Al-Farouk journal of sciences
Volume (2), Issue (3) (JUNE, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) ملحق العدد 3 يونيو 2026
ردمد: 3135-2359

الأمن السيبراني كأحد محددات القوة في النظام الدولي المعاصر

خالد عمران القريتلي
باحث دكتورا في مدرسة الدراسات الاستراتيجية الاقليمية والدولية، وباحث ومحلل عسكري - وزارة الدفاع - عضو هيئة تدريس بكلية القيادة والاركان
algritly@gmail.com

Cybersecurity as a Determinant of Power in the Contemporary International System

Khaled Omran Al-Quraitli
PhD Researcher at the School of Regional and International Strategic Studies, Researcher and Military Analyst - Ministry of Defense - Faculty Member at the Command and Staff College

تاريخ الاستلام: 2026/6/29 تاريخ المراجعة 7/20/ 2026 تاريخ القبول:2026/7/28- تاريخ النشر:8/17/ 2026

الملخص

هدفت هذه الدراسة إلى تحليل الأمن السيبراني بوصفه أحد محددات القوة في النظام الدولي المعاصر، من خلال بيان تطور مفهوم القوة وتحولها من الاعتماد الأساسي على القدرات العسكرية والاقتصادية إلى مفهوم أكثر شمولًا يتضمن القدرات التكنولوجية والمعلوماتية والسيبرانية. واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال مراجعة وتحليل الأدبيات والدراسات والتقارير الدولية ذات الصلة بالأمن السيبراني والعلاقات الدولية والقوة الوطنية. وتوصلت الدراسة إلى أن الأمن السيبراني أصبح عنصرا مهما في تعزيز القوة الوطنية، نظرا لدوره في حماية البنية التحتية الحيوية والمعلومات والأنظمة الحكومية والعسكرية والاقتصادية، فضلًا عن مساهمته في تعزيز الاستقلال الاستراتيجي للدولة. كما بينت النتائج أن الفضاء السيبراني أصبح مجالًا للتنافس الدولي، وأن امتلاك القدرات السيبرانية المتقدمة أصبح عاملًا مؤثرًا في قدرة الدول على حماية مصالحها وممارسة النفوذ والتعامل مع التهديدات الحديثة. وأظهرت الدراسة كذلك أن التهديدات السيبرانية، مثل التجسس والهجمات على البنية التحتية الحيوية والجرائم الإلكترونية والتضليل الرقمي، تفرض تحديات جديدة على استقرار النظام الدولي. وأوصت الدراسة بضرورة إدماج الأمن السيبراني ضمن استراتيجيات الأمن القومي، وتطوير القدرات التقنية والبشرية، وحماية البنية التحتية الحيوية، وتعزيز التعاون الدولي ووضع أطر قانونية وتنظيمية أكثر فاعلية لمواجهة التهديدات السيبرانية.

الكلمات المفتاحية: الأمن السيبراني، القوة الوطنية، القوة السيبرانية، النظام الدولي، التنافس الدولي، الأمن القومي.

Abstract

This study aimed to analyze cybersecurity as a determinant of power in the contemporary international system, by demonstrating the evolution of the concept of power and its shift from a primary reliance on military and economic capabilities to a more comprehensive concept encompassing technological, informational, and cyber capabilities. The study employed a descriptive-analytical approach, reviewing and analyzing relevant international literature, studies, and reports on cybersecurity, international relations, and national power. The study concluded that cybersecurity has become a crucial element in enhancing national power, given its role in protecting critical infrastructure, information, and governmental, military, and economic systems, as well as its contribution to strengthening a state's strategic independence. The findings also revealed that cyberspace has become an arena for international competition,

and that possessing advanced cyber capabilities has become a significant factor in a state's ability to protect its interests, exert influence, and address modern threats. Furthermore, the study demonstrated that cyber threats, such as espionage, attacks on critical infrastructure, cybercrime, and digital disinformation, pose new challenges to the stability of the international system. The study recommended integrating cybersecurity into national security strategies, developing technical and human capabilities, protecting critical infrastructure, strengthening international cooperation, and establishing more effective legal and regulatory frameworks to counter cyber threats.

Keywords: Cybersecurity, national power, cyber power, international system, international competition, national security.

المقدمة

شهد النظام الدولي في العقود الأخيرة تحولات سريعة بسبب التطور الكبير في تكنولوجيا المعلومات والاتصالات، والانتشار الواسع للإنترنت، والاعتماد المتزايد على الأنظمة الرقمية في إدارة القطاعات السياسية والاقتصادية والعسكرية والأمنية. ساهم هذا التحول في إعادة تشكيل العلاقات بين الدول ووسع مجالات التنافس الدولي لتتجاوز الأبعاد التقليدية للقوة. أصبح التفوق التكنولوجي، والقدرة على امتلاك المعلومات، وحمايتها، واستخدامها، من العوامل المؤثرة في مكانة الدولة وقدرتها على تحقيق مصالحها الوطنية. في هذا السياق، برز الفضاء السيبراني كحقل جديد من مجالات التفاعل والصراع الدولي. أصبح الأمن السيبراني جزءًا متزايد الأهمية من قضايا الأمن الوطني والدولي (حارك وحمدوش، 2022؛ Egloff & Shires, 2021).

لقد أدى الاعتماد المتزايد على البنية التحتية الرقمية إلى ظهور مجموعة متزايدة من المخاطر والتهديدات السيبرانية التي تستهدف الدول والمؤسسات والأفراد، بما في ذلك التجسس الإلكتروني، وسرقة المعلومات، وتعطيل البنى التحتية الحيوية، والهجمات على المؤسسات الحكومية والاقتصادية، فضلًا عن استخدام القدرات السيبرانية في سياق الصراعات الدولية. تكتسب هذه التهديدات خطورتها من تجاوز الفضاء السيبراني الحدود الجغرافية والسياسية التقليدية، مما يجعل آثار الهجمات السيبرانية تنتقل من دولة إلى أخرى، ويضع مفهوم السيادة الوطنية أمام تحديات جديدة. أظهرت دراسات عربية حديثة أن تزايد الجرائم والتهديدات السيبرانية يرتبط بشكل مباشر بالأمن القومي للدول، نظرًا لما يمكن أن تسببه من أضرار اقتصادية وأمنية وسيادية (الخضيري، 2024).

في ضوء هذه التحولات، لم يعد الأمن السيبراني مجرد قضية تقنية تقتصر على حماية الحواسيب والشبكات والبيانات، بل أصبح أحد المكونات الأساسية للأمن الوطني والاستراتيجي، إذ أصبحت حماية الأنظمة الرقمية الحكومية والعسكرية والاقتصادية، وتأمين البنية التحتية الحيوية، والقدرة على اكتشاف الهجمات السيبرانية والاستجابة لها جميعها مؤشرات على قدرة الدولة على حماية مواردها ومصالحها الحيوية. لذلك، يرتبط امتلاك الدولة لقدرات متقدمة في مجال الأمن السيبراني بدرجة قدرتها على المحافظة على سيادتها وتعزيز أمنها الوطني، مما يجعل الأمن السيبراني مرتبطًا بشكل مباشر بمفهوم القوة في العلاقات الدولية (إبراهيم، 2025).

من ناحية أخرى، أسهم الفضاء السيبراني في إعادة التفكير في مفهوم القوة ذاته، فلم تعد القوة الدولية تقاس فقط بحجم القوات المسلحة أو الموارد الاقتصادية، وإنما أصبحت القدرات التكنولوجية والمعلوماتية والسيبرانية جزءا من الموارد التي يمكن للدول استغلالها لتحقيق أهدافها الاستراتيجية. في هذا الإطار، يشير مفهوم القوة السيبرانية إلى قدرة الدولة على استخدام الموارد المرتبطة بالفضاء السيبراني لتحقيق أهداف سياسية وأمنية واقتصادية، سواء من خلال حماية بنيتها الرقمية أو التأثير في قدرات الخصوم. كما وأصبح امتلاك هذه القدرات عاملًا مهما في التنافس بين الدول، خاصة مع زيادة استخدام العمليات السيبرانية في التجسس والإكراه والتأثير والعمليات العسكرية (بوغازي، 2025).

هذا، وتزايدت القدرات السيبرانية الهجومية للدول، مما أدى إلى ظهور أنماط جديدة من التنافس والصراع الدولي. أصبحت العمليات السيبرانية أداة يمكن استخدامها لتحقيق أهداف استراتيجية دون الحاجة بالضرورة إلى القوة العسكرية التقليدية. تمتلك الدول قدرات سيبرانية يمكن استخدامها في سياقات مختلفة، إذ يمنح الغموض في تحديد الجهة المسؤولة عن بعض العمليات السيبرانية الدول مجالا للمناورة السياسية والاستراتيجية، كما يمكن أن يؤثر في حسابات الردع وإدارة الأزمات الدولية (Brown & Fazal, 2021).

تتزايد أهمية هذا الموضوع نظرا لأن استخدام القدرات السيبرانية من قبل الدول لم يعد يقتصر على التجسس أو جمع المعلومات بل امتد أيضا إلى إمكانية إحداث آثار مادية واقتصادية وأمنية كبيرة. إذ أظهرت بعض الهجمات السيبرانية الكبرى

قدرة الأدوات الرقمية على إحداث أضرار ملموسة في البنية التحتية والاقتصاد. هذا الأمر دفع إلى طرح تساؤلات حول العلاقة بين القوة السيبرانية والقوة العسكرية التقليدية، وحول إمكانية اعتبار الفضاء السيبراني مجالًا جديدًا للصراع الدولي. يرى Roguski (2021) أن انتشار القدرات السيبرانية الهجومية بين الدول يفرض تحديات جديدة على الأمن والسلم الدوليين، ويثير الحاجة إلى تطوير قواعد وآليات دولية أكثر فاعلية لتنظيم السلوك في الفضاء السيبراني.

يمكن القول إن الأمن السيبراني تجاوز وظيفته الدفاعية المباشرة ليصبح أحد العوامل التي تؤثر في قدرة الدولة على ممارسة القوة والنفوذ في النظام الدولي، فالدولة التي تمتلك بنية رقمية متطورة دون قدرة كافية على حمايتها قد تصبح عرضة لضغوط وتهديدات تقلل من قدرتها على تحقيق أهدافها الوطنية. بينما يمكن أن يعزز امتلاك قدرات سيبرانية متقدمة قدرتها على حماية بنيتها التحتية، ودعم أدواتها العسكرية والاقتصادية، وتوفير مستوى أعلى من الاستقلال الاستراتيجي. لذلك، أصبح التنافس في المجال السيبراني جزءًا من التنافس الأوسع بين القوى الدولية، وأصبح التفوق في هذا المجال أحد المؤشرات التي يمكن من خلالها قراءة التحولات في توزيع القوة داخل النظام الدولي (حارك وحمدوش، 2022؛ بوغازي، 2025).

في هذا الإطار، تكتسب دراسة الأمن السيبراني كأحد محددات القوة في النظام الدولي المعاصر أهميتها من محاولة فهم التحول الذي حدث في مصادر القوة وأدواتها، وتحديد موقع القدرات السيبرانية ضمن عناصر القوة الوطنية. لا تتعلق المسألة فقط بقدرة الدول على منع الهجمات الإلكترونية، بل تمتد أيضا إلى قدرتها على استخدام الفضاء السيبراني لحماية مصالحها وتعزيز أمنها وممارسة التأثير في البيئة الدولية. تزداد أهمية الموضوع مع التطورات السريعة في الذكاء الاصطناعي والتقنيات الرقمية، التي تفتح مجالات جديدة للدفاع السيبراني وتخلق أنماطا أكثر تعقيدا من التهديدات الرقمية (الخبيزي، 2024).

وعليه، تسعى هذه الدراسة إلى تحليل الأمن السيبراني كأحد المحددات المستجدة للقوة في النظام الدولي المعاصر، من خلال بحث تطور مفهوم القوة، وتوضيح موقع القدرات السيبرانية ضمن مصادر القوة الوطنية، وتحليل تأثير الأمن السيبراني في الأبعاد السياسية والاقتصادية والعسكرية للقوة. كما ستحلل دور الأمن السيبراني في التنافس بين القوى الدولية. تنطلق الدراسة من فرضية أساسية مفادها أن التحول الرقمي لم يغير أدوات الاتصال والعمل فحسب، بل ساهم أيضًا في إعادة تشكيل طبيعة القوة والصراع في النظام الدولي. أصبح امتلاك القدرة على حماية الفضاء السيبراني والسيطرة على بعض موارده واستخدامها جزءًا من عناصر القوة التي يمكن أن تؤثر في مكانة الدولة ونفوذها الدولي.

مشكلة الدراسة وأسئلتها

شَهِدَ النظام الدولي المعاصر تحولا في طبيعة مصادر القوة وأدواتها، فلم تعد القوة تقتصر على القدرات العسكرية والاقتصادية التقليدية، بل أصبحت التكنولوجيا والمعلومات والقدرات الرقمية من العناصر التي تؤثر في قدرة الدول على حماية مصالحها وتحقيق أهدافها الاستراتيجية. في هذا السياق، برز الفضاء السيبراني كحقل جديد للتفاعل والتنافس والصراع الدولي، وأصبح الأمن السيبراني جزءًا أساسيًا من منظومة الأمن الوطني للدول، نظرًا لما تمثله التهديدات السيبرانية من مخاطر على المؤسسات الحكومية والبنية التحتية الحيوية والقطاعات الاقتصادية والعسكرية.

تتمثل الإشكالية في أن التحول نحو البيئة الرقمية أوجد علاقة أكثر تعقيدا بين الأمن السيبراني والقوة الدولية، فامتلاك الدولة لقدرات سيبرانية متقدمة لا يقتصر أثره على حماية أنظمتها وشبكاتها، بل يمكن أن يعزز قدرتها على جمع المعلومات، وحماية بنيتها التحتية، ودعم قدراتها العسكرية، وتقليل تعرضها للضغوط الخارجية، فضلا عن إمكانية استخدام الفضاء السيبراني كأداة للتأثير والمنافسة الدولية. وفي المقابل، يمكن أن يتحول ضعف القدرات السيبرانية إلى مصدر تهديد للأمن الوطني ويحد من قدرة الدولة على ممارسة نفوذها وحماية مصالحها في البيئة الدولية.

تدور مشكلة الدراسة حول ما إذا كان الأمن السيبراني أحد المحددات الجديدة للقوة في النظام الدولي المعاصر، ومدى إسهام امتلاك القدرات السيبرانية وتطويرها في تعزيز القوة والنفوذ والمكانة الدولية للدول. كما تثير هذه الإشكالية تساؤلات أوسع حول ما إذا كانت القوة السيبرانية قد أصبحت مكونًا مستقلًا من مكونات القوة الوطنية، أم أنها تظل أداة داعمة لمصادر القوة العسكرية والاقتصادية والسياسية التقليدية.

وتتمثل مشكلة الدراسة في السؤال الرئيس الآتي:

إلى أي مدى يمثل الأمن السيبراني أحد محددات القوة في النظام الدولي المعاصر، وما مدى تأثير القدرات السيبرانية في القوة والنفوذ والمكانة الدولية للدولة؟

وينبثق عن السؤال الرئيس الأسئلة الفرعية التالية:

1. ما المقصود بالأمن السيبراني، وما أبرز أبعاده في إطار العلاقات الدولية؟
2. كيف تطور مفهوم القوة في النظام الدولي المعاصر في ظل التحولات التكنولوجية والرقمية؟
3. ما موقع القدرات السيبرانية ضمن مصادر القوة الوطنية للدولة؟
4. كيف يسهم الأمن السيبراني في تعزيز القوة السياسية والاقتصادية والعسكرية للدولة؟
5. إلى أي مدى أصبح الفضاء السيبراني مجالًا جديدًا للتنافس والصراع بين الدول؟
6. ما دور القدرات السيبرانية في تعزيز مكانة الدولة ونفوذها داخل النظام الدولي؟
7. ما أبرز التحديات التي تحد من قدرة الدول على توظيف الأمن السيبراني كأداة للقوة والنفوذ الدولي؟
8. هل يمثل التفوق السيبراني مصدرا مستقلًا للقوة، أم أنه يمثل عاملًا مضاعفًا لمصادر القوة التقليدية؟

أهداف الدراسة

في ضوء مشكلة الدراسة وأسئلتها، تهدف هذه الورقة إلى تحليل دور الأمن السيبراني بوصفه أحد المحددات المستجدة للقوة في النظام الدولي المعاصر، وذلك من خلال مجموعة من الأهداف الرئيسة والفرعية، تتمثل فيما يأتي:

تحليل مدى إسهام الأمن السيبراني والقدرات السيبرانية في تشكيل القوة والنفوذ ومكانة الدولة في النظام الدولي المعاصر.

وينبثق من الهدف الرئيس الأهداف الفرعية التالية:

1. توضيح مفهوم الأمن السيبراني وبيان أهم أبعاده وعلاقته بالأمن الوطني والدولي.
2. تحليل تطور مفهوم القوة في العلاقات الدولية في ضوء التحولات التكنولوجية والرقمية التي شهدها النظام الدولي المعاصر.
3. تحديد موقع القدرات السيبرانية ضمن مصادر القوة الوطنية، وبيان مدى ارتباطها بمصادر القوة التقليدية، ولا سيما القوة العسكرية والاقتصادية والسياسية.
4. تحليل دور الأمن السيبراني في تعزيز القوة السياسية للدولة، من خلال حماية المؤسسات والمعلومات والقرار السيادي ومواجهة التدخلات والتهديدات الخارجية.
5. بيان أثر القدرات السيبرانية في القوة الاقتصادية والعسكرية للدولة، ولا سيما في حماية البنية التحتية الحيوية والأنظمة المالية والعسكرية.
6. تحليل الفضاء السيبراني باعتباره مجالًا جديدًا للتنافس والصراع الدولي، وتحديد أبرز الأدوات التي تستخدمها الدول في هذا المجال.
7. دراسة العلاقة بين التفوق السيبراني ومكانة الدولة ونفوذها الدولي، ومدى إمكانية توظيف القدرات السيبرانية لتحقيق أهداف استراتيجية.
8. التعرف إلى أبرز التحديات التي تواجه الدول في بناء قدرات سيبرانية فاعلة، وانعكاسات هذه التحديات على أمنها ومكانتها في النظام الدولي.

أهمية الدراسة

تنبع أهمية الدراسة من التحولات التي طرأت على طبيعة القوة ومصادرها في البيئة الدولية، إذ لم تعد القوة مرتبطة فقط بالقدرات العسكرية والاقتصادية التقليدية، وإنما أصبحت القدرات التكنولوجية والرقمية والسيبرانية من العوامل المؤثرة في قدرة الدول على حماية مصالحها وتعزيز نفوذها ومكانتها الدولية. ويمكن توضيح أهمية الدراسة في جانبين رئيسين:

أولا: الأهمية النظرية

1. الإسهام في إثراء الأدبيات المتعلقة بالعلاقات الدولية والأمن الدولي من خلال تناول الأمن السيبراني باعتباره أحد الأبعاد الحديثة لمفهوم القوة.

2. توسيع مفهوم القوة في العلاقات الدولية من خلال الانتقال من التركيز على مصادر القوة التقليدية، كالقدرة العسكرية والاقتصادية، إلى دراسة الدور الذي تؤديه القدرات السيبرانية والتكنولوجية في تعزيز قوة الدولة.
3. توضيح العلاقة بين الأمن السيبراني والقوة الوطنية، وبيان كيف يمكن للقدرات السيبرانية أن تدعم القوة السياسية والاقتصادية والعسكرية للدولة.
4. الإسهام في فهم الفضاء السيبراني باعتباره مجالًا جديدًا للتنافس الدولي، خاصة في ظل تزايد استخدام الدول للأدوات السيبرانية في التجسس والتأثير والردع والصراع.
5. تقديم أساس نظري لدراسة القوة السيبرانية باعتبارها مفهومًا حديثًا يرتبط بالتغيرات التي يشهدها النظام الدولي والتحول المتزايد نحو الاعتماد على التكنولوجيا والبيانات.
6. فتح المجال أمام دراسات مستقبلية تتناول العلاقة بين الأمن السيبراني ومتغيرات أخرى في العلاقات الدولية، مثل الأمن القومي، والردع، وميزان القوى، والسيادة، والحروب الهجينة.

ثانيا: الأهمية التطبيقية

1. إبراز الأهمية الاستراتيجية للأمن السيبراني بالنسبة للدول، في ظل تزايد اعتماد المؤسسات الحكومية والاقتصادية والعسكرية على البنية التحتية الرقمية.
2. لفت الانتباه إلى أن ضعف القدرات السيبرانية قد يمثل مصدرًا للتهديد الوطني، وليس مجرد مشكلة تقنية، نتيجة إمكانية استهداف المؤسسات والبنية التحتية الحيوية والقطاعات الاقتصادية والعسكرية.
3. المساعدة في فهم أهمية بناء القدرات السيبرانية الوطنية وتطوير الكفاءات البشرية والتقنية القادرة على حماية الدولة من التهديدات السيبرانية.
4. إبراز دور الأمن السيبراني في تعزيز الاستقلال الاستراتيجي للدولة، من خلال تقليل اعتمادها على الأطراف الخارجية في حماية أنظمتها ومعلوماتها وبنيتها الرقمية.
5. توفير مؤشرات يمكن الاستفادة منها عند تقييم القوة الشاملة للدول، بحيث لا يقتصر تقييم القوة على المؤشرات العسكرية والاقتصادية، وإنما يأخذ في الاعتبار مستوى التطور والجاهزية السيبرانية.
6. المساهمة في دعم صانعي القرار في إدراك الأبعاد الاستراتيجية للفضاء السيبراني وضرورة دمج الأمن السيبراني ضمن سياسات الأمن الوطني والخطط الاستراتيجية للدولة.

الإطار النظري

الأمن السيبراني في العلاقات الدولية

أولا: مفهوم الأمن السيبراني وتطوره

يعتبر الأمن السيبراني مفهوما حديثا، حيث ارتبط ظهوره بالتوسع السريع في استخدام الحاسوب وشبكات الاتصالات والإنترنت، وتطورت أهميته مع زيادة اعتماد المؤسسات والدول على الأنظمة الرقمية. لا يقتصر الأمن السيبراني على حماية أجهزة الحاسوب أو منع الاختراقات، بل يشمل سياسات وإجراءات وتقنيات تهدف إلى حماية الأنظمة والشبكات والبيانات والموارد الرقمية من التهديدات التي قد تؤثر على سريتها وسلامتها وتوافرها. يعرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه مجموعة من الأدوات والسياسات والممارسات التي تستخدم لحماية البيئة السيبرانية وأصول المؤسسات والمستخدمين من المخاطر المرتبطة بها (ITU, 2024). هذا التعريف يتماشى مع بعض الأدبيات العربية التي ترى الأمن السيبراني كأحد العناصر الأساسية للمنظومة الأمنية المعاصرة، خاصة مع زيادة الاعتماد على التكنولوجيا وارتفاع التهديدات المستهدفة للمعلومات والبنية التحتية الرقمية (بارة، 2017؛ حارك وحمدوش، 2022؛ الخبيزي، 2024).

ويشير الأمن السيبراني أيضا إلى عملية مستمرة لإدارة المخاطر الرقمية، وليس مجرد مجموعة ثابتة من الوسائل الوقائية. وتتغير التهديدات السيبرانية بتغير التقنيات وأساليب استخدامها. لذلك، يضم الأمن السيبراني الوقاية من الهجمات، واكتشافها، والاستجابة لها، والتعافي من آثارها. كما يتطلب بناء القدرات المؤسسية والقانونية اللازمة للتعامل مع البيئة الرقمية. يؤكد Liebetrau & Monsees (2024) أن التحول الرقمي جعل الأمن السيبراني جزءا هاما من دراسة السياسة العالمية والعلاقات الدولية، إذ لم يعد مجرد مجال تقني متخصص. كما وتوضح بعض الأدبيات الحديثة أن الدراسات السيبرانية انتقلت من التركيز على المخاطر التقنية إلى الاهتمام بالقضايا الاستراتيجية والسياسية والنزاعات الدولية وحوكمة الفضاء السيبراني (Dunn Cavelty et al., 2024؛ Liebetrau & Monsees, 2024).

مر مفهوم الأمن السيبراني بمرحل متتالية ترتبط بتطور التكنولوجيا وزيادة الاعتماد على الفضاء الرقمي. في مراحله الأولى، كان التركيز على أمن الحاسوب وأمن المعلومات، خاصة حماية الأجهزة والبرمجيات والبيانات من الوصول غير المصرح به. ومع انتشار الشبكات والإنترنت في العقود الأخيرة من القرن العشرين، زادت المخاطر لتشمل الشبكات المتصلة، مما جعل من الضروري تضمين وسائل شاملة لحماية المعلومات والاتصالات من الفيروسات والبرمجيات الخبيثة. تشير الأدبيات العربية إلى أن الانتقال إلى الإدارة الإلكترونية وزيادة الاعتماد على الشبكات حول الأمن السيبراني إلى قضية أمنية تتجاوز التقنية، حيث تتصل بالأمن الوطني وحماية البنية التحتية للمعلومات (بارة، 2017؛ بن جدو، 2022).

ومع بداية القرن الحادي والعشرين، اتسع مفهوم الأمن السيبراني أكثر نتيجة اعتماد الدول على البنية التحتية الرقمية في عدة قطاعات مثل الطاقة والاتصالات والمصارف والنقل والصحة والدفاع. أي خلل أو هجوم يستهدف هذه الأنظمة قد يسبب آثارًا تتجاوز فقدان البيانات لتشمل تعطيل الخدمات وتدمير الاقتصاد والأمن. في هذا السياق، برز مفهوم المرونة السيبرانية كامتداد مهم لمفهوم الأمن السيبراني. لم تعد الحماية مقتصرة على منع الهجمات، بل أصبحت تشمل قدرة المؤسسات على الصمود أمام الهجمات واستعادة وظائفها والتعافي من آثارها. بدأ مفهوم المرونة السيبرانية بالظهور بشكل واضح منذ عام 2000، وازدادت أهميته مع تسارع الرقمنة وزيادة الاعتماد على الأنظمة الرقمية (Tzavara & Vassiliadis, 2024).

اليوم، انتقل الأمن السيبراني من كونه مجالا تقنيا لحماية الأنظمة إلى قضية استراتيجية تتعلق بالأمن القومي والعلاقات الدولية، إذ زاد اعتماد الدول على التكنولوجيا الرقمية من جعل الفضاء السيبراني مجالًا للتنافس، وأصبحت القدرات السيبرانية تستخدم في التجسس وجمع المعلومات والتأثير وتعطيل الأنظمة ودعم العمليات العسكرية. يوضح حارك وحمدوش (2022) كيف أثر الفضاء السيبراني على إعادة تشكيل بعض قواعد الهجوم والدفاع، إذ أصبحت رقمنة قطاعات الدولة مصدر قوة وهشاشة أمنية في آن واحد. لقد أصبح الأمن السيبراني مجالا رئيسيا لفهم السياسة الدولية، مع تطور دراسات الصراع السيبراني من الانشغال بالتعريفات والاستراتيجيات إلى دراسة العمليات السيبرانية والفاعلين المرتبطين بها (حارك وحمدوش، 2022؛ Liebetrau & Monsees, 2024؛ Dunn Cavelty et al., 2024).

كما ساهم ظهور الحوسبة السحابية وإنترنت الأشياء والذكاء الاصطناعي في توسيع نطاق الأمن السيبراني وتعقيد التهديدات. ومع تزايد ترابط الأنظمة واعتمادها على البيانات والخدمات الرقمية، تصبح نقاط الضعف المحتملة أكثر اتساعا. يتطلب الأمن السيبراني مزيجا من التدابير التقنية والتنظيمية والقانونية وبناء قدرات بشرية. تظهر هذه الفكرة بوضوح في مؤشر الأمن السيبراني العالمي 2024 من الاتحاد الدولي للاتصالات، الذي يقيس التزام الدول بالأمن السيبراني عبر خمسة مجالات رئيسة: التدابير القانونية، والتدابير التقنية، والتدابير التنظيمية، وتنمية القدرات، والتعاون (ITU, 2024). تعكس هذه التصنيفات انتقال الأمن السيبراني من مفهوم ضيق يركز على حماية الأنظمة إلى مفهوم شامل يتطلب بناء منظومة وطنية متكاملة. درست الأبحاث العربية الحديثة العلاقة بين الأمن السيبراني والذكاء الاصطناعي، مؤكدة أهمية تطوير آليات الحماية بموازاة التطور التقني (الخبيزي، 2024).

بذلك، يمكن القول إن مفهوم الأمن السيبراني انتقل من حماية الحواسيب والمعلومات إلى حماية البيئة الرقمية بشكل شامل، ثم تطور ليصبح أحد مكونات الأمن الوطني للدولة. هذا التطور مهم في سياق الدراسة الحالية، إذ لم يعد الأمن السيبراني قدرة دفاعية تهدف إلى منع الاختراقات فقط، بل أصبح يمثل قوة استراتيجية تستطيع أن تؤثر في نفوذ الدولة. خاصة عندما تمتلك الدولة إمكانيات متقدمة في حماية بنيتها الرقمية وإدارة المخاطر والاستجابة للهجمات واستخدام الفضاء السيبراني لتحقيق أهدافها الوطنية والدولية. يتصل تطور مفهوم الأمن السيبراني مباشرة بموضوع الدراسة، إذ يعتبر الأمن السيبراني أحد المحددات الحديثة للقوة في النظام الدولي المعاصر.

ثانيا: أبعاد الأمن السيبراني

يعتبر الأمن السيبراني مفهومًا متعدد الأبعاد. لا يمكن تحقيقه بالاعتماد فقط على الوسائل التقنية. يتطلب بناء منظومة متكاملة تشمل الأطر القانونية والتنظيمية والتقنية، وتنمية القدرات البشرية، والتعاون بين الأطراف المختلفة. يؤكد الاتحاد الدولي للاتصالات (ITU) (2024) في المؤشر العالمي للأمن السيبراني 2024 أن قياس التزام الدول بالأمن السيبراني يعتمد على خمسة أبعاد رئيسة: التدابير القانونية، والتدابير التقنية، والتدابير التنظيمية، وتنمية القدرات، والتعاون. يعكس هذا التصنيف الطبيعة الشاملة للأمن السيبراني باعتباره مسألة وطنية ودولية تتجاوز حدود الحماية التقنية للأنظمة والشبكات.

1. البعد القانوني والتشريعي

يمثل البعد القانوني أساسا رئيسيا للأمن السيبراني، ويتمثل في وجود منظومة تشريعية وتنظيمية تحدد الحقوق والالتزامات المرتبطة باستخدام الفضاء السيبراني، وتجرم الأفعال غير المشروعة، وتنظم حماية البيانات. وتزداد أهمية هذا البعد بسبب الطبيعة العابرة للحدود للجرائم والهجمات السيبرانية. يتطلب ذلك وجود قوانين وطنية متوافقة مع القواعد والمعايير الدولية، مما يسمح بملاحقة مرتكبي الجرائم السيبرانية والتعاون القضائي بين الدول. يشير الاتحاد الدولي للاتصالات (ITU)

(2024) إلى أن التدابير القانونية تشمل السياسات المتعلقة بالأمن السيبراني والجرائم الإلكترونية وحماية البيانات. يؤكد العوفي (2020) أن التدابير القانونية تمثل إحدى الركائز الأساسية التي اعتمدها الاتحاد الدولي في بناء الأمن السيبراني الوطني.

وتتضمن هذه القوانين سن قوانين خاصة بالجرائم الإلكترونية، وحماية البيانات الشخصية، والإبلاغ عن الاختراقات، وحماية البنية التحتية الحيوية. كما تحدد المسؤوليات القانونية للجهات الحكومية والخاصة. أظهر مؤشر الأمن السيبراني العالمي لعام 2024 أن التدابير القانونية تمثل أقوى ركائز الأمن السيبراني لدى معظم الدول، مما يعكس أهمية البيئة التشريعية في توفير الأساس لبقية مكونات المنظومة السيبرانية (ITU, 2024).

2. البعد التقني

يمثل البعد التقني الجانب المتعلق بالوسائل والأدوات والإجراءات المستخدمة لمنع التهديدات السيبرانية. تشمل هذه الوسائل حماية الشبكات والأنظمة وقواعد البيانات، واستخدام التشفير، وأنظمة كشف ومنع الاختراق، وآليات المصادقة، والنسخ الاحتياطي، وأنظمة الاستجابة للحوادث، بالإضافة إلى تأمين البنية التحتية الرقمية. ويؤكد المعهد الوطني الأمريكي للمعايير والتكنولوجيا (2015) (NIST) أن الأمن السيبراني يتعلق بحماية الأنظمة والاتصالات والمعلومات من الوصول أو الاستخدام أو الكشف أو التعطيل غير المصرح به، مع ضمان الخصائص الأساسية مثل السرية والسلامة والتوافر.

كما ويوضح الاتحاد الدولي للاتصالات (ITU) (2024) أن التدابير التقنية تشمل القدرات الوطنية والقطاعية اللازمة لكشف الحوادث السيبرانية والوقاية منها والاستجابة لها. تشمل هذه التدابير فرق الاستجابة للحوادث الحاسوبية وتطبيق المعايير للأمن السيبراني. تظهر أهمية البعد التقني بشكل خاص في حماية البنية التحتية الحيوية، مثل الطاقة والاتصالات، التي يمكن أن يؤدي اختراقها إلى آثار واسعة على الاقتصاد والأمن الوطنيين.

3. البعد التنظيمي والمؤسسي

لا يمكن تحقيق الأمن السيبراني بفعالية دون وجود هياكل تنظيمية ومؤسسية تحدد المسؤوليات وآليات التنسيق. يشمل هذا البعد وجود استراتيجية وطنية للأمن السيبراني، وهيئات متخصصة، وأطر لإدارة المخاطر، وسياسات واضحة، وتحديد المسؤوليات بين المؤسسات الحكومية والخاصة. يؤكد الاتحاد الدولي للاتصالات (ITU) (2024) أن التدابير التنظيمية ضرورية لتحديد الأهداف الاستراتيجية للدولة ووضع الخطط اللازمة لتنفيذها. تشمل هذه الإجراءات إنشاء الوكالات المسؤولة عن تنفيذ الاستراتيجية الوطنية للأمن السيبراني.

تبرز أهمية البعد المؤسسي في الدراسات العربية، حيث تناول العوفي (2020) التدابير التنظيمية كمكون أساسي للأمن السيبراني، بينما أشار حارك وحمدوش (2022) إلى أن التعامل مع الفضاء السيبراني يتطلب مؤسسات قادرة على إدارة المخاطر وتحقيق الأمن في بيئة رقمية معقدة. لذا، فإن قوة الدولة السيبرانية لا تعتمد فقط على التكنولوجيا، بل ترتبط أيضًا بقدرتها على تنظيم هذه التكنولوجيا وإدارتها ضمن إطار مؤسسي متكامل.

4. بعد تنمية القدرات البشرية والمعرفية

بعد تطوير القدرات البشرية والمعرفية، يعتبر العنصر البشري أحد المكونات الرئيسية للأمن السيبراني، فامتلاك أحدث التقنيات لا يكفي لمواجهة التهديدات إذا كانت الدولة تفتقر إلى الخبرات والمهارات اللازمة لتشغيلها وإدارتها. لذلك، يشمل هذا الجانب التعليم والتدريب والتوعية، وتأهيل المتخصصين، ودعم البحث والتطوير، وتطوير المناهج الأكاديمية، ونشر ثقافة الأمن السيبراني بين أفراد المجتمع. تتضمن تنمية القدرات برامج التوعية العامة، التدريب المهني، الشهادات المتخصصة، المناهج التعليمية، والبحث والتطوير. كل هذه العناصر تلعب دوراً أساسياً في بناء المعرفة والمهارات اللازمة لمواجهة التهديدات الرقمية (ITU. 2024).

تحظى تنمية القدرات بأهمية خاصة لأن التهديدات السيبرانية تتغير باستمرار، مما يجعل تطوير المهارات عملية مستمرة وليست إجراء مؤقتا. كذلك، يمثل الوعي الأمني لدى المستخدمين خط دفاع هام، حيث يرتبط جزء كبير من المخاطر الرقمية بالسلوك البشري، مثل ضعف كلمات المرور، التعامل غير الآمن مع الروابط والملفات، وعدم الالتزام بإجراءات الحماية. لهذا، يُعتبر بناء القدرات البشرية عنصراً مكملًا للتدابير التقنية والقانونية والتنظيمية (الخبيزي، 2024).

5. بعد التعاون والشراكة

بعد التعاون والشراكة، يتطلب الطابع العالمي للفضاء السيبراني تعاونا بين الدول والمؤسسات الحكومية والقطاع الخاص والمؤسسات الأكاديمية والمجتمع المدني، لأن التهديدات السيبرانية لا تتوقف عند الحدود الوطنية. يشمل هذا التعاون تبادل المعلومات والخبرات، والاستجابة للحوادث، والشراكات بين القطاعين العام والخاص، والتنسيق الإقليمي والدولي، والتعاون لمكافحة الجرائم السيبرانية. ويعد الأمن السيبراني مسؤولية مشتركة وتحد عابر للحدود، وأن التعاون وتبادل

المعلومات يمكن أن يعززا قدرات الدول في تقليل المخاطر والتحقيق في الحوادث السيبرانية وملاحقة الجهات الضارة (ITU, 2024).

لقد أصبح التعاون الدولي أكثر أهمية مع تزايد اعتماد الدول على الشبكات العالمية والخدمات الرقمية. قد تستهدف البنية التحتية في دولة معينة، بينما يكون المهاجم أو الخوادم المستخدمة في دول أخرى. لذا، يتطلب فعالية الأمن السيبراني آليات للتنسيق وتبادل المعلومات والخبرات، بالإضافة إلى الاتفاقيات والأطر الدولية التي تساعد في مواجهة التهديدات العابرة للحدود. أظهر المؤشر العالمي للأمن السيبراني (GCI) (2024) أن 166 دولة أبلغت عن مشاركتها في معاهدة دولية أو آلية مماثلة تتعلق بتنمية القدرات السيبرانية أو تبادل المعلومات أو كليهما (ITU, 2024).

6. البعد الأمني والاستراتيجي

يأتي البعد الأمني والاستراتيجي. بالإضافة إلى الأبعاد الخمسة التي يعتمدها المؤشر العالمي للأمن السيبراني في قياس التزام الدول، يمكن إظهار البعد الأمني والاستراتيجي للأمن السيبراني، وهو الأكثر ارتباطًا بموضوع هذه الورقة. يشير هذا البعد إلى انتقال الأمن السيبراني من مجرد حماية تقنية للأنظمة والمعلومات إلى معيار من معايير الأمن الوطني والقوة الاستراتيجية للدولة، إذ ازدادت أهمية حماية البنية التحتية الحيوية، والأنظمة العسكرية، والمؤسسات الحكومية، وشبكات الاتصالات، والقطاع المالي. هذه الجوانب مرتبطة مباشرة بقدرة الدولة على حماية سيادتها ومصالحها الوطنية.

أدى تصاعد الاعتماد على الفضاء السيبراني إلى جعله مجال تنافس بين الدول، حيث تُستخدم القدرات السيبرانية في جمع المعلومات، والتجسس، التأثير، وتعطيل الأنظمة، ودعم العمليات العسكرية. لذلك، يمكن أن يؤثر مستوى القدرات السيبرانية للدولة على قدرتها على الردع والحماية والاستقلال الاستراتيجي. لذا، يُعتبر الأمن السيبراني ذا صلة مباشرة بمفهوم القوة في النظام الدولي المعاصر (حارك وحمدوش، 2022؛ Liebetrau & Monsees, 2024).

تطور مفهوم القوة في النظام الدولي

تطور مفهوم القوة في النظام الدولي ارتبط منذ نشأة العلاقات الدولية الحديثة بقدرة الدولة على تحقيق مصالحها وحماية أمنها والتأثير في سلوك الدول الأخرى. احتلت القوة العسكرية موقعا مركزيا في التصورات التقليدية للقوة، خاصة في الفكر الواقعي الذي ينظر إلى النظام الدولي كبيئة تتسم بغياب سلطة مركزية، مما يدفع الدول للاعتماد على قدراتها الذاتية لضمان بقائها. يؤكد Morgenthau (1948) أن السياسة الدولية، مثل السياسة بشكل عام، تعتمد على مفهوم القوة والمصلحة المرتبطة بها، بينما يرى Waltz (1979) أن توزيع القدرات بين وحدات النظام الدولي يعد عنصرا أساسيا في تفسير سلوك الدول وبنية النظام الدولي. لذلك، ارتبطت القوة في التصور التقليدي ارتباطًا كبيرا بالقدرات العسكرية والاقتصادية وبقدرة الدولة على استخدام هذه الموارد لتحقيق أهدافها في البيئة الدولية.

ومع تطور النظام الدولي بعد الحرب العالمية الثانية، لم يعد تفسير القوة الدولية ممكنًا بالاعتماد على القوة العسكرية فقط. أصبحت القوة الاقتصادية والتكنولوجيا والسياسة ذات أهمية متزايدة في تحديد قدرة الدولة على تحقيق أهدافها. ساهمت التحولات الاقتصادية والتكنولوجية وتزايد الاعتماد المتبادل بين الدول في إعادة النظر في مفهوم القوة. أصبح امتلاك الموارد الاقتصادية والتكنولوجيا، القدرة على التأثير في المؤسسات الدولية، وتكوين التحالفات، من الأدوات التي تستخدمها الدول بجانب القوة العسكرية. في هذا السياق، لا تعني القوة فقط القدرة على إجبار الآخرين على ما لا يريدون، بل تشمل القدرة على جذبهم والتأثير في تفضيلاتهم، مما أدى إلى ظهور مفهوم القوة الناعمة بجانب القوة الصلبة (Nye, 1990؛ Nye, 2004).

لقد مثل مفهوم القوة الناعمة تحولا مهما في دراسة القوة الدولية، حيث ركز على قدرة الدولة على تحقيق النتائج المرغوبة من خلال الجاذبية والإقناع بدلاً من الإكراه أو الدفع بالمكافآت. تشمل مصادر القوة الناعمة الثقافة، القيم، والسياسات الخارجية عندما تكون مقبولة وجذابة للآخرين. لذلك، أصبح نفوذ الدولة مرتبطا بما تمتلكه من موارد مادية، وكذلك بقدرتها على تشكيل التفضيلات والتأثير في تصورات الآخرين. ومع ذلك، لا يعني ذلك تراجع أهمية القوة الصلبة، بل أظهر مفهوم القوة الذكية الذي يجمع بين أدوات القوة الصلبة والناعمة حسب طبيعة الهدف والظروف الدولية (Nye, 2004؛ Wilson, 2008).

لقد أدت التغيرات في النظام الدولي إلى اتساع مفهوم القوة ليشمل أبعادًا اقتصادية، تكنولوجية، ومعلوماتية، بجانب الأبعاد العسكرية والسياسية، إذ ساهمت الثورة المعلوماتية والاتصالية في تعزيز أهمية المعرفة والمعلومات كموردين استراتيجيين يمكن للدول استخدامها لتحقيق مصالحها وتعزيز نفوذها. أصبح التفوق في مجالات التكنولوجيا والاتصالات، بالإضافة إلى القدرة على إنتاج المعرفة وتوظيفها، عوامل تؤثر في مكانة الدولة داخل النظام الدولي (حارك وحمدوش، 2022؛ بوغازي، 2025).

ومع بداية القرن الحادي والعشرين، شهد مفهوم القوة تحولًا إضافيا بفعل الثورة الرقمية وانتشار الإنترنت، إذ ظهر الفضاء السيبراني كمساحة جديدة لممارسة القوة والتنافس الدولي، وأصبحت الدول تعتمد بشكل متزايد على البنية الرقمية في إدارة قطاعاتها الحكومية والاقتصادية والعسكرية، مما يجعل امتلاك التكنولوجيا والقدرة على حماية الأنظمة الرقمية والتحكم في المعلومات عناصر مهمة من عناصر القوة الوطنية. يوضح Nye (2011) أن الفضاء السيبراني لا يلغي أشكال القوة التقليدية، بل يضيف إليها مجالا جديدا يمكن الدول من ممارسة النفوذ وتحقيق أهداف استراتيجية. ترتبط القوة في الفضاء السيبراني بقدرة الفاعل على إنتاج النتائج المرغوبة من خلال الموارد المرتبطة بالشبكات الرقمية.

لقد أدى انتشار القدرات السيبرانية إلى بروز مفهوم القوة السيبرانية، الذي يعكس قدرة الدول على استخدام الموارد المتعلقة بالفضاء السيبراني لتحقيق أهداف سياسية واستراتيجية. لا تقتصر هذه القوة على امتلاك البنية التكنولوجية، بل تشمل القدرة على حماية الأنظمة والشبكات، جمع المعلومات، تنفيذ العمليات السيبرانية، التأثير في الخصوم، وتعزيز المرونة الرقمية. أصبح هذا النوع من القوة جزءًا من التنافس الاستراتيجي بين الدول، خاصة مع تزايد استخدام الفضاء السيبراني في التجسس والتأثير والعمليات العسكرية والصراعات الهجينة (Kello, 2017؛ Lindsay, 2013؛ Nye, 2011).

كما وساهم التطور التكنولوجي في ظهور تصور أكثر تعقيدًا للقوة، يقوم على تكامل مصادر القوة المختلفة بدلا من الفصل بينها. أصبحت القوة العسكرية تعتمد بصورة متزايدة على التكنولوجيا والاتصالات والذكاء الاصطناعي والبيانات، كما ارتبطت القوة الاقتصادية بالبنية الرقمية والأمن السيبراني، وأصبحت القوة السياسية مرتبطة بشكل كبير بالقدرة على إدارة المعلومات والتأثير في البيئة الرقمية. لذلك، لا تعمل القدرات السيبرانية باعتبارها بديلًا عن القوة التقليدية، بل يمكن أن تعزز فعالية الموارد العسكرية والاقتصادية والسياسية المتاحة للدولة (Kello, 2017؛ Lindsay, 2013؛ Nye, 2011).

وفي المرحلة الحالية، أصبح مفهوم القوة أكثر ارتباطا بقدرة الدولة على التحكم في الموارد الرقمية والمعلوماتية، وحماية بنيتها التحتية، وتطوير التكنولوجيا، وتقليل تعرضها للتهديدات السيبرانية، واستخدام القدرات الرقمية لتحقيق أهداف استراتيجية. لذلك، أصبح الأمن السيبراني جزءا من حسابات القوة الوطنية، فالدولة التي تمتلك قدرات رقمية متقدمة دون قدرة على حمايتها قد تكون عرضة للاختراق والتجسس والتعطيل، بينما تعزز الدولة التي تجمع بين التفوق التكنولوجي والقدرة على حماية فضائها السيبراني استقلالها الاستراتيجي ونفوذها الدولي. لم يعد الأمن السيبراني قضية تقنية منفصلة، بل أصبح مرتبطا مباشرة بدراسة القوة والسياسة العالمية والتنافس بين الدول (Dunn Cavelty et al., 2024؛ Liebetrau & Monsees, 2024).

وبناءً على ذلك، يمكن تتبع تطور مفهوم القوة في النظام الدولي بدءا من القوة العسكرية والمادية في التصورات التقليدية، إلى القوة الاقتصادية والتكنولوجية، ثم القوة الناعمة والقوة الذكية، وصولا إلى القوة السيبرانية التي برزت مع التحول الرقمي. لا يعني هذا التطور اختفاء مصادر القوة التقليدية، بل يشير إلى اتساع مفهوم القوة وتزايد ترابط عناصرها، فالدولة الأكثر قدرة على الجمع بين القوة العسكرية والاقتصادية والسياسية والتكنولوجية والسيبرانية تكون أكثر قدرة على حماية مصالحها وممارسة النفوذ في النظام الدولي. ومن هذا المنطلق، يكتسب الأمن السيبراني أهمية خاصة في الدراسة الحالية، ليس فقط كوسيلة لحماية الأنظمة الرقمية، بل كعوامل تعزز القوة الشاملة للدولة وتأثر في مكانتها ونفوذها داخل النظام الدولي المعاصر.

الأمن السيبراني كمحدد للقوة الوطنية

أصبح الأمن السيبراني خلال السنوات الأخيرة جزءا مهما من مفهوم القوة الوطنية. جاء ذلك نتيجة التحول الرقمي الذي شهدته الدول واعتمادها على الأنظمة الرقمية في إدارة مؤسساتها وقطاعاتها الاقتصادية والعسكرية والأمنية. لم تعد قدرات الدولة على تحقيق مصالحها الوطنية تعتمد فقط على الموارد العسكرية والاقتصادية والبشرية، بل أصبحت مرتبطة أيضا بقدرتها على حماية بنيتها الرقمية ومعلوماتها وأنظمتها الحيوية من التهديدات السيبرانية. في هذا السياق، يشير Benson (2022) إلى أن الأمن السيبراني يجب أن ينظر إليه كجزء من القوة الوطنية، وليس مجرد وسيلة لحماية الموارد الأخرى. المعلومات نفسها تمثل مصدر قوة، والأمن السيبراني هو عنصر أساسي في القوة المعلوماتية.

يكتسب الأمن السيبراني أهميته كمحدد للقوة الوطنية لأن الدولة الحديثة تعتمد بشكل كبير على الفضاء الرقمي في أداء وظائفها الأساسية، إذ تعتمد الحكومة، والقطاع المالي، وشبكات الطاقة والاتصالات، والنقل، والصحة، والمؤسسات العسكرية جميعها بدرجات متفاوتة على البنية التحتية الرقمية. لذلك، فإن قدرة الدولة على حماية هذه الأنظمة وضمان استمراريتها تمثل جزءا من قدرتها على تحقيق الأمن والاستقرار وممارسة وظائفها السيادية. يقوم الأمن السيبراني الوطني على مجموعة من القدرات القانونية والتقنية والتنظيمية والبشرية والتعاونية. هذا يعكس انتقال الأمن السيبراني إلى منظومة وطنية متكاملة (ITU, 2024). كما أصبح الأمن السيبراني جزءا من دراسة الأمن الوطني والسياسة الدولية وليس مجالًا تقنيًا منفصلًا عنها (Liebetrau & Monsees, 2024).

وتظهر تأثيرات الأمن السيبراني في القوة السياسية للدولة من خلال قدرته على حماية المؤسسات الحكومية والمعلومات الاستراتيجية والاتصالات الرسمية، وتقليل التدخلات الخارجية ومحاولات التأثير على القرار السياسي. في البيئة الرقمية، يمكن أن تستهدف العمليات السيبرانية المؤسسات الحكومية وقواعد البيانات وشبكات الاتصال بهدف الحصول على معلومات حساسة أو التأثير على صنع القرار أو زعزعة الثقة في المؤسسات. لذلك، أصبحت القدرة على حماية الفضاء المعلوماتي والسيبراني جزءًا من حماية السيادة الوطنية. يشير Özdemir & Karagül (2024) إلى أن التهديدات السيبرانية لم تعد تقتصر على إلحاق الضرر بالبنية التقنية للمؤسسات، بل يمكن أن تشمل أيضًا التأثير والتلاعب بالإدراك، مما يجعل الفضاء السيبراني ميدانًا مهمًا في التنافس على النفوذ السياسي.

كما يرتبط الأمن السيبراني بالقوة الاقتصادية للدولة، فأصبحت الاقتصادات الحديثة تعتمد على الأنظمة الرقمية والشبكات المالية وقواعد البيانات والخدمات الإلكترونية وسلاسل الإمداد الرقمية. لذا، فإن تعرض هذه الأنظمة لهجمات سيبرانية واسعة يمكن أن يؤدي إلى تعطل الأنشطة الاقتصادية وزيادة تكاليف التشغيل وضعف الثقة في المؤسسات وإلحاق أضرار بالبنية التحتية الحيوية. لذلك، يعد الاستثمار في الأمن السيبراني أكثر من مجرد تكلفة دفاعية، بل هو استثمار في حماية القدرة الاقتصادية للدولة واستمرارية نشاطها. في هذا السياق، يتضمن تحليل القوة السيبرانية للدول جوانب تتعلق بالبنية التحتية والقدرات والاعتماد الرقمي، بالإضافة إلى قدرة الدولة على توظيف الفضاء السيبراني لتحقيق أهداف استراتيجية (International Institute for Strategic Studies IISS, 2024).

يمتد تأثير الأمن السيبراني أيضا إلى القوة العسكرية والأمنية، حيث أصبحت العمليات العسكرية الحديثة تعتمد بشكل كبير على نظم الاتصالات والقيادة والسيطرة والاستخبارات والمراقبة والاستطلاع والأنظمة الرقمية. وبذلك، أصبحت حماية هذه الأنظمة من الاختراق أو التعطيل جزءا من القدرة العسكرية للدولة. ويمكن للدول ذات القدرات السيبرانية المتقدمة استخدام الفضاء السيبراني لجمع المعلومات أو التأثير في خصومها أو دعم عملياتها العسكرية. يشير Stevens and Kavanagh 2021)) إلى أن القوة السيبرانية يمكن أن تأخذ أشكالًا متعددة في العلاقات الدولية، بما في ذلك القوة الإكراهية والمؤسسية والبنيوية والإنتاجية. تستخدم الدول علاقاتها بالفاعلين والبنى الموجودة في النظام الدولي لتحقيق أهدافها الاستراتيجية عبر الفضاء السيبراني.

وتتضح العلاقة بين الأمن السيبراني والقوة السيبرانية، فالأمن السيبراني يركز بشكل أساسي على حماية الأنظمة والشبكات والبيانات وإدارة المخاطر والاستجابة للتهديدات، أما القوة السيبرانية فتشير إلى قدرة الدولة أو الفاعل على استغلال الفضاء السيبراني لتحقيق أهداف استراتيجية والتأثير في النتائج السياسية والأمنية. يجب عدم فهم القوة السيبرانية كموارد مادية منفصلة يمكن امتلاكها ببساطة، بل كعلاقات وقدرات يمكن استغلالها لتحقيق أهداف استراتيجية (Stevens and Kavanagh, 2021).

وتبرز أهمية الأمن السيبراني كمحدد للقوة الوطنية عند النظر إلى الاستقلال الاستراتيجي للدولة، فالدولة التي تعتمد بشكل مفرط على تقنيات أو بنى تحتية رقمية خارجية، ولا تمتلك القدرات اللازمة لحمايتها أو إدارة مخاطرها، وقد تكون أكثر عرضة للضغط أو الابتزاز أو التدخل الخارجي. وعلى العكس، فإن امتلاك قدرات وطنية في الأمن السيبراني، وتطوير الخبرات البشرية والتكنولوجية، وتنويع مصادر التكنولوجيا، وحماية البنية التحتية الحيوية يمكن أن تعزز قدرة الدولة على اتخاذ قرارات أكثر استقلالًا. لذا فإن الأمن السيبراني يرتبط بالاستقلال الاستراتيجي كما يرتبط بالأمن الوطني.

كذلك، لا تقتصر أهمية الأمن السيبراني للقوة الوطنية على القدرات الدفاعية، بل ترتبط أيضا بقدرة الدولة على تشكيل البيئة السيبرانية الدولية والتأثير فيها، إذ أن الدول ذات القدرات التكنولوجية والسيبرانية المتقدمة تستطيع المشاركة بفاعلية في وضع المعايير والقواعد الدولية المتعلقة بالفضاء السيبراني، وتطوير الشراكات والتحالفات الرقمية، والمساهمة في صياغة قواعد السلوك الدولي. لا تتعلق القوة السيبرانية بالدول فقط بالعمليات السيبرانية المباشرة، بل تشمل أيضًا القدرة على ممارسة النفوذ في الفضاء السيبراني وعلى المستوى الدولي، بما في ذلك البنية التحتية والقيادة العالمية في الشؤون السيبرانية (IISS, 2024).

عليه، يمكن اعتبار الأمن السيبراني أحد المحددات المتعددة الأبعاد للقوة الوطنية. فهو يدعم القوة السياسية من خلال حماية السيادة والمعلومات والقرار الوطني. كما يدعم القوة الاقتصادية من خلال حماية البنية التحتية والأسواق والخدمات الرقمية، ويساهم في تعزيز القوة العسكرية من خلال حماية نظم القيادة والاتصالات والمعلومات. الدعم للاستقلال الاستراتيجي للدولة والمشاركة في النفوذ في البيئة الدولية يعد جزءًا مهما من الأمن السيبراني. لذلك، أصبح مستوى الأمن السيبراني أحد المؤشرات التي يجب مراعاتها عند تقييم القوة الشاملة للدولة، إلى جانب الموارد العسكرية والاقتصادية والسياسية والتكنولوجية.

في ضوء ذلك، يمكن قول إن الأمن السيبراني لا يمثل بديلا لمصادر القوة التقليدية، بل يعمل كعامل مضاعف لها. تصبح القوة العسكرية المتقدمة أكثر فاعلية عندما تكون أنظمتها الرقمية محمية، فالاقتصاد القوي يصبح أكثر استقرارا عندما تكون بنيته الرقمية آمنة، وتزداد القدرة السياسية عندما تستطيع الدولة حماية معلوماتها ومؤسساتها من الاختراق والتأثير

الخارجي. لذا تكمن أهمية الأمن السيبراني في النظام الدولي الحالي في قدرته على تعزيز مختلف أبعاد القوة الوطنية، وفي الوقت نفسه توفير المجال الذي يمكن للدولة من خلاله استخدام التكنولوجيا والمعلومات لتحقيق أهدافها الاستراتيجية.

الأمن السيبراني والتنافس الدولي

أصبح الأمن السيبراني من المجالات المهمة في التنافس الدولي المعاصر، وجاء ذلك نتيجة للتحول المتزايد نحو الاعتماد على التكنولوجيا والفضاء الرقمي في المجالات السياسية والاقتصادية والعسكرية والأمنية، فلم يعد الفضاء السيبراني مجرد بيئة لتبادل المعلومات والاتصالات. بل أصبح مجالا استراتيجيا تتنافس فيه الدول على امتلاك القدرات التقنية، وحماية بنيتها التحتية الرقمية، وتأمين المعلومات الحساسة، وتعزيز قدرتها على تنفيذ العمليات السيبرانية والدفاع عنها. كما أصبحت القوة السيبرانية جزءا من العلاقات الدولية. أصبح تأثيرها مرتبطا بالقدرات التقنية والعلاقات والهياكل التي يمكن للفاعلين استخدامها لتحقيق أهداف سياسية واستراتيجية. وقد أضاف الفضاء السيبراني مجالا جديدا لممارسة القوة دون أن يلغى مصادر القوة التقليدية (Kavanagh & Stevens, 2021؛ Nye, 2011).

ويتخذ التنافس الدولي في المجال السيبراني عدة أشكال، يأتي في مقدمتها التجسس السيبراني وجمع المعلومات الاستراتيجية، إذ أصبحت القدرات الرقمية وسيلة للحصول على معلومات تتعلق بالسياسات الحكومية والقدرات العسكرية والبرامج الاقتصادية والتكنولوجية للدول المنافسة. توفر العمليات السيبرانية إمكانية الوصول إلى معلومات حساسة دون الحاجة إلى استخدام القوة العسكرية التقليدية، مما يجعل منها أداة مهمة في تحقيق بعض الأهداف الاستراتيجية. ولكن تظل فعاليتها مرتبطة بالسياق السياسي والعسكري والقيود التقنية والاستراتيجية التي تواجه الدول (Kello, 2017؛ Lindsay, 2013).

يظهر التنافس الدولي أيضا في استهداف البنية التحتية الحيوية والقطاعات الاقتصادية والاستراتيجية. تشمل هذه القطاعات شبكات الطاقة والمصارف والاتصالات والنقل والصحة والمؤسسات الحكومية. ويؤدي الاعتماد المتزايد على الأنظمة الرقمية إلى زيادة احتمالات تعرض هذه القطاعات للهجمات السيبرانية، وقد ينتج عن ذلك تعطيل الخدمات وإلحاق خسائر اقتصادية وأمنية وسياسية. لذلك، أصبحت حماية البنية التحتية الرقمية وتعزيز القدرة على اكتشاف الحوادث السيبرانية والاستجابة لها والتعافي من آثارها من العناصر الأساسية في بناء الأمن السيبراني الوطني (International Telecommunication Union [ITU], 2024؛ Kello, 2017).

ولا يقتصر التنافس الدولي في الفضاء السيبراني على العمليات الهجومية والدفاعية، بل يمتد أيضا إلى التنافس على التكنولوجيا والمعايير والقواعد التي تنظم الفضاء السيبراني، إذ تسعى الدول ذات القدرات التكنولوجية المتقدمة إلى تعزيز دورها في صياغة المعايير التقنية والقواعد الدولية المتعلقة باستخدام الفضاء السيبراني، ويساعد ذلك في حماية مصالحها وتعزيز نفوذها في البيئة الرقمية العالمية. يرتبط النفوذ السيبراني بالقدرة على التأثير في المؤسسات الدولية والتحالفات التكنولوجية والبنية التحتية الرقمية وسلاسل الإمداد المرتبطة بالتكنولوجيا. بذلك، تصبح القوة السيبرانية ذات أبعاد مؤسسية وبنيوية تتجاوز الاستخدام المباشر للهجمات الإلكترونية (Kavanagh & Stevens, 2021؛ International Institute for Strategic Studies [IISS], 2024).

لقد أدى تصاعد التنافس في المجال السيبراني إلى ظهور مفهوم الردع السيبراني، ويعتمد هذا المفهوم على محاولة منع الخصوم من تنفيذ عمليات سيبرانية ضارة من خلال امتلاك قدرات دفاعية وهجومية، ورفع تكلفة الهجمات المحتملة، وإظهار القدرة على اكتشاف الاعتداءات والاستجابة لها. يواجه الردع السيبراني مجموعة من التحديات. من أبرزها صعوبة تحديد هوية المهاجم، وإمكانية استخدام جهات غير حكومية أو وكلاء لتنفيذ العمليات، وصعوبة تقدير طبيعة الأضرار المحتملة، بالإضافة إلى انخفاض تكلفة تنفيذ بعض الهجمات مقارنة بالعمليات العسكرية التقليدية (Kello, 2017؛ بوغازي، 2025).

يرتبط التنافس السيبراني أيضا بزيادة الصراعات الهجينة، إذ يمكن دمج العمليات السيبرانية مع الأدوات الاقتصادية والإعلامية والسياسية والعسكرية لتحقيق أهداف استراتيجية. وأصبح من الممكن استخدام الهجمات السيبرانية جنبا إلى جنب مع حملات التضليل والتأثير المعلوماتي والضغوط الاقتصادية والعمليات العسكرية. وقد أدى ذلك إلى زيادة تعقيد الحدود بين الحرب والسلام، وأيضا بين الوسائل العسكرية وغير العسكرية. تطورت دراسة الصراع السيبراني من التركيز على الجوانب التقنية للهجمات إلى الاهتمام بالفاعلين والدوافع السياسية والاستراتيجية، وكذلك الآثار المترتبة على العمليات السيبرانية في العلاقات الدولية (Dunn Cavelty, Pulver, & Smeets, 2024؛ Kello, 2017).

في المقابل، أدت زيادة التنافس السيبراني إلى تعزيز التعاون الدولي والتحالفات السيبرانية، ويعود ذلك إلى الطبيعة العابرة للحدود للتهديدات الرقمية وصعوبة مواجهتها بالاعتماد على القدرات الوطنية فقط. يشمل التعاون السيبراني تبادل المعلومات والخبرات، والاستجابة المشتركة للحوادث، وتطوير القدرات الوطنية، والتنسيق بين المؤسسات الحكومية والقطاع الخاص، بالإضافة إلى المشاركة في وضع القواعد والمعايير الدولية المتعلقة بالسلوك المسؤول في الفضاء السيبراني. لقد أصبح التعاون الدولي جزءا أساسيا من بناء القدرات السيبرانية الوطنية وتعزيز القدرة على مواجهة المخاطر الرقمية المشتركة (Liebetrau & Monsees, 2024 ؛ITU, 2024).

لقد ارتبط الأمن السيبراني بصورة مباشرة بالأمن القومي والسيادة الوطنية، يعود ذلك إلى اعتماد الدول على البنية الرقمية في إدارة مؤسساتها وخدماتها الأساسية وقطاعاتها الاقتصادية والعسكرية. يؤدي ضعف الحماية السيبرانية إلى زيادة تعرض الدولة للتجسس والتخريب وسرقة المعلومات والتدخل الخارجي. بينما يؤدي تطوير القدرات السيبرانية إلى تعزيز قدرة الدولة على حماية بنيتها التحتية ومعلوماتها الحساسة واستمرارية وظائفها الأساسية. أصبح مستوى الجاهزية السيبرانية جزءًا من تقييم قدرة الدولة على حماية مصالحها الوطنية والحفاظ على استقلالها الاستراتيجي (ITU, 2024؛ Liebetrau & Monsees, 2024).

من جهته، يكشف التنافس الدولي في الفضاء السيبراني عن تحول مهم في طبيعة القوة في النظام الدولي المعاصر، إذ أصبحت القدرة على امتلاك التكنولوجيا والمعلومات وحمايتها واستخدامها عنصرا مؤثرا في مكانة الدولة ونفوذها، ولم تعد القوة مرتبطة فقط بحجم القوات المسلحة أو الموارد الاقتصادية، بل شملت أيضا القدرة على حماية الأنظمة الرقمية، وتطوير القدرات السيبرانية، وإدارة المخاطر الرقمية، والتأثير في البيئة السيبرانية الدولية. بذلك، أصبح الأمن السيبراني أحد العوامل التي يمكن أن تعزز القوة الوطنية، خاصة عندما تتكامل القدرات السيبرانية مع القدرات العسكرية والاقتصادية والسياسية والتكنولوجية (Nye, 2011؛ Kavanagh & Stevens, 2021؛ IISS, 2024).

بناء على ذلك، يمكن رؤية الأمن السيبراني والتنافس الدولي كظاهرتين مترابطتين في النظام الدولي المعاصر. فكلما زاد اعتماد الدول على الفضاء الرقمي، ازدادت أهمية حماية هذا الفضاء. في الوقت نفسه، تزداد فرص استخدامه في المنافسة والصراع والتأثير. الأمن السيبراني لا يمثل بديلًا عن مصادر القوة التقليدية. بل يعمل بشكل متزايد كعامل مضاعف للقوة الوطنية، بحيث يمكن للدولة ذات القدرات السيبرانية المتقدمة أن تحمي مواردها الأخرى، وتحد من نقاط ضعفها، وتعزز قدرتها على مواجهة الضغوط الخارجية والمنافسة في البيئة الدولية (Kavanagh & Stevens, 2021؛ Dunn Cavelty et al., 2024؛ ITU, 2024).

تحديات الأمن السيبراني وانعكاساتها على النظام الدولي

أصبح الأمن السيبراني يواجه مجموعة متزايدة من التحديات بسبب التطور السريع للتكنولوجيا وزيادة الاعتماد على الفضاء الرقمي في إدارة شؤون الدول والمجتمعات، فلم تعد التهديدات السيبرانية تقتصر على اختراق أجهزة الحاسوب أو سرقة البيانات، بل امتدت إلى استهداف البنية التحتية الحيوية، والتجسس، والابتزاز الرقمي، والتلاعب بالمعلومات، وتعطيل الخدمات الأساسية. ويزداد تعقيد هذه التحديات بسبب سرعة تطور الأدوات المستخدمة في تنفيذ الهجمات، وعدم وضوح الفاعلين المشاركين، وصعوبة تحديد المصادر بدقة. لذلك، أصبحت قضايا الأمن السيبراني تتجاوز المستوى التقني إلى المستويات السياسية والأمنية والاقتصادية الدولية. (International Telecommunication Union [ITU], 2024؛ Liebetrau & Monsees, 2024).

1. تطور التهديدات السيبرانية وتعقدها

يعتبر التطور المستمر للتهديدات الرقمية واحدا من أبرز تحديات الأمن السيبراني، إذ أصبحت الهجمات أكثر تنوعا وتعقيدا، وتشمل البرمجيات الخبيثة، وبرامج الفدية، وهجمات حجب الخدمة، والتصيد الإلكتروني، واختراق سلاسل الإمداد، واستغلال الثغرات في الأنظمة الرقمية. لقد أدى انتشار الحوسبة السحابية وإنترنت الأشياء والذكاء الاصطناعي إلى زيادة نقاط الضعف، بحيث أصبحت موزعة على عدد كبير من الأنظمة والأجهزة المتصلة. يصعب بناء دفاعات ثابتة لأن طبيعة التهديدات تتغير باستمرار. يتطلب ذلك تحديث القدرات التقنية والمؤسسية بشكل متواصل (ITU, 2024؛ NIST, 2024).

2. صعوبة تحديد هوية المهاجم

تمثل مشكلة تحديد هوية المهاجم أحد أهم التحديات في العلاقات الدولية، إذ يصعب كثيرا في الحالات تحديد الجهة المسؤولة عن تنفيذ الهجوم بدقة، كما يمكن للمهاجمين استخدام خوادم في دول مختلفة، أو الاستعانة بجهات وسيطة، أو استخدام أدوات مصممة لإخفاء مصدر العملية. وتؤدي هذه المشكلة إلى تعقيد عملية اتخاذ القرار السياسي، خاصة عندما تفكر الدولة

المستهدفة في الرد على الهجوم. توجيه رد ضد الجهة الخطأ قد يؤدي إلى تصعيد غير مقصود في العلاقات الدولية (Rid & Buchanan, 2015؛ Kello, 2017).

3. استهداف البنية التحتية الحيوية

أدى الاعتماد المتزايد على الأنظمة الرقمية إلى جعل البنية التحتية الحيوية من أهم أهداف الهجمات السيبرانية، وتشمل قطاعات الطاقة والمياه والاتصالات والمصارف والنقل والصحة والمؤسسات الحكومية. يمكن أن يؤثر نجاح هجوم واسع على هذه القطاعات على الخدمات الأساسية، كما وقد يسبب خسائر اقتصادية، وزيادة حالة عدم الاستقرار الداخلي. وقد يصبح استهداف البنية التحتية الحيوية أداة ضغط سياسي أو استراتيجي، خاصة في حالة النزاعات بين الدول. لذلك، أصبحت حماية هذه البنية جزءًا أساسيًا من الأمن الوطني للدول واستقرار النظام الدولي (ITU, 2024؛ Kello, 2017).

4. تصاعد الجرائم السيبرانية والابتزاز الرقمي

تعتبر الجرائم السيبرانية تحديا آخر بسبب سهولة استهداف الأفراد والمؤسسات عبر الحدود، وتشمل أساليب متنوعة بهدف الحصول على الأموال أو المعلومات. وتتضمن هذه الجرائم الاحتيال الإلكتروني، وسرقة الهوية، وبرامج الفدية، وسرقة البيانات، والابتزاز الرقمي. كما ويتم استغلال المنصات الرقمية في أنشطة غير مشروعة. وتزيد صعوبة مكافحة هذه الجرائم بسبب اختلاف التشريعات الوطنية وكثرة الاختصاصات القضائية، فيمكن أن يوجد الجاني والبنية التقنية المستخدمة في تنفيذ الجريمة في دول مختلفة. لذلك، تتطلب مكافحة الجرائم السيبرانية مستويات متقدمة من التعاون الدولي وتبادل المعلومات (ITU, 2024؛ UNODC, 2021).

5. استخدام الذكاء الاصطناعي في الهجمات السيبرانية

أدى التطور السريع في الذكاء الاصطناعي إلى إضافة تحديات جديدة للأمن السيبراني`K Y يمكن استخدام تكنولوجيا الذكاء الاصطناعي لتحسين اكتشاف التهديدات والدفاع عنهاK لكنها قد تستغل أيضا في تطوير الهجمات الإلكترونية، وأتمتة عمليات الهجوم، وإنشاء محتوى احتيالي أكثر إقناعا، وتطوير أساليب التصيد. يؤدي هذا إلى زيادة سرعة التهديدات وقدرتها على التكيف، ويستوجب ذلك من الدول والمؤسسات تطوير آليات دفاع أكثر تقدما وقدرة على الاستجابة السريعة. (NIST, 2024؛ ITU, 2024)

6. التهديدات المرتبطة بالمعلومات والتضليل

لم يعد الفضاء السيبراني مجالا للهجمات التقنية فقط، بل أصبح وسيلة للتأثير في المعلومات والإدراك العام، إذ يمكن استخدام المنصات الرقمية لنشر المعلومات المضللة، والتلاعب بالمحتوى، والتأثير في الرأي العام، وزيادة الاستقطاب السياسي والاجتماعي. وتزداد خطورة هذه الممارسات خلال الأزمات السياسية أو الانتخابات أو الصراعات، وقد تستهدف هذه الممارسات الثقة بالمؤسسات الحكومية والإعلامية، وتؤثر في تصورات الجمهور تجاه الأحداث. لذا، أصبح الأمن السيبراني مرتبطا بشكل متزايد بأمن المعلومات وبسلامة البيئة المعلوماتية التي تعمل فيها الدول والمجتمعات (Nye, 2011؛ Dunn Cavelty, Pulver, & Smeets, 2024).

7. نقص الكفاءات والقدرات السيبرانية

يمثل نقص المتخصصين في مجال الأمن السيبراني أحد التحديات الأساسية، إذ تتفاوت مستويات القدرات التقنية بين الدول. تمتلك بعض الدول موارد مالية وتكنولوجية تمكنها من تطوير أنظمة دفاعية متقدمة، بينما تواجه دول أخرى صعوبات في بناء بنية تحتية وتأهيل الكوادر وتوفير الموارد. يؤدي هذا التفاوت إلى حدوث فجوة رقمية وأمنية بين الدول، وقد يزيد ذلك من تعرض الدول ذات القدرات المحدودة للتهديدات (ITU, 2024؛ World Economic Forum, 2024)

8. ضعف الأطر القانونية والقواعد الدولية

يمثل التفاوت في التشريعات الوطنية وغياب قواعد دولية شاملة بشأن السلوك السيبراني تحديا في إدارة الفضاء السيبراني الدولي. ويختلف القانون حول الجرائم الإلكترونية وحماية البيانات، مما يجعل من تعقب بعض الجرائم العابرة للحدود أكثر تعقيدا. كما أن سرعة تطور التكنولوجيا تسبق أحيانا قدرة التشريعات على التكيف، يحدث ذلك نتيجة وجود فجوات قانونية تستغل من قبل الفاعلين السيبرانيين، وتظهر هذه المشكلة بشكل خاص عندما تتداخل العمليات السيبرانية مع قضايا الأمن الدولي (United Nations, 2021؛ Kello, 2017).

9. انعكاسات الأمن السيبراني على سيادة الدولة

أدى انتشار التهديدات السيبرانية إلى طرح مفهوم السيادة الوطنية في البيئة الرقمية، وأصبح بالإمكان الوصول إلى أنظمة الدولة ومعلوماتها، أو التأثير في بنيتها التحتية من خارج حدودها. كما وتحد هذه الطبيعة العابرة للحدود من قدرة الدول على السيطرة على الأنشطة الرقمية، ويتطلب ذلك إعادة التفكير في كيفية حماية السيادة في ظل وجود بنية تحتية وشبكات تعتمد على أطراف دولية متعددة. لقد أصبح الأمن السيبراني مرتبطًا بشكل مباشر بقدرة الدولة على حماية استقلالها ومصالحها الوطنية في بيئة مترابطة رقميا (Kavanagh & Stevens, 2021؛ Liebetrau & Monsees, 2024).

10. انعكاسات الأمن السيبراني على الاستقرار والتوازن الدولي

تؤثر التهديدات السيبرانية في استقرار النظام الدولي، وتزيد من احتمالات سوء التقدير والتصعيد بين الدول، خاصة عندما ترتبط العمليات بأهداف سياسية أو عسكرية. وتعد صعوبة تحديد المسؤول عن الهجوم، وعدم وضوح حدود الرد المشروع، وإمكانية تنفيذ عمليات مؤثرة دون إعلان حرب تقليدية جميعها عوامل قد تزيد من تعقيد إدارة الأزمات الدولية، كما قد يؤدي التنافس على القدرات السيبرانية إلى سباق تكنولوجي بين الدول، ويعزز ذلك منطق الردع المتبادل، ويضيف بعدا جديدا إلى التوازنات الاستراتيجية الدولية (Kello, 2017؛ Nye, 2011؛ Lindsay, 2013).

11. اتساع الفجوة السيبرانية بين الدول

لقد أدى التفاوت في الموارد والقدرات التقنية إلى ظهور فجوة سيبرانية دولية، إذ تتمتع بعض القوى الكبرى بقدرات متقدمة في التكنولوجيا والبحث والاستخبارات السيبرانية، بينما تواجه دول أخرى صعوبات في بناء أنظمة حماية فعالة، ولا يقتصر أثر هذه الفجوة على الجانب التقني فقط، بل يمكن أن يمتد إلى توزيع القوة والنفوذ في النظام الدولي، إذ أصبحت التكنولوجيا والقدرات السيبرانية عوامل مؤثرة في الاستقلال الاستراتيجي وحماية المصالح الوطنية (ITU, 2024؛ International Institute for Strategic Studies [IISS], 2024).

انعكاسات هذه التحديات على النظام الدولي

تؤدي تحديات الأمن السيبراني إلى تغييرات في طبيعة النظام الدولي، بعد أن أصبح الفضاء السيبراني ساحة جديدة للتنافس والصراع والتعاون. عمل ذلك على توسيع مفهوم الأمن الدولي ليشمل حماية البنية الرقمية والمعلومات والأنظمة الحيوية، كما أدى إلى ظهور أنماط جديدة من القوة والردع والصراع التي لا تعتمد بالضرورة على الاستخدام المباشر للقوة العسكرية. لقد أصبح التفوق التكنولوجي والسيبراني عاملا مهما في مكانة الدول وقدرتها على حماية مصالحها والتأثير في الآخرين، مما يسهم في إعادة تشكيل بعض عناصر توزيع القوة في النظام الدولي المعاصر.

وبناء على ذلك، ينبغي النظر إلى تحديات الأمن السيبراني كأزمات استراتيجية ذات أبعاد سياسية واقتصادية وأمنية وقانونية، فكلما زاد اعتماد الدول على التكنولوجيا والفضاء الرقمي، أصبحت قدرتها على حماية بنيتها الرقمية جزءاً من قدرتها على حماية أمنها القومي واستقلالها ومصالحها الاقتصادية والسياسية. من هنا، يتطلب التعامل مع هذه التحديات تطوير القدرات الوطنية وتعزيز التعاون الدولي وتحديث الأطر القانونية وتنمية الموارد البشرية وبناء آليات فعالة للردع والاستجابة، مما يساعد في تقليل المخاطر السيبرانية والحفاظ على استقرار النظام الدولي.

الدراسات السابقة

1. دراسة إبراهيم (2025) بعنوان: فاعلية الأمن السيبراني في المحافظة على السيادة الوطنية: دراسة وصفية تحليلية.

هدفت الدراسة إلى التعرف إلى الضوابط المرتبطة بالأمن السيبراني، وكشف الثغرات والتحديات التي يمكن أن تؤثر في فاعليته وفي قدرة الدولة على المحافظة على سيادتها الوطنية في ظل التحولات العالمية السريعة. اعتمدت الدراسة على المنهج الوصفي والتاريخي والتحليلي لتحليل مفهوم الأمن السيبراني، والتحديات التي تواجهه، وعلاقته بالسيادة الوطنية والأمن الإنساني. لم تعتمد على عينة ميدانية من الأفراد، بل قامت بتحليل الأدبيات والمصادر والمفاهيم والضوابط المرتبطة بالأمن السيبراني والسيادة الوطنية. توصلت الدراسة إلى أن الأمن السيبراني يرتبط ارتباطاً وثيقاً بالسيادة الوطنية. حماية الدولة في البيئة الرقمية تتطلب وضع ضوابط أمنية صارمة لمواجهة الثغرات والتهديدات السيبرانية. كما بينت أن المتغيرات الدولية والتطورات التقنية تفرض على الدول مراجعة منظوماتها القانونية والأمنية بشكل مستمر. أوصت الدراسة بالالتزام بالمتطلبات الأساسية التي تسهم في تحقيق السيادة الوطنية، ومراجعة القوانين والتشريعات المتعلقة بالأمن السيبراني بما يتماشى مع المتغيرات الدولية، وتعزيز احترام سيادة الدول في الفضاء السيبراني.

2. دراسة الرفيعي (2025) بعنوان: الأمن السيبراني وتأثيره في مستقبل الهيمنة الأمريكية. مجلة تكريت للعلوم السياسية.

هدفت الدراسة إلى تحليل دور الأمن السيبراني في الاستراتيجية الأمريكية، وبيان مدى مساهمة القدرات السيبرانية والتقنيات الحديثة، ولا سيما الذكاء الاصطناعي، في تعزيز القدرة الأمريكية لتحقيق أهدافها الاستراتيجية. اعتمدت الدراسة على المنهج الوصفي التحليلي لتحليل التحولات والتهديدات السيبرانية والاستراتيجية الأمريكية في هذا المجال. لم تعتمد على عينة بشرية، بل استندت إلى الأدبيات والمصادر والوثائق المتعلقة بالأمن السيبراني والاستراتيجية الأمريكية. توصلت الدراسة إلى أن القدرات التي تمتلكها الولايات المتحدة في مجال الأمن السيبراني تمثل مرتكزًا مهمًا في تنفيذ استراتيجيتها للأمن القومي. الذكاء الاصطناعي أصبح عنصراً مهماً في تطوير القدرات السيبرانية والحرب الإلكترونية، مما يعزز قدرة الولايات المتحدة على التأثير والمنافسة وتحقيق أهدافها الاستراتيجية. أوصت الدراسة بضرورة الاهتمام بتطوير القدرات السيبرانية

والتكنولوجية باعتبارها أحد مصادر القوة الحديثة، وتعزيز توظيف التقنيات المتقدمة في حماية الأمن القومي ومواجهة التهديدات السيبرانية.

3. دراسة راضي (2025) بعنوان: فاعلية الأمن السيبراني في السياسة العالمية (المفهوم والتدابير الأمنية للدول).

هدفت الدراسة إلى دراسة مفهوم الأمن السيبراني وبيان أهميته في السياسة العالمية، مع التعرف على التدابير التي تتخذها الدول لتعزيز أمنها السيبراني ومواجهة المخاطر والتهديدات التي يفرضها الفضاء السيبراني. اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال تحليل مفهوم الأمن السيبراني وأبعاده ودوره في السياسة العالمية. لم تعتمد على عينة ميدانية، بل ركزت على الأدبيات والمصادر المتعلقة بالأمن السيبراني والسياسة الدولية. توصلت الدراسة إلى أن الأمن السيبراني أصبح عنصرا مؤثرا في العلاقات والسياسة العالمية. حماية الفضاء السيبراني تتطلب تطوير القدرات الوطنية وتعزيز التعاون الدولي، إلى جانب تبني تدابير أمنية وقائية لمواجهة التهديدات المتزايدة. أوصت الدراسة بزيادة الاهتمام بالأمن السيبراني على المستوى الوطني والدولي، وتعزيز التعاون بين الدول وتبادل الخبرات والمعلومات لمواجهة التهديدات السيبرانية

4. دراسة بن جدو وبوصبع (2024) بعنوان: أثر سياسات الأمن السيبراني على الأمن القومي الأمريكي: قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائرية

هدفت إلى تحديد العلاقة بين سياسات الأمن السيبراني والأمن القومي، من خلال دراسة التجربة الأمريكية في هذا المجال، والبحث في إمكانية الاستفادة منها وتطبيقها في الحالة الجزائرية. اعتمدت الدراسة على المنهج الوصفي التحليلي ودراسة الحالة، مع التركيز على التجربة الأمريكية وتحليل السياسات السيبرانية التي اتبعتها الولايات المتحدة. استندت الدراسة إلى التجربة والسياسات والوثائق والمصادر ذات الصلة بالأمن السيبراني والأمن القومي، وتوصلت إلى أن التجربة الأمريكية تقوم في مجال الأمن السيبراني على ثلاثة مرتكزات رئيسية: الأطر القانونية والمؤسساتية، تطوير الصناعات التقنية المحلية، الاندماج في منظومة الأمن السيبراني الدولي. خلصت الدراسة إلى إمكانية الاستفادة من هذه التجربة في تعزيز الأمن السيبراني الجزائري في مواجهة التهديدات المتزايدة. أوصت بالاستفادة من التجربة الأمريكية في بناء منظومة وطنية متكاملة للأمن السيبراني، وتطوير الأطر القانونية والمؤسساتية والصناعات التقنية المحلية وتعزيز التعاون الدولي.

5. دراسة Akdağ (2025) بعنوان: Great Power Cyberpolitics and Global Cyberhegemony.

هدفت الدراسة إلى اختبار قدرة نظرية الواقعية الهجومية على تفسير سعي القوى الكبرى لتعزيز قوتها وهيمنتها في الفضاء السيبراني. كما عملت على تحليل العلاقة بين الأمن القومي والأمن السيبراني والقوة السيبرانية في العلاقات الدولية، مع التركيز على إمكانية انتقال الهيمنة من المستوى الإقليمي إلى المستوى العالمي في البيئة السيبرانية. اعتمدت الدراسة على المنهج التحليلي ودراسة الحالة الحاسمة، واختارت الولايات المتحدة كحالة للدراسة لارتباطها الوثيق بافتراضات الواقعية الهجومية. كما قامت بتحليل السياسات والاستراتيجيات السيبرانية الأمريكية الرئيسة بين عامي 2003 و2023. توصلت الدراسة إلى أن الواقعية الهجومية تمتلك قدرة تفسيرية وتنبؤية مهمة في الفضاء السيبراني، لكنها تحتاج إلى تعديل بعض افتراضاتها المتعلقة بنطاق الهيمنة. كما خلصت إلى أن الولايات المتحدة تسعى إلى هيمنة سيبرانية عالمية وليس إقليمية من خلال استراتيجيات هجومية تهدف إلى تعزيز قوتها السيبرانية وتحقيق الأمن السيبراني. بينت أن طبيعة الفضاء السيبراني العابرة للحدود وانخفاض تكلفة إسقاط القوة فيه يختلفان عن القيود الجغرافية والمادية التي تواجه القوة التقليدية. أوصت الدراسة بتعديل مفهوم الواقعية الهجومية ليتناسب مع واقع الفضاء السيبراني وتطوير إطار مفاهيمي خاص بالهيمنة السيبرانية، مما يمكن أن يسهم في بناء صيغة أكثر ملاءمة من الواقعية الهجومية لدراسة القوة والسياسة السيبرانية وصنع السياسات.

6. دراسة Czerwińska (2025) بعنوان: Geopolitics of Cybersecurity – International Power Dynamics and State Security in Cyberspace

هدفت الدراسة إلى تحليل العلاقة بين الجغرافيا السياسية والأمن السيبراني في سياق ديناميكيات القوة الدولية، والكشف عن تأثير التهديدات السيبرانية في الأمن القومي للدول، مع التركيز على كيفية تحول التوترات الجيوسياسية إلى عمليات وأنشطة في الفضاء السيبراني، والاستراتيجيات التي تتبعها الدول لبناء قدرتها على الصمود السيبراني. اعتمدت

الدراسة على منهج المراجعة المنهجية للأدبيات والتحليل المقارن لاستراتيجيات الأمن السيبراني لدى دول أعضاء في حلف شمال الأطلسي (NATO) والاتحاد الأوروبي (EU). كما استخدمت تحليل مضمون الوثائق الاستراتيجية وتقارير الأمن ودراسات الحالة المتعلقة بالهجمات السيبرانية التي استهدفت البنية التحتية الحيوية. توصلت الدراسة إلى أن الفضاء السيبراني أصبح مجالاً رئيسياً للتنافس الجيوسياسي، وأن التوترات الدولية تؤدي إلى زيادة الأنشطة السيبرانية التي تنفذها الجهات التابعة للدول، ولا سيما روسيا والصين وإيران وكوريا الشمالية. أوصت الدراسة بتطوير الاستراتيجيات الوطنية للأمن السيبراني، وتعزيز حماية البنية التحتية الحيوية، وتوسيع التعاون الدولي في مجال الدفاع السيبراني، وتطوير آليات أكثر فعالية لمواجهة التهديدات. كما دعت إلى دعم التعليم والتدريب المتخصص في الأمن السيبراني وتعزيز دوره في الدبلوماسية وإدارة المخاطر الجيوسياسية.

7. دراسة Dunn وآخرون (2024) بعنوان: The Evolution of Cyberconflict Studies.

هدفت الدراسة إلى تحليل تطور حقل الدراسات المتعلقة بالصراع السيبراني، والتعرف إلى خصائصه واتجاهاته المفاهيمية والمنهجية، كما بينت ما تعنيه هذه التطورات بالنسبة للعلاقة بين البحث العلمي وصنع السياسات في مجال الأمن السيبراني. اعتمدت الدراسة على المنهج التحليلي الببليومتري والمراجعة المنهجية للأدبيات، من خلال تحليل الدراسات المنشورة في أبرز مجلات العلوم السياسية والعلاقات الدولية. اختار الباحثون 125 مجلة وفق تصنيف SCImago لعام 2022، واستخدموا قاعدة بيانات Scopus لحصر الدراسات المنشورة حتى ديسمبر 2022. أسفر البحث الأولي عن 345 مقالًا، وبعد تطبيق معايير الاستبعاد والتنقيح اليدوي استقر corpus الدراسة النهائي على 174 مقالًا منشورًا في 44 مجلة. توصلت الدراسة إلى أن مجال دراسات الصراع السيبراني شهد توسعا وتنوعاً ملحوظا، انتقل من التركيز المبكر على التطوير المفاهيمي والقضايا الاستراتيجية إلى استخدام مناهج أكثر صرامة، ولا سيما التصاميم التجريبية. أوصت الدراسة بزيادة التنوع الجغرافي في البحوث المتعلقة بالصراع السيبراني، وتعزيز المقاربات متعددة التخصصات، وتشجيع التعاون بين الباحثين من مناطق ومدارس بحثية مختلفة. هدف ذلك إلى تحقيق توازن بين الصرامة المنهجية والأهمية العملية للبحوث بما يزيد من قدرتها على خدمة صانعي السياسات.

8. دراسة Liebetrau & Monsees (2024) بعنوان: Cybersecurity and International Relations: Developing Thinking Tools for Digital World Politics.

هدفت إلى تطوير أدوات ومقاربات تحليلية تساعد على فهم الأمن السيبراني ضمن حقل العلاقات الدولية، وتوضيح كيفية تأثير الرقمنة في السياسة العالمية، كما عملت على تجاوز النظرة التي تعامل الأمن السيبراني كقضية تقنية أو عسكرية منفصلة عن الأبعاد السياسية والاجتماعية والدولية. اعتمدت الدراسة على المنهج التحليلي والنقدي ومراجعة الأدبيات، من خلال فحص الأدبيات المتخصصة في الأمن السيبراني والعلاقات الدولية وتحليل المفاهيم والمقاربات المستخدمة في دراسة السياسة الرقمية العالمية. تمثلت مادة الدراسة في الأدبيات الأكاديمية والمقاربات النظرية والمفاهيمية المتعلقة بالأمن السيبراني والعلاقات الدولية. توصلت الدراسة إلى أن الأمن السيبراني أصبح جزءًا أساسياً من دراسة السياسة العالمية. التركيز المفرط على الدولة والتهديدات العسكرية والقوة يؤدي إلى تضييق فهم الأمن السيبراني. أوصت الدراسة بتوسيع نطاق الدراسات المتعلقة بالأمن السيبراني داخل حقل العلاقات الدولية، وتعزيز المقاربات متعددة التخصصات، وتطوير أدوات نظرية تتجاوز التركيز على الدولة والبعد العسكري، مما يسمح بفهم أكثر شمولًا للتحولات التي تفرضها الرقمنة.

منهجية الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي لأنه يتناسب مع طبيعة موضوع الأمن السيبراني كأحد محددات القوة في النظام الدولي المعاصر، إذ يتيح هذا المنهج وصف مفهوم الأمن السيبراني وتطوراته وأبعاده. كما يحلل علاقته بمصادر القوة الوطنية، والتنافس الدولي، والتحولات في النظام الدولي مع التوسع السريع في استخدام التكنولوجيا والفضاء الرقمي.

تستخدم الدراسة بيانات ومعلومات ثانوية مستمدة من الكتب والدراسات والأبحاث العلمية المحكمة والتقارير الدولية المتخصصة في الأمن السيبراني والعلاقات الدولية. بالإضافة إلى ذلك، تم الاستفادة من التقارير الصادرة عن المؤسسات والمنظمات الدولية ذات الصلة. تم تحليل هذه المصادر لتحديد طبيعة التحديات السيبرانية والانعكاسات على القوة الوطنية ومكانة الدول. كما تم تحليل دور القدرات السيبرانية في التنافس والتعاون الدولي.

كما استخدمت الدراسة أسلوب تحليل المضمون لدراسة الأدبيات والدراسات والتقارير ذات الصلة واستخلاص الاتجاهات والنتائج المشتركة المتعلقة بالعلاقة بين الأمن السيبراني والقوة في النظام الدولي. تمت مناقشة النتائج بناء على

الإطار النظري والدراسات السابقة، مما أدى إلى مجموعة من النتائج والتوصيات توضح أهمية تطوير القدرات السيبرانية كأحد المكونات الحديثة للقوة الوطنية.

حدود الدراسة

تتمثل حدود الدراسة في مجموعة من الأطر التي تحدد نطاق تناول موضوع الأمن السيبراني كأحد محددات القوة في النظام الدولي المعاصر، وذلك على النحو الآتي:

1. الحدود الموضوعية: تركز الدراسة على تحليل الأمن السيبراني بوصفه أحد عناصر القوة الوطنية، مع تناول أبعاده وعلاقته بالتنافس الدولي، وانعكاساته على الأمن القومي ومكانة الدولة واستقرار النظام الدولي، دون التوسع في الجوانب التقنية البحتة للأمن السيبراني.
2. الحدود المكانية: تتناول الدراسة الموضوع في إطار النظام الدولي، مع الاستفادة من الأدبيات والتقارير الدولية المتعلقة بالدول والفاعلين الرئيسيين في المجال السيبراني، دون حصر الدراسة في دولة معينة.

3. الحدود الزمنية: تركز الدراسة على الفترة المعاصرة، مع الاستفادة من الأدبيات السابقة اللازمة لتتبع تطور مفهوم الأمن السيبراني والقوة، وبصورة خاصة التطورات التي شهدها المجال خلال السنوات الأخيرة.

4. الحدود المنهجية: تعتمد الدراسة على المنهج الوصفي التحليلي وتحليل الأدبيات والدراسات والتقارير الدولية ذات الصلة، ولا تتضمن دراسة ميدانية أو استبانة أو مقابلات، وإنما تستند إلى البيانات والمعلومات الثانوية المتاحة في المصادر العلمية والوثائق والتقارير الموثوقة.

تحليل البيانات ومناقشتها

بناء على ما تم عرضه في الإطار النظري، يتضح أن الأمن السيبراني أصبح أحد المكونات المتنامية للقوة الوطنية. لم يعد تأثيره مقتصرا على حماية الأنظمة والشبكات والمعلومات، بل امتد إلى مجالات السياسة والاقتصاد والعسكرية والاستراتيجية. كما يكشف تحليل الأدبيات أن قدرة الدولة على حماية فضائها السيبراني وتطوير قدراتها الرقمية أصبحت مرتبطة بشكل كبير بحمايتها لمصالحها الوطنية وتعزيز استقلالها الاستراتيجي وممارسة النفوذ في البيئة الدولية. كما أن التحول الرقمي السريع أدى إلى زيادة اعتماد الدول على البنية التحتية الرقمية، مما جعل الأمن السيبراني عنصرًا أساسيًا في تقييم قدرة الدولة على مواجهة التهديدات والحفاظ على استمرارية وظائفها الأساسية (ITU, 2024؛ Liebetrau & Monsees, 2024).

يوضح تحليل مؤشر الأمن السيبراني العالمي لعام 2024 أن الأمن السيبراني أصبح مجالا متعدد الأبعاد، إذ يعتمد تقييم الدول على خمسة محاور رئيسة: التدابير القانونية، والتدابير التقنية، والتدابير التنظيمية، وتنمية القدرات، والتعاون. يعني هذا أن امتلاك التكنولوجيا وحده لا يكفي لبناء قوة سيبرانية فعالة، بل يتطلب نظاما متكاملا يجمع بين التشريعات والمؤسسات والموارد البشرية والقدرات التقنية والتعاون الدولي. لذلك، فإن الدول التي تنجح في تطوير هذه الأبعاد بشكل متوازن تكون أكثر قدرة على حماية بنيتها الرقمية وتحويل التكنولوجيا إلى مورد من موارد القوة الوطنية (ITU, 2024).

يظهر تحليل العلاقة بين الأمن السيبراني والقوة السياسية أن حماية المؤسسات الحكومية والبيانات الرسمية وشبكات الاتصال أصبحت جزءا من حماية السيادة الوطنية. يمكن أن تستهدف الهجمات السيبرانية المؤسسات الحكومية أو أنظمة الانتخابات أو قواعد البيانات أو وسائل الاتصال، مما قد يؤثر على الثقة بالمؤسسات وقدرة الدولة على إدارة شؤونها الداخلية. كما يوفر الفضاء السيبراني للدول أدوات جديدة للتأثير وجمع المعلومات وممارسة الضغط السياسي، مما يجعل القدرة على حماية البيئة المعلوماتية والسيبرانية عنصرا من عناصر القوة السياسية في النظام الدولي المعاصر (Nye, 2011؛ Kavanagh & Stevens, 2021).

وبالنسبة للاقتصاد، يظهر أن الأمن السيبراني مرتبط مباشرة بقدرة الدولة على الحفاظ على استقرار اقتصادها واستمرارية قطاعاتها الحيوية. أصبح النشاط الاقتصادي معتمدا بشكل متزايد على الأنظمة الرقمية، والخدمات الإلكترونية، والشبكات المالية، وسلاسل الإمداد الرقمية، مما يجعل تعرضها للهجمات السيبرانية مصدرا محتملًا لخسائر اقتصادية واسعة. لذلك، يعد الاستثمار في الأمن السيبراني ليس مجرد إنفاق على الحماية التقنية، بل يمكن اعتباره استثمارا في حماية القدرة الإنتاجية والاقتصادية للدولة وتعزيز قدرتها على مواجهة الأزمات والاضطرابات الرقمية (ITU, 2024؛ World Economic Forum, 2024).

كما يظهر ارتباط الأمن السيبراني بالقوة العسكرية والاستراتيجية، نظرا لاعتماد المؤسسات العسكرية الحديثة على شبكات الاتصالات والقيادة والسيطرة والاستخبارات ونظم الأسلحة والمعلومات الرقمية. يمكن أن يؤثر اختراق هذه الأنظمة أو تعطيلها على فعالية القدرات العسكرية التقليدية. في المقابل، يمكن للدول ذات القدرات السيبرانية المتقدمة استخدام الفضاء السيبراني لجمع المعلومات وتنفيذ عمليات تستهدف قدرات الخصوم أو دعم العمليات العسكرية التقليدية. لذا أصبحت القدرات السيبرانية جزءًا من الحسابات الاستراتيجية للدول، وأحد المجالات التي تنافس فيها القوى الكبرى على التفوق التكنولوجي (Lindsay, 2013 ؛Kello, 2017).

كما وتشير نتائج التحليل إلى أن التنافس السيبراني لا يقتصر على المجال العسكري، بل يمتد إلى التكنولوجيا والمعايير والبنية التحتية الرقمية والموارد البشرية، إذ تسعى الدول لامتلاك تقنيات متقدمة، وتطوير صناعاتها الرقمية، وتقليل اعتمادها على مصادر خارجية في المجالات التكنولوجية الحساسة، والمشاركة في وضع القواعد والمعايير المنظمة للفضاء السيبراني. تؤدي هذه الجهود إلى انتقال التنافس من مجرد حماية الأنظمة إلى التأثير في البيئة الرقمية الدولية ذاتها، مما يعزز البعد البنيوي والمؤسسي للقوة السيبرانية (Kavanagh & Stevens, 2021 ؛IISS, 2024).

كذلك أظهر تحليل الأدبيات أن صعوبة تحديد مصدر الهجمات السيبرانية تمثل عاملا مهما في تعقيد العلاقات الدولية، فإمكانية إخفاء هوية المهاجم أو استخدام بنى تحتية موجودة في دول أخرى تجعل عملية الإسناد أكثر صعوبة، مما قد يؤدي إلى سوء التقدير أو اتخاذ قرارات سياسية غير دقيقة. وتختلف العمليات السيبرانية عن الاعتداءات التقليدية حيث قد تواجه الدولة المستهدفة صعوبة في تحديد الجهة المسؤولة والتمييز بين الهجوم الذي قامت به دولة والهجوم الذي نفذته جهات غير حكومية. يؤثر ذلك في فعالية الردع وفي قدرة الدول على تحديد طبيعة الاستجابة المناسبة (Rid & Buchanan, 2015 ؛Kello, 2017).

لقد أصبح الأمن السيبراني عاملا مؤثرا في الاستقلال الاستراتيجي للدول، فكلما زاد اعتماد الدولة على التكنولوجيا والبنية التحتية الرقمية الخارجية، زادت احتمالات تعرضها للضغط أو الاضطراب في حال حدوث أزمات دولية أو قيود على التكنولوجيا وسلاسل الإمداد. لذلك، أصبح تطوير القدرات الوطنية في مجالات التكنولوجيا والأمن السيبراني والذكاء الاصطناعي والبيانات جزءًا من جهود الدول لتقليل مواطن الضعف وتعزيز قدرتها على اتخاذ قرارات مستقلة. يفسر هذا تزايد اهتمام الدول الكبرى ببناء قدراتها التكنولوجية والسيبرانية كجزء من الأمن القومي والقوة الوطنية (IISS, 2024 ؛ITU, 2024).

أما فيما يخص التنافس الدولي، فيوضح التحليل أن الفضاء السيبراني أصبح مساحة تجمع بين الصراع والتعاون. تستخدم الدول قدراتها السيبرانية في التجسس والتأثير والردع والدفاع والهجوم، وفي الوقت ذاته تتعاون في تبادل المعلومات وبناء القدرات ومكافحة الجرائم السيبرانية ووضع القواعد والمعايير الدولية. يعكس ذلك طبيعة النظام الدولي المعاصر، الذي لا يقوم على الصراع فقط، بل يجمع بين التنافس والتعاون حسب مصالح الدول ونوعية التهديدات التي تواجهها (ITU, 2024؛ Dunn Cavelty, Pulver, & Smeets, 2024).

كما أظهر تحليل الأدبيات وجود فجوة في القدرات السيبرانية بين الدول، إذ لا تمتلك جميع الدول الموارد التقنية والبشرية والمؤسسية نفسها، مما يؤدي إلى تفاوت في قدرة الدول على حماية بنيتها التحتية الرقمية والاستجابة للهجمات والاستفادة من التكنولوجيا لتحقيق أهدافها الوطنية. ويمكن أن تتحول الفجوة السيبرانية إلى أحد مظاهر التفاوت في القوة داخل النظام الدولي، حيث تتمتع الدول التي تمتلك بنية تكنولوجية متقدمة وكفاءات بشرية ومؤسسات سيبرانية قوية بقدرة أكبر على حماية مصالحها وممارسة النفوذ مقارنة بالدول ذات القدرات المحدودة (ITU, 2024؛ World Economic Forum, 2024).

نتائج الدراسة

في ضوء التحليل النظري ومراجعة الأدبيات والدراسات المرتبطة بالأمن السيبراني والقوة في النظام الدولي المعاصر، توصلت الدراسة إلى مجموعة من النتائج، يمكن عرضها على النحو الآتي:

1. أصبح الأمن السيبراني أحد المكونات المهمة للقوة الوطنية، ولم يعد يقتصر على الجانب التقني المتعلق بحماية الحواسيب والشبكات والبيانات، بل أصبح مرتبطًا بالأمن القومي والاستقلال الاستراتيجي وقدرة الدولة على حماية مصالحها ومؤسساتها وبنيتها التحتية الحيوية.
2. تغير مفهوم القوة في النظام الدولي المعاصر من التركيز على القدرات العسكرية والاقتصادية التقليدية إلى مفهوم أكثر شمولًا يتضمن التكنولوجيا والمعلومات والقدرات الرقمية والسيبرانية. وبذلك أصبحت القوة السيبرانية أحد الأبعاد الحديثة التي تساهم في تحديد مكانة الدولة وقدرتها على التأثير في البيئة الدولية.

3. يمثل الأمن السيبراني عاملًا مضاعفًا للقوة الوطنية؛ فحماية البنية الرقمية ترفع من فاعلية القدرات العسكرية والاقتصادية والسياسية، بينما يمكن أن يؤدي ضعف الأمن السيبراني إلى إضعاف هذه القدرات وتعريضها للاختراق أو التعطيل أو الاستغلال الخارجي.
4. أصبح الفضاء السيبراني مجالًا جديدًا للتنافس الدولي، حيث تتنافس الدول على تطوير التكنولوجيا والقدرات السيبرانية، وحماية البنية التحتية الرقمية، وجمع المعلومات، وتعزيز قدراتها الدفاعية والهجومية، إلى جانب التنافس على وضع القواعد والمعايير المنظمة للفضاء السيبراني.
5. تتجاوز التهديدات السيبرانية حدود الدولة، الأمر الذي يجعل الأمن السيبراني قضية دولية تتطلب التعاون بين الدول والمؤسسات والمنظمات الدولية، خصوصًا في مواجهة الجرائم السيبرانية والهجمات العابرة للحدود.
6. تمثل صعوبة تحديد مصدر الهجمات السيبرانية أحد أهم التحديات أمام الاستقرار الدولي، إذ إن صعوبة الإسناد قد تؤدي إلى سوء التقدير، وتحد من قدرة الدول على اتخاذ قرارات دقيقة بشأن الرد، وقد تزيد من احتمالات التصعيد غير المقصود.
7. أصبحت البنية التحتية الحيوية أحد أهم مجالات التنافس والتهديد السيبراني، نتيجة اعتماد قطاعات الطاقة والمياه والاتصالات والمصارف والصحة والنقل والمؤسسات الحكومية على الأنظمة الرقمية، مما يجعل حمايتها جزءًا أساسيًا من الأمن الوطني.
8. أدى التطور السريع للذكاء الاصطناعي والتقنيات الرقمية إلى زيادة تعقيد البيئة السيبرانية، إذ يمكن توظيف هذه التقنيات في تطوير وسائل الدفاع والكشف المبكر عن التهديدات، وفي الوقت نفسه يمكن استغلالها في تطوير الهجمات الإلكترونية والتضليل والهندسة الاجتماعية.

توصيات الدراسة

بناء على النتائج، توصي الدراسة بما يلي:

1. ضرورة إدماج الأمن السيبراني ضمن مفهوم الأمن القومي والقوة الوطنية، وعدم التعامل معه باعتباره قضية تقنية بحتة، نظرًا لارتباطه المباشر بالأمن السياسي والاقتصادي والعسكري والاستراتيجي للدولة.
2. تطوير استراتيجيات وطنية شاملة للأمن السيبراني تتضمن أهدافًا واضحة لحماية البنية التحتية الحيوية، وتأمين المعلومات الحكومية، ورفع مستوى الجاهزية والاستجابة للحوادث السيبرانية.
3. تعزيز الاستثمار في البنية التحتية والتكنولوجيا السيبرانية، مع الاهتمام بتطوير القدرات الوطنية في مجالات الذكاء الاصطناعي، والحوسبة السحابية، وتحليل البيانات، وأمن الشبكات، والتشفير، بما يقلل من مواطن الضعف التقنية.
4. الاستثمار في رأس المال البشري من خلال تطوير برامج أكاديمية وتدريبية متخصصة في الأمن السيبراني، وتأهيل الكوادر القادرة على التعامل مع التهديدات المتطورة، والحد من مشكلة نقص المتخصصين في هذا المجال.
5. تعزيز حماية البنية التحتية الحيوية، ووضع معايير أمنية متقدمة للقطاعات التي يعتمد عليها استقرار الدولة، خاصة الطاقة والمياه والاتصالات والمصارف والنقل والصحة والمؤسسات الحكومية.
6. تطوير الأطر القانونية والتشريعية المتعلقة بالأمن السيبراني بما يواكب التطورات التكنولوجية، ويحدد المسؤوليات والاختصاصات وآليات التعامل مع الجرائم والهجمات السيبرانية، مع تحقيق التوازن بين متطلبات الأمن وحماية الحقوق الرقمية.
7. تعزيز التعاون الدولي في مجال الأمن السيبراني من خلال تبادل المعلومات والخبرات، وتطوير آليات مشتركة للإنذار المبكر والاستجابة للحوادث، والتعاون في مكافحة الجرائم والهجمات السيبرانية العابرة للحدود.
8. المشاركة الفاعلة في صياغة القواعد والمعايير الدولية للفضاء السيبراني، بما يتيح للدول المساهمة في تشكيل البيئة القانونية والتنظيمية الدولية وحماية مصالحها في ظل تزايد أهمية الفضاء السيبراني في العلاقات الدولية.
9. تطوير آليات وطنية ودولية للحد من مخاطر سوء الإسناد والتصعيد السيبراني، من خلال تعزيز تبادل المعلومات والخبرات الفنية وتطوير قنوات الاتصال بين الدول، بما يساهم في منع تحول الحوادث السيبرانية إلى أزمات سياسية أو عسكرية.

قائمة المراجع

إبراهيم، أبكر عبد البنات آدم. (2025). *فاعلية الأمن السيبراني في المحافظة على السيادة الوطنية: دراسة وصفية تحليلية*. رماح للبحوث والدراسات، 115، 29–67.

الخبيزي، بدر عدنان أحمد سعد محمد. (2024). *توظيف الأمن السيبراني لاستثمار فرص الذكاء الاصطناعي والحد من تحدياته في مجال التعليم والتعلم*. المجلة العربية للدراسات الأمنية، 40(2)، 235–249.
الخضيري، علي إبراهيم يوسف. (2024). *سبل مكافحة الجرائم السبرانية العابرة للحدود: دراسة مقارنة*. مجلة جامعة الزيتونة الأردنية للدراسات القانونية، 5(عدد خاص)، 927–942.
الرفيعي، علي محمد أمنيف. (2025). *الأمن السيبراني وتأثيره في مستقبل الهيمنة الأمريكية*. مجلة تكريت للعلوم السياسية، 1(38)، 257–276. https://doi.org/10.25130/tjfps.v1i38.484
المرجان، عبد الرزاق، ولي، سيوكي، والزهراني، إبراهيم، والشقيران، سمية. (2024). *معجم أهم مصطلحات الجرائم السيبرانية والأدلة الرقمية: إنجليزي–عربي*. الرياض: دار جامعة نايف للنشر.
بارة، سمير. (2017). *الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات*. المجلة الجزائرية للأمن الإنساني، 2(2)، 255–280. https://doi.org/10.59791/arhs.v2i2.2552
بن جدو، بن علية. (2022). *تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية*. المجلة الجزائرية للأمن الإنساني، 7(2)، 299–319.
بوغازي، عبد القادر. (2025). *الردع السيبراني: مقاربة للطبيعة، الفواعل وقيود القانون الدولي*. المجلة الجزائرية للحقوق والعلوم السياسية، 10(1)، 855–869.
حارك، فاتح، وحمدوش، رياض. (2022). الدولة، بين الهيمنة وتحقيق الأمن في الفضاء السيبراني. المجلة الجزائرية للأمن الإنساني، 7(1)، 130–151. https://doi.org/10.59791/arhs.v7i1.1114
العوفي، دليلة. (2020). *آليات محاربة الجريمة المعلوماتية:* دراسة حالة الجزائر 2009–2016 [أطروحة دكتوراه، جامعة الجزائر 3]. المستودع الرقمي لجامعة الجزائر 3.

المراجع الأجنبية

Akdağ, Y. (2025). *Great Power Cyberpolitics and Global Cyberhegemony.* Perspectives on Politics. https://doi.org/10.1017/S1537592725000040
Benson, D. C. (2022). *Stop Selling Cybersecurity Short: Cybersecurity as a Component of National Power.* Air University / Purdue University CERIAS. https://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/1oc55hctllr6ejubslnsbadhh2
Brown, J. M., & Fazal, T. M. (2021). *SorryNotSorry: Why States Neither Confirm nor Deny Responsibility for Cyber Operations*. European Journal of International Security, 6(4), 401–417. https://doi.org/10.1017/eis.2021.18.
Czerwińska, M. (2025). Geopolitics of Cybersecurity – International Power Dynamics and State Security in Cyberspace. Humanities & Social Sciences Reviews, 13(2), 337–342.
Dunn Cavelty, M., Pulver, T., & Smeets, M. (2024). *The Evolution of Cyberconflict Studies. International Affairs*, 100(6), 2317–2339. https://doi.org/10.1093/ia/iiae175 Egloff, F. J., & Shires, J. (2021). *The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence.* European Journal of International Security. 8(1):130-149.
Fouad, N. S. (2022). *The Non-anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity*. Review of International Studies, 48(4), 766–785.
International Institute for Strategic Studies. (2024). *IISS Cyber Power Matrix*. IISS.
International Telecommunication Union. (2024). *Global Cybersecurity Index 2024*. ITU.
Kavanagh, C., & Stevens, T. (2021). *Cyber Power in International Relations. In P. Cornish (Ed.)*, The Oxford Handbook of Cyber Security (pp. 66–81). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.013.4
Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.
Liebetrau, T., & Monsees, L. (2024). *Cybersecurity and International Relations: Developing Thinking Tools for Digital World Politics.* International Affairs, 100(6), 2303–2315. https://doi.org/10.1093/ia/iiae232

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122
Morgenthau, H. J. (1948). *Politics Among Nations: The Struggle for Power and Peace*. Alfred A. Knopf.
Ramadan, S. I. (2026). gRPC (HTTP/2) vs REST (HTTP/1.1) in Distributed Systems: Performance, Scalability, and the Cryptographic Cost of TLS 1.3. *Al-Farooq Journal of Sciences*, *2*(3), 1031-1039.
Koresh, M. A., & Abzabez, A. A. (2026). The Future of the Libyan-European Geoeconomic Partnership in the Era of Global Energy Transition: A Conceptual Framework of Complex Interdependence. *Shihab Journal of Humanities*, *2*(2), 16-21.
National Institute of Standards and Technology. (2015). *Cybersecurity*. NIST Computer Security Resource Center.
National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)*. U.S. Department of Commerce.
Nye, J. S., Jr. (1990). *Soft Power*. Foreign Policy, 80, 153–171. https://doi.org/10.2307/1148580
Nye, J. S., Jr. (2004). *Soft Power: The Means to Success in World Politics.* PublicAffairs.
Nye, J. S., Jr. (2011). *The Future of Power.* PublicAffairs.
Özdemir, G., & Karagül, S. (2024). *National Security and the Tools of Cyber Power: A Review of the Areas of State Hegemony*. Yönetim Bilimleri Dergisi, 22(53), 852–875. https://doi.org/10.35408/comuybd.1360459
Rid, T., & Buchanan, B. (2015). *Attributing Cyber Attacks*. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
Roguski, P. (2021). *An Inspection Regime for Cyber Weapons: A Challenge Too Far?* AJIL Unbound, 115, 111–115. https://doi.org/10.1017/aju.2021.6
Stevens, T., & Kavanagh, C. (2021). *Cyber Power in International Relations*. In P. Cornish (Ed.), The Oxford Handbook of Cyber Security (pp. 66–81). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.013.4
Tzavara, V., & Vassiliadis, S. (2024). *Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review*. International Journal of Information Security, 23, 1695–1719. https://doi.org/10.1007/s10207-023-00811-x
United Nations. (2021). *Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations General Assembly.
United Nations Office on Drugs and Crime. (2021). Cybercrime Module 5: Cybercrime and International Law. United Nations.
Waltz, K. N. (1979). *Theory of International Politics*. McGraw-Hill.
World Economic Forum. (2024). *Global Cybersecurity Outlook 2024.* World Economic Forum.
Wilson, E. J., III. (2008). *Hard Power, Soft Power, Smart Power*. The Annals of the American Academy of Political and Social Science, 616(1), 110–124. https://doi.org/10.1177/0002716207312618