مجلة خليج العرب
للدراسات الإنسانية والاجتماعية

عتبة القوّة السيبرانيّة وتأثيرها في العلاقات الدوليّة المعاصرة

The Threshold of Cyber Power and Its Impact on Contemporary International Relations

Dr. Mohammad Zaitoun

الدكتور محمد زيتون

دكتوراه علوم سياسية في مجال السياسية السيبرانية وبناء استراتيجيات الامن السيبراني

مدير مشاريع للامن السيبراني وخدمات التحول الرقمي (الكويت- لبنان)

DOI: https://doi.org/10.64355/agjhss254

الملخص:
تتناول هذه الدراسة مفهوم عتبة القوة السيبرانية وفي آثارها على العلاقات الدولية المعاصرة. ومع تزايد أهمية الفضاء السيبراني كعنصر أساسي في قوة الدول واستراتيجياتها العالمية، تبرز الحاجة لفهم اللحظة التي تتحول فيها القدرات السيبرانية من أدوات تأثير إلى وسائل إكراه أو قوة استراتيجية. تحلل الدراسة كيف تدرك الدول هذه العتبات، وكيف تسهم في تشكيل أنماط الردع، والصراع، والتعاون في النظام الدولي. ومن خلال أطر نظرية ودراسات حالة مختارة، تهدف الدراسة إلى تقديم فهم أعمق لكيفية إعادة تشكيل القدرات السيبرانية لديناميكيات القوة العالمية

الكلمات المفتاحية: القوة السيبرانية، العلاقات الدولية، الفضاء السيبراني، الردع السيبراني، الاستراتيجيات السيبرانية.

Abstract:

This study addresses the concept of the cyber power threshold and its implications for contemporary international relations. As cyberspace increasingly becomes a core element of national power and global strategies, there is a growing need to understand the point at which cyber capabilities shift from tools of influence to instruments of coercion or strategic power. The study analyzes how states perceive these thresholds and how they contribute to shaping patterns of deterrence, conflict, and cooperation within the international system. Through theoretical frameworks and selected case studies, the study aims to provide a deeper understanding of how cyber capabilities are reshaping the dynamics of global power.

Keywords: Cyber Power, International Relations, Cyberspace, Cyber Deterrence, Cyber Strategies.

المقدمة:

مُنذُ أن خطا الإنسان أولى خطواته في مسيرة الحضارة، ارتبطت القوّة بالتطور، وتشكلت كأحد أعمدة الحكم بين الشعوب. كانت تُصاغ بأدوات رمزية، وكان الدين في مقدمتها. فقد تحوّل الدين إلى وسيلة لفرض الطاعة، ووسيلة لبناء هيبة تهزّ النفوس وتولّد الخوف والإجلال، ليُترجم ذلك إلى سلطة مطلقة. ومع توالي تطور المجتمعات والتحولات الكبرى، انتقلت سلطة رجل الدين إلى سطوة السيف، ومن المعبد إلى العرش.

فإذا فإنّ مظاهر القوة وأشكالها تختلف مع تطور المجتمعات، حيث كانت القوّة العسكريّة فيصل الصراعات، ولكن التطوّر البشري والمجتمعي وقيام التجارة الدوليّة جعلت من القوّة الاقتصاديّة أداة للتحكّم وتوجيه الخصم. وعندما أحرزت الألة البخاريّة عنصراً مهاً في نصر الحروب أصبحت قوّة إضافية قادرة على تشكيل العلاقات. كذلك في القرن الحادي والعشرين، شهدت الصناعات التكنولوجية ولا سيّما الإنترنت، تطورًا أدى إلى بروز مفاهيم جديدة أثّرت على جميع عناصر القوّة في الدول سواء الماديّة أو المعنويّة. وأصبح لكل دولة امتداد رقمي يُمكّنها من التحكم في مقدّراتها ويؤثر على علاقاتها الدوليّة في الفضاء السيبراني العالمي. وعندما اكتسبت الوسائل العسكرية بُعدًا رقميًا جعلها أكثر كفاءة في تحقيق أهدافها بأقل الخسائر البشرية والتكاليف المادية، أثرّت في الخيارات المتاحة أمام واضعي السياسات وصانعي القرارات، حيث أحدثت تغيراً في طبيعة القوّة وتحولات على مفاهيم الردّع والدبلوماسيّة وغيرها من عناصر العلاقات الدوليّة، وأصبحت عاملاً أساسيًّا يقوم عليه كثير من التطور الاجتماعي والاقتصادي والسياسيّ، وكذلك النظام العالمي والعلاقات بين الدّول.

تطور مفهوم هذه القوة وأصبحت تعتمد بشكل كبير على تقنيات متقدّمة مثل الذكاء الاصطناعي، والبيانات الضخمة، والخرائط الرقميّة، والعمليات السيبرانيّة،[1] حتى أُضيف عليها مصطلح "السايبر" للإشارة إلى كل ما يتعلق بالعالم الرقمي والمعلوماتي، حتى تشكّل لدينا مفهوم القوة السيبرانيّة، وبدأت تتعاظم أشكالها وتعزز قدرتها بسبب التصاعد الرقمي في كل المستويات، حتى غدت تمتلك سمات القوّة الصلبة والنّاعمة معًا، ما جعلها تؤثر في مسار الصراعات وتلعب دورًا فاعلًا في تشكيل التحالفات ضمن ساحة العلاقات الدوليّة، خاصة لما تمتلكه من قدرة على النفاذ إلى مواقع تعجز أدوات القوة التقليدية عن الوصول إليها. ورغم الشكّ حول العتبة التدميريّة التي يمكن أن تحدثها إلاّ إنها أصبحت تحد من حاجة استخدام القوّة التقليديّة في تحقيق الأهداف، والتحالفات وتشكيل العلاقات.

أهمية الموضوع: تكمن أهمية هذا البحث في تسليط الضوء على دور القوة السّيبرانية في تشكيل العلاقات الدولية كإحدى الوسائل الحديثة في الصراعات الدّوليّة، واستعراض ملامحها كأداة مبتكرة للتأثير والسيطرة.

[1] العمليات السيبرانية هي مصطلح ناشئ يُستخدم للإشارة إلى كافة الأنشطة التي تُمارس في الفضاء السيبراني (Cyber Space)، الهجمات السيبرانية، الدفاع السيبراني، التمّلك الرقمي، النفوذ السيبراني، استعمار البيانات، وأداة للسيطرة السياسية، وسيلة للحروب الحديثة، مصدرًا ناشئا للقوة الاقتصادية ، وقوة ناعمة وصلبة للهيمنة الثقافية.

أهداف البحث: تهدف الدراسة إلى تحقيق عدة أهداف، أبرزها، تعريف مفهوم القوة السّيبرانيّة وتحديد نطاقها ومكوناتها والعتبة او عتبة السيطرة العليا في العلاقات الدولية المعاصرة وتأثيرها في الحروب السيبرانية.

إشكالية البحث: أصبحت القوة السيبرانية ظاهرة متنامية في النظام الدولي المعاصر، وأداة استراتيجية في الفضاء السيبراني، الذي يُعد اليوم الميدان الخامس في الصراعات بين الدول. وقد بات هذا الفضاء ميدانًا جديدًا للصراع والتنافس على النفوذ. في هذا السياق، تبرز إشكالية تحديد مفهوم القوة السيبرانية ونطاق تأثيرها على السيادة، والعلاقات الدولية، والديناميكيات الجيوسياسية الأخرى. **كيف تُعرّف القوة السيبرانية في ظل التحولات التكنولوجية الراهنة؟ وهل باتت قادرة، بوصفها أحد أعتاب القوة الحديثة، على تحقيق المصالح الدولية من حيث السيطرة والتأثير؟**

منهجيّة البحث: سنتناول في هذا البحث المنهج الوصفي والتحليلي لتوصيف التحولات التي طرأت على القوة السّيبرانيّة، وتحليل أساليبها واستخدامها كمنهج جديد في الدّيناميكيات الدّوليّة في الفضاء السيبراني.

تصميم البحث:

المبحث الأوّل: عتبة القوّة السيبرانيّة ومحدّداتها المفاهيميّة والعمليّة

المطلب الثّاني: الإطار المفاهيمي للقوّة السيبرانيّة

المطلب الأوّل: عتبة استخدام القوّة السيبرانيّة

المبحث الثّاني: أثر القوّة السيبرانيّة في العلاقات الدوليّة المعاصرة

المطلب الأوّل: التحولات والتغيّرات التي طرأت على العلاقات الدوليّة في ظل القوّة السيبرانيّة

المطلب الثّاني: تأثير القوّة السيبرانيّة على العلاقات الدوليّة

- **المبحث الأوّل: عتبة القوّة السيبرانيّة ومحدداتها المفاهيميّة والعمليّة**

مع بروز الثورة الرقمية وتنامي الاعتماد على التكنولوجيا والفضاء السيبراني، برزت "القوة السيبرانية" كمفهوم جديد قادرا على تشكيل توازنات القوة التقليدية وتؤثر على العلاقات الدولية والمصالح. إذ لم تعد القوّة تقتصر على الوسائل العسكرية والاقتصادية الصلبة، بل اتسع مفهومها ليشمل القدرة على النفوذ والسيطرة عبر الفضاء السيبراني، بما ينطوي عليه من بيانات، وهياكل رقمية، وشبكات اتصالات. وتطوّرت من أداة فنية مساندة إلى قوة جانبية فاعلة تتمتع بخصائص مماثلة في بعض جوانبها لخصائص القوة التقليدية، من حيث التأثير، الردع، والاختراق الاستراتيجي. وتستخدمها الدول في الفضاء السيبراني لتحقيق أهدافها الجيوسياسية والاستراتيجية، سواء عبر العمليات السيبرانية والمعلوماتية، أو التأثير في الرأي العام وتوجيه السلوك السياسي.

وفي هذا الإطار، تبرز الحاجة إلى تحليل نظري لطبيعة القوة السيبرانية، لفهم مرتكزاتها، وتحديد ملامحها بوصفها شكلاً جديدًا من القوة ضمن النظام الدولي. ويستدعي ذلك العودة إلى المفاهيم الكلاسيكية للقوة، مثل القوة الصلبة والناعمة والذكية، وتفكيك كيفية اندماج أو تمايز القوة السيبرانية عنها، لذلك وفي ضوء التحولات التكنولوجية والتشابك العالمي المتزايد سنتناول في هذا المبحث مطلبين، نتناول في الأول الإطار النظري لنشأة القوّة التقليديّة والسيبرانيّة، والثاني نتناول عتبة استخدام القوّة السّيبرانيّة.

- **المطلب الأوّل: الإطار المفاهيمي للقوّة السيبرانيّة**

كما أشرنا، لم تعد القوة في العصر الحديث مقتصرة على العتاد العسكري أو التفوق الاقتصادي فقط، بل برز نوع جديد من القوة يتمثل في القوة السيبرانية، التي تعتمد على القدرات التقنية والمعلوماتية في الفضاء الرقمي. هذه القوة أصبحت عنصرًا حاسمًا في تحديد مكانة الدول رقميا، وتوجيه السياسات، وحتى التأثير على الأمن القومي والاقتصاد العالم في نظام عالمي جديد يساهم في قيامه الفضاء والقوة السيبرانيتين. سنعرض في هذا المطلب النشأة التاريخية للقوة وصولا للقوة السيبرانية وإلى ملامحها وعلاقتها بالقوة التقليدية.

1. **مفهوم القوّة(Power):** لا تعني القوة في معناها الضيق، بل هي القدرة على التأثير في سلوك الآخرين، أو التحكُّم في سلوكهم تجاه قضية معينة. ووسيلة لتحقيق غاية معينة بذاتها، ولذلك من الصعب تصوّر أن دولة ما تنفق الأموال والطاقات لامتلاك القوة لمجرد امتلاكها أو

لاستعراض قوتها في مواجهة الآخرين[2]. وهي ليست فعلاً ساكنًا إنما علاقة بين طرفين يتم في إطارها تفاعل وسائل تأثير وأساليبه في الإرادات والسلوك Actor. وفي مفهومها الواسع هي القوة القومية بمفهومها الشامل بمختلف عناصر الدولة بمكونات الامن القومي وتتنوع مصادرها من القوة الناعمة والقوة الصلبة، ونحصرها بتعريف "روبرت دال" يقول: إنّ القوة هي قدرة الفاعل(أ) على ان يجبر فاعل (ب) على ان يفعل شيئا أو يمتنع عن فعل شيء ما كان ليفعله لولا قدرة (أ).[3]

سابقا كانت ترتكز عناصر القوة بأشكال متعدِّدة ومتنوِّعة كالمساحة الجغرافية والتضاريس الاستراتيجية، وعدد السكان، والموارد الطبيعية، والقدرات الاقتصادية المتنوعة، والقوة العسكرية، والبنية التكنولوجية، والفعاليات الثقافية، والمؤسسات السياسية، وحالة النظام السياسي الحاكم ورضى الشعب، والحالة المعنوية للشعب وغيرها. وبعدما أصبحت القوة ركيزة للدول في تحديد مكانتها وفرض علاقاتها الدولية، أصبح لديها وسائل ولا سيما الوسيلة الاقتصادية، العسكرية، والاستخباراتية الدبلوماسية الوسائل الرمزية كالأدوات الأيديولوجية الرمزية التي تهدف إلى نشر تصوُّر مثالي شامل لما ينبغي أن يكون عليه المجتمع في المستقبل، بما يحمله ذلك من قيم تخدم مصالح الدولة الفاعلة في المدى الطويل.[4] بهدف تسويق توجُّهات معيَّنة، أو الدفع في اتجاه تأييد وضع معين أو رفضه، فقد أصبح الإعلام قوة خصوصًا مع تصاعد أهمية تأثيرات الرأي العام في التوجُّهات السياسية للدول[5]. وبناء عليه لم تعد القوة قيمة مطلقة بل تعتبر نسبية، فمن غير الممكن وصف طرف ما بأنه قوي أو ضعيف إلا في إطار مقارنته بطرف أو أطراف أخرى. وتلك المقارنة هي التي تحدِّد موقعه في هيكل القوة على المستوى الإقليمي أو الدولي.[6] ولم يقتصر تطور مفهوم القوة الى الجوانب التي ذكرت، بل تطور وأصبح للقوة مفاهيم أخرى أبرزها القوة الصلبة والناعمة والقوة الذكية التي تجمع بين المفهومين.

2. **من القوّة التقليديّة الى القوّة السيبرانيّة:** أشرنا في الفقرة السابقة إنّ القوة قيمة مطلقة بل تعتبر نسبيّة، والقوّة هي العنصر الذي يتطور مع تطور المجتمعات، فالقوّة دائما في حالة تكتل وتتعاظم بسبب التقدم البشري والتكيّف مع التطورات، وكل مفهوم أو أداة تتكتل مع القوة أو يتحول عن مفهوم القوة التقليدية هو مفهوم جانبي وله قدرة نسبيّة وعتبة في بلوغ الأهداف أو الغايات. لذلك تعتبر القوّة السيبرانية قوّة جانبية، وإذا لاحظنا تسلسل نشأتها، منذ بداية اعتراض الاتصالات والتشفير والتجسس، وفي الحرب العالمية الثانية، كان فك الشيفرات (مثل شيفرة "إنجما" الألمانية) أحد أبرز مظاهر الحرب المعلوماتية، وأسهم بشكل بارز في انتصار الحلفاء. خلال الحرب الباردة ومع تطور الحوسبة، بدأت الدول الكبرى في استخدام أجهزة الكمبيوتر لاعتراض وتحليل الاتصالات، حيث أنشأت وكالات مثل وكالة الأمن القومي الأمريكي قواعد حول العالم لجمع وتحليل الإشارات والاتصالات السوفيتية. كما شهدت هذه الفترة بدايات استخدام التشفير والحوسبة في حماية المعلومات العسكرية الحساسة. فبدأ مشهد التحول الرقمي وانتقلت الحركة السيبرانية من حالة الدفاع إلى الهجوم حيث ركزت الجهود السيبرانية على حماية الأنظمة العسكرية، وتطوير قنوات اتصال آمنة وتقنيات تشفير. ومع نهاية التسعينيات وبداية القرن الحادي والعشرين، بدأت الدول في تطوير قدرات هجومية سيبرانية، وأصبح التجسس والاختراق السيبراني وسيلة رئيسية لجمع المعلومات أو تعطيل الأنظمة الحيوية للخصوم.

وأبرز الأمثلة البارزة، في التسعينيات، شهد العالم أولى الهجمات السيبرانية المعروفة ضد مؤسسات عسكرية، مثل اختراق مركز سلاح الجو الأمريكي، والذي اعتُبر شرارة انطلاق الحرب السيبرانية الحديثة. وهجوم 2007 على إستونيا، الذي عطل البنية التحتية الرقمية للدولة، مثّل نقطة تحول في إدراك خطورة الهجمات السيبرانية على الأمن القومي. وفي القرن الحادي والعشرين برز مصطلح الحروب السيبرانية وشهدت المجتمعات تصاعداً كبيراً في أنشطة الحرب السيبرانية (العمليات السيبرانية)، حيث أصبحت الهجمات تستهدف البنى التحتية الحيوية مثل الكهرباء والمياه والبنوك، وتورطت فيها دول وفاعلون غير حكوميين (قراصنة، جماعات إرهابية، شركات، وأفراد). كما أصبح الفضاء السيبراني ساحة رئيسية للصراعات الدولية، وبدأت الدول تدمج القدرات السيبرانية في استراتيجياتها العسكرية.[7] ومنذ ذلك الوقت والقوة تشهد تحولات حتى برزت القوة السيبرانية تتميز بالمرونة والسرعة والخفاء وعدم الاسناد، ولم تعد القوة السيبرانية حكراً على الدول الكبرى، بل أصبح بإمكان فاعلين من غير الدول (أفراد، شركات، جماعات) التأثير على الأحداث الدولية،[8] ما فرض تحديات جديدة على سيادة الدول

---

[2] – عندما تقوم الحكومات بتنظيم استعراضات عسكرية لقواتها المسلَّحة وأسلحتها في عواصمها، يكون الهدف هو اكتساب مكانة سياسية دولية –إقليمية معينة أو تأكيدها، أو رفع الحالة المعنوية لشعوبها إن لم يكن تدعيم الردع، أو إرسال رسائل في اتجاه أو آخر.

[3] ليلى نقولا، **العلاقات الدولية. من تأثير القوة الى قوة التأثير**، الأرز للنشر، لبنان، 2021، ص211.

(4) - كمحاولات الترويج للفكر الماركسي اللينيني في فترة الحرب الباردة، أو لما سُمِّيَ النمط الأميركي للحياة، أو القيم الغربية، وفي الواقع صرفت أموال خيالية في هذا الإطار من قبل المعسكرين في محاولة لتلميع صورة النظام السياسي لكليهما.

(5) - Joseph S. Nye Jr, Soft Power: **"The Means to Success in World Politics"**, Public Affairs; (2005), ch2.

(6) - الهند قد تكون قوية عسكريًا بالنسبة إلى باكستان، لكن الصين قد تكون أقوى منها، والأخيرة أقل قوة بالنسبة إلى الولايات المتحدة الأميركية وهكذا.

[7] من التجسس إلى الحرب الشاملة: رحلة تطور الحروب السيبرانية عبر العصور، متوافر على موقع سيبرا،9-9-2024، الرابط:، https://cutt.ly/crWKkBz7، تاريخ الزيارة 19-5-2025.

[8] الفضاء السيبراني وتحولات القوة في العلاقات الدولية، متوافر على مواقع المركز العربي للأبحاث ودراسة السياسات، الرابط:، https://www.dohainstitute.org/ar/BooksAndJournals/Pages/cyberspace-and-power-shifts-in-international-relations.aspx، تاريخ الزيارة 25-5-2025.

وأمنها. كما شهدت السنوات الأخيرة تطوراً في أدوات الهجوم السيبراني، مثل البرمجيات الخبيثة، استغلال ثغرات يوم الصفر، والتهديدات المستمرة المتقدمة (APTs)، وتجدر الإشارة في هذا السياق إن العمليات السيبرانية (الهجومية والدفاعية) هي إحدى مركبات القوة السيبرانية.

أ-المفهوم اللغوي للقوّة السيبرانيّة: (Cyber power) القوّة في المفهوم الاصطلاحي العام هي امتلاك الوسائل أو القدرات التي تمكّن الفرد أو الجماعة من تحقيق ما يريدون، أو فرض إرادتهم على الآخرين، أو حماية أنفسهم من المخاطر. وهي كذلك القدرة على التأثير في سلوك الآخرين أو في مجريات الأحداث ونتائجها، سواء كان ذلك بشكل مباشر أو غير مباشر. أما كلمة "سايبر" فهي تعريب للكلمة الإنجليزية "Cyber"، وهي اختصار لمصطلح "Cybernetics" الذي تعني "التحكم الآلي" أو "علم التحكم والتواصل في الكائنات الحية والآلات". في الاستخدام الحديث، أصبحت كلمة "سايبر" تشير إلى كل ما يتعلق بالفضاء الإلكتروني أو الرقمي، مثل الإنترنت، الشبكات، الحواسيب، والأنظمة الرقمية. لذا نجد مصطلحات مثل "الأمن السيبراني" (Cybersecurity) أو "الهجمات السيبرانية" (Cyber Attacks) للدلالة على كل ما يتعلق بالأمن أو الهجوم في الفضاء الرقمي، ولذلك إن التصاق السايبر في مفهوم القوة أرسى مفهوم القوّة السيبرانيّة.[9]

ب-**القوّة السيبرانيّة:** القوّة السيبرانيّة أصبحت واقعًا فرض نفسه" تُعبّر بدقة عن التحوّل الكبير في ميزان القوى في العصر الرقمي، لذلك نرى من الأفضل تقديم تعريفها من اتجاهين، اتجاه علمي من الواقع العملي، واتجاه أكاديمي في اتجاه العلاقات الدولية. عمليا وعلميا، هي " القدرة على التحكم في البنية التحتيّة للمعلومات والاتصالات، والرد على الهجمات الإلكترونيّة وضمان الأمن السيبراني توفر قوة حقيقية وأصبحت واحدة من أهم القضايا السياسيّة والاقتصاديّة والتكنولوجيّة في القرن الحادي والعشرين".[10] وأكاديميا، يعرّفها فقيه القوّة جوزف ناي:" إنّ القوة السيبرانية بأنها القدرة على تحقيق النتائج المرجوة من خلال استخدام موارد المعلومات المترابطة إلكترونيًا ضمن الفضاء السيبراني. وقد أشار جوزيف ناي إلى أن القوة السيبرانية تتجسّد في توظيف إمكانات المعلومات والتكنولوجيا في المجال السيبراني لتحقيق أهداف سياسية أو اقتصادية أو عسكرية أو اجتماعية.[11]

ونستنتج إنّ القوّة السيبرانيّة أصبحت عنصرا مهما تتحكم في العلاقات الدولية بسمتين، سمة القوة الناعمة (Soft power) المتمثلة بالدبلوماسية الرقمية، والأدوات السيبرانية التي تفرض أو تساهم في توجه أفكار معينة، وسمة القوة الصلبة (Hard power) المتمثلة بالعمليات السيبرانية المتقدمة والتحكم بالإنترنت والبيانات وسياسات وتوجيه بروتوكولات التكنولوجيا والممارسات الرقمية. وفي السياق السيبراني سواء مفهوم القوة الناعمة أو الصلبة أو ما توصف به في أروقة الباحثين " بحرب الاصفار او الحرب السيبرانية او العمليات السيبرانية، هي قوة صامته ولكن لديها عتبة تأثير جانبية تلعب دورا لتوجيه الطرف الاخر أو الخصم ونادرا ما تحدث انفجارات وأصوات، وللإضاءة على مفهومها الناعم والصلب نشير في جدول(1) على أهم عناصرها:

جدول (1)، مقارنة القوة الناعمة والصلبة السيبرانييتين[12]

العنصر	القوة الناعمة السيبرانية	القوة الصلبة السيبرانية
التعريف	-التأثير غير المباشر عبر الفضاء السيبراني باستخدام الإعلام، الثقافة، والتكنولوجيا لجذب الآخرين	-استخدام الفضاء السيبراني للهجوم أو الإكراه بهدف فرض الإرادة أو شلّ الخصم
الوسائل والأدوات	-الإعلام الرقمي-التواصل الاجتماعي-الذكاء الاصطناعي-المؤثرون-الثقافة الرقمية	-برمجيات خبيثة-هجمات DDoS-اختراقات وتجسس-فيروسات وRansomware
طريقة التأثير	-الإقناع التدريجي والتأثير النفسي والمعرفي	-الإكراه، الإرباك، التهديد المباشر
الزمن	-طويل الأمد، تراكمي	-فوري، مفاجئ

[9] Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyberpower and National Security Policy, Center for Technology and National Security Policy, USA, 2009, P.528.

[10] Igli Tashi, Solange Ghernaouti, Information Security Evaluation A Holistic Approach, EPFL Press English Imprint, 2011, P.P. 135.145.

[11] محمد زيتون، **القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية**، متوافر على موقع المجلة العربية للنشر العلمي، الرابط: https://cutt.ly/Urmut6M8، تاريخ الزيارة 1-6-2025.

[12] نفس المصدر

الهدف	-كسب القلوب والعقول، تحسين الصورة، نشر القيم	-شلّ البنية التحتية، إضعاف الأنظمة، التأثير بالقوة
المجال القانوني	-غالبًا قانوني، ضمن حرية التعبير أو الثقافة	-غالبًا غير قانوني، يُعدّ عدوانًا سيبرانيًا أو جريمة إلكترونية
الفاعلين	-الحكومات، القراصنة، شركات كبرى، أفراد، كيانات لادولاتية	-الحكومات، منظمات إجرامية وإرهابية، شركات كبرى، أفراد، كيانات لادولاتية
الطبيعة	-افتراضية صرف: برمجية – معلوماتية	-افتراضية ومادية ملموسة – إلكترونية

ج-العلاقة بين القوة السيبرانية والقوة التقليدية: تُعد العلاقة بين القوة السيبرانية والقوة التقليدية علاقة تكاملية وتنافسية في آنٍ معًا. فالقوة السيبرانية، رغم طابعها الافتراضي، إلا إنّها عنصر أساسي في دعم أدوات القوة التقليدية وخاصة بعدما أصبحت معظم الأدوات الوسائل التقليدية ذات وجه رقمي يمكن التحكم بها عن بعد ولاسيما القدرات العسكرية، فأصبحت القوة السيبرانية تعزز القوة العسكرية لا سيما في الحرب الهجينة او الذكية لجمع المعلومات الاستخباراتية، والتحكم بالأسلحة الذكية، والطائرات المسيّرة. وخاصة بعدما أصبحت العمليات السيبرانية جزءًا من الاستراتيجية العسكرية الشاملة، في الحروب الهجينة (hybrid warfare) تستخدمها الدول لتعزيز عملياتها العسكرية في جمع المعلومات الاستخباراتية، والتأثير في الرأي العام لخدمة أهدافها السياسية. في المقابل، تتحدى القوة السيبرانية النمط التقليدي للنفوذ، حيث تمنح فاعلين من خارج الدولة (كالأفراد والمجموعات غير النظامية) القدرة على التأثير على دول وجيوش كاملة، دون الحاجة إلى قوة عسكرية أو موارد ضخمة. وبينما تبقى القوة التقليدية مرتبطة بالجغرافيا والوجود المادي، وتتجاوز القوة السيبرانية هذه الحدود، وتُحدث تأثيرًا يمتد من الفضاء الافتراضي إلى الواقع، مما يجعلها قوة هجينة تُعيد تشكيل ميزان القوى في العالم المعاصر، يوضح جدول رقم (2) مقارنة لخصائص القوة التقليدية والسيبرانية.

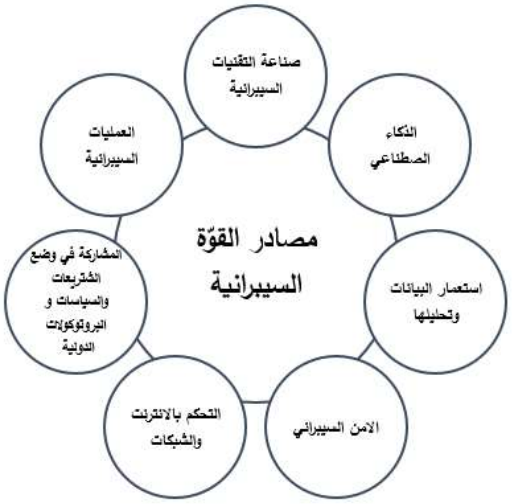
جدول (2) مقارنة بين القوة التقليدية والقوة السّيبرانيّة[13]

الخاصية	القوة التقليدية	القوة السيبرانية
الشكل	مادي (جيوش، سلاح، احتلال)	غير مادي (بيانات، برامج، شبكات)
حدود النفوذ	جغرافية ومباشرة	عابرة للحدود وغير مرئية
أدوات السيطرة	أسلحة، قواعد عسكرية، ضغوط اقتصادية	اختراقات، هجمات رقمية، تضليل إعلامي
مدى التأثير	فوري ومحسوس	تدريجي أو مفاجئ، وأحيانًا غير قابل للاكتشاف
الجهات الفاعلة	دول وجيوش رسمية	دول، شركات، أفراد، جماعات لا دولية
تطويرها	داخلي	داخلي، وعن بعد بدون حدود
الاسناد	سهل اسناد الهجمات	صعب اسنادها
قياس القوة	مدركة يمكن قياسها والشعور بها	غامضة غير قابلة للقياس والاستعراض

[13] محمد زيتون ، مصدر سابق.

الفاعلين	عادة الدول وبعض المقاومين	الدول – الشركات-الافراد – المنظمات
الهدف	مراكز عسكرية ومقومات الدول	بنية تحتية والأصول ذات الوجه الرقمي
التكلفة	مرتفعة	منخفضة
المجال	المجالات داخل الاقليم	كل المجالات المرقمنة
التنفيذ	يصعب تنفيذها	سهلة التنفيذ

4.مصادر القوة السيبرانية: تتمثل في مجموعة من العوامل والإمكانات التي تُمكّن الدول أو الفاعلين التأثير والتحكم في الفضاء السيبراني لتحقيق أهداف استراتيجية أو تكتيكية. وتشمل التكنولوجيا المتقدمة والبنية التحتية الرقمية التي تمكّنها من الصناعة السيبرانية والامن السيبراني التي تمنحها إمكانيات الهجوم والدفاع السيبراني، والذكاء الاصطناعي، والقدرة على جمع وتحليل البيانات الضخمة التي تمكن الجهة من القدرة على التأثير المعلوماتي والدعاية والرأي العام وتوجيه السياسات الاقتصادية خدمة في تحقيق الأهداف السياسية والاستراتيجية، وكذلك القدرة في التحكم في شبكات الاتصالات والبنية التحتية الحيوية. ومن إحدى مصادرها وجود لدى الجهة الموارد البشرية المؤهلة، إلى جانب وجود أطر قانونية وتشريعية متطورة تساعد على تنظيم الفضاء السيبراني وحمايته من التهديدات وحماية السيادة السيبرانية والمصالح الرقمية من الأنشطة السيبرانية.



رسم 1 مصادر القوة السيبرانية

وإلى جانب المصادر الآنفة في رسم (1)، هناك شركات كبرى مثل (جوجل، ومايكروسفت) وكيانات ومؤسسات دولية تمتلك بعض موارد الانترنت كالسحابة، ومراكز التخزين الدولية، وواضعي البروتوكولات وأفضل الممارسات لتحسين الانترنت والشبكات بما يتماشى مع أهدافها الاقتصادية والسياسية، لها أثر كبير على توجيه القوة السيبرانية أو تقييدها وعلى مجالات اخرى مذكورة في الجدول(3). وهذه المجالات هي سبب للصراعات الناشئة والحوار الدائم بين الصين وروسيا وامريكا والغرب بسبب رقمنة الفكر الشيوعي والليبرالي في الفضاء السيبراني.

جدول(3) الجهات الدولية التي تؤثر على القوة السيبرانية			
المجال	**كيف تدعمه الجهات الدولية**	**أثره على القوة السيبرانية**	**الجهة**
الأمن	تطوير المعايير والبروتوكولات	حماية البنى التحتية	IETF, ITU, W3C)
السيادة	إدارة أسماء النطاقات وIP	استقلال رقمي	ICANN, RIRs)
الابتكار	دعم تقنيات جديدة	تفوق تقني	W3C, IETF, ISOC)
السياسات	التأثير في الحوكمة العالمية	نفوذ سيبراني	ITU, IGF, OECD)
التعاون	التحالفات وتبادل المعلومات	ردع جماعي	ISOC, IGF, ITU)

- **المطلب الثّاني: عتبة استخدام القوّة السيبرانيّة**

في عالمنا المعاصر، بات الفضاء السيبراني يشكّل بعدًا استراتيجيًا جديدًا في معادلات القوة والنفوذ بين الدول والجهات الفاعلة. ومع تزايد الاعتماد على التكنولوجيا والبنية التحتية الرقمية، ظهرت القوة السيبرانية كأحد أبرز أشكال القوة الحديثة التي يصعب تحديد معالمها أو قياس آثارها المباشرة. فهي قوة غير ملموسة، لا يُشعر بها إقليميا أو دوليا، ولا يُمكن تتبّعها بسهولة او تحديد العتبة التي تحدثها، مما يجعل من مسألة إسناد العمليات السيبرانية إلى جهة معيّنة تحديًا حقيقيًا، خصوصًا حين تُستخدم في إطار المنطقة الرمادية الواقعة بين السلم والحرب. وعند التعمق في مفهوم القوة السيبرانية، نجد أنها تقوم على أسس تكنولوجية ديناميكية، تتميز بالمرونة في التطور والقدرة على تجاوز الحدود الجغرافية دون قيود. وتشمل هذه القوة مزيجًا من العمليات السيبرانية الهجومية والدفاعية، بالإضافة إلى التملّك الرقمي للمنصات والبيانات، واستعمار الفضاء الرقمي واحتكار أدوات البحث والسيطرة على تقنيات الذكاء الاصطناعي والبيانات الضخمة، مما يمنح الجهات الفاعلة قدرة هائلة على التأثير في البنية المعلوماتية العالمية.

1.عتبة القوّة السيبرانيّة (Cyber power Threshold) تشير إلى النقطة أو الحد الذي يتسبب فيه هجوم سيبراني في إحداث تأثيرات تعادل تلك التي تترتب على استخدام القوة التقليدية (مثل الهجمات العسكرية)، وبالتالي قد تبرر ردًا عسكريًا أو سياسياً مباشراً. بمعنى آخر، هي النقطة التي يتحول عندها الهجوم السيبراني من مجرد أداة تخريبية إلى عمل عدواني يُعادل الحرب أو انتهاك السيادة او تصعيد نحو الحرب في نظر الدولة المستهدفة.[14] والعتبة التي تُحدثها القوة السيبرانية تتحقق عندما تنتقل الدولة أو الجهة من الاستهلاك إلى التحكم والتأثير في المجالات الأربعة: العمليات السيبرانية، التكنولوجيا، البيانات، والذكاء الاصطناعي. كلما زاد التحكم الذاتي، وزادت القدرة على التأثير خارج الحدود، زادت قيمة القوة السيبرانية.

سنوضح في كل ما يلي عتبة كل مجال من مصادر القوّة السيبرانيّة أو السيطرة العليا التي يمكن للقوة السيبرانية احداثها في التأثير لتحقيق المزايا التي نريدها في تحقيق الاهداف:

2. **مجال العمليّات السيبرانية:(Cyber Operations)** أولا إنّ مفهوم "العمليات السيبرانية" يُعد المفهوم الأشمل الذي تندرج ضمنه كل أنواع الأنشطة السيبرانية سواء الهجومية والدفاعية أو أي نشاط آخر يهدد أو يستهدف كيانًا رقمياً بهدف تعطيله او تدميره. فكل فعل يؤثر على بنية رقمية يُعد جزءاً من العمليات السيبرانية. وما يُعرف بـ"الحرب الصامتة"، أو "حرب الأصفار" أو "الحرب السيبرانية"، كلها مفاهيم تستخدم نفس الأدوات والأساليب وتقع ضمن نطاق العمليات السيبرانية. والجدير بالذكر أن "الحرب السيبرانية" هي في الأصل مصطلح تم تبنّيه في الاروقة الأكاديمية، ولا يُعبر بالضرورة عن "حرب" بالمعنى التقليدي، بل يُقصد بها غالبًا عمليات تجسس رقمية او تسلل رقمي وتتبع او استهداف شبكي يؤثر على العمل الخدماتي للجهة أو الخصم.

(14) Solange Ghernaouti-Helie, Cyber Power Crime, Conflict and Security in Cyberspace, CRC Press, USA, 2016, P.P. 174-179

يشهد العالم تصاعد في الهجمات السيبرانية يوميا، تقدر بحوالي 600 مليون هجمة يوميا، ومعظمها يتم التعامل معها معظمها من الاحتيال المالي، إعلانات مزيفة التصيد الاحتيالي، هجمات DDoS، وهجمات الهندسة الاجتماعية، وتتبع مايكروسفت من خلال وحداتها الاستخباراتية التهديدات أكثر من 1500 مجموعة رقمية اجرامية، بما في ذلك أكثر من 600 تهديد على مستوى الدولة، و300 مجموعة جرائم إلكترونية، و200 مجموعة عمليات تأثير، ومئات المجموعات الأخرى.[15] وشهدنا هجمات متفرقة على مدى سنوات وأبرزها:

- **Stuxnet (2010)**: هجوم سيبراني ضد المنشآت النووية الإيرانية، يُعتبر أول استخدام معروف لسلاح سيبراني أحدث ضرر مادي تجاوز عتبة الضرر التقليدي لكنه لم يُقابل برد عسكري مباشر.
- **الهجمات على أوكرانيا (2015–2022)** استخدمت روسيا هجمات سيبرانية متزامنة مع العمليات العسكرية لتخريب البنى التحتية (الكهرباء، الإعلام، الاتصالات).
- هجوم **WannaCry** الذي وقع في مايو 2017 يُعد من أخطر هجمات برامج الفدية التي استهدفت قطاع الرعاية الصحية، وخاصة المستشفيات. استغل الهجوم ثغرة أمنية في أنظمة تشغيل ويندوز تُعرف باسم **MS17-010**، ما سمح للبرمجية الخبيثة بالانتشار بسرعة عبر الشبكات المحلية والعالمية، وتم إلغاء أكثر من 19,000 موعد طبي، بما في ذلك عمليات جراحية حرجة، وتأثرت الخدمات الصحية بشكل كبير، وتعطل أكثر من 1,200 جهاز طبي تشخيصي، واضطرت بعض المستشفيات إلى إخراج أجهزة أخرى من الخدمة كإجراء احترازي لمنع انتشار الفيروس.
- **هجوم SolarWinds (2020)** اختراق واسع للوكالات الأمريكية، لم يُصنّف كعمل حربي لكنه أثار مخاوف استراتيجية كبرى بسبب الوصول الى بيانات حساسة، ويعتقد أنه الهجوم الأول الذي تم باستخدام الذكاء الاصطناعي لأنه تماهى بأنه شهادة تحديث من مورد الانظمة.
- **هجمات البيجر(2024)** : هجمة غير مسبوقة استهدفت عناصر حزب الله عبر تفجير متزامن لآلاف أجهزة "البيجر" اللاسلكية التي كان يستخدمها عناصر الحزب في الاتصالات الداخلية. هذه الأجهزة، التي استُخدمت كوسيلة اتصال منخفضة التقنية لتفادي الرقابة الإسرائيلية، تم تفخيخها مسبقاً بمتفجرات دقيقة من خلال اختراق سلاسل الامداد، وتم تفجيرها عن بُعد في لحظة واحدة، ثمّ عقبها موجة انفجارات هزت الضاحية الجنوبية لبيروت ومناطق أخرى واستشهد ما لا يقل عن 12 شخصاً بينهم طفلان، وأصيب حوالي 2800 آخرين، بينهم نحو 300 في حالة حرجة، وفق وزارة الصحة اللبنانية.[16]

وفي سياق كتابة هذا البحث، ونحن نشهد حرب هجينة بين إيران وإسرائيل تعتبر نموذج للحرب الذكيّة التي استخدم فيها طائرات بدون طيار، وأدوات الذكاء الاصطناعي، وهذه الهجمات السيبرانية مثلّت تحولاً نوعياً في أساليب الصراع، حيث استُخدمت التكنولوجيا والذكاء الاصطناعي كسلاح فعّال لتعطيل البنية التحتية الحيوية، التأثير على الاقتصاد، وزعزعة الاستقرار الداخلي، إلى جانب العمليات العسكرية التقليدية. هذه الحرب أظهرت هشاشة الأنظمة الحيويّة أمام الهجمات السيبرانيّة، وأكدّت إنّ الأمن السيبراني بات جزءاً لا يتجزأ من الأمن القومي للدول المتصارعة، وإنّ هناك احتماليّة لقدرة العمليات السيبرانية إحداث ضرراً يعطّل القدرات العسكريّة المتصلة رقميا.[17]

كل هذه الأفعال تُصنّف انتهاكًا للقانون الدولي والأعراف الدولية، خصوصاً فيما يتعلق بالاستخدام السيبراني كوسيلة ألحقت ضرراً بالمدنيين كالبنية التحتية الحيوية المدينة، والشبكات المشتركة المدنيّة والعسكريّة، ومراكز الرعايا الصحيّة. وهذا ينذر إنّ هناك تتصاعد في عتبة العمليّات السيبرانيّة بعد وصولها الى أماكن حساسة ووصلت الى مرحلة الانفجارات خاصة الاستهداف السيبراني الأخير الذي أدى الى إراقة دماء في تفجير البيجر في لبنان. [18] ولكن رغم الضرر الذي تحدثه العمليات السيبرانية إلاّ إنها بحاجة إلى هدف رقمي للوصول، فالعتبة العليا هنا مرتبطة بالوصول الرقمي عبر الانترنت أو الشبكة، والحرب الإيرانية الإسرائيلية كانت أبرز مثال عندما أوقفت السلطات الإيرانية الانترنت لعدة أيام قوّض عتبة هذه القوة وشل قدرتها.

3. **مجال الاستعمار الرقمي:** الاستعمار الرقمي أصبح شكل جديد من الهيمنة العالمية وأصبح نمط معاصر من السيطرة تمارسه شركات التكنولوجيا الكبرى والدول القومية، من خلال الهيمنة على البيانات والبنية التحتية الرقمية في دول الجنوب العالمي. يُعيد هذا المفهوم إنتاج

---

[15] Microsoft Digital Defense Report: 600 million cyberattacks per day around the globe, Link:, https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/, accessed date 9-5-2025.

[16] نتنياهو وافق على هجمات بأجهزة بيجر متفجرة على حزب الله، متوافر على موقع سويس إنفو،11-11-2024، الرابط:، https://cutt.ly/orEAegFm، تاريخ الزيارة 1-6-2025.

[17] البيانات أقوى من الرصاص: تأثير الهجمات السيبرانية على الأمن القومي، 12-6-2025، متوافر على موقع نيوز روم، الرابط:https://newsroom.info/88166 ، تاريخ الزيارة 1-6-2025.

[18] محمد زيتون ، العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني، متوافر على موقع المجلة العربية للدراسات السياسية، الرابط: https://cutt.ly/4rmc7WmZ العدد (77)، تاريخ الزيارة 2-6-2025.

منطق الاستعمار الكلاسيكي، لكن بأدوات رقمية، حيث تُصبح البيانات هي المورد الجديد، والخوارزميات وسيلة للنفوذ، ومنصات التواصل فضاءً للسيطرة على الوعي وتوجيه الرأي العام. ومن خلال التحكم في شبكات الاتصال ومحركات البحث والسياسات الرقمية، تُقيد هذه الشركات السيادة الوطنية وتُعمق الفجوة الرقمية والثقافية بين المركز والأطراف.[19]

كما إن توزّع مفهوم الاستعمار الرقمي على جهات فاعلة متعددة كالشركات التكنولوجيا الغربية (غوغل، ميتا، أمازون، مايكروسوفت)، وشركات الإعلان والاستشارات التي تستفيد من البيانات المستخرجة، والشركات والأحزاب والمنظمات المحلية التي تستخدم هذه الأدوات لتحقيق أجنداتها. وأبرز الأمثلة محاولة فيسبوك فرض تطبيق Free Basics في الهند، الذي قُدّم كمبادرة خيرية لكنه في الواقع كان يقيد حرية الوصول للإنترنت ويمنح فيسبوك سيطرة على ما يمكن للمستخدمين الوصول إليه من محتوى.[20] والى جانب ما أشرنا الاستعمار الرقمية يلعب دورا كبيرا في عدة قضايا رقمية ويمنحها قدرة في التحكم بالعلاقات الدولية ويعطي الدول او الجهات الفاعلة سيطرة رقمية عليا في تحقيق الأهداف او توجيه المصالح وذلك عند استخدامها في تقييدها على الدول النامية او تجاه الدول التي تقييد سيادة بياناتها.

4.الاستحواذ التكنولوجي (technological acquisition): يُعد الاستحواذ وسيلة استراتيجية متكررة بين الشركات الكبرى والناشئة، بهدف تسريع الابتكار أو سد فجوة تقنية أو الدخول إلى أسواق جديدة، أو تعزيز القدرات التنافسية عبر الاستفادة من المعرفة والأصول التقنية للشركة المستهدفة. ولكن بسبب عسكرة الفضاء السيبراني تسعى بعض الدول القومية والشركات الكبرى، السيطرة على البيانات الضخمة يتيح للشركات العملاقة تعزيز قدراتها في جمع وتحليل البيانات، ما يمنحها ميزة تنافسية وهيمنة فريدة في تطوير الذكاء الاصطناعي. او بهدف بناء أنظمة بيئية مغلقة تجبر المستخدم (الدول والشركات، والافراد) على البقاء ضمنها، مثل ما يحدث مع جوجل أو ميتا (فيسبوك سابقاً)، ما يزيد من صعوبة انتقال المستخدمين إلى منصات أخرى ويعزز التبعية الرقمية. وكما تساهم في التأثير على السياسات والاقتصادات التأثير في السياسات الاقتصادية وحتى القرارات السيادية للدول، خاصة في ظل اعتماد الحكومات والشركات على البنى التحتية الرقمية وخدمات السحابة التي تديرها هذه الشركات. هذا النفوذ يُستخدم أحياناً كورقة ضغط جيوسياسية، كما حدث في العلاقة بين الولايات المتحدة وأوروبا.[21] وكما يعطيها قوة لتعزيز النفوذ الجيوسياسي عندما تحمل صفقات الاستحواذ أبعاداً سياسية وعسكرية، كما في حالة استحواذ جوجل على "ويز" الإسرائيلية، حيث ساهمت الصفقة في تعزيز نفوذ إسرائيل في مجال الأمن السيبراني، ودعمت مكانتها الإقليمية والدولية.[22] وهذا النوع من الهيمنة يمكن تصنيفه قوة سيبرانية صلبة بدون هجمات إنما شكل من اشكال الاستعمار الذي أشرنا اليه. لذلك نلاحظ **إن** بعض الدول لا تعتمد الدولة على مزودي خدمات أو برمجيات أجانب في البنية التحتية الرقمية الأساسية، وتحاول توطين قدراتها على تطوير أنظمة تشغيل، ومعدات اتصالات، وتشفير محلية كالصين وروسيا، اللذان يسعيان الى تقليل اعتمادهم على التكنولوجيا الأمريكية او المعادية، لذلك لجأت كل من الصين وروسيا الى تطوير "شبكات الجيل الخامس" و"أنظمة تشغيل " وطنية. وتبرز العتبة في هذا السياق، بعض الدول تسعى الى امتلاك أو تطوير تكنولوجيا متقدمة محليًا تضمن الاستقلال السيبراني والسيادة التقنية. والبعض الاخر يستفيد من التملك الرقمي والقدرات الرقمية في استخدامها في الحروب، على سبيل المثال إن تشعب إسرائيل في عمق الشركات الضخمة وجعلتها وسيلة في يدها اعطتها عتبة سيطرة عليا في إيقاف الخريطة الرقمية فوق قطاع غزة، والتسلل الى شبكة البيجر التابعة لحزب الله واستخدمتها في تحقيق اهداف عسكرية. وبعض الشركات تستخدمها في التحكم في المنصات مثل منصة (x) تويتر سابقا التي قيدت رئيس الولايات المتحدة ترامب من استخدام تويتر وتطبيقات أخرى. وهناك تقنيات ناشئة ذات الصلة أبرزها:

أ-البيانات الضخمة (Big Data Ownership): يتحقق التأثير السيبراني عند امتلاك منصات رقمية واسعة (مثل وسائل التواصل) تجمع بيانات ملايين المستخدمين. القدرة على تحليل البيانات لاكتشاف أنماط، تنبؤات، أو توجيه قرارات استراتيجية. استخدام البيانات لأغراض استخباراتية، اقتصادية، أو دعائية. مثل Google وMeta تمتلك "قوة سيبرانية ناعمة" لأنها تملك وتتحكم ببيانات المليارات. لفرض اليات التسويق والتوجه الرقمي. وتتحقق العتبة بالقدرة على تجميع وتحليل كميات ضخمة من البيانات بهدف الاستخلاص الذكي للمعلومات أو التأثير الاستراتيجي على الجهات الأخرى.

ب-**البنية التحتية التي تجمع البيانات:** هي عتبة قوة تحققها القوة السيبرانية في جميع البيانات مثل شبكات الإنترنت، تطبيقات الهواتف، وسائل التواصل الاجتماعي، محركات البحث. القوة السيبرانية تُمارس هنا عندما تفرض تطبيقاتها (مثل TikTok، Google، Facebook) نفسها في أسواق الدول الأخرى. وتكون عتبة السيطرة: عندما تصبح البيانات الخاصة بمواطني دولة ما تُجمع وتُخزن وتُحلل في دولة أجنبية دون رقابة محلية حقيقية. وهنا قد يتمكن الخصوم او الفاعلين خلق تبعية رقمية طويلة الأمد وتصبح الدول أو الشعوب تصبح معتمدة على التكنولوجيا

---

(19) الاستعمار الرقمي.. الجنوب العالمي أمام شاشات مغلقة، متوافر على الموقع الجزيرة الإلكتروني، الرابط:https://institute.aljazeera.net/ar/ajr/article/2962، تاريخ الزيارة 2-5-2025.

(20) Facebook’s Free Basics service has been banned in India, https://www.theverge.com/2016/2/8/10913398/free-basics-india-regulator-ruling

(21) التفوق الرقمي الأميركي يربك أوروبا..هل آن أوان الانفصال؟، متوافر على موقع العربية ، https://cutt.ly/wrEPJle4 ، تاريخ الزيارة 2-5-2025.

(22) استحواذ جوجل على "ويز" الاسرائيلية ..هل مجرد صفقة اقتصادية بحتة أم تحمل دلالات سياسية وعسكرية ايضا ؟، متوافر على موقع عالم رقمي،13-4-2025، الرابط: https://cutt.ly/3rEPJP47، تاريخ الزيارة 2-5-2025.

الأجنبية التي تتحكم في بياناتها. يصعب الفكاك من هذا النوع من "الاستعمار" لأنه غير مرئي، وغير عسكري. وهنا تكون عتبة السيطرة العليا عجز الدول على تطوير أنظمتها الرقمية، وتصبح رهينة لشركات أو دول أخرى تملي عليها السياسات الرقمية.

ج- الذكاء الاصطناعي (Artificial Intelligence): أصبح الذكاء الاصطناعي إحدى القدرات الناشئة الذي يميز الدولة بامتلاكها تكنولوجيا يجعلها فريدة عن غيرها ويعطيها أولوية على فرض رأيها واتجاهات الاقتصاد الرقمي، ويضيف الى اقتصادها والى قوتها العسكرية أدوات استراتيجية كاستخدام الذكاء الاصطناعي في الأمن السيبراني (مثل كشف التهديدات). او توظيفه في الطائرات المسيّرة، نظم الدفاع، الروبوتات العسكرية، أو الاغتيالات في (لبنان 2024 –ايران2025). أو في تطوير نماذج لغوية أو تحليلية تؤثر في الوعي الجماهيري أو صناعة القرار. وتكون عتبة السيطرة في امتلاك أنظمة ذكاء اصطناعي قادرة على اتخاذ قرارات ذات طابع استراتيجي أو قتالي أو تحليلي مستقل.

5.استقلال السيادة السيبرانية (Cyber Sovereignty) السيادة السيبرانية هي حق الدولة في التحكم الكامل بمحتوى، وبيانات، وبنية، وسياسات الإنترنت داخل حدودها السيادية، بما يشمل من يحق له الوصول إلى الإنترنت داخل الدولة، كيفية تنظيم البيانات ومرورها، الرقابة على المنصات والمحتوى، فرض القوانين المحلية على الفضاء السيبراني، تمامًا كما تُفرض على الأرض بالإضافة الى صياغة القوانين المحلية، وتبرز القوة السيبرانية المتمثلة بقدرة التحكم على البيانات والمراقبة تحدد عمل الانترنت، وكيفية استخدام الانترنت. فتكون عتبة السيطرة العليا داخليا على المواطنين، وخارجية بعدم مشاركة البيانات وتدفقاته باعتبارها أصل افتراضي للدولة وذلك يقوض المنفعة العامة وعدم مشاركتها في البحث الخارجي وداوت الذكاء الاصطناعي بما يعرف البيانات الضخمة. وأبرز الأمثلة، مفهوم السيادة السيبرانية لدى الصين وروسيا وكوريا الشمالية وإيران فهذه الدول لا تسمح بتدفق بياناتها بل تستخدم أنظمة كومبيوتر وبيئة خاصة بها حفاظا على أمنها القومي وخوفا من النهب الرقمي للبيانات واحتكارها لصالحها في فوائد الذكاء الاصطناعي، او خشية من جعلها تبعية رقمية للدول المستعمَرة لصالح المستعمِر. او خشية من سيطرة كيانات (دول، شركات، أو تحالفات) على بيانات شعوب أو دول أخرى دون موافقتها أو دون قدرة تلك الدول على حماية بياناتها واستخدام البيانات كوسيلة للهيمنة الاقتصادية والسياسية والثقافية، وهنا تبرز قدرة الدولة السيبرانية خارجيا على سيادة بيناتها وأصولها الافتراضية خارج وداخل حدودها الإقليمية.[23]

6.مجال الردع السيبراني: هو مفهوم حديث في مجال الأمن والدفاع، ويُقصد به منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني، ويرتكز الردع السيبراني على ثلاث ركائز رئيسية مصداقية الدفاع على حماية الأصول الرقمية والرد على الهجمات، والقدرة على الانتقام بامتلاك وسائل فعالة للرد على أي هجوم سيبراني بشكل مؤلم للمهاجم، والرغبة في الانتقام من خلال إظهار الاستعداد السياسي والعسكري لاستخدام هذه القدرات عند الضرورة، ولكن يواجه إشكاليات عديدة أهمها: مشكلة الإسناد، وعدم القدرة في قياس عتبة القوة السيبرانية، وتعدد الفاعلين. إلا إنّ هناك استراتيجيات مقترحة لتحقيق عتبة ما، كالردع السلبي لجعل الهجمات أقل جدوى وأسهل في الاكتشاف، والردع بالعقاب كالتهديد أو تنفيذ ردود مؤلمة (سيبرانية أو عسكرية) ضد المهاجمين. او العقوبات الاقتصادية والدبلوماسية كفرض عقوبات على الدول أو الجهات التي يثبت تورطها في هجمات سيبرانية، وهي الأكثر شيوعا، ففي سياق الردع السيبراني أصبحت العقوبات الاقتصادية تُستخدم كأداة ردع "واقعية"، وتُفعّل عندما تتجاوز الهجمات السيبرانية "العتبة" التي تمس الأمن القومي أو المصالح الاستراتيجية. وهذه الاستراتيجية تربط بين المجالين الرقمي والواقع، وأبرز الأمثلة حيال ذلك، العقوبات الأمريكية على روسيا بسبب هجمات SolarWinds السيبرانية.[24] وعقوبات على كوريا الشمالية بسبب هجومWannaCry عقوبات على كيانات صينية يُعتقد أنها مسؤولة اختراقات اقتصادية وتجارية لسرقة أسرار تجارية أو استراتيجيات شركات كبرى، مما يمكن أن يُعادل مليارات الدولارات من الخسائر وعلى سبيل المثال إيران وكوريا الشمالية، وكوريا الشمالية تستخدم العديد من الهجمات السيبرانية لتمويل أنظمتها السياسية.[25]

- المبحث الثّاني: أثر القوّة السيبرانيّة في العلاقات الدولية المعاصرة

شهد مفهوم القوّة السيبرانية في العلاقات الدولية تحوّلات كبيرة تماشياً مع التغيرات في البيئة الاستراتيجية والتكنولوجية. حيث أوجد الفضاء السيبراني مجالًا افتراضيًّا تتفاعل فيه الدول والكيانات اللادولاتية[26] ضمن صراعات وعلاقات جديدة. ويعتبره العديد من الباحثين المجال الحيوي الخامس بعد البر والبحر والجو. تستخدم الدول والكيانات اللادولاتية القدرات السيبرانية لتحقيق مصالحها الرقمية. وقد أدت مشاركة هذه الكيانات في هذا الفضاء إلى نشوء صراعات رقمية خارج إطار سلطة الدولة، تشارك فيها الحركات الاجتماعية والتنظيمات المرتبطة بالقوى الكبرى، ومن أبرزها مجموعة "دب الغسيل(Fancy Bear) "، التي تُعد من أخطر القراصنة الروس وتشكل الذراع السري للكرملين، بالإضافة إلى وحدة جيش التحرير الشعبي الصيني رقم 61398 وغيرها من الوحدات العسكرية الناشئة داخل الجيوش وخارجها. كل هذا

[23] Munish Sharma, Building China Into a Cyber Superpower Desires, Drivers, and Devices, Taylor & Francis,2024, New Delhi ,P.4

[24] محمد زيتون، رسالة دكتوراه غير منشورة، نحو استراتيجية دولية للأمن السيبرانية لمواجهة تداعيات العمليات السيبرانية، جامعة بيروت العربية، 2024.

[25] نفس المصدر.

[26] مصطلح ناشئ يستخدم في المقالات السياسية يعبّر عن: فاعلين جدد من غير الدول.

جعل الفضاء السيبراني أكثر فوضوية من النظام الدولي التقليدي، وشجّع الدول على السعي لتحقيق مصالحها من خلال ما يُعرف بـ"المنطقة الرمادية" (Gray Zone)، وهي المنطقة الفاصلة بين السلم والحرب، مستفيدة من انخفاض عتبة استخدام القوة السيبرانية.

- المطلب الأوّل: التحولات والتغيرات التي طرأت على العلاقات الدولية في ظل القوّة السيبرانيّة

شهد مفهوم القوة في العلاقات الدولية تطورًا نوعيًا، فلم يعد مقتصرًا على الأدوات التقليدية كالقوة العسكرية أو الاقتصادية، بل امتد ليشمل أشكالًا غير تقليدية وفي مقدمتها القوة السيبرانية. فقد أدى تصاعد الاعتماد على التكنولوجيا والمعرفة الرقمية إلى بروز الفضاء السيبراني كمجال استراتيجي فاعل في تشكيل التفاعلات الدولية، ما أتاح لجهات جديدة سواء دولاً صغيرة أو فاعلين من غير الدول القدرة على التأثير في النظام الدولي. مما جعل القوة السيبرانية أداةً رئيسة في إدارة الصراع والتنافس بين الكيانات، مما عكس تراجعًا نسبيًا في مركزية القوة التقليدية، ويؤشر إلى مرحلة جديدة في بنية العلاقات الدولية، تتسم بتحولات في ديناميكية الفضاء الرقمي و معادلات القوة والتأثير.

1.دور الفضاء السيبراني في تحولات العلاقات الدولية: ظهر مصطلح "الفضاء السيبراني" لأول مرة في أدب الخيال العلمي، وتحديداً في رواية "نيورومانسر" للكاتب ويليام جيبسون عام 1984، ثم أصبح يُستخدم على نطاق واسع في مجالات التكنولوجيا، الأمن السيبراني، والعمليات العسكرية، حتى أصبح يعبّر عن بيئة مركبة تضم عناصر مادية (مثل الأجهزة والشبكات) وافتراضيّة (كالبرمجيات والمعلومات) يُستخدم لتسهيل التواصل، تبادل البيانات، المشاركة الاجتماعية، ممارسة الأعمال التجارية، وغيرها من الأنشطة والمصالح الرقمية التابعة للدول والافراد والشركات الكبرى. ويؤكد هذا المفهوم التعريف الذي قدّمه المعهد الوطني للمعايير والتقنية (NIST) للفضاء السيبراني، بأنّه مجال افتراضي ينشأ من خلال الربط بين أجهزة الحاسوب، الشبكات، البرمجيات، البنية التحتية الرقمية، وأنظمة الاتصالات، ويتيح نقل وتخزين ومعالجة البيانات والتواصل الإلكتروني بين المستخدمين حول العالم. وكما يشمل كل ما يتعلق بشبكات الحاسوب والإنترنت، من الأجهزة المادية مثل الكابلات والخوادم، والبروتوكولات، وتفاعلات المستخدمين أنفسهم.[27]

هذه التفاعلات جعلته مجالا حيويًا للمصالح والصراعات، وبيئة رقمية معاصرة تحدث فيها جميع التفاعلات والأنشطة الإلكترونية عبر الإنترنت، ليصبح اليوم أحد أهم المجالات في الدراسات الدولية بسبب التحولات الذي أحدثها على عناصر العلاقات الدولية، حيث أدى إلى إعادة صياغة القوة التقليدية وأتاح ظهور أشكال جديدة من القوة السيبرانية التي ساهمت في تعظيم القوة التقليدية، وتسريع التغيرات في بنية النظام الدولي، ابرزها: إعادة تشكيل مفهوم السيادة حيث لم تعد مقتصرة على الحدود الجغرافية، بل امتدت إلى الفضاء السيبراني حيث اصبح مصلحة ناشئة من مسؤوليات الدول حمايتها وحماية بياناتها وشبكاتها، وتطالب بعض الدول بـ"الاستقلال الرقمي" في ظل تصاعد الدعوات إلى "سيادة الإنترنت" ولا سيما الصين وروسيا اللتان تسعيان إلى توطين أنظمتهما، وتطوّران شبكات وطنية مغلقة. وكما أسهم الفضاء الى تحول في الفاعلين الاساسين في العلاقات الدولية مثل ظهور فاعلين غير دوليين مدعومين من شركات أو جماعات أيديولوجية، وشركات تكنولوجيا عملاقة (مثل Google، Microsoft، Amazon) تمارس نفوذاً أقرب إلى نفوذ الدول، في السياسات الرقمية والدبلوماسية التكنولوجية، وأصبحوا قادرين على التأثير في علاقات الدول.[28]

وبعدما أن أصبح الفضاء السيبراني ساحة جديدة لتحقيق المصالح السياسية والاقتصادية والأمنية، وميدانًا تتقاطع وتتنافس فيه أطماع القوى لتحقيق النفوذ والسيطرة، برزت تهديدات سيبرانية متزايدة تستهدف البنية التحتية الحيوية، والمعلومات الحساسة، وأنظمة الاتصالات، الأمر الذي جعل الأمن السيبراني أولوية استراتيجية لا غنى عنها لضمان الاستقرار وحماية المصالح الوطنية للدول. فالدول القومية مثل الولايات المتحدة، روسيا، الصين، إيران، وكوريا الشمالية أصبحت أبرز الفاعلين في هذا المجال وتستخدم الهجمات كأدوات غير تقليدية في -"الحرب الهجينة" ضمن مناطق رمادية أسست التنافس الجيوسياسي الرقمي بين القوى الكبرى حول صراعات على البنية التحتية العالمية للإنترنت، المعايير التقنية، والهيمنة على سلاسل الإمداد الرقمية (مثل شبكات G5 لشركة هواوي والذكاء الاصطناعي).

كما شهد العالم تحولات وتغيرات في مفاهيم القوة والنفوذ بحيث القوة لم تعد مقتصرة على الموارد العسكرية أو الاقتصادية، بل امتدت إلى "القوة السيبرانية" وأصبحت بعض الدول الصغرى تملك قدرات سيبرانية متقدمة تمكّنها من التأثير غير المتناسب في النظام الدولي وتستخدم النفوذ السيبراني في التأثير على الانتخابات، الرأي العام، والحرب النفسية والمعلوماتية. كل ذلك أدى الى تنامي مفهوم "الدبلوماسية السيبرانية" كأداة للتفاوض، وبناء تحالفات لحوكمة الإنترنت والأمن الرقمي وتعزيز الحركة الرقمية لوزارة الخارجية. مما جعلت القانون الدولي يعاني من فراغ تشريع في مفاهيم الفضاء السيبراني، ويفتقر إلى قواعد دولية واضحة تحكم سلوك الدول فيه حول قانونية الفضاء السيبراني، وعتبة العمليات السيبرانية (الهجومية والدفاعية) مما خلق انقسامات حول ما إذا كانت قوانين الحرب التقليدية تنطبق على الفضاء السيبراني وحول ما إذا كان مبدأ الردع والهجوم الوقائي يمكن توظيفه في هذا الفضاء الذي تحوّل الى ساحة رمادة لتحقيق المصالح والنفوذ.

---

[27] ما هو الأمن السيبراني؟،متوافر عل الموقع الإلكتروني، الرابط: https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html، تاريخ الدخول 25-5-2025.

[28] محمد زيتون، القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية، متوافر على موقع المجلة العربية للنشر العلمي،5-2-2025، الرابط: https://cutt.ly/VrT79fVz، تاريخ الدخول 25-5-2025.

2.نظريات العلاقات الدولية: إنّ مفهوم القوّة السيبرانية الديناميكي والمتغير مع التقدم التكنولوجي أحدث تحولا على مفهوم النظريات التي تعنى في دراسة ظواهر العلاقات الدولية، حيث دعت الليبرالية إلى التعاون الدولي لحوكمة هذا الفضاء، وركزت البنائية على الأبعاد الثقافية والمعيارية، وانتقدت النظرية النقدية هيمنة القوى الكبرى عبر التكنولوجيا، وبما أننا نتناول القوة السيبرانية في موضوعنا سنركز على النظرية الواقعية، والتي تعتبر من أهم النظريات في العلاقات الدولية التي تناولت افتراضاتها القوة، واعتبارها الدولة هي الفاعل الرئيسي في النظام الدولي الذي يتسم بالفوضى، مما يدفع الدول للاعتماد على الذات وتحقيق أمنها القومي بالقوة، لا سيما العسكرية. وبسبب بصعود القوة السيبرانية حيث رأت الواقعية الفضاء السيبراني ميدانًا جديدًا للصراع والمنافسة ويمكن إسقاط هذه المفاهيم على الفضاء السيبراني، الذي يشهد صراعًا غير تقليدي يشمل تهديدات وهجمات سيبرانية معقدة، تتطلب من الدول تعزيز قدراتها الذاتية، كما يتضمن مشاركة فاعلين جدد من غير الدول. ورغم أن الواقعية تفسر بعض الجوانب في هذا الصراع، إلا أنها تواجه صعوبات كبيرة في تفسير طبيعته الهجينة وغير المتكافئة، مثل صعوبة الردع، وتحديد الفاعل أو اسناد الهجمات، وتعدد مستويات التهديد، وضعف قدرتها على تفسير الصراعات غير الحربية أو التعامل مع الفواعل غير الحكومية.

إنّ تصاعد تعقيد العمليات السيبرانية، ووصولها إلى منشآت حساسة مثل المنشآت النووية في إيران، وأنظمة "سولارويندز" الأمريكية، أصبحت يشكل تهديدًا فعليًا للأمن القومي للدول. ورغم إدماج الذكاء الاصطناعي في بعض الأنظمة الدفاعية، فما تزال مسألة إسناد الهجمات السيبرانية وتحديد الفاعلين بدقة تمثل تحديًا كبيرًا. لذلك، يرى العديد من الباحثين أن دراسة القوة السيبرانية وتأثيرها في العلاقات الدولية لا تزال بحاجة إلى مزيد من البحث والتطوير على مستوى المفاهيم والنظريات، خاصة أن المدرسة الواقعية لم تولِ في بداياتها اهتمامًا كافيًا للقوة السيبرانية، نظرًا لتركيزها التقليدي على الأبعاد المادية الصلبة كالقوة العسكرية. لذلك، تواجه الواقعية عدة إشكاليات في تفسير الظواهر السيبرانية، منها:

- عدم تفسير الصراعات منخفضة الحدة: إذ تركز الواقعية على الحرب الكاملة، بينما لا يمكن إسقاط هذا التصور على الهجمات السيبرانية مثل الابتزازات أو استهداف البنوك.
- صعوبة تقدير القوة السيبرانية: القدرات السيبرانية هجينة وغير ملموسة، يصعب قياسها كما تُقاس القوة العسكرية، كما أن أهداف الدول تختلف؛ فدول مثل كوريا الشمالية أقل عرضة للهجوم رغم قوتها الهجومية بسبب فصل شبكاتها العسكرية عن المدنية.
- إشكالية الردع السيبراني: إنّ غياب إمكانية تحديد مصدر الهجوم، وضعف فاعلية الهجمات الانتقامية يضعف منطق الردع التقليدي الذي تقوم عليه الواقعية.
- الدفاع السيبراني: بخلاف توجه الواقعية نحو القوة الهجومية، يتطلب الفضاء السيبراني تركيزًا كبيرًا على الدفاع لحماية البنى التحتية.
- دور الفواعل من غير الدول: مثل القراصنة، والشركات التكنولوجية، والتنظيمات الإرهابية، وهي أطراف لا تحظى باهتمام كافٍ في النظرية الواقعية التي تركز على الدول فقط.[29]

إن فشل تفسير الواقعية للقوة السيبرانية يؤدي حتماً إلى تآكل الثقة في البيئة الدولية، نظراً لخصوصية الفضاء السيبراني الذي يتجاوز مفاهيم الجغرافيا والسيادة التقليدية. إذ إن الاعتماد المفرط على مقاربة واقعية ترى القوة السيبرانية فقط من منظور الهيمنة والردع يتجاهل التهديدات المعقدة مثل الهجمات المدعومة من دول، والتحيز الكامن في خوارزميات الذكاء الاصطناعي، وتكتيكات الإسناد المضللة. ففي حالات عديدة، كالهجمات على البنية التحتية الحيوية في دول مثل أوكرانيا أو هجماتSolarWinds ، نجد أن غموض الفاعل الحقيقي وغياب قدرة دقيقة على الإسناد قد قوض الثقة بين الدول. كما أن تحيز الخوارزميات – سواء في منصات التواصل أو أنظمة المراقبة – يعزز الشكوك ويكرّس الانقسامات، ما يضعف من مصداقية المؤسسات ويؤدي إلى بيئة يسودها الريبة بدلاً من التعاون. من هنا، فإن الاقتصار على التفسير الواقعي دون فهم الأبعاد التقنية والرمزية والاجتماعية للفضاء السيبراني يُنتج فراغاً في الثقة، يُستغل من قبل الفاعلين العدائيين ويُغذّي دوامة من عدم الاستقرار رغم توضيح الواقعية أن الدول تسعى لتطوير قدراتها السيبرانية دفاعًا عن أمنها، كما فعلت الولايات المتحدة مع شركة "هواوي" خوفًا من الاختراق.[30]

3.إعادة تعريف القوة وتوزيعها: شهد مفهوم القوة، ولا سيما القوة السيبرانية، تحولات جذرية في العصر الرقمي، أعادت تعريف جوهر القوة وأساليب ممارستها. أصبحت المعرفة التقنية، والقدرة على التأثير عبر الفضاء الإلكتروني من أبرز مكونات القوة الحديثة. فاليوم، تُقاس القوة السيبرانية بمدى امتلاك الفاعل للابتكار الرقمي، والذكاء الاصطناعي، والبنية المعلوماتية المتقدمة، والمهارات الرقمية، سواء لتحقيق أهداف صلبة كالأمن والدفاع، أو ناعمة كالتأثير الثقافي والإعلامي. هذا التحول رافقه تغير في توزيع القوة، إذ لم تعد حكراً على الدول، بل أصبحت موزعة بين فاعلين جدد من غير الدول، كالجماعات والمنظمات، وحتى الأفراد ذوي الكفاءة التقنية العالية، ما زاد من صعوبة تتبع مصادر التأثير والسيطرة. فبإمكان فرد أو مجموعة صغيرة أن تحدث تأثيراً عالمياً يفوق أحياناً تأثير دول بأكملها، نتيجة امتلاكهم أدوات رقمية متقدمة

(29) المصدر نفسه

(30) إيهاب خليفه، الحالة السـيبرانية في نظريات العلاقات الدوليـة: الحاجة إلى مراجعة جديدة، مذكرة الكترونية، رئاسة مجلس الوزراء، مصر، 2021.

أو استراتيجيات هجومية فعالة. هذا التشتت في مراكز القوة أدى إلى تعقيد المشهد السيبراني، وتراجع احتكار الدول للسيطرة على المعلومات وصنع القرار، ما يستدعي إعادة التفكير في الأطر التنظيمية والأمنية لمواكبة التحديات الجديدة التي فرضها هذا الفضاء المفتوح والمتغير باستمرار.

إنّ مفهوم القوة السيبرانية ليس فقط الهجمات السيبرانية، او التملك الرقمي، القوة السيبرانية هي تلك القوة الجانبية المتمثلة في العمليات السيبرانية (هجومية ودفاعية)، والتملّك الرقمي من صناعة الادوات السيبرانية المادية والافتراضية، والتحكم بالإنترنت والبيانات وكل المعقد والمركب التي يرتبط في تقنية المعلومات. ونظرا لهذا التراكم والتنوع أعاد تشكيلها ككرة ثلج تتدحرج وتتعاظم مع التقدم التكنولوجي، ومؤخرا أُضيف إليها الذكاء الاصطناعي، والبيانات الضخمة وصناعة الروبوتات. فسمة المرونة والديناميكية جعلها تنمو لتصبح من أبرز العوامل المؤثرة في العلاقات الدولية المعاصرة، حيث أعادت تشكيل مفهوم القوة التقليدي، وغيّرت من طبيعة التفاعلات بين الدول والجهات غير الحكومية، وفرضت تحديات وفرصًا جديدة في النظام الدولي. حيث جلعت الفضاء السيبراني مسارا لها و"ساحة خامسة" للصراع الدولي، إلى جانب البر، والبحر، والجو، والفضاء الخارجي، وعاملاً في تحديد النفوذ الدولي او المكانة الرقمية في الفضاء السيبراني.

لتؤثر على التفاعلات الدولية السياسية، وقد تؤدي الى نظام أحادي القطب، ثنائي القطب، او نظام متعدد الأقطاب، والذي بدوره يؤدي الى تحالفات جيوسياسية مثل الناتو، البريكس، منظمة شنغهاي. وكذلك تلعب التغيرات الاقتصادية وتأثيرها على موازين القوى العالمية، الى جانب الأيديولوجيا والقيم السياسية التي تحكم توجهات الدول المختلفة. وفي هذا السياق أكدّت التطورات التكنولوجية، خصوصًا في مجال الأمن السيبراني والذكاء الاصطناعي تلعب دورا كبيرا في التحويلات الدولية ولا سيما على صعيد التعاون السيبراني لمواجهة تداعيات القوة السيبرانية على السيادة والثقة بين الدول. وتتجلى أنواع التفاعلات الدولية السياسية في أشكال متعددة من العلاقات بين الدول، وتبرز القوة السيبرانية كأداة محورية تؤثر في هذه التفاعلات. ففي إطار التعاون الدولي، تتزايد أهمية الأمن السيبراني في الاتفاقيات والتحالفات الاستراتيجية، مثل تبادل المعلومات الاستخباراتية الإلكترونية.[31] أما في الصراع والتنافس، فقد أصبحت الحرب السيبرانية والتجسس الرقمي من أبرز أدوات المواجهة غير المباشرة. وتُستخدم الدبلوماسية اليوم عبر الوسائل الرقمية والقنوات الإلكترونية لتقريب وجهات النظر أو تصعيد الضغوط. وتُعد القوة السيبرانية جزءًا من التأثير غير المباشر، حيث تُستثمر منصات التواصل والاختراقات المعلوماتية للتأثير على الرأي العام وصناع القرار. كما تُستخدم العقوبات السيبرانية كوسيلة جديدة للضغط الاقتصادي، عبر تعطيل أنظمة مالية أو تجارية.[32] وأخيرًا، تُطرح قضايا الهجمات السيبرانية ضمن القانون الدولي، ما يستدعي تدخل المنظمات الدولية لتقنين استخدام هذه القوة ووضع ضوابط لها.

4.تطور مفهوم السيادة السيبرانية: شهد مفهوم السيادة السيبرانية تطورًا ملحوظًا مع التحولات الرقمية المتسارعة، إذ يشير هذا المفهوم إلى قدرة الدولة على فرض سلطتها على الفضاء السيبراني، بما في ذلك إدارة الإنترنت، حماية البيانات، والتحكم في تدفق المعلومات والبرمجيات ضمن نطاقها الرقمي. وقد مر هذا المفهوم بمراحل تطور مهمة؛ ففي البداية كان مرتبطًا بالحدود الجغرافية التقليدية (الأرض، الجو، المياه الإقليمية)، لكن مع الثورة التكنولوجية توسعت السيادة لتشمل المجال السيبراني، حيث لم تعد هناك حدود واضحة تفصل بين الدول. وقد أدى الاعتماد المتزايد على الرقمنة إلى تحول الأفراد إلى "مواطنين رقميين" يكن بها (netizen)، وظهور مصالح وطنية رقمية، والمصالح امتدت إلى رقع افتراضية في أمكنه أخرى، ما فرض تحولات على المفهوم الكلاسيكي للسيادة. وبرزت السيادة السيبرانية كأداة لحماية الفضاء الرقمي من التدخلات الخارجية والحماية من العمليات السيبرانية، وفرض الرقابة والتحكم في البيانات، كما هو واضح في سياسات دول مثل روسيا والصين والسعودية وتركيا (التحكم بتدفقات الانترنت). ومن أبرز أسباب بروز هذا المفهوم، التطور المتسارع في تقنيات الاتصال وزيادة الترابط الشبكي، ما أدى إلى تنامي التهديدات السيبرانية العابرة للحدود، إضافة إلى تصاعد عمليات التجسس والهجمات الرقمية، مما دفع الدول إلى تبني استراتيجيات وتشريعات جديدة لحماية مصالحها. كذلك ساهم استخدام الفضاء السيبراني في المجالات العسكرية والاقتصادية والثقافية في تعزيز الحاجة إلى فرض السيادة الرقمية.[33] وتمتاز السيادة السيبرانية الحديثة بطابع داخلي يتمثل في إدارة الدولة لشؤونها الرقمية، وطابع خارجي يتمثل في التصدي للهجمات السيبرانية والتدخلات الأجنبية، وتشمل حوكمة الإنترنت، الرقابة على المحتوى، التحكم في البيانات، وحتى إمكانية قطع الإنترنت في أوقات الأزمات، مما يجعل من الفضاء السيبراني ميدانًا جديدًا لإعادة تعريف مفاهيم القوة والسيادة والأمن القومي في ظل تعدد الفاعلين، من دول، وشركات تقنية، ومجموعات هاكرز.

5.المصالح الدولية الناشئة: تُعد مصالح الدول الناشئة في الفضاء السيبراني امتدادًا طبيعيًا لسعيها نحو تعزيز مكانتها الإقليمية والدولية، إذ بات هذا الفضاء يشكل ساحة استراتيجية متعددة الأبعاد، تجمع بين الأمن القومي، والتنمية الاقتصادية، والسيادة الرقمية. ففي ظل التحديات غير التقليدية التي تفرضها الهجمات الإلكترونية العابرة للحدود، تحرص هذه الدول على حماية بنيتها التحتية الحيوية وفرض سيادتها على الفضاء الرقمي لضمان التحكم في البيانات وحماية الخصوصية داخل اقليمها، وحماية أمنها القومي. وبموازاة ذلك، يتيح الفضاء السيبراني

---

[31] Assessing Cyber Power , Link :, https://ccdcoe.org/uploads/2018/10/Art-01-Assessing-Cyber-Power.pdf, accessed date 9-6-2025.

[32] Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia, Link:, https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/, accessed date 10-6-2025.

[33] Andrey Baykov, Elena Zinovieva, Digital International Relations, Springer Nature Singapore,2023, P.P.77-82.

فرصًا نوعية لتوسيع النفوذ وتعزيز التأثير الدولي من خلال بناء استراتيجيات سيبرانية تؤهلها لعب أدوار تفوق حجمها التقليدي في النظام العالمي. كما يُعد التحول الرقمي مدخلًا رئيسيًا لتحقيق التنمية الاقتصادية، عبر تنمية البنية التحتية التكنولوجية وجذب الاستثمارات وتوفير فرص عمل جديدة. وتدرك الدول أيضًا أهمية التعاون الإقليمي والدولي لمواجهة التهديدات السيبرانية المشتركة، من خلال تبادل الخبرات والمشاركة في حوكمة الإنترنت ووضع أطر تنظيمية مشتركة.[34] إلى جانب ذلك، تسعى هذه الدول إلى تنظيم الفضاء الرقمي داخليًا عبر فرض سيادة سيبرانية متكاملة تواكب صعود الفاعلين غير الحكوميين الذين يشكلون تهديدًا متناميًا للأمن والاستقرار.[35] وبذلك، تتداخل مصالح الدول الناشئة في الفضاء السيبراني ضمن مشروع استراتيجي متكامل، يُمكّنها من حماية أمنها، وتحقيق تنميتها، وتثبيت مكانتها في النظام الدولي الرقمي المتشكل.

6.تمدد وتعقيد العمليات السيبرانية: تزامنا مع التقدم التكنولوجي وتطور مفهوم الفضاء والقوة السيبرانيتين والعمليات السيبرانية تشهد تطورًا كبيرًا من حيث التعقيد والاحترافية تتناسب طرديًا مع مستويات التطور التكنولوجي، مما أثار قلقًا دوليًا متزايدًا بشأن الأمن السيبراني. خاصة بعدما أصبحت عابرة للحدود، والمهاجمون يستخدمون تقنيات متقدمة مثل الذكاء الاصطناعي، والهندسة الاجتماعية الدقيقة، وأشكال هجينة من الاحتيال تجمع بين الرقمي والمادي، ما جعل الهجمات أكثر تنوعًا وصعوبة في الاكتشاف والتصدي. وتُظهر التقارير أن الاستهداف لم يعد عشوائيًا،[36] بل يتركز على البنى التحتية الحيوية والقطاعات الاستراتيجية، مع تصاعد استخدام أدوات مثل التزييف العميق (Deep fake)، وهجمات سلاسل التوريد، وبرامج الفدية كخدمة، التي تساهم في توسيع نطاق التهديدات. كما أدى تصاعد التوترات الجيوسياسية إلى توظيف الهجمات السيبرانية كجزء من استراتيجيات الصراع بين الدول، مما زاد من تعقيد البيئة السيبرانية والمخاطر العابرة للحدود. في ظل هذا الواقع، بات لزامًا على الدول والمؤسسات تعزيز قدراتها الدفاعية، وتبنّي استراتيجيات أمنية مرنة، والاستثمار في حلول تقنية متقدمة، إلى جانب دعم التعاون الدولي، إدراكًا بأن الأمن السيبراني لم يعد خيارًا بل ضرورة ومكون رئيسي في القوة السيبرانية، بل ضرورة لحماية الأمن القومي وضمان الاستقرار العالمي.

- المطلب الثّاني: تأثير القوّة السيبرانيّة على العلاقات الدوليّة

لقد أثّرت القوة السيبرانية بعمق على عناصر العلاقات الدولية، ليس فقط من خلال إعادة تشكيل مفهوم الأمن القومي ليشمل البُعد الرقمي، بل أيضًا عبر خلق تحالفات وتفاعلات جديدة بين الدول، تُشبه التفاعلات التقليدية لكن في إطار رقمي بحت .فالهجمات السيبرانية على البنى التحتية الحيوية (كمستشفيات وشبكات الطاقة) باتت تمثّل تهديدًا مباشرًا للسيادة الوطنية، بينما أصبحت المنافسة بين القوى الكبرى كالولايات المتحدة والصين تُدار جزئيًا عبر الفضاء السيبراني، في ظل سعي كل طرف إلى فرض هيمنته التكنولوجية والمعلوماتية. كذلك، استخدمت دول مثل روسيا الفضاء السيبراني كأداة هجومية في سياستها الخارجية، في حين برزت دول أصغر ككوريا الشمالية وإيران كقوى سيبرانية مؤثرة. ومع غياب إطار قانوني دولي ملزم لحوكمة هذا الفضاء، يُتوقع أن يسهم في نشوء نظام دولي جديد أكثر تعقيدًا، تتداخل فيه مصالح الدول، الشركات، والجهات غير الحكومية. وهكذا، أصبحت القوة السيبرانية أداة ضغط ونفوذ، تُستخدم للتأثير في السياسات والاقتصادات دون اللجوء إلى القوة التقليدية، مما يطرح تساؤلات حول فعالية الردع السيبراني، ومستقبل توازن القوى في ظل تصاعد سباق التسلح الرقمي.

1.أثر القوّة السيبرانيّة على عناصر العلاقات الدوليّة:

بالإضافة الى ما جاء في المطلب السابق، لقد أثّرت القوة السيبرانية بشكل كبير على عناصر العلاقات الدولية، وأصبحت تُعدّ أحد الأبعاد الأساسية في القوة الشاملة للدول، وطالت عناصر العلاقات الدولية التي تعتبر المكونات الأساسية التي تُبنى عليها دراسة وفهم التفاعلات بين الدول والفاعلين الدوليين، وأبرزها الدولة(State) التي تعد العنصر الرئيسي في العلاقات الدولية، والفاعل الأساسي الذي يمتلك السيادة، وحدودًا معترف بها، وحكومة، وسكانًا وتحكما على الإقليم وما فيها وعليها. وكذلك مفهوم السيادة(Sovereignty) الذي ينص على حق الدولة في ممارسة سلطتها بشكل مستقل داخل حدودها، دون تدخل خارجي. ومن الملاحظ في التفاعلات الدولية الحديثة ووصول القوة السيبرانية الى ما وراء الحدود تمّ إهمال القوة(Power) التقليدية التي كانت تشمل القوة العسكرية، الاقتصادية، التكنولوجية، وهي الأداة التي تستخدمها الدول لتحقيق مصالحها، بل أصبح للدول اهتمامات لتحقيق بعض مصالحها دون الحاجة الى تدخل عسكري او الدخول في صراعات، وذلك بسبب ميزة القوة السيبرانية المتمثلة بالعمليات السيبرانية التي تعبر الحدود، بتكلفه أقل ومن دون يُلاحظ إسنادها. اما بالنسبة لعنصر المصلحة الوطنية(National Interest) وغالبًا ما تشمل الأمن، الاستقرار، والازدهار الاقتصادي أصبح هناك مصالح ناشئة رقمية أصبحت دافعا وراء تصرفات بعض الدول في الساحة الدولية لشن هجمات سيبرانية او التدخل رقميا في شؤون الدول لأهداف سياسية، فأصبحت المصالح الوطنية ومصلحة الامن القوى منع الهجمات السيبرانية، وحماية البيانات وسيادة الأصول، وأصبح الامن السيبراني من

---

[34] Enhancing Cyber Resilience in Developing Countries ,link:, https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries, accessed date 15-6-2025.

[35] Emerging cyber powers: The threat to business Link:, https://dragonflyintelligence.com/news/emerging-cyber-powers-the-threat-to-business/, accessed date 15-6-2025.

[36] الملخص التنفيذي لتقرير CrowdStrike للتهديدات العالمية 2025 ، https://www.crowdstrike.com/ar-sa/global-threat-report/،، تاريخ الزيارة 19-5-2025.

أبرز أولويات الدول. إن توافر القوة وسهولة الحصول عليها تم توزيع القوة على كيانات لادولاتية متعددة كالفواعل غير الحكومية(Non-State Actors)التي تشمل المنظمات الدولية (مثل الأمم المتحدة)، الشركات متعددة الجنسيات، الجماعات الإرهابية، ومنظمات المجتمع المدني وذلك ساهم في إعادة تشكيل التفاعلات الدولية(International Interactions) في التعاون، الصراع، التحالفات، الحروب، المعاهدات، والمنظمات الدولية ولا سيما التوجه نحو وصالح وستفاليا رقمي. ولا شكّ إنّ هذه التغيرات قادرة الى خلق نظام دولي (International System) جديد يعتبر الإطار العام الذي تنتظم فيه العلاقات بين الدول، وقد يكون أحادي القطب، ثنائي القطب، أو متعدد الأقطاب.

إن هذه التغيرات التي طرأت على العناصر الأساسية في العالقات الدولية كفيلة على إعادة دراسة مفهوم العلاقات الدولية في إطار رقمي يبلور علاقات دولية معاصرة. وقد تعجز نظريات العلاقات الدولية على فهم هذه الظواهر السياسية الجديد لما تتسم فيه من سرعه وغموض وتطور رقمي سريع مرتبط في الحروب الذكية والهجينة والعناصر الأخرى.

2.مجالات التأثير السيبراني على العلاقات الدوليّة: أشرنا في تعريف القوة السيبرانية بأنها تشير إلى قدرة الدولة (أو أي فاعل آخر) على استخدام الفضاء السيبراني لتحقيق أهداف سياسية أو أمنية أو اقتصادية ، وذلك من خلال استخدام إحدى وسائل القوة السيبرانية كالعمليات السيبرانية (الهجومية والدفاعية) كالهجمات السيبرانية (Cyber Attack) ضد اصول الخصم، أو الدفاع السيبراني (Cyber Defense) كالتجسس السيبراني(Cyber Espionage) لجمع المعلومات، او التأثير عبر المعلومات (مثل التضليل والدعاية)، أو من خلال أي مكون للقوة الذي بدوره يؤدي الى الصراع او التفاعل في عدة مجالات، وأبرز هذه المجالات:

أ-التعاون وتشكيل الأحلاف: مثلما تساهم القوة السيبرانية في تآكل الثقة بين الدول بسبب غياب الاسناد، وغياب قياسها والشعور بها، فهي من جهة أخرى رغم التحديات، توفر القوة السيبرانية فرصًا للتعاون الدولي لمواجهة التهديدات السيبرانية كمكافحة الجرائم الإلكترونية وتأمين الفضاء السيبراني العالمي وتبادل الخبرات والتكنولوجيا الآمنة، وحماية البنى التحتية الحساسة وتبادل المعلومات الاستخباراتية حول التهديدات. وبرز عن هذا التعاون اتفاقية بودابست لمكافحة الجرائم السيبرانية،[37] واستراتيجيات الناتو في تعزيز سياسات ودفاعات الامن السيبراني ووضعها في صلب استراتيجياته الدفاعية، ودول البريكس ، والعيون الخمسة، الى جانب اتفاق أوروبي-بريطاني، تم توقيع اتفاق جديد بين الاتحاد الأوروبي والمملكة المتحدة لتعزيز الأمن والدفاع في مواجهة التهديدات السيبرانية والهجينة، مع التركيز على توسيع التعاون في الصناعات الدفاعية وتبادل الخبرات، ومبادرات الأمم المتحدة التي أقرت نص اتفاقية دولية جديدة لمكافحة الجرائم السيبرانية، تهدف إلى تسهيل التعاون القضائي وتبادل الأدلة الإلكترونية، وتقديم الدعم الفني للدول، خاصة النامية منها، لمواجهة التهديدات السيبرانية العابرة للحدود.[38]

ب-التدّخل رقميًّا: تشهد الساحة الدولية تصاعداً ملحوظاً في استخدام العمليات السيبرانية كأداة للتدخل في الشؤون الداخلية للدول، بهدف زعزعة الاستقرار السياسي والتأثير على أنظمة الحكم، وتوجه الرأي العام خلال الحملات الانتخابية، وذلك كان إحدى النماذج التي تمّ استخدامها في إستونيا، وروسيا ، وايران والويلات المتحدة وأدى الى ذلك إلى زيادة في التوترات الدبلوماسية وتصاعد في حدة التصريحات الدبلوماسية على لسان وزراء الخارجية ولا سيما وزير خارجية الولايات المتحدة بومبيو حيال الهجمات التي أطاحت بأنظمة الوكالات الامريكية التي تعرضت لهها أنظمة سولاروندز ووصفها آنذاك موبيو بأنها :" اجتياح رقمي لا مثيل له في تاريخ أمريكا"، مما دفع الرئيس الأمريكي السابق جو بايدن بإرسال قائمة من الأهداف يمنع كل من روسيا وايران والصين التعرض لها وإلا سيكون مواجه عسكرية في حال التعرض لها.[39] وما زالت الى الان الاتهامات المتبادلة بشأن التدخلات السيبرانية في الانتخابات أو سرقة الملكية الفكرية تؤدي إلى توتر دبلوماسي، كما حدث بين الولايات المتحدة وروسيا أو الصين. لذلك أصبح الفضاء السيبراني ساحة جديدة للصراعات الدولية، وأصبح مجالا تنشط القوة الناعمة والقوة الصلبة السيبرانيتين:

- **القوة الصلبة السيبرانية**: تتمثل القوة الصلبة في الهجمات على البنية التحتية الحيوية بهدف تعطيل أنظمة الطاقة، أو الاتصالات، أو المؤسسات الحكومية، ما يؤدي إلى إرباك عمل الدولة وإضعاف الثقة في النظام الحاكم. والتجسس السيبراني بهدف سرقة معلومات حساسة أو ابتزاز المسؤولين، ما قد يؤدي إلى زعزعة الاستقرار السياسي أو التأثير على قرارات الدولة.

-القوة السيبرانية الناعمة: تتمثل في التدخل في العمليات الانتخابية عبر اختراق الأنظمة الانتخابية أو نشر معلومات مضللة لتوجيه الرأي العام أو التشكيك في نزاهة الانتخابات. وحملات التضليل الإعلامي استخدام وسائل التواصل الاجتماعي لنشر الشائعات والأخبار الكاذبة بهدف

---

[37] للاطلاع على مضمون الاتفاقية ، متوافر على موقع مجلس أوروبا ، الرابط:،https://rm.coe.int/budapest-convention-in-arabic/1680739173 ، تاريخ الزيارة 19-5-2025.

[38] الأمم المتحدة تقر نص اتفاقية جديدة حول مكافحة الجرائم السيبرانية، متوافر على موقع جسور بوست، الرابط:،https://cutt.ly/CrWKv6xi ، تاريخ الزيارة 19-5-2025.

[39] ترامب يناقض وزير خارجيته بشأن اتهام روسيا بشن هجمات إلكترونية على بلاده، متوافر على موقع BBC ، 20/12/2020 ، الرابط:، https://www.alanba.com.kw/BBCNews/7766، تاريخ الزيارة 19-5-2025.

تقويض ثقة المواطنين بالحكومة أو إثارة الفتن والانقسامات الداخلية. التدخل في الشؤون الداخلية: يمكن استخدام الفضاء السيبراني للتأثير في الخطاب السياسي الأجنبي، وتوجيه الرأي العام، والتلاعب بالانتخابات عبر الحملات الرقمية والتضليل الإعلامي.

وأبرز الأمثلة الحية حيال ذلك، تتبادل روسيا ودول الغرب بعضهما التهم بتنفيذ هجمات سيبرانية تستهدف زعزعة استقرار الأنظمة السياسية، مثل التدخل في الانتخابات أو التأثير على الرأي العام عبر حملات التضليل الرقمي بهدف تفضيل مرشحين مثل التدخل الروسي المزعوم في الانتخابات الأمريكية 2016 تفضيل ترامب على هيلاري كلينتون. في حالات أخرى، تلجأ بعض الدول إلى فرض سيطرة رقمية مشددة (مثل قطع الإنترنت أو الرقابة على المحتوى) في أوقات الأزمات السياسية لحماية النظام من التدخلات الخارجية كما حصل في خلال الربيع العربي أو التظاهرات الإيرانية ضد النظام الحاكم.

3.تحولات الصراع العالمي وتوازن القوى في العصر الحديث

بالنظر إلى التحولات التي يشهدها العالم الرقمي، لقد تمّ رقمنت الصراعات بمفهومها التقليدي الى الفضاء السيبراني فالصين فرضت شيوعيتها وبنت جدار الصين الرقمي لحماية على أمنها الرقمي وسيادة بياناتها، ووطنت كل من الصين وروسيا أنظمته تشغيل بعيدة عن أنظمة ويندوز، وإن مفهوم توازن القوى السيبراني أدخل عليه فواعل جديدة وقوة متعددة الابعاد يصعب اسنادها او الشعور بها مما يعقّد مشهد التفاعل الدولي. وكل ذلك قد أعاد تشكيل العلاقات الدولية وفرض معايير جديدة للقوة والنفوذ. لم تعد القوة مقتصرة على حجم الجيوش أو الناتج القومي، بل أصبحت مرتبطة بشكل وثيق بالقدرة على التأثير في الفضاء السيبراني من خلال أدوات مثل الهجمات الإلكترونية، الذكاء الاصطناعي، وتكنولوجيا المعلومات.

أ-تغيير طبيعة الصراع الدولي: في العصر الرقمي أصبح الصراع لا يقتصر فقط على المجال العسكري التقليدي، بل انتقل إلى الفضاء السيبراني، حيث تقوم الدول القومية وكيانات لادولاتية بشن هجمات سيبرانية لتعطيل بنى تحتية حيوية مثل شبكات الكهرباء أو المؤسسات المالية، مثل الهجوم السيبراني على إيران(Stuxnet) ، والهجمات الروسية على أوكرانيا، والهجمات على البنوك وأنظمة سويفت. فالصراع أصبح فيه فواعل من غير الدول ودول صغرى لم تكن فاعلة في النظام الدولي أصبحت الان لها تأثير على السياسات الدولية. لذلك أصبحت تُعد العمليات السيبرانية الشكل الأكثر تقدمًا من الصراعات بعد الحرب العالمية الثانية، حيث توفر ميزة استراتيجية للدول الأضعف مثل كوريا الشمالية أو إيران لمواجهة قوى عظمى مثل الولايات المتحدة، من خلال هجمات منخفضة التكلفة وخفية ويصعب تتبع مصدرها. تعتمد الولايات المتحدة بشدة على البنية التحتية الرقمية، ما يجعلها عرضة للهجمات السيبرانية رغم قوتها الدفاعية. وفي نفس السياق، تُعد العمليات السيبرانية فعّالة ومجدية للدول الأضعف بسبب تكلفتها المنخفضة، وسهولة إخفاء مصدر الهجوم، وصعوبة نسب الهجمات لجهة محددة. في ظل النظام الدولي الفوضوي الحالي، حيث تهيمن الولايات المتحدة عسكريًا، تستفيد دول مثل كوريا الشمالية وإيران من القدرات السيبرانية لمعادلة ميزان القوى،[40] ولا سيما الصين وروسيا وكوريا الشمالية تعتبر الفضاء السيبراني منطقة رمادية (gray zone) كوسيلة لتحقيق الأهداف،[41] و من صفات المنطقة الرمادية النشاط عندما يكون العالم منشغل بالأحداث العالمية، فتسعى بعض الدول إلى تحقيق مصالحها وأهدافها من دون أي صدام مع الخصم. وأبرز الأمثلة:

- إستونيا (2007): أدى هجوم حجب الخدمة الموزع (DDoS) الضخم، المنسوب إلى روسيا، إلى شلل البنية التحتية الرقمية لإستونيا، مما يُظهر كيف يُمكن للهجمات الإلكترونية أن تُعطل دولًا بأكملها بموارد مادية محدودة.
- أرامكو السعودية (2012): أدى هجوم إلكتروني إلى تعطيل 30 ألف جهاز كمبيوتر، مما يُسلط الضوء على ضعف الأصول الاقتصادية الحيوية.
- أوكرانيا (2023): أدت الهجمات الإلكترونية خلال الصراع مع روسيا إلى تعطيل أنظمة الدفع والرعاية الطبية والخدمات الأساسية، مما يُوضح الأثر المجتمعي المباشر للحرب الإلكترونية.[42]

ب-توازن القوى في الحالة السيبرانية: لقد غيّر الفضاء السيبراني طبيعة القوة نفسها، حيث باتت القدرة على شن عمليات سيبرانية أو ردعها، والتحكم في تدفق المعلومات، وتطوير أنظمة الذكاء الاصطناعي، عوامل أساسية في تحديد مكانة الدول والكيانات الفاعلة، فالقوة لم تعد فقط فيمن يمتلك السلاح، بل فيمن يستطيع اختراق أنظمة العدو أو حماية بنيته التحتية من الهجمات غير المرئية. لذلك هناك أصبح مظاهر جديدة أثرت في التحول على توازن القوى السيبراني، ومن أبرز معالمه تعدد الفاعلين لم تعد الدول وحدها تحتكر التأثير السيبراني، بل دخلت شركات

[40] Cyber warfare is becoming the most progressive warfare domain after the Second World War. Which global actors benefit the most from this capability, Link:, https://securityaffairs.com/33448/cyber-warfare-2/cyber-warfare-balance-of-power.html, accessed date 20-6-2025.

[41] محمد زيتون ، مصدر سبق ذكره

[42] Hybrid Warfare: How Cyber Warfare is Transforming International Relations, Link:, https://www.sia-partners.com/en/insights/publications/hybrid-warfare-how-cyber-warfare-transforming-international-relations, accessed date 20-6-2025.

التكنولوجيا الكبرى، ومجموعات القرصنة المنظمة، وحتى الأفراد ذوو المهارات العالية، كأطراف مؤثرة في ميزان القوى[43]. وكما إنّ غموض فهم معايير القوة السيبرانية يصعّب قياسها أو تقييمها بسبب الطبيعة السرية للهجمات الإلكترونية والتقنيات المستخدمة فيها. هذا يزيد من صعوبة وضع تصنيفات دقيقة للقوى الفاعلة وبالتالي توازن القوى الجديد. فاذا تبرز التكنولوجيا المتقدمة كميدان جديد للتنافس، لا سيما بين القوى العظمى مثل الولايات المتحدة والصين، إذ أصبحت الأسبقية في الذكاء الاصطناعي، والحوسبة الكمية، والأمن السيبراني بمثابة أدوات استراتيجية جديدة لفرض النفوذ. لذلك أصبح لدينا أدوات إعادة تشكيل التوازن السيبراني أولها المرونة السيبرانية، وهي قدرة الدول والمؤسسات على الصمود والتعافي بسرعة بعد التعرض لهجوم. كما أصبح التعاون الدولي ضرورياً لمجابهة التهديدات العابرة للحدود، عبر تبادل المعلومات والتنسيق الأمني والتدريب المشترك وهذا ما ينذر بتبدل في نظام توازن القوى الجديد.[44]

ج-سباق التسلح السيبراني سباق التسلح السيبراني يعكس حالة من المنافسة المتسارعة بين القوى الكبرى لتطوير أدوات هجومية ودفاعية متقدمة في الفضاء الرقمي، لم يعد هدفها مجرد الحماية من الاختراقات، بل امتد ليشمل إنتاج "أسلحة سيبرانية" قادرة على التجسس، التعطيل، واختراق البنى التحتية الحيوية. هذا السباق تغذّيه عوامل عدة، أبرزها تصاعد الهجمات السيبرانية التي باتت تهدد مؤسسات حيوية في مختلف الدول، إلى جانب التوترات الجيوسياسية بين قوى كبرى كالصين، والولايات المتحدة، وروسيا، ما دفع إلى استثمارات هائلة في هذا المجال. دخول الذكاء الاصطناعي زاد من تعقيد هذه المعادلة، حيث بات يُستخدم لتصميم برمجيات هجومية تتعلم وتتطور ذاتياً، مما جعل الهجمات أسرع وأكثر دقة. من مظاهر هذا السباق أيضاً استخدام أدوات مثل هجمات الفدية وثغرات "اليوم صفر"، وتوجيه ضربات مباشرة لقطاعات الطاقة والنقل والصحة، وليس فقط لسرقة البيانات. ولم يعد السباق محصوراً بين الدول، إذ دخلت على الخط شركات كبرى، مجموعات إجرامية، وأفراد يملكون أدوات متطورة. عالمياً، تظهر أمثلة واضحة الصين تُظهر تقدماً في دمج قدراتها السيبرانية ضمن استراتيجية موحدة، مقابل تشتت المنظومة الأمريكية؛ الحرب الروسية الأوكرانية كشفت كيف يمكن للهجمات الرقمية أن تسير جنباً إلى جنب مع المعارك التقليدية؛ وفي شبه الجزيرة الكورية، يتصاعد التوتر بين نهج كوريا الشمالية الهجومي ونمط كوريا الجنوبية الدفاعي. ظهرت ملامح **سباق تسلح رقمي**، حيث تستثمر الدول في تطوير قدرات هجومية ودفاعية سيبرانية، كما تنشئ وحدات سيبرانية داخل جيوشها.[45]

ه-تعقيد الردع السيبراني والتنظيم الدولي: أصبح الردع السيبراني أحد أكثر المفاهيم تعقيداً في العلاقات الدولية الحديثة، نتيجة لطبيعة الفضاء السيبراني التي تفتقر إلى الحدود الجغرافية الواضحة، وتسمح بإخفاء الهوية، ما يصعّب إسناد (attribution) الهجمات إلى جهة محددة ويقلل من فاعلية القوانين والآليات الدولية التقليدية. في هذا السياق، تحاول الدول تطوير نماذج ردع سيبراني شبيهة بالردع النووي، تقوم على امتلاك قدرات هجومية متقدمة أو إظهار الجاهزية للرد بقوة، لردع الخصوم ومنعهم من تنفيذ هجمات محتملة. وتتنوع أدوات هذا الردع بين شن هجمات مضادة، وفرض عقوبات اقتصادية، أو حتى اللجوء للرد العسكري في حالات قصوى، بالإضافة إلى تعزيز الدفاعات الرقمية لرفع كلفة الهجوم على المهاجم. ومع ذلك، فإن الردع السيبراني يواجه تحديات جدية، أبرزها تعدد الفاعلين غير الدوليين، والغموض القانوني، والقيود الأخلاقية، فضلاً عن انخفاض تكلفة الهجوم وغياب الرادع الفعّال. وعلى عكس الردع النووي، يثبت الردع السيبراني محدودية تأثيره، حيث تستغل بعض الدول الأضعف الفضاء السيبراني لإرباك قوى أكبر وتحقيق مكاسب استراتيجية دون الدخول في مواجهة عسكرية مباشرة، ما يزيد من الحاجة إلى صياغة عقيدة دولية جديدة للردع السيبراني، تقوم على التعاون، وتبادل المعلومات، ووضع قواعد اشتباك واضحة تتماشى مع الواقع الرقمي المتغير.

5.من التهديدات الرقمية إلى إعادة تشكيل النظام الدولي: شهد النظام الدولي في العقود الأخيرة تحولات جوهرية بفعل صعود القوة السيبرانية، التي باتت تُعدُّ أحد المكونات الأساسية في الصراع العالمي المعاصر. فقد تحول الفضاء السيبراني إلى "الساحة الخامسة" للمواجهة، وأصبح مجالاً لتنافس القوى العظمى والجهات الفاعلة غير التقليدية مثل الشركات الكبرى، مجموعات الهاكرز، والمنظمات العابرة للحدود.

لقد أسفرت العمليات السيبرانية عن بروز تهديدات جديدة للبنى التحتية الحيوية للدول، حيث يمكن لمجرد اختراق رقمي أن يعطّل شبكات الكهرباء أو يشلّ مؤسسات الصحة والنقل، دون إطلاق رصاصة واحدة. ونتيجة لذلك، أصبح الأمن السيبراني جزءًا لا يتجزأ من الأمن القومي والسياسة الخارجية للدول، ما فرض إعادة نظر جذرية في مفهومي السيادة والردع. لم تعد السيادة محددة جغرافيًا، وأصبح التفوق السيبراني عاملاً حاسمًا في توازن القوى الدولية. كما أثرت القوة السيبرانية في التفاعلات الدولية من خلال نشوء الدبلوماسية السيبرانية، التي تسعى لتنسيق الجهود بين الحكومات، القطاع الخاص، والمنظمات الدولية، وتطوير معايير عالمية لضبط الأمن السيبراني. وفي الوقت ذاته، دفعت التهديدات الرقمية المتزايدة نحو تشكيل تحالفات جديدة، وتغيير طبيعة العلاقات التقليدية، إذ بات التعاون في هذا المجال ضروريًا لمواجهة المخاطر العابرة للحدود.

---

(43) محمد زيتون، مصدر سبق ذكره.

(44) الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي، متوافر على موقع ترندز للبحوث والاستشارات، الرابط: https://cutt.ly/zrUpAU4O ، تاريخ الزيارة 25-6-2025.

(45) سباق التسلّح السيبراني.. كيف تتفوق الصين على الولايات المتحدة؟، الرابط: https://www.erembusiness.com/technology/b17lqyx ، تاريخ الزيارة 1-7-2025.

من جهة أخرى، أتاح الفضاء السيبراني أدوات تأثير واسعة النطاق للجهات غير الحكومية، مما أربك موازين القوى التقليدية، وأعاد توزيع الأدوار في النظام الدولي. وباتت الدول مطالبة بصياغة استراتيجيات مرنة تجمع بين الردع، التعاون، وبناء القدرات الدفاعية والهجومية، لضمان حضورها وتأثيرها في هذا الفضاء المتغيّر باستمرار. في المحصلة، القوة السيبرانية لم تعد مجرد بعد تقني أو أمني، بل أصبحت عاملاً مركزيًا في تشكيل النظام العالمي، بما يحمله من فرص، تهديدات، وتغيرات في أنماط التحالفات والتفاعلات الدولية.

الخاتمة

في ضوء ما تقدّم، يمكن القول إن مفهوم "عتبة القوة السيبرانية" لا يزال يثير الكثير من الجدل في الأوساط البحثية. فبينما يُبالغ البعض في تقدير قدرتها على تغيير موازين القوى، إلا أن الأحداث الأخيرة – مثل دورها في النزاع بين إسرائيل ولبنان وما شهدته المواجهة السيبرانية المتصاعدة بين إيران وإسرائيل – تؤكد أنها لم تعد مجرد أدوات رمزية، بل باتت قادرة على التسبب بإراقة دماء، وإحداث تطورات نوعية في ساحة الصراع. ومع ذلك، لم تصل هذه العتبة بعد إلى الحد الذي يؤدي إلى اندلاع حروب تقليدية مباشرة بين الجيوش، مما يعكس طبيعتها المتغيرة والغامضة، ويضع السياسات الدولية أمام تحديات تتعلق بالوضوح واليقين في السلوك السيبراني، خصوصًا في ظل تنامي ما يُعرف بـ"المنطقة الرمادية."

رغم هذا، لا يمكن إنكار أن القوة السيبرانية أصبحت ركيزة أساسية في بنية العلاقات الدولية، تؤثر في مسارات الصراع، وتعيد تشكيل التحالفات، وتفرض نفسها كعنصر فاعل في أدوات النفوذ والردع الحديثة. فهي تمنح الدول القدرة على تحقيق أهداف استراتيجية دون اللجوء إلى القوة العسكرية التقليدية، لكن غموض حدود استخدامها يضفي على المشهد الدولي مزيدًا من الضبابية والتوتر.

استنتاجات وتوصيات:

- تؤكد الأمثلة والوقائع المعروضة أن عتبة القوة السيبرانية تُحدث فارقًا حقيقيًا في العلاقات الدولية، عبر أدوات جديدة للتأثير دون عنف مباشر.
- غير أن غموض هذه العتبة يجعل السياسات السيبرانية غير مستقرة وتدخل في نطاق المنطقة الرمادية.
- ضرورة تطوير نموذج عربي خاص لقياس القدرات السيبرانية، بما يعكس السياقات المحلية والإقليمية.
- التأكيد على أهمية تعزيز البُعد الأكاديمي في دراسة السياسة السيبرانية (Cyber Politics) بوصفها مساقًا ضروريًا لفهم تحولات النظام الدولي.
- الحاجة إلى نشر الثقافة السيبرانية وتوسيع الوعي المجتمعي من خلال محتوى معرفي عربي متخصص.
- توجيه الأجندات البحثية نحو دراسة القضايا الجوهرية التي يثيرها الفضاء السيبراني، خاصة ما يتعلق بالسيادة، الأمن، وبنية النظام العالمي المستقبلي .

لائحة المصادر:

أ. كتب عربية

خليفة، إ .(2021) .*الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة* .مذكرة إلكترونية، رئاسة مجلس الوزراء، مصر.

نقولا، ل .(2021) .*العلاقات الدولية: من تأثير القوة إلى قوة التأثير* (ص. 211). الأرز للنشر، لبنان.

ب. كتب إنجليزية

Baykov, A., & Zinovieva, E. (2023). *Digital international relations* (pp. 77–82). Springer Nature Singapore.

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security policy* (p. 528). Center for Technology and National Security Policy.

Tashi, I., & Ghernaouti, S. (2011). *Information security evaluation: A holistic approach* (pp. 135, 145). EPFL Press English Imprint.

Nye, J. S., Jr. (2005). *Soft power: The means to success in world politics* (ch. 2). Public Affairs.

Sharma, M. (2024). *Building China into a cyber superpower: Desires, drivers, and devices* (p. 4). Taylor & Francis, New Delhi.

Ghernaouti-Helie, S. (2016). *Cyber power: Crime, conflict and security in cyberspace* (pp. 174–179). CRC Press, USA.

ج. مواقع إلكترونية عربية

المركز العربي للأبحاث ودراسة السياسات. (د.ت). الفضاء السيبراني وتحولات القوة في العلاقات الدولية . https://www.dohainstitute.org/ar/BooksAndJournals/Pages/cyberspace-and-power-shifts-in-international-relations.aspx

BBC.(2020، ديسمبر 20). ترامب يناقض وزير خارجيته بشأن اتهام روسيا بشن هجمات إلكترونية على بلاده . https://www.alanba.com.kw/BBCNews/7766

Erem Business.(د.ت). سباق التسلّح السيبراني.. كيف تتفوق الصين على الولايات المتحدة؟ https://www.erembusiness.com/technology/b17lqyx

عالم رقمي. (2025، أبريل 13). استحواذ جوجل على "ويز" الاسرائيلية.. هل مجرد صفقة اقتصادية بحتة أم تحمل دلالات سياسية وعسكرية أيضا؟ https://cutt.ly/3rEPJP47

معهد الجزيرة للإعلام. (د.ت). الاستعمار الرقمي.. الجنوب العالمي أمام شاشات مغلقة . https://institute.aljazeera.net/ar/ajr/article/2962

جسور بوست. (د.ت). الأمم المتحدة تقر نص اتفاقية جديدة حول مكافحة الجرائم السيبرانية) https://cutt.ly/CrWKv6xi .تاريخ الزيارة:(2025، مايو 19)

ترندز للبحوث والاستشارات. (د.ت). الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي . https://cutt.ly/zrUpAU4O

نيوز روم. (2025، يونيو 12). البيانات أقوى من الرصاص: تأثير الهجمات السيبرانية على الأمن القومي . https://newsroom.info/88166

العربية. (د.ت). التفوق الرقمي الأميركي يربك أوروبا.. هل آن أوان الانفصال؟ https://cutt.ly/wrEPJIe

CrowdStrike. (2025).الملخص التنفيذي لتقرير CrowdStrike للتهديدات العالمية 2025 . https://www.crowdstrike.com/ar-sa/global-threat-report/ (تاريخ الزيارة: 2025، مايو 19)

المركز الوطني للأمن السيبراني. (د.ت). ما هو الأمن السيبراني؟ https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html

سيبرا. (2024، سبتمبر 9). من التجسس إلى الحرب الشاملة: رحلة تطور الحروب السيبرانية عبر العصور . https://cutt.ly/crWKkBz7 (تاريخ الزيارة: 2025، مايو 19)

سويس إنفو. (2024، نوفمبر 11). نتنياهو وافق على هجمات بأجهزة بيجر متفجرة على حزب الله https://cutt.ly/orEAegFm .

د. مواقع إلكترونية أجنبية

World Bank. (2025, January 29). *Enhancing cyber resilience in developing countries*. https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries

CCDCOE. (2018). *Assessing cyber power*. https://ccdcoe.org/uploads/2018/10/Art-01-Assessing-Cyber-Power.pdf

Security Affairs. (د.ت). *Cyber warfare is becoming the most progressive warfare domain after the Second World War. Which global actors benefit the most from this capability*. https://securityaffairs.com/33448/cyber-warfare-2/cyber-warfare-balance-of-power.html

Council of the EU. (2025, January 27). *Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia*. https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/

Dragonfly Intelligence. (د.ت). *Emerging cyber powers: The threat to business*. https://dragonflyintelligence.com/news/emerging-cyber-powers-the-threat-to-business/

The Verge. (2016, February 8). *Facebook's Free Basics service has been banned in India*. https://www.theverge.com/2016/2/8/10913398/free-basics-india-regulator-ruling

SIA Partners. (د.ت). *Hybrid warfare: How cyber warfare is transforming international relations*. https://www.sia-partners.com/en/insights/publications/hybrid-warfare-how-cyber-warfare-transforming-international-relations

Microsoft. (2024, November 29). *Microsoft Digital Defense Report: 600 million cyberattacks per day around the globe*. https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/

هـ. دراسات سابقة

زيتون، م. (د.ت). العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني. المجلة العربية للدراسات السياسية . https://cutt.ly/4rmc7WmZ

زيتون، م. (2024). *نحو استراتيجية دولية للأمن السيبرانية لمواجهة تداعيات العمليات السيبرانية* (رسالة دكتوراه غير منشورة). جامعة بيروت العربية.

زيتون، م. (2025). القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية. المجلة العربية للنشر العلمي . https://cutt.ly/Urmut6M8

زيتون، م. (2025، فبراير 5). القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية. المجلة العربية للنشر العلمي . https://cutt.ly/VrT79fVz