وزارة التعليم العالي و البحث العلمي.

المدرسة الوطنية العليا للعلوم السياسية الشهيد زدور محمد إبراهيم القاسم.

البعد السيبراني للأمـن القومي الجزائـري: دراسة مقارنة لنماذج دولية رائدة.

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في ميدان الحقوق والعلوم السياسية

شعبة العلوم السياسية، تخصص العلاقات الدولية.

إشراف الاستاذ: خننو فاتـح

من إعداد الطالب: بوطمين وائل خليل الرحمـان

لجنة المناقشة			
الاسم واللقب	الرتبة العلمية	الصفة	مؤسسة الانتماء
ا.د إبتسام أوعشرين	أستاذ	رئيسا	المدرسة الوطنية للعلوم السياسية
ا.د ناصر عامر	أستاذ	عضوا مناقشا	المدرسة الوطنية للعلوم السياسية
ا.د فاتح خننو	أستاذ	مشرفا و مقررا	المدرسة الوطنية للعلوم السياسية

السنة الجامعية : 2025/2024

الحمد لله الذي بنعمته تتم الصالحات نحمده و نستعينه و نستهديه، و نصلي و نسلم على سيدنا محمد و على آله و صحبه أجمعين .

"وَلَقَدْ صَرَّفْنَا فِي هَٰذَا الْقُرْآنِ لِلنَّاسِ مِن كُلِّ مَثَلٍ ۚ وَكَانَ الْإِنسَانُ أَكْثَرَ شَيْءٍ جَدَلًا."

الأية 54 من سورة الكهف

الشكر والإهداء:

أتقدم بجزيل الشكر و التقدير الى أساتذتي بمشواري الجامعي، و الى الأستاذ المشرف فاتح خننو على توجيهاته القيمة، و أتوجه بخالص الإمتنان لعائلتي الكريمة على دعمها الدائم، و لأصدقائي طيلة هذه الرحلة العلمية.

أهدي هذا العمل لوالديَّ العزيزين.

الملخص

يعالج الموضوع "**البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة**"، من خلال تحليل معمق للتهديدات السيبرانية باعتبارها أحد أبرز التحديات غير التقليدية التي تواجه الدول الحديثة، لاسيما تلك التي تعاني من هشاشة في بنيتها الرقمية. تنطلق الدراسة من فرضية مفادها أن التهديدات السيبرانية تتجاوز الطابع التقني، لتطال أبعاد السيادة الوطنية، والاستقرار المؤسساتي، والتماسك المجتمعي.

تناولنا تطور مفهوم الأمن في العلاقات الدولية ما بعد نهاية الحرب الباردة، وتوسعه ليشمل الجوانب السيبرانية، مع التركيز على الحالة الجزائرية في ظل بيئة رقمية معولمة. كما تستعرض نماذج عالمية رائدة في إدارة الأمن السيبراني (الولايات المتحدة، الصين، روسيا).

اعتمدنا على مناهج متعددة، واقترابات مفاهيمية متنوعة، مما مكن من مقاربة شاملة للظاهرة. وخلصت إلى ضرورة تبني استراتيجية وطنية متعددة الأبعاد لتعزيز السيادة الرقمية، ودمج الأمن السيبراني ضمن هندسة الأمن الوطني.

الكلمات المفتاحية:

الأمن السيبراني – التهديدات السيبرانية – الأمن الوطني...

Abstract

The topic "**The Cyber Dimension of Algerian National Security: A Comparative Study of Leading International Models**" addresses, through an in-depth analysis, the nature of cyber threats as one of the most prominent non-traditional challenges facing modern states—particularly those with fragile digital infrastructures. The study is based on the hypothesis that cyber threats extend beyond their technical scope,

impacting national sovereignty, institutional stability, and societal cohesion.

It examines the evolution of the concept of security in international relations after the end of the Cold War, highlighting its expansion to include cyber dimensions, with a particular focus on the Algerian case in a globalized digital environment. The research also reviews leading international models in cybersecurity governance, specifically the United States, China, and Russia.

By adopting multiple methodologies and diverse conceptual approaches, the study offers a comprehensive perspective on the phenomenon. It concludes with the necessity of adopting a multidimensional national strategy to reinforce digital sovereignty and to integrate cybersecurity into the broader architecture of national security.

Keywords):

Cybersecurity – Cyber threats – National security …

مقدمـــة

شهدت البيئة الدولية منذ مطلع التسعينيات، ومع نهاية الحرب الباردة وانهيار الثنائية القطبية، تحولات عميقة في القوة والأمن. فقد تراجع التركيز على التهديدات العسكرية التقليدية لصالح أنماط جديدة من التهديدات اللاتماثلية كالحروب بالوكالة، الحروب الهجينة، الدعاية و نشر المعلومات المضللة، وأبرزها **التهديدات السيبرانية**، التي سرعان ما تحولت إلى محور موضوع بحث قي أجندة الدرسات الدولية وموضوع محل اهتمام صناع القرار.

فمنذ ظهور الثورة التكنولوجية وتوسع استخداماتها في المستويين المدني والعسكري، أصبح **الفضاء السيبراني** مجالا حيويا جديدا للمنافسة والصراع، لا تحدّه الجغرافيا ولا تضبطه قواعد دولية واضحة. وتزايد هذا التوجه مع بروز مفهوم **الأمن السيبراني** كفرع مستقل من الدراسات الأمنية، يواكب تطّور التكنولوجيات الرقمية وتداخلها في مفاصل الدولة الحديثة، من الطاقة إلى الدفاع، ومن البنوك إلى الإعلام.

تعتبر الدول الأكثر تأثيرا في النظام الدولي كالولايات المتحدة، روسيا، والصين، الأمن السيبراني جزءا لا يتجزأ من أمنها القومي، وقد خصصت له عقائد عسكرية واستراتيجيات وطنية، بل وظفته كأداة ردع وهيمنة في علاقاتها الدولية. وفي المقابل، تجد بعض الدول الطامحة نفسها أمام معادلة معقدة: "الاستفادة من الثورة الرقمية دون الانكشاف الأمني والوقوع في تبعية تكنولوجية تهدد سيادتها الرقمية."

الجزائر، بدورها لم تكن بمنأى عن هذه التحولات. فمنذ بداية الألفية الثالثة، ومع تنامي الاعتماد على الرقمنة والإدارة الإلكترونية، بدأت ملامح تشكل التهديدات السيبرانية تظهر بشكل متزايد، سواء من خلال محاولات اختراق البنى التحتية، أو عبر حملات تضليل رقمي، أو من خلال تسريبات تمس مؤسسات حساسة.

إن خطورة هذه التهديدات لا تكمن فقط في بعدها التقني، بل في قدرتها على المساس بالأمن القومي الشامل، من خلال تعطيل مؤسسات الدولة، زعزعة الثقة العامة، توجيه الرأي العام،

وخلق اختلالات سياسية واقتصادية واجتماعية وثقافية عميقة. وهذا ما يجعل من **السيادة الرقمية** شرطا أساسيا لحماية الاستقلال الوطني في العصر الرقمي.

وعليه، تكتسي دراسة موضوع "**البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة** "أهمية متزايدة لكونه يعالج أحد أخطر التحديات المعاصرة، ويضع الجزائر في مواجهة ضرورة بلورة رؤية استراتيجية شاملة تعزز أمنها السيبراني، انطلاقا من تشخيص دقيق للواقع، واستفادة عقلانية من التجارب الدولية الرائدة.

وتهدف هذه الدراسة إلى تقديم مقاربة متعددة الأبعاد، تجمع بين التحليل النظري والاستعراض المقارن، من أجل فهم آليات التهديد، ورصد التحديات البنيوية، وتقديم بدائل استشرافية تضمن التحصين السيبراني للدولة الجزائرية، بوصفه رهانا سياديا واستراتيجيا في عالم رقمي متقلب.

1/المشكلة البحثية

في ظل التحولات الرقمية المتسارعة، أصبح الفضاء السيبراني ساحة جديدة للصراع الدولي، حيث لم تعد التهديدات تقتصر على المجال التقليدي العسكري، بل امتدت إلى تهديدات غير تقليدية، أبرزها الهجمات السيبرانية التي تمس السيادة الرقمية للدول وتهدد أمنها القومي. وتواجه الجزائر تحديات بنيوية وتقنية، داخلية وخارجية، تهدّد منظومة أمنها السيبراني بشكل كبير، مما يجعلها هدفا محتملا للهجمات الإلكترونية والتهديدات السيبرانية. وانطلاقا من هذا الواقع، تبرز الإشكالية المركزية للدراسة في التساؤل التالي:

كيف يشكل الأمن السيبراني تحديا إستراتيجيا لمنظومة الامن الوطني الجزائري، ضمن سياق البيئة الدولية المعقدة ؟

وينبثق عن هذه الإشكالية الرئيسية عدد من التساؤلات الفرعية أهمها:

1.ما هي أبرز التهديدات السيبرانية التي تواجه الدول ؟

2.كيف تؤثر هذه التهديدات على وظائف الدولة الحيوية (الدفاع، الاقتصاد، التعليم، البنى التحتية...)؟

3.كيف يمكن الاستفادة من التجارب الدولية (الأمريكية، الروسية، الصينية) لتعزيز الأمن السيبراني في الجزائر؟

2/الفروض العلمية :

الفرضية الأولى:

الاختراقات والهجمات على البنى التحتية الحيوية من ابرز التهديدات التي تمس ابعاد الامن الوطني .

الفرضية الثانية:

الاختراقات الإلكترونية تستهدف المؤسسات الحيوية مما يؤدي إلى شلل مؤقت في أدائها.

الفرضية الثالثة:

تمثل التجارب المقارنة للدول الرائدة في الامن السيبراني نموذجا بارزا يمكن الاستفادة منها لتعزيز المنظومة السيبرانية الوطنية الجزائرية .

3/مجالات الدراسة:

أ.المجال الموضوعي:

تعالج الدراسة موضوع الأمن السيبراني بوصفه أحد أبعاد الأمن القومي المعاصر، وذلك من خلال تحليل مفاهيمه النظرية وتطوراته التقنية إضافة إلى دراسة أجيال الصراع الدولي المرتبطة بالفضاء السيبراني وارتباطه بمفاهيم القوة والردع في العلاقات الدولية. كما تتناول الدراسة ظاهرة الجريمة السيبرانية باعتبارها تهديدا عابرا للحدود، مركزة على أبعادها القانونية والاستراتيجية.

ب.المجال المكاني:

تتوزع الدراسة عبر أربع بيئات جغرافية وسياسية مختلفة، حيث يتم تحليل النموذج الأمريكي

بوصفه مرجعا رائدا في بناء الاستراتيجيات السيبرانية، إلى جانب دراسة التجربتين الروسية والصينية من حيث الخصوصيات التقنية والأمنية في مواجهة التهديدات الرقمية، كما تتناول الدراسة الجزائر كنموذج عربي إفريقي ناشئ يسعى لتطوير بنيته السيبرانية الوطنية، مما يسمح بإجراء مقاربة مقارنة متعددة السياقات لفهم التفاوت في التعاطي مع الأمن السيبراني بين الدول ذات الإمكانيات المختلفة.

ج.المجال الزمني:

تمتد الدراسة من الفترة 2001 إلى السداسي الاول من سنة 2025، وهي مرحلة مفصلية شهدت تحولات كبرى في مفاهيم الأمن والصراع، نتيجة للثورة الرقمية وظهور الفضاء السيبراني كساحة صراع جديدة. وقد ركزت الدراسة بشكل خاص على مرحلة ما بعد 2010 التي تميزت بتصاعد الهجمات السيبرانية وتطور التشريعات والمؤسسات السيبرانية.

4/أهمية الدراسة:

تكتسب هذه الدراسة أهميتها من تناولها لموضوع **الأمن السيبراني** كأحد أبرز التحديات السيادية في عصر الثورة الرقمية، ضمن مقاربة شاملة تربط بين الأبعاد النظرية، الاستراتيجية، والقانونية، وذلك لعدة اعتبارات:

- الطابع المتسارع والمركب للتهديدات السيبرانية والتي أصبحت تتجاوز الحدود الجغرافية والتقليدية، وتمس جوهر الأمن القومي للدول عبر استهداف البنى التحتية والمجتمعات والمؤسسات الحيوية.
- أهمية فهم التحول في مفاهيم الصراع الدولي من الحروب التقليدية إلى الحروب السيبرانية الهجينة بما في ذلك استيعاب أجيال الحروب الحديثة وأدوات النفوذ غير التقليدية في بيئة رقمية متغيرة.

- الحاجة الملحة لبناء منظومة وطنية فعالة للأمن السيبراني في الجزائر سواء على المستوى التشريعي أو المؤسساتي أو الاستراتيجي لمواجهة التحديات المستجدة وتعزيز صمود الدولة أمام التهديدات العابرة للحدود.
- الفراغ البحثي العربي والمغاربي في دراسة الأمن السيبراني ضمن إطار مقارن يجمع بين النماذج الدولية الكبرى (الولايات المتحدة، روسيا، الصين) والسياق الجزائري، مما يمنح هذه الدراسة قيمة مضافة على مستوى التحليل المقارن والسياسات العمومية.
- إسهام الدراسة في تعميق الفهم الأكاديمي لمسارات الردع السيبراني، وأنماط الفاعلين الدولتيين وغير الدولتيين مما يثري أدبيات العلاقات الدولية والأمن غير التقليدي في البيئة الرقمية.

5/أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف العلمية والتحليلية المرتبطة بفهم وتحليل الأمن السيبراني كأداة صراع دولي ووسيلة تهديد للأمن القومي، من خلال:

- فهم الخلفيات النظرية والتاريخية لنشوء الأمن السيبراني وتطوره ضمن حقل العلاقات الدولية خاصة في ظل تصاعد أهمية الفضاء الرقمي كامتداد للنفوذ والسيادة.
- تحليل التهديدات السيبرانية في أبعادها العسكرية، الاقتصادية، القانونية، والمجتمعية، من خلال نماذج واقعية وتطبيقات دولية (الولايات المتحدة، روسيا، الصين).
- تسليط الضوء على تحولات مفهوم الصراع عبر أجيال الحروب الحديثة خصوصا الجيلين الخامس والسادس، وارتباطهما بالأدوات السيبرانية والهجينة.
- تشخيص واقع الأمن السيبراني في الجزائر من حيث الاستجابة القانونية، القدرات المؤسساتية، والمخاطر البنيوية، وموقعه ضمن منظومة الأمن القومي.
- رصد وتحليل الجريمة السيبرانية كتهديد ناشئ متعدد الأوجه واستعراض أبرز صورها وأهدافها وآليات مكافحتها، محليا ودوليا.

- تقديم توصيات عملية قابلة للتنفيذ من أجل دعم بناء استراتيجية وطنية متكاملة للأمن السيبراني في الجزائر، بالاستفادة من التجارب المقارنة.

6/أسباب اختيار الموضوع:

تم اختيار موضوع الأمن السيبراني كأحد أنماط الصراع الدولي والجريمة العابرة للحدود استجابة لعدة اعتبارات معرفية واستراتيجية أبرزها:

- تصاعد أهمية الفضاء السيبراني كساحة صراع مركزية في العلاقات الدولية وظهوره كأداة جديدة لإعادة تشكيل مفاهيم القوة والردع والتهديد خارج الأطر التقليدية.
- تزايد حجم وخطورة التهديدات السيبرانية الموجهة ضد البنى التحتية الحيوية والمؤسسات السيادية ما يفرض الحاجة إلى دراسات تحليلية معمقة لفهم طبيعتها وآليات مواجهتها.
- ندرة الدراسات الجزائرية التي تتناول الأمن السيبراني من منظور استراتيجي مقارن يدمج بين البعد التقني والبعد السياسي – القانوني ويقارن بين التجارب الدولية والسياق الوطني.
- الرغبة في المساهمة العلمية في حقل دراسات الأمن غير التقليدي واستكشاف تقاطعاته مع التكنولوجيا والقانون والسياسة، بما يعزز من الأدبيات العربية حول الموضوع.
- أهمية الموضوع من الناحية العملية الراهنة حيث يشكل أداة لصياغة سياسات وقائية واستباقية لحماية الأمن الوطني، ومجالا خصبا للبحث والتفكير الاستراتيجي في ظل البيئة الرقمية المتسارعة.

7/مناهج الدراسة:

نظرا للطبيعة المركبة والعابرة للتخصصات لموضوع **الأمن السيبراني كتهديد استراتيجي ناشئ** في حقل العلاقات الدولية، فقد تم اعتماد مجموعة من المناهج المتكاملة، المستمدة من مناهج **العلوم السياسية والدراسات الاستراتيجية**، وهي:

أ .المنهج الاستقرائي *(Inductive Method)*

ينطلق من الحالات الجزئية والوقائع الميدانية نحو تعميمات ونماذج تفسيرية أوسع.

تم توظيفه لتحليل أمثلة واقعية لهجمات سيبرانية مسجلة على الصعيدين الإقليمي والدولي بهدف استقراء خصائص التهديدات وأنماطها وتقدير إمكانية انعكاسها على السياق الجزائري. ساعد في بناء فرضيات أولية حول أنماط التهديدات، وتحديد مكامن الضعف في المنظومة الوطنية. مكن من استخراج تأثيرات ملموسة للهجمات على المؤسسات الاقتصادية، التعليمية، والسياسية.

ب .المنهج المقارن *(Comparative Method)*

يقوم على مقارنة السياسات والنماذج بين دول أو نظم مختلفة لاستخلاص نقاط القوة والضعف. استخدم لمقارنة التجربة الجزائرية في الأمن السيبراني مع تجارب دولية (الولايات المتحدة، روسيا، الصين، إستونيا...).

مكن من تحليل الفوارق في العقيدة السيبرانية، والأطر القانونية، والبنية المؤسسية. ساعد على تقديم مقترحات مستلهمة من النماذج الناجحة وقابلة للتكيف مع السياق المحلي.

8/النظريات و الاقترابات المعتمدة:

في إطار دراسة التهديدات السيبرانية كظاهرة دولية عابرة للحدود تم توظيف مجموعة من النظريات و الاقترابات المتكاملة التي سمحت بفهم الأبعاد المختلفة للأمن السيبراني من زوايا متعددة:

أ- الواقعية الجديدة(Neorealism)

تركز الواقعية الجديدة على الأمن من منظور الدولة، باعتبارها الفاعل الأساسي في النظام الدولي، ويرى أن الصراعات تنبع من سعي الدول إلى تعزيز بقائها ضمن بيئة دولية فوضوية.

مكنت من تحليل الأمن السيبراني كامتداد للأمن القومي التقليدي.

فسرت السباق بين القوى الكبرى لتطوير قدرات هجومية ودفاعية سيبرانية (سباق التسلح السيبراني).

ب-نظرية القوة الناعمة(Soft Power Theory – Joseph Nye)

قدم جوزيف ناي مفهوم القوة الناعمة باعتبارها القدرة على التأثير في سلوك الآخرين دون استخدام الإكراه أو القوة العسكرية. وفي السنوات الأخيرة تطور المفهوم ليشمل الفضاء السيبراني كمنصة لنشر القيم والتأثير الناعم و الصلب .

مكنت النظرية من تحليل استخدام بعض الدول للفضاء الرقمي كأداة جذب وتأثير من خلال المنصات الثقافية الدعاية السياسية أو الإعلام الرقمي الموجه. كما ساعدت على فهم كيف تتحول الهيمنة التقنية (مثل سيطرة الشركات الأمريكية على شبكات التواصل) إلى أدوات قوة ناعمة تؤثر في الرأي العام والسياسات داخل الدول الأخرى.

وفرت إطارا لفهم التنافس السيبراني بين القوى الكبرى ليس فقط على المستوى العسكري، بل أيضا على مستوى النفوذ الثقافي والرمزي في الفضاء الرقمي.

ج-نظرية الأمننة – مدرسة كوبنهاغن(Securitization Theory)

تعنى بكيفية "بناء" التهديدات من خلال الخطاب السياسي والإعلامي وليس فقط عبر وجود خطر مادي موضوعي.

فسرت كيف يقدم الأمن السيبراني كقضية وجودية للدولة من خلال خطابات الفاعلين الرسميين.

د- الاقتراب الجيوسياسي:

يرتكز هذا الاقتراب على فهم الدولة لطبيعة التهديدات السيبرانية وسبل التصدي لها، أو ما يعرف بجيوسياسة الفضاء السيبراني.

استخدم لتحليل كيفية تأثير التهديدات السيبرانية على الأمن الوطني والسيادة الرقمية، ودراسة استجابة الدولة لهذه التهديدات من خلال استراتيجيات الدفاع والهجوم المتكاملة.

و- الاقتراب البنيوي-الوظيفي

يركز على فهم العلاقة بين بنى الدولة ووظائفها الحيوية وتأثير التغيرات التقنية عليها.

استخدم لتحليل كيف تؤثر التهديدات السيبرانية على الوظائف الحيوية مثل الصحة، التعليم، الاقتصاد، والدفاع.

ز- الاقتراب القانوني والمؤسساتي

يتناول القواعد والتشريعات المنظمة للسلوك الدولي في مجال الأمن السيبراني وعلاقات التعاون أو الصراع.

ساعد على تحليل الاتفاقيات الدولية (مثل اتفاقية بودابست)، ومقارنتها بالتشريعات المحلية.

الفصل الأول :الإطار المفاهيمي والنظري للأمن السيبراني.

المبحث الأول: الأمن السيبراني و اجيال الصراع الدولي .

المطلب الأول: السياق التاريخي لنشأة الأمن السيبراني وتطوره في حقل العلاقات الدولية.

يعد الأمن السيبراني من القضايا الناشئة حديثا في حقل العلاقات الدولية، حيث يعكس تحولا نوعيا في فهم التهديدات الأمنية ضمن البيئة الرقمية المتغيرة. فقد ترافق تطور التكنولوجيا الرقمية مع بروز نقاشات أكاديمية حول تداعياتها على مفاهيم الأمن والسيادة والقوة وهو ما استدعى إعادة النظر في الأدوات التحليلية التقليدية داخل حقل الدراسات الأمنية.

في السبعينات ظهر أول فيروس رقمي على شبكة "**أربانت**"[1]، وهي واحدة من أوائل الشبكات التي نقلت البيانات باستخدام تقنية تبديل الرزم. على الرغم من أن هذا الفيروس لم يتسبب في أضرار جسيمة، إلا أنه كان حافزا لتطوير أساليب الوقاية والأمان على الشبكات. هذه الفترة شهدت بداية استخدام التشفير في شبكات الاتصال حيث طور معهد ماساتشوستس للتقنية في عام 1983 نظاما يعتمد على التشفير ويسمى **(Kerberos)** والذي أصبح أساسا لتقنيات الأمن السيبراني الحديثة.

شهدت التسعينات تحولا كبيرا مع ظهور الإنترنت وانتشاره الواسع، ما أدى إلى تغير ملامح الحرب السيبرانية. أصبحت الهجمات الإلكترونية أكثر تنوعا وتعقيدا، وبدأت تظهر تقنيات مثل التصيد الاحتيالي والهجمات الموزعة لحجب الخدمة. هذه الفترة، التي يمكن وصفها بـ "الحرب السيبرانية الباردة"، شهدت تسابق الدول على تطوير تقنيات الأمن السيبراني لحماية بنيتها التحتية

[1] شبكة ARPANET : هي شبكة حاسوبية أمريكية تم تطويرها في أواخر الستينات بواسطة وكالة مشاريع الأبحاث المتقدمة(DARPA) ، وكانت الأساس لتطوير الإنترنت الحديث. في السبعينات، تم تشغيل أول فيروس حاسوبي، وهو برنامجCreeper ، على شبكةARPANET ، وكان يهدف فقط إلى التنقل عبر الشبكة وعرض رسالة"I'm the creeper, catch me if you can!" ، دون التسبب في أضرار. ولوقف انتشاره، تم تطوير برنامجReaper ، الذي يُعتبر أول برنامج مكافحة الفيروسات.

الرقمية. بدأت الجيوش في استخدام تقنيات الإنترنت بشكل موسع، مما جعل الأمن السيبراني جزءا أساسيا من استراتيجيات الدفاع العسكري.

يمكن تتبع بدايات التفكير المنظم حول الأمن السيبراني إلى مطلع التسعينيات، لاسيما من خلال المفهومين الأساسيين :حرب الإنترنت (Netwar) والحرب السيبرانية(Cyberwar) ، واللذين ظهرا في سياق التحول الهيكلي بعد الحرب الباردة. حيث إن انتهاء الثنائية القطبية أفسح المجال أمام بروز قضايا أمنية جديدة تجاوزت التركيز الضيق على الدولة كفاعل وحيد ومركزي في إنتاج وفهم التهديدات.

في هذا السياق، اكتسبت المقاربات النقدية في الدراسات الأمنية – ولا سيما مدرسة كوبنهاغن –أهمية متزايدة في تحليل قضايا الأمن السيبراني. وقد قدم كل من باري بوزان Barry Buzan وأولي ويفر Ole Wæverإسهامات بارزة في إطار ما يعرف بـ"عملية الأمننة " (Securitization Process)، وهي مقاربة تحليلية تدرس كيف يتم بناء التهديدات وليس فقط رصدها موضوعيا، أي أن التهديد السيبراني لا يفهم من خلال خصائصه التقنية فقط، بل من خلال الخطابات والممارسات التي تضفي عليه طابعا أمنيا في سياق سياسي معين[2].

كما تطورت مفاهيم القوة في العلاقات الدولية استجابة للثورة الرقمية؛ فإلى جانب القوة الصلبة المتمثلة في الأبعاد العسكرية والاقتصادية، برزت القوة الناعمة المعتمدة على الجاذبية الثقافية والإقناع، ثم لاحقا ظهرت القوة السيبرانية (Cyber Power) كامتداد جديد لهما. وقد مكنت هذه الأخيرة فاعلين غير تقليديين كالشركات متعددة الجنسيات، والمجموعات الإجرامية، والهاكرز من التأثير في العلاقات الدولية، مما أضعف احتكار الدولة للقوة، وغير من أنماط السيطرة والنفوذ في النظام الدولي.

ويعود التحول البنيوي في إدراك التهديد السيبراني إلى عاملين أساسيين:

---

[2] د حزام القريطي: *الأمن السيبراني وحماية المعلومات* .(الإسكندرية: دار الفكر الجامعي، 2020)، ص17.

ظهور **الحوسبة الرقمية** في خمسينيات القرن الماضي، التي أسست لبيئة تعتمد على تخزين ومعالجة المعلومات بشكل رقمي. وقد تطورت هذه التكنولوجيا تدريجيا لتصبح العمود الفقري لمعظم مؤسسات الدولة والمجتمع.

ظهور **شبكة الإنترنت** في مطلع التسعينيات، والتي مثلت قفزة نوعية في الاتصال ونقل المعلومات، ما فتح المجال أمام توظيفها في المجالات الأمنية والعسكرية. هذا الاستخدام المتزايد للتكنولوجيا الرقمية أنتج تحديات أمنية غير مسبوقة، أدت إلى بروز ما يعرف بـ"الحرب السيبرانية الباردة (Cyber Cold War) "و"سباق التسلح السيبراني.(Cyber Arms Race) "

بناء عليه، بدأ حقل العلاقات الدولية إلى جانب فروعه الفرعية كالدراسات الأمنية والاستراتيجية في التعامل مع الأمن السيبراني باعتباره قضية تتقاطع فيها التكنولوجيا بالسياسة، والسيادة بالقوة، مما يستدعي نماذج تحليلية جديدة تستوعب ديناميكيات التهديدات العابرة للحدود وغير المتمركزة حول الدولة[3].

المطلب الثاني : السيبرانية وأجيال الصراع الدولي

الصراعات بين الشعوب والدول لم تكن يوما مجرد حوادث عابرة في التاريخ بل هي جزء ثابت وملازم لمسيرة البشرية. فمع مرور الزمن تطورت هذه النزاعات في أساليبها وأدواتها وطرق إدارتها، شأنها شأن باقي مجالات الحياة التي تخضع لتحولات فكرية وتكنولوجية واقتصادية. وغالبا ما تفرض الحرب كخيار أخير، سواء للدفاع عن الأرض والكرامة، أو لاسترجاع حقوق لم تفلح الوسائل السلمية في تحقيقها، أو حتى لتحقيق أهداف توسعية وأيديولوجية يعتبرها بعض الأطراف مصيرية.

ورغم أن الحرب تعد من حيث المبدأ تصرفا غير عقلاني لما تسببه من دمار واسع ومعاناة، إلا أنها لا تزال وسيلة تستخدم لحسم النزاعات، وغالبا ما تكون نتيجة لقرارات سياسية لا

[3] نفس المرجع السابق، ص18

تقدر عواقبها بدقة. وتخوض الدول هذه الحروب باستخدام جميع إمكانياتها، وفي مقدمتها الجيوش، بهدف تحقيق مصالح أو فرض واقع يخدم أجندات محلية أو إقليمية.

في المقابل، سعى الفكر الإنساني إلى ترسيخ مبادئ تحفظ كرامة الإنسان وتؤمن استقراره من خلال أنظمة قانونية وأخلاقية تدعو إلى الحوار وترفض العنف. لكن ضعف الوعي بهذه القيم والانحراف السياسي غالبا ما يعطل الحلول السلمية، محولا بعض الدول إلى ساحات صراع دائم، كما نشهد اليوم في مناطق عدة حول العالم. فالحروب، رغم كونها تبدو أحيانا مؤقتة، تترك آثارا نفسية واجتماعية عميقة، وتزرع مشاعر الكراهية والرغبة في الانتقام، ما يمهد لتكرار الصراع مستقبلا.

استمرار هذه الصراعات وتطور أهدافها ووسائلها، دفع المفكرين والخبراء العسكريين إلى تطوير نظريات لفهم الحرب وتحولاتها. ومع الوقت برزت الحاجة إلى تصنيف الحروب إلى أجيال متعاقبة، كل منها يعكس مستوى معينا من التقدم العسكري والتقني إضافة إلى مفاهيم جديدة في إدارة المعارك. وأصبح هذا التصنيف أداة مهمة لتحليل وفهم التغيرات الكبرى في طبيعة النزاعات المسلحة.

لقد مرت الحروب بمراحل متعددة عبر التاريخ، حمل كل منها رؤى وتصورات جديدة أثرت على التدريب والتسليح والتكتيك. وصنف الخبراء هذه الحروب إلى خمسة أجيال، يتميز كل منها بخصائص مختلفة، من نوعية السلاح، وأسلوب القتال، إلى الجهات الفاعلة فيها[4].

ومن المهم أن نلاحظ أن هذه الأجيال لا ترتبط بفترات زمنية محددة، بل تتحدد بناء على طبيعة الحرب وتطور الفكر والتقنية المستخدمين فيها. فكلما تطورت أدوات المعرفة والتكنولوجيا لدى الشعوب، تغير شكل الحروب التي تخوضها. ولهذا، فإن فهم أجيال الحروب يتطلب دراسة خصائصها وسياقاتها، وهو ما سيتم استعراضه لاحقا، بدءا من الجيل الأول وصولا إلى حروب

[4] نفس المرجع السابق.ص19

الجيل الخامس، التي باتت تشمل ساحات حديثة مثل الفضاء السيبراني، أحد ميادين الصراع الأساسية اليوم.

أولا: صراعات الجيل الأول

يطلق على صراعات الجيل الأول تلك الحروب التقليدية التي تدور بين جيشين نظاميين متقابلين في ميدان محدد على أرض واحدة، حيث تتم المواجهات المباشرة بين الأطراف المتنازعة على جبهة واحدة وبشكل تصادمي. تتميز هذه الصراعات بظهور قيم الفروسية والشجاعة والإقدام على مستوى القادة والأفراد، ولهذا السبب يشار إليها أحيانا بالقتال الخطي أو المواجهات المباشرة. تتسم حروب الجيل الأول بكونها نزاعا بين خصمين أو أكثر متقاربين في المستوى الحضاري أو بفوارق بسيطة، وتشمل جميع أنواع الأسلحة التقليدية والذخائر. وقد اتسمت هذه الحروب بعمليات عسكرية محدودة لكنها فعالة كعمليات المناورة والالتفاف لتطويق الخصم وضربه في أجنحته بهدف القضاء عليه وتدميره. يرجع تاريخ حروب الجيل الأول إلى عصور مبكرة جدا في تاريخ البشرية، واستمرت حتى فترة ما قبل الحرب العالمية الثانية، حيث مثلت الأسلوب السائد في خوض المعارك والصراعات المسلحة في ذلك الوقت[5].

ثانيا: صراعات الجيل الثاني

شهدت الصراعات العسكرية تطورا ملحوظا في المرحلة التالية، التي تعرف بصراعات الجيل الثاني والتي تشمل حروب العصابات أو الحروب الثورية. تتميز هذه المرحلة بوجود نزاعات بين جيوش نظامية تقليدية من جهة، ومجموعات مقاتلة صغيرة نسبيا من جهة أخرى، غالبا ما تتبنى أهدافا محددة وثورية. على الرغم من تشابه هذه الحروب إلى حد ما مع حروب الجيل الأول من حيث طبيعة النزاع، إلا أن التطور التقني في استخدام النيران ووسائل إطلاقها مثل الدبابات والطيران، أعطى لهذه الحروب خصوصية جديدة. وتتميز صراعات الجيل الثاني بتركيزها على إحداث أكبر قدر ممكن من الخسائر في صفوف الطرفين مع اعتمادها على أساليب غير تقليدية

[5] زينب فريّل، "أجيال الحرب: دراسة في محددات تطور الأجيال الخمس للحرب"، **دفاتر السياسة والقانون**، م 31، ع 20 (2020): 546.

مثل المفاجأة والمباغتة في العمليات القتالية. تنشأ هذه الحروب عادة من نزاعات طويلة الأمد تتطلب اتخاذ تدابير محددة تقوم على القتال في ظروف غير ملائمة للجيش النظامي، مما يمكن مجموعات القتال من توجيه ضربات موجعة ومتكررة في مواجهات صغيرة ومتعددة، بهدف إضعاف قدرة الخصم ودفعه للتراجع عن أهدافه. تتميز قيادة حروب العصابات بالتركيز على توحيد القيادة العسكرية والسياسية، وغالبا ما تلعب وسائل الإعلام دورا مهما في دعم العمليات من خلال الدعاية والحرب النفسية لكسب الأنصار والدعم المالي. وعلى الرغم من عدم وجود معايير محددة لتسليح هذه المجموعات، إلا أن الأسلحة الخفيفة والمتوسطة تبقى هي الأكثر استخداما بسبب طبيعة الحركة والديناميكية في عملياتها. انتشرت صراعات الجيل الثاني في العديد من دول العالم، وقد أصبحت من أكثر أشكال الحروب انتشارا وتعقيدا في العصر الحديث[6].

ثالثا: صراعات الجيل الثالث

نشأت حروب الجيل الثالث مستندة إلى نظرية الردع بالشك، وهي نظرية سياسية وعسكرية تطورت في الولايات المتحدة الأمريكية عقب انهيار الاتحاد السوفييتي السابق. وتعبر هذه النظرية عمليا عن مفهوم الضربة الاستباقيةأي شن حرب استباقية ضد أي تهديد محتمل للأمن القومي الأمريكي أو السلم العالمي، كما عبرت عنها الإدارة الأمريكية. يطلق على حروب الجيل الثالث أيضا اسم "حروب المناورات"، وهي استراتيجية تم تطويرها أولا من قبل الألمان خلال الحرب العالمية الثانية واستخدمت ضد بريطانيا عبر القصف المتواصل بالطائرات والصواريخ صواريخ V2 ,تتميز عمليات هذا الجيل بالمرونة والسرعة العالية في الحركة مع الاعتماد الكبير على عنصر المفاجأة إضافة إلى توجيه ضربات قوية وراء خطوط العدو.

تعتبر الأسلحة الجوية والقاذفات الاستراتيجية بعيدة المدى، إلى جانب الصواريخ الموجهة، من أبرز وسائل القتال في هذه الصراعات. كما ترافق هذه العمليات عادة حملات إعلامية مركزة

[6] زينب فريّل,مرجع سابق,ص 547.

تهدف إلى التأثير النفسي والسياسي على الخصم والرأي العام العالمي. ويعد مثال حرب العراق الثانية نموذجا واضحا لصراعات الجيل الثالث، حيث برزت فيها هذه الخصائص بوضوح[7].

رابعا: صراعات الجيل الرابع

تمت تسمية صراعات الجيل الرابع في سياق الحروب ضد المنظمات الإرهابية، وفقا للمفهوم الأمريكي، حيث يتقابل في هذه النزاعات جيش نظامي لدولة ما مع خصم لا دولة له ولا جيش نظامي، وإنما خلايا سرية منتشرة في أنحاء العالم. اتفق الخبراء العسكريون على أن حرب الجيل الرابع هي نوع من الحروب "اللامتماثلة"، نشأت وتطورت على يد قيادة الجيش الأمريكي، كرد فعل على مواجهة كيان لا يمتلك ترابا أو جيشا نظاميا، بل تنظيما يحمل طابعا دينيا أو سياسيا بأيديولوجية محددة، وينتشر عالميا مع قدرات ملموسة في استهداف مصالح الدول الحيوية بغية إضعافها أمام الرأي العام الدولي.

في هذا الجيل من الصراعات، تستخدم وسائل الإعلام الحديثة والتقليدية بشكل مكثف، إلى جانب العمليات الاستخبارية، لتوجيه ضربات معنوية ومادية تعزز من إضعاف الخصم. ويعد "الحرب على الإرهاب" التي قادتها الولايات المتحدة في السودان واليمن وأفغانستان وباكستان نموذجا رئيسيا لصراعات الجيل الرابع، والتي تستمر في خوضها حيثما شعرت بتهديد لأمنها أو مصالحها الحيوية[8].

خامسا: صراعات الجيل الخامس

يطلق على صراعات الجيل الخامس تسمية *الصراعات الهجينة*، وهي نمط متطور من النزاعات يتسم بتعقيد غير مسبوق ويصعب على الجيوش النظامية التقليدية التعامل معه باستخدام الأدوات والأساليب الكلاسيكية. في هذه الصراعات، لا يواجه الخصم بوسائل تقليدية، بل يظهر

[7] زينب فريّل, مرجع سابق, ص548
[8] ستيفان هالر و جونثان كلارك. التفرد الامريكي: المحافظون الجدد و النظام العالمي, ط1, ترجمة عمر الايوبي, دار الكتاب العربي,بيروت, 2005,ص 206

في صورة كيانات غير حكومية، فاعلين رقميين، أو حتى أفراد يعتمدون على تقنيات عالية التطور في بيئة غير متماثلة.

هذا التحول يعكس ما يعرف بمفهوم "قوة الضعيف"، حيث تصبح القدرات التكنولوجية المتقدمة، ولا سيما تلك المرتبطة بالفضاء السيبراني، عاملا مضاعفا للقوة، يسمح لجهات صغيرة أو غير تقليدية بالتأثير على كيانات كبرى عسكريا واقتصاديا وسياسيا. ويلاحظ في هذا السياق أن أدوات الجيل الخامس لا تقتصر على الأسلحة الفيزيائية، بل تشمل أيضا الهجمات السيبرانية، التضليل المعلوماتي، والحرب النفسية، وكلها تتم دون التقيد بالأطر الأخلاقية أو القانونية المتعارف عليها.

ومن أبرز تجليات هذه الحروب: تصاعد أهمية **الأمن السيبراني** كجبهة رئيسية في النزاعات الحديثة، إذ باتت البنى التحتية الحيوية، وقواعد البيانات الحساسة، ومنظومات الاتصالات، عرضة للاستهداف المباشر عبر الهجمات الرقمية، من قبل دول أو جهات فاعلة غير حكومية. ويزداد تعقيد هذا النوع من الصراعات مع استغلال الذكاء الاصطناعي، والبيانات الضخمة، وتقنيات التشفير، مما يجعل تعقب مصدر التهديد وتحديد نوايا الفاعلين أمرا بالغ الصعوبة[9].

في هذا الإطار، لا بد من الإشارة إلى أن الحرب السيبرانية أصبحت أداة مركزية في تكتيكات الجيل الخامس، حيث تستخدم لهدم الثقة في المؤسسات، وإرباك القيادة، وزعزعة الأمن العام، دون الحاجة إلى تدخل ميداني مباشر. وعليه فإن فهم الجيل الخامس من الصراعات لا يمكن فصله عن التطورات المتسارعة في ميدان التكنولوجيا الرقمية، ما يجعل الأمن السيبراني عنصرا مركزيا في تحليل معادلات القوة المعاصرة، وضرورة استراتيجية لحماية سيادة الدول وضمان استقرارها الداخلي في مواجهة تهديدات غير تقليدية، وعابرة للحدود.

سادسا: صراعات الجيل السادس

[9] نفس المرجع السابق.ص207

يتقارب الجيل السادس في أهدافه وتقنياته مع الجيل السابع، حيث يهدف كلاهما إلى القضاء التام على دولة أو كيان معين من خلال خوض حرب تدار عن بعد باستخدام تقنيات متقدمة. يشمل ذلك استخدام الأسلحة الذكية، وشبكات الإنترنت، وحتى توظيف الحيوانات مثل الطيور والأسماك كوسائل للتجسس والمراقبة.

يتم في هذه الصراعات توظيف جميع الوسائل والقدرات المتاحة، سواء كانت إعلامية أو تكنولوجية أو عسكرية، لخدمة مصلحة الطرف الذي يقود الحرب. ويتميز الجيل السادس بظاهرة "العمالة المزدوجة" للمعدات العسكرية، حيث تستخدم تلك المعدات ظاهريا لمحاربة الجماعات المتطرفة والإرهابية، لكنها في الوقت ذاته تقدم دعما لوجستيا وعسكريا لتلك الجماعات نفسها.

لا يقتصر استخدام التكنولوجيا المتقدمة مثل الأسلحة المتطورة، والصواريخ المضادة للدروع والطائرات على الدعم المباشر للدول في الاستخدام التقليدي، بل تتحول إلى أدوات مساندة للأعمال الإرهابية والعمليات الانتحارية، من خلال نصب الكمائن، واستهداف المدنيين وقوات الأمن، بهدف استنزافها وتشتيتها وإرغامها على الانسحاب أو الخضوع.

كما تتسم ساحة المعركة في هذا الجيل بسلوكيات وحشية مثل الذبح، والحرق، واستخدام السيارات المفخخة، إضافة إلى توظيف الثورة التقنية وشبكات المعلومات في تنفيذ تفجيرات نوعية عن بعد[10]، وهجمات متفرقة على المستوى العالمي. يستخدم التزييف الإعلامي بشكل واسع عبر مواد دعائية تهدف إلى زعزعة الثقة بالحكم وإثارة شعور بالانعدام الأمن، مع بث نتائج مزيفة عن انتصارات وهمية للجماعات الإرهابية لزيادة الارتباك وتقويض ثقة الجمهور في قيادته.

[10] جدو فؤاد، "تفجيرات الهواتف واختراقها في ظل تحولات حروب الجيل السابع"، مدونات الجزيرة، 25 سبتمبر 2024، https://www.aljazeera.net/blogs/2024/9/25/تفجيرات-الهواتف-واختراقها-في-ظل.

المطلب الثالث: التطور المفاهيمي للأمن السيبراني و أمن المعلومات في أدبيات العلاقات الدولية

الفرع الاول : مفهوم الامن السيبراني .

من حيث اللغة :السيبرانية مأخوذة من كلمة"Cyber" ، وهي صفة تطلق على كل ما هو مرتبط بثقافة الحواسيب، أو تقنيات المعلومات، أو الواقع الافتراضي. أصل الكلمة يعود إلى المصطلح اليوناني "Kybernetes" والذي ورد لأول مرة في مؤلفات الخيال العلمي، وكان يقصد به "قيادة ربان السفينة"[11].

من حيث الاصطلاح :تم استخدام مصطلح "السيبرانية" لأول مرة بمعناه الحديث من قبل عالم الرياضيات الأمريكي "نوربرت وينر (Norbert Wiener) "، أستاذ الرياضيات في معهد ماساتشوستس للتكنولوجيا(MIT) ، وذلك سنة 1948. وقد أعطى للمصطلح تعريفا يرتبط بنظرية "التغذية الراجعة(Feedback) "، التي تصف قدرة الأنظمة على استخدام مخرجاتها (outputs) للتحكم في مدخلاتها (inputs) من أجل تحسين الأداء وتحقيق الاستقرار[12]، مما يجعل من السيبرانية علما يعنى بضبط الأنظمة وتنظيمها وتوجيهها بطريقة ذاتية وفعالة.

يعتبر الفضاء السيبراني مفهوما مركزيا في فهم الأمن السيبراني، وقد قدمت عدة جهات تعاريف متعددة له تعكس طبيعته المعقدة والمتعددة الأبعاد. من بين هذه التعاريف، تعرف **الوكالة الفرنسية لأمن أنظمة الإعلام(ANSSI)** ، وهي جهة حكومية مختصة بالدفاع السيبراني، **الفضاء السيبراني بأنه :فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[13].**

---

[11] عبد العزيز بن فهد بن محمد بن داود، **الجرائم السيبرانية: دراسة تأصيلية مقارنة**، مجلة الاجتهاد للدراسات القانونية والاقتصادية 9، عدد 3 (2020): 148.

[12] إدريس عطية، **ماكنة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، مجلة مصداقية، كلية الحقوق والعلوم السياسية – جامعة العربي التبسي، تبسة، الجزائر 1، عدد 1 (2019): 103.

[13] **Agence nationale de la sécurité des systèmes d'information (ANSSI), « Définition de la cybersécurité », cyber.gouv.fr, consulté le 5 juin 2025, https://cyber.gouv.fr/resultats-recherche?search_api_fulltext=D%C3%A9finition+de+la+cybers%C3%A9curit%C3%A9&sort_by=title.**

هذا التعريف يوضح أن الفضاء السيبراني هو بيئة تفاعلية حديثة تضم عناصر مادية وغير مادية، تشمل أجهزة رقمية متعددة، وأنظمة شبكات، وبرمجيات، فضلا عن المستخدمين الذين يشغلون هذه المنظومات أو يستعملونها. كما ينظر إلى الفضاء السيبراني أحيانا على أنه **الذراع الرابعة للجيوش الحديثة**، دلالة على أهميته المتزايدة في العمليات العسكرية والأمنية.

و مما سبق نستنتج **تعريف اجرائي:** الأمن السيبراني هو مجموعة من الآليات التقنية والإجراءات الوقائية، والسياسات التنظيمية التي تهدف إلى حماية البنية التحتية المعلوماتية، والأنظمة الرقمية، والشبكات الاتصالية، من الهجمات السيبرانية بمختلف أنواعها، مثل الاختراق، التلاعب، التشويش، أو تسريب المعلومات. ويشمل ذلك الحفاظ على سرية البيانات(Confidentiality) ، سلامتها (Integrity)، وتوافرها(Availability) ، إضافة إلى رصد التهديدات، والتعامل الاستباقي مع المخاطر وضمان استمرارية الخدمة في بيئة رقمية متغيرة ومعقدة.

في سياق الدفاع الوطني والدولي، يبرز مفهوم **الردع السيبراني** كآلية استراتيجية تهدف إلى منع الأعمال الضارة التي تستهدف الأصول الوطنية في الفضاء السيبراني. يعرف الردع السيبراني بأنه:

"**منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية**".

ويرتكز الردع السيبراني على ثلاث ركائز أساسية:

مصداقية الدفاع :(Defense) قدرة الدولة على حماية أصولها الرقمية بفعالية.

القدرة على الانتقام :(An Ability to Retaliate) امتلاك الإمكانيات للرد على الهجمات.

الرغبة في الانتقام :(A Will to Retaliate) الاستعداد السياسي والاستراتيجي للرد[14].

[14] **حزام القريطي, مرجع سابق. ص15**

أما **الهجمات السيبرانية**، فيمكن تعريفها على أنها أفعال تهدف إلى تقويض قدرات ووظائف شبكات الحاسوب لأهداف قومية أو سياسية، من خلال استغلال نقاط الضعف التقنية في الأنظمة، مما يتيح للمهاجمين التلاعب بالنظام أو تعطيله[15].

وبالنسبة **لـالجريمة السيبرانية**، فهي تتضمن مجموعة من الأفعال غير القانونية التي ترتكب عبر أجهزة إلكترونية أو عبر الإنترنت، وتستلزم معرفة متخصصة بتقنيات الحاسوب ونظم المعلومات، سواء لارتكابها أو للتحقيق فيها ومقاضاة مرتكبيها. عرف الإنتربول الجريمة السيبرانية على أنها " أي فعل غير قانوني يرتكب باستخدام أنظمة معلوماتية، أو يستهدفها، ويشمل ذلك الوصول غير المصرح به إلى البيانات، أو اختراق الشبكات، أو نشر البرمجيات الخبيثة، أو الاحتيال الإلكتروني، أو الهجمات على البنية التحتية الرقمية"[16].

في ضوء هذه المفاهيم، تظهر **القوة السيبرانية** كامتداد لمفهوم القوة في العلاقات الدولية. يعرفها **جوزيف ناي (Joseph S. Nye)** بأنها" :القدرة على تحقيق النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي القدرة على توظيف الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث في البيئات التشغيلية الأخرى عبر أدوات سيبرانية[17]".

الفرع الثاني: مفهوم أمن المعلومات.

1/تعريف أمن المعلومات

أمن المعلومات يعرف بأنه مجموعة من الوسائل والإجراءات التي تضمن حماية المعلومات من التهديدات الداخلية والخارجية. هناك عدة تعريفات شائعة لهذا المفهوم، من أبرزها:

---

[15] مرزوق عنترة و حرشاوي بن محي الدين : "الأمن السيبراني كبعد جديدفي السياسة الدفاعية الجزائرية". ورقة بحث قدمت في الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السياسية و التحديات الاقليمية, ورقلة, الجزائر, 30, 31جانفي2017

[16] Africa Joint Forum on Cybersecurity (AJFOC), تقرير تقييم التهديدات السيبرانية في إفريقيا 2024، ص. 3، https://www.au.int/sites/default/files/documents/24COM005030-AJFOC_Africa_Cyberthreat_Assessment_Report_2024_complet_AR_LR.pdf

[17] Nye, Joseph S., Jr. "Cyber Power." In *The Future of Power*, 127. New York: PublicAffairs, 2011.

التعريف الأول" :أمن المعلومات هو الوسائل والأدوات والإجراءات اللازمة لضمان حماية المعلومات من الأخطار الداخلية والخارجية."

التعريف الثاني" :أمن المعلومات هو مجموعة من الإجراءات الوقائية التي تستخدم في المجالات التقنية أو الوقائية للحفاظ على المعلومات والأجهزة والبرمجيات، بالإضافة إلى الإجراءات المتعلقة بحماية العاملين في هذا المجال.[18]"

من هذه التعريفات، يمكن استخلاص أن أمن المعلومات هو مجموعة من الإجراءات الوقائية التي تهدف إلى حماية المعلومات والأجهزة والبرمجيات من المخاطر والتهديدات، سواء كانت داخلية أو خارجية[19].

2/أهمية وأهداف وأبعاد أمن المعلومات

أ/ أهمية أمن المعلومات

تكمن أهمية أمن المعلومات في عدة نقاط رئيسية:

1/ **الاعتماد الحيوي للقطاعات الاقتصادية على أمن المعلومات** :باتت فعالية الأنشطة التجارية والمؤسسات الاقتصادية مرهونة بقدرتها على حماية بياناتها من التلاعب، الاختراق أو السرقة، مما يجعل أمن المعلومات مكونا استراتيجيا من استقرار الاقتصاد الوطني.

2/ **ضرورة بناء منظومات أمنية وطنية لمواجهة المخاطر العابرة للحدود** :في ظل الفضاء السيبراني المفتوح، تحتاج الدول إلى آليات دفاع متطورة لحماية مصالحها السيادية عند التعامل مع جهات أجنبية أو تهديدات لا مركزية.

---

[18] علوطي ملني، "أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة"، **مجلة علوم إنسانية**، السنة 6، العدد 38 (2008): 2.

[19] الطيب مصطفى: "الفرق بين أمن المعلومات و الأمن السيبراني". مدونة علوم,08 أوت 2019 .Oolomالفرق بين أمن المعلومات والامن السيبراني." تم الدخول في 5 جوان 2025. https://www.oolom.com/6124/ ."

3/ **الحاجة الملحة إلى بيئة إلكترونية سيبرانية آمنة** :استخدام الحلول الرقمية في الإدارة العامة والخاصة يستدعي ضمان أمن هذه البيئات من الاختراقات والتلاعب لضمان الثقة الرقمية والاستقرار المؤسسي.

4/ **النمو المتسارع للتطبيقات الإلكترونية وارتفاع سطح الهجوم** :تزايد استخدام الخدمات الرقمية يجعلها هدفا جذابا للهجمات السيبرانية، مما يستدعي استباق المخاطر بتقنيات دفاع نشطة واستراتيجيات أمنية متعددة المستويات.

5/ **حماية البنية التحتية الحرجة للشبكات المعلوماتية** :تشكل قطاعات مثل الصحة، الطاقة، المالية، والنقل العمود الفقري للأمن الوطني، ويعد تأمين شبكاتها الرقمية أمرا جوهريا لضمان استمرارية الخدمات ومنع الكوارث السيبرانية.

6/ **تصاعد الجرائم الإلكترونية وتحولها إلى تهديدات أمنية منظمة** :لم تعد الهجمات السيبرانية مقتصرة على أفراد أو مجموعات، بل أصبحت أدوات في أيدي كيانات إجرامية منظمة أو حتى دول، مما يتطلب رصدا استخباراتيا إلكترونيا وتعاونا دوليا دائما[20].

ب/ أهداف أمن المعلومات

تهدف استراتيجيات ووسائل أمن المعلومات إلى تحقيق الأهداف التالية:

السرية أو الموثوقية :ضمان عدم كشف المعلومات أو الاطلاع عليها إلا من قبل الأشخاص المصرح لهم بذلك.

التكاملية وسلامة المحتوى :التأكد من أن المعلومات التي يتم حفظها صحيحة وغير معدلة، وأنه لا يمكن التلاعب بها.

استمرارية وتوافر المعلومات أو الخدمة :ضمان استمرارية عمل التكنولوجيا وأن الخدمة ستظل متاحة للمستخدمين دون انقطاع أو تعطل.

[20] نفس المرجع السابق.

عدم إنكار التصرف المتعلق بالمعلومات :التأكد من أن أي تصرف متصل بالمعلومات يمكن إثباته والتأكيد عليه، حيث لا يمكن للمستخدم إنكار القيام بذلك التصرف[21].

ج/ أبعاد أمن المعلومات

تشمل أبعاد أمن المعلومات الرئيسية ما يلي:

سرية المعلومات :أي عدم الإطلاع على أو تغيير المعلومات المخزنة على الأجهزة أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك.

سلامة المعلومات :التأكد من أن المعلومات المخزنة على الأجهزة أو المنقولة عبر الشبكة لم يتم تغييرها أو التلاعب بها.

جودة المعلومات :ضمان أن المعلومات المخزنة لا يتم حذفها أو تدميرها إلا من قبل الأشخاص المصرح لهم بذلك[22].

يعد أمن المعلومات عنصرا أساسيا لضمان حماية البيانات والمعلومات من التهديدات المختلفة التي قد تتعرض لها سواء من التهديدات الداخلية أو الخارجية .ومن خلال تبني إجراءات وقائية وتقنية فعالة، يمكن للمنظمات والأفراد ضمان سلامة المعلومات والحفاظ على استمرارية العمل وتفادي أضرار الاختراقات والهجمات الإلكترونية.

[21] نفس المرجع السابق

[22] قدايفية، أمينة. "استراتيجية أمن المعلومات ".مجلة دراسات اقتصادية وإدارية، العدد 8 (2016): 166 . https://www.asjp.cerist.dz/en/article/31120.

المبحث الثاني: الفواعل، الأبعاد والأنواع في الأمن السيبراني.

المطلب الأول: الفواعل الرئيسيون في الأمن السيبراني.

حدد **جوزيف ناي** ثلاثة أنواع رئيسية من الفواعل الذين يمتلكون القوة السيبرانية ويؤثرون في مجال الأمن السيبراني على المستوى الدولي:

الدول: تتمتع الدول بقدرة كبيرة على تنفيذ الهجمات السيبرانية وتطوير البنية التحتية الرقمية وممارسة سلطاتها ضمن حدودها الوطنية. تمثل الدولة الفاعل المحوري في الفضاء السيبراني، نظرا لتفوقها التكنولوجي وامتلاكها الموارد والمؤهلات التي تؤهلها للهيمنةوالتحكم في هذا المجال. كما أن الدول تمتلك القدرة على صياغة السياسات الوطنية والدولية المتعلقة بالأمن السيبراني، وتستخدم هذا المجال كجزء من استراتيجياتها الأمنية والدفاعية.

الفواعل غير الدولتية: يستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، لكن تنفيذ هجمات سيبرانية ذات تأثير كبير غالبا ما يتطلب دعما استخباراتيا متطورا. وتشمل هذه الفواعل عدة فئات:

الشركات متعددة الجنسيات، وخصوصا شركات التكنولوجيا الكبرى مثل *مايكروسوفت (Microsoft)*، و*فيسبوك(Facebook)* ، و*جوجل(Google)* ، التي تمتلك موارد قوة تقنية واقتصادية تفوق بعض الدول، وتمتلك قواعد بيانات ضخمة تؤثر على الاقتصاديات والثقافات وتوجهات المجتمعات، رغم افتقارها للشرعية السياسية في ممارسة القوة التي لا تزال حكرا على الدول.

الجماعات الإرهابية، التي برزت كفاعلين دوليين مهمين، خاصة بعد أحداث 11 سبتمبر، حيث تستخدم الفضاء السيبراني في التجنيد، التعبئة، الدعاية، جمع الأموال، وتدريب المجندين عن بعد.

ورغم ذلك، لم تصل هذه الجماعات حتى الآن إلى مرحلة تنفيذ هجمات سيبرانية ذات أثر على البنى التحتية للدول.

المنظمات الإجرامية، التي تنشط في عمليات القرصنة، سرقة المعلومات، اختراق الحسابات البنكية، وتحويل الأموال، كما تستغل الإنترنت المظلم (Dark Web)[23] في تجارة المخدرات، الأسلحة، والبشر.

الأفراد

أصبح الأفراد، بفضل تطور الفضاء السيبراني، فواعل مؤثرين في العلاقات الدولية.
أبرز نموذج على ذلك هو ظاهرة ويكيليكس(Wikileaks)[24] ، التي نجحت في نشر ملايين الوثائق السرية المتعلقة بالإدارة الأمريكية وقنصلياتها، ما أدى إلى إحداث مشاكل دبلوماسية بين الولايات المتحدة وحلفائها.

المطلب الثاني: الأبعاد المختلفة للأمن السيبراني.

1.البعد العسكري:

تعود البدايات الأولى لتكنولوجيا الإنترنت إلى بيئة عسكرية، حيث تم تطويرها لخدمة الأغراض الدفاعية والتواصل بين الوحدات العسكرية عبر العالم الافتراضي.
يمثل الأمن السيبراني ميزة نسبية للقوات المسلحة بقدرته على تسهيل تبادل المعلومات وسرعة إصدار الأوامر، مما يعزز تحقيق الأهداف العسكرية. ومع ذلك، قد تتحول هذه الميزة إلى نقطة

---

[23] **الويب المظلم:(Dark Web)**
هو جزء من الإنترنت لا يمكن الوصول إليه باستخدام محركات البحث التقليدية مثلGoogle ، ويتطلب متصفحات خاصة مثل Tor للدخول إليه. يُستخدم في الغالب للحفاظ على الخصوصية وإخفاء الهوية، لكنه أيضًا يُستغل في أنشطة غير قانونية مثل تجارة المخدرات، الأسلحة، وتبادل البيانات المسروقة، مما يجعله محل اهتمام كبير في مجالات أمن المعلومات والتحقيقات السيبرانية.

[24] **ويكيليكس:(WikiLeaks)**
هي منصة إلكترونية دولية تأسست سنة 2006 على يد جوليان أسانج، تهدف إلى نشر الوثائق السرية والحساسة المسربة من مصادر مجهولة، خاصة تلك التي تتعلق بالحكومات، الجيوش، أو الشركات الكبرى. اكتسبت شهرتها الواسعة بعد نشرها آلاف الوثائق الأمريكية السرية، ما أثار جدلاً عالميًا حول حرية التعبير، الأمن القومي، وحق الشعوب في الوصول إلى المعلومة. وتُعد ويكيليكس مثالًا صارخًا على التقاطع بين الشفافية والمخاطر السيبرانية.

ضعف إذا لم تكن الشبكات الإلكترونية مؤمنة بشكل كاف ضد الاختراقات والهجمات المضادة التي تستهدف قواعد البيانات العسكرية وأجهزة الاستخبارات[25].

2.البعد الاجتماعي:

يتيح الفضاء السيبراني، وخاصة من خلال المنصات المفتوحة مثل المدونات والشبكات الاجتماعية، لكل فرد التعبير عن آرائه السياسية والاجتماعية، مما يعزز المشاركة المجتمعية في الشؤون العامة. ينشأ من هذا الانفتاح تبادل للأفكار والخبرات، وظهور حاجات جديدة وآفاق تعاون بين المجتمعات.

غير أن هذا الانفتاح يعرض المجتمع لأخطار مثل انتشار المواد الإباحية، الفكر المتطرف، الإرهاب، ومحاولات تجنيد الشباب، فضلا عن صعوبة مراقبة المحتوى وحماية الهويات الرقمية من الاختراق، مما قد يهدد السلم الاجتماعي. لذا، يعد التوعية المجتمعية ضرورة أساسية لتحقيق الأمن السيبراني في بعده الاجتماعي[26].

3.البعد السياسي:

يكتسب البعد السياسي للأمن السيبراني أهمية متزايدة في ظل الأحداث السياسية العالمية التي تتأثر بتسريبات الوثائق الحساسة والحملات الرقمية.

تؤدي هذه التسريبات أحيانًا إلى أزمات دبلوماسية معقدة على الصعيد الدولي.

تُستخدم شبكات التواصل الاجتماعي كأدوات لتنظيم الحملات الانتخابية، التظاهرات الافتراضية، والحركات الاحتجاجية، كما تستغلها بعض الحكومات لأغراض مراقبة وتوجيه الرأي العام[27].

4.البعد الاقتصادي:

[25] حزام القريطي، .الأمن السيبراني وحماية المعلومات.مرجع سابق, ص23
[26] حزام القريطي.نفس المرجع, ص23
[27] حزام القريطي.نفس المرجع, ص24

يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد الرقمي، لا سيما في عصر اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات. توفر هذه التقنيات فرصًا لتعزيز التنمية الاقتصادية من خلال تحسين كفاءة الإنتاج وإدارة التكاليف. ومع انتشار المال الإلكتروني والمحافظ الرقمية، تتزايد استثمارات القطاع المالي في الأمن السيبراني للحفاظ على استقرار الأسواق وحماية المستهلكين. ومع ذلك، يشكل ارتفاع معدل الجرائم السيبرانية المنظمة تهديدًا مباشرًا لنمو الاقتصاد الرقمي، مما يستدعي تعزيز معايير الأمن السيبراني على مستوى الدول[28].

5.البعد القانوني:

تفرض التطورات التقنية المتسارعة ضرورة مواكبة التشريعات القانونية المتعلقة بالفضاء السيبراني. تعاني معظم الدول من نقص في الأطر القانونية الصارمة للتعامل مع الجريمة السيبرانية، وذلك بسبب طبيعة هذه الجرائم وصعوبة تحديد هوية مرتكبيها. كما أن الجرائم السيبرانية تتسم بعدم التقيد بالحدود الوطنية مما يستوجب تعزيز التعاون الدولي المشترك لمكافحتها بفعالية[29].

يمكن القول إن الأمن السيبراني يمثل بعدا جديدا ضمن أبعاد الأمن القومي، حيث أحدث تغييرات جوهرية في مفاهيم العلاقات الدولية مثل الصراع، القوة، والتهديد. أدى الانتقال من عالم مادي إلى عالم افتراضي معقد إلى **ضرورة تطوير استراتيجيات ومقاربات فعالة لمواجهة التهديدات السيبرانية** التي تتميز بالسرعة، الغموض، والدقة. ومن ثم بات تحقيق الأمن السيبراني والحفاظ على مكاسب الدولة وأمنها القومي مطلبا حتميا في عصرنا الرقمي.

المطلب الثالث: أنواع الأمن السيبراني و التهديدات السيبرانية.

الفرع الاول: أنواع الأمن السيبراني.

[28] حزام القريطي.نفس المرجع, ص24

[29] حزام القريطي. نفس المرجع, ص24-25

في ظل التحول الرقمي المتسارع أصبح الأمن السيبراني أحد ركائز الأمن القومي للدول، لما يشكله من خط دفاع أولي ضد التهديدات الرقمية العابرة للحدود. ويمكن تصنيف أبرز أنواع الأمن السيبراني، وفقا لمدى ارتباطها المباشر بحماية السيادة الوطنية والبنية التحتية الحرجة كما يلي:

1. أمن البنية التحتية الحيوية (Critical Infrastructure Security)

يعد من أكثر فروع الأمن السيبراني ارتباطا بالأمن القومي، إذ يستهدف حماية الأنظمة الرقمية التي تشغل القطاعات الحيوية كالكهرباء، الطاقة، المياه، الاتصالات، النقل، والمنشآت الحكومية. تعتمد هذه القطاعات غالبا على نظم تحكم صناعي مثل(SCADA)[30]، وهي هدف رئيس للهجمات المتقدمة (APT)[31] التي قد تؤدي إلى شلل اقتصادي وأمني[32].

2. أمن الشبكات (Network Security)

يشكل البوابة الأساسية لحماية تدفق البيانات داخل وخارج المؤسسات الحيوية. غالبية الهجمات السيبرانية تبدأ على مستوى الشبكة، مما يستدعي وجود أدوات لرصد التهديدات، منع التسلل، وتطبيق سياسات رقابة صارمة. ويعد أمن الشبكات عنصرا أساسيا في حماية المؤسسات السيادية ومراكز القرار[33].

3. الأمن التشغيلي (Operational Security – OPSEC)

يختص بتأمين المعلومات الحساسة من خلال التحكم في الوصول، ورصد السلوكيات غير الطبيعية داخل الأنظمة. يستخدم هذا النوع بشكل مكثف في القطاعات الأمنية والعسكرية لحماية البيانات المصنفة سرية ومنع التسربات[34].

---

[30] **SCADA (Supervisory Control and Data Acquisition): نظام تحكم صناعي يُستخدم لمراقبة العمليات الحيوية وإدارتها عن بُعد في قطاعات حساسة كالكهرباء والمياه والغاز، ويُعد من البنى التحتية الحرجة المعرضة للهجمات السيبرانية.**

[31] **APT (Advanced Persistent Threat): نمط من الهجمات السيبرانية المتقدمة والموجّهة، تنفذها غالبًا جهات مدعومة من دول، وتهدف إلى التسلل إلى الأنظمة الحساسة والبقاء داخلها لفترات طويلة لجمع معلومات أو تخريب البنية الرقمية.**

[32] SailPoint. "Types of Cybersecurity." *SailPoint Identity Library*. Accessed June 6, 2025. https://www.sailpoint.com/identity-library/five-types-of-cybersecurity.

[33] **Ibid.**

[34] **Ibid.**

4.أمن البيانات(Data Security)

يمثل لب حماية السيادة الرقمية، خاصة عند التعامل مع قواعد بيانات المواطنين، المعلومات المالية، والسجلات الصحية. يهدف هذا المجال إلى ضمان ثلاثية الأمن: السرية، النزاهة، وتوافر البيانات، سواء أثناء التخزين أو النقل[35].

5.أمن السحابة(Cloud Security)

نظرا لاعتماد الحكومات والمؤسسات على التخزين السحابي، أصبح أمن السحابة مسألة سيادية. يدار وفق نموذج المسؤولية المشتركة بين المستخدم ومزود الخدمة، مما يتطلب إطارا قانونيا وتشغيليا لحماية المعلومات المُخزنة في بنى تحتية قد تكون خارج الحدود الوطنية[36].

6.نموذج الثقة المعدومة(Zero Trust Architecture)

يمثل تحولا في فلسفة الحماية حيث يمنع أي مستخدم – داخلي أو خارجي – من الوصول إلى الموارد دون تحقق مستمر وتمنح الصلاحيات وفق مبدأ "أقل امتياز ممكن". هذا النموذج يدعم صمود الأنظمة ضد التهديدات الداخلية والخارجية على حد سواء[37].

7.أمن التطبيقات(Application Security)

تتزايد أهمية هذا النوع مع تنامي الخدمات الرقمية الحكومية. ويُستخدم للكشف عن الثغرات البرمجية أثناء مراحل التصميم والتطوير، كما يوفر الحماية بعد النشر، خصوصًا في التطبيقات المرتبطة بالخدمات السيادية أو المعاملات الإلكترونية الحساسة[38].

8.أمن الأجهزة الطرفية(Endpoint Security)

[35] **Ibid.**
[36] **Ibid.**
[37] **Ibid.**
[38] **Ibid.**

تشكل الأجهزة المتصلة بالنظام (كالحواسيب، الخوادم، والهواتف) نقاط دخول مفضلة للمهاجمين. يستخدم هذا النوع لحماية تلك النقاط ومنع استخدامها كنقطة اختراق، خاصة في بيئات العمل عن بعد أو في المؤسسات المتصلة بالبنية التحتية الوطنية[39].

.9أمن الأجهزة المحمولة(Mobile Security)

تزداد الحاجة لهذا النوع من الأمن مع انتشار العمل باستخدام الهواتف والأجهزة المحمولة. ويتضمن تقنيات لمنع الاختراقات، التتبع، وسرقة البيانات، خاصة بالنسبة للمستخدمين الرسميين أو العسكريين[40].

.10أمن إنترنت الأشياء(IoT Security)

مع توسع استخدام الأجهزة الذكية (مثل الكاميرات، المجسات، نظم التحكم)، تبرز الحاجة لحمايتها من الاختراق. ورغم أنها الأقل نضجا من حيث الضوابط، فإن المخاطر المرتبطة بها آخذة في التصاعد، خاصة عند دمجها في البنية التحتية الحيوية[41].

تمثل الأنواع المذكورة أعلاه نسيجا مترابطا من التدابير السيبرانية التي تساهم مجتمعة في تحقيق الأمن القومي الرقمي، وتؤكد الحاجة إلى استراتيجية متكاملة تأخذ بعين الاعتبار مختلف مستويات الحماية: من التطبيق والنقطة النهائية، مرورا بالبنية التحتية، وصولا إلى نموذج الحوكمة المبني على انعدام الثقة.

الفرع الثاني: أنواع التهديدات السيبرانية

تنقسم التهديدات السيبرانية التي تستهدف الأجهزة والشبكات إلى ثلاث فئات رئيسية ترتكز على مبادئ الأمن الأساسية :**السرية، النزاهة،** و**التوافر**.

[39] **Ibid.**
[40] **Ibid.**
[41] **Ibid.**

الهجمات على السرية(Confidentiality) : تتمثل هذه الهجمات في سرقة المعلومات الحساسة مثل بيانات التعريف الشخصية، حسابات البنوك، ومعلومات بطاقات الائتمان. يقوم المهاجمون بسرقة هذه البيانات وبيعها في الأسواق السوداء على شبكة الإنترنت المظلمة(Dark Web) ، حيث يتم استخدامها بطرق غير شرعية، مما يعرض الأفراد والمؤسسات لخطر الاحتيال وسوء الاستخدام[42].

الهجمات على النزاهة(Integrity) : تتضمن هذه الهجمات عمليات تخريب تستهدف الأفراد أو المؤسسات، وغالبا ما تأخذ شكل تسريبات معلوماتية. يقوم المهاجمون بالحصول على معلومات حساسة ونشرها بهدف التشهير، كشف الأسرار، أو التأثير السلبي على سمعة المؤسسة أو الشخص المعني، مما يؤدي إلى فقدان الثقة لدى الجمهور[43].

الهجمات على التوافر(Availability) : تهدف هذه الهجمات إلى منع المستخدمين من الوصول إلى بياناتهم أو خدماتهم، وغالبا ما يتم ذلك من خلال هجمات رفض الخدمة (DoS)[44] أو برامج الفدية.(Ransomware)[45] يطالب المهاجمون عادة بدفع فدية مالية مقابل استعادة الوصول إلى البيانات أو الأنظمة، مما يشكل تهديدًا مباشرًا لاستمرارية الأعمال والمؤسسات[46].

---

[42] **حزام القريطي,الأمن السيبراني و حماية المعلومات,ص29.**

[43] **نفس المرجع السابق,ص29.**

[44] **هجمات رفض الخدمة :(Denial of Service - DoS)** هجمات إلكترونية تهدف إلى إغراق الخوادم أو الشبكات بطلبات وهمية بشكل مكثف، ما يؤدي إلى إبطائها أو تعطيلها كليًا، ويمنع المستخدمين الشرعيين من الوصول إلى الخدمة.

[45] **برامج الفدية :(Ransomware)** نوع من البرمجيات الخبيثة يقوم بتشفير بيانات الضحية أو حجب الوصول إلى النظام، ويطالب المهاجم بفدية مالية مقابل فك التشفير أو استعادة البيانات، وغالبًا ما تُستخدم في هجمات تستهدف مؤسسات حيوية.

[46] **نفس المرجع السابق,ص29.**

المبحث الثالث: الجريمة السيبرانية كتهديد ناشئ في البيئة الرقمية.

تشير الجرائم السيبرانية إلى الأنشطة الإلكترونية التي ترتكب عمدا بدافع إجرامي بهدف إلحاق ضرر مادي أو معنوي بشخص أو جهة ما، سواء بشكل مباشر أو غير مباشر.

يمكن تعريفها على أنها **ممارسات إجرامية توقع ضد فرد أو مجموعة مع توفر باعث إجرامي واضح يهدف إلى التسبب في أذى لسمعة الضحية عمدا، أو إلحاق الضرر النفسي والجسدي بها، وذلك سواء بأسلوب مباشر أو غير مباشر من خلال الاستعانة بشبكات الاتصال الحديثة كالإنترنت وما تتبعها من أدوات، مثل البريد الإلكتروني وغرف المحادثة، والهواتف المحمولة مع رسائل الوسائط المتعددة**[47]. وتشمل الجرائم السيبرانية أي نشاط إجرامي يتم عبر أجهزة الحاسوب والشبكات الإلكترونية، ويتراوح نطاقها بين:

الاحتيال الإلكتروني غير المرغوب فيه، مثل رسائل البريد الإلكتروني المزعجة.(Spam)

سرقة البيانات الحكومية وأسرار الشركات عبر التعدي على الأنظمة البعيدة المنتشرة حول العالم.

عمليات الاختراق والقرصنة التي تستهدف نظم الحاسوب والشبكات.

استخدام شبكات الاتصال الحديثة، بما في ذلك الإنترنت، غرف الدردشة، البريد الإلكتروني، والهواتف المحمولة مع الرسائل النصية القصيرة والرسائل متعددة الوسائط.

بالتالي، فإن الجريمة السيبرانية هي جريمة متعددة الأوجه، تستخدم التكنولوجيا الرقمية كوسيلة لتحقيق أهداف إجرامية، وتؤثر على الأفراد والمؤسسات والدول، وتتنوع بين أفعال الاحتيال، التزوير، السرقة، والاعتداء على البيانات والمعلومات.

المطلب الأول: أنواع الجرائم السيبرانية.

[47] علي زياد، **الصراع والأمن الجيوسياسي في السياسة الدولية**، عمّان: دار أمجد للنشر والتوزيع، الطبعة الأولى، **81–82.**

تتعدد أنواع الجرائم السيبرانية وتتخذ أشكالا متنوعة، ومن أبرزها:

1. الاحتيال والجرائم المالية

يشمل هذا النوع مجموعة واسعة من أساليب الاحتيال عبر الإنترنت، وأهمها:

التصيد الاحتيالي :(Phishing) حيث ترسل رسائل مرفقة بملفات خبيثة تظهر كأنها سليمة، وبمجرد فتحها يتم اختراق الجهاز[48].

الهندسة الاجتماعية :وهي أساليب خداع تستهدف المستخدمين أو الموظفين في الشركات بهدف الحصول على معلومات سرية أو التحكم في الأنظمة.

الاحتيال الداخلي :حيث يقوم بعض الموظفين بإدخال بيانات خاطئة، أو استخدام عمليات غير مصرح بها للسرقة أو تعديل البيانات.

الاحتيال ببطاقات الائتمان :سرقة بيانات بطاقات الائتمان واستخدامها بشكل غير قانوني للسرقة المالية.

2. .الإرهاب السيبراني

يتمثل في الهجمات المنظمة التي يقوم بها إرهابيون إلكترونيون، أو وكالات مخابرات أجنبية، تستهدف الأنظمة الحيوية للدول أو المؤسسات بهدف:

الضغط على الحكومات لتحقيق أهداف سياسية أو اجتماعية.

تعطيل البنى التحتية الحيوية مثل شبكات الطاقة والاتصالات.

تنفيذ هجمات إلكترونية تهدد الأمن القومي[49].

3. .الابتزاز السيبراني

[48] "الجرائم الإلكترونية: عندما تصبح الإنترنت سلاحًا ".الجزيرة نت، 6 أبريل 2015. تم الدخول في 6 جوان 2025 . https://www.aljazeera.net/tech/2015/4/6/الجرائم-الإلكترونية-عندما-تصبح-2.

[49] نفس المرجع السابق

يشمل هجمات مثل:

هجمات الحرمان من الخدمة الموزعة(DDoS) ، وهي اختصار لـ Distributed Denial of Service، تمثل نوعًا من الهجمات الإلكترونية التي تهدف إلى تعطيل الخوادم أو الشبكات عن طريق إغراقها بكمّ هائل من الطلبات من مصادر متعددة في وقت واحد، مما يؤدي إلى توقف الخدمة عن المستخدمين الشرعيين. وغالبا ما تستخدم شبكات من الأجهزة المخترقة (botnets) لتنفيذ هذا النوع من الهجمات[50].

فيروسات الفدية (Ransomware) هي نوع من البرمجيات الخبيثة التي تقوم بتشفير ملفات الضحية أو حجب نظامه الرقمي، وتطلب فدية مالية (غالبًا بعملة مشفّرة) مقابل إعادة الوصول إلى البيانات. تُعد من أكثر الهجمات الإلكترونية انتشارًا وخطورة، وتستهدف الأفراد والمؤسسات على حد سواء.[51]

التهديد المالي عبر الهجمات المتكررة :مطالبة الضحية بدفع مبالغ مالية لوقف الهجمات.

4. .الحرب السيبرانية

هي الحروب التي تستخدم فيها الدول الأسلحة الإلكترونية، مثل:

هجمات البنية التحتية الوطنية (كالهجوم على إستونيا عام 2007).

استهداف الأنظمة الحكومية أو العسكرية بهدف تدمير البنى التحتية أو سرقة المعلومات.

وجود جيوش إلكترونية تنفذ هجمات ممنهجة، مثل "الجيش الإلكتروني الروسي" و"الجيش الإيراني الإلكتروني."

5. .القرصنة السيبرانية

[50] Cloudflare. "What is a DDoS Attack?" **Cloudflare Learning Center**. تم الدخول في 6 جوان 2025. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[51] Norton. "What Is Ransomware?" *Norton Cyber Safety*. تم الدخول في 6 جوان 2025. https://us.norton.com/blog/malware/what-is-ransomware.

تمثل أي نشاط غير قانوني يستهدف التحايل أو التلاعب في نظم المعالجة الآلية للبيانات، وقد تشمل:

إتلاف المستندات الرقمية.

تدمير أنظمة الحاسوب.

استخدام برامج القرصنة الجاهزة أو كتابة شفرات خبيثة.

6. المطاردة السيبرانية(Cyberstalking)

استخدام الإنترنت ووسائل الاتصال الإلكترونية لتعقب أو مضايقة الأفراد، من خلال:

جمع معلومات شخصية مثل الاسم، العائلة، مكان السكن والعمل.

نشر معلومات محرجة أو تهديدات.

التسبب في الإزعاج النفسي والمادي للضحية[52].

7.الجريمة الفيروسية(Viral Cybercrime)

هي شكل من أشكال الجريمة السيبرانية يتم فيه استخدام برمجيات خبيثة (Malware) مصممة لإلحاق الضرر بالأجهزة أو سرقة البيانات، وتتميز بما يلي:

قدرة الفيروسات على التناسخ الذاتي والانتشار تلقائيا.

ارتباطها ببرامج "حاضنة" لتفعيلها.

سهولة انتقالها بين الأجهزة عبر وسائط متعددة.

[52] ابتسام علي حسين، "فرص وقيود الأطراف المتنازعة على 'المجال العام السيبراني''، مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208 ، مركز الأهرام للدراسات والبحوث الإستراتيجية. القاهرة2017

فيروس:(2000) ILOVEYOU انتشر هذا الفيروس عبر البريد الإلكتروني تحت عنوان "I love you"، وعند فتحه، بدأ بنسخ نفسه وإرسال نفسه إلى كل جهات الاتصال، مسببا أضرارا كبيرة في الأنظمة حول العالم[53].

فيروس:(1999) Melissa كان يرفق بوثيقة Word تحتوي على ماكرو خبيث، وعند فتحها، يرسل نفسه تلقائيا عبر البريد الإلكتروني إلى 50 جهة اتصال، مما أدى إلى إيقاف أنظمة البريد في شركات كبرى[54].

فيروس:(2010) Stuxnet يعد من أخطر الفيروسات، استُخدم في مهاجمة برنامج إيران النووي، حيث استهدف أنظمة SCADA الصناعية وتسبب في تخريب أجهزة الطرد المركزي دون أن يتم كشفه بسهولة[55].

8.جرائم إلكترونية إضافية:

.عدم تسليم البضائع أو الدفع الإلكتروني :في حالات التجارة الإلكترونية.

.سرقة الهوية :انتحال شخصية الضحية لأغراض احتيالية.

.الرسائل غير المرغوب فيها :(Spam) مزعجة وتستخدم أحيانا في الاحتيال.

.التهديدات عبر الإنترنت :مثل تهديد السلامة الشخصية عبر شبكات الحاسوب.

.جرائم المزادات الوهمية :تنظيم مزادات إلكترونية مزيفة للاحتيال.

9.إحصائيات مهمة حول الجرائم السيبرانية:

[53] **BBC. "The Love Bug: Most Destructive Computer Virus Ever?" BBC News, May 4, 2020. https://www.bbc.com/news/technology-52535161.**
[54] **Zetter, Kim. "The Strange Story of the Melissa Virus." *Wired*, March 26, 2014. https://www.wired.com/2014/03/melissa-virus-15-years-later/.**
[55] **Sanger, David E. Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New York: Crown Publishing, 2012.**

•الخسائر السنوية الناتجة عن الجرائم السيبرانية بلغت حوالي 9.5 تريليون دولار أمريكي[56].

•متوسط تكلفة اختراق البيانات لشركة واحدة بلغ 4.88 مليون دولار[57].

•كل شركة كبرى تتعرض لما يقارب 130 هجوما سيبرانيا سنويا[58].

•المؤسسات تتعرض إلى 1,876 هجومًا إلكترونيًا أسبوعيًا في المتوسط[59].

•برمجيات الفدية تمثل 70% من مجموع الحوادث السيبرانية المسجلة[60].

•متوسط مبلغ الفدية المطلوب في الهجمات بلغ 5.2 مليون دولار[61].

• 72%من الشركات الصغيرة والمتوسطة في كندا تعرضت لهجمات إلكترونية[62].

• 65%من الشركات في المكسيك أبلغت عن تعرضها لاختراقات سيبرانية[63].

• 88%من الحوادث ناتجة عن أخطاء بشرية مثل ضعف كلمات المرور أو النقر على روابط خبيثة[64].

•متوسط مدة بقاء المهاجمين داخل النظام قبل اكتشافهم يصل إلى 194 يومًا.

•الصناعة التحويلية كانت القطاع الأكثر استهدافًا بهجمات سيبرانية في 2024.

•قطاع الرعاية الصحية تصدّر القطاعات المستهدفة بهجمات الفدية.

•شركة مايكروسوفت تسجل أكثر من 600 مليون محاولة هجوم يوميا على خدماتها[65].

• 43.9%من ضحايا سرقة الهوية تعرضوا لاحتيال عبر بطاقات الائتمان.

---

[56] **Cybersecurity Ventures. "Cybercrime To Cost The World $9.5 Trillion USD In 2024." Cybersecurity Almanac 2024. Accessed June 6, 2025. https://cybersecurityventures.com/cybersecurity-almanac-2024/.**

[57] **Varonis. "60 Must-Know Cybersecurity Statistics for 2024." Varonis Blog. Accessed June 6, 2025. https://www.varonis.com/blog/cybersecurity-statistics.**

[58] **PurpleSec. "2024 Cyber Security Statistics." Accessed June 6, 2025. https://purplesec.us/resources/cybersecurity-statistics/.**

[59] **Secureframe. "Cybersecurity Statistics You Need to Know in 2024." Accessed June 6, 2025. https://secureframe.com/blog/cybersecurity-statistics.**

[60] **NinjaOne. "Ransomware Statistics and Trends 2024." Accessed June 6, 2025. https://www.ninjaone.com/blog/cybersecurity-statistics/.**

[61] • Embroker. "Cyber Attack Statistics for 2024." Accessed June 6, 2025. https://www.embroker.com/blog/cyber-attack-statistics/.

[62] **Cobalt. "Top Cybersecurity Statistics You Need to Know in 2024." Accessed June 6, 2025. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025.**

[63] **Ibid**

[64] **Ibid**

[65] **Microsoft. "600 Million Cyberattacks Per Day Around the Globe." Microsoft Digital Defense Report 2024. Accessed June 6, 2025. https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/.**

•الهجمات المعتمدة على الذكاء الاصطناعي ارتفعت بنسبة 42.%

•بلغ عدد عمليات المسح التلقائي بواسطة أدوات هجومية مدعومة بالذكاء الاصطناعي 36,000 عملية في الثانية.

•كلمة المرور "123456" لا تزال من أكثر كلمات المرور استخدامًا بين ضحايا الاختراق.

المطلب الثاني :خصائص الجريمة السيبرانية، أهدافها، وسبل الحد منها.

الفرع الاول: خصائص الجرائم السيبرانية.

تتميز الجرائم الإلكترونية بعدة خصائص تميزها عن الجرائم التقليدية، منها:

صعوبة معرفة مرتكب الجريمة :حيث لا يمكن تحديد الفاعل بسهولة إلا باستخدام وسائل أمنية وتقنية متقدمة، بسبب طبيعة الفضاء الإلكتروني.

صعوبة قياس الضرر :يتراوح الضرر بين معاناة الكيانات المعنوية، مثل السمعة والقيم الأخلاقية، والمادية، أو كلاهما معا، مما يعقد تقييم حجم الضرر.

سهولة وقوع الجريمة :نتيجة لغياب أو ضعف الرقابة الأمنية على الشبكات والأنظمة الإلكترونية.

سهولة إخفاء آثار الجريمة :حيث يتم طمس معالم الجريمة والدلائل التي تدل على مرتكبها بطرق تقنية متطورة.

أقل جهدا وعنفا جسديا :مقارنة بالجرائم التقليدية التي تتطلب تواجدًا ماديًا واستخدام القوة.

سلوك غير أخلاقي :تعكس هذه الجرائم ممارسات مرفوضة أخلاقيًا في المجتمع.

غياب التقيد بالمكان والزمان :حيث يمكن ارتكاب الجريمة من أي مكان وفي أي وقت دون قيود جغرافية أو زمنية[66].

الفرع الثاني: أهداف الجرائم السيبرانية.

تتعدد الأهداف التي تسعى الجرائم السيبرانية إلى تحقيقها، ومن أبرزها:

تحقيق مكاسب غير مشروعة :سياسية أو مادية أو معنوية، عبر استخدام تقنيات المعلومات، مثل تزوير بطاقات الائتمان، الاختراق، تدمير المواقع الإلكترونية، وسرقة الحسابات المالية.

الحصول على معلومات ووثائق سرية :خاصة بالمؤسسات الحكومية، المصرفية، أو الشخصية، بهدف ابتزاز الضحايا أو استخدامها لأغراض أخرى.

الوصول غير المصرح به إلى المعلومات :سرقتها أو حذفها أو تعطيلها أو تعديلها بما يخدم مصالح الجناة.

الفرع الثالث: سبل مكافحة الجرائم السيبرانية والحد منها.

تسعى الدول والحكومات إلى التصدي للجرائم الإلكترونية عبر عدة آليات، منها:

فرض سياسات دولية وعقوبات رادعة :تهدف إلى ردع مرتكبي الجرائم الإلكترونية، من خلال التعاون الدولي وتوحيد الجهود.

تفعيل أحدث التقنيات الأمنية :للكشف عن هوية الفاعلين وتتبعهم، وتطوير نظم الحماية الإلكترونية.

نشر التوعية المجتمعية :بتثقيف الأفراد حول مخاطر الجرائم السيبرانية وطرق الحفاظ على معلوماتهم الشخصية، مثل حماية الحسابات البنكية وبطاقات الائتمان.

[66] علي زياد: الصراع و الامن الجيوسيبراني في الساحة الدولية.مرجع سابق,ص89.

إنشاء مؤسسات متخصصة وخطوط ساخنة :لتلقي بلاغات الجرائم الإلكترونية وتقديم الدعم القانوني والفني للضحايا.

تحديث التشريعات والقوانين :لمواكبة التطورات التكنولوجية، وفرض قوانين جديدة تتعلق بالأشكال المستجدة من الجرائم الإلكترونية[67].

المطلب الثالث : المسؤولية الجنائية للجرائم الإلكترونية — نماذج مختارة.

تعد المسؤولية الجنائية للجرائم الإلكترونية من المواضيع الحيوية التي تتطلب تشريعات متخصصة لمواكبة التطورات التقنية وحماية الأمن المعلوماتي، سواء على المستوى الوطني أو الدولي. فيما يلي نماذج مختارة من التشريعات التي تناولت هذه المسؤولية:

الفرع الاول: القانون الجنائي الروسي.

ينظم القانون الجنائي للاتحاد الروسي الجرائم المرتكبة في ميدان المعلومات الحاسوبية، ويعرفها على أنها الجرائم التي تنتهك أمن المعلومات التي يكون موضوعها معلومات أو مرافق حاسوبية. وقد أُدرجت هذه الجرائم ضمن قانون جنائي مستقل لأول مرة عام 1996.

أهم المواد المتعلقة بالجرائم الإلكترونية في القانون الروسي:

المادة 272 :الوصول غير المصرح به إلى المعلومات الحاسوبية.

المادة 273 :إنشاء واستخدام وتوزيع البرامج الحاسوبية الضارة.

المادة 274 :انتهاك قواعد تخزين المعلومات الحاسوبية وإلحاق الأضرار بشبكات الاتصالات.

المادة 303 :إلغاء أو تدمير أو تعديل البيانات.

ويعنى مكتب "K" التابع لوزارة الشؤون الداخلية الروسية بمكافحة الجرائم في مجال تكنولوجيا المعلومات، عبر مكتب التدابير التقنية الخاصة[68].

[67] نفس المرجع السابق,ص89-90.

الفرع الثاني: القانون الجنائي الألماني.

يشمل القانون الجنائي الألماني جرائم أمن المعلومات الحاسوبية، منها:

نسخ أو إعادة إنتاج أو نقل المعلومات إلكترونياً أو مغناطيسياً (الفقرة 202 أ).

انتهاك سرية الاتصالات (المادة 206).

التزوير باستخدام سجلات تقنية وهمية (المادة 268).

تزييف البيانات ذات القيمة الإثباتية (المادة 269).

تدمير أو تعديل السجلات التقنية (المادة 274).

إتلاف وحدات معالجة البيانات أو ناقلات البيانات (الفقرة 303 ب).

التداخل غير المشروع في منشآت الاتصالات السلكية واللاسلكية (المادة 317).

كما يجرم القانون الألماني الاحتيال الحاسوبي، ويُعرف بأنه استخدام متعمد لبيانات غير صحيحة أو برامج مزيفة للحصول على مكاسب غير مشروعة[69].

الفرع الثالث: القانون الجنائي للوكسمبورغ.

يتضمن القانون الجنائي في لوكسمبورغ نصوصًا واضحة للجرائم السيبرانية، من أبرزها:

المادة 509–1 :المسؤولية عن الوصول غير المصرح به إلى نظم معالجة البيانات، مع عقوبات تشمل الغرامة أو السجن من شهرين إلى سنة، وتصل إلى سنتين إذا نتج عن الفعل تعديل أو تدمير البيانات.

المادة 509–2 :حظر التعطيل المتعمد أو تغيير أداء نظام معالجة البيانات، مع عقوبات تصل إلى 3 سنوات سجن.

---

[68] نفس المرجع السابق.ص91-92.
[69] نفس المرجع السابق.ص92-93

المادة 509–3 :حماية سلامة البيانات، ومسؤولية أي تعديل أو حذف أو تغيير تشغيل النظام.

المادة 524–4 :جريمة التدخل في الاتصالات السلكية واللاسلكية، بعقوبات غرامة أو سجن تصل إلى 3 سنوات[70].

الفرع الرابع: الجريمة الإلكترونية في القانون الدولي.

نظرا لأن الجرائم الإلكترونية غالبا ما تكون عابرة للحدود، فإن التعاون الدولي ضروري لمكافحتها. ومن أبرز الاتفاقيات الدولية:

اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية (اتفاقية بودابست 2001) :وقع عليها العديد من الدول الأعضاء في مجلس أوروبا، بالإضافة إلى دول من خارج القارة مثل الولايات المتحدة واليابان. تهدف الاتفاقية إلى توحيد الإطار القانوني للجرائم الإلكترونية وتعزيز التعاون الدولي في ملاحقتها[71].

تقسم الاتفاقية الجرائم المرتكبة في الفضاء السيبراني إلى أربع مجموعات رئيسية:

الجرائم المرتبطة بأنظمة الحواسيب: مثل الدخول غير المشروع إلى نظام معلوماتي (Unauthorized Access)، أو الاعتراض غير المشروع للبيانات.(Interception)

الجرائم المرتبطة بالبيانات: مثل تعديل البيانات بدون إذن (Data Interference) أو حذفها عمدا، وتخريب سلامتها الرقمية.

الجرائم المرتبطة بالمحتوى: كإنتاج أو نشر أو الوصول إلى مواد غير قانونية (مثل المواد الإباحية المتعلقة بالأطفال).

[70] **نفس المرجع السابق.ص93-94.**

[71] Council of Europe. *Convention on Cybercrime (Budapest Convention)*, ETS No. 185, Budapest, 23.XI.2001. تم الدخول في 6 جوان 2025. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

الجرائم المرتبطة بالتحايل والاحتيال الإلكتروني: وتشمل الاستخدام غير المشروع للبيانات، والتلاعب في المعاملات المالية الإلكترونية.

وتنص الاتفاقية أيضا على ضرورة تحديث التشريعات الوطنية، وتأسيس آليات للتعاون القضائي الفوري بين الدول، خصوصا لتبادل المعلومات الإلكترونية قبل أن يتم محوها[72].

[72] نفس المرجع السابق.ص93

الفصل الثاني : استراتيجية الدول الرائدة للأمن السيبراني (الو.م.أ، الصين، روسيا)

المبحث الاول :استراتيجية الولايات المتحدة للأمن السيبراني.

المطلب الأول: الإطار المؤسسي والفني للأمن السيبراني في الولايات المتحدة.

الفرع الاول: إطار العمل للأمن السيبراني(Cyber Security Framework – CSF)

يشكل إطار العمل للأمن السيبراني للولايات المتحدة (Cyber Security Framework – CSF) حجر الزاوية في المقاربة الاستراتيجية لحماية الأصول الرقمية والفيزيائية الحيوية للدولة. وقد أطلقه المعهد الوطني للمعايير والتكنولوجيا (NIST) كمبادرة رائدة تهدف إلى تمكين المؤسسات من بناء قدراتها الدفاعية بطريقة منظمة، قابلة للقياس، ومتكاملة مع الأهداف التجارية.

ينظم هذا الإطار عمليات الأمن السيبراني عبر **خمس وظائف أساسية** متداخلة ومتواصلة، تمثل دورة حياة إدارة المخاطر السيبرانية. لا ينحصر هدفها في الوقاية فقط، بل يمتد إلى الكشف، الاستجابة، والتعافي، ضمن منطق تكاملي يعكس وعيًا متقدمًا بترابط المجالات التقنية، المؤسساتية، والإنسانية[73].

1: التعرف(Identify)

تهدف هذه الوظيفة إلى **تأسيس وعي تنظيمي معمّق بالمخاطر السيبرانية** من خلال تحليل الأصول، السياق التشغيلي، وسلاسل التوريد. تشمل هذه الوظيفة ست فئات رئيسية:

إدارة الأصول

بيئة الأعمال

[73] U.S. General Services Administration. "Cybersecurity Framework." Last modified April 2025. https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/cybersecurity-framework.

الحوكمة

تقييم المخاطر

استراتيجية إدارة المخاطر

إدارة مخاطر سلسلة التوريد

تعد هذه المرحلة ضرورية لفهم ما ينبغي حمايته، ولماذا، وكيف يمكن تقييم تهديداته وتبعاته.

2: الحماية(Protect)

تُعنى هذه الوظيفة بوضع الضوابط الوقائية المناسبة لتقليل احتمالية الحوادث السيبرانية وتعطيل العمليات. وتتضمن سبع فئات منها:

إدارة الهوية والتحكم في الوصول

التوعية والتدريب

حماية البيانات وأمان المعلومات

الصيانة

واستخدام التقنيات الوقائية الحديثة

تشدد هذه الوظيفة على البعد البشري عبر تعزيز ثقافة الأمن داخل المؤسسة، إلى جانب الاعتماد على أدوات التحكم المتقدمة.

3: الكشف(Detect)

تركّز على **القدرة على التعرف السريع على الحوادث السيبرانية** من خلال أنظمة مراقبة دقيقة تعتمد على مؤشرات الشذوذ ونقاط التهديد.

تشمل هذه الوظيفة فئات كـ:

الشذوذ والأحداث

المراقبة الأمنية المستمرة

وآليات التحليل والاستجابة اللحظية

تعكس هذه الوظيفة انتقالًا نوعيًا من الدفاع التقليدي إلى نهج **استخباراتي تنبؤي** يعتمد على التحليل السلوكي للبيانات.

4: الاستجابة(Respond)

تضع هذه الوظيفة الإطار العملي لاتخاذ قرارات تكتيكية واستراتيجية **عند وقوع هجوم سيبراني مؤكد.**

تركّز على فئات مثل:

تخطيط الاستجابة

الاتصالات المؤسسية والداخلية

التحليل العملياتي

التخفيف من آثار الهجوم

التحسين المستمر بعد الحادثة

تهدف هذه الوظيفة إلى الحد من الضرر، استعادة الثقة، وتفادي تكرار السيناريوهات المماثلة.

5: التعافي(Recover)

تعنى بوضع خطط مرونة رقمية تساعد في **استعادة الخدمات والقدرات الحرجة** في أقصر وقت ممكن بعد الهجوم، دون المساس باستمرارية الأعمال. وتشمل هذه الوظيفة فئات:

تخطيط التعافي

الاتصالات

التحسينات المستندة إلى الدروس المستفادة

يشكل هذا الجزء صمام أمان لقياس نجاعة السياسات، وتصحيح الاختلالات البنيوية التي ظهرت أثناء الأزمة.

الوظيفة	الهدف	الفئات
التعرف (identify)	تطوير فهم تنظيمي لإدارة مخاطر الأمن السيبراني المتعلقة بالأنظمة، والأصول، والبيانات، والقدرات.	إدارة الأصول، بيئة الأعمال، الحوكمة، تقييم المخاطر، استراتيجية إدارة المخاطر، إدارة مخاطر سلسلة التوريد
الحماية (protect)	تطوير وتنفيذ التدابير الوقائية المناسبة لضمان تقديم خدمات البنية التحتية الحيوية.	إدارة الهوية، التوثيق والتحكم في الوصول، التوعية والتدريب، أمان البيانات، حماية المعلومات والإجراءات، الصيانة، التكنولوجيا الوقائية
الكشف (detect)	تطوير وتنفيذ الأنشطة المناسبة للتعرف على حدوث حدث أمني سيبراني.	الشذوذ والأحداث، المراقبة الأمنية المستمرة، عملية الكشف
الاستجابة (respond)	تطوير وتنفيذ الأنشطة المناسبة لاتخاذ إجراءات تجاه حدث أمني سيبراني تم اكتشافه.	تخطيط الاستجابة، الاتصالات، التحليل، التخفيف، التحسينات
التعافي (recover)	تطوير وتنفيذ الأنشطة المناسبة للحفاظ على خطط المرونة واستعادة أي قدرات أو خدمات تضررت بسبب حادث أمني.	تخطيط التعافي، التحسينات، الاتصالات

الفرع الثاني: التهديدات الداخلية وسبل مواجهتها.

في الوقت الذي تركز فيه الاستراتيجيات السيبرانية على التهديدات الخارجية، أظهرت الدراسات الأمنية الحديثة أن التهديد الداخلي يشكل أحد أخطر التحديات الأمنية التي تواجه المؤسسات

العامة والخاصة، لكونه يأتي من أفراد يمتلكون صلاحيات ونفاذًا شرعيًا إلى الأنظمة والبنية التحتية الحيوية. وقد أولت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) اهتماما بالغا بهذه الظاهرة، فوضعت تعريفا شاملا وعمليا للتهديد الداخلي، مؤكدة على أبعاده النفسية والسلوكية والتقنية في آن واحد.

1: تعريف التهديد الداخلي وأبعاده

يعرف التهديد الداخلي بأنه: أي خطر ناتج عن شخص يمتلك أو امتلك سابقا حق الوصول المصرح به إلى أنظمة أو معلومات المؤسسة، ويستخدم هذا النفاذ لإلحاق ضرر متعمد أو غير متعمد بسلامة المؤسسة أو مواردها أو أفرادها أو معلوماتها أو بنيتها التحتية[74]". يشمل هذا المفهوم طيفا واسعا من الأفعال، تمتد من الإهمال العرضي إلى التخريب المتعمد، مرورا بالتجسس وسرقة الملكية الفكرية.

2: تصنيف التهديدات الداخلية

تنقسم التهديدات الداخلية إلى ثلاثة أنماط رئيسية:

التهديدات غير المتعمدة:(Unintentional Threats)

ناتجة عن إهمال أو جهل المستخدم (مثال: فتح رابط تصيد، استخدام كلمة مرور ضعيفة، تجاهل التحديثات الأمنية).

تشكل غالبا مدخلا للهجمات الخارجية[75].

التهديدات المتعمدة:(Malicious Insiders)

[74] **ersecurity and Infrastructure Security Agency. Insider Threat Mitigation Guide. U.S. Department of Homeland Security, November 2020. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.cisa.gov**

[75] **Ibid**

تشمل الأفراد الذين يسعون عمدا إلى الإضرار بالمؤسسة بدافع الانتقام أو الطمع أو دوافع أيديولوجية.

من أمثلتها: تسريب بيانات سرية، تخريب الأنظمة، سرقة معلومات الملكية الفكرية[76].

التهديدات التواطؤية والطرف الثالث:(Third-Party and Collusion)

عندما يتعاون موظف داخلي مع جهة خارجية (هاكرز، جهات استخباراتية، منافسين).

أو عندما يشكل المقاولون أو موردو الخدمات مصدرا للتهديد بسبب امتلاكهم صلاحيات الوصول[77].

3: المؤشرات السلوكية والتقنية للتهديد الداخلي

أصبح من الضروري تطوير آليات إنذار مبكر لرصد التهديدات الداخلية قبل أن تتحول إلى حوادث فعلية. ومن بين أبرز المؤشرات:

تغييرات سلوكية مفاجئة (عزلة، غضب، سلوك عدواني).

محاولات وصول غير مبرر إلى ملفات حساسة.

تحميل كميات كبيرة من البيانات إلى أجهزة خارجية.

الدخول إلى الأنظمة خارج أوقات العمل.

استخدام أدوات تشفير أو مسح آثاري غير مصرح بها[78].

4: استراتيجيات المواجهة والتقليل من المخاطر

[76] lbid
[77] lbid
[78] lbid

توصي الأدبيات السيبرانية الحديثة باعتماد نهج شامل متعدد الأبعاد يجمع بين التكنولوجيا والموارد البشرية والسياسات المؤسساتية، ومن أبرز التدابير:

إجراءات تقنية:

أنظمة إدارة الوصول[79].(IAM)

تحليل السلوك الرقمي[80].(UBA/UEBA)

أنظمة SIEM[81] لمراقبة الأحداث وتنبيهات الوقت الحقيقي.

سياسات داخلية صارمة:

تحديد صلاحيات النفاذ وفق مبدأ الحد الأدنى من الامتياز .(Least Privilege)

تقييم دوري للأذونات[82].

بروتوكولات للإبلاغ عن السلوكيات المشبوهة.

الوعي والتكوين:

برامج توعية دورية حول أمن المعلومات.

تدريب الموظفين على اكتشاف الهندسة الاجتماعية.

تعزيز ثقافة الإبلاغ الآمن دون خوف من العقاب.(Safe Reporting Channels)

---

[79] **IAM – Identity and Access Management إدارة الهوية والتحكم في الوصول**
نظام يُستخدم لإدارة وتحديد هويات المستخدمين والتحكم في صلاحياتهم داخل المؤسسة.
يسمح بتحديد من يمكنه الوصول إلى ماذا، متى، ومن أي جهاز، بناءً على أدوار محددة.

[80] **UBA/UEBA – User (and Entity) Behavior Analytics تحليلات سلوك المستخدم والكيانات:**
تقنيات تعتمد على الذكاء الاصطناعي لتحليل سلوكيات المستخدمين داخل الشبكة، واكتشاف الأنشطة الشاذة أو غير الاعتيادية.

[81] **SIEM – Security Information and Event Management إدارة معلومات وأحداث الأمن**
نظام مركزي يُستخدم لجمع وتحليل وتنبيه البيانات الأمنية التي تولدها مختلف الأنظمة والبنى التحتية في الوقت الحقيقي.

[82] **التقييم الدوري للأذونات(Periodic Permissions Review)**
هو إجراء أمني تقوم من خلاله المؤسسات بمراجعة منتظمة للصلاحيات (الأذونات) الممنوحة للمستخدمين داخل الأنظمة الرقمية والشبكات.

تعاون استخباراتي داخلي/خارجي:

تبادل المعلومات مع وكالات إنفاذ القانون ومراكز الاستجابة للحوادث.

الاستفادة من قواعد بيانات التهديدات ومؤشرات الخطر السيبراني[83].(IoCs)

إن فهم التهديد الداخلي لا يقتصر على تحديد الجاني أو تحليل النوايا، بل يستدعي بناء منظومة وقائية واستباقية تعتمد على البيانات والسلوكيات والحوكمة الذكية. وفي سياق الأمن السيبراني الأمريكي، أصبح هذا النوع من التهديد أحد المحاور الأساسية التي توجه السياسات والاستثمارات والتقنيات، بوصفه خطرًا «من الداخل» قد يكون أكثر فتكًا من آلاف الهجمات من الخارج .

المطلب الثاني: العقيدة العسكرية السيبرانية للولايات المتحدة.

الفرع الاول: الاعتراف الرسمي بالعمليات السيبرانية التكتيكية.

شهدت العقيدة العسكرية الأمريكية تحولا جوهريا في تصورها للفضاء السيبراني، تمثل في إدراج العمليات السيبرانية التكتيكية ضمن العقيدة الرسمية، وذلك في النسخة المحدثة من الوثيقة المشتركة" JP 3–12 عمليات الفضاء السيبراني"، الصادرة في ديسمبر 2022 عن وزارة الدفاع الأمريكية .(DoD) رغم عدم تصنيفها كمعلومات سرية، إلا أن الوثيقة متاحة فقط لحاملي بطاقات الوصول المشترك(CAC) ، ما يعكس حساسيتها الاستراتيجية[84].

من أبرز ما جاء في هذا الإصدار هو الاعتراف الرسمي بمفهوم "العمليات السيبرانية الاستكشافية " (Expeditionary Cyberspace Operations)، والتي تعرف بأنها:

"العمليات السيبرانية التي تتطلب نشر القوات السيبرانية ضمن المجالات الفيزيائية".

---

[83] **Indicators of Compromise (IoCs) : مؤشرات الخطر السيبراني (IoCs) هي بيانات رقمية تُستخدم لاكتشاف الأنشطة الخبيثة أو الاستجابة للحوادث الأمنية، وتشمل عناوين IP مشبوهة، أسماء نطاقات ضارة، تجزئة ملفات خبيثة، أو أنماط سلوك غير طبيعية في الشبكة.**

[84] U.S. Department of Defense. *Joint Publication (JP) 3-12: Cyberspace Operations*. Washington, D.C.: Joint Chiefs of Staff, December 2022. *(Access restricted via Common Access Card - CAC).*

هذا التعريف يترجم نضوج المقاربة السيبرانية الأمريكية، ويعكس تحولا نوعيا من نموذج "الهجمات عن بعد" إلى قدرات هجومية ميدانية تمكن من الوصول الفعال إلى أهداف حساسة، لا يمكن استهدافها عبر الإنترنت فقط، إما لكونها معزولة، أو محمية ببنى تحتية لا تسمح بالنفاذ التقليدي.

1: دور القيادة السيبرانية الأمريكية(Cybercom) .

تتولى القيادة السيبرانية الأمريكية (Cybercom) مسؤولية التخطيط والإشراف على كافة العمليات السيبرانية الهجومية والدفاعية داخل وزارة الدفاع، حيث تعمل بالتنسيق مع الفروع الأربعة للقوات المسلحة، التي توفر فرقا سيبرانية متخصصة.

•تقليديا كانت صلاحيات تنفيذ هذه العمليات مركزية وتخضع للموافقة على أعلى مستويات الدولة.

•مؤخرا تم تفويض بعض الصلاحيات الهجومية للمستويات الأدنى بهدف تحسين سرعة الاستجابة وتخفيف البيروقراطية، مع المحافظة على التنسيق الاستخباراتي[85].

رغم ذلك، لا تزال غالبية العمليات تنفذ من قواعد أو مواقع نائية، وتتركز على الشبكات المرتبطة ببروتوكول الإنترنت(IP-based networks) ، ما يحدّ من فاعليتها في مواجهة البنى المعزولة أو الشبكات ذات الطبقة الفيزيائية غير المرتبطة بالإنترنت.

2: الحاجة إلى قدرات ميدانية هجومية.

تبرز الوثيقة المحدثة أن الوصول إلى بعض الأهداف السيبرانية الحساسة يتطلب الوجود الفيزيائي المباشر[86] للقوات السيبرانية في الميدان. تشمل الأسباب:

[85] U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Fort Meade, MD: U.S. Cyber Command, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

[86] **Joint Chiefs of Staff. *Joint Concept for Entry Operations*. Washington, D.C.: U.S. Department of Defense, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jceo.pdf**

شبكات معزولة :(Air-Gapped) مثل أنظمة التحكم الصناعية أو البنى التحتية الحيوية غير المتصلة بالإنترنت.

التكتيك التأخيري للوصول عن بعد :بعض الأهداف تتطلب وقتا طويلا للاختراق، مما قد يفشل الأثر الزمني المطلوب للعملية.

الحاجة إلى تأثيرات فورية وموضعية :مثل تعطيل أنظمة دفاعية لحظيا قبل أو أثناء عملية عسكرية تقليدية.

وبذلك، ظهرت العمليات السيبرانية الاستكشافية كحل استراتيجي لخلق تأثيرات هجومية مباشرة أو غير مباشرة على الأرض، سواء عبر الفرق السيبرانية أو بالتحالف مع قوات العمليات الخاصة (SOF).[87]

3: التكامل مع مجتمع الاستخبارات والتخطيط العملياتي

تنص العقيدة الجديدة على أن كل عملية سيبرانية ميدانية يجب أن تنسق مع مجتمع الاستخبارات الأمريكي لتفادي ما يعرف بـ تعارض المكاسب والخسائر الاستخباراتية (Intelligence Gain/Loss Deconfliction)،[88] وهو مبدأ ينص على وجوب الموازنة بين:

الفائدة الاستخباراتية من استمرار اختراق معين

مقابل التأثير العملياتي الناتج عن استخدام هذا الاختراق في هجوم فعلي

وهو توازن دقيق يُدار في غرف قيادة مشتركة تضم ممثلين عن وزارة الدفاع، وكالة الأمن القومي (NSA)، ووكالة الاستخبارات المركزية.(CIA)

4: دعم القيادة القتالية عبر الانتشار السيبراني الأمامي

[87] Special Operations Forces: قوات العمليات الخاصة (SOF) هي وحدات عسكرية أمريكية عالية التدريب والتجهيز، تُكلّف بمهام حساسة ومعقدة مثل مكافحة الإرهاب، الاستطلاع الخاص، والعمليات غير التقليدية، وتُستخدم غالبًا في البيئات عالية الخطورة أو ذات الطبيعة الاستراتيجية الدقيقة.

[88] Joint Chiefs of Staff. Joint Targeting School Student Guide. Washington, D.C.: U.S. Department of Defense, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf.

استجابة لتطور التهديدات وتزايد الطلب على القدرات السيبرانية، توصي العقيدة الجديدة بما يسمى "الامتداد إلى الأمام(Forward Deployment) "، والذي يتضمن:

نشر فرق سيبرانية مجهزة في مسارح العمليات)أوامر القتال(COCOMs

إمكانية تنفيذ هجمات سيبرانية محلية أو إقليمية بتنسيق لحظي

دعم العمليات المشتركة بمرونة أكبر، خصوصا عند الحاجة إلى قرارات هجومية فورية(Zero-hour execution)

وقد صرح الجنرال كيفن كينيدي (قائد القوات الجوية السيبرانية) أن هذه النقطة تمثل منعطفا استراتيجيا في كيفية تفكير الجيش في دمج القوات السيبرانية ضمن الخطط التكتيكية الميدانية، من خلال استخدام المنصات الجوية والجنود الميدانيين كمصادر قوة رقمية هجومية[89].

5: إعادة هيكلة الفرق السيبرانية حسب الفروع العسكرية

لم تعد جميع القدرات السيبرانية الأمريكية مركزية ضمن .Cybercom بل بدأت كل من القوات الجوية، البحرية، البرية والمارينز في:

بناء فرقها السيبرانية الخاصة

دمج الحروب السيبرانية مع الحرب الإلكترونية(EW)

إنشاء وحدات "تأثيرات غير حركية(Non-Kinetic Effects Teams) "

توسيع نطاق مهام كتائب الحرب السيبرانية التكتيكية كالكتيبة الحادية عشرة في الجيش الأمريكي

[89] U.S. Department of Defense. 2023 Cyber Strategy Summary. Washington, D.C.: U.S. Department of Defense, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY_SUMMARY.PDF.

هذا التحول يؤشر إلى ظهور عقيدة لا مركزية هجومية مرنة، قادرة على الاستجابة السريعة، وتكييف القدرات الرقمية مع متطلبات بيئات المعارك الحديثة، خصوصا تلك المتوقعة بحلول عام 2030، حيث ستصبح البيئة السيبرانية جزءا لا يتجزأ من ميدان المعركة الشاملة[90].

الفرع الثاني: استجابة الفروع العسكرية الأمريكية للتكامل السيبراني التكتيكي.

مع التحول التدريجي نحو تضمين القدرات السيبرانية في صلب العمليات التكتيكية، لم تعد القوات المسلحة الأمريكية تتعامل مع الأمن السيبراني كمجال منفصل أو داعم فقط، بل بدأت بتضمينه في هيكلها العملياتي والتنظيمي، عبر إنشاء وحدات متخصصة وتطوير عقائد قتالية هجينة. ينعكس هذا التطور في تعامل كل فرع عسكري مع القدرات السيبرانية من منظور عملياتي مستقل ومتكامل في آن واحد.

1: القوات الجوية الأمريكية(U.S. Air Force)

أظهرت القوات الجوية وعيا استراتيجيا مبكرا بأهمية القدرات السيبرانية الاستكشافية (Expeditionary Cyber Capabilities)، حيث صرح الفريق كيفن كينيدي، قائد "القوات الجوية السيبرانية – 16th Air Force"، بأن التكامل بين المنصات الجوية والوحدات الأرضية يفتح آفاقا جديدة لإنشاء تأثيرات سيبرانية متزامنة مع الهجمات التقليدية[91].

تستفيد القوات الجوية من الانتشار الواسع للأصول الجوية كمنصات هجومية واستطلاعية في المجال السيبراني، مما يتيح تنفيذ هجمات رقمية ميدانية أو عبر الجو لدعم المهام الجوية أو العمليات البرية المتزامنة.

2: القوات البحرية الأمريكية(U.S. Navy)

[90] U.S. Department of Defense. 2023 Cyber Strategy Summary. Washington, D.C.: U.S. Department of Defense, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY_SUMMARY.P

[91] U.S. Air Force. "16th Air Force Cyber Warriors Increase Interoperability During Cyber Coalition 2023." December 6, 2023. https://www.cybercom.mil/Media/News/Article/3633256/16th-air-force-cyber-warriors-increase-interoperability-during-cyber-coalition/.

تبنت البحرية نهجا تكامليا عبر تأسيس فرق التأثيرات غير الحركية (Non-Kinetic Effects Teams)، التي تدمج القدرات السيبرانية والمعلوماتية في بيئة بحرية.

كما أنشأت قيادة المعلومات البحرية(MCIC) ، وهي بنية قيادية جديدة تهدف إلى توحيد جهود الحرب السيبرانية، الاستخبارات العسكرية، والعمليات الفضائية، من أجل دعم المهام البحرية الاستراتيجية[92].

تسمح هذه البنية للبحرية بشن عمليات سيبرانية هجومية انطلاقا من البحر، سواء من السفن القتالية أو الغواصات، مما يعزز من مرونة الانتشار السيبراني في المحيطات والمياه الدولية.

3: الجيش الأمريكي(U.S. Army)

كان الجيش الأمريكي من أوائل الفروع التي أدركت أهمية العمليات السيبرانية التكتيكية المصاحبة للقوات الميدانية، حيث أنشأ الكتيبة السيبرانية الحادية عشرة(11th Cyber Battalion) ، والتي تضم اختصاصات في:

العمليات السيبرانية الهجومية

الحرب الإلكترونية(Electronic Warfare – EW)

عمليات المعلومات(Information Operations – IO)

بالإضافة إلى ذلك، شُكِّلت فرق(CEMA (Cyber and Electromagnetic Activities ، التي ترافق الوحدات القتالية في الميدان وتوفر تغطية رقمية وإلكترونية في الوقت الفعلي[93].

يعكس هذا التحول دمجا فعليا للقدرات الرقمية في العمليات القتالية البرية، عبر وحدات قادرة على تعطيل الاتصالات، اختراق الشبكات المعادية، أو حماية الأصول الرقمية الميدانية.

[92] U.S. Navy. "Navy Establishes Naval Information Warfare Development Center." October 1, 2020. https://www.navy.mil/Press-Office/News-Stories/Article/2369341/navy-establishes-naval-information-warfare-development-center/.

[93] U.S. Army. "Army Activates First Cyber Battalion." August 23, 2019. https://www.army.mil/article/225221/army_activates_first_cyber_battalion.

4: سلاح مشاة البحرية(U.S. Marine Corps)

تبنى مشاة البحرية نهجا شاملا منذ عام 2017 بإنشاء وحدات معلومات قتالية (MIGs) لدعم عملياتهم البرمائية. ثم أُطلقت لاحقا قيادة المعلومات البحرية[94](MCIC) ، التي تعد همزة الوصل بين:

القدرات السيبرانية

الاستخبارات الميدانية

الفضاء السيبراني العسكري

ما يميز سلاح مشاة البحرية هو سعيه إلى الاستقلال العملياتي عنCybercom ، حيث تسعى وحداته للاستفادة من القدرات السيبرانية بشكل مباشر وفوري أثناء العمليات، دون الاعتماد على التنسيق البيروقراطي مع الوكالات الاستخباراتية الكبرى.

يُمكّن هذا النموذج الفرق القتالية البرمائية من شن عمليات هجومية رقمية متزامنة مع الإنزال العسكري، ما يجعلهم أكثر مرونة في مسارح القتال الديناميكية.

الفرع الثالث: الرؤية المستقبلية: ملامح الحرب السيبرانية القادمة.

إن استجابات الفروع العسكرية الأمريكية تشير إلى تحول عقائدي جذري في مفهوم الأمن السيبراني العسكري[95]، يمكن تلخيص ملامحه المستقبلية فيما يلي:

تغيير نمط الهجمات السيبرانية: لم يعد الهجوم الرقمي مقصورا على مراكز القيادة أو الأنظمة الاستراتيجية، بل بات أداة ميدانية تستخدم لحظيا في المعركة، كما تستخدم الأسلحة التقليدية.

[94] U.S. Marine Corps. "Marine Corps Activates Information Command." October 1, 2019. https://www.marines.mil/News/News-Display/Article/1975474/marine-corps-activates-information-command/.

[95] U.S. Department of Defense. "2023 Cyber Strategy Summary." September 12, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY_SUMMARY.PDF.

اندماج السيبراني مع الحرب الإلكترونية:(EW) يؤدي التقارب بين الترددات الراديوية والأنظمة المغلقة إلى دمج تقنيات التشويش، الاختراق، والهجوم الإلكتروني في منظومة واحدة.

تفكيك المركزية السيبرانية: أصبحت كل قوة عسكرية تمتلك قدرات سيبرانية ذات طابع ميداني مستقل، مما يسمح لها بالتصرف السريع دون الرجوع إلى مراكز القرار البعيدة.

دخول الذكاء الاصطناعي والأنظمة المستقلة: تتوقع هيمنة الذكاء الاصطناعي على مجال الحرب السيبرانية التكتيكية، عبر تطوير أدوات ذاتية التشغيل قادرة على اتخاذ القرار في بيئة ميدان الحرب متعددة المخاطر.

المطلب الثالث: حماية البنية التحتية الحيوية في سياق الأمن السيبراني.

الفرع الاول: التوجيهات الرئاسية HSPD-7 و PPD-21 .

أدركت الولايات المتحدة الأمريكية، منذ مطلع القرن الحادي والعشرين، أن حماية البنية التحتية الحيوية لا يمكن أن تظل حبيسة المقاربات التقليدية، خاصة في ظل تزايد التهديدات السيبرانية والهجمات الإرهابية المعقدة. ولتحقيق قدر من الحصانة الاستراتيجية، أُصدرت عدة توجيهات رئاسية تُشكل الإطار المرجعي للسياسات الفيدرالية ذات الصلة، أهمها :التوجيه الرئاسي للأمن الداخلي رقم 7 (HSPD-7) والتوجيه الرئاسي للسياسة رقم 21.(PPD-21)

1/ التوجيه الرئاسي – HSPD-7 حجر الأساس الاستراتيجي:

صدر HSPD-7 سنة 2003 ليُحدد سياسة وطنية واضحة لحماية البنية التحتية الحيوية والموارد الأساسية من الهجمات الإرهابية، مع التأكيد على تفعيل التنسيق بين جميع مستويات الحكومة والقطاع الخاص[96].

أ.أهداف التوجيه:

[96] U.S. Department of Homeland Security. "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." December 17, 2003. https://www.dhs.gov/homeland-security-presidential-directive-7.

يرتكز HSPD-7 على هدف مزدوج:

تحديد الأولويات الوطنية في حماية البنية التحتية.

تقليص مواطن الضعف التي يمكن أن تستغلها الجماعات الإرهابية أو الجهات المعادية.

ويؤكد التوجيه أن تعطيل البنية التحتية الحيوية قد يؤدي إلى آثار صحية كارثية أو اضطرابات اقتصادية عميقة أو زعزعة الثقة العامة، ما يجعل من تعزيز الحماية ضرورة أمن قومي.

مكونات البنية التحتية المشمولة: يعرف التوجيه البنية التحتية الحيوية بأنها تشمل:

الأصول الفيزيائية)مباني، منشآت صناعية، محطات طاقة(...

والأنظمة السيبرانية)شبكات المعلومات، التحكم الصناعي، مراكز البيانات(...

وتمتد هذه الأصول لتغطي جميع القطاعات الاقتصادية، مما يبرز التداخل الشديد بين الأمن السيبراني والتنمية الاقتصادية والاجتماعية.

ب. آليات السياسة الفيدرالية في حماية البنية التحتية

مسؤوليات وزارة الأمن الداخلي(DHS)

تضطلع وزارة الأمن الداخلي بالدور القيادي في:

تنسيق الاستراتيجيات الوطنية.

إعداد تقارير الأمن الدوري.

إدارة قنوات تبادل المعلومات بين الفيدراليين، الولايات، والقطاع الخاص[97].

دور باقي الوزارات والوكالات

[97] lbid

تم توزيع المسؤوليات حسب طبيعة البنية التحتية، كما يلي:

الجهة	مجال الحماية
وزارة الدفاع(DoD)	المنشآت العسكرية
وزارة العدلFBI /	التحقيقات في التهديدات الإرهابية
وزارة الطاقة(DOE)	محطات توليد الكهرباء، منشآت الغاز والنفط
وزارة الصحة والخدمات الإنسانية(HHS)	البنية الصحية والاستجابة البيولوجية
وزارة الخزانة	الأسواق والمؤسسات المالية
وكالة حماية البيئة(EPA)	منشآت معالجة المياه والصرف الصحي

يعكس هذا التوزيع إدراكا مؤسساتيا بأن الأمن السيبراني لا يمكن أن يُفصل عن السياقات القطاعية، بل يجب أن يدمج ضمن خطط وقائية متخصصة.

ج. التنسيق مع الولايات والقطاع الخاص

بحكم أن معظم البنية التحتية الحيوية مملوكة للقطاع الخاص أو للولايات، يُشدد HSPD-7 على:

تقديم المساعدة الفنية والمالية للولايات والمحليات لتطوير خطط الأمن.

تعزيز الشراكة الاستراتيجية مع القطاع الخاص لتبادل المعلومات الحساسة، وبناء آليات استجابة مشتركة للهجمات المحتملة[98].

هذا النموذج التشاركي يُعد سابقة في السياسات العامة، حيث ينتقل الأمن من كونه شأنا حكوميا صرفا إلى مسؤولية جماعية متعددة الأطراف.

د. أثر التوجيه على الأمن السيبراني

[98] Ibid

يشير التوجيه إلى أن حماية البنية التحتية لا تكتمل إلا بتعزيز أمنها السيبراني، خاصة في ظل الاعتماد المتزايد على الشبكات الذكية، نظم التحكم الصناعية(SCADA) ، وخدمات الحوسبة السحابية. كما أنه يُقر بأن أي اختراق سيبراني واسع قد يؤدي إلى شلل وظيفي في قطاعات الطاقة، النقل، الاتصالات، والمالية.

2/ PPD-21 :استكمال وتحديث المسار

في 2013، صدر التوجيه الرئاسي للسياسة رقم 21 (PPD-21) لتحديث فلسفة HSPD-7 بما يتلاءم مع التحديات الحديثة، لا سيما:

دمج الأمن السيبراني بشكل أعمق في تقييم المخاطر.

تعزيز الصمود (resilience) وليس فقط الحماية.

التأكيد على أهمية التحليل متعدد القطاعات لتفادي التأثير المتسلسل (Domino Effect) لهجمات كبرى[99].

يعد HSPD-7 و PPD-21تجسيدا لتحول نوعي في تصور الدولة الأمريكية لمفهوم الحماية الوطنية، حيث أصبح الأمن السيبراني عنصرا مدمجا في السياسات الدفاعية، الاقتصادية، والاجتماعية.

وتظهر أهمية هذه التوجيهات في كونها لا تحدد فقط من سيحمي وماذا، بل كيف يتم ذلك ضمن بيئة متعددة الجهات ومتغيرة التهديدات، مما يجعل منها مرجعا دوليا في الحوكمة السيبرانية الوقائية.

الفرع الثاني: القطاعات الحيوية للبنية التحتية وأولوية الحماية السيبرانية.

1: التداخل البنيوي بين القطاعات الحيوية.

[99] The White House. "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience." February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

تعد **القطاعات الستة عشر للبنية التحتية الحيوية** التي حددها التوجيه الرئاسي رقم 21 (PPD-21)الركائز الأساسية للأمن القومي والاقتصادي للولايات المتحدة. وتمتد هذه القطاعات لتشمل أنظمة وخدمات مادية وافتراضية، يمكن أن يؤدي تعطلها أو تدميرها إلى تأثيرات جسيمة على **الصحة العامة، السلامة، الاقتصاد، أو الأمن الوطني.**

يتزايد الوعي الإستراتيجي بأن الحماية السيبرانية لهذه القطاعات لم تعد اختيارا، بل ضرورة وجودية أمام تصاعد التهديدات الرقمية المعقدة.

تتسم هذه القطاعات بدرجة عالية من **الاعتماد المتبادل(Interdependence)** ، حيث إن تعطل قطاع واحد قد يحدث سلسلة من الانقطاعات في قطاعات أخرى.

فعلى سبيل المثال:

أي **هجوم سيبراني** على قطاع الطاقة يمكن أن يعطل شبكات الاتصالات والنقل.

واختراق في أنظمة **الخدمات المالية** قد يعرض سلسلة التوريد بأكملها للخطر.

ومن هنا، تبنت الوكالات الأمريكية **منهجية شاملة للحماية** تراعي هذه العلاقات المعقدة[100].

2: قائمة القطاعات الستة عشر حسب التوجيه PPD-21 .

[100] **Cybersecurity and Infrastructure Security Agency (CISA). "Critical Infrastructure Sectors." Accessed June 7, 2025. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.**

فيما يلي تصنيف القطاعات الحيوية مع لمحة عن أهميتها ومخاطرها السيبرانية:

القطاع	الأهمية	مخاطر الأمن السيبراني
الطاقة(Energy)	يعد المحرك الرئيسي للاقتصاد، ويغذي كافة القطاعات	شبكاتSCADA ، منشآت الكهرباء، أنابيب النفط
الاتصالات(Communications)	البنية التحتية للربط الوطني والقيادة والسيطرة	اختراق الشبكات، التشويش، انقطاع الخدمة
تكنولوجيا المعلومات(IT)	أساس الرقمنة والإدارة الذكية	هجمات البرمجيات الخبيثة، تسريب البيانات
الخدمات المالية (Financial Services)	تمويل الاقتصاد، المعاملات البنكية، الأسواق	الاحتيال الرقمي، هجمات الفدية، تعطل الأنظمة
الرعاية الصحية والصحة العامة (Healthcare & Public Health)	حماية الأرواح وسلامة المجتمع	تسريب السجلات الطبية، تعطيل أجهزة الرعاية
أنظمة المياه والصرف الصحي (Water & Wastewater Systems)	الصحة العامة والبيئة	تلويث المياه، تعطيل المضخات الذكية
أنظمة النقل (Transportation Systems)	حركة البضائع والركاب	هجمات على الطيران، القطارات، الموانئ
الغذاء والزراعة(Food & Agriculture)	الأمن الغذائي، الاستقرار الاجتماعي	تخريب سلاسل الإمداد، الهجمات على المعدات

الصناعة الدفاعية (Defense Industrial Base)	دعم العمليات العسكرية والبحوث الدفاعية	التجسس الصناعي، استهداف أنظمة التصميم
المنشآت التجارية (Commercial Facilities)	التجمعات العامة، مراكز الأعمال	هجمات على مراكز البيانات، أنظمة الحجز
الخدمات الحكومية (Government Facilities)	مؤسسات الدولة، العدالة، التعليم	تسريب المعلومات، تزييف الهوية، تعطيل العمل
قطاع الكيمياء (Chemical)	صناعة آلاف المنتجات الحيوية	تخريب منشآت التخزين أو التحكم الإلكتروني
قطاع التصنيع الحيوي (Critical Manufacturing)	إنتاج السلع الحيوية	استهداف الآلات، سرقة التصاميم
قطاع السدود (Dams)	التحكم في المياه والطاقة الكهرومائية	فتح البوابات عن بُعد، التلاعب بأنظمة الضغط
قطاع المفاعلات النووية (Nuclear Reactors, Materials & Waste)	الطاقة النووية والبحوث الإشعاعية	تعطل أنظمة التبريد، تسريب بيانات حساسة
خدمات الطوارئ (Emergency Services)	الإسعاف، الإطفاء، الشرطة، الدفاع المدني	تعطيل أنظمة الاتصال، شلّ الاستجابة السريعة

الفرع الثالث: مقاربة الحماية السيبرانية لهذه القطاعات.

1. التقييم الدوري للمخاطر

تقوم كل وكالة قطاعية محددة (SSA) بإجراء تقييمات[101] دورية تشمل:

تحليل التهديدات السيبرانية المحتملة.

فحص الثغرات التقنية والتنظيمية.

[101] **Ibid**

تصنيف الأصول وفقًا للأهمية الحرجة.

.2تحديث معايير الأمن الرقمي

تم تطوير أطر مثل:

NIST Cybersecurity Framework

CISA Sector-Specific Guidelines

وذلك لضمان توافق سياسات الحماية مع المعايير الفيدرالية، وتعميم أفضل الممارسات على الشركاء في القطاع الخاص[102].

.3التعاون الاستخباراتي والتشغيلي

تشارك القطاعات المعلومات مع:

وزارة الأمن الداخلي(DHS)

وكالةCISA

مركز تبادل وتحليل المعلومات القطاعي(ISACs)

لتنشيط آليات **الاستجابة السريعة والتحذير المبكر**.

الفرع الرابع: التحديات المستقبلية وأولويات السياسات العامة.

رغم الجهود المبذولة تبقى عدة تحديات قائمة:

تسارع التقنيات التخريبية مثل الذكاء الاصطناعي والأسلحة السيبرانية الذاتية.

الهجمات المعقدة التي تستهدف التفاعل بين قطاعات متعددة.(multi-vector attacks)

[102] **Ibid**

النقص في القوى العاملة المؤهلة في مجال الأمن السيبراني الصناعي[103].(ICS)

وتتمثل أبرز الأولويات المستقبلية في:

بناء **مراكز تنسيق متعددة القطاعات.**

تعميم استخدام **أنظمة الإنذار السيبراني المبكر.**

إدماج الأمن السيبراني في **تصميم البنية التحتية الجديدة منذ البداية (security by design).**

إن القطاعات الستة عشر تشكل بنية وظيفية متداخلة ومعقدة، لا يمكن حمايتها إلا من خلال **رؤية سيبرانية جماعية موحدة،** تجمع بين التقييم المستمر، الجهوزية التقنية، والقدرة على التكيف مع التهديدات الديناميكية. وقد برهنت التجارب الأمريكية أن حماية البنية التحتية لم تعد مسألة جدران وحواجز، بل أصبحت **مسألة خوارزميات واستخبارات رقمية وتنسيق استراتيجي عبر كافة المستويات.**

[103] يشير مصطلح الأمن السيبراني الصناعي (ICS Cybersecurity) إلى حماية أنظمة التحكم الصناعية مثل SCADA و PLCمن التهديدات الرقمية، ويُعد مجالًا متخصصًا يُعنى بتأمين البنية التحتية الحيوية كشبكات الكهرباء، المياه، النقل، والمصانع من الهجمات السيبرانية التي تستهدف المعدات الميدانية والعمليات التشغيلية.

المبحث الثاني: استراتيجية الصين للأمن السيبراني وقدراتها.

المطلب الأول: الاستراتيجية والعقيدة العسكرية الصينية في الأمن السيبراني.

تقوم الاستراتيجية الصينية للأمن السيبراني على رؤية شاملة تستند إلى تهديدات متعددة الأبعاد من الولايات المتحدة، تشمل التهديدات الأيديولوجية والاقتصادية والعسكرية[104]، حيث تأثرت الصين بتطورات مبدأ الأمن السيبراني الأمريكي وخاصة من خلال العمليات العسكرية الأمريكية التي استخدمت الفضاء السيبراني، وكذلك دعم الولايات المتحدة للثورات السياسية عبر الإنترنت في بعض الدول.

في البداية، كان تركيز الصين الرئيسي داخليا بهدف منع انتشار الأفكار الليبرالية الغربية عبر الإنترنت، وقد تبنت مفهوم "السيادة السيبرانية" الذي يسمح للدول بالسيطرة على جزء الإنترنت الذي يقع ضمن سيادتها. ولتفعيل هذا المفهوم، نفذت الصين مشروع "الدرع الذهبي[105] Golden) " (Shield Projectأو "الجدار الناري العظيم" للرقابة والتصفية، وبدأت حظر بعض التطبيقات الأمريكية مثل فيسبوك وتويتر ويوتيوب بسبب تعارضها مع قوانين الرقابة الصينية[106].

في 2013 أدى كشف تسريبات إدوارد سنودن إلى إدراك الصينيين للفجوة الكبيرة بين قدراتهم السيبرانية والدفاعية مقارنة بالولايات المتحدة، ما دفع الرئيس شي جين بينغ لإجراء إصلاحات تنظيمية وقانونية واسعة لجعل الصين قوة سيبرانية كبرى. تأسست لجان ومؤسسات جديدة، منها لجنة مركزية للإعلام والأمن السيبراني[107] (CCIC) وإدارة الفضاء السيبراني في

---

[104] IISS, Cyber Capabilities and National Power: A Net Assessment, pp. 89–90.

[105] الدرع الذهبي:(Golden Shield Project)
هو برنامج أطلقته وزارة الأمن العام الصينية سنة 2003 بهدف تطوير منظومة وطنية للمراقبة الإلكترونية. يشمل المشروع مجموعة من الأنظمة التي تسمح للسلطات الصينية بمراقبة حركة الإنترنت، وتصفية المحتوى، وتعقب الأفراد. يُعرف عالميًا باسم "الجدار الناري العظيم (Great Firewall of China)" نظرًا لدوره في حجب مواقع ومنصات مثل Google و Facebookو Twitter، ويُعد أحد أقوى أنظمة الرقابة الرقمية في العالم.

[106] Ibid

[107] اللجنة المركزية للإعلام والأمن السيبراني (CCIC – Central Cyberspace Affairs Commission):
هي هيئة تابعة للحزب الشيوعي الصيني، تمثل أعلى سلطة لصياغة وتوجيه السياسات المتعلقة بالإعلام والفضاء السيبراني. تأسست عام

الصين[108](CAC) ، وأصدرت الصين استراتيجيتها الوطنية للأمن السيبراني في 2016 وقانون الأمن السيبراني في 2017[109].

تتضمن الاستراتيجية الصينية تسع مهام رئيسية مع تركيز قوي على السيادة الوطنية وتحسين القدرات الدفاعية السيبرانية، بما في ذلك تطوير الصناعة والتعليم في مجال الأمن السيبراني[110].

في الجانب الصناعي، أطلقت الصين استراتيجية "صنع في الصين 2025" التي تهدف إلى تقليل الاعتماد على الموردين الأجانب في التكنولوجيا الأساسية للإنترنت، بحيث تكون 70% من هذه التكنولوجيا محلية بحلول 2025، مع طموح لتصبح رائدة عالمياً بحلول 2030. ويكمل ذلك مبادرة "الحزام والطريق" التي تتضمن مكونا رقميا يسعى إلى فتح الأسواق العالمية لتكنولوجيا المعلومات الصينية[111].

على الصعيد العسكري، ترى الصين أن الحرب السيبرانية جزء من الحرب المعلوماتية الشاملة، حيث تشمل أنشطة الاستطلاع والهجوم والدفاع والردع. وفقًا لكتابات جيش التحرير الشعبي، تستهدف العمليات السيبرانية تعطيل شبكات العدو المدنية والعسكرية، مع أهمية كبيرة للاستراتيجية الوقائية التي تعتمد على الضربات الأولى للحد من قدرة العدو على التحكم والرد. وقد تطورت هذه العقيدة لتشمل مفاهيم مثل "مواجهة النظم" و"السيطرة على تدفق المعلومات"، وهي تستند إلى تجارب الصراع التي شهدتها أمريكا في حروبها، حيث استُهدفت أنظمة القيادة والسيطرة.

كما تستهدف الاستراتيجية استخدام القدرات السيبرانية في الحرب النفسية وكسب الهيمنة في الفضاء السيبراني دون تصعيد مفتوح، مع الاعتراف بالحاجة إلى تطوير شبكة دفاعية قوية وشاملة.

2014وتم رفع مستواها في 2018 لتُدار مباشرة من قبل القيادة العليا، وعلى رأسها الرئيس شي جين بينغ. تهدف إلى دمج الأمن السيبراني ضمن الأمن القومي الشامل، وتنسيق أعمال الرقابة والتحكم في الإنترنت.

[108] إدارة الفضاء السيبراني في الصين:(CAC – Cyberspace Administration of China)
هي الجهاز التنفيذي والإداري التابع للجنة المركزية(CCIC) ، وتُشرف على تنفيذ السياسات السيبرانية في جميع المقاطعات الصينية. تضطلع CACبمسؤوليات تشمل الرقابة على المحتوى الرقمي، تنظيم شركات الإنترنت، وحماية أمن المعلومات على المستوى الوطني.

[109] Ibid

[110] Ibid

[111] Lbid.p91

باختصار، تعكس الاستراتيجية والعقيدة الصينية للأمن السيبراني:

حرصا شديدا على الحفاظ على "السيادة السيبرانية" الوطنية والرقابة الداخلية.

توجها متزامنا نحو بناء قوة هجومية ودفاعية سيبرانية متقدمة قادرة على العمل في زمن الحرب والسلام.

دمج الأمن السيبراني في الخطط الصناعية والتنموية الوطنية، وخاصة تقليل الاعتماد على التكنولوجيا الأجنبية.

إدراكا بأن الأمن السيبراني جزء لا يتجزأ من الاستراتيجية العسكرية الحديثة والحرب المعلوماتية.

تطوير مؤسسات تنظيمية وقانونية متكاملة لضبط الفضاء السيبراني داخليا وخارجيا.

تُظهر الاستراتيجية والعقيدة الصينية للأمن السيبراني ملامح تكاملية متعددة تعكس تحول الصين إلى قوة رقمية صاعدة ذات طابع سيادي ومركزي. في صميم هذه الاستراتيجية، يبرز **مفهوم السيادة السيبرانية** كأولوية قصوى، إذ تسعى بكين إلى فرض سيطرتها الكاملة على الفضاء الرقمي الداخلي من خلال أدوات رقابية وتشريعية متقدمة. كما تتبنى الصين نهجًا **تركيبيا يجمع بين البعدين العسكري والصناعي**، حيث يتم توجيه الصناعة الرقمية الوطنية لخدمة أهداف الأمن القومي، خاصة عبر مبادرات مثل "صنع في الصين 2025" والحزام الرقمي ضمن مبادرة "الحزام والطريق". وتعزز هذه الرؤية من خلال **بنية مؤسساتية وقانونية متماسكة** تشمل اللجنة المركزية للإعلام والأمن السيبراني (CCIC) وإدارة الفضاء السيبراني(CAC) ، إلى جانب ترسانة من القوانين الحديثة. وفي الإطار العملياتي، تعمل الصين على **تطوير قدرات هجومية ودفاعية مرنة وشاملة**، تدار ضمن عقيدة معلوماتية تدمج الحرب السيبرانية بالحرب النفسية والاستباقية. وتستند هذه العقيدة إلى **النموذج الأمريكي في الحروب الحديثة**، خاصة في اعتماد الضربات الأولى كوسيلة لشل قدرات الخصم المعلوماتية منذ اللحظات الأولى للنزاع.

المطلب الثاني: الحوكمة، القيادة، والسيطرة في الأمن السيبراني الصيني.

تمثل الحوكمة والقيادة والسيطرة أركانا مركزية في الاستراتيجية السيبرانية لجمهورية الصين الشعبية، حيث تعكس نموذجا فريدا يجمع بين مركزية القرار السياسي بقيادة شي جين بينغ وتكامل الجهود المدنية والعسكرية ضمن منظومة متجانسة تسعى إلى الهيمنة السيبرانية الداخلية والخارجية.

الفرع الاول: مركزية القيادة وتوحيد السلطة السيبرانية.

منذ العام 2014، بسط الرئيس الصيني شي جين بينغ هيمنته على الفضاء السيبراني الوطني، فجمع مقاليد القيادة السيبرانية تحت سلطته المباشرة، مُكرّسا رؤيته حول ضرورة بناء قوة سيبرانية كبرى تمكّن الصين من مواجهة ما يعتبره تهديدات أيديولوجية وتكنولوجية غربية. وقد تجسد هذا التوجه في إنشاء اللجنة المركزية للأمن السيبراني والمعلوماتية، برئاسة شي جين بينغ، لتشكل المرجعية العليا في رسم السياسات وتوجيه الهيئات التنفيذية[112].

الفرع الثاني: الحوكمة المدنية والهيكل الإداري.

يتولى مكتب إدارة الفضاء السيبراني في الصين (CAC) المسؤولية التنفيذية لقيادة وتنظيم سياسات الأمن السيبراني في المجال المدني. ورغم وجود مؤسسات تنفيذية موازية كوزارة الأمن العام (MPS)[113]ووزارة الأمن الوطني(MSS)[114] ، فقد استطاعت CAC فرض نفسها كجهاز تنسيقي وهيكلي محوري، خصوصًا بعد إصدار قوانين وطنية وتنظيم عمل فروعها في كافة المقاطعات

[112] **"Xi Jinping Leads China's New Internet Security Group,"** ***The Diplomat,*** **February 28, 2014, https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/.**

[113] **MPS – Ministry of Public Security وزارة الأمن العام**
وزارة حكومية مسؤولة عن الأمن الداخلي، تشمل مهامها مكافحة الجرائم السيبرانية، ومراقبة المحتوى الرقمي، وضمان النظام العام في الفضاء الإلكتروني. تُعد الذراع الأمنية للشرطة في الصين.

[114] **MSS – Ministry of State Security وزارة أمن الدولة**
جهاز استخباراتي يُعنى بالأمن القومي، يشرف على مكافحة التجسس الرقمي والاختراقات السيبرانية ذات الطابع السياسي أو الأجنبي، ويعمل بشكل سري ويوازي في صلاحياته وكالات الاستخبارات المركزية في الدول الأخرى.

الـ31. وقد تجسد دورها في قيادة التشريعات الخاصة بحوكمة البيانات، الأمن السيبراني، ومراقبة المحتوى، مما أضفى طابعا شموليا على سيطرة الدولة الرقمية[115].

الفرع الثالث: القيادة العسكرية والهيكلة العملياتية.

على الصعيد العسكري، شهد العام 2015 ميلاد أحد أبرز التحولات في العقيدة السيبرانية الصينية مع إنشاء قوة الدعم الاستراتيجي(SSF)[116] ، التي أوكلت إليها مهام تنفيذ معظم القدرات السيبرانية للجيش الشعبي لتحرير الصين. وقد جاءت هذه الخطوة ضمن إصلاحات عسكرية واسعة هدفت إلى:

دمج القدرات المجزأة (الاستخبارات، الحرب النفسية، الحرب الإلكترونية، الدفاع السيبراني) ضمن بنية موحدة.

تحقيق جاهزية الحرب السيبرانية عبر تسريع التحول من وضع السلم إلى النزاع، ودمج العمليات السيبرانية ضمن العقيدة القتالية الشاملة.

تفعيل قدرة السيطرة المعلوماتية في الأزمات، باستخدام قدرات الحرب النفسية والهجمات السيبرانية والهجمات الحركية المتزامنة.

وترتبط SSF مباشرة بـ اللجنة العسكرية المركزية، ما يجعلها أداة تنفيذية فعالة للقرار السيادي الصيني في المجال السيبراني[117].

الفرع الرابع: التحديات البنيوية والتنسيقية.

---

[115] **"What Is the Cyberspace Administration of China (CAC)?," *Chinafy*, accessed June 7, 2025, https://www.chinafy.com/blog/what-is-the-cyberspace-administration-of-china-cac.**

[116] **SSF – Strategic Support Force قوة الدعم الاستراتيجي**
هي وحدة عسكرية أنشأها الجيش الشعبي لتحرير الصين في ديسمبر 2015 كجزء من إصلاحات هيكلية كبرى، وتهدف إلى دمج القدرات السيبرانية، والحرب الإلكترونية، والعمليات الفضائية، والحرب النفسية ضمن هيكل موحد. تُعد SSF الذراع المعلوماتية والتقنية الأساسية للجيش، وتتبع مباشرة اللجنة العسكرية المركزية، مما يمنحها دورًا مركزيًا في تنفيذ العمليات السيبرانية الدفاعية والهجومية.

[117] **Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR2058.html.**

رغم طابع المركزية الذي طبع إنشاء SSF ، لا تزال هناك تحديات على مستوى تنسيق العمل بين الوحدات التقليدية التابعة للجيش الصيني وقوات الدعم الجديدة، خاصة ضمن القيادات الإقليمية المشتركة. كما أن تقييمات المؤسسة العسكرية تُظهر أن إعادة هيكلة الوحدات السيبرانية لا تزال في مرحلة التشكل رغم التقدم المسجل[118].

الفرع الخامس: الحوكمة المتكاملة(المدني والعسكري)

تشير المعطيات إلى أن الحوكمة السيبرانية الصينية تعتمد على نموذج مركب:

مدنيا: يقوم على هيمنة الأجهزة التنظيمية والتشريعية CAC، MPS، MSS لتنظيم المحتوى الرقمي وحماية البيانات وبسط الرقابة الاجتماعية.

عسكريا: يعتمد على تركيز القيادة والعمليات تحت بنية موحدة (SSF)تمكن من تنفيذ عمليات هجومية ودفاعية متزامنة على المستويين السيبراني والإلكتروني[119].

تجسد الحوكمة والقيادة والسيطرة في النموذج الصيني للأمن السيبراني مقاربة شمولية ذات طابع سلطوي ومركزي، تتكامل فيها السلطات المدنية والعسكرية تحت قيادة سياسية موحدة. ويسعى هذا النموذج إلى تحقيق جاهزية سيبرانية قتالية كاملة، وتعزيز الرقابة الداخلية، ومواجهة التحديات الجيوسياسية من خلال إعادة تعريف سيادة الدولة في الفضاء الرقمي.

المطلب الثالث: القدرات السيبرانية الفعلية: الاستخباراتية، الهجومية، والتشريعية.

[118] **Demetri Sevastopulo and Ryan McMorrow, "Xi Jinping Tightens Grip on China's Military with New Information Warfare Unit,"** ***Financial Times,*** **April 20, 2024, https://www.ft.com/content/5584feb4-0e58-4b6c-8140-f9c6e8e3ba5e.**

[119] **James A. Lewis, "China's Emerging Cyber Governance System,"** ***Center for Strategic and International Studies (CSIS),*** **accessed June 7, 2025, https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber.**

يمثل هذا المطلب المرحلة التطبيقية في فهم استراتيجية الصين السيبرانية، حيث يتم التركيز على بنية وكفاءة أجهزتها الاستخباراتية، القدرات الهجومية السيبرانية، والإطار القانوني والتنظيمي الذي يُمكّن الدولة من السيطرة المحكمة على فضائها الرقمي.

الفرع الاول: القدرات الاستخباراتية السيبرانية.

تبنى البنية الاستخباراتية السيبرانية في الصين على منظومة مؤسساتية معقدة تجمع بين الطابع الأمني، السياسي والعسكري، وتندرج ضمن استراتيجية مركزية تهدف إلى الحفاظ على هيمنة الدولة على المجال الرقمي. ويتجلى هذا التنظيم من خلال ثلاث مؤسسات رئيسية:

وزارة أمن الدولة :(Ministry of State Security – MSS) تمثل الجهاز الاستخباراتي الأعلى في الصين، وتعنى بالأمن القومي ومكافحة التجسس، مع مهام موسعة تشمل عمليات جمع معلومات سرية في الداخل والخارج واستهداف البنى التحتية الحساسة ومصادر الابتكار التقني الأجنبية.

وزارة الأمن العام :(Ministry of Public Security – MPS) تضطلع بدور محوري في حفظ النظام العام الرقمي، من خلال الإشراف على البنية التحتية للمراقبة الداخلية، وإدارة قواعد البيانات الحكومية المرتبطة بالمواطنين، فضلا عن مكافحة الجريمة السيبرانية.

قوة الدعم الاستراتيجي :(Strategic Support Force – SSF) تمثل الذراع العسكرية السيبرانية لجيش التحرير الشعبي، وقد أُنشئت سنة 2015 لدمج القدرات السيبرانية، الفضائية، والحرب الإلكترونية ضمن هيكل عملياتي موحد، يعزز من قدرات الجيش في جمع الاستخبارات الإلكترونية وتنفيذ العمليات الهجومية.

تهدف هذه المنظومة المؤسسية إلى ترسيخ السلطة السياسية للحزب الشيوعي الصيني، وضمان الأمن الداخلي، وتعزيز تنافسية الصين عبر الحصول على المعلومات الاقتصادية والتقنية الاستراتيجية، إلى جانب تنفيذ حملات تأثير إعلامي ونفسي على الصعيدين الداخلي والخارجي.

وتعتمد الدولة الصينية في هذا الإطار على مجموعة من البرامج التكنولوجية المتقدمة لمراقبة السكان، أبرزها مشروع "**الدرع الذهبي** "الذي يشكل البنية التحتية للرقابة على الإنترنت، و"**سكاي نت**[120]" الذي يستخدم تقنيات التعرف على الوجوه في الزمن الحقيقي، بالإضافة إلى مشروع "**العيون الحادة** [121]"الذي يعزز المشاركة المجتمعية في عمليات الرصد. وتعتمد هذه المشاريع بشكل متزايد على أدوات الذكاء الاصطناعي لدمج وتحليل المعطيات البيومترية، والمراقبة البصرية، والسجلات الرقمية الرسمية، بما يسمح ببناء منظومة مراقبة شاملة ودقيقة ذات طابع استباقي[122].

الفرع الثاني: القدرات الهجومية السيبرانية والعسكرية.

تدرج الصين العمليات السيبرانية ضمن عقيدة "الحرب المعلوماتية الشاملة"، وقد قامت بإعادة هيكلة قواتها لتفعيل هذا التوجه:

تأسيس قوة الدعم الاستراتيجي (SSF) في 2015، وتوحيد القدرات السيبرانية والفضائية والإلكترونية تحت قيادة موحدة.

تطبيق مبدأ السيطرة على المعلومات وتعطيل أنظمة القيادة والسيطرة لدى الخصوم.

استخدام البرمجيات الخبيثة وهجمات متدرجة تتفادى التصعيد المباشر.

اعتماد مراحل الهجوم: استطلاع الشبكات، تحديد نقاط الضعف، تنفيذ الهجوم، تحليل الأثر.

---

[120] **"سكاي نت:(Skynet) "**
نظام مراقبة وطني واسع النطاق أطلقته الصين في إطار جهودها لبناء بنية أمنية رقمية متقدمة. يعتمد البرنامج على شبكة ضخمة من الكاميرات الذكية المدعّمة بتقنيات التعرف على الوجوه والذكاء الاصطناعي، ويهدف إلى تتبع الأفراد في الزمن الحقيقي، خاصة في المناطق الحضرية. يُعدّ هذا النظام أحد أكبر مشاريع المراقبة في العالم من حيث التغطية والقدرات التقنية، ويستخدم لتعزيز الأمن الداخلي ومكافحة الجريمة والانفصال الاجتماعي.

[121] **"العيون الحادة:(Sharp Eyes Project) "**
مشروع رقابة مجتمعية تكميلي لـ"سكاي نت"، يُركّز على توسيع رقعة المراقبة لتشمل المناطق الريفية والأحياء السكنية من خلال إشراك السكان في عمليات الرصد. يدمج المشروع بين الكاميرات العامة والخاصة، مع إمكانية وصول الأفراد إلى البث الحي من شاشات مثبتة في منازلهم أو مراكز مجتمعية، في إطار شعار "يشاهد الجميع، كل شيء، في أي وقت". يهدف المشروع إلى ترسيخ الرقابة الاجتماعية وخلق بيئة يُشرف فيها المواطنون على بعضهم البعض.

[122] **John Costello and Joe McReynolds, China's Strategic Support Force: A Force for a New Era, China Strategic Perspectives 13, National Defense University, 2018, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.**

تسخير الذكاء الاصطناعي في أنظمة الدفاع والهجوم السيبراني.

وتوظف الصين هذه القدرات في:

التجسس الصناعي وسرقة الملكية الفكرية.

تنفيذ اختراقات ضد الحكومات والشركات الأجنبية.

بناء قاعدة بيانات عالمية للمعلومات الاستراتيجية[123].

الفرع الثالث: الإطار القانوني والتنظيمي.

في سياق تعزيز مفهوم "السيادة السيبرانية"، شرعت الصين في بناء إطار قانوني صارم ومتكامل ينظم جميع جوانب الفضاء الرقمي، وذلك من خلال إصدار ثلاثة تشريعات مركزية تُشكّل البنية التشريعية الأساسية للأمن السيبراني في البلاد:

قانون الأمن السيبراني:(Cybersecurity Law – CSL)

صدر في عام 2017، ويُعد الركيزة التشريعية الأولى لحوكمة الفضاء الرقمي، حيث يحدد المعايير الخاصة بحماية البنية التحتية الحيوية للمعلومات، وتنظيم نشاطات مشغلي الشبكات، وتعزيز أمن المعلومات ضمن المجال السيبراني الوطني.

قانون أمن البيانات:(Data Security Law – DSL)

دخل حيّز التنفيذ في عام 2021، ويهدف إلى تنظيم تصنيف البيانات ومعالجتها وفقًا لدرجة حساسيتها وتأثيرها المحتمل على الأمن القومي، مما يسمح للدولة بتقييد أو منع تدفق أنواع محددة من البيانات عبر الحدود.

قانون حماية المعلومات الشخصية – Personal Information Protection Law)

:(PIPL أقر في عام 2021، ويعد أول إطار قانوني شامل لحماية البيانات الشخصية في

[123] **William C. Hannas et al., Chinese Industrial Espionage: Technology Acquisition and Military Modernization (London: Routledge, 2013), 145.**

الصين، حيث يفرض قيودًا صارمة على جمع ومعالجة وتخزين البيانات الفردية، مع إلزام الفاعلين الرقميين باحترام مبدأ الحد الأدنى والشفافية في معالجة البيانات.

تتميز هذه المنظومة التشريعية بعدد من السمات الصارمة التي تؤكد مركزية الدولة في ضبط المجال الرقمي، من بينها:

الإلزام المحلي لتخزين البيانات (Data Localization): تُلزم القوانين الجهات الفاعلة الرقمية، لا سيما الشركات الأجنبية، بتخزين البيانات داخل الحدود الصينية.

تقييد نقل البيانات عبر الحدود: يُحظر تصدير البيانات ذات الحساسية الوطنية إلا وفقا لآليات مراجعة أمنية تُقرّها الدولة.

إخضاع الكيانات الأجنبية للفحص الأمني المسبق: ولا سيما تلك العاملة في القطاعات التقنية أو التعليمية، بما يعكس القلق المتزايد من النفوذ الأجنبي في البنية التحتية الرقمية[124].

اعتبار البيانات موردا استراتيجيا: يعامل القانون البيانات على أنها مكون حيوي للأمن القومي، بما في ذلك البيانات التجارية والأكاديمية، كما يتضح من حالات مثل تغريم شركة **DiDi** [125] الصينية بسبب خروقات تتعلق بنقل البيانات، أو فرض مراجعة شاملة على منصة **CNKI** [126] الأكاديمية.

---

[124] **Samantha Hoffman and Peter Mattis, "Managing the Power Within: China's Cybersecurity Law and the Organizational Logic of Authoritarian Control," War on the Rocks, July 18, 2016, https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission.**

[125] **شركة:DiDi (滴滴出行 – DiDi Chuxing)**

هي شركة صينية رائدة في خدمات النقل الذكي تشبهUber ، توفر خدمات حجز السيارات والتوصيل عبر تطبيقات الهاتف. في عام 2021، واجهت DiDi إجراءات رقابية صارمة من قبل إدارة الفضاء السيبراني في الصين (CAC) بعد طرحها في بورصة نيويورك، وذلك بسبب مخاوف تتعلق بنقل بيانات المستخدمين الحساسة إلى الخارج دون إذن، وهو ما اعتُبر انتهاكًا لقوانين الأمن السيبراني والبيانات. وقد أُجبرت الشركة على سحب تطبيقها من المتاجر الإلكترونية، وتعرضت لغرامة تجاوزت 1.2 مليار دولار في 2022، في واحدة من أقوى الرسائل السياسية تجاه شركات التكنولوجيا الكبرى في الصين.

[126] **منصة:CNKI (China National Knowledge Infrastructure)**

تُعد أكبر قاعدة بيانات رقمية أكاديمية في الصين، وتوفر ملايين المقالات والرسائل الجامعية والكتب الإلكترونية. في عام 2022، خضعت CNKI لتحقيقات من قبل الهيئة الصينية لضبط السوق، بسبب احتكارها لسوق المحتوى الأكاديمي، وفرضها أسعارًا مرتفعة، بالإضافة إلى مخاوف تتعلق بعدم امتثالها الكامل لقوانين حماية البيانات. وقد فُرضت عليها مراجعة شاملة شملت بنيتها التحتية للبيانات وسياستها في مشاركة المحتوى العلمي، في إطار تعزيز الدولة لرقابتها على القطاع المعرفي والبحثي.

تجسد هذه القوانين الثلاثة توجها واضحا نحو سيطرة تنظيمية مشددة، تمنح السلطات أدوات قانونية قوية لضبط التدفقات الرقمية والتحكم في الشركات العاملة ضمن الاقتصاد الرقمي، في إطار رؤية سيادية تعتبر البيانات سلعة استراتيجية في خدمة الأمن القومي والسيادة المعلوماتية.

الفرع الرابع: التمكين التكنولوجي والاقتصادي.

ترتبط القوة السيبرانية الصينية بالنهضة التكنولوجية الجارية، حيث تعتمد بكين على تقنيات الجيل الخامس(5G) ، الذكاء الاصطناعي، الحوسبة الكمومية[127]، والأقمار الصناعية في دعم:

تطوير أنظمة الهجوم والدفاع السيبراني.

تأمين شبكات الاتصالات المحلية.

دعم النفوذ الجيوسياسي عبر مشاريع مثل "طريق الحرير الرقمي."

ورغم هذا، لا تزال الصين تعتمد جزئيًا على الرقائق الدقيقة والتقنيات الأمريكية، ما يجعل الأمن السيبراني مرتبطًا بتحقيق الاكتفاء الذاتي التكنولوجي.

الفرع الخامس: الريادة السيبرانية على الساحة الدولية.

تولي الصين أهمية استراتيجية متزايدة لتعزيز حضورها وتأثيرها في صياغة المعايير والممارسات العالمية في مجال الأمن السيبراني. ويعكس هذا التوجه رغبة بكين في الانتقال من موقع التلقي والانضباط للمعايير الغربية إلى موقع الفاعل المعياري(Norm-maker) ، خصوصا في ظل التنافس التكنولوجي الحاد مع الولايات المتحدة. ولهذا الغرض، تعتمد الصين مقاربة متعددة الأبعاد تشمل:

[127] • Elsa B. Kania and John K. Costello, "Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership," Center for a New American Security (CNAS), September 2018, https://www.cnas.org/publications/reports/quantum-hegemony.

ترسيخ مبدأ "السيادة السيبرانية" كإطار مرجعي عالمي، وذلك من خلال الدفاع عنه في المحافل متعددة الأطراف مثل الأمم المتحدة، ومنظمة التعاون الرقمي، والمنتديات المرتبطة بمجموعة البريكس. تسعى الصين إلى تقنين هذا المفهوم باعتباره حقًا سياديًا للدول في تنظيم فضائها الرقمي الداخلي بعيدًا عن تدخلات خارجية.

توسيع شبكة التحالفات السيبرانية، لا سيما عبر التعاون مع روسيا ومنظمة شنغهاي للتعاون، في محاولة لتشكيل تكتل مضاد للهيمنة الغربية على البنية التحتية والحوكمة الرقمية، وتقديم نموذج بديل ذي طابع مركزي وسلطوي في إدارة الفضاء الرقمي.

التأثير في المفاوضات الدولية بشأن حوكمة الفضاء السيبراني، من خلال دعم مقاربات ترفض "الإنترنت المفتوح" وتفضل تنظيما محليا للمحتوى والمعلومات، بما يعكس الرؤية الصينية للأمن الرقمي كامتداد مباشر للأمن القومي والسيادة السياسية.

نقل البنية التحتية الرقمية الصينية إلى الدول النامية، خاصة عبر مشاريع "طريق الحرير الرقمي"، ما يتيح لبكين تصدير نموذجها الرقمي وتوسيع مجالها الحيوي السيبراني، وذلك عبر توفير معدات الاتصالات، وشبكات الجيل الخامس، وأنظمة الرقابة والتحليل البياني[128].

إن هذه الدينامية الدولية تشير إلى أن القدرات السيبرانية الصينية لم تعد محصورة في بعدها الدفاعي أو الداخلي، بل أضحت أداة جيواستراتيجية تسعى عبرها الصين إلى إعادة تشكيل النظام السيبراني العالمي وفقا لأولوياتها السيادية. ويبدو الأمن السيبراني في هذا السياق ليس مجرد بنية تقنية، بل أداة قوة ناعمة وصلبة في آن واحد، توظف لضمان التفوق السياسي والاقتصادي، ولفرض نموذج صيني بديل في حوكمة الفضاء الرقمي العالمي.

[128] James A. Lewis, "China's Cyber Power in a New Era," Center for Strategic and International Studies (CSIS), October 2020, https://www.csis.org/james-lewis-publications.

المبحث الثالث: استراتيجية روسيا في الفضاء السيبراني والمواجهة المعلوماتية.

المطلب الأول: الأسس المفاهيمية والعقائدية للمواجهة المعلوماتية الروسية.

تقدم روسيا نموذجا مغايرا للفهم الغربي للفضاء السيبراني، حيث لا ينظر إليه كأداة تقنية فحسب، بل كمجال استراتيجي متكامل ضمن ما يُعرف بـ"المواجهة المعلوماتية". يهدف هذا المفهوم إلى تحقيق السيطرة الشاملة على المجال المعلوماتي، بما في ذلك البنية التحتية، المحتوى، والإدراك الجماعي.

الفرع الاول: مفهوم "المواجهة المعلوماتية".

تعرف روسيا الفضاء السيبراني كجزء من إطار أوسع يسمى "المواجهة المعلوماتية " (Информационное противоборство)، وهو صراع استراتيجي دائم يستهدف التأثير على الإدراك الجماعي وصياغة السرديات. حيث تركّز روسيا على العمليات النفسية والإعلامية إلى جانب العمليات التقنية ما يجعل الهدف الأساسي هو التأثير في "عقول الناس" لا فقط الأنظمة. و يتجاوز مفهوم الفضاء المعلوماتي البنية التقنية ليشمل جميع وسائط إنتاج وتداول المعلومات، والمجال النفسي للمجتمع.

الفرع الثاني: الأمن المعلوماتي والسيادة الرقمية.

تعد روسيا من الدول الرائدة في تبني مفهوم الأمن المعلوماتي (Information Security)بمنظور شامل يتجاوز المعنى التقني الضيق يشمل أبعادا معرفية واجتماعية إلى جانب الأبعاد التقنية، في إطار رؤية استراتيجية تهدف إلى حماية الفضاء السيبراني الروسي من التهديدات الداخلية والخارجية. ويندرج هذا التوجه ضمن ما يعرف بمفهوم "السيادة الرقمية"، أي قدرة الدولة على التحكم الكامل في تدفق المعلومات والبيانات داخل حدودها السيادية، سواء من حيث البنية التحتية أو المحتوى أو مصادر التأثير الخارجي.

الأمن المعلوماتي في السياق الروسي لا يقتصر على حماية الأنظمة من الهجمات السيبرانية، بل يمتد ليشمل حماية الوعي العام، ومراقبة الخطاب الإعلامي، ومنع الحروب المعلوماتية التي قد تستهدف استقرار الدولة أو تماسكها الاجتماعي. ولهذا تعتبر روسيا أن نشر الأفكار الموجهة أو التأثير الأجنبي في الرأي العام يشكل تهديدا للأمن القومي لا يقل خطورة عن الهجمات التقنية[129].

في هذا السياق، قامت روسيا بتطوير إطار قانوني متكامل يدعم هذا التوجه، وأبرز ما فيه:

1 قانون "الإنترنت السيادي(2019) ":

يتيح هذا القانون للسلطات الروسية فصل البلاد تقنيا عن شبكة الإنترنت العالمية (Global Internet) في حال حدوث تهديد خارجي، عبر إنشاء بنية تحتية بديلة تُعرف باسم RuNet. كما يفرض القانون على مزودي خدمات الإنترنت تركيب أجهزة تسمح للهيئات الرقابية بتصفية وتوجيه حركة المرور المحلي داخليا، وهو ما يُمكّن الدولة من التحكم الكلي في تدفق المعلومات[130].

2 نظام:SORM (System for Operative Investigative Activities)

وهو نظام رقابة متقدم يُفرض على جميع شركات الاتصالات، يتيح لأجهزة الأمن الروسية مثل FSB[131] مراقبة المكالمات، الرسائل النصية، والبيانات الرقمية دون الحاجة لأمر قضائي مباشر.

[129] Giles, Keir. Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. London: Chatham House, 2016. https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf

[130] Internet Society. "Russia's Sovereign Internet Law." Internet Society. Last modified 2019. https://www.internetsociety.org/resources/internet-fragmentation/russias-sovereign-internet-law/?utm_source=chatgpt.com.

[131] FSB: اختصار لـ Federal'naya Sluzhba Bezopasnosti، أي "جهاز الأمن الفيدرالي الروسي"، وهو الوريث الرئيسي للـ KGBالسوفيتي، ويُعد أبرز جهاز استخبارات داخلية في روسيا، مسؤول عن الأمن الداخلي، ومكافحة التجسس، والرقابة السيبرانية.

ويمثل SORM أحد أركان المراقبة الجماعية التي تعزز من قدرة الدولة على تتبع ومراقبة المواطنين والجهات الفاعلة داخل الفضاء الرقمي[132].

3الإنترنت الروسي البديلRuNet :

تسعى روسيا من خلال مشروع RuNetإلى إنشاء شبكة إنترنت داخلية مغلقة، تشبه في فلسفتها مشروع "الجدار الناري العظيم" الصيني(Great Firewall) ، حيث تهدف إلى:

حماية البنية التحتية الوطنية من الهجمات السيبرانية.

ضمان الاستقلال الرقمي من التأثيرات الغربية، خصوصًا الأمريكية.

التحكم في المعلومات المتداولة داخل البلاد، وتقليص الاعتماد على خوادم وشركات أجنبية[133].

هذا التوجه يعبر عن تحول جوهري في مفهوم الأمن السيبراني حيث أصبح ينظر إليه باعتباره ركيزة للسيادة الوطنية .لكنه يثير في الوقت ذاته إشكاليات تتعلق بحرية التعبير، وحقوق الخصوصية، ومخاوف من تحول الإنترنت الروسي إلى نظام مغلق يعزز من الرقابة المركزية ويقيد الحريات الرقمية.

الفرع الثالث: العقيدة الروسية في العمليات السيبرانية والمعلوماتية.

تظهر العقيدة الروسية تطورا نوعيا في إدراك الأبعاد الجديدة للصراع، حيث لم تعد الحروب تخاض فقط عبر الجيوش التقليدية، بل أصبحت تخاض أيضا في ميادين غير مرئية، أبرزها الفضاء السيبراني والمعلوماتي .وضمن هذا الإطار، لا تفصل روسيا بين العمليات السيبرانية والعمليات الإعلامية والنفسية، بل تدمج جميعها ضمن ما تسميه "عمليات التأثير الشامل."

[132] Piscium. "SORM: The Digital Surveillance Network and Its Global Impact." Piscium, April 1, 2025. https://www.piscium.net/2025/04/01/sorm-the-digital-surveillance-network-and-its-global-impact-2/?utm_source=chatgpt.com.

[133] Atlantic Council. "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior." Atlantic Council. Accessed June 7, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/

1.العمليات السيبرانية كأداة تأثير استراتيجي

وفقا للعقيدة الروسية، تعتبر العمليات السيبرانية جزءا من مجموعة أدوات الحرب النفسية والمعلوماتية، وتشمل:

الهجمات السيبرانية على البنية التحتية الحيوية للعدو (بنوك، شبكات طاقة، إعلام...).

التجسس الإلكتروني على المؤسسات الحكومية والعسكرية والاقتصادية.

التضليل المعلوماتي(Disinformation) ، ويشمل نشر محتوى زائف أو مشوه لتوجيه الرأي العام أو خلق الفوضى.

زرع الانقسام الاجتماعي والسياسي في الدول المستهدفة (كما اتهمت روسيا به خلال الانتخابات الأمريكية 2016).

الحرب النفسية من خلال بث محتوى يثير القلق أو عدم الثقة بالسلطات[134].

بهذا، تتحول العمليات السيبرانية من مجرد أداة هجومية تقنية إلى وسيلة سيادية لبسط النفوذ السياسي والإعلامي عالميا.

2.المرجعيات العقائدية: الأمن المعلوماتي والعقيدة العسكرية

المنظور الروسي مؤطر قانونيا وعقائديا عبر وثيقتين مركزيتين:

أ/عقيدة الأمن المعلوماتي:(2016)

صدرت عقيدة الأمن المعلوماتي الجديدة للاتحاد الروسي بموجب مرسوم رئاسي وقّعه الرئيس فلاديمير بوتين في 5 ديسمبر 2016، كوثيقة استراتيجية تحدد الإطار المفاهيمي والعملياتي

[134] **Reiber, Jonathan, and Nora Bensahel. "Russia's Shadow War Against the West."** ***Center for Strategic and International Studies (CSIS),*** **June 2025. https://www.csis.org/analysis/russias-shadow-war-against-west.**

للأمن المعلوماتي في روسيا، وتعد تحديثا لنسخة عام 2000، بما يتلاءم مع طبيعة التهديدات المتصاعدة في البيئة الرقمية الدولية[135].

السمات الرئيسة للعقيدة:

التوسيع المفاهيمي للأمن المعلوماتي: لا يقتصر الأمن المعلوماتي، وفق العقيدة، على حماية البنية التحتية المعلوماتية من الهجمات السيبرانية، بل يشمل كذلك:

حماية المجال المعرفي والسيكولوجي.

منع التأثيرات الخارجية في الرأي العام الروسي.

ضمان سيادة الدولة على تدفق المعلومات داخل الحدود الوطنية.

المعلومات كسلاح: تقر الوثيقة أن المعلومات تستخدم من قبل أطراف خارجية كأداة لتهديد السيادة الوطنية، عبر:

بث الفوضى المعلوماتية.

زرع مفاهيم معادية داخل المجتمع الروسي.

التحريض على تغيير الأنظمة السياسية.

التهديدات المحددة: تتهم العقيدة بعض الدول الغربية، خاصة الولايات المتحدة، بـ:

السعي للهيمنة على الفضاء المعلوماتي العالمي.

التدخل في الشؤون الداخلية لدول أخرى عبر أدوات إعلامية وتكنولوجية.

استخدام المنظمات غير الحكومية والتقنيات الرقمية لتقويض استقرار الدول.

---

[135] **Wilde, Gavin, and Justin Sherman. "No Water's Edge: Russia's Information War and Regime Security." Carnegie Endowment for International Peace, January 2023. https://carnegieendowment.org/research/2023/01/no-waters-edge-russias-information-war-and-regime-security?utm**

أولويات الرد:

تطوير بنية تحتية رقمية مستقلة مثل RuNet .

السيطرة على وسائل الإعلام وشبكات التواصل.

تعزيز التعليم والتوجيه الإعلامي لحماية "الوعي الوطني." [136]

ب/العقيدة العسكرية الروسية (2014):

نشرت العقيدة العسكرية الرسمية لروسيا في ديسمبر 2014، وتم تعزيز مضامينها عبر تحديثات متتالية أبرزها في 2016، لتؤكد على دمج الفضاء السيبراني والإعلامي ضمن أدوات الحرب الحديثة[137]، مما يعكس تحولا نحو مفهوم "الحرب الهجينة" التي تجمع بين التقليدي وغير التقليدي، و أبرز توجيهاتها:

الفضاء السيبراني كساحة معركة: تصنف الهجمات على البنية المعلوماتية كأعمال عدائية قد تستوجب ردا عسكريا، كما تقر العقيدة أن الفضاء السيبراني بات:

مسرحا للعمليات العسكرية الوقائية.

وسيلة لتحقيق الردع المعلوماتي.

أداة لاختراق الإرادة السياسية للخصوم.

استخدام الوسائل غير العسكرية: تشدد الوثيقة على أن الصراعات المعاصرة قد تحسم دون قتال فعلي، بل عبر:

التأثير الإعلامي والنفسي.

---

[136] RT Arabic. "بوتين يصدق على العقيدة الجديدة لأمن المعلومات في روسيا." **RT Arabic**, December 6, 2016. https://arabic.rt.com/news/853042-بوتين-يصدق-العقيدة-أمن-المعلومات/.

[137] Dalsjö, Robert. "Russia's Hybrid War Against the West." **NATO Review**, April 26, 2024. https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html?utm

الحرب القانونية والمعلوماتية.

الهجمات السيبرانية الوقائية.

الربط بالعقيدة الأمنية والسياسية: تمثل العقيدة العسكرية الروسية امتدادًا لمبادئ الأمن المعلوماتي، حيث تعتبر الدفاع عن السيادة الرقمية جزءًا لا يتجزأ من الردع الاستراتيجي الشامل.

الردع المعرفي والإعلامي:

يتمثل في صياغة روايات استراتيجية.

نشر إعلام موجّه عالميا) عبر قنوات مثل RT و .(Sputnik

الاستثمار في "التحكم الانعكاسي" للتأثير على قرارات الخصم[138].

3.رؤية بوتين: المواجهة المعلوماتية كمعركة دائمة.

يجسد الرئيس الروسي فلاديمير بوتين هذا التوجه في خطاباته، حيث يعتبر أن العالم اليوم يعيش حالة "حرب معلوماتية مستمرة"، لا تتوقف، ولا تقاس بالنصر التقليدي، بل بتوازن القوى في مجال التأثير. وفي هذا السياق:

يفضل الكرملين الوسائل غير العسكرية (Soft Power)مثل الإعلام الخارجي، المنصات الرقمية، والهجمات السيبرانية الخفية.

يعتبر التحكم في المعلومات ونشر الرواية الروسية عالميا ركيزة في مواجهة النفوذ الغربي.

يعتمد على مؤسسات مثل RTو Sputnikكأذرع إعلامية تخدم أهداف العمليات المعلوماتية الموجهة للخارج.

[138] RAND Corporation. “Russia’s New Military Doctrine: Same as the Old Doctrine, Mostly.” RAND Commentary, January 2015. https://www.rand.org/commentary/2015/01/russias-new-military-doctrine.html.

تظهر العقيدة الروسية أن الفضاء السيبراني لم يعد مجالا تقنيا فقط، بل أداة جيواستراتيجية تستخدم للتأثير، الردع، وفرض الإرادة السياسية دون اللجوء إلى الحرب التقليدية. وهذا يعيد تعريف مفاهيم الصراع والسيادة في العصر الرقمي.

الفرع الرابع: جذور المفهوم الروسي للتهديدات

إن فهم السياسات الروسية في المجال السيبراني والمعلوماتي لا يكتمل دون العودة إلى الخلفية التاريخية والسيكولوجية التي تشكل تصورها للتهديدات. فروسيا كقوة عظمى لها إرث تاريخي معقد، ترى نفسها دائما محاطة بأعداء محتملين، ما خلق لديها عقيدة تقوم على الاستباق والسيطرة، لا الدفاع فقط[139].

1.الإرث التاريخي: من الغزوات إلى استراتيجية القلعة المحاصرة.

شهدت روسيا على مر تاريخها غزوات متكررة من الغرب والشرق (مثل غزوات نابليون، وهتلر، والمغول)، وهو ما ولد لديها شعورا عميقا بالهشاشة الجيوسياسية .هذه التجارب التاريخية زرعت في الوعي الاستراتيجي الروسي فكرة محورية: "**إن الأمن القومي لا يتحقق برد الفعل، بل بالفعل الوقائي، والسيطرة على نقاط النفوذ المحيطة**[140]".

وبالتالي، فإن روسيا ترى في المجال الحيوي الخارجي(Near Abroad) ، أي دول الاتحاد السوفيتي السابق، (منطقة أمن قومي ممتد) يجب أن تبقى تحت تأثيرها السياسي والمعلوماتي والاقتصادي.

2.توسيع النفوذ لا الدفاع التقليدي.

[139] Hakala, Janne, and Jazlyn Melnychuk. Russia's Strategy in Cyberspace. Edited by Sanda Svetoka. Designed by Kārlis Ulmanis. Riga: NATO Strategic Communications Centre of Excellence, 2020. ISBN: 978-9934-564-90-1.

[140] **Ibid**

على عكس المفهوم الغربي الذي غالبا ما يربط الأمن بالدفاع والردع، يرى صناع القرار في موسكو أن الوقوف على الحدود وانتظار التهديد هو انتحار سياسي واستراتيجي .ولهذا تعتمد روسيا على:

الهجوم السيبراني والإعلامي الاستباقي لتقويض خصومها من الداخل.

التدخلات الناعمة (Soft Interventions)عبر الإعلام، والأحزاب، والشبكات الدينية والثقافية.

إضعاف الخصم داخليا بدلا من مواجهته عسكريا خارجيا.

3.الرؤية الروسية للثورات الملونة والربيع العربي.

تفسر روسيا التحركات الشعبية التي شهدتها دول مثل جورجيا (2003)، أوكرانيا (2004 و2014)، وتونس ومصر وسوريا في موجات "الربيع العربي" على أنها هندسة غربية لانقلابات ناعمة، وليست تعبيرا ذاتيا عن إرادة الشعوب. من منظور الكرملين:

تستخدم الأدوات المعلوماتية مثل وسائل التواصل الاجتماعي، والمنظمات غير الحكومية (المدعومة من الغرب) كوسائل لإشعال الاحتجاجات.

توظف الحرب النفسية من خلال تصوير الأنظمة على أنها قمعية لإثارة الرأي العام.

الهدف هو زعزعة الأنظمة القريبة من روسيا وخلق أنظمة موالية للغرب.

ومن هنا، تعززت لدى موسكو قناعة استراتيجية بأن حماية الداخل تتطلب ضبط الخارج،[141] ليس فقط عبر النفوذ السياسي، بل أيضا عبر الهيمنة المعلوماتية والسيبرانية.

جذور المفهوم الروسي للتهديدات ليست وليدة العصر الرقمي فقط، بل هي امتداد لعقيدة استراتيجية تاريخية ترى في كل اضطراب قريب تهديدا مباشرا. وهذا ما يفسر توجه روسيا نحو

[141] **Ibid**

تبني سياسات هجومية في الفضاء السيبراني والإعلامي، وإعادة تعريف مفاهيم الأمن القومي والسيادة.

الفرع الخامس: المبادئ التطبيقية للمواجهة المعلوماتية.

تعتمد روسيا في تنفيذ استراتيجياتها السيبرانية والإعلامية على منظومة متكاملة من المبادئ العملياتية المستندة إلى مفاهيم عسكرية واستخباراتية راسخة، طورتها منذ العهد السوفيتي، ثم أعادت تكييفها في العصر الرقمي. هذه المبادئ لا تستهدف فقط التشويش أو التعطيل، بل إعادة تشكيل الواقع السياسي والإعلامي داخل الدول المستهدفة[142].

1.الإجراءات النشطة(Active Measures) .

وهو مصطلح يعود إلى أجهزة الاستخبارات السوفيتية(KGB) ، ويشير إلى مجموعة من العمليات غير المباشرة والخفية التي تهدف إلى:

التأثير على السياسات العامة في الدول المعادية لروسيا.

زرع الانقسامات الداخلية عبر دعم جماعات متطرفة أو معارضة.

اختراق المشهد الإعلامي والسياسي باستخدام عملاء، صحفيين، أو حتى مؤثرين على شبكات التواصل[143].

في السياق المعاصر، تشمل "الإجراءات النشطة" أيضًا:

التلاعب بالانتخابات عبر التضليل السيبراني (كما حدث في الولايات المتحدة عام 2016).

اختراق المنصات الرقمية لنشر محتوى زائف (Fake News) أو مسيس.

2.التحكم الانعكاسي(Reflexive Control) .

[142] Lauder M.A (2019), Gunshots by computers, p. 16.; Meakins J. (2018). Living in (Digital) Denial: Russia's Approach to Cyber Deterrence, European Leadership Network.
[143] Ibid

يعد من أكثر المفاهيم تعقيدا في العقيدة الروسية، حيث يقوم هذا المبدأ على التأثير غير المباشر في عملية صنع القرار لدى العدو، من خلال:

تغذية الخصم بمعلومات مضللة أو انتقائية تُدخله في حسابات خاطئة.

دفعه لاتخاذ قرارات يظن أنها تصب في مصلحته، بينما هي في الحقيقة تخدم المصالح الروسية.

مثال تطبيقي: قد تستخدم روسيا معلومات استخباراتية مسربة بعناية لإقناع خصمها أن هجوما وشيكا سيحدث من اتجاه معين، مما يدفعه لنقل قواته إلى موقع خاطئ، ثم تفاجئه من جهة أخرى[144].

3.التمويه والخداع(Maskirovka) .

هذا المبدأ عسكري في الأصل، ويعني "التمويه"، لكنه تطور ليشمل الحرب المعلوماتية، وهو قائم على:

خلق ضبابية إعلامية وتشويش في السرديات.

نشر روايات متضاربة لإضعاف ثقة الجمهور بمصادر المعلومات.

تضخيم أحداث أو تقزيمها حسب الأجندة الروسية، ما يؤدي إلى تآكل الإدراك الجمعي للحقيقة.

في الفضاء الرقمي، يطبق هذا من خلال:

شبكات الحسابات الزائفة (bots & trolls) التي تنشر محتوى متضاربا[145].

تصميم حملات تشويه السمعة ضد سياسيين أو مؤسسات إعلامية.

[144] lbid
[145] lbid

تُظهر هذه المبادئ التطبيقية أن روسيا لا تخوض "حرب معلوماتية" فقط، بل تمارس هندسة شاملة للإدراك السياسي والاجتماعي لدى خصومها. فالمعركة بالنسبة لها لا تقتصر على تدمير البنية التحتية أو اختراق الأنظمة، بل تشكيل بيئة القرار داخل عقل العدو.

الفرع السادس: الردع الاستراتيجي في العقيدة الروسية.

يعيد المفهوم الروسي للردع الاستراتيجي تعريف هذا المصطلح التقليدي، الذي كان مرتبطا تاريخيا بالسلاح النووي كأداة لردع العدو عن شن هجوم مباشر. في المقابل تعتمد العقيدة الروسية الحالية مقاربة موسعة ومتعددة الأبعاد تجعل من الأدوات المعلوماتية والسيبرانية جزءا محوريا في منظومة الردع الشامل.

1.ردع دون صواريخ: أدوات معلوماتية كبدائل استراتيجية

ترى روسيا أن الصراعات الحديثة لا تخاض فقط في ميادين القتال بل في ميادين المعلومات. لذلك يشمل ردعها الاستراتيجي:

التدخل الإعلامي والسيبراني لإرباك الأنظمة السياسية في الدول الخصمة.

التضليل واسع النطاق لإضعاف ثقة الشعوب بحكوماتها.

خلق واقع إعلامي موازي يجعل من الصعب اتخاذ قرارات موحدة في المجتمعات الديمقراطية.

بهذا، يصبح الردع غير عسكري، لكنه بنفس الفعالية في تحقيق الأهداف الجيوسياسية، دون إطلاق رصاصة واحدة[146].

2.نماذج تطبيقية: من أوكرانيا إلى واشنطن.

[146] **Mey, Holger. *Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to Deterrence*. Security Insights Paper. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, June 2023.**

ضم شبه جزيرة القرم:(2014) سبق الضم هجوم إعلامي منظم لتشكيل رأي عام محلي ودولي مهيأ لتقبل التدخل الروسي. كما استُخدمت أدوات سيبرانية لإرباك الاتصالات والمعلومات داخل أوكرانيا.

التدخل في الانتخابات الأمريكية:(2016) يعد مثالا بارزا على "الردع المعلوماتي الهجومي"، حيث استخدمت روسيا حملات رقمية، حسابات زائفة، وتسريب معلومات لخلق انقسام سياسي داخلي، وتثبيط الثقة بالعملية الديمقراطية.

3.الردع عبر السيطرة على المعرفة والسرد.

الردع الروسي لا يهدف فقط لمنع العدو من الهجوم، بل لشل قدرته على الفعل السياسي أو الاستراتيجي، وذلك عبر:

صياغة السرديات:(Narrative Framing) تتحكم روسيا في كيفية تفسير الأحداث، سواء عبر منصاتها الإعلامية مثل RT، أو عبر دعم روايات بديلة في الدول المستهدفة.

التأثير على البنى التحتية المعرفية: مثل منصات التواصل، الصحافة الرقمية، أنظمة التعليم، بما يؤدي إلى تآكل الحقيقة وخلق ما يُعرف بـ"ما بعد الحقيقة(Post-Truth)."[147]

زعزعة استقرار الأنظمة الديمقراطية: من خلال تضخيم الانقسامات العرقية، الدينية، أو السياسية، بما يخلق بيئة داخلية متوترة تُضعف القرار الخارجي.

في العقيدة الروسية، أصبح الردع لا يعتمد على توازن الرعب النووي فقط، بل على توازن التأثير المعلوماتي .أي أن روسيا اليوم تردع خصومها ليس بتهديدهم بالتدمير، بل بتهديدهم بفقدان السيطرة على شعوبهم وروايتهم الداخلية.

المطلب الثاني: البنية القانونية والتنظيمية للفضاء السيبراني الروسي.

[147] **Kofman, Michael. "Russian Deterrence Strategy: The Evolving Concept of Sderzhivanie." Arms Control Today, July 2017. https://www.armscontrol.org/act/2017-07/features/russian-deterrence-strategy-evolving-concept-sderzhivanie.**

تشكل المنظومة القانونية والتنظيمية في روسيا حجر الأساس الذي تستند إليه الدولة في فرض سيادتها الرقمية، وتُعد من بين الأكثر صرامة وتوسعًا على مستوى العالم. لا تقتصر هذه المنظومة على حماية البنية التحتية المعلوماتية، بل تهدف كذلك إلى التحكم في تدفق المعلومات، مراقبة المحتوى، وتنظيم الوصول إلى شبكة الإنترنت بما يخدم المصالح الاستراتيجية الروسية.

الفرع الاول :التشريعات الأساسية.

1.قانون(2012) GosSOPKA

يعتبر هذا القانون اللبنة الأولى في بناء منظومة الأمن المعلوماتي الروسي. ينشئ ما يعرف بـ:

"النظام الوطني للكشف عن الهجمات على موارد المعلومات الحكومية."

يسمح بإنشاء بنية رقابية مركزية لرصد، تحليل، والتفاعل مع التهديدات السيبرانية.

يلزم الهيئات الحكومية بمشاركة البيانات المتعلقة بالحوادث الأمنية مع الجهات المختصة.

هذا النظام يدار غالبا بالتنسيق مع جهاز الأمن الفيدرالي(FSB) ويهدف إلى تعزيز الجاهزية السيبرانية للدولة[148].

2.قانون حماية البنية التحتية الحيوية للمعلومات(2017)

هذا القانون يوسع من الصلاحيات القانونية الممنوحة لـFSB، حيث:

يعطي الجهاز سلطة الرقابة المباشرة على شبكات وأنظمة المعلومات المصنفة كـ"حيوية ("مصارف، طاقة، دفاع، نقل....)

يجبر المؤسسات الحساسة على:

تبني أنظمة دفاع سيبراني متوافقة مع المعايير الحكومية.

[148] **Turovskiy D. Moscow's cyber-defense: How the Russian government plans to protect the country from the coming cyberwar. Meduza, 19 July, 2017**

التصريح بالحوادث الأمنية ومصادرها فورا.

يسمح بفرض غرامات أو عقوبات على المؤسسات غير المتعاونة أو التي تخفي حوادث اختراق[149].

يعد هذا القانون جزءا من محاولة روسيا عزل فضائها السيبراني عن المخاطر الغربية، وتعزيز الاكتفاء التقني الداخلي.

3.قانون ياروفايا(2016)

يعتبر من أكثر القوانين جدلا، إذ يقدم مزيجا من الرقابة الأمنية ومكافحة الإرهاب عبر الإنترنت . ينص القانون على:

إجبار مزودي خدمات الإنترنت والاتصالات على:

تخزين البيانات الوصفية (metadata) لجميع المستخدمين لمدة 3 سنوات.

الاحتفاظ بالمحتوى الكامل للاتصالات (بما في ذلك المكالمات والرسائل) لمدة 6 أشهر.

منح الأجهزة الأمنية حق الوصول الفوري إلى هذه البيانات دون أمر قضائي مسبق.

إلزام الشركات بتوفير مفاتيح فك التشفير (backdoors)للسلطات عند الطلب.

رغم تبرير القانون بـ"مكافحة الإرهاب"، إلا أن العديد من المراقبين يرونه جزءا من سياسة المراقبة الواسعة وقمع حرية التعبير[150].

تمثل هذه القوانين أدوات قانونية قوية تمكّن الدولة من ضبط فضائها الرقمي الداخلي وفق منظور أمني سيادي .فهي لا تستهدف فقط صد الهجمات السيبرانية بل تسعى إلى فرض الانضباط المعلوماتي ومراقبة المجتمع من خلال السيطرة على البيانات، الاتصالات، والمحتوى

[149] Kukkola J., Ristolainen M., Nikkarila J-P (2017). Game Changer: Structural transformation of cyberspace, p.346
[150] Polyakova A and Meserole C. (2019). Exporting Digital Authoritarianism: the Russian and Chinese Models. Brookings Institution

الإعلامي. ومع أن هذه المنظومة تعزز "السيادة الرقمية"، إلا أنها تقابل بانتقادات دولية واسعة حول انتهاك الخصوصية وحرية التعبير.

الفرع الثاني :قوانين داعمة للتحكم بالفضاء المعلوماتي.

إلى جانب التشريعات الأمنية الصريحة، أقرت روسيا مجموعة من القوانين التي تعزز قبضتها التنظيمية على الفضاء السيبراني من زوايا قانونية، إعلامية، وبنيوية، وهو ما يترجم عمليا في تكريس نموذج "الإنترنت السيادي "الذي يخضع لرقابة مركزية ويحد من الانفتاح العالمي. هذه القوانين لا تُصنَّف فقط كأدوات رقابة، بل كجزء من مشروع هندسة الفضاء المعلوماتي ضمن رؤية الأمن القومي الروسي.

1.القائمة السوداء للإنترنت(2012)

أنشأت هذه الآلية من خلال تعديل قانون الإعلام، وتسمح لـ"الهيئة الفيدرالية للرقابة على الاتصالات Roskomnadzor ":

بحظر المواقع الإلكترونية دون إذن قضائي بمجرد اعتبارها تهديدا لـ"الأمن القومي، الأخلاق العامة، أو الأطفال[151]."

يشمل الحظر:

محتوى "متطرف."

مواقع تعليم الانتحار أو المخدرات.

منصات سياسية تصنف على أنها "غير مرغوبة."

[151] **Meduza. "From 'Protecting Children' to 'Discrediting the Army': A Brief History of Roskomnadzor Blacklists." Meduza, November 6, 2022. https://meduza.io/en/feature/2022/11/06/from-protecting-children-to-discrediting-the-army.**

يؤدي ذلك إلى إضفاء طابع بيروقراطي على حرية التعبير الرقمية، ويمنح السلطات سلطة تقديرية واسعة[152].

2.قانون المدونين(2014)

يندرج ضمن استراتيجية روسيا لإخضاع الفواعل الرقمية غير المؤسساتية (المدونين والمؤثرين) للرقابة القانونية. حيث ينص على:

إجبار كل مدون يتجاوز عدد متابعيه 3,000 شخص يوميا على:

التسجيل رسميا لدى السلطات.

الامتثال لقوانين الإعلام.

تحمّل المسؤولية الجنائية عن أي محتوى يعد "مضللا أو متطرفا."

كما يحظر عليهم:

نشر معلومات دون التحقق من صحتها.

استخدام الشبكات لنشر دعايات سياسية غير مرخصة.

هذا القانون يفرغ الإعلام الرقمي من طابعه الحر، ويحوله إلى إعلام خاضع تنظيميا على الطريقة التقليدية.

3.قانون توطين البيانات(2014)

يمثل هذا القانون ركيزة سيادية في البنية التحتية الرقمية، إذ يفرض على الشركات الأجنبية مث:(ل Google، Facebook)، وغيرها

تخزين ومعالجة بيانات المستخدمين الروس داخل الأراضي الروسية.

[152] **Hakala and Melnychuk, Russia's Strategy in Cyberspace, p15-16**

إقامة مراكز بيانات محلية، بما يُمكّن السلطات الروسية من الوصول القانوني المباشر إلى هذه المعلومات.

المخالفون عرضة للحظر والغرامات، كما حدث مع LinkedIn (2016).

هذا التوطين يهدف إلى:

تقليص الاعتماد على البنى التحتية الغربية.

تعزيز سيطرة الدولة على تدفق البيانات وحمايتها من "التجسس الأجنبي."[153]

4.قانون الإنترنت السيادي(2019)

يعتبر حجر الزاوية في مشروع "الإنترنت الروسي المستقل"(RuNet) ، حيث يمنح الدولة:

صلاحية فصل الإنترنت المحلي عن الشبكة العالمية في حالة التهديد أو الطوارئ.

فرض توجيه حركة مرور الإنترنت عبر نقاط تحكم مركزية تحت إشراف Roskomnadzor.

إجبار مزودي الخدمة على تركيب معدات Deep Packet Inspection (DPI) ، ما يسمح بفلترة المحتوى، ورصد الاتصالات بدقة[154].

يعد القانون خطوة استراتيجية باتجاه خلق "إنترنت روسي مغلق "شبيه بالنموذج الصيني، يتيح التحكم الكامل في الاتصال، المحتوى، والمصادر[155].

[153] **Hakala and Melnychuk, Russia's Strategy in Cyberspace, p-16**

[154] **Epifanova, Alena. Deciphering Russia's "Sovereign Internet Law". DGAP Policy Brief, January 2020. https://www.dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf.**

[155] **Human Rights Watch. "Russia: New Law Expands Government Control Online." Human Rights Watch, October 31, 2019. https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online.**

ملخص القوانين الروسية المتعلقة بالإنترنت

السنة	القانون	أبرز الأحكام
2012	القائمة السوداء للإنترنت(139-FZ)	يمنح Roskomnadzor سلطة حظر المواقع دون أمر قضائي؛ يشمل أكثر من 100,000 عنوان IP.
2012	قانون العملاء الأجانب(190-FZ)	إلزام المنظمات غير الحكومية ذات التمويل الأجنبي بالتسجيل كـ"عملاء أجانب."
2014	قانون الروايات التاريخية(128-FZ)	السجن حتى 5 سنوات لنشر معلومات "زائفة" عن دور الاتحاد السوفيتي في الحرب العالمية الثانية.
2014	قانون التدوين(97-FZ)	المدونون الذين يتجاوز عدد زوارهم 3000 يومياً يجب أن يسجلوا ويتحملوا مسؤولية التعليقات.
2014	قانون توطين البيانات(242-FZ)	يُلزم الشركات بتخزين بيانات المواطنين الروس داخل البلاد وإبلاغ السلطات بموقعها.
2014	مرسوم رقم الهاتف للواي فاي(758)	يجب على مستخدمي الواي فاي العام تقديم رقم هاتف؛ شراء شريحة يتطلب جواز سفر.
2016	حزمة قوانين ياروفايا 374-FZ) و375-FZ)	إلزام مزودي خدمات الاتصالات بتخزين المحتوى والبيانات الوصفية وتسليمها لـ FSB دون أمر قضائي.
2017	تنظيم خدمات المراسلة(241-FZ)	يُطلب من مزودي الإنترنت تخزين الرسائل والصور 6 أشهر وتوفير مفاتيح فك التشفير للسلطات.
2017	قانون حظر VPN (276-FZ)	يحظر استخدام خدمات البروكسي والشبكات الخاصة الافتراضية داخل روسيا.

2019	قانون الإنترنت السيادي(FZ-90)	يتطلب تركيب برامج لمراقبة وتوجيه حركة الإنترنت؛ يسمح بعزل الإنترنت الروسي في حال الطوارئ.

تشكل هذه القوانين "حلقات إحكام" متدرجة ومتعددة الأبعاد، تعكس التحول الروسي نحو نموذج "السيادة الرقمية الكاملة ."لكنها في الوقت ذاته ثير مخاوف داخلية ودولية بشأن الرقابة، القمع المعلوماتي، وانتهاك الخصوصية وحرية التعبير.

الفرع الثالث :الجهات الفاعلة الرسمية في الفضاء السيبراني الروسي.

تقوم المنظومة السيبرانية الروسية على تعدد المؤسسات وتوزيع الأدوار بين أجهزة أمنية وعسكرية، يعمل كل منها ضمن مجال اختصاص محدد، لكنه في الوقت نفسه منسق ومترابط لتحقيق الغاية الكبرى :حماية السيادة الرقمية وتنفيذ الاستراتيجية المعلوماتية لروسيا داخليا وخارجيا.

1.جهاز الأمن الفيدرالي(the Federal Security Service FSB)

يعد FSB الوريث المباشر لجهاز الـ KGBالسوفيتي، ويضطلع بمهام الأمن السيبراني الداخلي . تشمل أدواره:

مراقبة الإنترنت الوطني وإدارة أدوات الرقابة مثل .SORM

الإشراف على حماية البنى التحتية الحيوية للمعلومات وفق قانون 2017.

إصدار التعليمات الفنية والتشريعية لمزودي الخدمة وفرض تركيب معدات التفتيش العميق (DPI).

تنفيذ عمليات رصد وتحقيق إلكتروني داخل الأراضي الروسية ضد المعارضين، الإعلام، والمجتمع المدني.

يعمل FSB ضمن الإطار القانوني للقوانين مثل GosSOPKAوقانون ياروفايا، ويمثل ركيزة الأمن الداخلي الرقمي[156].

2.إدارة الاستخبارات العسكرية(GRU)

تُعد GRU الجناح الهجومي والتخريبي للقدرات السيبرانية الروسية، وتُشرف على:

شن الهجمات السيبرانية الهجومية على أهداف أجنبية، مثل شبكات الطاقة، الاتصالات، البنوك، والمؤسسات الحكومية.

تنفيذ عمليات اختراق وتسريب معلومات بهدف زعزعة الاستقرار، كما حدث مع "فرقة Sandworm" و"APT28" المرتبطة بالـGRU.

إدارة عمليات التشويش السيبراني خلال النزاعات العسكرية مثلا في أوكرانيا وسوريا.[157]

تعتبر GRU المحرك الأساسي للهجمات التي يصنفها الغرب ضمن "التهديدات السيبرانية العالمية."

3.جهاز الاستخبارات الخارجية(Foreign Intelligence Service SVR)

يُركّز SVR على العمليات الرقمية السرية طويلة المدى خارج البلاد، ويُعتبر الذراع الاستراتيجية للمراقبة العالمية. مهامه تشمل:

التجسس السيبراني على الحكومات والشركات الأجنبية.

جمع معلومات استخباراتية استراتيجية عبر الإنترنت والشبكات الدبلوماسية.

بناء قواعد بيانات حول النخب، المؤثرين، وصناع القرار في الدول المستهدفة[158].

---

[156] **Connell, Michael, and Sarah Vogler. *Russia's Approach to Cyber Warfare*. Arlington, VA: CNA Analysis & Solutions, September 2016.p07 https://www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf.**

[157] **Lilly, B., and J. Cheravitch. "The Past, Present and Future of Russia's Cyber Strategy and Forces." In *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*, 142–146. Fort Leavenworth, KS: Foreign Military Studies Office, 2019.**

ويعتمد SVR على أساليب خفية أقل وضوحًا منGRU ، موجهة أساسًا لجمع المعلومات أكثر من تدمير الأنظمة.

4.القوات المسلحة الروسية (وزارة الدفاع)

قامت القوات المسلحة الروسية منذ 2013 بتطوير قدراتها السيبرانية ضمن إطار "الحرب الهجينة"، وتشمل:

إنشاء وحدات سيبرانية متخصصة داخل هيكل القيادة العسكرية.

استخدام القدرات السيبرانية في الحروب الحديثة، بالتوازي مع الهجمات العسكرية التقليدية.

تدريب كوادر عسكرية على استخدام تكنولوجيا المعلومات كأسلحة رقمية.

تنسق هذه الوحدات عملياتها غالبا معGRU ، ضمن عقيدة موحدة للردع والهجوم السيبراني.

تظهر هذه البنية المؤسسية أن الفضاء السيبراني في روسيا ليس مجالا مدنيا محضا، بل ساحة تعمل فيها أجهزة الأمن والاستخبارات والجيش بشكل تكاملي ومنسّق .ويمثّل هذا النموذج أحد أكثر أنظمة الأمن السيبراني مركزية وأمنية في العالم.

الفرع الرابع: الجهات الفاعلة غير الرسمية والمدعومة من الدولة .

في إطار العقيدة السيبرانية الروسية لا تقتصر أدوات التنفيذ على المؤسسات الرسمية بل يتم توظيف فاعلين غير رسميين ضمن استراتيجيات الدولة، ما يوفر هامشا من الإنكار الرسمي (Plausible Deniability)ويعقد من جهود التتبع والمحاسبة الدولية. هؤلاء الفاعلون لا يعملون بشكل منفصل، بل ضمن مناخ من الحماية الضمنية والتواطؤ المؤسسي.

1.الهاكرز الوطنيون(Nationalist Hackers)

يمثلون مجموعات غير رسمية من القراصنة الروس ذوي التوجه القومي.

[158] **Connell, Michael, and Sarah Vogler.p7-8**

ينشطون في شن هجمات رقمية على أهداف تعتبرها الدولة "معادية"، مثل:

مؤسسات غربية.

وسائل إعلام معارضة.

منظمات مجتمع مدني أجنبية.

غالبا ما تُظهر الدولة عدم تورطها، لكنها تتغاضى عن ملاحقتهم بل أحيانا تكرمهم علنا.

مثال: مجموعة Killnetالتي استهدفت مواقع أوروبية مؤيدة لأوكرانيا عام 2022[159].

2.القراصنة الإجراميون المدعومون(State–Tolerated Criminal Hackers)

يشكلون فئة من المجموعات الإجرامية السيبرانية التي تعمل لتحقيق أهداف مالية، لكنها في بعض الحالات تُستخدم من قبل الدولة الروسية لشن هجمات مركزة.

يتم توظيفهم في:

الهجمات بالفدية.(Ransomware)

التجسس التجاري.

تخريب البنية التحتية في الدول المعادية.

تقدم الدولة لهم بيئة قانونية آمنة ما داموا لا يهاجمون الداخل الروسي، وهو ما يُسمى أحيانا بـ"التحالف المظلم بين الجريمة والسياسة[160]."

3.وكالة بحوث الإنترنت(IRA – Internet Research Agency)

كيان يدار من سانت بطرسبورغ، ارتبط مباشرة بحملات التدخل في:

[159] **Maurer, Tim. Cyber Mercenaries: The State, Hackers, and Power. Cambridge: Cambridge University Press, 2018, 94–95.**
[160] **Connell, Michael, and Sarah Vogler.p11-10**

الانتخابات الأمريكية.(2016)

استفتاء بريكست.

أزمات أوروبا الشرقية.

تختص بـ: إنشاء حسابات وهمية على وسائل التواصل.

نشر الروايات المؤيدة للكرملين[161].

بث الانقسام في المجتمعات الغربية)عبر قضايا عرقية، سياسية، دينية.(...

تعد IRA نموذجا متطورا من "الجيوش الإلكترونية" التي تحارب بالخطاب، لا بالسلاح.

يعكس الإطار القانوني والمؤسسي الروسي توجها ممنهجا نحو السيطرة الكاملة على الفضاء السيبراني، من خلال:

ترسانة قوانين تنظيمية وأمنية تضمن الرقابة والتحكم بالمحتوى وتخزين البيانات محليا.

جهاز أمني وعسكري متعدد الأذرع يدمج الدفاع بالهجوم، ويستثمر أدوات الحرب الهجينة.

توظيف فاعلين غير رسميين لتنفيذ عمليات هجومية قابلة للإنكار وتخدم مصالح الدولة دون تورط مباشر.

كل هذه العناصر تندرج ضمن رؤية استراتيجية للسيادة الرقمية الروسية، والتي لا تكتفي بحماية الداخل، بل تطمح إلى التأثير، والتفوق المعلوماتي على المستوى الدولي عبر أدوات القوة الناعمة والعمليات غير التقليدية.

[161]**Booth, Robert, Matthew Weaver, Alex Hern et al. "Russia Used Hundreds of Fake Accounts to Tweet about Brexit, Data Shows."** ***The Guardian*****, November 14, 2017.** **https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-brexit-tweets.**

الفصل الثالث : الامن السيبراني الجزائري

المبحث الأول: واقع الأمن السيبراني في الجزائر وتحدياته.

المطلب 1: السياق الدولي والوطني لتنامي التهديدات السيبرانية .

يمكن القول إن تصاعد معدلات التهديدات السيبرانية يرتبط ارتباطا وثيقا بطبيعة البيئة الدولية، الذي يشكل بيئة محفزة لزيادة هذه الهجمات. وقد ساهم انتشار فيروس كورونا على الصعيد العالمي في تسريع وتيرة التحول الرقمي في العديد من المجتمعات[162]، وزيادة الاعتماد على التكنولوجيا في مختلف المجالات. غير أن هذا الاعتماد المتزايد أدى بدوره إلى تصاعد وتيرة الهجمات السيبرانية، لاسيما في ظل التوسع الهائل في استخدام الأجهزة المتصلة بشبكة الإنترنت ضمن إطار "إنترنت الأشياء". وقد زاد هذا التوسع، إلى جانب تنامي الدوافع السياسية والاقتصادية لاستغلال شبكة المعلومات الدولية، لا سيما خلال فترة الجائحة، من مخاطر الأمن السيبراني وارتفاع معدلات الاختراقات والهجمات الرقمية.

وفي ضوء هذه التهديدات المتزايدة، أصبح تحقيق الأمن القومي أولوية قصوى لدى جميع الدول، بغض النظر عن مكانتها في النظام الدولي أو حجم تأثيرها فيه. ففي عالم تتطور فيه التهديدات الأمنية بسرعة فائقة وتتغير باستمرار، لم يعد تبني الدول لاستراتيجيات مرنة ومتكيفة مع هذه المستجدات خيارا، بل ضرورة تفرضها طبيعة العصر الرقمي الحديث.

وإلى جانب التهديدات التقليدية التي تبذل الدول جهودا لمواجهتها من خلال تطوير استراتيجيات وطنية وتفعيل التعاون مع شركاء داخليين وخارجيين، فرضت الثورة الرقمية والمعلوماتية جملة من التهديدات المستحدثة والمعقدة، المتعددة المصادر والأشكال والآثار، مما يتطلب من الدول تعبئة جهود مضاعفة لحماية فضائها الرقمي[163]. ونظرا لاختلاف الفضاء السيبراني عن المجالات التقليدية سواء من حيث خصائصه التقنية أو آليات التفاعل فيه، فإن الدول أصبحت بحاجة ملحة

[162] **World Economic Forum.** ***Global Cybersecurity Outlook 2021*****. Geneva: WEF, 2021, pp. 11–15.**

[163] **قدايفة، أمينة .*إستراتيجية أمن المعلومات: مقاربة نظرية*. جامعة أمحمد بوقرة بومرداس، 2022، ص. 17–20.**

إلى تطوير استراتيجيات دفاعية جديدة، تتسم بالتنوع والابتكار، وتختلف جذريا عن تلك المستخدمة في مواجهة التهديدات الأمنية التقليدية.

ورغم الاهتمام المتزايد بالمسائل المتعلقة بالأمن السيبراني من طرف العديد من الدول، إلا أن أكثر الدول انخراطا في تطوير استراتيجيات فعالة للدفاع الإلكتروني هي تلك التي تعتمد بدرجة كبيرة على الفضاء السيبراني في تسيير شؤونها، مما يجعلها في الوقت ذاته الأكثر عرضة للمخاطر والأكثر حاجة إلى الحماية.

وبشكل عام، تتعدد آليات واستراتيجيات الدفاع السيبراني التي تمكن الدول من حماية بنيتها الإلكترونية ضد الاعتداءات، وتعد الجزائر من بين الدول التي اعتمدت على مقاربة تقوم على تقييم المخاطر وتحديد البرامج والمبادرات اللازمة لمواجهتها، من خلال الجمع بين الاستباقية والوقاية لضمان جاهزية الدولة في حال وقوع اختراقات، أو عمليات تجسس أو تخريب. و منح الفضاء الإلكتروني والمعلوماتي أولوية وطنية، بما يضمن تعزيز الأمن والدفاع السيبرانيين. كذلك الاستثمار في الكفاءات البشرية، من خلال تكوين وتأهيل الأطر المكلفة بحماية الأنظمة الإلكترونية الوطنية. إشراك كافة الفاعلين المعنيين، بمن فيهم القطاع الخاص، مع تعزيز التعاون الدولي لضمان فعالية الجهود المبذولة في مجال الأمن السيبراني. والتحكم في الوصول إلى الأنظمة الإلكترونية، من خلال تقييد قدرة المستخدمين غير المخولين على الولوج إلى هذه الأنظمة. ووضع أنظمة حماية إضافية لحماية البيانات والبرمجيات الحساسة، بالإضافة إلى أنظمة رقابة داخلية لمواجهة التهديدات الداخلية. و إعداد تقارير دورية لتحليل المخاطر الإلكترونية، وتحديد استراتيجيات التعامل مع الكوارث، مع إجراء مراجعات مستمرة لفعالية السياسات الأمنية وتحديثها وفق المستجدات[164].

[164]" واقع وتحديات الأمن السيبراني في الجزائر "،*مجلة الدفاع الوطني*، العدد 45 (2021): ص. 33–36.

المطلب 2: مؤشرات الأداء الوطني في الفضاء السيبراني

بلغ عدد مستخدمي الإنترنت في الجزائر حوالي **33.49مليون مستخدم** مع مطلع عام 2024، أي بنسبة تغطية بلغت **72.9 % من إجمالي السكان**[165].

كما قدر عدد مستخدمي وسائل التواصل الاجتماعي بحوالي **24.85مليون مستخدم**، ما يعادل **54.1 % من السكان** [166]. أما عدد اشتراكات الهاتف المحمول الفعالة، فقد بلغ حوالي **50.65 مليون اشتراك**، أي **110.2 %** من عدد السكان[167]. وقد شهدت الجزائر نموا في عدد مستخدمي الإنترنت بحوالي **488ألف مستخدم جديد** خلال الفترة ما بين يناير 2023 ويناير 2024، بزيادة سنوية قدرها 1.4% +.[168]

بلغ متوسط **سرعة الاتصال بالإنترنت عبر الهاتف المحمول** حوالي **21.36ميغابت/ثانية** في يناير 2024. أما متوسط **سرعة الإنترنت الثابت** فبلغ **12.32ميغابت/ثانية** في نفس الفترة[169].

يقدر عدد سكان الجزائر بحوالي **47.40 مليون نسمة** في منتصف2025،[170] ما يعني أن التغطية الرقمية تمس أغلب شرائح المجتمع. هذا النمو المتواصل في الانتشار الرقمي يعكس حاجة ملحة لتعزيز الأمن السيبراني وضمان حماية البنية التحتية الرقمية من التهديدات الناشئة.

تصنيف الجزائر في مؤشر الأمن السيبراني العالمي(ITU)

[165] DataReportal, Digital 2024: Algeria, January 2024, https://datareportal.com/reports/digital-2024-algeria.
[166] Ibid
[167] Ibid
[168] Ibid
[169] Ookla, Speedtest Global Index: Algeria, accessed June 2025, https://www.speedtest.net/global-index/algeria.
[170] Worldometers, "Algeria Population (2025)," Worldometers, accessed June 9, 2025, https://www.worldometers.info/world-population/algeria-population/.

وفقا لتقرير المؤشر العالمي للأمن السيبراني 2024 – **Global Cybersecurity Index**) (**GCI**الصادر عن الاتحاد الدولي للاتصالات، أدرجت الجزائر ضمن الفئة الثالثة – **Tier 3**) (**Establishing**بحصولها على 65.87 نقطة من أصل 100 . وجاء توزيع أدائها عبر المحاور الخمسة كالآتي:

التدابير القانونية20 / 19.18 :

التدابير التقنية20 / 8.57 :

التدابير التنظيمية20 / 11.02 :

تنمية القدرات20 / 13.91 :

التعاون الدولي[171]20 / 13.19 :

على المستوى القانوني، فقد سجلت الجزائر تنويعات إيجابية من خلال إصدار قوانين حديثة لحماية البيانات وتعزيز العقوبات على الجرائم السيبرانية. ولكن المدخل التقني لا يزال قيد التطوير، ويحتاج إلى استثمارات في بنيات كشف التسلل وفرق استجابة فعالة(CERT/CIRT) . كما أن البعد التنظيمي (حوكمة، تنسيق، إشراف) لا يزال في بداياته ويستلزم إنشاء هيئات مستقلة ذات صلاحيات واضحة. من الناحية البشرية تظهر الجزائر طموحا في تنمية الموارد البشرية عبر برامج تدريبية وتطبيقية. وأخيرا هناك فرصة لتعزيز تعاون أوسع على الصعيد الدولي من خلال الانضمام إلى الاتفاقيات مثل **بودابست** والمشاركة في المبادرات العالمية.

على الرغم من أن تقرير مؤشر الأمن السيبراني العالمي 2024 الصادر عن الاتحاد الدولي للاتصالات يقدم إطارا مرجعيا مفيدا لتقييم مدى جاهزية الدول سيبرانيا، إلا أنه لا يعد مرجعا كافيا أو كاشفا بشكل دقيق عن السياسات الأمنية السيبرانية المطبقة فعليا خصوصا في الدول التي تتبنى مقاربات أمنية غير معلنة أو تقوم بتدابير غير مصرح بها علنا لدواع سيادية. وبالتالي فإن

[171] **International Telecommunication Union (ITU), Global Cybersecurity Index 2024, 5th edition, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (accessed June 9, 2025).**

التقدم نحو الفئة الأولى من التصنيف لا يمكن أن يقاس فقط بمؤشرات تقنية أو تنظيمية ظاهرية، بل يتطلب رؤية وطنية متكاملة تقوم على:

هيكلة الاستراتيجية الوطنية للأمن السيبراني بما يعكس التهديدات الحقيقية وسياق الدولة،

تعزيز البنية التحتية التقنية والحوكمة التنظيمية بآليات أكثر مرونة واستباقية،

إعادة صياغة نهج التعاون الدولي على أساس المصالح السيادية لا مجرد الانخراط الشكلي،

الاستثمار الممنهج في تكوين الموارد البشرية المتخصصة وتطوير أدوات الدفاع السيبراني الوطنية[172].

المطلب الثالث: التحديات البنيوية والتقنية الداخلية والخارجية للأمن السيبراني في الجزائر.

صانع القرار تأكد من ان الحرب الحديثة والتهديدات الناشئة تنبع من الفضاء السيبراني وبالتالي اخذت الدولة على عاتقها استراتجية حينية لمواجهة هذه التهديدات من خلال تبني استراتجية الرقمنة على كل المستويات و تعزيز بنيتها السيبرانية

رغم ما شهدته الجزائر من خطوات أولية في مجال تعزيز أمنها السيبراني، فإن واقع الأداء الوطني يكشف عن وجود تحديات بنيوية وتقنية جوهرية ضرورية لبناء منظومة سيبرانية فعالة وشاملة. فعلى المستوى البنيوي الداخلي، قامة الدولة ببناء و تصليح هشاشة البنية التحتية الرقمية، سواء من حيث قدم التجهيزات أو ضعف شبكات الربط بين المؤسسات، أو غياب منصات رقمية مؤمنة لإدارة البيانات الحساسة.[173] أما النصوص القانونية الناظمة للأمن الرقمي – مثل قانون 09-04

[172] **Ibid.**

[173] **حميدي، حياة، ونسيمة طايلب. .مدخل مفاهيمي حول الأمن السيبراني .مجلة مدار للدراسات الاتصالية الرقمية، العدد 2، نوفمبر2022، جامعة الشلف.ص12-13**

لسنة 2009 – لا تزال دون المستوى المطلوب لمواجهة التهديدات الحديثة كالهجمات على البنى التحتية الحيوية، التجسس السيبراني، وهجمات الابتزاز عبر برمجيات الفدية(Ransomware) .

أما على الصعيد الخارجي، فتبرز تعقيدات البيئة السيبرانية العالمية كعامل مضاعف للمخاطر، حيث يتميز هذا الفضاء بسرعة التغير، وتعدد مصادر التهديد، واستخدام تقنيات متقدمة من قبل المهاجمين، و كحال الجزائر التي بادرت في مواجهة هذه التحديات والمخاطر الناتجة من التهديدات السيبرانية الامر الذي يحتم عليها تطوير منظومة سيبرانية فعالة وناجعةو تطوير آليات للاستجابة. وتعتبر **مشكلة الإسناد (Attribution)** واحدة من أخطر التحديات، إذ يصعب تحديد الجهة الحقيقية المسؤولة عن الهجمات بسبب استخدام تقنيات تمويه متقدمة، مثل الشبكات المظلمة(Darknet) ، البروكسيات المشفرة، وتعدد القفزات الجغرافية للعناوين الرقمية، وهو ما يتطلب تفعيل مبدأ الردع أو المطالبة بالمساءلة الدولية. بناء عليه فإن تجاوز هذه التحديات يقتضي تبني رؤية وطنية شاملة تتقاطع فيها أبعاد التمويل، التشريع، البنية التحتية، والموارد البشرية، مع الانخراط الفعلي في المنظومات الدولية المتخصصة من أجل بناء قدرات سيبرانية ذات طابع وقائي واستباقي فعال[174].

يتضح أن واقع الأمن السيبراني في الجزائر يواجه جملة من التحديات المتداخلة تتراوح بين التحولات السريعة في السياق الدولي والتزايد المطرد للاعتماد على الفضاء الرقمي، وصولا إلى التحديات البنيوية والتقنية والتشريعية على المستوى الوطني. و تتضح الجهود المبذولة لتدارك هذا الوضع من خلال اعتماد مقاربات وقائية، ناهيك أن حجم التهديدات وحساسيتها يتطلب استجابة أكثر شمولا واحترافية تقوم على تعزيز البنية التحتية الرقمية، وتحديث الإطار القانوني باستمرار، وبناء هيئات مستقلة ذات كفاءة، إلى جانب تطوير الكفاءات البشرية المتخصصة. وعليه فإن تعزيز الأمن السيبراني في الجزائر لم يعد مسألة تقنية بحتة، بل أصبح ضرورة استراتيجية تمس ركائز السيادة الوطنية، وتتطلب رؤية استباقية متعددة الأبعاد قادرة على التفاعل بفعالية مع البيئة الرقمية.

[174] **لعور، وهيبة. .الأمن السيبراني في الجزائر: السياسات والمؤسسات .مجلة الفكر الشرطي2022 ، العدد 28، ص. 275–277.**

المبحث الثاني: المنظومة القانونية والمؤسساتية للأمن السيبراني في الجزائر.

المطلب 1: الإطار التشريعي الوطني المنظم للأمن السيبراني.

أعطى المشرع الجزائري تعريفا للأمن السيبراني في الفقرة الثالثة من المادة العاشرة من القانون رقم 18-04 بأنه : "**مجموع الأدوات و السياسات و مفاهيم الأمن و الآليات الأمنية و المبادئ التوجيهية و طرق تسيير المخاطر و الأعمال و التكوين و الممارسات الجيدة و الضمانات و التكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية من أي حدث من شأنه المساس بتوفير و سلامة البايانات المخزنة أو المعالجة أو المرسلة**" .[175]

الفرع الاول:القوانين والتشريعات الأساسية.

1.قانون العقوبات – القانون رقم 04-15(2004)

عدل قانون العقوبات بإضافة قسم خاص تحت عنوان" :المساس بأنظمة المعالجة الآلية للمعطيات."

يتضمن هذا القسم الجرائم المتعلقة بالاختراق والقرصنة والعبث بالمعطيات الإلكترونية.

يشمل المواد من 394 مكرر إلى 394 مكرر 7[176].

2.قانون الإجراءات الجزائية – القانون رقم 06-22(2006)

عدل قانون الإجراءات الجزائية بإدراج إجراءات خاصة للتحقيق في الجرائم الإلكترونية.

---

[175] أنظر المادة 3/10 من القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق لـ 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات الإلكترونية، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 27، بتاريخ 13 مايو 2018، الصفحة 3.

[176] انظر المواد من 394 مكرر إلى 394 مكرر 7 من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الصادر في الجريدة الرسمية للجمهورية الجزائرية، رقم 71، المتضمن تعديل قانون العقوبات لسنة 2004، الصفحتان 11 و12.

أبرزها: اعتراض المراسلات الإلكترونية، التنصت، المراقبة الإلكترونية، جمع الأدلة الرقمية، تحت ضوابط قانونية[177].

3. قانون رقم 09-04(2009)

يتعلق بـالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ينص على تشجيع التعاون الدولي والمساعدة القضائية.

عرف الجريمة السيبرانية بأنها:

"**كل جريمة تُرتكب أو تُسهل عن طريق منظومة معلوماتية أو الاتصالات الإلكترونية**[178]".

4. قانون رقم 18-04(2018)

يحدد القواعد العامة للبريد والاتصالات الإلكترونية.

يساهم في تنظيم وتسيير الأمن السيبراني من زاوية البنية التحتية والتشغيلية[179].

الفرع الثاني:التدابير الإجرائية والتقنية.

1.الإجراءات القانونية الوقائية والردعية:

تجريم أفعال مثل: الاختراق، تعطيل المواقع، سرقة البيانات، إساءة استخدام نظم المعلومات.

2.الإجراءات التقنية:

[177] القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق لـ 20 ديسمبر سنة 2006، المعدّل والمتمم للأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966، والمتضمن قانون الإجراءات الجزائية، الصادر في الجريدة الرسمية للجمهورية الجزائرية، العدد 84، المنشور بتاريخ 24 ديسمبر سنة 2006، الصفحة 4.

[178] أنظر المادة 02 (مكرر أ) من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية للجمهورية الجزائرية، العدد 47، بتاريخ 16 أوت سنة 2009.

[179] قانون رقم 18-04 مؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 27، مؤرخة في 13 ماي 2018، الصفحة 3.

السماح بالتنصت والتسجيل والتصوير في إطار تحقيقات الجرائم الإلكترونية، وفق ضوابط قانونية صارمة.

المطلب 2: التدابير التقنية والإجرائية المصاحبة للتشريعات.

في إطار السعي نحو تفعيل الإطار التشريعي المتعلق بالأمن السيبراني، تبنت الجزائر مجموعة من التدابير التقنية والإجرائية المكملة للنصوص القانونية بهدف تعزيز فعالية الاستجابة الوطنية للتهديدات الرقمية. وتتمثل

الفرع الاول:آليات الوقاية والردع القانونية.

في تجريم طيف واسع من الأفعال المرتبطة بالجريمة السيبرانية، مثل اختراق أنظمة المعالجة الآلية للمعطيات، تعطيل مواقع إلكترونية عمومية أو خاصة، الاستيلاء على بيانات محمية، أو إساءة استخدام نظم المعلومات لأغراض احتيالية أو تخريبية.[180] وقد جاءت هذه التدابير ضمن تعديل قانون العقوبات بموجب القانون 04-15، الذي أدخل قسما خاصا حول "المساس بأنظمة المعالجة الآلية"، وكرس مواد قانونية جزائية (من 394 مكرر إلى 394 مكرر 7) تحدد الأوصاف الجرمية والعقوبات المقررة مما يضفي طابعا ردعيا على السلوكيات المهددة للأمن السيبراني الوطني.

وفي الجانب الإجرائي، نص قانون الإجراءات الجزائية المعدل بموجب القانون 06-22 على **إجراءات تحقيق رقمية متخصصة**، تأخذ بعين الاعتبار خصوصية الجريمة الإلكترونية، سواء من حيث طبيعة الأدلة أو سرعة زوالها. وتشمل هذه الإجراءات الترخيص القانوني بـ**اعتراض المراسلات الإلكترونية، التنصت على الاتصالات الرقمية، المراقبة المستمرة لحركة البيانات، والتصوير أو التسجيل المعلوماتي**،[181] وذلك تحت إشراف السلطة القضائية المختصة، وضمن

---

[180] ياحي، علي. "تطوير المنظومة القضائية والأمنية في الجزائر لمواجهة الجرائم المعلوماتية ".إندبندنت عربية، 7 مارس 2022. تاريخ الاطلاع: 09/جوان2025 https://www.independentarabia.com/node/309351 .

[181] أنظر المادة 18 من المرسوم الرئاسي رقم 19-172 المؤرخ في 25 جوان 2019، المتعلق بإنشاء الوكالة الوطنية للأمن السيبراني وتنظيمها وسيرها، الجريدة الرسمية، العدد 41، ص. 17.

ضوابط صارمة تضمن التوازن بين متطلبات الأمن وحماية الحقوق الأساسية للأفراد، خصوصا الحق في الخصوصية. كما أُقرت إمكانية **اللجوء إلى الوسائل التكنولوجية المتقدمة في التحري وجمع الأدلة**، كتوظيف برامج تتبع النشاط الرقمي، وتحليل البرمجيات الخبيثة، والاستعانة بخبراء في الطب الشرعي الرقمي لتوثيق الانتهاكات المعلوماتية بطريقة مقبولة قضائيًا.

وعليه، فإن هذه التدابير تعد مكملا وظيفيا للتشريع، إذ تضمن قابلية تفعيل القواعد القانونية في الواقع العملي، وتمنح الجهات الأمنية والقضائية الوسائل القانونية والتقنية اللازمة للتدخل الفوري والفعال عند وقوع الجرائم السيبرانية. غير أن فاعلية هذه الإجراءات تظل رهينة بتطوير قدرات الفاعلين في إنفاذ القانون، وتحديث المعدات والتقنيات المستخدمة في التحقيقات الرقمية، إلى جانب ضرورة مراجعة دورية للضوابط القانونية المصاحبة بما يواكب تسارع التطور التكنولوجي وطبيعة التهديدات المستجدة.

الفرع الثاني: الهيئات والهياكل المؤسسية.

1.المؤسسات الأمنية والعدلية المختصة:

تضطلع المؤسسات الأمنية والعدلية بدور محوري في مواجهة الجرائم السيبرانية، نظرا لطبيعتها التنفيذية وتداخل مهامها مع المجال القضائي والتقني. وتعتبر **المصلحة المركزية لمكافحة الجريمة المعلوماتية**، التابعة لمديرية الأمن الوطني أبرز هذه الجهات، إذ أنشئت سنة 2011 وأعيدت هيكلتها عام 2015 لتتكيف مع التطورات المتسارعة في عالم الجريمة الإلكترونية. وتكمن وظيفتها الأساسية في التحقيق والتحري بشأن الجرائم السيبرانية، والتنسيق مع النيابة العامة وخبراء التكنولوجيا في إعداد الملفات التقنية والقضائية ما يجعلها تمثل الدعامة المركزية للشرطة القضائية في هذا المجال.[182] من جهة أخرى يعد **مركز الوقاية من جرائم الإعلام الآلي التابع للدرك الوطني** مؤسسة أمنية تقنية تعنى برصد وتحليل الجرائم الرقمية وتحديد هوية مرتكبيها، وقد أنشئ سنة 2008 كمركز متخصص في دعم التحقيقات السيبرانية، خاصة في التنسيق مع المؤسسات

[182] إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي - تبسة، صـ113.

المالية والمصرفية، مما يعزز من قدراته في مجال مكافحة الجرائم الإلكترونية ذات الطابع الاقتصادي.[183] أما **المعهد الوطني للأدلة الجنائية وعلم الإجرام**، الذي تأسس بموجب مرسوم رئاسي سنة 2004 وبدأ نشاطه الفعلي عام 2009، فهو يتبع لوزارة الدفاع الوطني، ويضم مصالح متخصصة في تحليل الأدلة الرقمية وكشف الاختراقات المعلوماتية، إلى جانب تقديم خدمات الخبرة التقنية للسلطات القضائية.[184] وتستكمل هذه المنظومة بوجود النيابات القضائية المتخصصة التي تتولى معالجة ملفات الجرائم المعلوماتية بالتنسيق المباشر مع الهيئات الأمنية وخبراء الأدلة الرقمية، مما يضمن متابعة قانونية دقيقة ومتماسكة للانتهاكات السيبرانية.

2..الهيئات الإدارية والتنظيمية المستقلة:

تعد **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها** أحد الركائز التنظيمية الأساسية في البنية المؤسسية للأمن السيبراني بالجزائر، حيث أنشئت بموجب المادة 13 من القانون 09-04 المؤرخ في 5 أوت 2009، والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومكافحتها. وقد تم تنظيم مهامها وهيكلتها إجرائيا وفق أحكام المرسوم الرئاسي رقم 261-15، الذي حدد طبيعتها الإدارية باعتبارها هيئة مستقلة تابعة لوزارة العدل وتخضع لإشراف لجنة وزارية عليا يترأسها وزير العدل. تضطلع هذه الهيئة بجملة من المهام الاستراتيجية ذات الطابع التنسيقي والوقائي، من أبرزها اقتراح السياسات الوطنية الخاصة بالوقاية من الجرائم السيبرانية، بما يشمل إعداد التوصيات وتنظيم الخطط التنفيذية التي تعزز من أمن الفضاء الرقمي الوطني. كما تتولى الهيئة تنسيق جهود مكافحة الجرائم الإلكترونية بين مختلف الفاعلين الأمنيين والقضائيين، وتسهم في دعم الشرطة والنيابة العامة عبر تقديم المعلومات الفنية والخبرات التحليلية، خاصة في الجرائم المعقدة التي تتطلب فهما دقيقا للبنية التقنية للأنظمة المعلوماتية.[185] وإضافة إلى ذلك، تضطلع الهيئة بدور استباقي في مراقبة الاتصالات الإلكترونية

---

[183] المرجع نفسه، صـ 114.

[184] أمسهان بوضياف، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مج. 3، ع. 3 (2018): ص370.

[185] زانيت، محمد السعيد. "الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ".مجلة إليزي للبحوث والدراسات .المركز الجامعي إليزي. المجلد 2، العدد 1 (ديسمبر 2017): 3.

بهدف الكشف المبكر عن النشاطات التخريبية أو الإرهابية ذات الطابع الرقمي، وذلك في إطار احترام الضوابط القانونية لحماية الحريات الفردية. وبذلك، تمثل الهيئة أداة مؤسساتية حيوية في تعزيز الحوكمة الرقمية، وتحقيق التوازن بين ضرورات الأمن ومتطلبات احترام الخصوصية الرقمية للمواطنين[186].

3..مؤسسات الدعم والتكوين والتحليل:

تلعب مؤسسات الدعم والتكوين والتحليل دورا جوهريا في تدعيم المنظومة الوطنية للأمن السيبراني، ليس فقط عبر تقديم الخبرة التقنية، بل من خلال تطوير رأس المال البشري وتعزيز القدرات التحليلية والمؤسسية. ويبرز في هذا الإطار **معهد علم الإجرام** التابع لوزارة الدفاع الوطني، الذي يتخذ من بوشاوي مقرا له، كمؤسسة أكاديمية–أمنية متخصصة، تضطلع بمهمة التكوين ما بعد التدرج في مجال علم الإجرام الرقمي، وهو تخصص دقيق يعنى بفهم أنماط الجريمة الإلكترونية وتحليل سلوكيات مرتكبيها وآثارها التقنية والاجتماعية. كما يسهم المعهد في تطوير خبرات الكوادر الأمنية والعسكرية من خلال برامج تدريبية متقدمة، تركز على تحليل البيانات الإلكترونية، الكشف عن الهجمات السيبرانية، وفهم ديناميكيات الشبكات الرقمية المهددة. ومن جهة أخرى، يعد **المرصد الوطني لمجتمع المعلومات** جهازا تحليليا واستشرافيا، يعنى بـ رصد مستوى نفاذ تكنولوجيا المعلومات والاتصالات داخل المؤسسات الجزائرية، سواء من حيث البنية التحتية الرقمية، أو استخدام الأدوات التكنولوجية في تسيير المرافق العمومية. وتكمن أهمية المرصد في دوره التوجيهي، إذ يوفر بيانات كمية ونوعية تستخدم في بناء السياسات العمومية الرقمية، وتسهم في تقييم درجة الجاهزية الرقمية الوطنية، وهو ما يعد عاملا بالغ الأهمية في وضع استراتيجيات أمن سيبراني واقعية وفعالة. وتتكامل أدوار هذه المؤسسات مع الجهود الأمنية والقضائية، من خلال تغذية المنظومة السيبرانية الوطنية بالمعرفة، والتكوين، والتحليل الاستباقي، ما يجعلها حلقة أساسية في إدارة المخاطر الرقمية ومواجهتها بفعالية.

---

[186] عبد الحفيظ بوضياف، الآليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني: الجزائر نموذجاً، مذكرة ماجستير، جامعة محمد بوضياف – المسيلة، ، ص. [88].

جدول المؤسسات الوطنية الجزائرية المختصة بالأمنالمعلوماتي/السيبراني

اسم المؤسسة	التبعية	سنة الإنشاء	المهام الأساسية
المصلحة المركزية لمكافحة الجريمة المعلوماتية	مديرية الأمن الوطني	إعادة الهيكلة) 2011 2015)	**التحقيق في الجرائم السيبرانية، تنسيق الشرطة القضائية**
مركز الوقاية من جرائم الإعلام الآلي	الدرك الوطني	2008	**رصد وتحليل الجرائم المعلوماتية، دعم المؤسسات الرسمية**
المعهد الوطني للأدلة الجنائية وعلم الإجرام	وزارة الدفاع الوطني	نشاط فعلي) 2004 2009)	**تقديم خبرة رقمية متخصصة، التكوين في علم الإجرام السيبراني**
الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال	وزارة العدل(هيئة مستقلة)	تنظيم فعلي) 2009 2015)	**اقتراح السياسات، المراقبة الوقائية، دعم القضاء والشرطة، التعاون الدولي**
النيابات القضائية المتخصصة	وزارة العدل	—	**متابعة ومقاضاة مرتكبي الجرائم السيبرانية**
المرصد الوطني لمجتمع المعلومات	—	—	**مراقبة نفاذ واستخدام تكنولوجيا المعلومات، مرجع تحليلي**

من خلال ما سبق، يمكن القول إن الجهود التي تبذلها الجزائر في مجال تحقيق الأمن السيبراني هي قيد التنفيذ، ما يعكس انطباعا عاما بأن الدولة الجزائرية تتخذ الطريق الصحيح، خاصة فيما يتعلق بالجوانب **التقنية والتنظيمية** للأمن السيبراني. فقد انصبت أغلب المبادرات على كل الجوانب اللازمة[187]

[187] **نفس المرجع السابق**

المبحث الثالث: الأمن السيبراني كمرتكز لتحقيق الاستراتيجية والسياسات العامة في الدولة الجزائرية: مقاربة تحليلية في سياق العلاقات الدولية.

المطلب الاول: التحديات البنيوية والتقنية أمام تجسيد السيادة السيبرانية في الجزائر.

الفرع الاول:التحديات الخارجية لتطور الأمن السيبراني في الجزائر.

حسب واقع التحركات الرسمية نحو تحسين الجاهزية السيبرانية للجزائر واعطاء الرقمنة اولوية اساسية هناك تحديات تم رفعها و كسب رهانها من خلال تحديث البنية السيبرانية للدولة كأحد ابعاد منظومة الامن الوطني، و هذا لا يعني أن هناك مجموعة من التحديات الخارجية البنيوية والتقنية التي تشكل عوائق حقيقية أمام بناء استراتيجية سيبرانية فعالة في الجزائر. وفيما يلي عرض مفصل لها:

1. تعقيد البيئة السيبرانية العالمية

البيئة السيبرانية تتسم بسرعة التغير والتعقيد المتزايد، نتيجة لاندماج تقنيات حديثة مثل الذكاء الاصطناعي، الحوسبة السحابية،[188] الإنترنت الصناعي للأشياء(IIoT) ، مما يؤدي إلى توسع غير مسبوق في سطح الهجوم(attack surface) . ويجعل هذا الواقع المتحول وضع استراتيجيات وقائية فعالة أمرا صعبا للغاية، لأن التهديدات تتغير بوتيرة أسرع من قدرة الدول على تطوير آليات الاستجابة[189].

[188] أهم 16 مشكلة أمنية - Cloud المخاطر والتهديدات والتحديات، OPSWATبالعربية، نُشر قبل 4 أشهر، تاريخ الاطلاع: 9 جوان 2025، https://arabic.opswat.com/blog/cloud-security-challenges.

[189] ما هي أهم التهديدات السيبرانية المحدقة بأمن الحوسبة السحابية؟، *ميترا بالعربية*، 15 سبتمبر 2022، تاريخ الاطلاع: 9 جوان 2025، https://mittrarabia.com/blog/cloud-cybersecurity-risks.

2.الانتشار السريع للإنترنت وتوسيع نطاق الهجمات

مع ارتفاع عدد المستخدمين في الجزائر، وخصوصا عبر الأجهزة المحمولة، تزداد كمية البيانات المعرضة للاختراق، وتتشعب النقاط الضعيفة الممكن استهدافها، خاصة في ظل الاستخدام غير المؤمن لتطبيقات الإنترنت. فزيادة الاعتماد المجتمعي على الخدمات الرقمية يرافقه نقص في الأمن السيبراني الشخصي ، مما يخلق بيئة خصبة للهجمات السيبرانية الجماعية مثل برمجيات الفدية (ransomware) والهجمات الموجهة[190].(APT)

3. تعقيد الأدلة الرقمية

تعد مسألة الإثبات الرقمي من أعقد الجوانب في ميدان الأمن السيبراني، إذ أن الهجمات الإلكترونية غالبا ما تصمم بطريقة تخفي آثارها. الأدلة (logs, traces) قد تحذف أو تعدل عن بعد، مما يجعل من الصعب تقديم أدلة قاطعة في المحاكم أو التحقيقات. كما أن غياب التشريع الخاص بحفظ الأدلة الرقمية في الجزائر يضعف من قابلية الاستجابة القضائية[191].

4.صعوبة تحديد هوية المهاجم

تعتبر "مشكلة الإسناد" واحدة من أخطر العقبات، حيث يمكن للمهاجم استخدام تقنيات متقدمة مثل VPN، البروكسي، التشفير المتعدد، أو الشبكات المظلمة(DarkNet) ، ما يعقد تحديد مصدر الهجوم، وبالتالي تأخير مبدأ الردع، الذي يعتمد على معرفة الجهة المعتدية واتخاذ رد فعل مناسب تجاهها.

5.غياب الحدود الجغرافية والزمنية

الفضاء السيبراني لا يعرف حدودا، مما يعقد من مسألة تطبيق القانون. على سبيل المثال، قد تشن هجمة إلكترونية على خادم حكومي جزائري من عنوان IP مسجل في بلد ثالث، بينما المهاجم

---

[190] الجزيرة نت، «600 ألف هجوم سيبراني في 3 أشهر.. هل نحن جاهزون للعاصفة الرقمية؟»، 9 مارس 2025، تاريخ الاطلاع: 9 جوان 2025، https://www.aljazeera.net/news/science/2025/3/9/600k-cyberattacks-in-3-months

[191] عدنان ابراهيم و فايز خضر، «الأدلة الرقمية وإثبات الجرائم السيبرانية: بين التأصيل والتأويل»، **المجلة الفلسطينية للأبحاث القانونية**، العدد 1، تشرين أول 2021، صـ 144،

الحقيقي موجود في بلد رابع. كما أن الهجمات قد تقع في أي وقت، ما يستوجب جاهزية دائمة 7/24، وهو ما يمثل تحديا على القدرات التقنية والبشرية.

6.اختلال ميزان القوة السيبرانية

الدول المتقدمة تملك ما يعرف بـ"الردع السيبراني"، سواء عبر إمكانات هجومية أو دفاعية، التي استحدثت مقاربات سيبرانية للقدرات الهجومية والدفاعية على حد سواء، ما يجعلها هدفا مفضلا للجهات الإجرامية أو حتى بعض الدول المعادية التي تستخدم الفضاء الإلكتروني كأداة تأثير سياسي أو اقتصادي. [192]

7.صعوبة تقييم المخاطر وغياب إطار موحد لإدارتها

تقييم المخاطر السيبرانية يتطلب:

فهما عميقا للبنية التحتية الرقمية الوطنية،

تقدير قدرة الخصوم (state actors, hackers) على استغلال نقاط الضعف،

تحليل سيناريوهات الأثر المحتمل في حال نجاح الاختراق (انقطاع الخدمات، تسريب البيانات، تعطيل الاقتصاد...).

الفرع الثاني:التحديات الداخلية لتطوير الأمن السيبراني في الجزائر.

على غرار التحديات الخارجية، تواجه الجزائر مراحل داخلية بنيوية ووظيفية تمهد لوتيرة تبني استراتيجية سيبرانية فعالة، وتزيد من جاهزيتها الرقمية في مواجهة التهديدات الحديثة. هذه العوامل تمس بالأساس الهياكل الإدارية، الموارد البشرية، التشريعات، ومستوى الوعي المجتمعي.

1.بداية الخبرة السيبرانية الوطنية

[192] نفس المرجع السابق

تم تأخر إدراج الأمن السيبراني كأولوية وطنية مقارنة بالقطاعات التقليدية مثل الأمن العسكري التقليدي، إلا أنه في الوقت الحالي يتم تبني استراتيجية شاملة في هذا المجال. هناك جهود مستمرة لتحسين الأداء في مواجهة التهديدات السيبرانية، من خلال تعزيز الدولة لمجموعة من الأطر المؤسسية القادرة على التصدي لتلك التهديدات وضمان أمن الدولة في هذا البعد. ومن الأمثلة على هذه الجهود، إنشاء المدرسة العليا للأمن السيبراني التي تساهم في تأهيل الكوادر الوطنية المتخصصة، وكذلك وكالة المعطيات الشخصية التي تسعى لضمان حماية البيانات الشخصية وحقوق الأفراد في الفضاء الرقمي. بالإضافة إلى ذلك، تم إنشاء المحافظة السامية للرقمنة التي تعمل على تطوير استراتيجية شاملة للتحول الرقمي، والتي تشمل تعزيز الأمن السيبراني كجزء أساسي من بنيتها المؤسسية. كما أن هناك خبرات جديدة قيد التكوين في هذه المجالات بهدف تعزيز القدرة على التصدي للتهديدات الرقمية وتحقيق استدامة في أمن الفضاء السيبراني الوطني[193] .

2. الاعتماد المؤسساتي على التكنولوجيا

رغم التحديات الحالية، فإن المؤسسات الجزائرية تشهد تحولا تدريجيا نحو الاعتماد على التكنولوجيا الرقمية، وهو ما يعكس استعدادها للتطوير والتحسين. هناك جهود متزايدة لتسريع التحول الرقمي في الإدارة العمومية وتعزيز البنية التحتية الرقمية. هذه التحولات تتضمن أيضا زيادة الوعي بالتهديدات الرقمية وأهمية رقمنة المعاملات، مما يسهم في رفع مستوى الأمان السيبراني. كما أن الاستثمار في الأنظمة الذكية يتيح إمكانيات أفضل للكشف المبكر عن أي تهديدات أو محاولات تسلل، مما يعزز من استباقية المؤسسات في مواجهة التحديات الرقمية.يؤدي هذا الواقع إلى قوة الاستباقية الرقمية، إذ أن وجود الأنظمة الذكية يزيد من إمكانيات الكشف المبكر عن الاختراقات أو محاولات التسلل[194].

[193] الأمن السيبراني في الجزائر: السياسات والمؤسسات، ASJP، من إعداد مجموعة باحثين، المركز الجامعي عبد الحفيظ بوالصوف، ميلانة، الجزائر، تاريخ النشر غير مذكور، صـ275.
[194] نفس المرجع السابق

3.التمويل المخصص للأمن السيبراني

تظهر البيانات والمؤشرات أن الميزانية الموجهة للبحث والتطوير في مجال الأمن السيبراني في تزايد مستمر مقارنة بالقطاعات الأخرى، وحتى بالمقارنة مع الناتج المحلي الإجمالي. وهذا يعكس اهتماما متزايدا بتطوير قدرات الدولة في مواجهة التحديات السيبرانية. ومع ذلك، لا يزال هناك حاجة لتوجيه الاستثمارات بشكل أكبر نحو بعض المجالات الأساسية التي تساهم في تعزيز الأمن السيبراني. فعلى سبيل المثال، هناك حاجة ملحة لتعزيز التكنولوجيا الدفاعية مثل أنظمة كشف التسلل(**IDS/IPS**) ، بالإضافة إلى توسيع بناء مراكز الاستجابة للطوارئ السيبرانية (**CERTs**)التي تعتبر أساسية في التعامل مع الحوادث الرقمية. كما أن تطوير القدرة على اقتناء أدوات التحليل المتقدمة مثل أدوات التحقيق الجنائي الرقمي(**forensics**) ، أنظمة إدارة معلومات الأمان(**SIEM**) ، و تقنيات العزل (**sandboxing**) يعد خطوة حاسمة لتحسين الأداء الأمني[195].

4.التحديات التشريعية والتنظيمية

لا تزال الجزائر تعتمد على قوانين سيبرانية تحتاج للتحديث المستمر، مثل قانون 09-04 لسنة 2009، وهو غير كاف لمجابهة تطور الهجمات مثل:

هجمات الابتزاز المالي,(ransomware)

التجسس الرقمي على المؤسسات،

استهداف البنى التحتية الحيوية.

[195] نفس المرجع السابق

كما أن غياب إطار قانوني واضح لحوكمة البيانات الشخصية يزيد من هشاشة التعامل مع المعلومات الحساسة، خاصة في غياب هيئة مستقلة لتنظيم الأمن السيبراني على غرار الدول الرائدة[196].

5.الاستثمار في الكفاءات البشرية المتخصصة

رغم التقدم الذي تحقق في مجال التعليم الجامعي التقني، إلا أن هناك فرصة كبيرة لتعزيز البرامج الجامعية لتغطية موضوعات الأمن السيبراني الحديثة بعمق أكبر، مثل التشفير (cryptography)، القرصنة الأخلاقية(ethical hacking) ، وقانون الأمن السيبراني (cyberlaw) ،وهو ما سيساهم في تزويد الطلاب بالمعرفة والمهارات الأكثر تطورا. كما أن تعزيز التكوين العملي من خلال إنشاء مختبرات رقمية متقدمة سيكون له دور كبير في تهيئة الخريجين للواقع المهني، مما يرفع من استعدادهم للعمل في بيئات مهنية متطورة. بالإضافة إلى ذلك، يمكن تحفيز العقول المتخصصة من خلال خلق بيئات عمل محلية مشجعة، مما يسهم في احتفاظ الكفاءات المحلية في البلاد بدلا من هجرة العقول إلى الخارج، والعمل على إثراء السوق المحلي بالخبرات الضرورية لدفع عجلة التنمية في مجال الأمن السيبراني[197].

يشهد الأمن السيبراني اهتماما متزايدا في الجزائر، في ظل الوعي المتنامي بأهمية الفضاء الرقمي في حماية المصالح الوطنية. وقد تم اتخاذ عدة خطوات مهمة، كإصدار تشريعات أولية، وإنشاء بعض الهيئات المتخصصة، والانخراط في تعاونات إقليمية ودولية. ومع ذلك، فإن تعزيز الأمن السيبراني يظل ورشة مفتوحة تتطلب تضافر الجهود وتطوير الرؤية الشاملة.

فعلى المستوى الخارجي، تفرض التهديدات الرقمية تحديات تقنية معقدة بسبب الطابع المتغير والديناميكي للهجمات السيبرانية، وغياب الحدود الجغرافية، وصعوبة التتبع الرقمي. أما داخليا، فتسجل الجزائر بعض التحديات البنيوية، من بينها الحاجة إلى التحديث المستمر للبنية التحتية

[196] نفس المرجع السابق
[197] نفس المرجع السابق.

الرقمية، و مواصلة تطوير الكفاءات البشرية المتخصصة، وتعزيز الإطار القانوني والتنظيمي ليواكب التحولات التكنولوجية.

ومع أن هذه التحديات مشتركة بين كل الدول، إلا أن الفرصة سانحة أمام الجزائر لبناء منظومة أمن سيبراني فعالة، إذا ما تم الاستثمار في المجالات التالية:

دعم التعليم والتكوين في مجالات الأمن الرقمي والبحث التطبيقي.

ترسيخ ثقافة رقمية واعية داخل المؤسسات والمجتمع.

استحداث آلية وطنية موحدة لتنسيق السياسات السيبرانية على المستوى الاستراتيجي.

تشجيع الشراكة مع القطاع الخاص والجامعات لتسريع وتيرة التحول الرقمي الآمن.

المطلب الثاني: آفاق استفادة الجزائر من النماذج الاستراتيجية الكبرى في الأمن السيبراني (الولايات المتحدة، الصين، روسيا)

في ظل تصاعد التهديدات السيبرانية وتنامي التحديات التي تواجه الجزائر في بناء منظومة رقمية محمية وذات سيادة، تبرز الحاجة الملحة إلى تبني نماذج دولية رائدة يمكن الاستفادة منها وتكييفها بما يتماشى مع الخصوصية الجزائرية. وتمثل استراتيجيات كل من الولايات المتحدة الأمريكية، الصين، وروسيا مرجعيات متكاملة، تختلف من حيث الفلسفة، الهيكلة، والأولويات، لكنها تشترك في كونها تجارب ناضجة استطاعت تطوير سياسات دفاعية وهجومية متعددة المستويات، مما يوفر للجزائر فرصة لتبني مقاربة هجينة ومرنة.

فعلى مستوى النموذج الأمريكي، تعتمد الولايات المتحدة مقاربة شاملة قائمة على مفهوم الدفاع المتقدم(Forward Defense) ، والذي يدمج الردع، والهجوم الاستباقي، والعمق الدفاعي الرقمي، من خلال وكالة الأمن القومي (NSA) وقيادة الأمن السيبراني (USCYBERCOM) . كما تعطي الولايات المتحدة أهمية قصوى للشراكة بين القطاعين العام والخاص، حيث توظف الشركات التكنولوجية الكبرى(Microsoft ، Google، Cisco ...)كخط دفاع أول. يمكن

للجزائر الاستفادة من هذا النموذج عبر تفعيل الشراكات المحلية مع الشركات الناشئة، وتعزيز القطاع السيبراني الخاص، وتطوير وحدات تنسيق بين المؤسسات الأمنية والجامعات، بما يشبه "القطاع الثالث" للأمن الرقمي.

أما النموذج الصيني، فيقوم على مبدأ السيادة الرقمية الكاملة والتحكم المركزي الصارم، من خلال دمج الأمن السيبراني في مفهوم الأمن القومي الشامل تحت إشراف "الإدارة المركزية للفضاء السيبراني". وتركز الصين على تطوير تكنولوجيا محلية بديلة، وتقليل الاعتماد على الغرب، مع الاستثمار في الذكاء الاصطناعي والبيانات الضخمة. وتكمن استفادة الجزائر هنا في تعزيز الاستقلال التكنولوجي، ودعم البحث العلمي الوطني في الأمن السيبراني، وتحفيز إنشاء مراكز ابتكار سيبراني، مع فرض سياسات أمنية واضحة لحوكمة البيانات الوطنية.

أما النموذج الروسي، فيعتمد على المرونة السيادية والهندسة الدفاعية متعددة الطبقات، ويدمج بين القدرات الهجومية والدفاعية تحت إشراف "جهاز الأمن الفيدرالي "(FSB) ووزارة الدفاع. كما تركز روسيا على أمن البنية التحتية الحيوية، والقدرة على فصل الشبكة الداخلية (RuNet)في حالة الطوارئ. ويمكن للجزائر من هذا النموذج أن تستلهم بناء نظام وطني للإنذار المبكر السيبراني، وتطوير خطط طوارئ لعزل البنى التحتية الرقمية الحساسة، خاصة في قطاعات الطاقة، النقل، والمالية.

بناء على ما سبق، فإن الجزائر رغم محدودية تطورها في مجال الأمن السيبراني مقارنة بالقوى الكبرى، تمتلك مقومات فريدة تؤهلها لاعتماد مقاربة بناءة واستباقية. ويعد تفوقها الإقليمي في المجال العسكري فرصة استراتيجية يمكن توظيفها كرافعة لبناء منظومة أمن سيبراني فعالة، تتكامل مع منظومتها الدفاعية التقليدية.

في هذا السياق، لا يكمن السبيل في نسخ التجارب الدولية حرفيا، بل في الاستفادة الذكية من عناصر قوتها كأن تستلهم الجزائر من **النموذج الأمريكي ديناميكية الشراكة بين القطاعين العام والخاص وتطوير القدرات الردعية التقنية**، ومن **النموذج الصيني فلسفة السيادة الرقمية**

والانضباط المؤسسي، ومن **النموذج الروسي القدرة على الدمج بين الأمن السيبراني والدفاع الوطني الشامل** .ومن خلال التكيف التدريجي مع هذه التجارب، يمكن للجزائر أن تؤسس **لنموذج سيبراني وطني متوازن،** يراعي خصوصياتها، ويبنى على مراحل، في إطار رؤية استراتيجية متكاملة، تعزز حضورها السيبراني إقليميا وتمنحها قدرة أكبر على مواجهة التهديدات غير المتماثلة .

الخاتمـــــة

في ضوء التحليل النظري والتطبيقي لموضوع "**البعد السيبراني للأمن القومي الجزائري: دراسة مقارنة لنماذج دولية رائدة**"، يمكن القول إن الإشكالية المركزية للدراسة" **:كيف يشكل الأمن السيبراني تحديا استراتيجيا لمنظومة الأمن الوطني الجزائري، ضمن سياق البيئة الدولية المعقدة؟**" قد تمت معالجتها من خلال تفكيك أبعاد التهديدات السيبرانية، واستكشاف تداعياتها على وظائف الدولة الحيوية، وتقييم مستوى جاهزية البنية الوطنية لمواجهتها.

أثبتت الدراسة، من خلال المقاربات النظرية المعتمدة (نظرية الأمن الموسّع، المقاربة البنيوية...)، ملاءمة الإطار المفاهيمي والنظري لفهم طبيعة هذه التهديدات التي لم تعد مقتصرة على الطابع العسكري أو الأمني الضيق، بل اتسعت لتشمل الأمن الرقمي، الاقتصادي، المجتمعي وحتى السيادي.

أما بخصوص اختبار الفرضيات، فقد بيّنت النتائج أن:

- التهديدات السيبرانية تشكل فعلا تحديا مباشرا للأمن الوطني، خاصة في ظل الاعتماد المتزايد على الرقمنة.
- تأثير هذه التهديدات على وظائف الدولة الحيوية يتجلى بوضوح في القطاعات الحساسة، على غرار الطاقة، الاقتصاد، التعليم والدفاع، مما يجعلها عنصرا حاسما في أجندة الدول.
- الاستفادة من النماذج الدولية (الأمريكي، الصيني، الروسي) تظهر أهمية تبني نموذج جزائري متوازن، يجمع بين الصرامة التنظيمية، التكوين البشري، مع مراعاة الخصوصية القانونية والسياسية الوطنية.

توصلت الدراسة من خلال عرض فصولها الثلاثة الى مجموع النتائج التالية :

-أثبتت أن الأمن السيبراني يمثل تحديا استراتيجيا للجزائر، سواء من حيث البنية التحتية الرقمية أو مجابهة التكنولوجية الغربية، أو التنسيق المؤسساتي، أو استحضار رؤية وطنية متكاملة

للأمن السيبراني. وقد كشفت الدراسة عن مجموعة من الثغرات التي يمكن أن تشكل مدخلا لهجمات سيبرانية تمس بمؤسسات حيوية كقطاع الصحة، التعليم، الاتصالات، والإعلام. كما بينت التجارب الدولية المدروسة (الولايات المتحدة، روسيا، الصين) أن التهديدات السيبرانية أصبحت أداة جيوسياسية تستخدمها القوى الكبرى ضمن عقائدها العسكرية، ما يستدعي من الجزائر تطوير مقاربتها من مجرد ردود فعل تقنية إلى استراتيجية وطنية شاملة.

-كما بينت الدراسة أن الخطر السيبراني لا يهدد فقط البنية التقنية بل يمتد إلى الأمن المجتمعي في أبعاده النفسية، الثقافية، والسياسية، من خلال الحملات التضليلية، اختراق الخصوصية، والتلاعب بالرأي العام، ما يستوجب تحصين الجبهة الداخلية عبر نشر ثقافة سيبرانية ورفع الوعي الرقمي لدى المواطنين.

إن الوصول إلى أمن سيبراني فعال يتطلب مواصلة إرساء فلسفة متينة للأمن القومي الجزائري، ومواصلة دمج البعد السيبراني ضمن أولويات الدولة، من خلال:

- تبني قانون شامل للأمن السيبراني يتماشى مع البيئة الدولية المعقدة. check
- دعم البحث العلمي والتكوين المتخصص في مجال الأمن المعلوماتي. check
- إرساء هياكل وطنية دائمة ومتعددة الاختصاصات لرصد وتحليل التهديدات. check

في الختام، تفرض التهديدات السيبرانية اليوم واقعا جديدا يضع الدول، ومنها الجزائر، أمام خيارين لا ثالث لهما: إما مواكبة التطور ومواصلة بناء **سيادة رقمية قوية**، أو البقاء رهينة لتقنيات الغير وصراعاتهم. وتأسيسا على ذلك، توصي هذه الدراسة بمواصلة تبني **الاستراتيجية الوطنية الشاملة للأمن السيبراني**، التي تبنى على أسس المنطق الاستباقي الوقائي الردعي، الجاهزية، السيادة، والشراكة المجتمعية، باعتبار أن الأمن السيبراني لم يعد ترفا مؤسساتيا، بل ركيزة من ركائز بقاء الدولة الحديثة.

قائمة المراجع:

الكتب

1. القريطي، حزام .*الأمن السيبراني وحماية المعلومات* .الإسكندرية: دار الفكر الجامعي، 2020.
2. ستيفان هالر، وجونثان كلارك .*التفرد الأمريكي: المحافظون الجدد والنظام العالمي* .ترجمة عمر الأيوبي. بيروت: دار الكتاب العربي، 2005.
3. زياد، علي .*الصراع والأمن الجيوسياسي في السياسة الدولية* .عمان: دار أمجد للنشر والتوزيع، الطبعة الأولى،2020
4. Nye, Joseph S., Jr. "Cyber Power." In *The Future of Power*, New York: PublicAffairs, 2011.
5. Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*. London: Routledge, 2013.
6. Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.
7. Giles, Keir. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016.

8. Mey, Holger. *Strategic Sderzhivanie: Understanding Contemporary Russian Approaches to Deterrence*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, 2023.

9. Hakala, Janne, and Jazlyn Melnychuk. *Russia's Strategy in Cyberspace*. Edited by Sanda Svetoka. Riga: NATO Strategic Communications Centre of Excellence, 2020.

10. Lilly, B., and J. Cheravitch. "The Past, Present and Future of Russia's Cyber Strategy and Forces." In *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*, 142–146. Fort Leavenworth, KS: Foreign Military Studies Office, 2019.

المقالات الأكاديمية

1. زينب فريّل. "أجيال الحرب: دراسة في محددات تطور الأجيال الخمس للحرب ". *دفاتر السياسة والقانون*، م 31، ع 20 (2020): 546.

2. عبد العزيز بن فهد بن محمد بن داود. "الجرائم السيبرانية: دراسة تأصيلية مقارنة ".*مجلة الاجتهاد للدراسات القانونية والاقتصادية* 9، عدد 3 (2020): 148.

3. إدريس عطية. "ماكنة الأمن السيبراني في منظومة الأمن الوطني الجزائري ". *مجلة مصداقية، كلية الحقوق والعلوم السياسية – جامعة العربي التبسي، تبسة*، عدد 1 (2019): 103.

4. علوطي ملني. "أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة ".*مجلة علوم إنسانية*، السنة 6، العدد 38 (2008): 2.

5. قدايفية، أمينة. "استراتيجية أمن المعلومات ".*مجلة دراسات اقتصادية وإدارية*، العدد 8 (2016): 166.

6. ابتسام علي حسين. "فرص وقيود الأطراف المتنازعة على 'المجال العام السيبراني ". *'مجلة السياسة الدولية*، ملحق اتجاهات نظرية، العدد 208، مركز الأهرام، القاهرة، 2017.

7. أمسهان بوضياف. "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر ".*مجلة الأستاذ الباحث للدراسات القانونية والسياسية*، مج. 3، ع. 3 (2018): ص370.

8. زانيت، محمد السعيد. "الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية ".*مجلة إليزي للبحوث والدراسات*، المجلد 2، العدد 1 (ديسمبر 2017): 3.

9. عدنان ابراهيم و فايز خضر. "الأدلة الرقمية وإثبات الجرائم السيبرانية: بين التأصيل والتأويل ".*المجلة الفلسطينية للأبحاث القانونية*، العدد 1، تشرين أول 2021، صـ 144.

10. حميدي، حياة، ونسيمة طايلب. "مدخل مفاهيمي حول الأمن السيبراني ". *مجلة مدار للدراسات الاتصالية الرقمية*، العدد 2، نوفمبر 2022، جامعة الشلف، ص12-13.

11. المواقع الإلكترونية

12. جدو فؤاد. "تفجيرات الهواتف واختراقها في ظل تحولات حروب الجيل السابع "*مدونات الجزيرة*. نُشر في 25 سبتمبر 2024 . https://www.aljazeera.net/blogs/2024/9/25 /

13. Agence nationale de la sécurité des systèmes d'information (ANSSI). "Définition de la cybersécurité." *cyber.gouv.fr*. Consulté le 5 juin 2025. https://cyber.gouv.fr/resultats-recherche?search_api_fulltext=D%C3%A9finition+de+la+cybers%C3%A9curit%C3%A9&sort_by=title.

14. " Oolom. الفرق بين أمن المعلومات والامن السيبراني." تم الدخول في 5 يونيو 2025. https://www.oolom.com/6124/ .

15. قدايفية، أمينة. "استراتيجية أمن المعلومات *ASJP:* "*مجلة دراسات اقتصادية وإدارية*، العدد 8 (2016): 166 . https://www.asjp.cerist.dz/en/article/31120.

16. الجزيرة نت. "الجرائم الإلكترونية: عندما تصبح الإنترنت سلاحًا." نُشر في 6 أبريل 2015. تم الدخول في 6 يونيو 2025 .

https://www.aljazeera.net/tech/2015/4/6/الجرائم-الإلكترونية-عندما-تصبح-2.

17. Cloudflare. "What is a DDoS Attack?" *Cloudflare Learning Center*. Accessed June 6, 2025. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

18. Norton. "What Is Ransomware?" *Norton Cyber Safety*. Accessed June 6, 2025. https://us.norton.com/blog/malware/what-is-ransomware.

19. BBC. "The Love Bug: Most Destructive Computer Virus Ever?" *BBC News*, May 4, 2020. https://www.bbc.com/news/technology-52535161.

20. Zetter, Kim. "The Strange Story of the Melissa Virus." *Wired*, March 26, 2014. https://www.wired.com/2014/03/melissa-virus-15-years-later/.

21. Cybersecurity Ventures. "Cybercrime To Cost The World $9.5 Trillion USD In 2024." *Cybersecurity Almanac 2024*. Accessed June 6, 2025. https://cybersecurityventures.com/cybersecurity-almanac-2024/.

22. Varonis. "60 Must-Know Cybersecurity Statistics for 2024." *Varonis Blog*. Accessed June 6, 2025. https://www.varonis.com/blog/cybersecurity-statistics.

23. PurpleSec. "2024 Cyber Security Statistics." Accessed June 6, 2025. https://purplesec.us/resources/cybersecurity-statistics/.

24. Secureframe. "Cybersecurity Statistics You Need to Know in 2024." Accessed June 6, 2025. https://secureframe.com/blog/cybersecurity-statistics.

25. NinjaOne. "Ransomware Statistics and Trends 2024." Accessed June 6, 2025. https://www.ninjaone.com/blog/cybersecurity-statistics/.

26. Embroker. "Cyber Attack Statistics for 2024." Accessed June 6, 2025. https://www.embroker.com/blog/cyber-attack-statistics/.

27. Cobalt. "Top Cybersecurity Statistics You Need to Know in 2024." Accessed June 6, 2025. https://www.cobalt.io/blog/top-cybersecurity-statistics-2025.

28. Microsoft. "600 Million Cyberattacks Per Day Around the Globe." *Microsoft Digital Defense Report 2024*.

Accessed June 6, 2025. https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/.

29. The White House. "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience." February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

30. Cybersecurity and Infrastructure Security Agency (CISA). "Critical Infrastructure Sectors." Accessed June 7, 2025. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

31. Chinafy. "What Is the Cyberspace Administration of China (CAC)?" Accessed June 7, 2025. https://www.chinafy.com/blog/what-is-the-cyberspace-administration-of-china-cac.

32. Sevastopulo, Demetri, and Ryan McMorrow. “Xi Jinping Tightens Grip on China’s Military with New Information Warfare Unit.” *Financial Times*, April 20, 2024. https://www.ft.com/content/5584feb4-0e58-4b6c-8140-f9c6e8e3ba5e.

33. James A. Lewis. "China's Emerging Cyber Governance System." *CSIS*. Accessed June 7, 2025. https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber.

34. War on the Rocks. "Managing the Power Within: China's Cybersecurity Law and the Organizational Logic of Authoritarian Control." July 18, 2016. https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission.

35. Piscium. "SORM: The Digital Surveillance Network and Its Global Impact." April 1, 2025. https://www.piscium.net/2025/04/01/sorm-the-digital-surveillance-network-and-its-global-impact-2/.

36. Atlantic Council. "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior." Accessed June 7, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/

التقارير الرسمية والمؤسسات الدولية

1. Africa Joint Forum on Cybersecurity (AJFOC). تقرير تقييم *التهديدات السيبرانية في إفريقيا 2024*. ص. 3 . https://www.au.int/sites/default/files/documents/24COM005030-AJFOC_Africa_Cyberthreat_Assessment_Report_2024_complet_AR_LR.pdf.
2. International Telecommunication Union (ITU). *Global Cybersecurity Index 2024*, 5th edition. Accessed June 9, 2025. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.
3. Council of Europe. *Convention on Cybercrime (Budapest Convention)*, ETS No. 185, Budapest, 23.XI.2001. Accessed June 6, 2025. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
4. U.S. Department of Defense. *Joint Publication (JP) 3-12: Cyberspace Operations*. Washington, D.C.: Joint Chiefs of Staff, December 2022.

5. U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*. Fort Meade, MD: U.S. Cyber Command, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

6. Joint Chiefs of Staff. *Joint Concept for Entry Operations*. Washington, D.C.: U.S. Department of Defense, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jceo.pdf.

7. Joint Chiefs of Staff. *Joint Targeting School Student Guide*. Washington, D.C.: U.S. Department of Defense, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf.

8. U.S. Department of Defense. *2023 Cyber Strategy Summary*. Washington, D.C.: U.S. Department of Defense, 2023. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_CYBER_STRATEGY_SUMMARY.PDF.

9. U.S. General Services Administration. "Cybersecurity Framework." Last modified April 2025.

https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/cybersecurity-framework.

10. Cybersecurity and Infrastructure Security Agency (CISA). *Insider Threat Mitigation Guide*. U.S. Department of Homeland Security, November 2020. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf .

11. The White House. "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience." February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

12. RAND Corporation. *Russia's New Military Doctrine: Same as the Old Doctrine, Mostly*. January 2015. https://www.rand.org/commentary/2015/01/russias-new-military-doctrine.html.

13. RAND Corporation. *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*. 2017. https://www.rand.org/pubs/research_reports/RR2058.html.

14. Center for Strategic and International Studies (CSIS). "China's Cyber Power in a New Era." October 2020. https://www.csis.org/james-lewis-publications.

15. National Defense University. *China's Strategic Support Force: A Force for a New Era*. China Strategic Perspectives 13. 2018. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

16. Center for a New American Security (CNAS). Kania, Elsa B., and John K. Costello. *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*. September 2018. https://www.cnas.org/publications/reports/quantum-hegemony.

17. DataReportal. *Digital 2024: Algeria*. January 2024. https://datareportal.com/reports/digital-2024-algeria.

18. Ookla. *Speedtest Global Index: Algeria*. Accessed June 2025. https://www.speedtest.net/global-index/algeria.

19. Worldometers. "Algeria Population (2025)." Accessed June 9, 2025. https://www.worldometers.info/world-population/algeria-population/.

النصوص القانونية الجزائرية

1. **القانون رقم 18-04** المؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، *الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية*، العدد 27، مؤرخة في 13 ماي 2018، الصفحة 3.
2. **القانون رقم 04-15** المؤرخ في 10 نوفمبر 2004، يتضمن تعديل قانون العقوبات، *الجريدة الرسمية للجمهورية الجزائرية*، رقم 71، الصفحتان 11 و12.
3. **القانون رقم 06-22** المؤرخ في 20 ديسمبر 2006، المعدِّل والمتمم للأمر رقم 66-155 المؤرخ في 8 يونيو 1966، والمتضمن قانون الإجراءات الجزائية، *الجريدة الرسمية*، العدد 84، بتاريخ 24 ديسمبر 2006، الصفحة 4.
4. **القانون رقم 09-04** المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، *الجريدة الرسمية*، العدد 47، بتاريخ 16 أوت 2009.
5. **المرسوم الرئاسي رقم 19-172** المؤرخ في 25 جوان 2019، المتعلق بإنشاء الوكالة الوطنية للأمن السيبراني وتنظيمها وسيرها، *الجريدة الرسمية*، العدد 41، ص. 17.
6. **المادة 3/10** من القانون رقم 18-04، الجريدة الرسمية، العدد 27، 13 ماي 2018، ص. 3.
7. **المواد من 394 مكرر إلى 394 مكرر 7** من القانون رقم 04-15، الجريدة الرسمية، العدد 71، 10 نوفمبر 2004، ص. 11-12.

8. **المادة 02 (مكرر أ)** من القانون رقم 09-04، *الجريدة الرسمية*، العدد 47، 16 أوت 2009.

المذكرات والرسائل الجامعية

1. عبد الحفيظ بوضياف .*الآليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني: الجزائر نموذجاً* .مذكرة ماجستير، جامعة محمد بوضياف – المسيلة، ص. 88.
2. إدريس عطية .*مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري* .كلية الحقوق والعلوم السياسية، جامعة العربي التبسي – تبسة، ص. 113.

فهرس المحتويات:

فهرس المحتويات:

فهرس المحتويات:

فهرس المحتويات: