسيا من منظومة الأمن الوطني المعاصرة.
- التهديدات السيبرانية تشكل خطرا حقيقيا على السيادة الوطنية والمؤسسات والبنى التحتية الحيوية.

- اعتمدت الجزائر جملة من الآليات القانونية والمؤسساتية والاستراتيجية المتطورة لمواجهة التهديدات السيبرانية.
- يساهم تطوير القدرات البشرية والتقنية في رفع فعالية منظومة الأمن السيبراني.
- تحقيق الأمن السيبراني يتطلب تعاونا مستمرا بين مختلف الفاعلين الوطنيين والدوليين.
- يمثل تعزيز "السيادة الرقمية" وتوطين البيانات أحد أهم رهانات الأمن الوطني الجزائري في المستقبل.

قائمة المراجع:

النصوص القانونية والتنظيمية

1. الجمهورية الجزائرية الديمقراطية الشعبية. دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996. الجريدة الرسمية، العدد 76، 8 ديسمبر 1996.

2. الجمهورية الجزائرية الديمقراطية الشعبية. دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2016. الجريدة الرسمية، العدد 14، 7 مارس 2016.

3. الجمهورية الجزائرية الديمقراطية الشعبية. دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 2020. الجريدة الرسمية، العدد 82، 30 ديسمبر 2020.

4. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات. الجريدة الرسمية، العدد 71.

5. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون العقوبات. الجريدة الرسمية، العدد 84.

6. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات. الجريدة الرسمية، العدد 84.

7. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 09-04 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 47.

8. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 15-04 المؤرخ في 1 فيفري 2015، المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين. الجريدة الرسمية، العدد 6.

9. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 18-04 المؤرخ في 10 ماي 2018، المتعلق بالبريد والاتصالات الإلكترونية. الجريدة الرسمية، العدد 27.

10. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية. الجريدة الرسمية، العدد 28.

11. الجمهورية الجزائرية الديمقراطية الشعبية. القانون رقم 18-07 المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. الجريدة الرسمية، العدد 34.

12. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 04-183 المؤرخ في 8 جوان 2004، المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني. الجريدة الرسمية، العدد 41.

13. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 53.

14. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية. الجريدة الرسمية، العدد 4.

15. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، العدد 86.

16. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 23-314 المؤرخ في 6 سبتمبر 2023، المتضمن إنشاء المحافظة السامية للرقمنة وتحديد مهامها وتنظيمها وسيرها. الجريدة الرسمية، العدد 59.

17. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 24-63 المؤرخ في 1 فيفري 2024، المتضمن إنشاء المحافظة السامية للرقمنة وتحديد مهامها وتنظيمها وسيرها. الجريدة الرسمية، العدد 8.

18. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 26-07 المؤرخ في 7 جانفي 2026، المتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات. الجريدة الرسمية، العدد 4.

19. الجمهورية الجزائرية الديمقراطية الشعبية. المرسوم الرئاسي رقم 25-320 المؤرخ في 30 ديسمبر 2025، المتضمن وضع منظومة وطنية لحوكمة البيانات. الجريدة الرسمية، العدد 87.

الكتب:

1. أحمد، أشرف السعيد. تكنولوجيا المعلومات وحروب الجيل السادس. 2019.

2. الأشقر جبور، منى. السيبرانية هاجس العصر. المركز العربي للبحوث القانونية والقضائية، 2016.

3. البعلبكي، منير. قاموس المورد: عربي-إنجليزي. بيروت: دار الملايين، 2004.

4. القريطي، دحان حزام. الأمن السيبراني وحماية أمن المعلومات. الإسكندرية: دار الفكر الجامعي، 2021.

5. خماس، علاء الدين حسين. الحرب السيبرانية: مستقبل الحروب في عالم ما وراء الجغرافيا، دراسة استراتيجية في طبيعة حروب القرن الحادي والعشرين في العصر الرقمي. عمان: شركة دار الأكاديميون للنشر والتوزيع، 2025.

6. شاكر، فراس جمال. السيبرانية وتحولات القوة في النظام الدولي. عمان: دار أمجد للنشر والتوزيع، 2023.

7. عبد الله، عماد حسين. إدارة الأمن في المدن الكبرى. الرياض: المركز العربي للدراسات الأمنية والتدريب، 1991.

8. كلارك، ريتشارد، وروبرت نيك. حرب الفضاء الإلكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه. مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012.

9. نوران، شفيق. أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني. القاهرة: المكتب العربي للمعارف، 2016.

المقالات الاكاديمية:

1. أماني، عصام محمد. "استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية." مجلة كلية الاقتصاد والعلوم السياسية (أكتوبر 2021).
2. بارة، سمير. "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات." جامعة قاصدي مرباح ورقلة.
3. بالة، عمار. "إسهامات مدرسة كوبنهاغن في توسيع مفهوم الأمن: من الأمن العسكري إلى الأمن المجتمعي." مجلة الحقوق والحريات، المجلد 10، العدد 2 (2022).
4. بلفرد، لطفي لمين، وبرقوق، امحند. "الفضاء السيبراني: فواعل وتهديدات." مجلة آفاق للعلوم، المجلد 9، العدد 3 (2024).
5. بوغرارة، يوسف. "الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني." مجلة الدراسات الإفريقية وحوض النيل، المجلد 1، العدد 3 (2018).
6. بوقرص، ساعد. "الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة." مجلة الأبحاث في الحماية الاجتماعية، المدرسة العليا للضمان الاجتماعي محمد الصالح منتوري (2022).
7. بوعرعار، عادل. "الآليات المسخرة لمواجهة تحديات الأمن السيبراني في الجزائر." مجلة سوسيولوجيا الجريمة للبحوث والدراسات في الظواهر الإجرامية، المجلد 6 (2025).
8. بوازدية، جمال. "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية." مجلة العلوم القانونية والسياسية، المجلد 10 (2019).
9. رابح، سعاد. "ضوابط مكافحة الجريمة المعلوماتية." مجلة القانون الجزائري العام والمقارن، المجلد 7، العدد 1 (جوان 2021).
10. رضا، مهدي. "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري." مجلة إيليزا للبحوث والدراسات، المجلد 6، العدد 2 (2021).
11. زروقة، إسماعيل. "الفضاء السيبراني والتحول في مفاهيم القوة والصراع." مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1 (أفريل 2019).

12. شويرب، جيلالي، ومراد، فائزة. "مفهوم الحروب السيبرانية والأمن السيبراني." مجلة الحقوق والحريات، المجلد 11 (2023).

13. عطية، إدريس. "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري." مجلة مصداقية، المجلد 1، العدد 1 (ديسمبر 2019).

14. السيد، محمد طه. "مفهوم الأمن القومي". مجلة الأمن القومي والاستراتيجية أكاديمية ناصر العسكرية للدراسات العليا، (2023).

15. الفتلاوي، أحمد عبسي نعمة. "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر." مجلة المحقق للعلوم القانونية والسياسية.

16. الغنجة، هيشام داود. "جيوبوليتيكا الأمن السيبراني: دراسة حالة الصراع الصيني الأمريكي في الفضاء السيبراني." مجلة الفكر القانوني والسياسي، المجلد 9 (2025).

17. قطينة، فهد. **"**الهجمات السيرانية دليل أشهر أنواع الهجمات السيبرانية الشامل.**"** أكاديمية الأمن السيبراني.

18. أحداد،مراد، وجاب الله،حكيمة. "استخدامات الذكاء الاصطناعي في تعزيز الأمن السيبراني : دراسة في الفرص والتحديات"، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 9، العدد 5، 2025.

19. مقري، صونيا وبن لعامر، وليد. المنظومة الوطنية لأمن الأنظمة المعلوماتية كآلية مؤسساتية لمكافحة الجريمة المعلوماتية وفقا للمرسوم الرئاسي رقم 20-05، مجلة البحوث في العقود وقانون الاعمال، المجلد10، العدد2 (2025).

20. كواشي، عتيقة. "تداعيات الإرهاب السيبراني على الامن القومي الجزائري". المجلة الجزائرية للأمن والتنمية، المجلد 12، العدد 3(2023).

التقارير والوثائق الرسمية:

- المحافظة السامية للرقمنة. الاستراتيجية الوطنية للتحول الرقمي في الجزائر. أوت 2024. https://www.hcn.dz/SNTN-Ar.pdf

- وكالة أمن الأنظمة المعلوماتية. الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2025–2029. https://www.mdn.dz/assi/nsiss_ar.pdf.

الرسائل الجامعية:

- بدرين، سيد علي. الاستراتيجية الأمنية الجزائرية لمواجهة التهديدات السيبرانية. مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2023.
- بوطمين، وائل خليل الرحمان. البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة. مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2025.
- شلحة، رشيد. آليات مواجهة التهديدات السيبرانية في الجزائر. مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2019.
- جمعي، مصطفى. التهديدات الأمنية السيبرانية وأثرها على الأمن الوطني الجزائري 2018–2020. مذكرة ماستر، المدرسة الوطنية العليا للعلوم السياسية، 2021.

المواقع الإلكترونية

1. CloudSEK. "تهديدات الجرائم الإلكترونية: أهم 10 دول مستهدفة في عام 2025." تاريخ التصفح 23 مارس 2026. https://www.cloudsek.com/ar/knowledge-base/countries-most-targeted-by-cyberattacks.
2. اتصالات الجزائر. Shirudo – تكوين في الأمن السيبراني. تاريخ التصفح 16 أفريل 2026. https://www.algerietelecom.dz/ar/produits/shirudo-formation-en-cyber-securite-en-ligne-prod179.
3. الاذاعة الجزائرية. الموقع الرسمي. تاريخ التصفح 29 أفريل 2026. https://news.radioalgerie.dz/ar/node/21741
4. الشرطة الجزائرية. الموقع الرسمي. تاريخ التصفح 17 أفريل 2026. https://www.algeriepolice.dz/.

5. السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. الموقع الرسمي. تاريخ التصفح 16 أفريل 2026. https://anpdp.dz/ar/.

6. المجلس الأعلى للشباب. الموقع الرسمي. تاريخ التصفح 16 أفريل 2026. https://www.csj.gov.dz/.

7. المحافظة السامية للرقمنة. الموقع الرسمي. تاريخ التصفح 17 أفريل 2026. https://www.hcn.dz/.

8. المدرسة الوطنية العليا للذكاء الاصطناعي. الموقع الرسمي. تاريخ التصفح 15أفريل 2026. https://www.ensia.edu.dz/ar/.

9. المدرسة العليا الجزائرية للأعمال. الموقع الرسمي. تاريخ التصفح 15 أفريل 2026. https://www.esaa.dz/ar/.

10. المديرية العامة للأمن الوطني. الحصيلة السنوية لنشاطات المصالح العملياتية للأمن الوطني لسنة 2023. تاريخ التصفح1 أفريل 2026. https://www.algeriepolice.dz/IMG/pdf/dpj.pdf.

11. وزارة البريد والمواصلات السلكية واللاسلكية. الموقع الرسمي. تاريخ التصفح 30 مارس 2026. https://www.mpt.gov.dz/.

12. وزارة البريد والمواصلات السلكية واللاسلكية. الصفحة الرسمية على فيسبوك. تاريخ التصفح 18ماي 2026. https://web.facebook.com/mpt.gov.dz.

13. وزارة التكوين والتعليم المهنيين. الموقع الرسمي. تاريخ التصفح 15 أفريل 2026. https://mvet.gov.dz/.

14. وزارة الدفاع الوطني. الموقع الرسمي. تاريخ التصفح 16 أفريل 2026. https://www.mdn.dz/.

15. وزارة الشؤون الخارجية. الموقع الرسمي. تاريخ التصفح 30أفريل 2026. https://www.mfa.gov.dz/ar.

16. وكالة الأنباء الجزائرية. الموقع الرسمي. تاريخ التصفح 15 أفريل 2026. https://www.aps.dz/.

17. جامعة الجزائر 1 بن يوسف بن خدة. الموقع الرسمي. تاريخ التصفح 16 أفريل 2026. https://www.univ-alger.dz/?p=7138&lang=fr.

18. الحصيلة السنوية لنشاطات المصالح العملياتية للأمن الوطني خلال سنة 2025. منصة يوتيوب، منشور من طرف المديرية العامة للأمن الوطني. تاريخ التصفح 8 أفريل 2026. https://www.youtube.com/watch?v=ByAbWkRnTcc.

المراجع باللغة الأجنبية:

الكتب:

1. Larousse Dictionnaire de français. Malesherbes : Imprimerie Maury, mars 2010

2. Ney, Joseph S., Jr. Cyber Power. Cambridge: Harvard Kennedy School, 2010

التقارير:

1. Agence nationale de la sécurité des systèmes d'information (ANSSI). CyberDico. Consulté le 5 avril 2026. https://www.info.gouv.fr/upload/media/content/0001/11/a5fcaf7ccf1f6058d70e3a17570037569b979d84.pdf

2. Trump, Donald J. President Trump's Cyber Strategy for America. Washington, DC: The White House, March 2026. Accessed April 10, 2026. https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf

3. Ministère de la Poste et des Télécommunications (MPTT). Référentiel National de Sécurité de l'Information (RNSI), version finale 2020. Alger: MPTT, 2020. Consulté le 16 mai 2026. https://www.mpt.gov.dz/wp-content/uploads/2023/12/Referentiel-National-de-la-Securite-de-lInformation-2020-VERSION-FINALE-1-1.pdf

4. World Economic Forum. Global Cybersecurity Outlook 2025: Navigating Through Rising Cyber Complexities. Geneva: World Economic Forum,2025. Accessed April 23, 2026.

https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

5. CMS Law. Data Protection and Cybersecurity Laws in Algeria. CMS Expert Guide. 27 January 2026. Accessed 25 May 2026. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/algeria2

6. Agence nationale de la sécurité des systèmes d'information (ANSSI). CyberDico. Consulté le 5 avril 2026. https://www.info.gouv.fr/upload/media/content/0001/11/a5fcaf7ccf1f6058d70e3a17570037569b979d84.pdf

7. NIST, Guide for Conducting Risk Assessments, Special Publication 800-30 Revision 1. Accessed 25 April 2026. https://csrc.nist.rip/library/alt-SP800-30.pdf

المواقع الالكترونية:

1. AFRIPOL. Site officiel. Consulté le 30 Avril 2026. https://afripol.africa-union.org/fr

2. Kaspersky. "About Kaspersky." Accessed May 20, 2026. https://www.kaspersky.fr/about

3. Kapersky. "CYBERTHREAT LIVE MAP." Accessed April 27, 2026. https://cybermap.kaspersky.com/

الملاحق

ملحق رقم (1): دليل المقابلة

مقابلة مع إطار عن المصلحة الولائية للشرطة القضائية بأمن ولاية الجزائر بتاريخ 10 ماي 2026.

أسئلة المقابلة:

- **السؤال 1:**

ما هي أكثر أنواع الجرائم السيبرانية التي تعاملت معها مصالح أمن ولاية الجزائر خلال السنتين الأخيرتين (2024–2025)؟

- **السؤال 2:**

في إطار توزيع المهام، هل يقتصر نشاط المصلحة المركزية لمكافحة الجرائم السيبرانية على التهديدات التي تمس السيادة الرقمية والمؤسسات الحساسة، أم يمتد ليشمل الجرائم التي تمس المواطن العادي؟

- **السؤال 3:**

هل تم تسجيل قضايا تمس مؤسسات عمومية أو اقتصادية كان سببها اختراق ناتج عن خطأ بشري (مثل الوقوع في فخ الهندسة الاجتماعية)؟

- **السؤال 4:**

هل تواجهون صعوبات أو تحديات عند التعامل مع القضايا العابرة للحدود، خاصة فيما يتعلق بملاحقة المجرمين دوليًا؟

- **السؤال 5:**

هل يمكن تقديم إحصائيات سنوية حول القضايا المتعلقة بتكنولوجيات الإعلام والاتصال خلال السنتين 2024–2025؟

نتائج المقابلة:

- **السؤال 1:**

ما هي أكثر أنواع الجرائم السيبرانية التي تعاملت معها مصالح أمن ولاية الجزائر خلال السنتين الأخيرتين (2024–2025)؟

- **الجواب:**

تتمثل أبرز الجرائم السيبرانية المسجلة خلال هذه الفترة في جرائم القذف والتشهير عبر الإنترنت، إضافة إلى جرائم النصب والاحتيال الإلكتروني، والتي عرفت انتشارا ملحوظا.

- **السؤال 2:**

في إطار توزيع المهام، هل يقتصر نشاط المصلحة المركزية لمكافحة الجرائم السيبرانية على التهديدات التي تمس السيادة الرقمية والمؤسسات الحساسة، أم يمتد ليشمل الجرائم التي تمس المواطن العادي؟

- **الجواب:**

يشمل نشاط المصلحة كلا الجانبين معًا، حيث تتكفل بمعالجة التهديدات التي تستهدف السيادة الرقمية والمؤسسات الحساسة، كما تمتد مهامها لتشمل الجرائم السيبرانية التي تمس المواطنين العاديين.

- **السؤال 3:**

هل تم تسجيل قضايا تمس مؤسسات عمومية أو اقتصادية كان سببها اختراق ناتج عن خطأ بشري (مثل الوقوع في فخ الهندسة الاجتماعية)؟

- **الجواب:**

نعم، تم تسجيل مثل هذه الحالات، حيث إن العامل البشري يعد من أهم نقاط الضعف. كما تعمل المؤسسات حاليًا على تعزيز التكوين والتوعية لتقليل هذه المخاطر.

- **السؤال 4:**

هل يتم تكوين الموارد البشرية والخبراء العاملين في مجال الأمن السيبراني؟

- **الجواب:**

نعم، يتم تكوين الموارد البشرية والخبراء بشكل مستمر بهدف مواكبة التطورات التكنولوجية، خاصة ما يتعلق بتقنيات الذكاء الاصطناعي والأمن الرقمي.

- **السؤال5:**

هل تواجهون صعوبات أو تحديات عند التعامل مع القضايا العابرة للحدود، خاصة فيما يتعلق بملاحقة المجرمين دوليًا؟

- **الجواب:**

تتمثل أبرز الصعوبات في بطء الإجراءات عندما تغيب اتفاقيات التعاون الدولي، بينما يسير التعاون بشكل أفضل مع الدول التي تربطها بالجزائر اتفاقيات ثنائية، حيث يعتمد نجاح الملاحقة القضائية على مبدأ المعاملة بالمثل وتفعيل آليات التعاون القضائي الدولي، إضافة إلى تحديات تتعلق بتتبع الأثر الرقمي للمجرمين.

ملحق رقم (2): دليل المقابلة

مقابلة مع إطار عن المصلحة الولائية للشرطة القضائية بأمن ولاية الجزائر بتاريخ 10 ماي 2026.

- **السؤال(1) :**

هل يمكن تقديم إحصائيات سنوية حول القضايا المتعلقة بتكنولوجيات الإعلام والاتصال خلال السنتين 2024–2025؟

نتائج المقابلة

- **الجواب**

خلال سنة 2024 تم تسجيل 977 قضية أين تم معالجة 411 قضية وتوقيف 531 شخص تم إيداع 72 منه الحبس المؤقت.

نوع الجريمة	عدد القضايا المسجلة	عدد القضايا المعالجة
المساس وإلحاق الضرر بالأنظمة الآلية لمعالجة المعطيات	89	34
جرائم المساس بالأفراد عبر الانترنت	420	197
الشذوذ في الانترنت	04	04
استعمال الانترنت لأغراض لها علاقة بأفعال موصوفة بأفعال إرهابية	07	07
النصب عن طريق الانترنت	239	68
التحريض على الكراهية بين المواطنين والسكان	14	13
نشر محتويات ضد النظام العام عبر الانترنت	18	15
بيع سلع محظورة عبر الانترنت	10	06
جرائم انترنت اخرى	176	76

خلال سنة 2025 تم تسجيل 1701 قضية أين تم معالجة 674 قضية وتوقيف 765 شخص تم إيداع 141 منه الحبس المؤقت.

نوع الجريمة	عدد القضايا المسجلة	عدد القضايا المعالجة
المساس وإلحاق الضرر بالأنظمة الآلية لمعالجة المعطيات	72	27
جرائم المساس بالأفراد عبر الانترنت	616	239
الشذوذ في الانترنت	04	04
استعمال الانترنت لأغراض لها علاقة بأفعال موصوفة بأفعال إرهابية	04	04
النصب عن طريق الانترنت	441	144
التحريض على الكراهية بين المواطنين والسكان	37	12
نشر محتويات ضد النظام العام عبر الانترنت	61	47
بيع سلع محظورة عبر الانترنت	06	06
جرائم انترنت اخرى	460	192

ملحق رقم (3): دليل المقابلة

مقابلة مع إطار في وكالة الانباء الجزائرية بتاريخ 12 ماي 2026.

أسئلة المقابلة:

- **السؤال 1:**

ما هي طبيعة التهديدات السيبرانية التي تستهدف وكالة الأنباء الجزائرية؟

- **السؤال 2:**

كيف تؤمّن المؤسسات العمومية شبكاتها وبياناتها من الاختراقات الداخلية والخارجية؟

- **السؤال 3:**

هل تعود الاختراقات السيبرانية إلى أخطاء تقنية أم إلى أخطاء بشرية؟

- **السؤال 4:**

هل تعاني المؤسسات من نقص في الكفاءات في مجال الأمن السيبراني؟

نتائج المقابلة:

- **السؤال 1:**

ما هي طبيعة التهديدات السيبرانية التي تستهدف وكالة الأنباء الجزائرية؟

- **الجواب:**

تم تسجيل خلال شهر أفريل 2025 تعرض الموقع الإلكتروني لوكالة الأنباء الجزائرية لأربع هجمات من نوع حجب الخدمة الموزعة (DDoS) خلال أسبوع واحد، وهو ما يعكس تصاعد الهجمات الموجهة ضد المؤسسات الوطنية الحساسة. كما يتعرض البريد الإلكتروني المهني للمؤسسة يوميًا لأكثر من 500 محاولة هجوم إلكتروني يتم التصدي لها وحجبها عبر أنظمة الحماية، مما يبرز حجم التهديدات السيبرانية المتزايد.

- **السؤال2:**

كيف تؤمن المؤسسات العمومية شبكاتها وبياناتها من الاختراقات الداخلية والخارجية؟

- **الجواب:**

تعتمد المؤسسات العمومية على حلول تقنية متقدمة، مثل جدران الحماية (Firewalls) وأنظمة كشف ومنع التسلل(IDS/IPS) ، بهدف تأمين الشبكات الداخلية وحماية البيانات من التهديدات الداخلية والخارجية.

- **السؤال3:**

هل تعود الاختراقات السيبرانية إلى أخطاء تقنية أم بشرية؟

- **الجواب:**

يمثل العامل البشري ثغرة أمنية لا تقل خطورة عن الثغرات التقنية، حيث تعود نسبة كبيرة من الاختراقات (حوالي 70%) إلى أخطاء الموظفين الناتجة عن ضعف الوعي الرقمي أو الوقوع في فخ الهندسة الاجتماعية، مما يفرض ضرورة تعزيز التكوين والوعي السيبراني.

- **السؤال4:**

هل تعاني المؤسسات من نقص في الكفاءات في مجال الأمن السيبراني؟

- **الجواب:**

نعم، تعاني بعض المؤسسات من نقص في الكفاءات المتخصصة في مجال الأمن السيبراني، باعتبار أن هذا المجال حديث ويتطلب خبرات تقنية متقدمة وتكوينا مستمرا.

فهرس الجداول

الجدول	الصفحة
الجدول رقم (1): احصائيات القضايا المتصلة بتكنولوجيات الاعلام والاتصال المسجلة على المستوى الوطني خلال سنتين 2020-2021	**63**
الجدول رقم (2): احصائيات الجرائم السيبرانية في الجزائر خلال السنتين 2022-2023	**64**
الجدول رقم (3): احصائيات الجرائم السيبرانية المسجلة من طرف أمن ولاية الجزائر خلال السنتين 2024-2025	**65**

فهرس الأشكال

الشكل	الصفحة
الشكل رقم (1): الهيكل التنظيمي للمحافظة السامية للرقمنة	**58**
الشكل رقم (2): ترتيب الدول حسب نسبة التعرض للهجمات السيبرانية عالميا خلال الفترة الممتدة من 27 مارس الى27 أفريل2026	**61**
الشكل رقم (3): أبرز أنواع البرمجيات الخبيثة المكتشفة في الجزائر خلال الفترة الممتدة من 27 مارس الى27 أفريل 2026	**62**
الشكل رقم (4): كيف تتعامل المنظمات مع فجوة المهارات في المجال السيبراني	**85**

فهرس المحتويات

الاهداء

الشكر والعرفان

الملخص

مقدمة..... 1

الإطار المنهجي والنظري للدراسة..... 2

1. المشكلة البحثية 2

2. الفروض العلمية 3

3. مجالات الدراسة..... 3

4. الأهمية العلمية والعملية للدراسة: 4

5. أهداف الدراسة..... 4

6. أسباب اختيار الموضوع 5

7. مناهج الدراسة 6

8. الاقترابات المعتمدة 6

9. أدوات جمع البيانات..... 7

10. الدراسات السابقة 7

11.صعوبات الدراسة..... 8...

الفصل الأول: الإطار المفاهيمي والنظري للأمن السيبراني..... 10

المبحث الأول: مقاربة مفاهيمية للفضاء السيبراني والامن السيبراني 12

المطلب الأول: مفهوم السيبرانية، الفضاء السيبراني والامن السيبراني 12

الفرع الأول: تعريف السيبرانية 12

الفرع الثاني: تعريف الفضاء السيبراني 13

الفرع الثالث: تعريف الامن السيبراني 14

المطلب الثاني: الفواعل في الفضاء السيبراني 17

الفرع الأول: الفواعل الدولاتية 17

الفرع الثاني: الفواعل الغير الدولاتية 17

1. المنظمات الغير حكومية 17

2.الشركات المتعددة الجنسيات 18

3. الجماعات الإرهابية 18

الفرع الثالث: الأفراد 18

المطلب الثالث: ابعاد الأمن السيبراني.....19

1. البعد العسكري 19

2. البعد الاقتصادي 19

3. البعد الاجتماعي 19

4. البعد السياسي..... 19

5. البعد القانوني 20

المبحث الثاني: التهديدات الأمنية السيبرانية..... 21

المطلب الأول: مفهوم التهديد السيبراني..... 21

المطلب الثاني: أساليب تنفيذ الهجمات السيبرانية 21

1. هجمات التصيد Phishing 22
2. هجمات وقف الخدمة DDOS 22
3.البرمجيات الخبيثة 22
4.الهندسة الاجتماعية 23
المطلب الثالث: أشكال التهديدات السيبرانية 23
الفرع الأول: التجسس السيبراني 23
الفرع الثاني: الجريمة السيبرانية 24
الفرع الثالث: الإرهاب السيبراني 24
الفرع الرابع: الحرب السيبرانية 25
المبحث الثالث: استراتيجيات الدول الرائدة للأمن السيبراني 27
المطلب الأول: الإستراتيجية الصينية للأمن السيبراني 27
المطلب الثاني: الإستراتيجية الامريكية للأمن السيبراني 29
المطلب الثالث: الاستراتيجية الروسية للأمن السيبراني 31
الفصل الثاني: آليات مواجهة التهديدات السيبرانية في الجزائر 34
المبحث الأول: الإطار القانوني والمؤسساتي للأمن السيبراني في الجزائر 36
المطلب الأول: الإطار القانوني والتنظيمي للفضاء الرقمي في الجزائر 36
الفرع الأول: التكريس الدستوري لحماية الفضاء الرقمي والبيانات 36
1. دستور1996 36
2. دستور2016 36
3. دستور 2020 37
الفرع الثاني: الترسانة القانونية المنظمة للمجال السيبراني 37
1.مكافحة الجرائم المعلوماتية 38

2.التوقيع والتصديق الإلكتروني 38
3.الاتصالات والتجارة الإلكترونية 40
4. حماية المعطيات الشخصية 41
5. حماية المعطيات في المؤسسات والإدارات والهيئات العمومية 42
الفرع الثالث: الآليات الجنائية وتقنيات التحري الخاصة 43
1. قانون العقوبات (تعديل 04-15) 43
2. قانون الإجراءات الجزائية 44
المطلب الثاني: الهيئات المسؤولة عن الأمن السيبراني في الجزائر 45
الفرع الأول: وكالة أمن الأنظمة المعلوماتية ASSI..... 45
1. المجلس وطني لأمن الأنظمة المعلوماتية 46
2.وكالة أمن الأنظمة المعلوماتية 47
الفرع الثاني: الهيئات التابعة لوزارة الدفاع الوطني 49
1.المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني 49
2. مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية للدرك الوطني 50
الفرع الثالث: المصلحة المركزية لمكافحة الجرائم السيبرانية 52
الفرع الرابع: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 52
الفرع الخامس: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي 53
الفرع السادس: المحافظة السامية للرقمنة 56
الفرع السابع: المرجع الوطني لأمن نظم المعلومات (RNSI) 58
المبحث الثالث: تأثير التهديدات السيبرانية على الأمن الوطني الجزائري 60
المطلب الأول: أشكال التهديدات السيبرانية التي تواجه الجزائر 60
الفرع الأول: احصائيات شركة كاسبرسكي 60
الفرع الثاني: احصائيات الجرائم السيبرانية في الجزائر من سنة 2020 الى سنة 2025 63

1. احصائيات الجرائم السيبرانية خلال سنتين 2020-2021 63
2. احصائيات الجرائم السيبرانية خلال السنتين 2022-2023 64
3. احصائيات الجرائم السيبرانية خلال السنتين 2024-2025 64
المطلب الثاني: تداعيات التهديدات الأمنية السيبرانية على الجزائر 69
المبحث الثالث: محاور الاستراتيجية الوطنية الجزائرية لمواجهة التهديدات السيبرانية..... 71
المطلب الأول: حماية البنى التحتية الحيوية 71
المطلب الثاني: التكوين والتحسيس في المجال السيبراني..... 73
الفرع الأول: التكوين في المجال السيبراني. 73
الفرع الثاني: التحسيس في المجال السيبراني 75
المطلب الثالث: التعاون الوطني والدولي في المجال السيبراني. 79
الفرع الأول: التعاون الوطني 79
الفرع الثاني: التعاون الدولي 79
الفصل الثالث: تحديات ورهانات مواجهة التهديدات السيبرانية في الجزائر 80
المبحث الأول: التحديات التي تواجه الاستراتيجية الوطنية للأمن السيبراني..... 83
المطلب الأول :التحديات التقنية والتكنولوجية..... 84
المطلب الثاني :التحديات البشرية والتكوينية..... 86
المطلب الثالث :التحديات القانونية والتنظيمية..... 88
الفرع الأول: تحدي البيئة التشريعية الداخلية 89
الفرع الثاني: تحديات الملاحقة الدولية والسيادة الرقمية 89
المبحث الثاني: الرهانات المستقبلية لتعزيز الأمن السيبراني في الجزائر 90
المطلب الأول: السيادة الرقمية وحماية المعطيات..... 90

1. توطين البيانات والبنية التحتية: 90
2. الاستقلالية التكنولوجية 90
3. حماية الخصوصية 90
4. الهوية الرقمية الوطنية 90
المطلب الثاني: الأمن السيبراني كشرط للتنمية الاقتصادية والتحول الرقمي 91
1.تحصين الاقتصاد الرقمي 91
2. أمن المعاملات المالية 91
3. حماية البنى التحتية الحساسة 91
4.جذب الاستثمارات 91
5. دعم المؤسسات الناشئة 91
المطلب الثالث: تموقع الجزائر في الحوكمة السيبرانية الدولية 92
1. تصدير الخدمات الرقمية 92
2.المساهمة في التشريع الدولي 92
3.تأطير التعاون الدولي 92
4.الحفاظ على الكفاءات 92
الخاتمة 94
قائمة المراجع 97
الملاحق 106
فهرس الجداول 112
فهرس الأشكال 113
فهرس المحتويات 114