وزارة التعليم العالي والبحث العلمي

جامعة عباس لغرور خنشلة

كلية الحقوق والعلوم السياسية

قسم: العلوم السياسية

الأمن السيبراني في الحرب الروسية الأوكرانية وانعكاساته على الفكر الاستراتيجي الجزائري 2014-2025

مذكرة مكملة لنيل شهادة الماستر في شعبة: العلوم السياسية

تخصص: دراسات إستراتيجية وأمنية

إعداد الطالبة:

روميسة بن عبيد

إشراف الدكتورة:

هاجر خلالفة

أعضاء لجنة المناقشة:

الأستاذ	الدرجة العلمية	الصفة
مريم بوشيربي	أستاذ التعليم العالي	رئيسة
هاجر خلالفة	أستاذة محاضرة "أ"	مُشرفة ومُقررة
ريمة كاية	أستاذ مساعد "أ"	عضوًا ممتحنًا

السنة الجامعية:2026/2025

شكر و عرفان

الحمد لله الذي أمدَّني بالعزم ووفَّقني لإتمام هذا العمل، فله سبحانه الحمد والفضل في البداية والختام.

أتقدَّم بخالص عبارات الشكر والتقدير إلى الأستاذة المُشرفة **هاجر خلالفة** تقديرًا لإشرافها العلمي ومتابعتها الجادة، وما قدَّمته من توجيهات ومُلاحظات قيمة أسهمت في توجيه هذا العمل وإثرائه.

كما أتوجَّه بجزيل الشكر للسادة أعضاء لجنة المناقشة، الذين شرفوني بقبول قراءة هذا العمل ومناقشته. وعلى ما أسدوه من نصائح وتوجيهات علمية قيمة.

كما أتقدَّم بخالص الإمتنان لجميع أساتذتي الكرام: لما قدَّموه من علم وتوجيه ونصائح قيمة رافقت مساري العلمي طيلة سنوات الدراسة.

الحمد لله ربِّ العالمين

إهداء

إلى روحي التي غادرت هذا العالم، **جدّي الحبيب**، كان حُلمي أن أراك فرحًا بِتخرُّجي، فإليك أُهدي هذه اللحظة التي كانت ستملأ قلبك بالفخر والابتسامة.

إلى أبي، سندي الأول وملاذي الأبدي، الذي غمر حياتي بحبه ودعمه اللامحدود، فلولاك لما كُنت ما أنا عليه اليوم... كلمات الشُّكر تعجز عن ردِّ جُزءٍ من فضلك، وقلبي لا يعرف سوى الإمتنان العميق لك في كلِّ لحظة.

إلى أمي، دعواتُكِ كانت نجاةً لي في كل امتحان، وحنانُكِ سندٌ أحتضنُ به كلِّ خُطوة، فكُلُّ نجاحٍ يحمل بصمتكِ الطيّبة وروحُكِ الحانية

إلى أخي الوحيد عبد المجيب، دعَمتنِي بِصمتِكَ، وقلبي يعلمُ كم تمنَّيتَ لي الخير في الخفاء.

إلى أختي أُلفت، توأم روحي، التي جعلت فرحتي جزءًا من فرحتها، شُكرًا لأنَّكِ دائمًا معي.

إلى شقيقاتي الغاليَّات، جميلات الروح، لكلِّ واحدة منكُنَّ أُهدي هذا النجاح.

إلى كلِّ قريبٍ وبعيد، تمنَّى لي الخير وشاركَ فرحتي، أُهديكم ثمرة هذا العمل المُتواضع، لَعسى أن يكون لكم كما كُنتم لي: أملاً وسعادة.

الملخص:

يعتبر الأمن السيبراني أداة استراتيجية في الحرب الروسية–الأوكرانية، بالنظر إلى تحول الفضاء الرقمي إلى مسرح رئيسي للصراعات الدولية المعاصرة؛ فقد برزت الهجمات السيبرانية كعنصر محوري في الحروب الهجينة لقدرتها العالية على تجاوز الحدود الجغرافية التقليدية وإحداث أثر استراتيجي عابر للقارات. وقد استغلت روسيا هذا السلاح لتعطيل البنى التحتية والتأثير على مراكز صنع القرار، مما أفرز تداعيات أمنية لم تتوقف عند مسرح العمليات الأوروبي، بل امتدت لتلقي بظلالها على المنطلقات الدفاعية للدول الإقليمية كالجزائر. بناء على ذلك، فرضت الحرب ضرورة مراجعة الفكر الاستراتيجي الجزائري وتطوير أطره التشريعية والمؤسساتية لمواجهة هذا النمط من التهديدات العابرة للحدود. وفي هذا السياق، سعت الدراسة إلى استشراف مستقبل السيادة الرقمية الوطنية في أفق 2025، سعيا لضمان بناء عقيدة أمنية استباقية قادرة على مواكبة المخاطر السيبرانية المتجاوزة للحدود الوطنية.

Abstract

Cybersecurity considered as a strategic tool in the Russian-Ukrainian war focusing on the transformation of cyberspace into a primary arena for contemporary international conflicts. Cyberattacks have emerged as a pivotal element in hybrid warfare due to their significant ability to transcend traditional geographical boundaries and create a transcontinental strategic impact. Russia has leveraged this weapon to disrupt critical infrastructure and influence decision-making centers resulting in security repercussions that extended far beyond the European theater to affect the defensive principles of regional states like Algeria. Consequently this war necessitated a review of Algerian strategic thought and the development of its legislative and institutional frameworks to counter such threats. In this context the study seeks to foresee the future of national digital sovereignty by 2025 aiming to establish a proactive security doctrine capable of keeping pace with cyber threats that bypass national borders.

خطة الدراسة:

مقدمة

الفصل الأول: الإطار المفاهيمي والنظري للأمن السيبراني والفكر الاستراتيجي

المبحث الأول: مفهوم الأمن السيبراني

المطلب الأول: نشأة وتعريف الأمن السيبراني

المطلب الثاني: المفاهيم ذات الصلة بالأمن السيبراني

المطلب الثالث: أبعاد الأمن السيبراني

المبحث الثاني: مفهوم الفكر الاستراتيجي

المطلب الأول: تطور وتعريف الفكر الاستراتيجي

المطلب الثاني: أهمية الفكر الاستراتيجي في حقل الدراسات الأمنية

المطلب الثالث: الأمن السيبراني كمتغيّر بنيوي في إعادة تشكيل الفكر الاستراتيجي المعاصر

المبحث الثالث: الإطار النظري المفسر للعلاقة بين الأمن السيبراني والفكر الاستراتيجي

المطلب الأول: النظرية الواقعية الجديدة

المطلب الثاني: النظرية الليبيرالية المؤسساتية

المطلب الثالث: النظريات الجيوبوليتيكية

الفصل الثاني: التهديدات السيبرانية في الحرب الروسية – الأوكرانية 2025/2014

المبحث الأول: دراسة جيوبوليتيكية لمسار الحرب الروسية – الأوكرانية 2025/2014

المطلب الأول: مراحل تطور الحرب الروسية – الأوكرانية2014 –2025

المطلب الثاني: أسباب الحرب الروسية – الأوكرانية 2014–2025

المطلب الثالث: الآثار المرحلية للحرب الروسية – الأوكرانية على الدولتين المتنازعتين

المبحث الثاني: الاستراتيجيات السيبرانية المُتبعة في الحرب الروسية– الأوكرانية

المطلب الأول: الاستراتيجية الروسية في الفضاء السيبراني

المطلب الثاني: الاستراتيجية الأوكرانية في الفضاء السيبراني

المبحث الثالث: انعكاسات الحرب السيبرانية الروسية – الأوكرانية على الأمن الإقليمي الأوروبي

المطلب الأول: انعكاسات الحرب على المجال العسكري والسياسي

المطلب الثاني: انعكاسات الحرب على المجال الاقتصادي والاجتماعي

الفصل الثالث: الفكر الاستراتيجي الجزائري في ظل الحرب الروسية – الأوكرانية

المبحث الأول: واقع الأمن السيبراني في الجزائر

المطلب الأول: الإطار التشريعي والمؤسساتي للأمن السيبراني في الجزائر

المطلب الثاني: السياسات والبرامج الجزائرية في حماية البنى التحتية الحساسة

المبحث الثاني: تأثيرات الحرب الروسية – الأوكرانية على التحولات في الفكر الاستراتيجي الجزائري

المطلب الأول: إدراج التهديدات السيبرانية في المقاربة الاستراتيجية للدولة الجزائرية

مقدمة:

يعد الفضاء السيبراني في الوقت الراهن البعد الخامس للمواجهة في الحروب الحديثة؛ حيث تزايدت أهميته الجيوسياسية لتضاهي أبعاد البر، البحر، الجو، والفضاء. مع تداخل الأبعاد التقنية العالية بكيان الدولة وبقائها، جعل من مفهوم الأمن القومي لا يقتصر على حماية الحدود الجغرافية المادية، بل امتد ليشمل السيادة الرقمية وتأمين النظم المعلوماتية التي باتت تشكل العصب الحيوي للاقتصاد والإدارة والدفاع. إن هذا التحول البنيوي في طبيعة القوة الدولية أدى إلى ظهور نمط جديد من الصراعات التي لا تعترف بالحدود التقليدية؛ حيث أصبحت الهجمات السيبرانية أداة فعالة لتحقيق مكاسب استراتيجية كبرى بأقل التكاليف وبأعلى درجات التخفي.

على الصعيد العالمي، لم تعد قضايا الأمن السيبراني مجرد تحديات تقنية معزولة، بل أضحت تشكل جوهر "الحروب الهجينة" التي تدمج بين القوة الصلبة والأسلحة الرقمية لتعطيل البنى التحتية، تشكيل الرأي العام، والتأثير على مراكز صنع القرار. ومن هذا المنطلق، يظهر أن استقرار الدول في العصر الرقمي بات مرتبطا بقدرتها على مواكبة الثورة التكنولوجية وتطوير استراتيجيات دفاعية مرنة، إذ أن التفاوت في القدرات السيبرانية بين الدول أوجد "فجوة أمنية" تدفع القوى الكبرى والمنافسين الإقليميين إلى التنافس الحاد لفرض السيطرة على الفضاء المعلوماتي وتوظيفه كأداة للردع أو الهجوم.

هذا النزاع أعاد تعريف مفاهيم "الأمن والسيادة"؛ حيث استخدمت موسكو ورقة التفوق السيبراني كجزء من عقيدتها في "حرب المعلومات" لزعزعة استقرار الخصم وإرباك تحالفاته الدولية، وهو ما كشف عن هشاشة النظام الأمني التقليدي أمام التهديدات السيبرانية المتقدمة.

في هذا السياق، تبرز ضرورة قراءة هذه التحولات الدولية من منظور الفكر الاستراتيجي الجزائري؛ إذ أن الجزائر بموقعها الجيوسياسي المحوري وتوجهها نحو الرقمنة الشاملة، ليست

بمعزل عن هذه الارتدادات الرقمية العابرة للقارات، إذ أن دروس الحرب الروسية–الأوكرانية تفرض على صانع القرار الاستراتيجي في الجزائر إعادة تقييم التهديدات غير التقليدية، وتحصين الأمن القومي وفق رؤية استشرافية.

التعريف بالموضوع:

تدور هذه الدراسة حول تحليل العلاقة بين "الأمن السيبراني" كمتغير مستقل و"الفكر الاستراتيجي" كمتغير تابع، في ظل الحرب الروسية–الأوكرانية. تكمن العلاقة في أن هذا الصراع لم يستخدم الفضاء الرقمي كأداة ثانوية، وتسعى الدراسة إلى تحليل الكيفية التي استغلت بها القوى المتنافسة نقاط الضعف الرقمية لتعزيز نفوذها، الأمر الذي أفرز بيئة أمنية جديدة تفرض على الجزائر ضرورة إعادة تكييف عقيدتها الدفاعية وتحديث أطرها التشريعية، بما يضمن القدرة على مواجهة هذا الشكل المتطور من الحروب الهجينة.

أسباب اختيار الموضوع:

تتعدد الأسباب الكامنة وراء اختيار هذا، ويمكن حصرها في:

الأسباب الموضوعية:

- حداثة الإشكالية وأبعادها الجيوسياسية؛ حيث لم يعد الصراع عسكريا بحتا بل امتد للفضاء السيبراني، وهو ما يتجسد بوضوح في النزاع الروسي–الأوكراني.
- ندرة الدراسات الأكاديمية الجزائرية خاصة التي تربط بشكل منهجي بين التكتيكات السيبرانية الحديثة وبين انعكاساتها على العقيدة الأمنية للدول البعيدة عن مسرح الصراع المباشر.
- محاولة فهم كيف ساهمت هذه الحرب في إعادة صياغة المفاهيم الاستراتيجية الكبرى، وتأثير ذلك على موازين القوى الرقمية عالميا.

الأسباب الذاتية:

- الرغبة في التعمق في تخصص الدراسات الأمنية والاستراتيجية، ومواكبة التطورات المتسارعة في هذا الحقل المعرفي.
- التطلع لاستكشاف الفكر الاستراتيجي الروسي وكيفية توظيفه للأدوات غير التقليدية في إدارة الصراعات الحديثة.
- الالتزام بمحاولة استخلاص دروس مستفادة يمكن أن تساهم في إثراء الفكر الاستراتيجي الجزائري، وتعزيز الوعي بضرورة تحصين الأمن القومي الرقمي بناء على المعطيات الدولية الراهنة.

أهمية الموضوع:

تكمن أهمية الموضوع هذا الموضوع في قيمتين أساسيتين:

-**القيمة العلمية:** يساعد هذا الموضوع على توسيع الفهم حول مكانة الأمن السيبراني في العلاقات الدولية، خاصة في ظل التحولات التي يشهدها العالم اليوم. كما يساهم في توضيح كيف أصبح الفضاء الرقمي مجالا مهما في الصراعات الحديثة، ودوره في التأثير على مفاهيم مثل السيادة والردع. وهذا من شأنه أن يدعم الجانب النظري للدراسات الأمنية ويمنح رؤية أوضح لطبيعة التهديدات الجديدة.

-**القيمة العملية:** تكمن أهمية الموضوع عمليا في ارتباطه بالواقع الأمني، خاصة بالنسبة للجزائر؛ حيث يبرز ضرورة الانتباه إلى التهديدات السيبرانية المتزايدة. كما يساهم في لفت الانتباه إلى أهمية تطوير السياسات الدفاعية وتعزيز الحماية الرقمية، بما يساعد على مواجهة التحديات الحديثة والحفاظ على الأمن الوطني في ظل التغيرات المتسارعة.

أهداف الدراسة:

تهدف هذه الدراسة إلى تقديم تحليل معمق للأمن السيبراني كأداة نفوذ استراتيجي خلال الحرب الروسية–الأوكرانية؛ حيث تم التركيز على تتبع الآليات التي اعتمدتها موسكو لتحقيق أهدافها الجيوسياسية وتقييم مدى فاعلية هذه السياسات في التأثير على توازن القوى الرقمي. كما تسعى لاستكشاف ردود الفعل الدولية تجاه هذا النمط من الحروب، مع تسليط الضوء بشكل أساسي على كيفية انعكاس هذه الدروس الميدانية على الفكر الاستراتيجي الجزائري؛ حيث تهدف الدراسة إلى تحديد الفجوات القائمة في المنظومة الدفاعية الوطنية واقتراح سبل لتعزيز السيادة الرقمية.

إشكالية الدراسة:

يتصاعد الجدل حول الدور الذي تلعبه القوة السيبرانية كأداة تأثير رئيسية في السياسة الدولية، كما ظهر ذلك جليا في الحرب بين روسيا وأوكرانيا 2014–2025. فمن خلال توظيف الهجمات الرقمية لتعطيل المؤسسات الحيوية، استخدمت هذه الوسائل كأداة ضغط استراتيجي غير مسبوقة تمتد لتلقي ظلالها على العقائد الأمنية للدول الفاعلة إقليميا كالجزائر التي بات فكرها الاستراتيجي أمام حتمية مواكبة هذه التحولات. ومن هذا المنطلق تبرز الإشكالية التالية:

كيف تأثر الفكر الاستراتيجي الجزائري بتوظيف الأمن السيبراني في الحرب الروسية–الأوكرانية 2014–2025؟

الأسئلة الفرعية:

تندرج تحت الإشكالية الأسئلة الفرعية التالية:

1. فيما يتمثل الإطار المفاهيمي والنظري للأمن السيبراني والفكر الاستراتيجي؟

2. ما ملامح بروز الأمن السيبراني في الحرب الروسية–الأوكرانية 2014–2025؟
3. ماهي الخطوات التي حققها الفكر الاستراتيجي الجزائري في مجال الأمن السيبراني؟
4.

الفرضيات:

للإجابة عن إشكالية الدراسة والأسئلة الفرعية، تم صياغة الفرضيات التالية لتكون منطلقات للتحليل:

1. يسهم توظيف البعد السيبراني في الحرب الروسية–الأوكرانية إلى إحداث تغييرات في ديناميات الصراع لتشمل الفضاء الرقمي.
2. إدماج البعد الرقمي ضمن المنظومة الدفاعية يزيد من تحكم الجزائر في مجال الأمن السيبراني.

حدود الدراسة:

تم تحديد الإطار الزماني والمكاني للدراسة كالتالي:

الحدود الزمانية: تمتد الدراسة خلال الفترة الزمنية من سنة 2014 إلى غاية سنة 2025؛ حيث تم اختيار سنة 2014 لارتباطها ببداية التصعيد في الأزمة الروسية–الأوكرانية، وما رافق ذلك من بروز متزايد لاستخدام الفضاء السيبراني كأداة للصراع. كما تم اعتماد سنة 2025 كحد زمني أخير لكونها تمثل مرحلة حديثة تعكس تطور التهديدات السيبرانية وتنامي دورها في الحروب المعاصرة.

الحدود المكانية: تتناول الدراسة في بعدها المكاني نطاقين أساسيين؛ يتمثل الأول في البيئة الدولية المرتبطة بالحرب الروسية–الأوكرانية باعتبارها مجالا لتجليات الصراع السيبراني،

بينما يتمثل الثاني في الجزائر، من خلال التركيز على انعكاسات هذه التطورات على الفكر الاستراتيجي الجزائري، دون التوسع في مناطق أخرى إلا بالقدر الذي يخدم تحليل الموضوع.

المقاربة المنهجية:

تقتضي طبيعة الدراسة اعتماد تكامل منهجي يجمع بين عدة مناهج علمية للإحاطة بجميع أبعاد الظاهرة السيبرانية وتأثيراتها العابرة للحدود؛ حيث تم الاعتماد على توليفة منهجية تتناسب مع المتغيرات المستقلة والتابعة لموضوع البحث، وذلك وفق التفصيل الآتي:

-**المنهج التاريخي:** يبرز استخدام المنهج التاريخي في هذه الدراسة من خلال تتبع تطور الحرب بين روسيا وأوكرانيا عبر مراحلها المختلفة، انطلاقا من سنة 2014 التي شكلت نقطة تحول في طبيعة العلاقات بين الطرفين، وصولا إلى التطورات الحديثة. إذ يتضح أن هذا المنهج يستخدم عبر رصد أهم الأحداث التي طبعت هذا النزاع، مع محاولة فهم السياقات التي ظهرت فيها، بدل الاكتفاء بسردها فقط.

- **منهج دراسة حالة:** استخدم هذا المنهج بتركيز عال على الدولة الجزائرية باعتبارها الحالة المعنية باختبار ارتدادات التجربة السيبرانية الروسية-الأوكرانية. ومن خلاله، تم اسقاط الدروس المستخلصة من الحرب على الواقع الاستراتيجي الجزائري لتحليل مدى تأثر المنظومة الأمنية الوطنية بهذه الحرب العابرة للحدود وكيفية تكييف الدفاع السيبراني الجزائري مع هذه المعطيات الجديدة.

-**نظرية الدور**: تم توظيف نظرية الدور في هذه الدراسة لتحليل طبيعة الأدوار التي مارستها كل من روسيا وأوكرانيا داخل الفضاء السيبراني خلال فترة الحرب، من خلال إبراز كيفية استخدام القدرات الرقمية كأداة للتأثير وتحقيق الأهداف الاستراتيجية. كما ساهمت هذه النظرية في تفسير توجه الجزائر نحو تعزيز حضورها في المجال السيبراني وإعادة صياغة تصوراتها

الأمنية بما يتماشى مع التحولات التي فرضتها التهديدات الإلكترونية المعاصرة وانعكاساتها على الفكر الاستراتيجي الوطني.

-**نظرية المباريات:** اعتمدت الدراسة على نظرية المباريات باعتبارها أداة تحليلية لفهم طبيعة التفاعلات الاستراتيجية بين أطراف الحرب الروسية-الأوكرانية في المجال السيبراني، من خلال دراسة القرارات المتبادلة المرتبطة بالهجوم والدفاع وتحقيق التوازن الاستراتيجي. كما ساهمت في تحليل كيفية استيعاب الجزائر لهذه التحولات ضمن مقاربتها الأمنية الجديدة، خاصة فيما يتعلق بتطوير آليات التوقع والاستجابة للتهديدات السيبرانية في إطار تحديث الفكر الاستراتيجي الجزائري.

أدبيات الدراسة:

تظهر مراجعة الأدبيات الأمنية والاستراتيجية التي قاربت موضوع الأمن السيبراني في الحرب الروسية-الأوكرانية وجود تباين في زوايا المعالجة؛ حيث يمكن حصر أبرزها في مجموعة من الدراسات التي شكلت إطارا معرفيا للموضوع. ومن ذلك دراسة "ريتشارد كلارك وروبرت كناكي" في كتابهما المعنون بـ cyber War The Next Threat to National Security and What to Do About it الصادر باللغة الإنجليزية سنة 2022؛ حيث حلل المؤلفان كيف تحول الفضاء الرقمي إلى ساحة حرب حقيقية من خلال استعراض القدرات السيبرانية الروسية والأوكرانية كنموذج للمواجهة بين القوى الكبرى، مع التركيز على استراتيجيات الدفاع عن البنى التحتية الحيوية. وبالرغم من عمق هذه الدراسة، إلا أنها ركزت على المنظور الأمريكي والغربي في تقييم التهديد واكتفت بالتحليل التقني والعسكري؛ حيث أغفلت انعكاس هذه الحرب على العقائد الأمنية للدول الإقليمية كالجزائر، وهو ما سيعالجه البحث الحالي بربط هذه التحولات بخصوصية الفكر الاستراتيجي الجزائري.

في سياق متصل، تناول "دانيال بيرغين" في كتابه " The New Map Energy Climate and the Clash of Nations" الصادر باللغة الإنجليزية سنة 2023 الذي يتناول الجيوسياسية السيبرانية في الحرب الروسية–الأوكرانية؛ حيث بين كيف تم دمج الهجمات الرقمية مع سلاح الطاقة لزعزعة استقرار الخصوم وتغيير موازين القوى الدولية. ورغم القيمة الجيوسياسية لهذا الطرح، إلا أن الباحث ركز على أمن الطاقة وتوازن القوى العالمي؛ حيث تجاهل الكيفية التي أدت بها هذه الحرب السيبرانية الهجينة إلى إعادة صياغة الفكر الدفاعي وتطوير الأطر المؤسساتية الرقمية وتحديدا في الجزائر للفترة 2014–2025، وهو الفراغ الذي تسعى هذه الدراسة لدراسته بعمق.

أما على مستوى الدراسات الوطنية، تبرز دراسة الدكتور عبد الكريم بن خالد بعنوان "الأمن السيبراني في الجزائر" قراءة في ASJP المنشورة على منصة الأطر القانونية والمؤسساتية المستحدثة، باللغة العربية؛ حيث استعرض المقال التطور التشريعي في الجزائر بدءا من دستور 2022 والقوانين المتعلقة بحماية المعطيات والوكالة الوطنية لأمن النظم المعلوماتية لبيان جاهزية الدولة قانونيا لمواجهة الجرائم السيبرانية.

غير أن هذه الدراسة ظلت ذات صيغة قانونية وصفية بحتة؛ حيث لم تربط بين الإصلاحات التشريعية والدروس الميدانية المستقاة من الحرب الروسية–الأوكرانية، كما لم تحلل التحول في لعقيدة العسكرية الجزائرية من الدفاع التقليدي إلى الدفاع السيبراني الاستباقي، وهو الفراغ المعرفي الذي تدعي دراستنا الحالية ملأه.

وعليه، فإن دراستنا الحالية تختلف عن الدراسات السابقة في كونها تحاول تجاوز الوصف التقني أو القانوني المجرد، لتغوص في تحليل "الأثر الارتدادي" لصراع دولي بين روسيا وأوكرانيا على بنية الفكر الاستراتيجي الجزائري؛ حيث يتم استشراف آفاق عام 2025 كحلقة مفصلية في بناء السيادة الرقمية الوطنية.

صعوبات الدراسة:

واجهت الدراسة عدة عقبات موضوعية ومنهجية تطلبت جهدا مضاعفا لتجاوزها؛ حيث تبرز في مقدمتها قلة المصادر والمراجع الأكاديمية الحديثة باللغة العربية التي تعالج الأمن السيبراني من منظور استراتيجي صرف، مما حتم الاعتماد المكثف على التقارير والمراجع الأجنبية.

كما شكلت طبيعة الموضوع المتغيرة بسرعة نتيجة تطورات الحرب الروسية–الأوكرانية تحديا كبيرا؛ حيث أن تسارع الهجمات السيبرانية وتطور الأدوات التقنية يجعل من عملية الإحاطة بكل المعطيات في وقتها الزمني أمرا معقدا. إضافة إلى ذلك واجه البحث صعوبة في الوصول إلى بعض الوثائق الرسمية والبيانات الدقيقة المتعلقة بالقدرات الدفاعية السيبرانية الوطنية نظرا لطابع السرية الذي يغلف الأمن القومي؛ حيث تم تعويض هذا النقص بتحليل التشريعات المعلنة والخطابات الرسمية.

تبرير خطة الدراسة:

جاءت خطة الدراسة موزعة على ثلاثة فصول، اعتمدت منطقا تصاعديا يبدأ من التأصيل الآفاق المستقبلية لضمان معالجة الإشكالية بشكل متدرج يراعي تعقيد الظاهرة السيبرانية وتعدد أبعادها.

الفصل الأول؛ والذي قسم إلى ثلاث مباحث كل مبحث يحتوي على ثلاث مطالب، تم تخصيص هذا الفصل كمنطلق أساسي للدراسة؛ حيث أن الضرورة المنهجية تقتضي أولا ضبط المفاهيم وتحديد الأطر النظرية المفسرة للظاهرة السيبرانية. والعلة من هذا التقسيم هي بناء قاعدة معرفية تسمح بالانتقال من الوصف التقني للهجمات السيبرانية إلى تحليلها كفعل استراتيجي ضمن حقل الدراسات الأمنية، من خلال الربط بين الأمن السيبراني والفكر

الاستراتيجي بأدوات تحليلية كالواقعية البنيوية، الليبيرالية المؤسساتية والنظريات الجيوبوليتيكية لتفسير دوافع الدول وتوجهاتها في الفضاء الرقمي.

الفصل الثاني يمثل الجانب التطبيقي للدراسة، قسم إلى ثلاث مباحث متفاوتة من مطلبين إلى ثلاث مطالب داخل كل مبحث؛ تم اختياره لتحليل كيفية تحول العقائد العسكرية التقليدية إلى حروب هجينة تستخدم الفضاء السيبراني كمسرح رئيسي للعمليات. والهدف من تقسيم عناصر هذا الفصل تتبع مسار الحرب وتحليل الاستراتيجيات بين الطرفين روسيا وأوكرانيا ميدانيا، بما يسمح برصد الانعكاسات الفعلية للحرب على الأمن الإقليمي والدولي.

الفصل الثالث يعد الغاية الاستراتيجية والوطنية للبحث، تم تخصيصه لتقييم مدى تأثر المنظومة الأمنية الجزائرية بالتحولات الرقمية العابرة للحدود. من خلال إجراء دراسة مسحية للأطر التشريعية والبرامج الوطنية لحماية المنشآت الحيوية في الجزائر، عبر تشخيص واقع الأمن السيبراني الوطني بناء على الدروس المستقاة من الحرب الروسية–الأوكرانية، وصولا إلى رسم رؤية استشرافية لأفق عام 2025.

الفصل الأول:

الإطار المفاهيمي والنظري للأمن السيبراني والفكر الاستراتيجي

الفصل الأول: الإطار المفاهيمي والنظري للأمن السيبراني والفكر الاستراتيجي

يعتبر الأمن السيبراني من القضايا الإستراتيجية المعاصرة التي ارتبطت بالاعتماد على الفضاء الرقمي في إدارة شؤون الدول والمجتمعات، مما جعله بعدا أساسيا من أبعاد الأمن القومي. وفي هذا الإطار يبرز الفكر الاستراتيجي كمرجعية تحليلية لفهم طبيعة التهديدات السيبرانية وآليات التعامل معها، لذلك يهدف هذا الفصل إلى ضبط المفاهيم الأساسية وتبيان الأسس النظرية التي تحكم العلاقة بين الأمن السيبراني والفكر الاستراتيجي.

يتناول هذا الفصل الموسوم ب "الإطار المفاهيمي والنظري للأمن السيبراني والفكر الاستراتيجي" ثلاثة مباحث رئيسية؛ خصص المبحث الأول لضبط مفهوم الأمن السيبراني من خلال التطرق إلى تعريفه، نشأته، أبعاده، وأهم المفاهيم ذات الصلة. أما المبحث الثاني فيعالج مفهوم الفكر الاستراتيجي عبر تبيان تعريفه، تطوره، أهميته في حقل الدراسات الأمنية، إضافة إلى ابراز الأمن السيبراني كمتغير بنيوي أسهم في إعادة تشكيل الفكر الاستراتيجي المعاصر. في حين يركز المبحث الثالث على الإطار النظري المفسر للعلاقة بين الأمن السيبراني والفكر الاستراتيجي، من خلال عرض أهم المقاربات النظرية المتمثلة في: النظرية الواقعية الجديدة، الليبيرالية المؤسساتية، إلى جانب النظريات الجيوبوليتيكية.

المبحث الأول: مفهوم الأمن السيبراني

يعد الأمن السيبراني مفهوما حديثا في حقل الدراسات الأمنية؛ حيث اكتسب أهمية متزايدة خاصة بعد بداية القرن الحادي والعشرين، مع التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصال وتصاعد الهجمات الالكترونية التي استهدفت الدول والمؤسسات الحيوية.

يهدف هذا المبحث إلى تأصيل مفهوم الأمن السيبراني وضبط حدوده المعرفية، وذلك من خلال تناوله في ثلاثة مطالب مترابطة؛ إذ يتناول المطلب الأول نشأة الأمن السيبراني والسياق التاريخي والتكنولوجي الذي أدى إلى ظهوره، وكذا تعريف الأمن السيبراني من مختلف التصورات مع تقديم تعريف اجرائي له، في حين عالج المطلب الثاني المفاهيم ذات الصلة به من أجل تمييزه وتحديد مجاله بدقة ضمن حقل الدراسات الأمنية، بينما ركز المطلب الثالث على أبعاده ومستوياته المتعددة.

المطلب الأول: نشأة وتعريف الأمن السيبراني

يستدعي التعرف على الأمن السيبراني الانطلاق من البوادر الأولى التي أدت إلى ظهوره، ثم تحليل مجموعة من التعاريف المقدمة لهذا المفهوم.

أولا: نشأة الأمن السيبراني

يرتبط الحديث عن نشأة الأمن السيبراني بتتبع المراحل الأولى لظهوره في سياق التطور التكنولوجي المتسارع، خاصة مع بروز الحواسيب والشبكات في النصف الثاني من القرن العشرين، وما رافق ذلك من تهديدات رقمية استدعت التفكير في آليات الحماية والتأمين المعلوماتي. ومن ثم فإن فهم الأمن السيبراني يقتضي العودة إلى نشأته والظروف التي أسهمت في تشكله.

- **المرحلة الأولى: البدايات المبكرة للفضاء السيبراني1861-1888:** يمكن تتبع البذور الأولى للفضاء السيبراني إلى سنة **1861**، خلال الحرب الأهلية الأمريكية، حين استخدم التلغراف لأول مرة في إدارة العمليات الحربية، وأصبح جزءًا مهمًا من منظومة الحرب. وفي سنة1888، أظهرت الدراسات العلمية أن الطاقة الكهربائية تولد ترددات يمكن ارسالها في الفضاء ورصدها، وهو ما مهد الطريق لفهم الظواهر المرتبطة بالاتصالات اللاسلكية، وتمهيدا لتطوير نظام الراديو لاحقًا.**(قطاف، 2022، صفحة 45)**
- **المرحلة الثانية: التطبيقات العسكرية الأولى للتقنية 1904 وما بعدها:** شهدت بدايات القرن العشرين تحولا مفصليا في تاريخ تأمين المعلومات؛ حيث انتقلت الممارسة من الاعتماد الكلي على "كتب الشفرات" والتدوين اليدوي للنصوص المشفرة إلى مرحلة "المكننة" الأولية. في هذه الفترة، ظهرت آلات بدائية مخصصة حصرا لعمليات التشفير وفك التشفير، وهو ما مثل استجابة تقنية لتعقيدات المشهد الدولي آنذاك، إذ لم يعد التشفير مجرد ترف فكري، بل صار ضرورة حتمية في الشؤون العسكرية والتحركات الدبلوماسية الخارجية التي تطلبت مستويات عليا من السرية لتأمين المراسلات العابرة للحدود.**(iwasaki, 2017, p. 3)**
- **المرحلة الثالثة: الحربان العالميتان والتقدم التكنولوجي النصف الأول من القرن العشرين:** تعتبر هذه المرحلة العصر الذهبي لتطور التشفير الكهروميكانيكي؛ حيث تداخلت فيها الحاجات الاقتصادية بالضرورات العسكرية لتنتج تقنيات أمنية معقدة. وقد برزت آلة "إنجما" كأهم ابتكار في هذا السياق. ومع اندلاع الحرب العالمية الثانية، أدى الانفجار في حجم البيانات والرسائل العسكرية المطلوبة إلى فرض واقع جديد استوجب التخلي عن الطرق التقليدية لصالح "التشفير الآلي" على نطاق واسع. مما جعل هذه الحقبة تمثل أول مواجهة حقيقية وشاملة في "حرب المعلومات التقنية".**(kumari, 2020, pp. 1-2)**

- **المرحلة الرابعة: التركيز على المعلومات وأمنها الستينيات:** في أوائل الستينيات أصبح التركيز على المعلومات باعتبارها مصدرا رئيسيا للميزة التنافسية، فبدأت التطبيقات الأمنية تحمي جميع المعلومات داخل المؤسسات، من جمعها على تخزينها ومعالجتها وتسليمها، لمنع الوصول غير المصرح به. ظهر مفهوم "أمن المعلومات" الذي يشمل حماية البيانات ونظم المعلومات، بالإضافة إلى الحماية المادية للأنظمة التقنية.
- **المرحلة الخامسة: توسع مفهوم الأمن السيبراني بعد الستينيات:** مع انتشار استخدام تكنولوجيا المعلومات والاتصالات، توسع المفهوم ليشمل أمن الشبكات، التجارة الالكترونية، والمعاملات الرقمية بين الأطراف المختلفة. وأصبح الأمن السيبراني يشمل عدة مستويات: التهديديات السيبرانية على المستوى الاستراتيجي، الحماية القانونية والخصوصية على المستوى القانوني، وحماية الأنشطة الاقتصادية على المستوى الاقتصادي، ليصبح مفهومًا متعدد الأبعاد وشاملاً.**(قطاف، 2022، صفحة 45)**

تكشف نشأة الأمن السيبراني عن ارتباط وثيق بين التطور التكنولوجي والتحول في طبيعة التهديدات الأمنية، حيث لم تعد المخاطر محصورة في المجال المادي، بل امتدت إلى الفضاء الافتراضي، ما استدعى إعادة تعريف مفهوم الأمن ذاته.

شكل رقم 01: مخطط نشأة الأمن السيبراني

المصدر : إعداد الطالبة

ثانيا: تعريف الأمن السيبراني

انطلاقا من دراسة المراحل المختلفة لنشأة الأمن السيبراني، سيتم فيما يلي تقديم المفاهيم الأكثر ملاءمة لهذا المصطلح وبيان دلالاتها من خلال:

يعرف الأمن السيبراني في توصية الاتحاد الأوروبي للاتصالات أنه "مجموعة من الأدوات و السياسات و المفاهيم الأمنية و الضمانات الأمنية و المبادئ التوجيهية و نهج إدارة المخاطر و الإجراءات و التدريب، وأفضل الممارسات وسبل الضمان و التكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية، وتشمل المنظمة وأصول المستعملين تجهيزات الحواسيب الموصولة؛ الموظفين، البنية التحتية و التطبيقات، الخدمات و أنظمة الاتصالات والحصيلة الكلية للمعلومات المرسلة والمخزنة في البيئة السيبرانية ومن شأن خدمات الأمن السيبراني كفالة تحقيق والحفاظ على الخواص الأمنية للمنظمات وأصول المستعملين والمخاطر الأمنية ذات الصلة في البيئة السيبرانية".**(الفتلاوي، 2016، صفحة 615)**

يركز هذا التعريف على الأمن السيبراني وصفه منظومة متكاملة تضم السياسات والأدوات والممارسات، والإجراءات الهادفة إلى حماية البنية التحتية الرقمية، وإدارة المخاطر وضمان سلامة الأنظمة والخدمات داخل المؤسسات والدول. هذا التعريف تغاضى عن البعد العسكري والتهديدات الأمنية الصلبة، وهي الجوانب التي ركز عليها تعريف وزارة الدفاع الأمريكي.

كما يعرف الأمن السيبراني بأنه: "عبارة عن مجموعة من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء استغلال المعلومات أو البيانات الالكترونية الموجودة على نظم الاتصالات والمعلومات كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف".**(شاهين، 2023، الصفحات 8-9)**

ينظر هذا التعريف إلى الأمن السيبراني باعتباره مجموعة من التدابير العملية التي تُتخذ لمنع الاختراقات والتجسس وسوء استخدام المعلومات. أغفل التعريف أهمية الإطار المؤسسي والسياساتي الذي شكل محور تعريف الاتحاد الأوروبي للاتصالات.

وقد عرفته وزارة الدفاع الأمريكية البنتاغون باعتباره: "جميع الإجراءات التنظيمية واللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية من مختلف الجرائم، الهجمات، التخريب، التجسس، والحوادث".**(القريطي، 2021، صفحة 13)**

يربط هذا التعريف الأمن السيبراني بالأمن القومي والتهديدات المعادية. نجد فيه حضور محدود للأبعاد المدنية والتنموية وإدارة المخاطر التنظيمية التي ظهرت في التعريفات ذات الطابع المؤسسي.

في حين تم تعريفه من طرف الاتحاد الأوروبي على أنه: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات".**(القريطي، 2021، صفحة 13)**

يبرز هذا التعريف البعد الحمائي–الدفاعي، ويركز على مرونة الأنظمة واستجابتها للهجمات. في حين لم يتوسع في عرض الأدوات والوسائل التقنية التفصيلية التي حضرت في تعريف إدوارد راموس.

كما عُرّف الأمن السيبراني عند إدوارد راموسو بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة.**(الحمامصة، 2022، صفحة 15)**

يتجه هذا التعريف إلى التركيز على الوسائل التقنية المستخدمة للحد من الهجمات على البرمجيات والأجهزة والشبكات، مثل أدوات مكافحة الفيروسات والتشفير، باعتبارها عناصر أساسية في تحقيق الحماية داخل البيئة السيبرانية. مقابل غياب النسق الاستراتيجي والقانوني والسياساتي الذي شكل جوهر تعريفات المؤسسات والهيئات الأمنية.

بناء على ما سبق يمكن تقديم تعريف اجرائي للأمن السيبراني بأنه: "منظومة متكاملة من السياسات والتدابير التقنية والتنظيمية والوقائية، التي تُعتمد لحماية الفضاء المعلوماتي بمكوناته البشرية والتقنية والبرمجية مع ضمان سرية البيانات وسلامتها، والحد من مخاطر الاختراق والهجمات والتجسس، بما يكفل استمرارية عمل الأنظمة والخدمات، وتحقيق القدرة على الاستجابة والمرونة في مواجهة التهديدات داخل البيئة الرقمية".

المطلب الثاني: المفاهيم ذات الصلة بالأمن السيبراني

يشكل تناول المفاهيم ذات الصلة بالأمن السيبراني خطوة تحليلية أساسية لفهم الإطار الذي يتحرك ضمنه هذا المجال. فالأمن السيبراني لا يتحدد فقط من خلال تعريفاته المباشرة، بل يتقاطع مع جملة من المفاهيم المرتبطة به مثل الردع، الصراع، القوة، والتهديد في البيئة السيبرانية، وهي مفاهيم تعكس طبيعة التفاعلات الجديدة داخل هذا الفضاء.

1.**الردع السيبراني:** يمكن تعريفه بوصفه آلية حماية فعالة تُفعل داخل النظام الرقمي بهدف اكتشاف الثغرات الأمنية التي قد تُستغل لشن هجمات سيبرانية بالغة الخطورة. كما يُنظر إليه أيضا باعتباره وسيلة لمنع الأعمال العدائية التي تستهدف الأصول الوطنية في الفضاء السيبراني، ولا سيما تلك المرتبطة بدعم العمليات ذات الطابع الفضائي. ويستند الردع السيبراني في مجال الاستراتيجية الدفاعية إلى ثلاث مرتكزات رئيسية، تتمثل في: تعزيز مصداقية الدفاع من خلال توفير أنظمة نسخ احتياطي تضمن استمرارية العمل وتقليل آثار الهجمات، إضافة إلى امتلاك القدرة على الانتقام. ويُعد تكبيد المهاجم خسائر تفوق ما يتوقعه من مكاسب عنصرًا حاسمًا في فعالية الردع، إذ أن الرغبة في الانتقام والقدرة عليه وحدهما لا تكفيان لتحقيق الردع بصورة كاملة.**(شاري و صادقي، 2024/2023، صفحة 22)**

يعد هذا التعريف شاملا لكونه يربط بين الجانب التقني والجانب النفسي الاستراتيجي، مما يعكس فلسفة الردع المعاصر التي لا تكتفي بتحصين الأنظمة، بل تسعى لرفع "تكلفة الهجوم" لإحباط إرادة الخصم قبل التنفيذ.

2.**الهجمات السيبرانية:** عرفها الخبير القانوني الأمريكي ميشال سميث بأنها "عمل يُنفذ في الفضاء السيبراني بهدف إحداث آثار في العالم الواقعي، كما عرفها عبد القادر محمد فهمي بأنها هجمات يُستعمل فيها النظام الشبكي والأجهزة الحاسوبية التابعة للدولة، أو تلك التي يستخدمها فاعلون من غير الدول، هدف تعطيل كفاءة السيطرة والقدرة على التحكم في منظومة الأجهزة أو شبكات الحاسوب، وما تتضمنه من بيانات ومعلومات تخص الفاعلين الآخرين، سواء كانوا من الدول أو من غير الدول، وذلك من أجل تقليلها أو تدميرها، بما قد يفضي إلى تهديد الأمن القومي للدولة، خصوصًا على مستوى منظوماتها العسكرية. (michael.n.smith, 2013, p. 158)

يركز هذا التعريف على الطبيعة "العابرة للحدود" والفاعلين غير الدوليين؛ حيث يبرز الهجمة كأداة تخريبية تتجاوز الفضاء الرقمي لتحدث أثرا ماديا ملموسا، مما يطمس الفواصل التقليدية بين التهديدات الافتراضية والواقعية.

3.**القوة السيبرانية:** تعرف القوة السيبرانية على أنها القدرة التي يمتلكها أي فاعل، سواء كان دولة، منظمة، أو حتى فرد، على استخدام الفضاء السيبراني كوسيلة لتحقيق مزايا استراتيجية والتأثير في سلوك وقرارات الآخرين. وتتجاوز هذه القدرة مجرد امتلاك الموارد التقنية، لتشمل الإمكانات التي تُتيح للفاعل إدارة المعلومات بشكل فعال، وتوجيه الانطباعات، والتحكم في تدفقات البيانات بما يخدم أهدافه. كما تشمل القوة السيبرانية القدرة على إجراء عمليات هجومية لدعم مصالح الفاعل، وعمليات دفاعية لحماية بنيته التحتية الرقمية، وكل ذلك ضمن إطار يؤثر على مجالات استراتيجية أوسع خارج نطاق الفضاء السيبراني نفسه، مثل: السياسة، الاقتصاد، والأمن الوطني. باختصار، هي مزيج من النفوذ الرقمي والتقني الذي يُمكن الفاعل من التحكم والتأثير عبر الشبكات الرقمية وتحقيق أهدافه الاستراتيجية طريقة متكاملة وشاملة.**(nyejr, 2010, p. 04)**

يتسم هذا التعريف بالعمق الاستراتيجي، كونه ينقل المفهوم من مجرد "امتلاك الأدوات التقنية" إلى "القدرة على التأثير وتوجيه السلوك"، فهي مزيج من النفوذ الرقمي والسياسي الذي يمنح الفاعل تفوقا في إدارة المعلومات وفرض الإرادة الدولية.

4.**الحروب السيبرانية:** يتم تعريفها بأنها توظيف القدرات السيبرانية بهدف تحقيق غرض رئيسي يتمثل في تحقيق أهداف أو آثار عسكرية داخل الفضاء الإلكتروني أو عبره. وبناءً على ذلك، يُمكن تلخيص مفهوم الحروب السيبرانية على أنها هجمات تشنها بعض الدول ويكون الفضاء الإلكتروني مسرحًا لها، بهدف إلحاق الضرر بالمنشآت والبنى التحتية والأهداف العسكرية للدولة التي تتعرض للهجوم. كما تتميز حروب الفضاء الإلكتروني بإمكانية أن تكون صادرة

عن فاعلين من غير الدول، الأمر الذي يؤدي إلى صعوبة تحديد العدو أو الجهة المهاجمة.**(مسيكة، 2022، صفحة 456)**

يظهر هذا التعريف التحول النوعي في العقيدة العسكرية؛ حيث أصبح الفضاء الإلكتروني مسرحا رابعا للعمليات، وتبرز قيمته الأكاديمية في الإشارة إلى معضلة "النسب" وهي صعوبة تحديد هوية المهاجم، مما يجعلها أداة صراع غير متماثلة ومعقدة.

تتجلى المفاهيم المرتبطة بالأمن السيبراني بوصفها إطارًا تحليليًا يعكس انتقال هذا المجال من بُعده التقني الضيق إلى فضاء استراتيجي مركب، تتداخل فيه آليات الردع، الهجوم، ومقومات القوة مع أنماط الصراع الحديثة.

شكل رقم 02: المفاهيم ذات الصلة بالأمن السيبراني

المصدر: إعداد الطالبة

المطلب الثالث: أبعاد الأمن السيبراني

يمثل الوقوف على أبعاد الأمن السيبراني مدخلاً تحليليًا مهمًا لفهم طبيعته المركبة وتعدد مجالات اشتغاله، خاصة في ظل التحولات الرقمية المتسارعة وتزايد الاعتماد على الفضاء السيبراني في مختلف القطاعات الحيوية. فالأمن السيبراني لم يعد يُختزل في الجانب التقني فقط، بل بات يرتبط بأبعاد أمنية، اقتصادية، اجتماعية، سياسية، قانونية متداخلة.

1.البعد العسكري: تتحدد الأهمية النسبية للقوة السيبرانية في المجال العسكري من خلال قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية داخل الفضاء الإلكتروني، بما يُسهل عملية تبادل المعلومات وتدفقها بسرعة، ويُعزز كفاءة إصدار الأوامر العسكرية وتنفيذها. غير أن هذه الميزة قد تتحول إلى نقطة ضعف في حال عدم تأمين الشبكات الإلكترونية المستخدمة بالشكل الكافي، الأمر الذي يفتح المجال أمام الاختراقات الخارجية التي قد تُستغل في شن هجمات إلكترونية مضادة تستهدف شبكات القوات المسلحة وأجهزة الاستخبارات، بما يسمح بعمليات التجسس على الأمن العسكري للدول، وقطع أنظمة الاتصال بين الوحدات العسكرية.**(عطية ا.، 2019، صفحة 105)**

2.البعد الاقتصادي: يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد في ظل التلازم بين اقتصاد المعرفة والتوسع في استخدام تقنيات المعلومات والاتصالات، خاصة مع تزايد حجم البيانات والمعلومات المتداولة والمخزنة والمستخدمة عبر الشبكات، الأمر الذي أسهم في دعم التنمية الاقتصادية لدى العديد من الدول. كما تَكرس ذلك مع دخول العالم عصر الاقتصاد الإلكتروني ضمن بيئة رقمية متحركة؛ حيث تنامت استثمارات المصارف المالية في المجال المالي الرقمي، واشتدت المنافسة لتطوير تطبيقات الدفع الآمن، ما دفع بعض الدول إلى سن تشريعات لحماية الأموال والحد من الجرائم الاقتصادية والمالية.**(بكرش، 2019/2018، صفحة 11)**

3.البعد السياسي: تتمثل الأبعاد السياسية للأمن السيبراني في مسؤولية الدولة وسيادتها، إذ تضطلع بدور أساسي في توفير الأمن السيبراني من خلال دعم البحث والتطوير، وترسيخ الثقافة الأمنية على المستوى الاستراتيجي، ونشر الوعي بأفضل الممارسات في مجالات الوقاية، الإبلاغ، تبادل المعلومات، الإنذار المبكر، وإدارة المخاطر بوصفها قضايا رئيسية تستوجب المعالجة. وفي سياق سيادة الدول، يبرز تعقد متطلبات أمن البيانات والأنظمة ما يدفع إلى الاستعانة بمصادر وخبرات خارجية، الأمر الذي قد يفضي إلى درجة من التبعية تُشكل خطرًا أمنيًا.**(عيساوي و زيتون، 2024/2023، الصفحات 29-30)**

4.البعد الاجتماعي: تتيح طبيعة الأنترنت المفتوحة، خاصة عبر وسائل التواصل الاجتماعي، للأفراد التعبير عن آرائهم السياسية وتطلعاتهم الاجتماعية، كما تُعزز مشاركة مختلف فئات المجتمع في التنمية من خلال الاطلاع على أفكار ومعلومات جديدة. ويُسهم تواصل المجتمعات عبر الفضاء الإلكتروني في تبادل الخبرات والمعارف، وتسهيل الوصول إلى الخدمات والمعلومات لفئات متعددة مثل كبار السن، المرضى، ذوي الاحتياجات الخاصة، وفي دعم تبادل المعلومات أثناء الأزمات والكوارث. ولا تقتصر الأبعاد الاجتماعية للأمن السيبراني على توفير الحماية للمواطن في حياته اليومية عبر تكنولوجيا المعلومات، بل تشمل أيضًا صيانة القيم الأساسية للمجتمع ونشر الوعي بها. وفي المقابل، يُؤدي انتشار المحتويات غير القانونية وغير الملائمة إلى تهديد القيم الاجتماعية وزيادة الجرائم.**(عطية ا.، 2025، صفحة 448)**

5.البعد القانوني: يشكل تنظيم الأمن السيبراني من قبل الأفراد والمؤسسات والحكومات أمرًا بالغ الأهمية، لما يترتب عليه من نتائج قانونية وحاجة إلى وضع قواعد لمعالجة النزاعات الإلكترونية. ومع ظهور مجتمع المعلومات، ظهرت حقوق جديدة إلى جانب الحقوق والحريات الأساسية، مثل الحق في الوصول إلى الأنترنت، حق إنشاء المدونات الإلكترونية، وحماية ملكية البرمجيات والمعلومات. كما استوجبت التحولات الرقمية سن تشريعات لحماية البيانات

والخصوصية، ومراقبة المخالفات والجرائم المرتبطة بالتحول الرقمي. **(عطية ا.، 2025، صفحة 445)**

يمثل الأمن السيبراني ركيزة استراتيجية شاملة تتقاطع فيها الاعتبارات العسكرية، الاقتصادية، السياسية، الاجتماعية، والقانونية، في ظل التحول الرقمي المتسارع. فحماية الفضاء السيبراني لم تعد مسألة تقنية محضة، بل أضحت شرطًا لضمان السيادة الوطنية، استقرار الاقتصاد الرقمين وسلامة المجتمع، وفعالية المنظومة التشريعية. وعليه، فإن تحقيق أمن سيبراني فعال يقتضي رؤية تكاملية ترتكز على التنسيق المؤسسي، تعزيز الوعي، وتطوير الأطر القانونية.

الشكل رقم 03: أبعاد الأمن السيبراني

المصدر : إعداد الطالبة

المبحث الثاني: مفهوم الفكر الاستراتيجي

يشكل الفكر الاستراتيجي إطارًا معرفيًا ناظمًا لفهم ديناميات البيئة الأمنية وتحليل أنماط التفاعل والصراع في العلاقات الدولية، انطلاقا من ارتباطه بعمليات تقدير التهديدات وصياغة البدائل وتوجيه السلوك الأمني في ظل تحولات القوة وتسارع التطور التكنولوجي. وفي هذا السياق، يتجه هذا المبحث إلى تأصيل مفهوم الفكر الاستراتيجي وإبراز امتداداته النظرية

والوظيفية عبر معالجة ثلاثة مطالب مترابطة؛ يركز المطلب الأول على تتبع مسار تطور الفكر الاستراتيجي وضبط دلالاته المفاهيمية، وينصرف المطلب الثاني إلى تبيان أهميته داخل حقل الدراسات الأمنية بوصفه أداة تفسيرية لصناعة القرار وإدارة التهديدات، بينما يتناول المطلب الثالث الأمن السيبراني باعتباره متغيرا بنيويا أسهم في إعادة تشكيل الفكر الاستراتيجي المعاصر.

المطلب الأول: تطور وتعريف الفكر الاستراتيجي

لفهم الفكر الاستراتيجي بصورة أدق لا بد أولا من التطرق إلى المراحل التي مر بها عبر مختلف الفترات التاريخية والتي ساهمت في تطوره، ثم التعرف على أبرز لتعاريف التي تناولت مفهوم الفكر الاستراتيجي وتحليل مضامينها.

أولا: تطور الفكر الاستراتيجي

خضع الفكر الاستراتيجي لتطور مستمر انعكس على ممارسات التخطيط العسكري وتحليل التهديدات وصنع القرار الأمني إذ تأثر بالتحولات التاريخية والسياسية والتكنولوجية، ما أسهم في تشكيله تدريجيا من منظور متكامل يجمع بين البُعد النظري والتطبيقي في الدراسات الأمنية.

1.الفكر الاستراتيجي في العصر القديم: يرجع أصل الفكر الاستراتيجي الصيني إلى كتابات سون تزو الذي اعتبر الحرب قضية مصيرية لا يجوز التعامل معها باستخفاف، لأنها تتصل ببقاء الدولة بين الحياة والموت، مما يفرض دراستها بعمق. وقد تأثر هذا الفكر بالفلسفة الكونفوشيوسية، وهو ما يظهر في تركيزه على تحقيق النصر بأقل كلفة مُمكنة، وتفضيل الحسم دون قتال كلما أمكن ذلك. إضافة إلى تفضيل إخضاع العدو بأقل خسائر بدل تدميره أو تكرار الانتصارات في معارك مُتعددة.

أما الفكر الاستراتيجي اليوناني والروماني فقد ارتبطا بتطور المُمارسة العسكرية ومحاولة تنظيمها، إذ نظر اليونانيون إلى الاستراتيجية بوصفها توظيفًا للإمكانات الذهنية والعسكرية من أجل مباغتة العدو وإرباكه. ويُعد الاسبرطيون أوائل من أسهموا في بلورة المبادئ الأولى للاستراتيجية اعتمادًا على خبرتهم الحربية. وفي المقابل، تناول الرومان الاستراتيجية ضمن تصور علمي قائم على الانضباط وتراكم التجربة، غير أن هذا الفكر ظل في الغالب أقرب إلى التطبيق منه إلى بناء نظرية متكاملة.**(البسومي، 2026، الصفحات 5-6)**

2.الفكر الاستراتيجي في عصر النهضة: يمثل عصر النهضة مرحلة انتقالية بين العصر القديم والعصر الحديث، وقد شهدت بروز مفكرين اهتموا بالحرب وكتبوا حولها، وفي مقدمتهم نيكولا ميكيافيلي الذي قد أفكارًا فتحت المجال أمام تطور التفكير الاستراتيجي لاحقًا. فقد اعتبر الحرب ضرورة سياسية لا يُمكن تجاهلها، ورأى أنها صراع بين قوى متنافسة لا يُفسر فقط بالاعتبارات الدينية أو الأخلاقية، بل تحكمه أيضا عوامل اقتصادية، سياسية، وقومية.

كما سعى إلى وضع قواعد عامة للاستراتيجية وربطها بهدف الحرب، مؤكدا أن الغاية من القتال ينبغي أن تكون تحقيق مصلحة الدولة ككُل. وفي هذه المرحلة اتسع مفهوم الاستراتيجية ليشمل تعبئة موارد الأمة وتنظيمها لخدمة أهداف الحرب، مع تطور ملحوظ في الأسلحة وخصوصًا المدفعية، رغم استمرار بعض السمات التقليدية. كما برزت محاولات لإحياء الفن العسكري وتحديثه، إلى جانب ظهور الجيش النظامي وتطوير التدريب والاهتمام بميدان المعركة، وهو ما أعاد الاعتبار للقوة المسلحة كعامل حاسم، وجعل من عنصر المفاجأة والاحتلال السريع لمواقع استراتيجية جزءًا جوهريًا من التحضير للانتصار.**(البسومي، 2026، صفحة 7)**

3.الفكر الاستراتيجي في العصر الحديث: يعتبر الفكر الاستراتيجي الأوروبي في بدايات العصر الحديث امتدادًا متأخرًا لما بدأ في العصور الوُسطى، لكنه لم يتبلور بشكل واضح إلا ابتداءً من النصف الثاني للقرن الخامس عشر. وقد ظهر ذلك من خلال مؤلفات عسكرية

مُبكرة في اسبانيا وفرنسا وانجلترا وألمانيا وإيطاليا، ركزت على تحليل الحرب، تنظيم الجيش، وتطوير أساليب القتال، وارتبطت هذه الكتابات بتغيرات واقعية فرضتها التحولات السياسية والعسكرية داخل أوروبا. كما برزت في هذه المرحلة مُساهمات مفكرين وكُتاب عسكريين اهتموا بتحديد العلاقة بين الاستراتيجية والتكتيك، تنظيم الجيوش، دور التدريب والانضباط، وأهمية المدفعية والأسلحة النارية، إضافة إلى التأكيد على المفاجأة وإدارة الموارد. وقد ساهمت الحروب الأوروبية الكبرى، مثل حرب المائة عام والحروب الإيطالية، في دفع هذا الإنتاج الفكري وتوسيعه.**(البسومي، 2026، الصفحات 8-9)**

4.الفكر الاستراتيجي في العصر المعاصر: شهدت الفترة المُمتدة بين 1789 و1815 حروبًا أوروبية متواصلة أفرزت تحولات عميقة في التفكير الاستراتيجي، إذ برزت محاولات تنظيرية مُبكرة ركزت على الدفاع عن المراكز الحيوية وتطوير أسس الفن العسكري، كما ظهرت كتابات تناولت نظام الحرب الحديثة ومبادئ الاستراتيجية والتكتيك. ويُعد أنطوان هنري جوميني من أبرز المؤسسين الأوائل للفكر الاستراتيجي المُعاصر حيث أسهم في تقنين مبادئ الحرب من خلال تحليل العمليات العسكرية وحروب نابليون، مع ادخال تعديلات نظرية مُستمدة من خبرته الميدانية، مما جعله مرجعًا مؤثرًا في الفكر الاستراتيجي الأوروبي والأمريكي على حدٍ سواء. أما كارل فون كلاوزفيتز فيُنظر إليه بوصفه أحد أهم المُنظرين العسكريين، إذ قدم تصورًا عميقًا للحرب باعتبارها امتدادًا للسياسة بوسائل أخرى، واعتمد على تحليل تاريخي للحملات العسكرية وصياغة نظرية شاملة للحرب الكبرى والتكتيك، رغم أن مشروعه الفكري ظل غير مُكتمل بسبب وفاته.**(نيوف، الصفحات 51-56)**

الشكل رقم 04: مراحل تطوُّر الفكر الاستراتيجي

المصدر: إعداد الطالبة

بعد استعراض تطور الفكر الاستراتيجي عبر مراحله التاريخية المختلفة، يتضح أن هذا المفهوم لم يبقَ ثابتًا، بل شهد تحولات عميقة ارتبطت بتغير طبيعة الصراع وأدواته.

ثانيا: تعريف الفكر الاستراتيجي

من خلال ذلك سيتم فيما يلي عرض مجموعة من التعاريف التي تناولت مفهوم الفكر الاستراتيجي، من بينها:

عرف كينيتشي أوه ماي الفكر الاستراتيجي على أنه: "هو أسلوب في حل المُشكلات يقوم على التركيز على العوامل الأكثر حسمًا والسعي إلى تحقيق ميزة تنافسية واضحة".

يُركز هذا التعريف على الفكر الاستراتيجي بوصفه أسلوبًا لحل المُشكلات وتحقيق ميزة تنافسية، أي أنه ينطلق من منظور عملي إداري. أبرز أهمية التركيز على العوامل الحاسمة، وخزل الفكر الاستراتيجي في حل المُشكلات والتنافسية فقط دون الإشارة إلى الاستشراف والبُعد طويل المدى.**(kenichi, 1982, p. 13)**

كما يعرف الفكر الاستراتيجي على أنه: "مجموعة الانضباطات الذهنية التي يستخدمها القادة للتعرف على التهديدات والفرص المُحتملة، وترتيب أولويات تركيزهم، وحشد منظماتهم نحو مسارات واعدة إلى الأمام".**(walkins, 2020, p. 66)**

يبرز هذا التعريف الفكر الاستراتيجي كنشاط ذهني قيادي يقوم على تحليل التهديدات والفرص، ترتيب الأولويات، وتوجيه المُنظمة. ركز على دور القيادة والبيئة؛ لكنه حصره في القيادة الفردية ولم يُظهر طابعه المُؤسسي أو أدواته التحليلية.

في حين يشير تعريف آخر أن الفكر الاستراتيجي: "يعد ضروريا للقادة في التعامل مع البيئات المعقدة والسريعة التغير"

يقدم هذا التعريف الفكر الاستراتيجي كضرورة للتعامل مع البيئات المُعقدة وسريعة التغير، مُركزًا على التكيف مع التحولات. لكنه بقي عامًا ولم يُوضح آليات التفكير أو أهدافه الاستراتيجية.

في حين جاء تعريف آخر يُبرز أن الفكر الاستراتيجي هو: "مفهوم يُستخدم لوصف الإطار الفكري والدراسات المُتخصصة في فهم العلاقات الدولية والأمن القومي، ويتضمن فهم الطبيعة الاستراتيجية للأحداث، تحليل مُتغيرات البيئة الأمنية، الاستشراف المُستقبلي، وتحديد بدائل وسُبل الوُصول إلى الأهداف العُليا للأمن والاستقرار".**(walkins, 2020)**

ينظر هذا التعريف إلى الفكر الاستراتيجي كمفهوم تحليلي يُستخدم في فهم العلاقات الدولية والأمن القومي، ويتضمن تحليل البيئة والاستشراف وتحديد البدائل. ركز على البُعد الأمني والتحليلي؛ لكنه أخفق في إظهار الُعد التطبيقي وصنع القرار.

هذا ما يقودنا إلى تقديم تعريف إجرائي للفكر الاستراتيجي يتمثل في أن: " الفكر الاستراتيجي هو عملية ذهنية تحليلية تُستخدم لفهم طبيعة البيئة الداخلية والخارجية وتحولاتها، ولا سيما ما يرتبط بالمخاطر والتهديدات الأمنية، وتحديد الفُرص، ترتيب الأولويات، صياغة

بدائل العمل، واختيار أنسبها، بما يُمكن صانع القرار من توجيه الموارد والقدرات نحو تحقيق أهداف بعيدة المدى، وتعزيز الأمن والاستقرار، وضمان التكيف مع التعقيد والتغير".

المطلب الثاني: أهمية الفكر الاستراتيجي في حقل الدراسات الأمنية

في سياق التحولات المُتسارعة التي تشهدها البيئة الدولية وتنامي التهديدات غير التقليدية، برز الفكر الاستراتيجي كإطار تحليلي لفهم القضايا الأمنية وتفسير ديناميكاتها، وهو ما يُمهد لتناول موقعه ودوره ضمن حقل الدراسات الأمنية.

تتمثل أهمية الفكر الاستراتيجي في حقل الدراسات الأمنية في كونه أداة محورية لتطوير الأداء الأمني وتعزيز كفاءة القيادات الأمنية، بما يُمكنها من التعامل مع التحديات البيئية والمخاطر المُستقبلية بكفاءة أكبر. كما يُسهم الفكر الاستراتيجي في تحسين قدرات الأجهزة الأمنية على التشخيص الدقيق للمشكلات، استشراف التهديدات، واتخاذ القرارات المُناسبة في ظل المُتغيرات المُتسارعة في البيئة الأمنية. ويؤدي كذلك دورًا مركزيًا في تنمية مهارات العاملين ورفع مستوى الإبداع والكفاءة لديهم، الأمر الذي يدعم جاهزية المُؤسسات الأمنية لمواجهة الأزمات والتهديدات المُختلفة بصورة أكثر فاعلية وتنظيمًا.**(الحيجاوي و الصريديذ، 2019، صفحة 18)**

كما يعكس تطور بيئة الأمن في الدراسات الأمنية ضرورة اعتماد الدول على الفكر الاستراتيجي كأداة مركزية لإدارة المخاطر والتهديدات. فالفكر الاستراتيجي يُمكن صانعي القرار من تقييم المخاطر بشكل منهجي، والتخطيط لتوظيف الموارد العسكرية والدبلوماسية والعلمية بشكل متكامل، بما يُعزز قدرة الدولة على الوقاية والتكيف مع التغيرات الأمنية المُتسارعة.

علاوة على ذلك، يوفر استخدام نماذج تحليلية مثل نظرية الألعاب إطارًا لفهم العلاقات المُعقدة بين السياسات الدولية والاستراتيجيات الدفاعية، ما يجعل الفكر الاستراتيجي ليس مُجرد أداة نظرية، بل آلية عمل لتعزيز أمن الدولة واستدامة مصالحها الوطنية.(2011, p. 67)

من هذا المنظور يظهر الفكر الاستراتيجي كعنصر حاسم يربط بين الرؤية التحليلية والتخطيط العملي في حقل الدراسات الأمنية، مؤكدًا أن أي إدارة فعالة للأمن لا يُمكن أن تتحقق دون إدراك دقيق للبُعد الاستراتيجي للمخاطر والتحديات. ومنه فإن الفكر الاستراتيجي يُمثل أهمية كبيرة في حقل الدراسات الأمنية، إذ يبرز كحلقة وصل بين الرؤية التحليلية والتخطيط العملي، ما يجعله عُنصرًا جوهريًا لتعزيز أمن الدولة واستدامة مصالحها الوطنية.**(anthony craig, 2018, p. 85)**

المطلب الثالث: الأمن السيبراني كمُتغير بنيوي في إعادة تشكيل الفكر الاستراتيجي المُعاصر

يشكل الأمن السيبراني مُتغيرًا بنيويًا يفرض إعادة النظر في الفكر الاستراتيجي المُعاصر، إذ يُؤثر بشكل مُباشر في طُرق التحليل والتخطيط واتخاذ القرار الأمني، ويجعل حماية المعلومات والأنظمة الرقمية محورًا أساسيًا لضمان الفاعلية الاستراتيجية في مواجهة التهديدات الحديثة.

أدى التطور التكنولوجي المُتسارع إلى إحداث تحول بنيوي في طبيعة التهديدات الأمنية، إذ لم تعد هذه التهديدات محصورة في أبعادها التقليدية المُرتبطة بالمجالين البري والبحري أو حتى الجوي، بل امتدت إلى الفضاء السيبراني باعتباره مجالاً جديدًا للصراع وإعادة إنتاج مصادر القوة. وقد فرض هذا التحول على الدول مراجعة مقارباتها الأمنية والدفاعية، وإعادة مواءمة استراتيجياتها مع طبيعة المخاطر السيبرانية المُستجدة التي تتسم بالتعقيد والتشابك والتطور المُستمر.**(نجمة، 2023، صفحة 76)**

وفي هذا الإطار، تحول الفضاء السيبراني إلى حيز فاعل ضمن بنية التفاعلات الدولية، حيث أفرزت البيئة الرقمية أنماطًا مُتعددة لاستخداماته ذات الطبيعة المدنية والعسكرية على السواء. وقد أفضى ذلك إلى تكريسه كساحة جديدة للتنافس والصراع بين الدول وكذلك بين

الفواعل من غير الدول، في سياق السعي على تعظيم النفوذ وإعادة توزيع أدوات التأثير داخل النظام الدولي المُعاصر. ومع ترسخ الفضاء السيبراني كمجال صراعي مُستقل، بدأت ملامح الحرب السيبرانية تتبلور بصورة تختلف جوهريًا عن الحروب التقليدية، سواء من حيث الإطار المفاهيمي، آليات التخطيط والتدبير، طبيعة التنفيذ، أو حتى حدود ميدان التأثير.**(علي، 2022، الصفحات 15-16)**

وانطلاقا من هذا التحول، يُنظر إلى الحرب الإلكترونية بوصفها حرًبا استراتيجية في عصر المعلومات، على نحو يُماثل الدور الذي اضطلعت به الحرب النووية في القرن العشرين ضمن معادلات الردع والتوازن الدولي. ويؤسس هذا التصور لفهم الحرب السيبرانية باعتبارها ركيزة مركزية في منظومة الأمن القومي، لما تنطوي عليه من قدرة على التأثير العنيق الذي لا يقتصر على المجال العسكري، بل يمتد إلى الاقتصاد، الدبلوماسية، والتنمية الاجتماعية.**(علي، 2022، صفحة 24)**

وعليه أضحى الأمن السيبراني أحد الأبعاد البنيوية للقوة الاستراتيجية الحديثة، نظرًا لدوره الحيوي في حماية المصالح الجوهرية للدول، ولا سيما البنى التحتية الحيوية والأنظمة المعلوماتية الحساسة. **(نجمة، 2023، صفحة 82)**

كما بات لهذا البُعد السيبراني انعكاس مباشر على موازين القوى وديناميات الصراع الدولي، الأمر الذي يعكس تحولاً في أدوات التأثير الاستراتيجي ويُكرس مسألة تأمين الفضاء الإلكتروني كقضية استراتيجية بامتياز ضمن سياقات التنافس الدولي.**(نجمة، 2023، صفحة 77)**

المبحث الثالث: الإطار النظري المُفسر للعلاقة بين الأمن السيبراني والفكر الاستراتيجي

يقتضي تحليل العلاقة بين الأمن السيبراني والفكر الاستراتيجي الاستناد إلى إطار نظري يُفسر كيفية إدماج الفضاء السيبراني ضمن الحسابات الاستراتيجية للدول، في ظل التحولات

التي مست طبيعة القوة والتهديد في البيئة الدولية المُعاصرة. حيث يتناول هذا المبحث دراسة هذه العلاقة من خلال ثلاث مطالب رئيسية؛ المطلب الأول يدرس الواقعية الجديدة/ البنيوية، المطلب الثاني تمثل في الليبيرالية المؤسساتية، المطلب الثالث والأخير تجلى في النظريات الجيوبوليتيكية.

المطلب الأول: النظرية الواقعية الجديدة/البنيوية

شهدت النظرية الواقعية خلال سبعينيات القرن العشرين تراجُعًا نسبيًا نتيجة تراجع مظاهر الترابُط المُتبادل وتراجع حدة بعض التوترات الدولية، غير أنها استعادت موقعها بقوة في حقل العلاقات الدولية مع نهاية العقد نفسه تحت مسمى "الواقعية الجديدة"، متأثرة بعودة أجواء الحرب الباردة. وقد أسهم في بلورة هذا التوجه عدد من المنظرين البارزين، من بينهم كينيث والتز.

وتميزت الواقعية البُنيوية ابتعادها النسبي عن الطروحات الكلاسيكية لهانس مورغنثاو، واقترابها من تصورات ريمون آرون؛ حيث ركزت على البنية الفوضوية للنظام الدولي وأعادت النظر في مفاهيم مركزية مثل المصلحة القومية والقوة.(السيساوي، 2025، صفحة 15)

تقوم النظرية الواقعية الجديدة عند كينيث والتز على تصور النظام الدولي كبنية منظمة وفق مجموعة مُحددة من المبادئ الأساسية. إذ يرى والتز أن البنى السياسية تُعرف أولاً بالمبدأ الذي تُنظم بموجبه، وثانيًا بتحديد وظائف الوحدات المُتميزة شكليًا، وثالثًا بتوزيع القدرات بين هذه الوحدات.**(waltz, 1979, p. 79)**

وفي إطار المقارنة بين النظامين الداخلي والدولي، يُوضح أن البنى السياسية الداخلية تُنظم وفق مبدأ التدرج الهرمي، في حين أن البنى السياسية الدولية تُبنى على مبدأ الفوضى.

ويؤكد أيضا أن الوحدات الفاعلة في النظام الدولي، وعلى الرغم من اختلافاتها، مُتشابهة وظيفيًا. وأن الهدف الأعلى لهذه الوحدات، أي الدول، هو ضمان بقائها واستمرارها.

1.الافتراضات الأساسية للنظرية الواقعية:

سعى ستيفن لامي إلى بلورة الافتراضات الكبرى للواقعية الجديدة، مع الأخذ في الاعتبار التباينات الواضحة بين منظريها، ولا سيما الخلافات بين كينيث والتز وجون ميرشايمر بشأن تفسير طبيعة العلاقات الدولية. ويُمكن إجمال أبرز هذه الافتراضات فيما يأتي:

– تتفاعل الدول داخل بيئة دولية فوضوية، أي في ظل غياب سُلطة مركزية عليا تفرض القواعد أو تحمي المصالح العامة للنظام الدولي.

– تعد بنية النظام الدولي المُحدد الرئيس لسلوك الدول، إذ تنطلق السياسة الخارجية من ضغوط البيئة الدولية وقيودها البنيوية.

– تتسم الدول بتوجه مصلحين وفي إطار الفوضى والمنافسة تميل إلى تفضيل الاعتماد على الذات بدل التعويل على التعاون؛ لأن بنية النظام لا تضمن نوايا الآخرين.

– تُعتبر الدول فواعل عقلانية تسعى إلى تعظيم مكاسبها وتقليل خسائرها، ويُقاس سلوكها بمدى خدمته لمصالحها الوطنية.

– يُشكل البقاء في ظل الفوضى الإشكالية المركزية التي تؤطر سلوك الدول وتوجه خياراتها الاستراتيجية.

– تنظر الدول إلى بعضها البعض بريبة، وقد تتعامل معها بوصفها خصومًا أو مصادر تهديد مُحتملة، ما يُفضي إلى انعدام الثقة وتنامي المخاوف الأمنية، وهو ما يُفسر جانبًا كبيرًا من سياساتها.**(محلف، صفحة 2018)**

2.الأمن السيبراني والفكر الاستراتيجي من منظور النظرية الواقعية الجديدة:

تبرز المقاربة الواقعية الجديدة أن تصاعد حجم الهجمات السيبرانية واتساع نطاق أضرارها دفعا حقل العلاقات الدولية إلى إدراج سلوك الدولة في الفضاء السيبراني ضمن أُطر تفسيرية بنيوية، حيث يُقدم تحليل واقعي جديد يعتمد أدوات كمية لفهم هذا السلوك في سياق فوضوي دولي. **(arslan, 2023, p. 1)**

وفي هذا الإطار، تُظهر النتائج أن تعزيز الدول لقدراتها في الأمن السيبراني يرتبط بزيادة انخراطها في أنشطة سيبرانية تخريبية ضد دول أخرى، بما يعكس ديناميات "معضلة الأمن" التي تجعل سعي الدولة لتعظيم أمنها مُحفزًا لاستجابات تصعيدية متبادلة. **(arslan, 2023)**

علاوة على ذلك، أدى انتشار تكنولوجيا المعلومات والاتصالات إلى ترسيخ موقع الأمن السيبراني في صُلب الاهتمامين السياسي والأكاديمي، إذ يُنظر إلى الفضاء السيبراني بوصفه المجال الخامس للحرب**(craig & valeriane, 2018, p. 85)**.

كما يمكن تفسير سباق التسلح السيبراني باعتباره استجابة طبيعية للتهديد في نظام دولي فوضوي تسعى فيه الدول إلى تعظيم أمنها في ظل غياب سلطة مركزية عُليا **anthony craig, 2018, pp. 87-88)**.

وهو ما يؤكد أن الفضاء الرقمي لا يخرج عن منطق القوة وتوازنها؛ بل يُمثل امتدادًا بنيويًا له.**(anthony craig, 2018, p. 86)**

وبما أن هذا السياق البنيوي يُشكل الأساس لتحديد الخيارات الاستراتيجية للدولة، فإن النظرية الواقعية الجديدة تعتبر أن السلوك الاستراتيجي للدول في النظام الدولي يُحدد بدرجة كبيرة عبر البنية الفوضوية للنظام؛ حيث يفترض أن الدول تسعى أولاً إلى البقاء كشرط أساسي لتحقيق أي أهداف أخرى، وأن السعي وراء القوة والأمن يُشكل محور استراتيجياتها الكبرى.**(mearsheimer, 2001, p. 01)**

من هذا المنطلق، يُشير تحليل الواقعية الجديدة إلى أن الخيارات الاستراتيجية للدول ليست نتاج إرادة فردية منفصلة؛ بل هي مقيدة بالخصائص البنيوية للنظام الدولي، بما في ذلك الفوضى وعدم التوازن في توزيع القدرات بين الدول.**(kramer, pp. 11-12)**

وعليه، يمكن التمييز بين النسخة الدفاعية للواقعية الجديدة التي تُؤكد ضبط الاستراتيجية عبر البنية، والنسخة الهجومية التي ترى في زيادة القوة النسبية أداة رئيسية لتعظيم الأمن في ظل التهديدات المتبادلة**(snyder, p. 08)**.

وهو ما يوضح أن تعزيز القوة المادية يُمثل الطريق الأكثر فاعلية لتحقيق الأمن الاستراتيجي ضمن الإطار البنيوي.**(j.w. taliaferoco, pp. 3-4)**

علاوة على ذلك، يُوفر هذا المنظور تفسيرًا متماسكًا لكيفية صياغة الدول لاستراتيجياتها الكبرى، إذ أن السعي المتواصل نحو القوة يظل مُوجهًا ومُقيدًا بالحقائق البنيوية للنظام الدولي، بما يجعل كل قرار استراتيجي مُرتبطًا بتقييم الدولة لموقعها النسبي وللسياسات التنافسية للآخرين في بيئة دولية فوضوية.**(snyde, pp. 01-02)** يُظهر هذا التفسير كيف يرتبط تطوير القدرات السيبرانية بشكل مباشر بصياغة الاستراتيجيات الكبرى، ما يعكس التفاعل البنيوي بين الأمن الرقمي والفكر الاستراتيجي في ظل منافسة القوة بين الدول.**(kramer, pp. 11-12)**

المطلب الثاني: النظرية الليبيرالية المؤسساتية

تعد المدرسة الليبيرالية من أكثر اتجاهات العلاقات الدولية إعلاء لقيمة التعاون بين الدول، إذ تنظر إليه بوصفه الحالة الطبيعية التي تحكم التفاعلات الدولية، في مقابل اعتبار النزاعات والحروب حالات استثنائية ورغم غياب بناء نظري موحد ومتماسك للنظرية الليبيرالية، فإنها شكلت إطارًا فكريًا تعددت داخله التيارات التي تندرج ضمن ما يُعرف بالليبيراليات. فقد عرف المنظور الليبيرالي تطورًا ملحوظًا خلال سبعينيات وثمانينيات القرن العشرين، تزامُنًا مع

بروز نظرية الاعتماد المُتبادل وتزايد ترابط العلاقات الاقتصادية الدولية وتشابكها، حيث قدم الاتجاه الليبيرالي الجديد مقاربات حديثة سعت إلى تفسير سبُل تعزيز السلم.**(بوستي، 2019/2018، صفحة 13)**

تركز النظرية الليبيرالية المؤسساتية على دور المؤسسات الدولية والقواعد المشتركة في تعزيز التعاون وتقليل الصراعات بين الدول، بما يُتيح تفسيرًا أكثر دقة لسلوك الفاعلين الدوليين في مجالات متعددة، من بينها الأمن والسياسة الاستراتيجية.

1.الافتراضات الأساسية للنظرية الليبيرالية الجديدة / المؤسساتية:

يمكن تلخيص أبرز افتراضات النظرية الليبيرالية المؤسساتية أو الليبيرالية الجديدة كاتجاه ضمن عائلة الليبيراليات، في:

– المؤسسات الدولية تلعب دورًا مركزيًا في تنظيم العلاقات بين الدول وتقليل النزاعات، وتعكس قيم الرأسمالية والديمقراطية.

– مأسسة الأمن تعمل على تعزيز التعاون بين الدول وتقليل المخاطر والغش من خلال التنشئة الاجتماعية للفاعلين الدوليين.

– استقلالية الدولة تتراجع نسبيًا بسبب النفوذ المتنامي للمؤسسات، ما يجعل العلاقات بين الدول أقل صراعية.

– المؤسسات الاندماجية، مثل الاتحاد الأوروبي وحلف الشمال الأطلسي، تسهم في تطوير أنظمة أمنية مستقرة وتحد من السلوك العسكري للدول.

– استمرار المؤسسات بعد الحرب الباردة يُثبت أن قواعدها وأنظمتها تمنع زوالها، كما تؤثر في صناع القرار لتعزيز التعاون الدولي وتوسيع التحالفات. **(بالة، 2012، الصفحات 54–55)**

2.الأمن السيبراني والفكر الاستراتيجي من منظور الليبيرالية المؤسساتية:

تفسر النظرية الليبيرالية المؤسساتية الأمن السيبراني انطلاقا من الطبيعة البنيوية للفضاء الرقمي بوصفه مجالاً عابرًا للحدود لا يُمكن تأمينه عبر السياسات الأحادية، إذ أن الترابط العالمي لشبكات الأنترنت يجعل الأمن فيه مسؤولية مشتركة تتجاوز القدرات المُنفردة للدول. **(singer & friedman, 2014, p. 168)**

وفي هذا السياق، يرسخ الاعتماد المتبادل الرقمي شبكة من المصالح المتقاطعة التي تنتج حوافز موضوعية للتعاون، حتى في ظل استمرار انعدام الثقة بين الفاعلين الدوليين. **(cavelty, 2019, p. 92)**

ومن ثم، يصبح اللجوء إلى المعايير الدولية، المؤسسات التنظيمية، وترتيبات الحوكمة مُتعددة الأطراف ضرورةً وظيفية لضبط السلوك السيبراني وتقليل احتمالات التصعيد، بما يعكس المنطق المؤسسي الذي يفترض إمكانية إدارة الفوضى الدولية عبر القواعد والأنظمة المشتركة.**(hansen & nissenbaum, 2010, p. 15)**

وعليه، فالأمن السيبراني وفق هذا المنظور لا يُفهم بوصفه مجالاً للصراع الصفري، بل كساحة يُعاد فيها إنتاج أنماط التعاون المؤسسي لتقليل عدم اليقين وتعزيز الاستقرار الدولي في البيئة الرقمية.

وبنفس المنطق المؤسسي الذي يُفسر ديناميات التعاون الدولي في الأمن السيبراني، تمتد تطبيقات النظرية الليبيرالية المؤسساتية إلى الفكر الاستراتيجي من خلال دور المؤسسات الدولية في تقليل تكاليف التنسيق وتنفيذ الاتفاقيات، وتوفير المعلومات اللازمة لدعم التعاون بين الدول. **(keohane & nye, 2012, p. 21)**

كما أن الاعتماد المتبادل بين مجالات متعددة من القضايا يخلق مصالح مشتركة تُحفز على تنسيق السياسات واتخاذ الإجراءات الاستراتيجية بشكل متكامل. **(keohane & nye, 2012, p. 21)**

وفي هذا الإطار، تشكل الأنظمة والمعايير الدولية السلوك الاستراتيجي من خلال تحديد توقعات واضحة حول كيفية استجابة الدول لبعضها البعض، بما يُسهم في تقليل المخاطر وتعزيز الاستقرار في البيئة الدولية.**(krasmer, 1989, p. 190)**

ومن ثم، يمكن فهم الفكر الاستراتيجي وفق هذا المنظور على أنه عملية مؤسسية تُنسق بين القدرات والسياسات والمصالح المشتركة لتحقيق الاستقرار والتعاون الدولي.

المطلب الثالث: النظريات الجيوبوليتيكية

تعد النظريات الجيوبوليتيكية إطارًا تفسيريًا يُبرز أثر الجغرافيا في تشكيل موازين القوة الدولية، من بين هذه النظريات نجد:

النظرية الأوراسية الجديدة: تشكلت الأوراسية الجديدة عند كإطار نظري جيوسياسي يهدف إلى تفسير موقع روسيا المركزي في قارة أوراسيا باعتباره ميزة استراتيجية حاسمة.

1.نشأة وأسس الأوراسية الجديدة:

وفق هذه النظرية، فإن القوة التي تُسيطر على قلب أوراسيا تستطيع تحقيق الهيمنة العالمية، وهو تصور يستند إلى تراث المدرسة الجيوسياسية الكلاسيكية. وقد أعاد إحياء هذا الطرح مفكرو الأوراسيين الجدد، على رأسهم "دوغين"، الذين انطلقوا من اعتبار أن الجغرافيا التاريخية والإرث الثقافي لروسيا يؤهلانها للاضطلاع بدور قيادي في الفضاء الأوراسي.

وقد تطورت هذه الرؤية لتؤكد أن بقاء روسيا كقوة فاعلة يقتضي الحفاظ على نفوذها داخل أوراسيا من خلال تبني توجه توسعي يعزز حضورها في القارة.

وترتكز هذه المقاربة على اعتبار أوراسيا مجالا جيوسياسيا مضادا للهيمنة الغربية؛ حيث إن تحقيق التكامل السياسي والاقتصادي والثقافي داخل القارة من شأنه تعزيز قدرة روسيا على التأثير في التوازن الدولي.**(kurnaz, 2024, pp. 347-377)**

2.الأمن السيبراني والفكر الاستراتيجي من منظور الأوراسية الجديدة:

تضع الرؤية الأوراسية الناشئة للأمن السيبراني الأمن الرقمي ضمن إطار جيوسياسي وقانوني أوسع. غالبًا ما تقوم القوى العظمى بتسييس المعايير القانونية والخطابات لتشكيل تنظيم الفضاء السيبراني وفق المصالح الاستراتيجية الإقليمية، وبينما لم تقم روسيا بعد بإنشاء قانون أوراسي دولي كامل وفعَّال للفضاء السيبراني؛ إلاَّ أنها وجهت الدول المُجاورة لتتوافق مع أهدافها الاستراتيجية.**(khasnova & simonyan, 2025, p. 24)**

يعالج النظام الأمني الأوراسي الجديد التهديدات الهجينة، بما في ذلك الحرب المعلوماتية، وتحديات الأمن الرقمي، والتدخل في العمليات الداخلية، وتسييس الأنظمة الاقتصادية والمالية.**(xiaoyum, 2025, pp. 1-2)**

وتعكس هذه التطورات إنشاء مُمارسات معيارية عبر المُنظمات الإقليمية مثل رابطة الدول المُستقلة، ومنظمة شنغهاي للتعاون، ومنظمة معاهدة الأمن الجماعي، والاتحاد الاقتصادي الأوراسي، مُمهِّدة بذلك الأساس لنظام قانوني إقليمي يحكم الفضاء السيبراني. **(khasanore & simonyan, p. 01)**

في حين تفسر الأوراسية الجديدة الفكر الاستراتيجي باعتباره أداة للحفاظ على الهوية الحضارية لروسيا وتعزيز تأثيرها في الشؤون العالمية.**(diec, 2024, p. 389)**

تصور الساحة الدولية على أنها صراع بين العالم الأطلسي ونظام أوراسي مُتمركز حول روسيا، مع التركيز على حماية التنوُّع الثقافي والوطني كقيمة استراتيجية. **(gasimov & laruelle, 2026, p. 06)**

وبدلا من تقديم تعليمات مباشرة، توفر أفكار "دوغين" إطارا رمزيًا يقوم الفاعلون المحليون بتكييفه لتوجيه القرارات السياسية والفكرية.**(dugin, 2022, p. 13)**

لقد أسهمت الرؤية الأوراسية في صياغة السياسات الاستراتيجية والمواقف السياسية الروسية؛ حيث تبرز دور الامبراطوريات كجهات فاعلة رئيسية في العلاقات الدولية، مدفوعة دائمًا بالسعي للتوسُّع والتنافس على الهيمنة الجيوسياسية.**(kurnaz, 2024, p. 377)**

نظرية قلب العالم:تعد نظرية قلب العالم لـ "ماكيندر" من أبرز النظريات الجيوبوليتيكية الكلاسيكية التي فسرت منطق الهيمنة العلمية انطلاقًا من المُحدد الجغرافي.

1.نشأة وأسس قلب العالم:

تعود نشأة نظرية قلب العالم إلى الجغرافي والسياسي البريطاني هالفورد ماكيندر، الذي عرضها في مقاله الشهير المعنون بـ {محور الارتكاز الجغرافي في تعاليم التاريخ}؛ حيث غَدَت أول نظرية عامة في الاستراتيجية الكبرى وتفسير توازنات القوى العالمية من منظور جغرافي. وقد تأسست هذه النظرية منذ بدايتها على تصور جيوبوليتيكي قاري يقوم على تقسيم العالم إلى ثلاث مجالات رئيسية؛ هي قلب الأرض الذي يشمل أوروبا الشرقية وروسيا الأوروبية والآسيوية، والجزيرة العالمية التي تضُم قارات العالم القديم: أوروبا، آسيا، إفريقيا ويجمعها البحر المتوسط، ثم الهلالان الداخلي والخارجي اللذان يُحيطان بالجزيرة العالمية ويُغلفانها جيوسياسيا.**(شارنرش، 2024، الصفحات 5-7)**

انطلاقا من هذا البناء النظري صاغ ماكيندر معادلته الجيوبوليتيكية الشهيرة التي تربط بين السيطرة على شرق أوروبا والهيمنة على قلب الأرض، ومن ثمَّ السيطرة على الجزيرة العالمية وصولا إلى التحكم في العالم، وهو ما يعكس الطبيعة التأسيسية للنظرية اعتبارها إطارًا تفسيريًا شاملاً للعلاقة بين الجغرافيا والقوة العالمية.**(شارنرش، 2024)**

2.الأمن السيبراني والفكر الاستراتيجي من منظور قلب العالم:

انطلاقا من التصور الجيوبوليتيكي الذي طرحه هالفورد ماكيندر، تقوم نظرية قلب العالم على مركزية المجال الجغرافي في تحديد موازين القوة الدولية؛ حيث يُعدُّ "القلب" مركز الثقل الذي يمنح الدولة القُدرة على التأثير والهيمنة. غير أن التحولات التكنولوجية تؤكد أن التطور الرقمي أعاد تشكيل مفهوم المجال الجيوبوليتيكي، بحيث لم يعد محصورا في الإقليم المادي، بل امتد ليشمل الفضاء السيبراني باعتباره إقليمًا جديدًا في النظام الدولي. وعليه، يمكن تحليل الفضاء السيبراني في ضوء نظرية قلب العالم من خلال إعادة تعريف "القلب" بوصفه مركزًا رقميا للقوة، يتمثل في البنية التحتية المعلوماتية وشبكات الاتصال وتدفقات البيانات. فكما ارتبطت السيطرة في التحليل –الكلاسيكي– بالتحكم في المجال الجغرافي المحوري، أصبحت ترتبط اليوم القدرة على حماية المجال السيبراني وتأمينه. **(عمر، 2025)**

من جهة أخرى، تظل نظرية قلب العالم لماكيندر مُؤثرة في الفكر الاستراتيجي الحديث، ولا سيما عند تحليل الجغرافيا السياسية لأوراسيا وتنافس القوى الكبرى، إذ أصبح هذا الإطار التحليلي مرجعًا أساسيًا لفهم كيفية توزيع النفوذ والهيمنة بين الدول الكبرى. **(sloan, 2017, p. 583)**

تمثل هذه النظرية أداة فعَّالة لدراسة الأهمية الاستراتيجية للمناطق المركزية في أوراسيا؛ حيث تلعب هذه التضاريس دورًا محوريًا في ديناميات صراع القوى الكبرى وتشكيل موازين القوة الدولية. (flint, 2006, p. 47)

وتجسد رؤية ماكيندر إدراكا بأن المنطقة المحورية تشكل الارتفاع الاستراتيجي في السياسة الدولية، فهي مقاومة للسيطرة البحرية وتشكل مركز القوة القارية، ما يجعلها محورا رئيسيا لفهم آليات الهيمنة والصراع.(sloan, 2017, p. 83)

علاوة على ذلك، يرى ماكيندر أن السيطرة على قلب العالم ليست مجرد غزو إقليمي، بل تشكل مفتاحا للتأثير على هياكل القوة العالمية وإمكانية إحباط الهيمنة البحرية لمنافسي القوى الكبرى، ما يجعلها حجر الزاوية في استراتيجيات الدول الطامحة للنفوذ العالمي. **(toksoz & zengin, 2018, p. 99)**

الشكل رقم 05: النظريات المُفسِرة للأمن السيبراني والفكر الاستراتيجي

المصدر: إعداد الطالبة

خلاصة الفصل:

تأسست مخرجات هذا الفصل على ضرورة بناء قاعدة تحليلية صلبة تبدأ من ضبط المفاهيم؛ حيث استنتج أن "مفهوم الأمن السيبراني" ليس مجرد مصطلح تقني جامد، بل هو مفهوم ديناميكي تطور أكاديميا مع توسع تكنولوجيات الإعلام والاتصال. فقد أفرز هذا السياق الرقمي الجديد منظومة مفاهيمية متكاملة تشمل الفضاء السيبراني، الهجمات الرقمية، وهي مفاهيم تعكس في جوهرها تحول التهديدات الأمنية المعاصرة من طابعها المادي الملموس إلى أبعاد افتراضية معقدة تتجاوز الحدود التقليدية للدول.

وفي سياق متصل، أكدت الدراسة أن هذا التحول المفاهيمي استوجب معالجة نظرية عميقة ضمن حقل الدراسات الأمنية؛ حيث برز الفكر الاستراتيجي كأداة لا غنى عنها لتحليل البيئة الدولية المتغيرة وفهم التهديدات التكنولوجية المستجدة. ومن خلال اسقاط النظريات الكبرى في العلاقات الدولية على هذا المجال، يتضح أن الفضاء السيبراني أصبح مسرحا جديدا لتوازنات القوى؛ فبينما تفسر المقاربة الواقعية هذا الفضاء بوصفه أداة للصراع والهيمنة، تراهن المقاربات الليبيرالية المؤسساتية على التعاون المؤسساتي كسبيل وحيد للحد من مخاطره. وتأسيسا على ذلك، نخلص إلى أن الأمن السيبراني قد أضحى المتغير الأكثر تأثير في إعادة صياغة السياسات الأمنية الدولية، مشكلا بذلك أحد أهم المجالات الاستراتيجية التي تتقاطع فيها رهانات القوة والتنافس بين الفاعلين الدوليين في العصر الراهن.

الفصل الثاني

التهديدات السيبرانية في الحرب الروسية – الأوكرانية 2025/2014

الفصل الثاني: التهديدات السيبرانية في الحرب الروسية – الأوكرانية2014/2025

يشكل تصاعد التهديدات السيبرانية في الحرب بين روسيا وأوكرانيا منذ سنة 2014 تحوُّلاً نوعيًا في طبيعة الصراعات المعاصرة؛ حيث لم يعد الفضاء السيبراني داعمًا للعمليات العسكرية فحسب، بل أصبح ساحة مواجهة قائمة بذاتها تؤثر في مسار الحرب ونتائجها الاستراتيجية.

قد تداخلت الأدوات الرقمية مع الحسابات الجيوبوليتيكية، وتحولت الهجمات السيبرانية إلى وسيلة لإعادة تشكيل موازين القوة، استنزاف القدرات، والتأثير في المجالين السياسي والاقتصادي، بما يعكس بروز نمط من الحروب الهجينة التي تجمع بين القوة الصلبة والرقمية في آنٍ واحد. في هذا السياق التحليلي، يهدف هذا الفصل إلى دراسة التهديدات السيبرانية في الحرب الروسية – الأوكرانية خلال الفترة ما بين 2014–2025، عبر مقاربة تدمج بين البعد الجيوبوليتيكي والتحليل الاستراتيجي ورصد الانعكاسات الإقليمية.

بناء على هذا التصور المنهجي، جاء هذا الفصل موزعًا على ثلاثة مباحث رئيسية؛ يتناول المبحث الأول دراسة جيوبوليتيكية لمسار الحرب الروسية – الأوكرانية 2014–2025، من خلال ثلاثة مطالب تتمثل في مراحل تطور الحرب، أسبابها، ثم الآثار المرحلية المُترتبة على الدولتين المُتنازعتين، أما المبحث الثاني فيُعالج الاستراتيجيات السيبرانية المُعتمدة في الحرب؛ حيث خُصص المطلب الأول لعرض الاستراتيجية الروسية في الفضاء السيبراني، بينما تناول المطلب الثاني الاستراتيجية الأوكرانية في المجال ذاته. في حين يُركز المبحث الثالث على تداعيات الحرب السيبرانية الروسية – الأوكرانية على الأمن الإقليمي، وذلك عبر دراسة الهجمات الرقمية في المجال العسكري، ثم المجال السياسي، وأخيرًا في المجال الاقتصادي والاجتماعي، بما يتيح تقديم رؤية تحليلية مُتكاملة لطبيعة التهديدات السيبرانية وآثارها متعددة المستويات.

المبحث الأول: دراسة جيوبوليتيكة لمسار الحرب الروسية – الأوكرانية 2014-2025

يعد تحليل المسار الجيوبوليتيكي للحرب بين روسيا وأوكرانيا مدخلا ضروريا لفهم طبيعة التحولات التي عرفها هذا الصراع منذ سنة 2014، باعتبار أن تفاعلاته لم تكن عسكرية فحسب، بل ارتبطت بإعادة ترتيب موازين القوة في المجال الإقليمي وتداخل الاعتبارات الجغرافية بالأبعاد الأمنية والاستراتيجية.

انطلاقًا من ذلك، يتناول هذا المبحث دراسة جيوبوليتيكية لمسار الحرب الروسية – الأوكرانية خلال الفترة 2014–2025، من خلال عرض مراحل تطورها، تحليل أسباب اندلاعها، ثم بيان آثارها المرحلية على الدولتين المتنازعتين، بما يُوفر إطارا تفسيريا عاما لفهم ديناميات الصراع في سياقه الشامل.

المطلب الأول: مراحل تطور الحرب الروسية – الأوكرانية 2014–2025

بدأت الحرب الروسية الأوكرانية عام 2014 كتعبير عن تصاعد التوترات الإقليمية والدولية في المنطقة، وقد شهدت تحولات استراتيجية وأمنية متعددة على مدى سنوات متتالية. لفهم ديناميكيات هذا النزاع، يُمكن تقسيم مساره إلى خمس مراحل أساسية:

المرحلة الأولى: ضم جزيرة القرم واندلاع حرب دونباس فيفري 2014: تبلور أحدث أوجه الصراع بين روسيا والغرب في سياق الأزمة الأوكرانية لعام 2014، والتي شكلت نقطة انطلاق مرحلة جديدة من التوترات بين الطرفين. فقد جاءت هذه التطورات عقب احتجاجات "اليوروميدان" التي شهدتها أوكرانيا، وما أعقبها من إقصاء الرئيس الأوكراني فيكتور يانوكوفيتش من السلطة. وفي خضم هذه التحولات السياسية الداخلية، أقدمت روسيا في مارس/آذار 2014 على ضم شبه جزيرة القرم، في خطوة كان لها أثر بالغ في إعادة تشكيل مسار العلاقات الروسية–الغربية.

ولم يتوقف الأمر عند حدود ضم القرم، إذ أعقب ذلك إعلان جماعات انفصالية موالية لروسيا في شرق أوكرانيا استقلالها، وهو ما أفضى إلى اندلاع نزاع مسلح بين القوات الأوكرانية وهذه الجماعات المدعومة من روسيا. وبهذا المعنى، لم تعد الأزمة الأوكرانية مجرد حدث عابر، بل تحولت إلى منعطف مفصلي لتدخل في مرحلة جديدة اتسمت بتصاعد التوتر والمواجهة. **(taraskuzior & paul, 2018, p. 03)**

المرحلة الثانية: الجمود النسبي واتفاقيات مينسك 2015-2021: في عام 2015، تم توقيع اتفاقيتي مينسك الأولى والثانية، بهدف وقف الأعمال العدائية وتوفير إطار سياسي للحل الشامل للنزاع. ورغم توقيع الاتفاقيات، استمرت الاشتباكات المُتفرقة والمُتقطعة في مناطق دونيتسك ولوهانسك، ما أظهر محدودية قدرة الاتفاقيات على خلق هدنة فعالة. وفي الوقت ذاته، بدأ الجيش الأوكراني تدريجيًا تحسين تنسيقه وكفاءته الدفاعية، إلا أن السيطرة الإقليمية ظلت أغلبها بيد القوات الانفصالية. خلال الفترة المُمتدة من 2016 حتى 2021، استمرت الاشتباكات منخفضة الكثافة، وبرزت انتهاكات مُتكررة للهدنات المعلنة، مع تبادل الاتهامات بين الطرفين حول الاستفزازات والانتهاكات. واستمرت روسيا في دعم الانفصاليين، عبر تقديم الدعم اللوجستي والاستخباراتي، ونشر وحدات شبه عسكرية عند الحاجة، ممَّا أدى إلى استمرار حالة الجمود العسكري والسياسي في المنطقة.**(h.yasui & h, 2025, pp. 75-78)**

المرحلة الثالثة: الغزو الروسي الشامل 24 فيفري 2022: في 24 فبراير 2022، شنت روسيا غزوًا شاملاً لأوكرانيا، مُستهدفة عدة مدن رئيسية منها كييف، خاركيف، وماريوبول، بالإضافة إلى المناطق الجنوبية. وحاولت القوات الروسية تطويق المدن الكبرى بسرعة؛ لكن التحديات اللوجستية، وقوة الدفاع الأوكراني، بالإضافة إلى العقوبات الدولية المفروضة على روسيا، أثرت على تقدُّم العمليات العسكرية. شكل هذا الغزو تحولاً جوهريًا في طبيعة النزاع، من صراع مُجمَّد إلى حرب دولية مفتوحة.**(h.yasui & h, 2025, pp. 90-92)**

المرحلة الرابعة: الهجوم المضاد والتوازن العسكري 2022–2024: من منتصف 2022 فصاعدًا، بادرت القوات الأوكرانية بشن هجمات مُضادة في مناطق خاركيفوخيرسون، مما أدى إلى استعادة الأراضي في عدة مُقاطعات. وفي هذه المرحلة، دخلت الحرب في حالة استنزاف مع وُقوع خسائر بشرية كبيرة، واستمرار الاشتباكات المحلية على طول خطوط الجبهة. واصلت روسيا تعزيز مواقعها في الأراضي التي احتلتها، بينما تلقَّت أوكرانيا دعمًا عسكريًا متزايدًا من حلفائها الغربيين. وأُجريت محاولات متفرقة للتفاوض على وقف إطلاق النار؛ لكنها لم تُؤدِّ إلى أي تسوية دائمة بحلول أكتوبر 2024.**(h.yasui & h, 2025, pp. 95–98)**

المرحلة الخامسة: حصيلة الحرب الروسية–الأوكرانية لعام 2025: شهد عام 2025 ترسيخ القوات الروسية سيطرتها على مناطق دونباس ولوجانسك، بينما احتفظت القوات الأوكرانية ببعض الجيوش شمالا وغربا، مع تكبدها خسائر عسكرية كبيرة مقارنة بالعام السابق. واستمر استخدام الطائرات المسيرة وأنظمة الصواريخ الدقيقة دون تغيير ملموس في خطوط السيطرة.

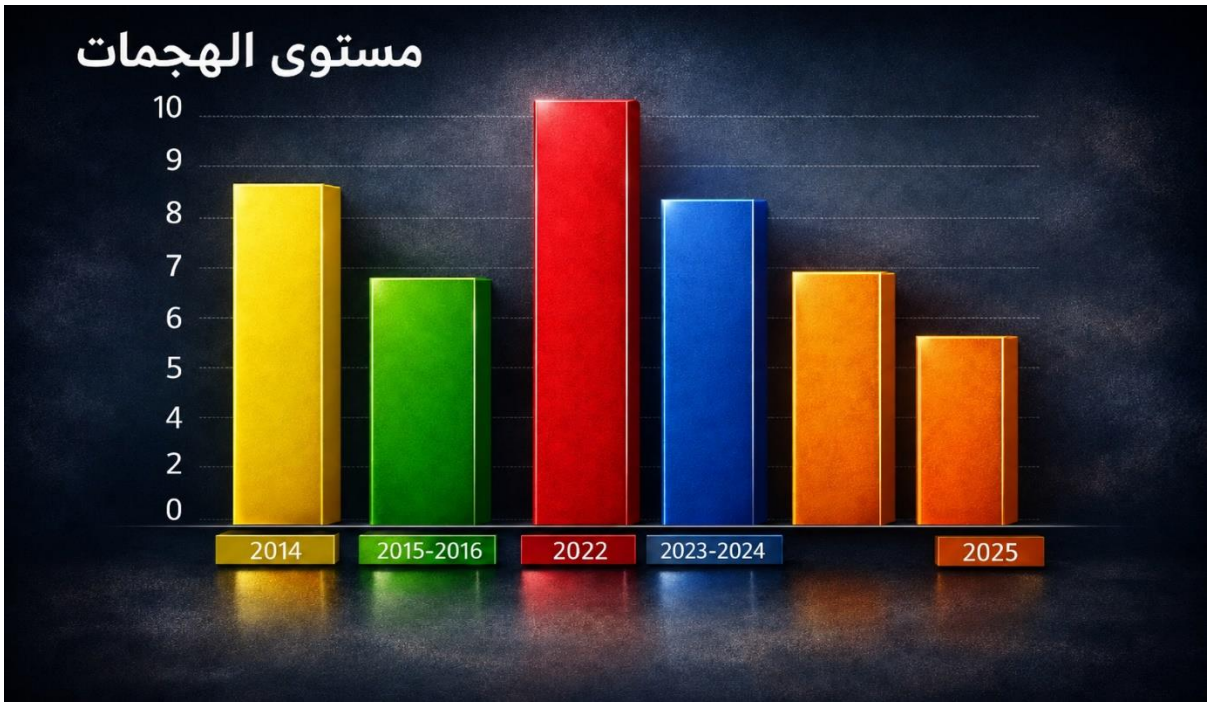
على الصعيد السياسي لم يتم التوصل إلى أي اتفاق سلام شامل خلال العام، واستمرت العقوبات الغربية على روسيا دون تخفيف، في حين رفضت أوكرانيا التنازل عن الأراضي المحتلة.

أما من الناحية البشرية والمادية، فقد أسفرت الحرب عن آلاف القتلى والجرحى، مع أضرار كبيرة للبنية التحتية في المناطق الشرقية، فيما تأثرت روسيا جزئيًا بالعقوبات على صادرات الطاقة لكنها حافظت على استقرار نسبي في اقتصادها بفضل إعادة توجيه الصادرات.

إقليميًا ودوليا، أدت الحرب إلى ارتفاع أسعار الطاقة والغذاء في أوروبا، واستمر الدعم الغربي لأوكرانيا؛ لكنه لم يكن كافيًا لتحرير السيطرة على المناطق الشرقية، كما بقيت العلاقات بين روسيا والدول الغربية مُتوترة مع استمرار عزلة روسيا في بعض المُؤسسات الدولية.**(الوائلي، مركز حمورابي للبحوث، 2026)**

تعكس مراحل تطور الحرب الروسية–الأوكرانية2014–2025 عن تصاعد تدريجي من نزاع محدود إلى حرب شاملة ثم إلى صراع استنزاف طويل، بدءا بضم القرم ودونباس، مُرورًا بجمود نسبي ضمن اتفاقيَّات مينسك، ثمَّ الغزو الشامل عام 2022، وما تبعه من هجوم مُضاد وتوازن عسكري نسبي، وصولا إلى حصيلة عام 2025 التي تؤكد غياب الحسم واستمرار تعقيد المشهد بما يعكس تداخل الأبعاد العسكرية، السياسية، والجيوسياسية في صراع مفتوح على أبعاد متعددة.

الشكل رقم 06: تطور الهجمات العسكرية في الحرب الروسية الأوكرانية 2014–2025



المصدر: إعداد الطالبة

يظهر المخطط تذبذبا في كثافة الهجمات العسكرية ضمن الصراع الروسي–الأوكراني بين عامي 2014 و2025؛ حيث بلغت الهجمات ذروتها القصوى عام 2022 بالتزامن مع الغزو الشامل، تلاها منحنى تراجعي تدريجي في السنوات اللاحقة وفقا للتقديرات المدروسة في المخطط البياني.

المطلب الثاني: أسباب الحرب الروسية الأوكرانية 2014-2025

تمثل الحرب بين روسيا وأوكرانيا 2014-2025 أحد أبرز الصراعات المُعاصرة التي نتجت عن تداخل مجموعة من العوامل المتشابكة. فلم يكن اندلاعها نتيجة سبب واحد بل جاء نتيجة تراكم أسباب متعددة شملت أبعادًا سياسية، عسكرية، أمنية، جيوسياسية، واجتماعية.

تتدرج وفق ما يلي:

1.الأسباب السياسية: ترتبط الأسباب السياسية للحرب الروسية-الأوكرانية بمجموعة من التوترات المتراكمة في العلاقات بين روسيا والغرب، منها:

- اعتقاد روسيا ان الدول الغربية أخلَّت بالوعود التي قُدمت للاتحاد السوفياتي بعد نهاية الحرب الباردة، خاصَّة فيما يتعلَّق بعدم توسُّع حلف الشمال الأطلسي شرقًا نحو الحدود الروسية، وهو ما اعتبرته موسكو تهديدًا مباشرًا لمصالحها الأمنية.
- استمرار توسُّع حلف الشمال الأطلسي بعد تفكُّك الاتحاد السوفياتي وضم عدد من دوَّل أوروبا الشرقية ودوَّل مجاورة لروسيا، الأمر الذي أدى إلى تزايد التوتر بين روسيا والغرب مع اقتراب البنية العسكرية للحلف من الحدود الروسية.
- تصاعد التوتر بشكل أكبر بعد إعلان قمة بوخارست سنة 2008 إمكانية انضمام كل من أوكرانيا وجورجيا إلى حلف الناتو مُستقبلاً، وهو ما اعتبرته روسيا خطوة تُهدِّد توازن القوى الإقليمي وتُعمِّق المُواجهة السياسية بينها وبين الغرب. **(katchanovski, 2026, pp. 31-32)**

2.الأسباب الجيوسياسية: تعود الأسباب الجيوسياسية للحرب الروسية-الأوكرانية أساسًا إلى الصراع على النفوذ الاستراتيجي في أوراسيا بين روسيا والغرب، لا سيما فيما يتعلَّق بتوسُّع الناتو وضم أوكرانيا للغرب؛ حيث يمكن إجمالها في:

- توسُّع الناتو شرقًا بعد انهيار الاتحاد السوفياتي اعتُبر من قِبل موسكو تدخُّلاً مُباشرًا في نفوذها الجيوسياسي، وقد استغلَّت القوى الغربية فترة ضُعف روسيا إلى التسعينيات لتعزيز وجودها في أوروبا الشرقية، ما شكَّل أساسًا للتوترات الجيوسياسية بين روسيا والغرب.
- اعتبرت موسكو تحويل أوكرانيا إلى عضو في الاتحاد الأوروبي وحلف الناتو تهديدًا وُجوديًا مُباشرًا لأمنها القومي، إذ يُشكِّل ذلك معقلاً غربيًا على حدودها.
- تُمثل الحرب صراعًا جيوسياسيًا بين روسيا والقوى الغربية على السيطرة على الفضاء الاستراتيجي في أوراسيا؛ حيث تجاوز النزاع حدود العلاقة الثنائية بين روسيا وأوكرانيا ليُصبح جزءً من مُنافسة كبرى بين القوى العالمية على النفوذ الإقليمي. **(mohammed & danish, 2024, pp. 31-33)**

3.**الأسباب العسكرية:** ترتبط الأسباب العسكرية للحرب الروسية-الأوكرانية بتطوُّر الصراع المُسلَّح في شرق أوكرانيا منذ عام 2014؛ حيث لعبت العمليات العسكرية والدعم الخارجي دورًا مهمًا في تصعيد النزاع، تتجسَّد هذه الأسباب في:

- ارتبط استمرار الكيانات الانفصالية في دونيتسك ولوهانسك بدرجة الدعم العسكري والمادي الذي وفرته روسيا، وهو ما ساعد هذه الكيانات على الاستمرار في مواجهة القوى الأوكرانية.
- أدى التدخُّل العسكري الروسي في معركة إيلوفايسك 2014 إلى تغيير مسار العمليات العسكرية وإلحاق خسائر كبيرة بالقوات الأوكرانية، الأمر الذي دفع القيادة الأوكرانية إلى البحث عن تسوية للصراع.
- ساهمت المعارك الحاسمة في إقليم دونباس في تعزيز موقع القوات المدعومة من روسيا وإضعاف القُدُرات العسكرية الأوكرانية، ممَّا أدى إلى استمرار الصراع المُسلَّح في المنطقة.**(wilson, 2017, pp. 105-127)**

4.الأسباب الأمنية: ترتبط الأسباب الأمنية للحرب الروسية–الأوكرانية بجملة من العوامل الاستراتيجية التي تطوَّرت مُنذ اندلاع حرب دونباس عام 2014، أبرزها:

- أدى التدخُّل الروسي في النزاع إلى تصعيد الصراع الأمني وإضعاف فرص التسويَّة المُبكرة، بعدما اعتُبر جزءً من صراع إقليمي أوسع مرتبط بالمصالح الاستراتيجية لروسيا في محيطها الجغرافي.
- استمرار الصراع غير المحسوم منذ عام 2014 أدى إلى تطوُّره تدريجيًا نحو مُواجهة عسكرية أوسع تُوِّجت بالغزو الروسي الشامل لأوكرانيا عام 2022.
- أدت الخسائر العسكرية الكبيرة للطرفين بعد عام 2022 إلى ظهور حالة من الجمود العسكري النسبي واستمرار الصراع بدعم دولي خاصَّة من الدوَّل الغربية لأوكرانيا. **(h.yasui & h, 2025, pp. 72–79)**

5.الأسباب الاجتماعية: تعود بعض أسباب الحرب الروسية–الأوكرانية إلى عوامل اجتماعية داخل المجتمع الأوكراني، من ضمنها:

- اتسمت منطقة دونباس تاريخيا بالشك تجاه النزعة القومية التي برزت في المناطق الغربية من أوكرانيا، خاصة بعد أحداث يوروميدان وما ترتب عليها من تغيرات سياسية.
- عانت المنطقة من هيمنة شبكات محلية من النخب الاقتصادية والسياسية المرتبطة بالفساد، وهو ما ساهم في تعميق الفجوة بينها وبين الحكومة المركزية في كييف.
- أدى تدهور الصناعات الأساسية مثل الفحم والصلب والكيماويات إلى تراجع الأوضاع الاقتصادية والاجتماعية في المنطقة، وهو ما ساعد على زيادة حالة الاستياء وعدم الاستقرار. **(wilson, 2017, pp. 124–127)**

تبرز أسباب الحرب الروسية الأوكرانية 2014–2025 من خلال تداخل مجموعة من العوامل المتشابكة؛ حيث لعبت الدوافع السياسية دورا في صراع الشرعية وتوجهات الحُكم، إلى جانب اعتبارات جيوسياسية مرتبطة بتوازن القوى والنفوذ الإقليمي، مدعومة بعوامل عسكريَّة تتعلَّق

بسباق التسلح وإعادة التموضع الاستراتيجي، وأخرى أمنية تتصل بإدراك التهديدات وضمان الحدود، فضلا عن أسباب اجتماعية انعكست في التباينات الداخلية والانقسامات، مما يوضح أن الحرب لم تكن نتيجة سبب واحد بل حصيلة تفاعل مركب لهذه العوامل.

الشكل رقم 07: أسباب الحرب الروسية–الأوكرانية 2025/2014

المصدر: إعداد الطالبة

المطلب الثالث: الآثار المرحلية للحرب الروسية-الأوكرانية على الدولتين المتنازعتين

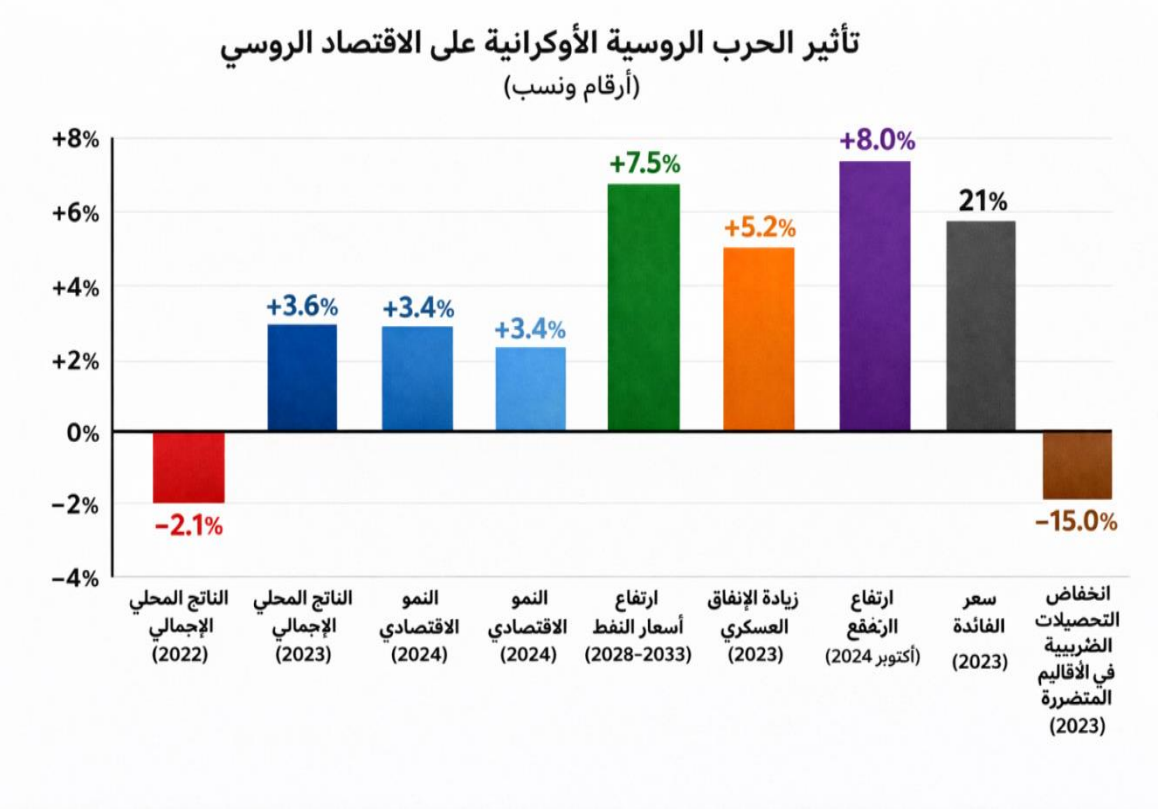
برزت الحرب الروسية-الأوكرانية كواحدة من أبرز النزاعات الإقليمية في العصر الحديث، وأسفرت عن تداعيات ملموسة على المُستوى السياسي، الاقتصادي، والاجتماعي لكلا الطرفين. حيث سيتم دراسة في هذا المطلب الآثار المرحلية لهذه الحرب لكل دولة على حدة، كونها حرب لازالت مستمرة.

أولا: الآثار المرحلية للحرب على دولة روسيا: شهدت روسيا مُنذ اندلاع الحرب الروسية-الأوكرانية تحوُّلات ملحوظة مسَّت مختلف المجالات؛ لاسيَّما الجوانب الاقتصادية، العسكرية، الاجتماعية، نتيجة الضغوط الداخلية والخارجية التي فرضها مسار الصراع، وفق ما يلي:

1.المجال الاقتصادي: مع بدء الغزو الروسي في فبراير 2022، تعرَّض الاقتصاد الروسي لصدمات مالية وتجارية وحالة من عدم اليقين إلا أن الناتج المحلِّي الإجمالي انخفض بنسبة 2.1 بالمئة فقط، مدعومًا بارتفاع إيرادات الصادرات النفطيَّة وارتفاع أسعار النفط، وإغلاق ميزانية 2023 بعجز أقل من المُتوقَّع مع إعادة توجيه التجارة. تَركَّز النمُو أساسًا على النشاط العسكري وزيادة الرواتب، فيما شهِدت أقاليم النفط والغاز والمُدُن الكُبرى استفادة، بينما تكبَّدت أقاليم الخُطوط الأمامية ومناطق المعادن والأقاليم النائية خسائر كبيرة في التحصيلات الضريبية، كما أثر انسحاب شركات السيارات على الإنتاج في كالوغا وكالينينغراد. **(yushkov & micheal, 2024, pp. 03-07)**

في هذا السياق تباطأ الاقتصاد الروسي إلى 3.4 بالمئة في 2024، قبل أن ينخفض أكثر في 2025 ليصل إلى 3.1 بالمئة مدفوعًا بالإنفاق العسكري وجهود الاستبدال المحلي رغم العقوبات، مع استمرار القيود الإنتاجية ونقص العمالة. **(2025, pp. 61-62)**

الشكل رقم 08: تأثير الحرب الروسية–الأوكرانية على الاقتصاد الروسي



المصدر: إعداد الطالبة

نقلا عن: Yushkov Andrey, Micheal Alesceev, Fiscale and economic effects of the Russo–Ukranian war, 2024.

يعكس التباين الصارخ بين نمو الناتج المحلي الإجمالي بنسبة 3.6 بالمئة والانكماش الحاد في التحصيلات بنسبة 15– بالمئة اقتصادا يعاني من اختلالات هيكلية عميقة وتفاوت إقليمي حاد. كما تشير معدلات الفائدة المُرتفعة عند 21 بالمئة مع تضخم بنسبة 8 بالمئة إلى ضغوط نقدية هائلة تحاول كبح جماح السيولة المتدفقة من الانفاق العسكري المُتسارع.

2.المجال العسكري: ترتبت على الحرب الروسية–الأوكرانية آثار عسكريَّة مُتباينة على الدولة الروسية؛ ففي سنة 2022 انتقلت موسكو من التلويح بالمُناورات إلى تفعيل "الردع الخشن"

ببدء العملية العسكرية لفرض واقع أمني جديد، لتواجه في سنة 2023 تداعيات "حرب استنزاف" التي فرضت إعادة هيكلة جذرية لاستراتيجياتها الميدانية.**(البلعزي، 2024، الصفحات 1490-1491)**

وبحلول سنة 2024، تعمق الأثر العسكري من خلال زيادة الاعتماد على الكثافة المادية المرتفعة، وصولا إلى سنة 2025التي تجلّت فيها الآثار عبر تبنِّي تكتيكات "الالتفاف العمليَّاتي" وتطويع المناخ لتحييد المسيرات، مع بروز معضلة استدامة الزخم نتيجة الاختلال الحاد بين حجم الخسائر البشريَّة والمكاسب الإقليمية المحدودة. **(russian of fensive compaign assessment:strategic shifts and tacticakal progress in the zaporizhia and donetsk directins, 2025)**

3.المجال الاجتماعي: تجسدت تداعيَّات الاقتصاد الحربي في روسيا في جملة من التحوُّلات الاجتماعية؛ حيث أفضت إلى ارتفاع معدَّلات التضخُّم وتراجُع الأُجور والقُدرة الشرائية، فضلاً عن أزمة سيولة ماليَّة في القطاع المصرفي. كما فرضت السيَّاسات المُرتبطة بالحرب ضُغوطًا إضافيَّة على العُمَّال من خلال تقليص الإجازات المدفوعة، إطالة ساعات العمل، فرض العمل الإضافي، إلى جانب اعتماد نظام العمل المُتواصل أو العمل لستة أيَّام أُسبُوعيًا. وفي سيَّاق متصل، برز عجز كبير في اليد العاملة يقدر بين 140.000 و400.000 عامِل؛ أي ما يقارب 20 بالمئة من إجمالي العاملين في القطاع الصناعي العسكري، وهو ما يعكس اختلالاً هيكليًا في سوق العمل. ويُضاف إلى ذلك نُقص حاد في الكفاءات المُؤهلة؛ حيث لا يتمثَّل الإشكال في الكم بل في نوعيَّة العمالة، في ظل هيمنة فئة عُمريَّة مُتقدِّمة، إذ يتجاوز متوسَّط أعمار العاملين في القطاع 70 سنة.**(boulegue, 2025, pp. 04-07)**

الشكل رقم 09: الآثار الاجتماعية للحرب الروسية–الأوكرانية على دولة روسيا

المصدر: إعداد الطالبة

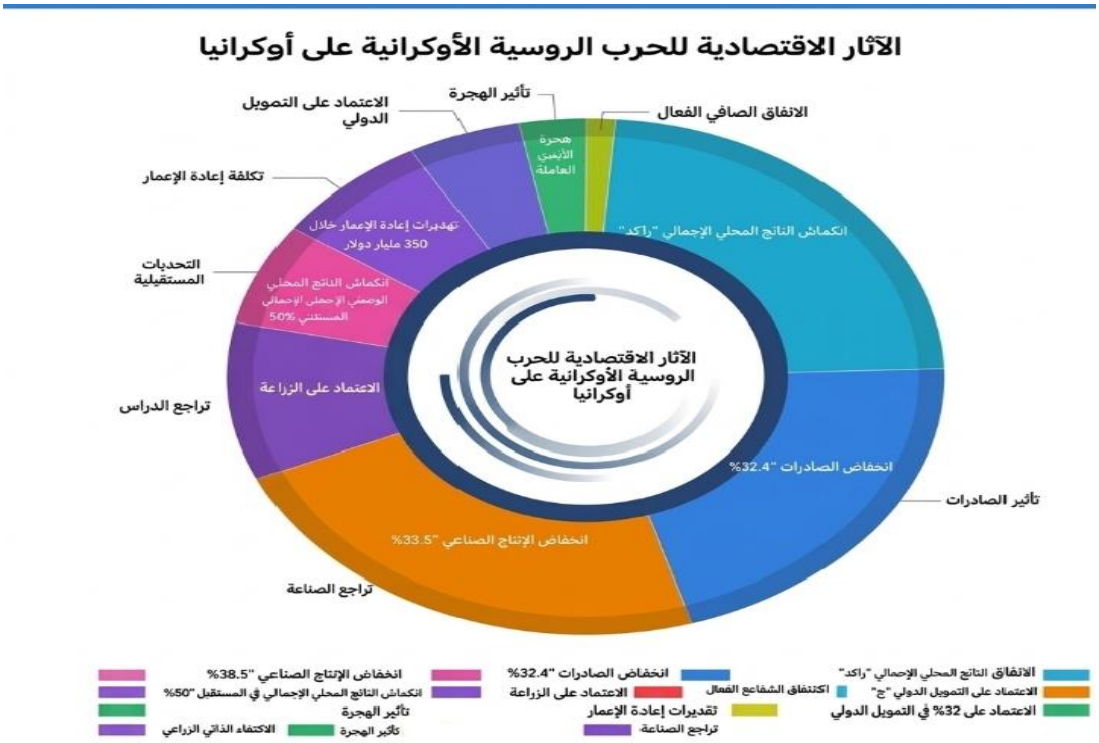
نقلا عن: Boulegue Mathieu, Russia's struggle to modernize its military industry: How sanctins, war and innovatin stagnation are weakning moscow's capabilities, 2025.

يكشف التذبذب الحاد في المؤشرات الاجتماعية عن أزمة عمالة خانقة؛ حيث وصل العجز في الكفاءات إلى 400 ألف عامِل، مع نقص بنسبة 20 بالمئة في القطاع العسكري الصناعي تحديدا. كما يتسبب الارتفاع المستمر في التضخم بنسبة 10.9 بالمئة في تآكل القدرة الشرائية للمواطنين، مما دفع الدولة لإطالة ساعات العمل وتخفيض الإجازات بنسبة 16.5 بالمئة لتعويض النقص الحاد في الإنتاجية.

ثانيًا: الآثار المرحليَّة للحرب على دولة أوكرانيا: رغم امتداد تداعيَّات الحرب الروسية–الأوكرانية في أوكرانيا لتشمل مختلف جوانب الدولة؛ إلاَّ أنَّ حدَّتها تجلَّت بشكل مباشر وعميق في المجال الاقتصادي، العسكري، الاجتماعي، من خلال:

1.المجال الاقتصادي: استمر تدهوُر الميزان التجاري الأوكراني ليصل العجز إلى ذُروته عام 2023 بقيمة 27.3 مليار دولار نتيجة انخفاض الإنتاج في الأقاليم الأماميَّة. وبحلول عامي 2024 و2025، تم تحول هيكلي دائم؛ حيث استقر الاعتماد على القطاع الزراعي كمصدر رئيسي للصادرات بنسبة 32.4 بالمئة، بينما واجهت الصناعات المعدنيَّة والثقيلة تراجُعًا مستمرًا. كما تنظر الرؤية لسنة 2026 إلى ضرورة تحديث قدرات الإنتاج وتنويع العلاقات التجاريَّة الخارجيَّة كجزء من استراتيجية التعافي بعد الحرب، مع الإشارة إلى أن استقرار العملة الوطنيَّة ظلَّ مرهُونًا بالتمويل الدوَّلي والقُيود على حركة رأس المال حتى هذه الفترة. **(saeidah, 2026, pp. 05-08)**

الشكل رقم 10: الآثار الاقتصادية للحرب الروسية–الأوكرانية على دولة أوكرانيا



المصدر: إعداد الطالبة

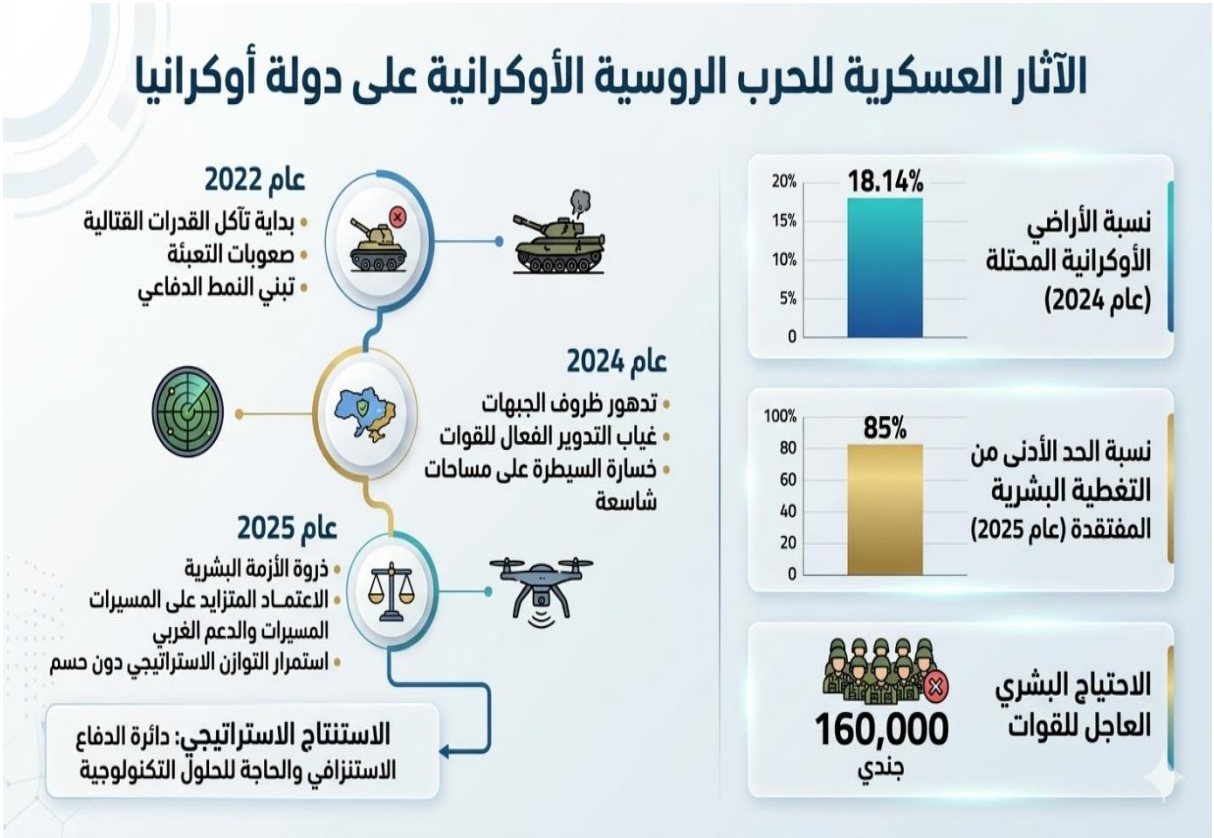
نقلا عن: Saeidah Almuzoughi, Socio- Economic consequences of the Russian- Ukrainian war, 2026.

يشير الانكماش الحاد في الصادرات بنسبة 32.4 بالمئة وتراجُع الإنتاج الصناعي بنسبة 33.5 بالمئة إلى انهيار واسع في القواعد الإنتاجيَّة التقليدية للاقتصاد الأوكراني تحت وطأة الحرب. كما تضع تقديرات إعادة الإعمار البالِغة 350 مليار دولار والاعتماد المُتزايد على التمويل الدولي ضُغوطًا هائلة على الاستدامة الماليَّة المُستقبليَّة، وسط نزيف حاد في القوى العامِلة نتيجة الهِجرة.

2.المجال العسكري: منذ عام 2022، شهدت أوكرانيا بداية تآكل قدراتها القتالية نتيجة الاستنزاف وصُعوبات التعبئة، ممَّا دفعها إلى تبني نمط دفاعي لإبطاء التقدُّم الرُّوسي، ومع

استمرار الحرب تصاعدت الضغوط العسكريَّة في عام 2024؛ حيث بلغت نسبة الأراضي المُحتلَّة نحو 18.14 بالمئة بالتوازي مع تدهوُر ظُروف الجبهات واستمرار القِتال دون تدوير فعَّال للقوَّات، وبحلول عام 2025 بلغت الأزمة البشريَّة ذُروتها، إذ احتاجت كييف إلى نحو 160 ألف جُندي لتحقيق حد أدنى من التَّغطيَّة بنسبة 85 بالمئة، وهو ما دفعها إلى الاعتماد المُتزايد على الدعم الغربي و الطائرات بدون طيَّار لتعويض النُّقص البشري، ومع ذلك لم تؤدِّ هذه الجهود إلى أي تغيير حاسم في ميزان القوى الاستراتيجي، ما يعكس استمرار الصراع في دائرة الدفاع الاستنزافي وضرورة اللجوء إلى حلول تكنولوجية لتعويض القُيود البشريَّة. **(cobo, 2025, pp. 05-08)**

الشكل رقم 11: الآثار العسكرية للحرب الروسية-الأوكرانية على دولة أوكرانيا



المصدر: إعداد الطالبة

3.المجال الاجتماعي: تطوَّرت الأزمة الاجتماعية من نُزوح اضطراري في البداية إلى خلل ديموغرافي هيكلي طويل الأمد استمرَّ حتى عام 2025. حيث أنه بحلول هذه الفترة، أصبح الاعتماد على الأُجور المُكتسبة في الخارج مثل بولندا استونيا هو المصدر الأساسي لتمويل الأُسر الأوكرانية. كما يشير التحليل الخاص بعام 2026 إلى تفاقُم "نُقص العمالة الماهرة" في قطاعي الزراعة والصناعة نتيجة طول أمد الحرب واستمرار لجوء الملايين؛ حيث أ، الفوارق الإقليمية بين شرق أوكرانيا وغربها أصبحت واقِعًا اجتماعيًا يتطلَّب سياسات تعافٍ تكامُليَّة طويلة الأمد لمواجهة فقدان الثقة ورأس المال الاجتماعي.

لقد أظهرت الحرب الروسية–الأوكرانية آثارًا مرحليَّة مُتعدِّدة على روسيا وأوكرانيا، إذ تكبَّدت روسيا ضُغوطًا اقتصادية نتيجة العقوبات وتباطُؤ النُّمو، بينما تكبَّدت أوكرانيا خسائر ماديَّة وبشريَّة جسيمة في البنية التحتيَّة والإنتاج، وعلى الصعيد العسكري، استنزفت الحرب الموارد البشريَّة والماديَّة للطرفين؛ أمَّا اجتماعيًّا فقد تسبَّبت في نزوح واسع وأزمات إنسانية عميقة، ما يعكس تعدُّد أبعاد النزاع وتأثيراته المُباشرة على الدَّولتين. **(saeidah, 2026, pp. 09-10)**

المبحث الثاني: الاستراتيجيات السيبرانية المُتَّبعة في الحرب الروسية–الأوكرانية

أصبح الفضاء السيبراني أحد أهم ميادين الصراع في العصر الحديث؛ حيث تلجأ الدوَّل إلى استخدام الهجمات والدفاعات الرقميَّة لتحقيق أهدافها الاستراتيجية. وتُعتبر الحرب الروسية–الأوكرانية نموذجًا بارزًا لتوضيح دور الأمن السيبراني في النزاعات المعاصرة.

يسعى هذا المبحث إلى دراسة الاستراتيجيات السيبرانية لكل من دولة روسيا وأوكرانيا، من خلال مبحثين متتابعين؛ يتناول الأول الاستراتيجية الروسية في الفضاء السيبراني على أبعادها الدفاعيَّة والهجوميَّة، بينما يُركِّز المطلب الثاني على الاستراتيجية الأوكرانية بنفس التقسيم.

المطلب الأول: الاستراتيجية السيبرانية الروسية في الفضاء السيبراني

تعتمد روسيا في الفضاء السيبراني على مزيج من القُدُرات الدفاعيَّة لحماية بنيتها الرقميَّة، والهجومية لزعزعة خصومها، ما يعكس دور الفضاء السيبراني كأداة استراتيجية في تحقيق أهدافها العسكرية والأمنية، وفق ما يلي:

أولا: الاستراتيجية الهجوميَّة: منذ بداية الغزو الروسي لأوكرانيا في فبراير2022، اعتمدت روسيا توظيفًا هجوميًا واضحًا ومُكثَّفًا للقدرات السيبرانية ضمن إطار العمليَّات العسكريَّة المُصاحبة للعمليَّات التقليديَّة؛ حيث استُخدمت الضربات السيبرانيَّة التمهيديَّة لإضعاف البنية التحتيَّة الرقميَّة ومنظومات الاتصالات الأوكرانية، وهو ما تجسَّد في الهجوم الذي استهدف شبكة الأقمار الصناعيَّةKA–SAT التابعة لشركة viasat عبر برمجيَّة المسح AcidRain والذي أدَّى إلى تعطيل آلاف أجهزة المودم المُستخدمة في الاتصالات العسكريَّة الأوكرانية مُنذ اليوم الأوَّل للحرب.**(black, 2023, p. 08)**

كما لجأت روسيا قبل اندلاع العمليَّات العسكريَّة مُباشرة إلى استخدام برمجيَّات التدمير الرقمي من نوع WipermalwarمثلWhisperGateضدَّ مؤسسات حكوميَّة وقطاعات تكنولوجيا المعلومات الأوكرانية، في إطار عمليَّات سيبرانيَّة تمهيديَّة هدفت إلى إضعاف القُدُرات المُؤسسية للدولة الأوكرانيةِ.**(aorenstein, 2022, p. 08)**

وفي السياق ذاته، اتَّجهت العمليَّات السيبرانية الروسية خلال المرحلة الافتتاحيَّة للحرب إلى توظيف أدوات تدميريَّة على نطاق أوسع مُقارنةً بالفترة السابقة لعام 2022، عبر تنفيذ هجمات شبكيَّة واسعة ومُتزامنة استهدفت البنية التحتيَّة المعلوماتيَّة المدنيَّة والعسكريَّة بالتوازي مع العمليَّات الميدانيَّة، بما في ذلك تعطيل منظومة الاتصالات الحيويَّة المُرتبطة بالقوَّات المُسلَّحة الأوكرانية، وهو ما عكس انتقال العمليَّات السيبرانية الروسية من نمط الهجمات

المحدودة إلى نمط العمليَّات التراكميَّة واسعة النطاق الداعمة للجهد العسكري التقليدي. (aorenstein, p. 08)

كما شمِلت هذه الأنشطة تنفيذ حملات سيبرانية مُتعددة الوظائف تمثَّلت في جمع المعلومات الاستخباراتية، تعطيل القدرات العسكرية الأوكرانية أو خداعها، وتنفيذ عمليَّات تأثير نفسي مُوجَّهة ضد المجتمع الأوكراني، على جانب الاستفادة من اختراق شبكات الاتصالات الأوكرانية في دعم التخطيط العمليَّاتي والتكتيكي الروسي خلال مُجريات الحرب. **(schulze & mika, 2023, p. 04)**

ثانيًا: الاستراتيجية الدفاعيَّة: خلال الحرب الروسية–الأوكرانية، تبنَّت روسيا استراتيجية دفاعيَّة سيبرانية مُتعددة الطبقات تهدف إلى حماية المجال المعلوماتي الداخلي والتحكُّم في تدفق المعلومات، مع الاعتماد على الاستخبارات السيبرانية والمعلوماتية بدل الهجمات التدميرية المباشرة. مكَّنت مُمارسات الأمن المعلوماتي الصَّارمة الدولة من عزل المجال الداخلي عن التأثير الغربي، بينما استغلَّت سنوات من الاختراق المُسبق للشبكات الأوكرانية ورسم خرائط للبنية التحتيَّة الحيويَّة لتعزيز السيطرة على الفضاء السيبراني دون تعطيله، كما ظهر في سيطرتها على شركات الاتصالات والبنية التحتيَّة والشبكات المُتداخلة. تركَّزت الاستراتيجية أيضًا على الاستفادة من التجسُّس السيبراني لدعم التخطيط العسكري والتكيُّف الضغوط المُستمرَّة، مع تجنُّب العمليَّات التي قد تؤدِّي إلى تصعيد غير مرغوب فيه أو استنزاف الموارد، إلى جانب تنويع الأدوات وبناء وسائل وُصول احتياطيَّة لضمان استمراريَّة القدرة العملياتيَّة الروسية على الفضاء السيبراني.**(libicki, 2023, pp. 11-48-49-52)**

وبهذا شكَّلت الاستراتيجية الروسية مزيجًا متوازنًا من السيطرة المُسبقة على المجال السيبراني، التحصين الداخلي، الاستطلاع طويل المدى، والتكيف العملياتي. ما مكَّنها من تحقيق تفوُّق معلوماتي واستراتيجي على الخصم دون اللُّجوء إلى التدمير الشامل للبنية التحتيَّة. **(schulze & mika, 2023, p. 04)**

الاستراتيجية السيبرانية الروسية كما تمَّ تحليلها، تقوم على تكامُل واضح بين القدرات الدفاعيَّة والهجوميَّة، بما يعكس توظيفًا منهجيًا للفضاء السيبراني في تحقيق الأهداف. وقد أبرز من خلال الاعتماد النموذج طبيعة التوجُّه الروسي في توظيف الحرب السيبرانية كأداة مركزيَّة في الصراع.

الشكل 12: الاستراتيجية الروسية في الفضاء السيبراني

المصدر: إعداد الطالبة

المطلب الثاني: الاستراتيجية السيبرانية الأوكرانية في الفضاء السيبراني

تمثل الاستراتيجية الأوكرانية في الفضاء السيبراني مزيجا من الدفاع والهجوم؛ حيث سعت أوكرانيا لحماية بنيتها التحتية الرقمية من الهجمات الروسية وفي الوقت نفسه شن عمليات مضادة لتعطيل القدرات السيبرانية للخصم.

أولاً: الاستراتيجية الهجومية: لم تتجه الاستراتيجية السيبرانية في الحرب الروسية–الأوكرانية نحو الحسم المباشر؛ بل ارتكزت على التوظيف التراكمي المندمج مع العمليات العسكرية؛

حيث تمارس كأنشطة مترابطة تعزز التأثير العملياتي تدريجيا بدلا من إحداث نتائج حاسمة منفردة.**(discon, 2025, p. 56)**

وفي هذا السياق، برزت الاستخبارات السيبرانية كالأداة الهجومية الأكثر فاعلية، بعد تحوُّلها إلى عُنصر داعم للعمليات الميدانيَّة في الزمن الحقيقي. ويُجسد ذلك استخدام برمجيَّة Infamous Chisel التي مكَّنت من تتبُّع تحرُّكات القوَّات وتوجيه الضربات بدِقَّة. **(discon, 2025, p. 57)**

في المُقابل، ظلَّ التخريب السيبراني محدود الأثر الاستراتيجي، خاصَّةً عند مقارنته بعمليَّات تقليديَّة مثل Operation Spiders web ذات التأثير المادي المُباشر. **(discon, 2025, pp. 55-59)**

وعليه، لم تُحقق العمليات السيبرانية تأثيرًا حاسمًا في إضعاف القدرة الأوكرانية، إذ انحصرت أهميتها في الاستطلاع والاستخبارات ودعم الاستهداف العسكري، كما يظهر في استخدام أدوات مثل X-Agent لتحديد مواقع المِدفعيَّة وتوجيه النيران المُضادَّة. **(schulze & mika, 2023, pp. 01-02)**

ثانيًا: الاستراتيجية الدفاعيَّة: برزت الاستراتيجية الأوكرانية من خلال تفوُّق دفاعي قائم على التكيُّف المُؤسسي والمرونة؛ حيث شكَّل الدفاع السيبراني العامل الحاسم في الحدِّ من فعالية الهجمات الروسية.**(black, 2023, p. 03)**

ويعود ذلك إلى اعتماد نموذج متكامل يقُوم على التنسيق بين الدولة والقطاع الخاص والشركاء الدوليين، ما مكَّن من كشف الهجمات واحتوائها بفعالية، كما في مواجهة عمليات التخريب السيبراني.**(discon, 2025, p. 05)**

كما ارتكزت هذه الاستراتيجية على المُواجهة المُبكِّرة وتعزيز الدفاعات بما يُقوِّض خُطط الخصم قبل تحقق آثارها.**(black, 2023, p. 03)**

إلى جانب ذلك، شكَّلت المرونة التنظيميةOrganizational Agility عُنصرًا حاسمًا في تفوُّق النموذج الأوكراني، إذ سمحت بسرعة التكيُّف والتكامُل، مُتجاوزة القيود التقليدية، ومحققة فعالية أغلى في إدارة الصراع السيبراني.**(discon, 2025, p. 55)**

الشكل رقم 13: الاستراتيجية السيبرانية الأوكرانية في الفضاء السيبراني

المصدر: إعداد الطالبة

من خلال ما تم دراسته، يتضح أن الاستراتيجية السيبرانية الأوكرانية تجمع بين الدفاع المرِن والهجوم المحدود، في إطار يعكس تكيُّفًا مع متطلبات المُواجهة. وقد سمح توظيف هذه الاستراتيجية بإبراز دور الفضاء السيبراني كعُنصر فاعل في تعزيز الصُّمود والتأثير.

المبحث الثالث: انعكاسات الحرب السيبرانية الروسية–الأوكرانية على الأمن الإقليمي الأوروبي

تجسد الحرب السيبرانية الروسية–الأوكرانية تحوُّلاً في العقيدة القتالية وتوازنات القوى الإقليمية، ممَّا فرض واقعًا أمنيًا رقميًا جديدًا. ويسعى هذا المبحث لتحليل تداعيات هذا الصراع من خلال مطلبين؛ يتناول الأول الهجمات الرقمية في المجال العسكري والسياسي، فيما يُعالج الثاني أبعادها في المجال الاقتصادي والاجتماعي.

المطلب الأول: انعكاسات الحرب على المجال العسكري والسياسي:

تعد الحرب الروسية–الأوكرانية مثالا حيويا على كيفية تحول النزاعات التقليدية إلى صراعات متعددة الأبعاد؛ حيث يمتد تأثيرها إلى المجال السيبراني والهجين، محدثة انعكاسات مباشرة على الأمن الإقليمي الأوروبي. مما يجعل دراسة تأثير انعكاساتها على المستويين العسكري والسياسي أمرا ضروريا لفهم التحديات الجديدة التي تواجه الأمن الأوروبي.

أولاً: المجال العسكري: أضحت العمليات السيبرانية في سياق الحرب الروسية–الأوكرانية عنصرًا مزدوج الوظيفة؛ إذ تؤدِّي دورًا تكميليًا للعمليات العسكرية التقليدية، وفي الوقت ذاته تُمثِّل أداة حاسمة قائمة بذاتها في إدارة الصراع. كما استُخدمت الهجمات السيبرانية لاستهداف أنظمة المعلومات، بما يهدف إلى تضليل السكَّان، تعطيل الأنشطة الحيوية، شلُّ البنى التحتيّة الوطنية، فضلاً عن جمع معلومات استخباراتية دقيقة حول القدرات العسكرية ونقاط الضُّعف الأمنية للدول المُستهدفة.**(radu, 2023, p. 39)**

وعلى المستوى العمليَّاتي، أسهمت التقنيات السيبرانية في تعطيل شبكات المعلومات، إحداث شلل في أنظمة القيَّادة والسيطرة، وإرباك قنوات الاتصال، بما عزَّز من استراتيجيات الحرب الهجينة، إلى جانب استهداف البنية التحتية الحيوية الأوكرانية ذات الطابع العسكري. **(radu, 2023, pp. 43-47)**

ولم تقتصر هذه التأثيرات على ساحة الصِّراع، بل امتدَّت إلى المجال الأوروبي، إذ برزت دوَّل مثل بولندا في صدارة الدول المُستهدفة، إلى جانب دول البلطيق والدنمارك والنرويج وفنلندا والسويد وتركيا، التي شهدت تصاعُدًا ملحوظًا في الحوادث السيبرانية المُرتبطة بالحرب. كما سعَت هذه العمليَّات إلى تعطيل البنى التحتيَّة الوطنيَّة والتأثير في الأنشطة العسكرية، بما يعكس اتِّساع نطاق التهديد السيبراني على المُستوى الإقليمي.**(radu, 2023, p. 50)**

ثانيًا: المجال السياسي: أسهمت الحرب الروسية–الأوكرانية في إعادة تشكيل التصوُّر الأوروبي للأمن، باعتبارها امتدادًا لصراع طويل الأمد، لعِبت فيه الأدوات الهجينة، وعلى رأسها الهجمات السيبرانية وحروب المعلومات، دورًا فاعلاً في التأثير على البنى السياسية للدول الأوروبية. **(kelemen, 2023, p. 76)**

وفي هذا السيَّاق، وعلى الرَّغم من الانخراط المُباشر لدول الاتحاد الأوروبي في النزاع، إلاَّ أن بنياتها الرقمية والسياسية تعرَّضت لاستهداف مُتزايِد، ممَّا يعكس الطبيعة العابرة للحدود للحرب السيبرانية، وقدرتها على اختراق الفضاءات السيادية للدول والتأثير في استقرارها الداخلي. إذ لم تقتصر هذه الهجمات على الجوانب التقنية، بل امتدَّت لتشمُل المجال السياسي، من خلال تهديد استقرار الأنظمة والمؤسسات، وإمكانية زعزعة الثقة العامَّة في الهياكل السياسية.**(kelemen, 2023, pp. 77–80)**

وتبرز حالة فرنسا كنموذج واضح لهذا النّمط من التهديدات؛ حيث تمَّ توظيف أدوات الحرب الهجينة، خاصَّةً حملات التضليل الإعلامي المُرتبطة بحركة "السترات الصفراء"، بهدف التأثير على الرأي العام وتغذيَّة الاضطرابات الداخليَّة، وقد ساهمت هذه العمليَّات في نشر أخبار زائفة على نطاق واسِع، ما يعكس الاستخدام الاستراتيجي للفضاء السيبراني كوسيلة للتدخَّل في الشؤون السياسية الداخلية للدول الأوروبية.(kelemen, 2023, pp. 76–77)

لقد أبرزت الحرب السيبرانية الروسية–الأوكرانية هشاشة الأمن الإقليمي الأوروبي، إذ أظهرت تداخُل التهديدات الرقمية مع البنى العسكرية والسياسية، مما دفع الاتحاد الأوروبي

لإعادة تقييم استراتيجياته الدفاعية وتعزيز آليات التعاون الأمني لمواجهة التصعيد السيبراني المُستمر.

الشكل رقم 14: انعكاسات الحرب على المجال العسكري والسياسي

المصدر: إعداد الطالبة

المطلب الثاني: انعكاسات الحرب على المجال الاقتصادي والاجتماعي

تعكس الحرب السيبرانية الروسية–الأوكرانية تأثيرات ملموسة على الأمن الإقليمي الأوروبي اقتصاديًا واجتماعيًا؛ حيث مسَّت الهجمات السيبرانية البنى التحتية الحيويَّة وحتَّى التأثير على المجتمعات والثقة بالمؤسسات الديمقراطيَّة.

أولا: المجال الاقتصادي: أدت الحرب السيبرانية الروسية–الأوكرانية إلى تصاعُد استهداف الفضاء السيبراني الأوروبي؛ حيث طالت الهجمات الروسية مؤسسات حكومية ومُشغِّلي البنية التحتية الحيوية وقطاعات الدفاع والطاقة والاتصالات وتكنولوجيا المعلومات داخل الاتحاد

الأوروبي وحلف الناتو، بما يعكس انتقال التأثير إلى ركائز الاقتصاد الرقمي الأوروبي. (thachuk, 2025, p. 19)

كما استهدفت العمليات السيبرانية الروسية أنظمة الأقمار الصناعية الأوروبية عبر التشويش والتعطيل، ما أثر على خدمات الاتصالات والبنية التحتية المرتبطة بها، إضافة إلى تسجيل اضطرابات في نظام الملاحة عبر الأقمار الصناعية انعكست على سلامة الطيران المدني داخل الاتحاد الأوروبي.(thachuk, 2025, p. 19)

وشملت هذه العمليات التدخُّل في شبكات أقمار صناعية أوروبية Hot Bird 13 الفرنسيَّة و Astra-4 التابعة للوكسمبورغ إضافة إلى استهداف مزود الاتصالات اللاتفيBlaticom وهو ما يعكس امتداد التأثير إلى البنية الرقمية الوطنيَّة لدول أوروبية.(thachuk, 2025, p. 20)

كما أظهرت برمجية Not Petya المُرتبطة بالحرب قدرة الهجمات السيبرانية على الانتشار إلى شبكات أوروبية وعالمية، مُتسببة بخسائر قدرت بنحو 10 مليارات دولار، بما يكشف حجم التأثير الاقتصادي العابر للحدود للحرب السيبرانية الروسية.(kapsokoli, 2025, p. 75)

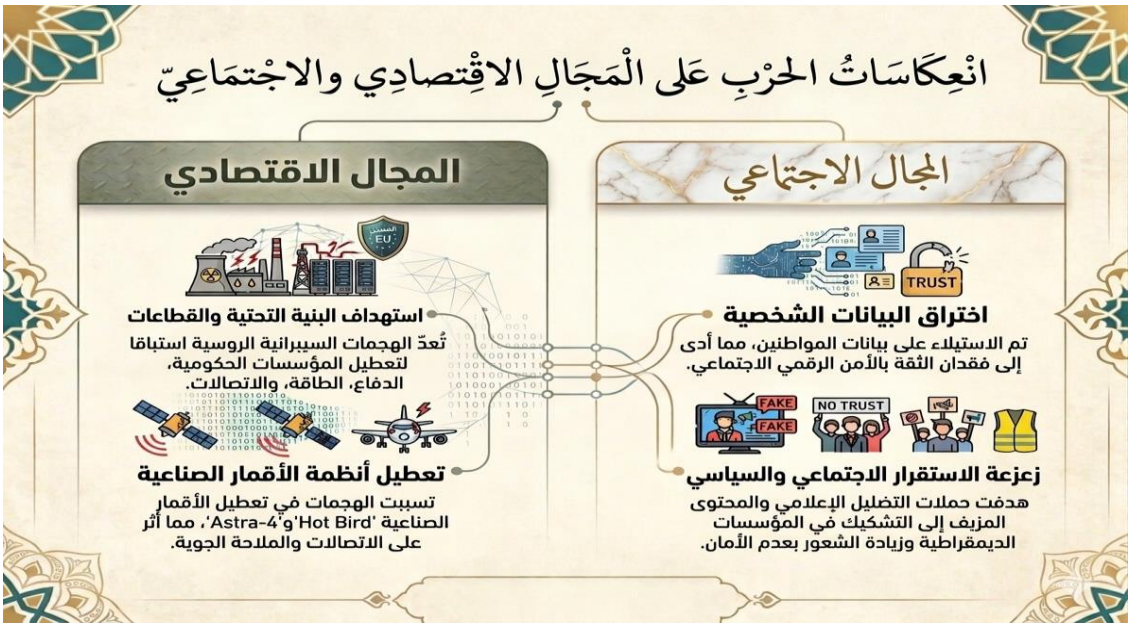
ثانيًا: المجال الاجتماعي: امتدت انعكاسات الحرب السيبرانية الروسية-الأوكرانية إلى المجال المُجتمعي الأوروبي عبر تنفيذ عمليات سيبرانية ومعلوماتية استهدفت السكان في الدول الغربية، شملت تفويض عمل البنية التحتية الحيوية، الاستيلاء على البيانات الشخصية للمواطنين، ومحاولات التأثير في العمليات الانتخابية داخل الدول الأوروبية، بما يعكس استهداف الاستقرار المجتمعي والسياسي الأوروبي.(thachuk, 2025, p. 05)

كما رافقت هذه العمليات حملات تضليل إعلامي واسعة هدفت إلى التأثير في الرأي العام وإضعاف الدعم الأوروبي لأوكرانيا من خلال نشر الأخبار المضللة والمحتوى المزيف والتأثير على الإدراك العام داخل المجتمعات الأوروبية.(kapsokoli, 2025, p. 76)

إضافة إلى ذلك، سعت العمليَّات السيبرانية الروسية إلى تقويض الثقة بالمؤسسات الديمقراطية وزيادة الشعور بعدم الأمن داخل المجتمعات الغربية، بما يعكس اتساع التأثيرات الاجتماعية للحرب السيبرانية داخل البيئة الأوروبية الأطلسية.(kapsokoli, 2025, p. 74)

تظهر الحرب السيبرانية الروسية–الأوكرانية تأثيرات ملمُوسة على الأمن الإقليمي الأوروبي اقتصاديًا من خلال اضطراب البنية التحتيَّة الحيوية والاتصالات والخسائر المالية عبر دوَّل الاتحاد الأوروبي وحلف الناتو، واجتماعيًا عبر التَّضليل الإعلامي وتقويض الثقة بالمؤسَّسات واستهداف بيانات المواطنين، ممَّا يُؤكِّد الحاجة لتعزيز القُدرات الدفاعيَّة السيبرانية الأوروبية لمُواجهة هذه التهديدات العابرة للحدود.

الشكل رقم 15: انعكاسات الحرب على المجال الاقتصادي والاجتماعي



المصدر: إعداد الطالبة

خريطة رقم 01: التوزيع المكاني لممرات العبور السيبراني في أوروبا

المصدر : إعداد الطالبة بتوجيه تقني لتطبيقGemini نقلا عن:

Ronald Kelemen, The Impact of the Russian– Ukrainian Hybrid War on the European Union's Cyber Security Policies and Regulations 2023

توضح الخريطة "تعدي الأثر السيبراني" للحدود الجغرافية للنزاع؛ حيث تستخدم البنية التحتية الأوكرانية كمنصة انطلاق "ترانزيت" لاستهداف العمق الأوروبي. هذا ما يؤكد أن التهديد السيبراني لا يعترف بالحياد الجغرافي، مما يفرض ضرورة تبني استراتيجيات أمن جماعي عابرة للحدود.

خلاصة الفصل الثاني:

تكشف دراسة مسار لحرب الروسية–الأوكرانية 2014–2025 عن تحول جذري في طبيعة الحروب الحديثة؛ حيث لم يعد الصدام العسكري التقليدي كافيا لحسم الصراعات دون دمج البعد السيبراني للأمن. فقد أثبتت التجربة الميدانية أن توظيف القوة الرقمية، سواء في شقها الدفاعي أو الهجومي، يمتلك القدرة على شل قدرات الخصم والتأثير في موازين القوى السياسية والميدانية، مما يجعل الفضاء الرقمي ساحة معركة لا تقل أهمية عن الجبهات الأرضية.

من جانب آخر، يتضح أن هذه الحرب قدمت نموذجا حيا لما يعرف بـ "الحروب الهجينة"؛ حيث يمتزج البعد الجيوبوليتيكي بالقدرات التكنولوجية المتطورة. وقد امتدت تداعيات هذا الصراع لتحدث زلزالا في منظومة الأمن الإقليمي الأوروبي، مما أجبر الدول على إعادة ترتيب أولويات أمنها القومي وتغيير موازين القوى العسكرية والسياسية في القارة، إذ أن الخلاصة الجوهرية هنا هي أن الاستراتيجيات الرقمية قد أصبحت العنصر الحاسم في إدارة الصراعات المعاصرة وتحديد مآلاتها على المستويين الإقليمي والدولي.

الفصل الثالث:

الفكر الاستراتيجي الجزائري في ظل الحرب الروسية-الأوكرانية

الفصل الثالث: الفكر الاستراتيجي الجزائري في ظل الحرب الروسية–الأوكرانية

ينظر إلى الفكر الاستراتيجي الجزائري باعتباره منظومة ديناميكية تسعى باستمرار للتكيف مع التحولات الجيوسياسية المتسارعة، خاصة في ظل بروز أنماط جديدة من الصراعات الدولية التي تتجاوز البعد التقليدي للقوة. وتأتي الحرب الروسية–الأوكرانية لتمثل نقطة تحول مفصلية فرضت على صانع القرار الاستراتيجي في الجزائر إعادة قراءة البيئة الأمنية بمنظور يدمج بين تحديات الأمن المادي والتهديدات السيبرانية العابرة للحدود.

من خلال هذا، جاء هذا الفصل مقسما على ثلاث مباحث رئيسية؛ يتناول المبحث الأول دراسة مسحية للأمن السيبراني في الجزائر، من خلال مطلبين يعالجان الإطار التشريعي والمؤسساتي وكذا السياسات الوطنية لحماية البنى التحتية الحساسة. أما المبحث الثاني يدرس تأثيرات الحرب الروسية–الأوكرانية على التحولات في الفكر الاستراتيجي الجزائري؛ حيث خصص المطلب الأول لإدراج التهديدات السيبرانية في المقاربة الاستراتيجية للدولة، بينما يتناول توجيه المطلب الثاني توجيه السياسة الجزائرية نحو الأمن الرقمي، وصولا للمطلب الثالث الذي يناقش ادماج البعد الرقمي في العقيدة الدفاعية. بينما يركز المبحث الثالث على تقييم المقاربة الأمنية الرقمية الجزائرية عبر دراسة تحديات الأمن السيبراني وآفاق تطوير هذه المقاربة استراتيجيا، بما يتيح تقديم رؤية تحليلية متكاملة لمدى استجابة الجزائر للتهديدات الناشئة وآثارها متعددة المستويات.

المبحث الأول: واقع الأمن السيبراني في الجزائر

تجسد الدراسة المسحية لواقع الأمن السيبراني ركيزة جوهرية لتقييم جاهزية الجزائر في مواجهة التهديدات الرقمية الناشئة عن النزاعات الدولية المعاصرة. وبِوصف الفضاء السيبراني "الجبهة الخامسة" في الحروب الحديثة؛ حيث أضحى رصد المقدرات الوطنية ضرورة استراتيجية لحماية السيادة وتأمين البنى التحتية الحيوية للدولة.

انطلاقا من ذلك، يتناول هذا المبحث تشخيصا دقيقا لواقع الأمن السيبراني في الجزائر عبر مستويين أساسيين؛ حيث يركز المستوى الأول على تحليل الإطار التشريعي والمؤسساتي المنظم لهذا الفضاء، بينما ينصرف المستوى الثاني لتقييم السياسات والبرامج الوطنية الموجهة لحماية البنى التحتية الحساسة، مما يمهد الطريق لفهم التحولات الاستراتيجية اللاحقة في العقيدة الدفاعية الجزائرية.

المطلب الأول: الإطار التشريعي والمؤسساتي للأمن السيبراني في الجزائر

يستلزم تعزيز الأمن الرقمي الوطني وجود إطار تشريعي ومؤسساتي قادر على مواكبة التحولات الجيوسياسية الراهنة. انطلاقا من ذلك، يهدف هذا المطلب إلى تبيان المرتكزات القانونية التي تحكم الفضاء السيبراني الجزائري، مع تسليط الضوء على الأدوار الوظيفية للمؤسسات السيادية المكلَفة بضمان الحماية والرقابة الرقمية.

أولا: الإطار التشريعي للأمن السيبراني في الجزائر: شهد الإطار التشريعي للأمن السيبراني في الجزائر تحولات ملحوظة بعد سنة 2022، في ظل تصاعد التهديدات الرقمية وتزايد الاعتماد على الفضاء السيبراني؛ حيث اتجه المشرع الجزائري نحو تحديث المنظومة القانونية بما ينسجم مع التحولات التكنولوجية والرهانات الأمنية الجديدة.

برزت الديناميكية التشريعية من خلال تعزيز وتحيين القوانين المرتبطة بحماية المعطيات الشخصية؛ حيث تم تفعيل وتحيين تطبيقات القانون تتجلى أساسا في أحكام المادة رقم 47 من

دستور 2020، التي كرست حماية الحياة الخاصة وحرمة المعطيات ذات الطابع الشخصي، إضافة إلى ضمان سرية المراسلات والاتصالات بمختلف أشكالها، وهو ما يشكل قاعدة قانونية مباشرة لحماية الأفراد في الفضاء الرقمي.**(الجمهورية الجزائرية الديموقراطية الشعبية. دستور 2020، 2020)**

ويفهم من مضمون هذه المادة أن المشرع الدستوري قد وسع نطاق الحماية ليشمل ليس فقط العلاقات التقليدية، بل أيضا التفاعلات الرقمية، الأمر الذي يجعلها حجر الزاوية في تأطير الجرائم السيبرانية المرتبطة بانتهاك الخصوصية واختراق البيانات.

في المقابل، تعزز المادة 48 من الدستور هذه الحماية من خلال تكريس مبدأ حرمة المسكن، والذي لا يقتصر في التحليل المعاصر على المجال المادي فقط، بل يمكن اسقاطه على الفضاء الرقمي الخاص.**(الجمهورية الجزائرية الديموقراطية الشعبية. دستور 2020، 2020)**

ومن ثم فإن هذه المادة تؤسس بشكل غير مباشر لحماية المجال السيبراني من أي اختراق أو دخول غير مشروع.

في إطار التوجهات الرسمية الحديثة، أكدت وزارة الدفاع الوطني في تقريرها الموسوم بـ "الأمن السيبراني.. ورشة الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية 2024" أن الأمن السيبراني أضحى يشكل رهانا استراتيجيا في ظل تصاعد التهديدات الرقمية، الأمر الذي يفرض ضرورة تطوير استراتيجية وطنية متكاملة لأمن الأنظمة المعلوماتية. كما شددت على أهمية تعزيز حماية البنى التحتية الحساسة وتكثيف التنسيق بين مختلف الفاعلين، بما يضمن رفع مستوى الجاهزية لمواجهة المخاطر السيبرانية المتزايدة.**(وزارة الدفاع الوطني الجزائري، 2024)**

ويؤكد هذا التوجه مشروع قانون الأمن السيبراني لسنة 2025 ضمن مساعي تحديث الإطار التشريعي في الجزائر؛ حيث يهدف إلى وضع منظومة قانونية متكاملة لحماية الأنظمة المعلوماتية، مع تكريس إلزامية التبليغ عن الحوادث السيبرانية، وتعزيز حماية البنى التحتية

الرقمية الحساسة، بما يعكس توجها نحو بناء مقاربة وقائية واستباقية في مواجهة التهديدات السيبرانية.)مشروع قانون الامن السيبيراني على طاولة الحكومة(2025 ,

رغم أن الدستور الجزائري لا ينص صراحة على الأمن السيبراني، إلا أنه يؤسس له من خلال حماية الحياة الخاصة وسرية الاتصالات والمعطيات الشخصية، وهو ما يشكل الأساس الدستوري للتشريع السيبراني في الجزائر.

الشكل رقم16: الإطار التشريعي للأمن السيبراني

المصدر: إعداد الطالبة

ثانيا: الإطار المؤسساتي للأمن السيبراني في الجزائر:

اتجهت الجزائر إلى بناء إطار مؤسساتي للأمن السيبراني يقوم على تعدد الهيئات وتكامل أدوارها بين الجوانب التنسيقية، الأمنية، والتقنية، بما يهدف إلى تعزيز حماية الفضاء الرقمي ومواجهة التهديدات السيبرانية؛ أهمها:

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: تعد هذه الهيئة من أبرز مكونات الإطار المؤسساتي؛ حيث تتمتع بطابع سلطة إدارية مستقلة ذات شخصية قانونية واستقلال مالي، وتخضع لسلطة رئيس الجمهورية، ما يمنحها مكانة مركزية في منظومة الوقاية من الجرائم السيبرانية ومكافحتها. **(sehailia, 2025, p. 483)**
- المصلحة المركزية لمكافحة الجريمة المعلوماتية: تندرج هذه المصلحة ضمن الأجهزة الأمنية التابعة للأمن الوطني، وقد أنشئت سنة 2011؛ حيث تتولى معالجة الجرائم السيبرانية ومتابعتها في إطار مؤسسي منظم، بما يعكس الدور العملياتي للأجهزة الأمنية في حماية الفضاء الرقمي.**(sehailia, 2025, p. 485)**
- مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة: تمثل هذه المصلحة البعد العسكري في الإطار المؤسساتي؛ حيث أنشئت على مستوى الجيش الوطني الشعبي، وتعني بحماية الأنظمة والمنشآت الحيوية من التهديدات السيبرانية، بما يعكس إدماج البعد السيبراني ضمن المنظومة الدفاعية للدولة.**(قبطة، صفحة 11)**
- المعهد الوطني للأدلة الجنائية وعلم الإجرام: هذا المعهد عبارة عن مؤسسة تقنية متخصصة تابعة للدرك الوطني، تعتمد على الخبرة العلمية في تحليل الأدلة الجنائية، خاصة الرقمية منها، ما يجعله عنصرا داعما للتحقيقات في الجرائم السيبرانية ضمن الإطار المؤسساتي.**(قبطة، صفحة 10)**

يتسم الإطار المؤسساتي للأمن السيبراني في الجزائر بتعدد الفاعلين وتكامل أدوارهم بين الهيئات التنسيقية والأجهزة الأمنية والمؤسسات التقنية، بما يعزز فعالية مواجهة التهديدات السيبرانية.

الشكل رقم17: الإطار المؤسساتي للأمن السيبراني

المصدر: إعداد الطالبة

المطلب الثاني: السياسات والبرامج الوطنية في حماية البنى التحتية الحساسة

لم يعد تأمين البنى التحتية الحساسة في الدولة الجزائرية يقتصر على الجوانب المادية أو الحماية الفيزيائية للمنشآت، بل أضحى مرتبطا بشكل عضوي بمدى حصانة الأنظمة المعلوماتية التي تدير هذه المرافق. وتعتمد الجزائر في هذا الصدد على مزيج بين التخطيط الاستراتيجي بعيد المدى، وبين الآليات الدفاعية والوقائية التي تضمن استمرارية الخدمات الحيوية في ظل تزايد التهديدات السيبرانية المعقدة. أبرزها:

1-استراتيجية المرونة الرقمية وتأمين الفضاء المعلوماتي: تضع الدولة الجزائرية حماية البنى التحتية الحساسة كشرط بنيوي لتحقيق "التحول الرقمي المنشود"، فوفقا للوثيقة الاستراتيجية الوطنية 2025-2029، فإن السياسة الوطنية تهدف إلى إيجاد بيئة آمنة تتوفر فيها كافة الظروف والتدابير على مستويات متعددة: وظيفية، تقنية، وهيكلية.

وتتوسع هذه الاستراتيجية في رسم خارطة طريق تعتمد على "المقاربات المبتكرة" التي تتماشى مع الأهداف المرجوة؛ حيث يتم التركيز على التكفل الفعال بالأنظمة المعلوماتية التي تشغل المرافق الحساسة، من خلال توفير آليات حماية تتوافق مع المتطلبات الشاملة لتأمين الفضاء السيبراني الوطني، ما يعكس انتقالا من مجرد رد الفعل إلى "الاستباقية الاستراتيجية" في حماية أصول الدولة.**(2024، الصفحات 2-3)**

2-برامج الحماية الدفاعية والوقاية من التهديدات السيبرانية: تشير الدراسات إلى أن الجزائر اعتمدت "تقنيات دفاعية وتدابير وقائية" كجزء أساسي من عقيدتها الأمنية؛ حيث تهدف هذه البرامج إلى بناء قدرات وطنية قادرة على رصد التهديدات المتزايدة في الفضاء السيبراني والتعامل معها قبل وصولها إلى النواة الصلبة للبيانات الحساسة.

تشمل هذه السياسة اتخاذ مجموعة من الآليات التي تضمن "أمن المعلومات بشكل دائم ومستمر"، من خلال تفعيل دور الهيئات المتخصصة في مراقبة حركة البيانات وحماية البنية التحتية الرقمية للدولة، بما يشمل أصولها المادية ومواردها البشرية.**(sehailia، 2025، صفحة 465)**

وقد تجسد ذلك ميدانيا من خلال نجاح مصالح الأمن الوطني في تفكيك شبكات متخصصة في الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، إضافة إلى توقيف أفراد تورطوا في عمليات احتيال الكتروني وسرقة بيانات حسابات بنكية رقمية، وهو ما يعكس تفعيل آليات التتبع الرقمي والتحقيق الإلكتروني في مواجهة الجرائم السيبرانية. **(أونلاين، 2024)**

تهدف هذه المقاربة الدفاعية بالأساس إلى تحصين السيادة الرقمية ومنع أي اختراق قد يؤدي إلى تعطيل الخدمات الأساسية للمواطنين.**(عيساوي ر.، 2024، صفحة 6)**

3-استراتيجية إدارة الأزمات وتأمين القطاعات الحيوية: تولي البرامج الجزائرية أولوية قصوى لما يعرف بـ "البنية التحتية الوطنية الحساسة" والتي تضم قطاعات الطاقة، المياه، النقل، والرعاية الصحية. نظرا لاعتماد هذه القطاعات المتزايد على "الأنظمة الرقمية المترابطة"، فقد أصبحت هدفا محتملا لهجمات سيبرانية متطورة.**(yigit, ferrage, & autre, 2024, p. 1)**

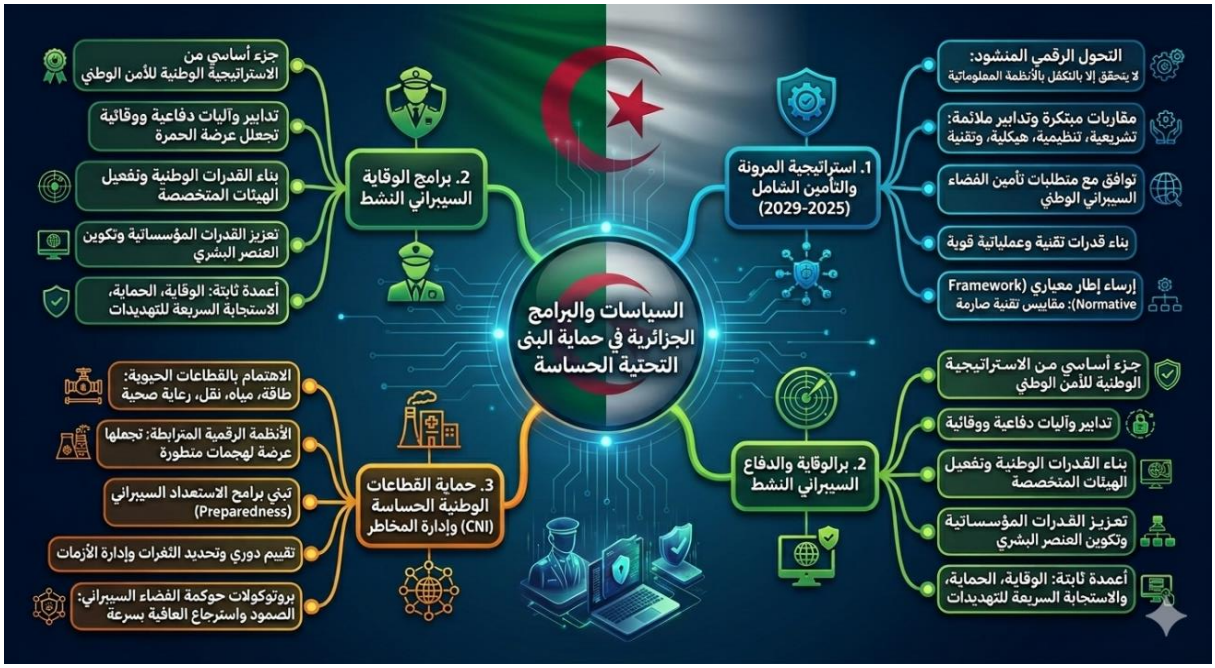
بناء على هذا التشخيص، تركز الاستراتيجية الوطنية على "الاستعداد السيبراني" عبر إجراء فحص وتقييم دقيق للبنى التحتية القائمة، وتطوير استراتيجيات فعالة لإدارة الأزمات تضمن الاستجابة السريعة في حالة وقوع هجوم.

كما تهدف الجزائر من خلال برامجها إلى تعزيز قدرة هذه المؤسسات على الصمود من خلال سن لوائح تنظيمية صارمة تفرض معايير أمنية محددة على كل قطاع حيوي، مع التركيز على "الاستجابة السريعة" كآلية للتقليل من الأضرار وضمان السيادة القومية في العصر الرقمي.) **عيساوي ر(2024, p. 6 , .**

وقد برز ذلك من خلال تسجيل محاولات اختراق إلكتروني استهدفت بعض المؤسسات الجزائرية خلال السنوات الأخيرة، الأمر الذي دفع الجهات المختصة إلى تعزيز أنظمة الحماية الرقمية ورفع مستوى التأمين السيبراني للمنشآت الحساسة. **(أونلاين ا.، 2023)**

ومنه، يمكن القول إن استراتيجيات الدولة الجزائرية في حماية البنى التحتية الحساسة قد تبلورت في شكل منظومة متكاملة تجمع بين "الحماية التقنية" و"الاستعداد العملياتي". فمن خلل تنفيذ برامج الاستراتيجية الوطنية 2025-2029، تسعى الجزائر إلى تأمين قطاعاتها الحيوية: الطاقة، النقل، البيانات، عبر آليات استجابة سريعة وتدابير وقائية تضمن تحصين الدولة ضد أي تهديد يمس استقرارها الرقمي وسيادتها الوطنية.

الشكل رقم18: السياسات والبرامج الوطنية في حماية البنى التحتية الحساسة



المصدر: إعداد الطالبة

المبحث الثاني: تأثيرات الحرب الروسية–الأوكرانية على التحولات في الفكر الاستراتيجي الجزائري

يشكل اندلاع الحرب الروسية–الأوكرانية، بما حمله من أبعاد عسكرية ورقمية متداخلة، نقطة تحول في طبيعة التفكير الاستراتيجي للدول؛ حيث برز الفضاء السيبراني كأحد أبرز ميادين الصراع الحديثة، ما دفع دولا عدة، من بينها الجزائر إلى إعادة تقييم مقارباتها الأمنية بما يتماشى مع هذه التحولات.

وعليه، يسعى هذا المبحث إلى إبراز تأثيرات هذه الحرب في إعادة تشكيل الفكر الاستراتيجي الجزائري، من خلال التطرق أولا إلى إدراج التهديدات السيبرانية ضمن المقاربة الاستراتيجية للدولة، ثم كيفية إدماج البعد الرقمي في العقيدة الدفاعية الجزائرية، بما يعكس توجها متناميا نحو تبني رؤية أمنية شاملة ومتكاملة تستجيب لمتطلبات الأمن في العصر الرقمي.

المطلب الأول: إدراج التهديدات السيبرانية في المقاربة الاستراتيجية للدولة الجزائرية

تتأسس المقاربة الاستراتيجية للدولة الجزائرية في مواجهة التهديدات السيبرانية على إدراك عميق للتحولات الجيوسياسية الراهنة؛ حيث أضحى الفضاء الرقمي مسرحا استراتيجيا تتداخل فيه المصالح الأمنية والعسكرية. وبناء على هذا التصور، سنعالج في هذا المطلب طبيعة إدراج هذه التهديدات ضمن الاستراتيجية الوطنية، من خلال رصد أبعادها الأمنية والجيوسياسية وتحليل انعكاساتها على السيادة الوطنية في ظل التوترات الدولية المعاصرة، وذلك على النحو التالي:

1-السيادة الرقمية كحتمية استراتيجية في ظل التحولات الدولية: تبنت الجزائر ضمن مقاربتها الاستراتيجية مبدأ جوهريا مفاده أن تعزيز الأمن السيبراني هو الركيزة الأساسية لحماية السيادة الوطنية في القرن الحادي والعشرين. فلم تعد المسألة تقتصر على النطاق التقني الصرف، بل تحولت إلى حتمية سيادية تهدف إلى تحصين البنى التحتية الحيوية من الاختراقات التي قد تشل مفاصل الدولة. وهو توجه تعاظم أثره بعد الدروس المستفادة من النزاعات الدولية الحديثة، لا سيما الحرب الروسية-الأوكرانية، التي أثبتت ميدانيا أن التهديد السيبراني أضحى سلاحا استراتيجيا يسبق ويرافق العمل العسكري التقليدي، بل وقد يتفوق عليه في إرباك الجبهة الداخلية وتعطيل منظومات القيادة والسيطرة.**(draou, 2025, p. 312)**

1-التهديدات السيبرانية في عقيدة مواجهة حروب الجيل الجديد: تدرج الدولة الجزائرية التهديدات السيبرانية ضمن سياق "حروب الجيل الخامس" أو الحروب الهجينة، وهي الاستراتيجيات التي تعتمد على استهداف الجبهات الداخلية عبر فضاءات رقمية مفتوحة غير محكومة بحدود جغرافية. وتشير الأدبيات العسكرية الجزائرية، لا سيما ما ينشر عبر مجلة الجيش، إلى أن استهداف الوعي المجتمعي وتعطيل الأنظمة الرقمية يعدان من أخطر أدوات

التدمير الحديثة. وتعد التجربة الروسية–الأوكرانية نموذجا واقعيا لهذه التهديدات التي تسعى لإضعاف الدول وتفتيت سيادتها من الداخل، مما استوجب تموقعا استراتيجيا جزائريا يضع الأمن المعلوماتي كخط دفاع أول في العقيدة الدفاعية الوطنية، مع التركيز على حماية البيانات الحساسة من التجسس أو التخريب.**(khadidja & djamel, 2025, p. 170)**

3–تفعيل "الردع السيبراني" كأداة للأمن القومي: تتضمن المقاربة الاستراتيجية الجزائرية ضرورة الانتقال من وضعية الدفاع الساكن إلى مفهوم "الردع السيبراني" الفعال. فكما أظهرت الحرب في أوكرانيا أهمية القدرات الدفاعية الرقمية في شل فاعلية الهجمات الاستباقية، تسعى الجزائر لخلق بيئة رقمية وطنية محصنة تضمن سلامة قواعد البيانات الوطنية وتدعم مكانتها في منظومة التعاون الدولي. إن هذا الردع لا يهدف فقط إلى صد الهجمات، بل إلى رفع تكلفة أي محاولة اختراق، مما يعزز من قدرة الدولة على حماية الأصول المادية والحيوية من الوصول غير المشروع عبر القنوات الرقمية. **(draou, 2025, p. 311)**

4–بناء فضاء سيبراني مرن لمواجهة تداعيات النزاعات الرقمية: تسعى الاستراتيجية الوطنية للأمن السيبراني في الجزائر إلى تحقيق مفهوم "المرونة الرقمية"، وهي المقاربة التي أثبتت الأزمات الدولية الراهنة ضرورتها القصوى لضمان استمرارية الدولة والاقتصاد الرقمي تحت الضغط. فالهدف الاستراتيجي هو بناء منظومة قادرة على الصمود والعمل تحت وطأة الهجمات السيبرانية المكثفة، اقتداء بالنماذج الدولية التي فرضت ضرورة حماية الرفاه الاجتماعي والنمو الاقتصادي من التذبذبات الأمنية العالمية المرافقة للنزاعات الكبرى.**(sereir, 2023, p. 13)**

إن المرونة هنا تعني القدرة على التعافي السريع واستعادة الأنظمة لوظائفها دون المساس بالاستقرار الوطني.

5–التهديدات السيبرانية في المنظور الجيوسياسي والنزاعات غير التقليدية: تدرك المقاربة الجزائرية أن الهجمات الرقمية أصبحت أداة ضغط استراتيجية في الصراعات الإقليمية

والدولية، على غرار ما يشهده العالم في الحرب الروسية–الأوكرانية من استخدام للسيبرانية كبديل أو مكمل للأسلحة التقليدية لضرب العمق الاستراتيجي. لذا تضع الدولة في حسبانها أن تأمين البنى التحتية العسكرية والاقتصادية يمثل أولوية قصوى لمواجهة أي محاولات لتعطيل القطاعات الحساسة عبر القنوات الرقمية في ظل بيئة دولية غير مستقرة. **(sipos, 2023, p. 66)**

نستخلص مما سبق أن إدراج التهديدات السيبرانية في المقاربة الاستراتيجية للدولة الجزائرية قد تجاوز البعد التقني الضيق ليصبح ركيزة أساسية في العقيدة الأمنية الشاملة للدولة. وهي مقاربة متأثرة مباشرة بالدروس المستقاة من النزاعات الدولية المعاصرة، وتتجلى في بناء منظومة ردع وحماية متكاملة تهدف إلى تحقيق السيادة الرقمية الكاملة وحماية المصالح الجيوسياسية العليا للجزائر في بيئة إقليمية ودولية شديدة التعقيد والتغير.

الشكل رقم19: ادراج التهديدات السيبرانية في المقاربة الاستراتيجية للدولة الجزائرية

المصدر: إعداد الطالبة

المطلب الثاني: إدماج البعد الرقمي في العقيدة الدفاعية الجزائرية

لم يعد الفضاء السيبراني في المنظور العسكري الجزائري مجرد بيئة تقنية داعمة، بل أضحى "المجال الحيوي الخامس" الذي تتقاطع فيه موازين القوى الدولية. وتفرض التحولات الراهنة في المشهد الأمني العالمي ضرورة إعادة صياغة المفاهيم التقليدية للدفاع الوطني لتستوعب المتغيرات الرقمية المتسارعة، لا سيما في ظل تصاعد التهديدات الهجينة التي تتجاوز الحدود الجغرافية للدول. وعليه، سنعمل في هذا السياق على استعراض العناصر التي تجسد هذا التحول العقائدي، من خلال:

1-التحول الجوهري في "فلسفة الدفاع" من الحماية السلبية إلى الردع الرقمي النشط: تشهد العقيدة الدفاعية الجزائرية في الآونة الأخيرة انعطافة استراتيجية كبرى تتمثل في الانتقال من "الأمن التقني" المحدود إلى استراتيجية "الصمود الاستباقي". إن إدماج البعد الرقمي في هذا السياق يمثل نقطة تحول مفصلية؛ حيث لم يعد ينظر للفضاء السيبراني كأداة للربط بين الوحدات، بل كـ "مسرح عمليات سيادي" قائم بذاته. وتجلت هذه الرؤية في ضرورة فرض السيطرة والردع الرقمي؛ إذ أن العقيدة الجديدة تؤمن بأن الدفاع عن الحوزة الترابية يبدأ من تحصين الفضاء الرقمي ومنع أي محاولات للاختراق أو التجسس أو التخريب المعلوماتي قبل وصولها إلى أهدافها المادية.**(benlarbi, 2024, p. 58)**

2-رقمنة هيكل القيادة والسيطرة وتطبيقات "الحرب المرتكزة على الشبكات": في إطار التحديث العقائدي، برز مفهوم "الحرب المرتكزة على الشبكات" كركيزة هيكلية في الفكر العسكري الجزائري المعاصر. هذا الإدماج الرقمي يتجاوز مجرد اقتناء أجهزة حاسوب أو برمجيات، بل هو "إعادة هندسة" شاملة لمنظومات C4ISR التي تشمل القيادة، السيطرة، الاتصالات، الحاسب الاستخبارات، المراقبة، والاستطلاع. وتؤكد العقيدة العسكرية في نسختها المحينة أن "رقمنة ساحة المعركة" أصبحت ضرورة حتمية للحفاظ على التفوق العملياتي ومواجهة التهديدات غير النمطية.**(mitchel, 2025, p. 142)**

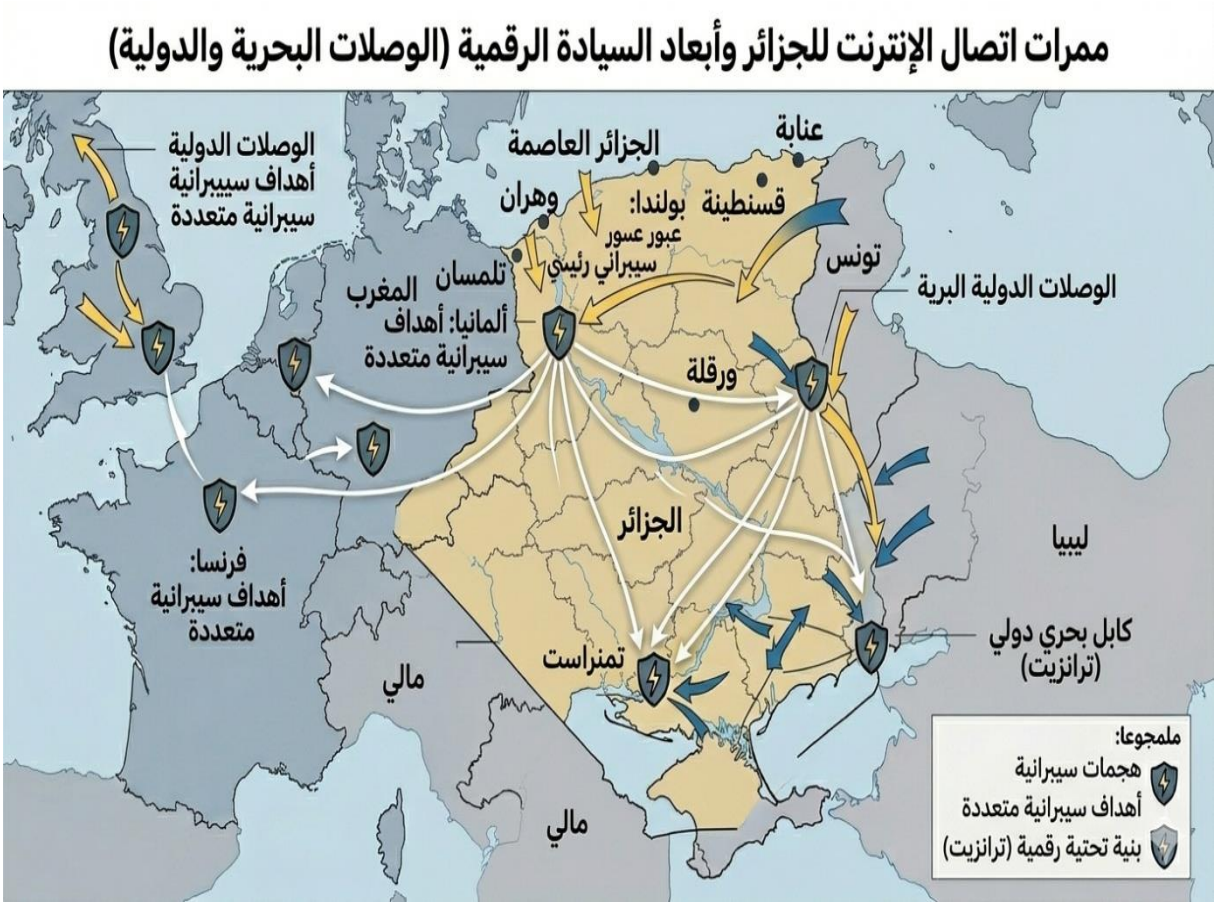
3-"السيادة التكنولوجية" و"الدرع البرمجي" كضمانة لاستقلال القرار العسكري: تعتبر "السيادة التكنولوجية" و"الاستقلال البرمجي" القلب النابض لعقيدة الدفاع الرقمي الجزائرية ففي ظل الاعتماد المتزايد على الأنظمة الذكية، أدركت القيادة العليا أن استيراد التكنولوجيا العسكرية دون التحكم في شيفراتها المصدرية يمثل ثغرة أمنية قاتلة ما يعرف بالأبواب الخلفية Backdoors. لذلك، تفرض العقيدة العسكرية الجزائرية بصرامة ضرورة تطوير حلول تشفير وطنية وأنظمة تشغيل مؤمنة محليا، لضمان استقلالية تامة في اتخاذ القرار العسكري بعيدا عن ضغوط الشركات المصنعة أو القوى التكنولوجية الكبرى.**(esposito, 2023, p. 205)**

نخلص إلى أن إدماج البعد الرقمي في العقيدة الدفاعية الجزائرية ليس مجرد خيار تقني، بل هو ضرورة استراتيجية تفرضها تحديات القرن الحادي والعشرين. لقد فقد أدت الدروس المستقاة من النزاعات الدولية المعاصرة إلى بلورة رؤية تقوم على "الردع الرقمي" و"السيادة التكنولوجية" كضمانات أساسية للأمن القومي الجزائري.

الشكل رقم20: إدماج البعد الرقمي في العقيدة الدفاعية الجزائرية

المصدر: إعداد الطالبة

خريطة رقم02: ممرات اتصال الجزائر بالأنترنت



المصدر: إعداد الطالبة بتوجيه تقني لتطبيق Gemini نقلا عن:

Sarah Mitchel, Strategic Defense Modernization in North Africa: Impact of Global Conflicts 2025

تبرز الخريطة "نقاط الاختناق الاستراتيجية" للسيادة الرقمية الجزائرية المتمثلة في محطات الإنزال البحرية والوصلات البرية. أي استهداف لهذه النقاط الحيوية يعني عزلا رقميا شاملا، مما يفرض إدماج حماية هذه "الممرات السيادية" كأولوية قصوى في العقيدة الدفاعية الوطنية الجديدة.

المبحث الثالث: تقييم المقاربة الأمنية الرقمية الجزائرية

يشهد الفضاء الرقمي تحولات متسارعة جعلت الأمن السيبراني عنصرا أساسيا في حماية الدول واستقرارها، خاصة مع تزايد التهديدات الإلكترونية. في هذا الإطار، تسعى الجزائر إلى تبني مقاربة أمنية رقمية لتعزيز قدراتها في مواجهة هذه المخاطر، غير أنها تواجه عدة تحديات. يهدف هذا المبحث إلى تقييم هذه المقاربة من خلال عرض تحديات الأمن السيبراني في الجزائر، ثم استشراف آفاق تطويرها مستقبلا.

المطلب الأول: تحديات الأمن السيبراني في الجزائر

في ظل التوسع المتزايد لاستخدام التكنولوجيا الرقمية، برزت تحديات متعددة تعيق تحقيق أمن سيبراني فعال في الجزائر، نتيجة تطور التهديدات الإلكترونية وتسارع وتيرتها. كما ترتبط هذه التحديات بعوامل تقنية، بشرية، وقانونية. مما يفرض ضرورة فهمها وتحليلها. وليه، يتناول هذا المطلب أبرز التحديات التي تواجه الأمن السيبراني في الجزائر.

أولا: جهود الدولة الجزائرية في تعزيز منظومة الأمن السيبراني: تبرز الدراسات أن الجزائر قطعت خطوات متعددة في مجال الأمن السيبراني؛ حيث اتجهت الدولة إلى تطوير منظومتها القانونية والمؤسساتية لمواجهة التهديدات الإلكترونية المتزايدة، وذلك من خلال سن قوانين خاصة تجرم مختلف صور الاعتداءات الإلكترونية، إلى جانب إنشاء هياكل امنية متخصصة مكلفة بمهام التحري والمتابعة ومكافحة الجريمة الإلكترونية، وهو ما يعكس وجود إرادة مؤسساتية واضحة لتعزيز الحماية الرقمية داخل الدولة. **(guedouari & allouache, 2025, p. 347)**

كما يتضح من التجربة الجزائرية أن مواجهة التهديدات السيبرانية لم تقتصر على الجانب الوطني فقط، بل شملت أيضا الانفتاح على التعاون الدولي، من خلال إبرام اتفاقيات وتبني

آليات للتنسيق وتبادل المعلومات مع الدول الأخرى، وهو ما يهدف إلى التصدي للجرائم الإلكترونية العابرة للحدود التي تتجاوز الإطار الجغرافي التقليدي للجريمة.

كما دعمت الجزائر هذه الجهود من خلال تنظيم حملات وطنية تحسيسية حول مخاطر الجرائم الإلكترونية، استهدفت الطلبة ومستخدمي مواقع التواصل الاجتماعي بهدف نشر الثقافة الأمنية الرقمية وتعزيز الوعي السيبراني لدى المواطنين. **(الجزائرية، 2024)**

وفي السياق ذاته، يظهر الإطار القانوني الجزائري تطورا تدريجيا في التعامل مع الجريمة الإلكترونية؛ حيث تم تجريم العديد من الأفعال المرتبطة بالولوج غير المشروع للأنظمة المعلوماتية، التلاعب بالمعطيات، والاستيلاء عليها أو اتلافها.**(يحيى و سليمان، 2024، صفحة 2)**

كما أن تطور النصوص القانونية لم يقتصر على التجريم فقط، بل شمل أيضا تعزيز الآليات الإجرائية مثل مراقبة الاتصالات الإلكترونية، تفتيش المنظومات المعلوماتية، وحجز المعطيات الرقمية. وهي إجراءات تعكس تطور أدوات الدولة في التعامل مع الجرائم الحديثة، خاصة في ظل تعقيد البيئة الرقمية وضرورة اعتماد وسائل تقنية متقدمة في التحري.**(يحيى و سليمان، 2024، الصفحات 3-7)**

ثانيا: الإشكالات المرتبطة بمواجهة الجرائم والتهديدات السيبرانية في الجزائر: تواجه الجزائر في مجال الأمن السيبراني جملة من التحديات المعقدة الناتجة عن التطور السريع للتكنولوجيا الرقمية؛ حيث أفرزت البيئة المعلوماتية الحديثة أنواعا متعددة من الجرائم الإلكترونية التي أثرت بشكل مباشر على الأفراد، المجتمع، والدولة، مما جعل هذه الجرائم تمثل تهديدا حقيقيا للأمن الوطني بمختلف أبعاده.

وتتميز الجريمة الإلكترونية بخصائص تجعل مكافحتها أكثر تعقيدا مقارنة بالجرائم التقليدية، إذ تتسم بطابعها غير المرئي والخفي، مما يجعل اكتشافها صعبا حتى أثناء وقوعها، كما أن

مرتكبيها يمتلكون قدرات تقنية تمكنهم من تنفيذ هجماتهم بدقة عالية مع ترك آثار محدودة أو شبه معدومة، وهو ما يصعب عملية جمع الأدلة الرقمية وتحليلها من قبل الجهات المختصة.**(guedouari و allouache، 2025، الصفحات 347-349)**

إضافة إلى ذلك، تعاني الجزائر من تحديات مرتبطة بتطور أشكال الجريمة الإلكترونية وتعددها؛ حيث تشمل هذه الجرائم عمليات التزوير المعلوماتي، الاختراق غير المشروع للأنظمة، الاستيلاء على المعطيات، إضافة إلى الإتلاف والاحتيال الإلكتروني، وهي جرائم تعتمد على التلاعب بالبيانات الرقمية وتوظيف الثغرات التقنية في الأنظمة المعلوماتية، مما يزيد من تعقيد مواجهتها.

كما تبرز صعوبات قانونية وتقنية في مكافحة هذا النوع من الجرائم، رغم وجود إطار تشريعي متطور نسبيا، إلا أن الطبيعة التقنية المعقدة لهذه الجرائم، وسرعة تطورها، واعتمادها على وسائل متقدمة، تجعل عملية الضبط والمتابعة والتتبع القضائي أكثر صعوبة، وهو ما يتطلب باستمرار تطوير أدوات التحري والتقنيات المستخدمة في المكافحة.**(يحيى و سليمان، 2024، الصفحات 3-6)**

وقد عالجت المصالح المختصة في الجزائر العديد من قضايا التشهير والابتزاز الإلكتروني المرتبطة بالحسابات الوهمية واستغلال الصور الشخصية، ما يعكس تنامي هذا النوع من الجرائم وصعوبة مكافحته في البيئة الرقمية الحديثة. **(الجزائرية ج.، 2024)**

يتضح أن الأمن السيبراني في الجزائر يمثل مجالا يتطور بشكل متسارع في ظل تزايد الجرائم الإلكترونية وتعقدها؛ حيث استطاعت الدولة الجزائرية تحقيق خطوات مهمة من خلال تطوير الإطار القانوني وإنشاء هياكل متخصصة لمكافحة هذه الجرائم. ومع ذلك، لا تزال هذه الجهود تواجه تحديات مرتبطة بطبيعة الجرائم الإلكترونية العابرة للحدود وصعوبة تتبعها تقنيا وقانونيا، مما يجعل تعزيز القدرات التقنية والتشريعية ضرورة مستمرة لمواكبة التحول الرقمي وحماية الأمن الوطني.

الشكل رقم21: تحديات الأمن السيبراني في الجزائر

المصدر: إعداد الطالبة

المطلب الثاني: آفاق تطوير المقاربة الاستراتيجية الجزائرية في الأمن السيبراني

تتجه المقاربة الاستراتيجية الجزائرية في مجال الأمن السيبراني نحو مرحلة من النضج المؤسساتي والتشريعي؛ حيث لم تعد تقتصر على الجوانب الدفاعية التقليدية، بل انتقلت إلى نموذج شامل يدمج بين حماية البنى التحتية الحيوية، السيادة الرقمية، وتطوير القدرات البشرية. تبرز الآفاق المستقبلية لهذه الآثار من خلال:

أولا: التحول نحو الاستباقية الاستراتيجية 2025-2029:

- التحول من الدفاع إلى الاستباق: يبرز التحليل الاستراتيجي أن الجزائر تتبنى "مقاربة فهم المسببات"، وهي استراتيجية تعتمد على التنبؤ بالنقاط العمياء في المنظومة قبل استغلالها من قبل الفواعل المهددة، مما ينقل الأمن السيبراني من خانة "تسيير الأزمات" إلى خانة "الوقاية البنيوية".
- عقيدة حماية البنى التحتية الحيوية: تهدف المقاربة المستقبلية إلى فك الارتباط بين الخدمات الأساسية للدولة والاحتمالات العالية للاختراق، من خلال دمج الأمن السيبراني

كجزء لا يتجزأ من مفهوم "السيادة الوطنية" في الفضاء الرقمي.**(المعلوماتية، 2024، الصفحات 2-6)**

ثانيا: البعد التحليلي لتوظيف الذكاء الاصطناعي في الردع السيبراني:

- الذكاء الاصطناعي كأداة للتحول الجيوسياسي: لا ينظر للذكاء الاصطناعي في المقاربة الجزائرية كأذاة تقنية فقط، بل كآلية لـ "أتمتة الدفاع"؛ حيث يتيح هذا التحول القدرة على مواجهة التهديدات السيبرانية التي تتجاوز سرعة الاستجابة البشرية التقليدية.
- تطوير نظم الاستجابة الذكية ضد الجرائم المعقدة: تشير الآفاق إلى ضرورة تبني نماذج تقنية تعتمد على "التعلم الآلي" لرصد أنماط الجريمة المنظمة، مما يعزز من قدرة الدولة على التكيف من التهديدات المتغيرة باستمرار.**(guedouari و allouache، 2025، صفحة 356)**

ثالثا: تحليل محورية "رأس المال البشري" في المنظومة الأمنية:

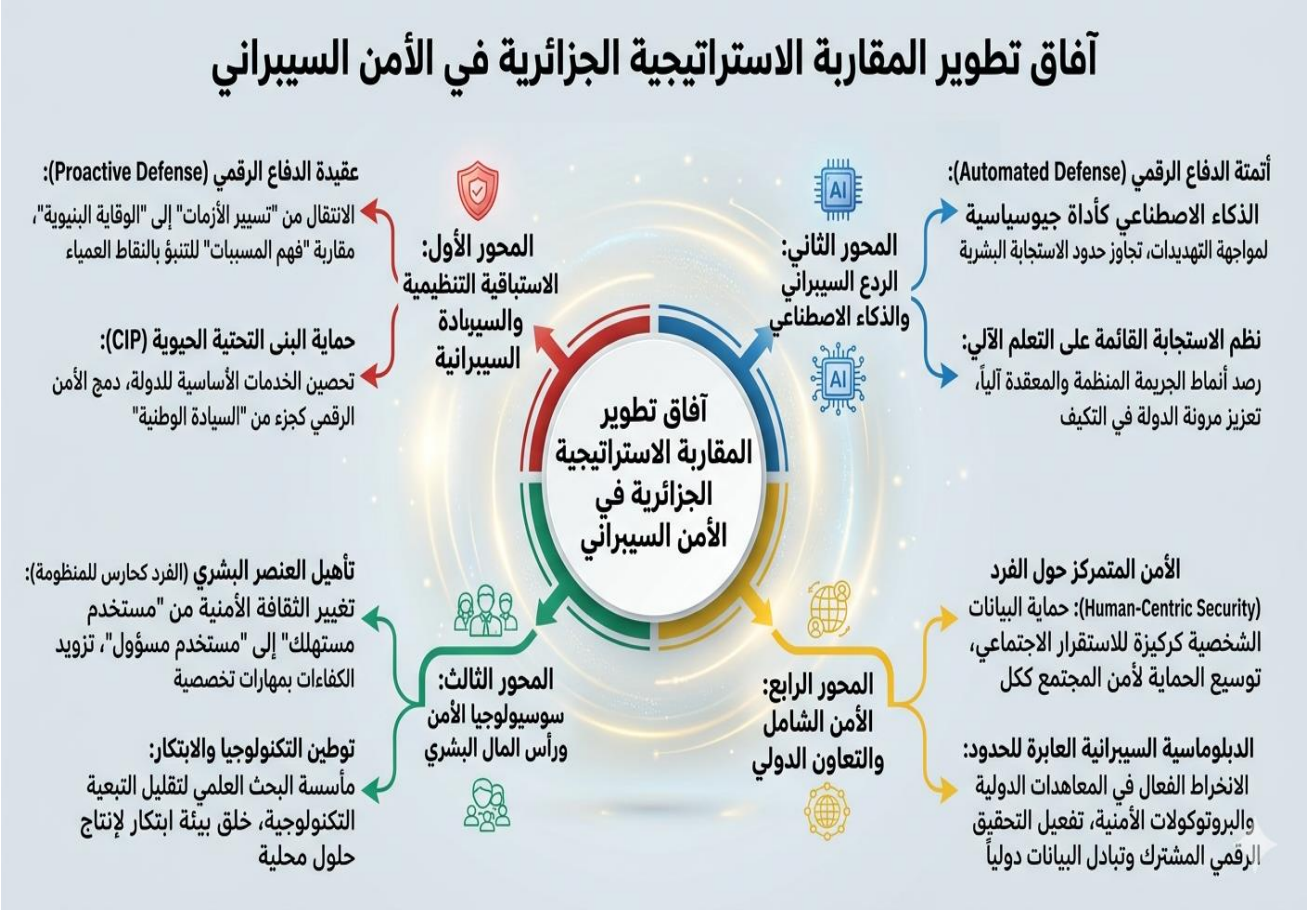
- سوسيولوجيا الأمن السيبراني: تنطلق المقاربة من فرضية أن "الإنسان هو الثغرة والأمان في آن واحد"؛ لذا تهدف الاستراتيجية إلى تحويل الفرد من مستخدم للمنظومة إلى حارس لها عبر تزويده بمهارات تخصصية تضمن الفعالية العملياتية.
- مأسسة الابتكار والبحث والتطوير: تتبنى الدولة رؤية تهدف إلى توطين التكنولوجيا السيبرانية من خلال دعم البحث العلمي، مما يقلل من التبعية التكنولوجية للخارج ويخلق بيئة ابتكار وطنية قادرة على انتاج حلول أمنية محلية الصنع.**(المعلوماتية، 2024، صفحة 11)**

رابعا: الانتقال نحو "الأمن الشامل" والتعاون العابر للحدود:

- الانزياح نحو الأمن المتمركز حول الفرد: تعكس السياسة الأمنية الجديدة تحولا جوهريا؛ حيث لم يعد الهدف حماية أجهزة الدولة فحسب، بل تأمين المعطيات الشخصية وحماية المجتمع من الهجمات التي تستهد الاستقرار الاجتماعي الرقمي.
- الدبلوماسية السيبرانية والتعاون الدولي: نظرا لطبيعة التهديدات الرقمية العابرة للحدود.**(djilali, 2026, pp. 499-512)**
- تتجه المقاربة نحو الانخراط الفعال في المعاهدات الدولية، كضرورة حتمية لتسهيل التحقيقات الرقمية المشتركة وتبادل البيانات الأمنية.

تعد المقاربة الاستراتيجية الجزائرية في الأمن السيبراني نموذجا متطورا يعكس الانتقال من الحلول التقنية الظرفية إلى رؤية وطنية شاملة ومتعددة الأبعاد، تهدف إلى ضمان السيادة الرقمية للدولة وحماية نسيجها المجتمعي وتستند هذه المقاربة في آفاقها المستقبلية على أربعة ركائز أساسية: أولها الاستباقية التنظيمية عبر سد الفجوات التشريعية وتحديث الأطر القانونية، وثانيها الابتكار التكنولوجي من خلال دمج الذكاء الاصطناعي في أنظمة الدفاع الرقمي، وثالثها الاستثمار في الرأسمال البشري لترسيخ ثقافة أمنية مستدامة، وأخيرا التكامل المؤسساتي.

الشكل رقم 22: آفاق تطوير المقاربة الاستراتيجية الجزائرية في الأمن السيبراني



المصدر: إعداد الطالبة

خلاصة الفصل الثالث:

يتضح من خلال هذا الفصل، أن الفكر الاستراتيجي الجزائري يتجه نحو ادماج البعد السيبراني كعنصر أساسي في منظومة الأمن الوطني، استجابة للتحولات التي أفرزتها النظام الدولي من بينها الحرب الروسية الأوكرانية. فقد أبرز تحليل واقع الأمن السيبراني في الجزائر وجود جهود تشريعية ومؤسساتية متنامية، مدعومة بسياسات وطنية تهدف إلى حماية البنى التحتية الحساسة وتعزيز الفضاء الرقمي، رغم استمرار بعض التحديات المرتبطة بتطور التهديدات وتعقيدها.

كما أظهرت الدراسة أن هذه الحرب أسهمت في إعادة تشكيل إدراك التهديدات؛ حيث أضحت الهجمات السيبرانية أداة استراتيجية مؤثرة، مما دفع الجزائر إلى ادراجها ضمن مقاربتها الاستراتيجية وتعزيز مفهوم السيادة الرقمية، مع التوجه نحو إدماج البعد الرقمي في العقيدة الدفاعية. وفي هذا السياق، تبين من خلال تقييم المقاربة الأمنية الرقمية أنها تتجه نحو تبني نموذج استباقي قائم على الوقاية والتخطيط المسبق، غير أن فعاليته تظل رهينة بتطوير القدرات التكنولوجية، تعزيز التنسيق المؤسساتي، والاستثمار في لموارد البشرية، بما يضمن التكيف مع التهديدات السيبرانية المتسارعة.

الخاتمة:

إن التحولات الجيوسياسية الراهنة التي فرضتها الثورة السيبرانية؛ حيث لم تعد الحرب الروسية–الأوكرانية مجرد نزاع حدودي كلاسيكي، بل أضحت مختبرا حيا لاستراتيجيات الحرب الهجينة التي تداخلت فيها الأسلحة التقليدية بالهجمات الرقمية. ومن خلال هذه الحركية، استطاع البحث رصد التحول الجوهري في الفكر الاستراتيجي المعاصر الذي انتقل من التركيز على الميدان الجغرافي الصرف إلى السيطرة على التدفقات المعلوماتية وتأمين البنى التحتية الحرجة، وهو ما استدعى بالضرورة فحص الانعكاسات المباشرة لهذا التحول على العقيدة الأمنية الجزائرية.

وفي سياق الإجابة على إشكالية الدراسة، فقد تأكد من خلال التحليل أن التوظيف السيبراني في الصراع الروسي–الأوكراني لم يكن أداة تكميلية، بل كان متغيرا مستقلا أحدث قطيعة مع المفاهيم الأمنية التقليدية، مما أدى بالضرورة إلى إعادة هيكلة الأولويات الاستراتيجية للدول الطامحة لحماية سيادتها، ومنها الجزائر. وقد أفضى هذا التحليل إلى إثبات صحة الفرضيات التي انطلقت منها الدراسة؛ فمن جهة ثبت أن الفضاء السيبراني بات يمثل "المجال الخامس" في الحروب الحديثة، ومن جهة أخرى تأكد أن صانع القرار الاستراتيجي الجزائري قد أدرك مبكرا أن التهديد الرقمي هو تهديد عابر للحدود، مما دفعه لتبني مقاربة استباقية تتجاوز الحلول التقنية لتصل إلى بناء منظومة دفاعية متكاملة.

من خلال الدراسة تم التوصل إلى النتائج التالية:

–انتقال مفهوم الأمن السيبراني من دائرة "الحماية التقنية" الضيقة إلى فضاء "الأمن القومي الوجودي"؛ حيث أصبح المعطى الرقمي هو المحدد الأساسي لموازين القوى في العلاقات الدولية المعاصرة.

-أثبتت الحرب الروسية-الأوكرانية فاعلية "السلاح السيبراني" في شل القدرات الحيوية للخصم دون الحاجة للتدخل العسكري المباشر في المراحل الأولى، مما شرعن استخدام الهجمات الرقمية كأداة ردع استراتيجي.

-تبين أن العقيدة الأمنية الجزائرية شهدت تحولا نوعيا من خلال الانتقال من "المقاربات الدفاعية السلبية" إلى "المأسسة الاستراتيجية للأمن الرقمي"، وهو ما ظهر في إنشاء الوكالة الوطنية لأمن النظم المعلوماتية وتحديث الأطر القانونية.

-السيادة الوطنية في العصر الرقمي أصبحت مرتبطة بمدى القدرة على توطين البيانات وحماية الشبكات الطاقوية والمالية من الاختراقات العابرة للحدود.

بناء على الدروس المستخلصة، نتقدم بالتوصيات التالية لتعزيز المنظومة الاستراتيجية الوطنية:

-إنشاء "مرصد وطني للدراسات الجيوسيبرانية" يجمع بين المختصين في العلوم السياسية ومهندسي البرمجيات، لتحليل أنماط الصراعات الرقمية الناشئة وتقديم تقارير دورية لصناع القرار.

-إدراج مقياس "الحروب الهجينة والأمن الرقمي" كمتطلب أساسي في جميع أطوار التعليم العالي، لرفع مستوى الوعي الاستراتيجي لدى النخبة القادمة.

-الإسراع في تنفيذ مشروع "السيادة السحابية الوطنية" لضمان استضافة البيانات الحساسة للمؤسسات السيادية الجزائرية بعيدا عن الخوادم الأجنبية التي قد تخضع لإملاءات القوى الكبرى في حالات النزاع.

-تفعيل نظام "المحاكاة الاستراتيجية للأزمات السيبرانية" بصفة دورية بين المؤسسات العسكرية والمدنية، لاختبار جاهزية البنى التحتية الوطنية لمواجهة سيناريوهات التخريب الرقمي.

-تبني "دبلوماسية سيبرانية" نشطة تهدف إلى بناء تحالفات تقنية مع دول الجنوب لتبادل التكنولوجيا الرقمية، بما يكسر احتكار القوى الغربية للبرمجيات والأنظمة الأمنية.

-تحفيز الشركات الناشئة الجزائرية المتخصصة في "الأمن البرمجي" من خلال صفقات عمومية، لتوطين حلول الحماية الرقمية وجعلها "جزائرية الصنع" بنسبة مئة بالمئة، مما يقلل من مخاطر "الأبواب الخلفية" في البرمجيات المستوردة.

قائمة المصادر والمراجع

أولا: المصادر

1.الجمهورية الجزائرية الديموقراطية الشعبية .دستور .(2020) .2020الجريدة الرسمية..1

ثانيا: المراجع

أ: المراجع باللغة العربية

الكتب

1.البسومي ,م ..تطور الفكر الاستراتيجي :Récupéré sur scribd .(15 02 ,2026) https://,www.scribd.com

2.الحمامصة ,ف .م .(2022) .الأمن السيبراني :المفهوم وتحديات العصر .(1 .éd) الأردن :دار الخليج للنشر والتوزيع.

3.شاهين ,م .ع .(2023) .الامن السيبراني و نظم حماية المعلومات.الاردن :دار يافا العلمية للنشر والتوزيع.

4.علي ,م .م .(2022) .الحروب السيبيرانية و نطور الاستراتيجية العسكرية للدول.مصر : دار الوفاء.

المقالات

1.الأمن السيبراني والمفاهيم المرتبطة بهمجلة طيبة للدراسات العلمية الأكاديمية 2022ص 44.

2.البلعزي ,ا .خ .(2024) .الحرب الروسية الاوكرانية:تداعياتها و تبعاتها الجيوسياسية و الاقتصادية و العسكرية على النظام الدولي .مجلة المشدى الاكاديمي.

3.الحيجاوي ,ا& .,الصريديذ ,س .م .(12 ,2019) .اثر الفكر الاستراتيجي في ريادة العمل الامني .المجلة العلميبة كلية التجارة.

4.الفتلاوي ,أ .ع .(2016) .الهجمات السيبرانية:مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر .مجلة المحقق المحلي للعلوم السياسية والقانونية.615 ,

الفضاء السيبراني وتحديات الأمن القومي للدول2022مجلة العلوم القانونية والاجتماعية47456

5.شاري ,خ& .,صادقي ,ا .(2023/2024) .الامن السيبيراني و اثره في تحقيق الامن القومي.الجزائر .برج بوعريريج.

6.عطية ,ا .ح .(2025) .الابعاد القانونية و الاجتماعيةللامن السيبيراني .مجلة الشرق الاوسط للدراسات القانونية و الفقهية.

7.عطية ,ا .(2019) .مكانة الامن السيبيراني في منظومة الامن الوطني الجزائري .مجلة مصداقية.

8.عمر ,ي .(07 ,2025) .اثر التكنولوجيا على نظريات الجغرافيا السياسية :الفضاء السيبيراني باعتباره اقليم جديد .المركز الديموقراطي العربي.

9.قبطة ,ف .ا .(s.d.) .استراتيجيات تعزيز الامن السيبيراني في الجزائر .مجلة الدراسات القانونية والسياسية.(2)

10.نجمة ,ش .(12 ,2023) .التطور المستمر للامن السيبيراني في العقيدة الدفاعية ج : الفرص و القيود .المجلة الجزائرية للسياسة.

11.نيوف ,ص .مدخل الى الغكر الاستراتيجي .الدنمارك :الاكاديمية العربية المفتوحة.

مذكرات واطروحات

1.القريطي ,د .ح .(2021) .الأمن السيبراني وحماية أمن المعلومات .(éd. 1)الاسكندرية : دار الفكر الجامعي.

2.بالة ,ع .(2012) .التهديدات الامنية في منطقة الساحل الافريقي وتداعياتها على الامن القومي الجزائري مالي انموذجا.باتنة :جامعة باتنة.

3.بكرش ,ا .(2018/2019) .انعكاسات التهديدات السيبيرانية على الامن الوطني الجزائري.تبسة :جامعة العربي التبسي.

4.بوستي ,ت .(2018/2019) .دراسات الامن الدولي:مقدمة في تطور مفهوم الامن عبر منظارات العلاقات الدولية .(p. 13) .جامعة 5ماي :جامعة 5ماي.

5.عيساوي ,ر .(2024) .استراتيجية مواجهة التهديدات الامنية السيبيرانية في الجزائر.كلية العلوم السياسية :جامعة قسنطينة.3

6.عيساوي ,ع .ا& .,زيتون ,س .(2023/2024) .اثار الذكاء الاصطناعي على الامن السيبيراني.دراسة حالة الجزائر.الوادي.

7.يحيى ,م& .,سليمان ,ن .(2024) .الجريمة الاليكترونية و تحديات الامن السيبيراني في الجزائر .مداخلة مقدمة الى ملتقى علمي.الجزائر :جامعة الوادي.

تقارير

1.الاستراتيجية الوطنية للانظمة المعلوماتية.2029-2025الجزائر :وكالة امن الانكمة المعلوماتية 2024 .

2.المعلوماتية ,و .ا .(2024) .الاستراتيجية الوطنية لامن الانظمة المعلوماتية-2025 .2029الجزائر :رئاسة الجمهورية :وكالة امن الانظمة المعلوماتية.

3.وزارة الدفاع الوطني الجزائري .(29 4 ,2024) .الامن السيبيراني

ملتقيات

1.محلف ,م .خ .(s.d.) .الواقعية الجديدة في العلاقات الدولية الافتراضات، التصنيفات، الاسس، رؤية تحليلية.2018 .

محاضرات

1.شارنرش .(2024) .المقاربة الجيوسياسية الروسية في منطقة البحر المتوسط، ابعاد للدراسات الاستراتيجية.

مواقع الكترونية

1.السيساوي ,م .ح .(11 02 ,2025) .النظرية الواقعية فب العلاقات الدولية Récupéré . sur Noor book: https://www.noor-book.com

2.الوائلي ,ع .ع .(02 ,2026) .مركز حمورابي للبحوث ,2026 ,27 3 Consulté le . sur hersiraq: http://www.hersiraq.net

3.مشروع قانون الامن السيبيراني على طاولة الحكومة .(30 6 ,2025) Consulté le . 4 1, 2026, sur africa press: http:/www.africapress.com

ب: المراجع باللغة الأجنبية

Book :

1.Anthony Craig, B. V. (2018). Realism and Cyber Conflict: Security in the Digital Age. Bristol: E-International Relations.

2.Cavelty, M. D. (2019). The Politics of Cyber Security. Cambridge University Press.

3.Esposito, M. (2023). Géopolitique du Cyberspace Méditerranéen et Doctrines Militaires. Lyon: Édition de la Méditerranée.

4.Flint, G. (2006). The Geopolitics of Eurasia. London: Routledge.

5.Hansen, L., & Nissenbaum, H. (2010). Cyber Security and Global Governance. London: Routledge.

6.Katchanovski, I. (2026). The Russian Ukraine War and Its Origins: From the Maidan to Ukraine War. Cham, Switzerland: Palgrave Macmillan.

7.Kenichi, O. (1982). The Mind of the Strategist: The Art of Japanese Business. New York: McGraw-Hill.

8.Keohane, R. O., & Nye, J. S. (2012). Power and Interdependence. New York: Longman.

9.Mearsheimer, J. (2001). The Tragedy of Great Power Politics. New York: W.W. Norton.

10.Singer, P., & Friedman, A. (2014). Cyber Security and Cyber War: What Everyone Needs to Know. New York: Oxford University Press.

11.Taras Kuzio, & Paul, D. A. (2018). The Sources of Russia's Great Power Politics: Ukraine and the Challenge to the European Order. Bristol: International Relations.

12.Walkins, M. (2020). The Six Disciplines of Strategic Thinking. Boston: Harvard Business Review Press.

13.Waltz, K. (1979). Theory of International Politics. Reading, MA: Addison-Wesley.

14.Wilson, A. (2017). Ukraine in Conflict. Bristol: International Relations.

Journal Articles:

1.Diec, J. (2024). War as an Inevitable Factor of Change: The Impact of Neo-Eurasianist Geopolitics on the Dynamics of Russia's Security Policy After 1991. Politeja.

2.Djilali, O. (2026). The Algerian Public: Security Policy on Combating Cyber Crime. Academic Journal of Legal and Political Researches, 10(01).

3.Draou, A. (2025). Cyber Security in Algeria: A Strategic Approach to Address Regional Challenges. Journal of Economic Integration, 13(02).

4.Gasimov, K., & Laruelle, M. (2026). Eurasia and Eschatology: Dugin's Antiliberal Resonances in the Muslim World. Studies in East European Thought.

5.Guedouari, F. Z., & Allouache, m. (2025). The Role of Cyber Security in Combating Cyber Crime in Algeria. Revue des Sciences Humaines, (36).

6.Kapsokoli, E. (2025). Weaponizing Cyberspace: The Russia–Ukrainian War. Security Science Journal, 6.

7.Kelemen, R. (2023). The Impact of the Russian–Ukrainian Hybrid War on the European Union's Cyber Security Policies. Academic and Applied Research in Military and Public Management Science, 22.

8.Khadidja, K., & Djamel, B. (2025). The Strategy of the Algerian State for Information Security. The Journal of El-Ryssala for Studies and Research in Humanities, 10(04).

9.Krasner, S. D. (1989). Structural Causes and Regime Consequences: Regimes as Intervening Variables. International Organization.

10.Kurnaz, I. (2024). Rus Imparatorluk Geopolitiginin Yenideolojisisin Tahayyulu. Selcuk Universitesi Sosyal Bilimler Enstitusu Dergisi.

11.Mohamed, D., & Danish, A. (2024). The Russian-Ukraine War: Causes, Consequences and Solutions. Eurasian Journal of Management and Social Sciences, 5.

12.Saeidah, A. (2026). Socio-Economic Consequences of the Russian-Ukrainian War. Scientia Fructuosa.

13.Sehailia, S. (2025). Algeria's Cyber Security Strategy: Defensive Techniques. Journal of Al-Nepad for Political Studies, 1.

14.Sereir, H. (2023). An In-depth Study for a Proposed National Cyber Security Strategy for Digital Economy in Algeria. Journal of Economies and Management, 23(01).

15.Sipos, Z. (2023). Cyber Security in Algeria. Journal of Security and Sustainability Issues, 13.

16.Sloan, G. (2017). Sir Halford Mackinder: The Heartland Theory Then and Now. Orbis.

17.Toksoz, G., & Zengin, F. (2018). Heartland Revisited: Mackinder in the 21st Century. Geopolitics.

Theses & Dissertations:

1.Benlarbi, A. E. (2024). La transformation numérique des armées au Maghreb: Le cas de l'Algérie. Alger: École Nationale Supérieure de Guerre.

2.Kyoto University (2017). Study on Permutation Polynomials Over a Ring of Modulo 2w and Their Applications to Cryptography.

Reports & Analysis:

1.Aorenstein, M. (2022). Russia's Use of Cyber Attacks: Lessons from the Second Ukraine War. Foreign Policy Research Institute Analysis.

2.Black, D. (2023). Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences. London.

3.Boulegue, M. (2025). Russia's Struggle to Modernize its Military Industry. Chatham House.

4.Cobo, I. F. (2025). The War in Ukraine in 2025. IEEE Analysis Document.

5.Dugin, A. (2022). Philosophy and Strategy. Analytical Paper Strategies.

6.Russia (2025). Russian Offensive Campaign Assessment. ISW: Institute for the Study of War.

7.Schulze, m., & Mika, K. (2023). Cyber Operations in Russia's War against Ukraine. SWP Comment.

8.World Bank (2025). Global Economic Prospects. America: World Bank.

Conferences & Preprints:

1.Arslan, A. S. (2023). Neorealist Analysis of Security Dilemma in Cyber Space. APSA Preprints.

2.Enigma (2020). A Review on Mathematical Strength and Analysis of Enigma. arXiv preprint.

3.Thachuk, N. (2025). Ukraine as the Frontline of European Cyber Aggression. NATO Cooperative Cyber Defence Centre of Excellence.

4.Yigit, Y., Ferrag, M. A., et al. (2024). Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities. arXiv preprint.

Lectures & Contributions:

1.H. Yasui, & H. S. (2025). The Scope of the Ripeness Theory in the Russo-Ukrainian War. In: The Impact of the Russo-Ukrainian War. Singapore: Kutuyiv.

2.Michael N. Smith (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge.

3.State Security Objectives and International Security Protocols (2011). National Open University of Nigeria. Abuja.

4.Yushkov, A., & Micheal, A. (2024). Fiscal and Economic Effects of the Russo-Ukrainian War. In: Russian Regions in Wartime.

Newspapers:

1.Discon, W. (2025). Ukraine as the Cyber Spanish Civil War. Ukrainian Polity Maker.

Electronic Sources:

1.Kramer, M. (s.d.). Neorealism Nuclear Proliferation and East Central Europe. Retrieved from: https://csis.org

2.Snyder, G. (s.d.). Realism and the Struggle for Security. Retrieved from: https://politics.org

فهرس الخرائط / الأشكال

فهرس الخرائط:

فهرس الأشكال:

فهرس الموضوعات