

ورقـــة أمنيـــة

المغالبـــة والتنافـــس فـــي القـــدرات السيبرانيـــــة الأمريكيـــــة الصينيـــــة

إعـــداد

مركز المتوسط للدراسات الإستراتيجية

www.mediterraneancss.uk

مركز المتوسط للدراسات الإستراتيجية

مؤسسة بحث وتفكير إستراتيجي، تأسست في بريطانيا،يناير 2020، تقوم على إعداد البحوث والدراسات والتقديرات وأوراق السياسات، وإدارة المشروعات البحثية، وتنظيم الفعاليات العلمية، وتقديم الإستشارات حول التفاعلات السياسية والإستراتيجية في منطقة المتوسط ومايرتبط بها من تفاعلات إقليمية ودولية.

جميع الحقوق محفوظة لمركز المتوسط للدراسات الإستراتيجية - 2024

د. خالد وليد محمود

دكتوراه العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة بيروت العربية، رئيس أول قسم الإعلام والاتصال، معهد الدوحة للدراسات العليا، قطر.

الملخص:

تتناول هذه الدراسة التغيرات الحاصلة في مجال القدرات السيبرانية وتأثيرها على العلاقات الدولية، وذلك بالتركيز على أهمية التطورات التكنولوجية ودورها في تغيير ديناميكيات الصراعات الدولية ووسائل التنافس، وباعتبار أن الولايات المتحدة الأمريكية والصين تعتبران أبرز القوى الرائدة عالمياً في مجال القدرات السيبرانية، فإن الدراسة تسلط الضوء على هاتين الدولتين، حيث تحتل الولايات المتحدة مكانة ريادية في مجال الفضاء السيبراني نظراً لقوتها السياسية والاقتصادية والعسكرية والتكنولوجية، بينما تتطور الصين بسرعة كقوة اقتصادية ناشئة، وتستثمر بشكل كبير في تعزيز قدراتها السيبرانية.

تهدف هذه الدراسة إلى استعراض وتحليل القدرات السيبرانية للولايات المتحدة الأمريكية والصين، وتقديم نظرة شاملة عن استراتيجياتهما وأهدافهما في مجال القدرات السيبرانية، ودراسة تطور تلك القدرات وكيفية استخدامها لتعزيز مكانة البلدين في المنافسة الدولية، بالإضافة إلى دورها في التصدي للتحديات السيبرانية المتزايدة.

وتشير نتائج هذه الدراسة إلى أن أن التنافس بين القدرات السيبرانية الأمريكية والصينية سيستمر في تحديد المشهد الدولي الذي تعززه التطورات والتحولات الهائلة في الديناميات الجيوسياسية والتكنولوجية السيبرانية المتقدمة التي ستمثل عاملاً محورياً يحدد القواعد الجديدة للقوة والتأثير العالمي مستقبلاً.

الكلمات المفتاحية: التنافس الدولي، القدرات السيبرانية، الولايات المتحدة، الصين، العلاقات الدولية.

مقدمة:

في إطار التمييز بين القوة السيبرانية (Cyber Power)، والقدرات السيبرانية (Cyber Capabilities)، فإن القوة السيبرانية تمثل مفهوماً شاملاً يرتبط بالقدرة الشاملة لكيان ما، كالدولة أو المؤسسة، على تحقيق أهدافها وحماية مصالحها في الفضاء السيبراني. وتستند إلى الاستخدام الفعّال للعناصر السيبرانية المتاحة، مثل التكنولوجيا والمعرفة والقوانين والقدرات البشرية. تجمع القوة السيبرانية بين القدرة على الدفاع عن الأصول الرقمية والبيانات الحساسة، والقدرة على تنفيذ هجمات سيبرانية عند الضرورة، وتعكس قوة السيبرانية التأثير والتحكم في الفضاء السيبراني بصورة شاملة.

أما القدرات السيبرانية فتتعلق بالعناصر الفعلية التي تمتلكها الدول أو الكيانات لتنفيذ الأنشطة والعمليات في الفضاء السيبراني؛ تشمل هذه القدرات الأنظمة والتقنيات والأدوات والمعرفة والمهارات التي تستخدم لتحقيق أهداف معينة. على سبيل المثال تتضمن القدرات السيبرانية الأدوات والبرمجيات والمعرفة التي تمكن من القيام بأنشطة سيبرانية مثل: الاختراقات والتجسس والتدمير السيبراني، وتحسين الأمن السيبراني والدفاع عن البنية التحتية السيبرانية للدولة أو المؤسسة.

انطلاقاً مما سبق يمكن القول إن القوة السيبرانية تمثل التقييم الشامل للقدرة على التأثير والتحكم في الفضاء السيبراني، بينما القدرات السيبرانية تشير إلى العناصر والأدوات الفعلية التي تمكن الكيان من ممارسة هذا التأثير والتحكم. بشكل عام، يمكن تصور القدرات السيبرانية كوسائل وأدوات تستخدم لتحقيق القوة السيبرانية. الدول والكيانات السياسية يسعون لزيادة قدراتهم السيبرانية لضمان أمنهم السيبراني وتعزيز تأثيرهم في العالم الرقمي([1]).

تسعى الكثير من الدول لتعزيز قوتها السيبرانية والاستثمار في القدرات السيبرانية، حيث أصبحت هذه الأخيرة تأخذ شكلاً جديداً في طبيعتها ووسائلها وأدواتها ومعطياتها ومؤشراتها([2])، وفي الوقت الحاضر، نشهد كيف أن الصراع الدولي يتّجه بالأساس نحو المنافسة وتعزيز النفوذ في مجال التكنولوجيا والابتكار، الذي غير من شكل الصراعات والحروب وأدواتها، وأثر في الفواعل فيها، وساهم في إعادة التفكير في حركية وديناميكية العلاقات الدولية.

وقد أسفرت حوادث الهجمات السيبرانية عن تسارع ملحوظ في التسلح السيبراني وتوجهات الاستثمار نحو تعزيز الأمن السيبراني وتطبيقات الذكاء الاصطناعي. وقد أعلنت بعض الدول أن مجال "السايبر" هو المجال العسكري الخامس بعد القوات البرية والبحرية والجوية والفضائية. وفي هذا السياق، قامت العديد من الدول بإنشاء ميزانيات ضخمة لتعزيز القدرات السيبرانية العسكرية سواء الهجومية أو الدفاعية.

وقد أصبحت القدرات السيبرانية مجالاً مهماً لممارسة النفوذ وتحقيق التفوق والتنافس الدولي، خاصة بعد تطور قدرات بعض الدول في هذا المجال. فخلال الثلاث عقود الأخيرة، شهد العالم سلسلة من الهجمات السيبرانية ذات الطابع التخريبي، تمثلت في تشويه المواقع الإلكترونية، وشن هجمات سيبرانية متقدمة،

[1] Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyberpower and National Security, Center for Technology and National Security Policy ; Potomac Books, Washington, D C, National Defense University Press, 2009, P. 24.

[2] Max Smeets, Herbert S. Lin, Offensive Cyber Capabilities: To What Ends?, 2018 10th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, 2018, P.58.

واستهداف بعض أنظمة المعلومات وقواعد البيانات، والتلاعب بالبيانات المُخزَّنة على أجهزة الكمبيوتر التابعة لمختلف المؤسسات الحكومية والكيانات الخاصة([1]).

وباعتبار أن الولايات المتحدة الأمريكية والصين تمثلان إحدى أهم الدول الرائدة عالمياً في مجال القدرات السيبرانية، فالولايات المتحدة تحتل مكانة ريادية بسبب قوتها السياسية والاقتصادية والعسكرية والتكنولوجية؛ حيث تمتلك إمكانيات وقدرات كبيرة في مجال الفضاء السيبراني. من جهة أخرى تنمو الصين بسرعة كقوة اقتصادية ناشئة، وتستثمر بشكل كبير في تطوير قدراتها السيبرانية بشكل ملحوظ.

كما تتصدر كل من الولايات المتحدة الأمريكية والصين التقارير العالمية لقياس القدرات السيبرانية ومؤشرات الأمن السيبراني العالمية، وذلك بفضل قدرتهما على التأثير والسيطرة في الفضاء السيبراني ومواجهة التحديات السيبرانية، والتكيف مع المتطلبات المتزايدة في هذا المجال على صعيد البنية الرقمية.

لذلك تهدف هذه الدراسة إلى استعراض وتحليل القدرات السيبرانية للولايات المتحدة الأمريكية والصين، وتقديم نظرة شاملة عن استراتيجياتهما وأهدافهما في مجال القدرات السيبرانية، ودراسة تطور تلك القدرات، وكيفية استخدامها لتعزيز مكانة البلدين في المنافسة الدولية، بالإضافة إلى دورها في المواجهة والتصدي للتحديات السيبرانية المتزايدة.

وينطلق هذا البحث من السؤال المركزي الآتي: كيف يؤثر التنافس السيبراني بين الولايات المتحدة والصين في تعزيز نفوذهما العالمي، وكيف يتجلى ذلك في الاستراتيجيات السيبرانية لكل منهما؟

أولاً: القدرات السيبرانية للولايات المتحدة الأمريكية

بدأت الولايات المتحدة منذ أكثر من عقدين بالقلق إزاء نقاط الضعف في المجال السيبراني وذلك بالبحث عن طرق للحد منه. وفي الوقت نفسه، بدأت بشكل سري في تطوير واستخدام العمليات السيبرانية الهجومية لأغراض عسكرية مع ضمان تعديل وكالات الاستخبارات التابعة لها لتكييف أنشطة جمع المعلومات الخاصة بها ليشمل استحواذ على شبكة الإنترنت([2]).

وباعتبار الهيمنة على الإنترنت والفضاء السيبراني هدفاً استراتيجياً للولايات المتحدة؛ فقد اعتبرها بعض الخبراء بأنها الدولة الوحيدة التي تتمتع ببصمة عالمية كبيرة في مجال القدرات السيبرانية([3])، حيث يرى

---

[1] - رغدة البهي، **أبعاد التطور في القدرات السيبرانية الروسية عقب الحرب الأوكرانية**، مركز انتريجنال للتحليلات الاستراتيجية، مصر، (2023/9/20) ، تاريخ الزيارة في:https://cutt.us/alpaC، 2023/6/18.

[2] - James A. Lewis, "A Necessary Contest: An Overview of U.S. Cyber Capabilities." Asia Policy, vol. 27 no. 2, 2020, P. 84.

[3] - يعد الصحافي الأمريكي "فرد كابلان" من أهم منظري التكامل الاستراتيجي الأمريكي، للمزيد أنظر في: فرد كابلان، المنطقة المعتمة التاريخ السري للحرب السيبرانية، ترجمة: لؤي عبد المجيد، المجلس الوطني للثقافة والفنون والآداب، سلسلة عالم المعرفة، الكويت، 2019، ص 12.

"ديفيد كلارك" أن الولايات المتحدة هي من أنشأت الإنترنت، وهي الدولة الأقوى من حيث امتلاك القدرات السيبرانية عبر الشركات التكنولوجية العملاقة التي تسيطر عليها([1]).

وقد أشار تقرير صادر عن مركز الأبحاث البريطاني عام 2021 إلى أن الولايات المتحدة تتصدر قائمة "الدول الرائدة الأولى" في مجال القدرات السيبرانية على مستوى العالم دون وجود منافس لها على هذا اللقب، وذلك على الرغم من تصورها بأنها تواجه تهديدات كبيرة من الصين وروسيا وكوريا الشمالية في هذا المجال([2]).

وأكد تقرير صادر عن المعهد الدولي للدراسات الاستراتيجية بأن الولايات المتحدة تتمتع بمكانة فريدة كقوة سيبرانية من الدرجة الأولى في العالم، غير أنه من المتوقع في السنوات القادمة الحديث عن الصين كمنافس نظير بارز ذو قدرات عالية، وجاء في التقرير أيضاً أن "الهيمنة على الفضاء السيبراني كانت هدفاً استراتيجياً للولايات المتحدة منذ منتصف التسعينيات، فهي تظهر كدولة فريدة تمتلك بصمة عالمية قوية في استخدامات الفضاء السيبراني، سواء في المجال المدني أو العسكري([3]).

وتُعتبر الولايات المتحدة، من الدول الرائدة في مجال امتلاك القدرات السيبرانية والعسكرية، وتمتلك "**القيادة السيبرانية الموحدة USCYBERCOM** " تابعة لوزارة الدفاع الأمريكية، وتتمتع بسلطة توجيهية لعمليات الفضاء السيبراني. تأسست هذه القيادة في 23 يونيو عام 2009 بمقر وكالة الأمن القومي في فورت ج ميد، ماريلاند، كقيادة فرعية موحدة تحت القيادة الاستراتيجية الأمريكية، وقد جاء إنشائها للأهمية المتزايدة وضعف أجهزة الكمبيوتر والشبكات في الولايات المتحدة وحول العالم في ذلك الوقت، ونتيجة الاعتماد المتزايد لوزارة الدفاع الأمريكية على أنظمة الفضاء السيبراني لقيادة قواتها والسيطرة عليها، وبالتالي فقد أدركت الحاجة إلى حماية هذه الأنظمة الحيوية والدفاع عنها([4]).

وتنسق القيادة في عملها مع شبكات وكالة الأمن القومي، ويرأسها مدير وكالة الأمن القومي الأمريكي، الجنرال بول ناكاسوني([5]). وعلى الرغم من أن هذه القيادة تم إنشاؤها في الأصل لأغراض دفاعية، إلا أنها يُنظر إليها على أنها قوة هجومية تعتمد على خمسة مكونات أساسية، هي: القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة السيبرانية للقوات الجوية، والقيادة السيبرانية لقوات مشاة البحرية وخفر السواحل،

1- David Clarke, Cyber War, Op. cit, P.144.

2- Cyber Capabilities and National Power: A Net Assessment, Op. cit, P. 15.

3- Brad D. Williams , US 'Retains Clear Superiority' In Cyber; China Rising: IISS Study, Breaking Defense, 28/6/2021, https://urlz.fr/q0Lm,Accessed: (5/9/2023)

4- Lisa Ferdinando, Cybercom to Elevate to Combatant Command, US Department of Defence, May 3, 2018, https://urlz.fr/q0LA Accessed: (21/9/2023)

5- Paul M. Nakasone, US Department of Defense, https://urlz.fr/pZFQ, Accessed: (21/9/2023)

إضافة إلى وحدات الحرس الوطني([1]). ويبلغ عدد الفرق السيبرانية في هذه القيادة نحو 133 فريقاً تضطلع بمهمات مختلفة في مجال حماية الأمن السيبراني([2]).

وقد أطلقت وزارة الدفاع الأمريكية (البنتاغون)، في سبتمبر عام 2023، وثيقة "استراتيجية وزارة الدفاع السيبرانية لعام 2023"، والتي تحدد كيفية عمل الوزارة لحماية الشعب الأمريكي وتعزيز أولويات الدفاع في المجال السيبراني([3]).

وتستند الوثيقة إلى استراتيجية الأمن القومي والدفاع الوطني والأمن السيبراني، وترتكز الاستراتيجية على العمليات السيبرانية التي نفذها البنتاغون منذ عام 2018، وتطرح تحديات مثل: الحرب الروسية على أوكرانيا والدروس المستخلصة منها، وأبرزها أهمية التكامل بين القدرات السيبرانية والقدرات القتالية التقليدية، وأيضاً تحدد الاستراتيجية كيفية قيام وزارة الدفاع بتعظيم قدراتها السيبرانية لدعم الردع المتكامل واستخدام عمليات الفضاء السيبراني بالتنسيق مع أدوات القوة الوطنية الأخرى، وأيضاً تسلط الاستراتيجية الضوء على إجراءات وزارة الدفاع للاستثمار في ضمان الدفاع والتوافر والموثوقية والمرونة لشبكاتها السيبرانية والبنية التحتية لدعم الوكالات غير التابعة لوزارة الدفاع في أدوارها ذات الصلة ولحماية القاعدة الصناعية الدفاعية.

وتتضمن الاستراتيجية الأمريكية لعام 2023 تحديات رئيسية تتمثل في كوريا الشمالية والصين، تهدف"البنتاغون" من خلال هذه الاستراتيجية إلى تحقيق أربعة أهداف في مجال الدفاع السيبراني والجهوزية السيبرانية، بما في ذلك بناء شبكة لحماية المجال السيبراني مع الحلفاء والشركاء، وإجراء إصلاحات في المؤسسات التابعة للوزارة لتعزيز التقدم في هذا المجال. كما تؤكد الاستراتيجية على أهمية التعاون والتنسيق مع المؤسسات الفيدرالية الأخرى لبناء قدرات سيبرانية قوية ومتكاملة([4]).

وترتكز الاستراتيجية على مبدأ "الدفاع المتقدم"، لذا يُنظر إلى القوة السيبرانية الأمريكية على أنها قوة هجومية في المقام الأول، تستند على دمج القدرات التكنولوجية في جميع مراحل العمليات التي تقوم بها([5]).

وفي 16 ديسمبر 2022 صادق مجلس الشيوخ الأمريكي على الميزانية الدفاعية الجديدة لعام 2023، على تخصيص 11.2 مليار دولار لحماية الفضاء السيبراني الذي أصبح ساحة رئيسية للمواجهة بين القوى

---

[1]- U.S. Cyber Command, cybercom, https://urlz.fr/q0Nk , Accessed: (18/9/2023).

[2]- C. Todd Lopez, Cyber Mission Force Set to Add More Teams, US Department of Defence, April 6, 2022, https://urlz.fr/pZFS , Accessed: (21/9/2023).

[3]- Department of Defense Releases 2023 Cyber Strategy Summary, U.S Department of Defense, Sept. 12, 2023, https://urlz.fr/pZFT , Accessed: (18/9/2023).

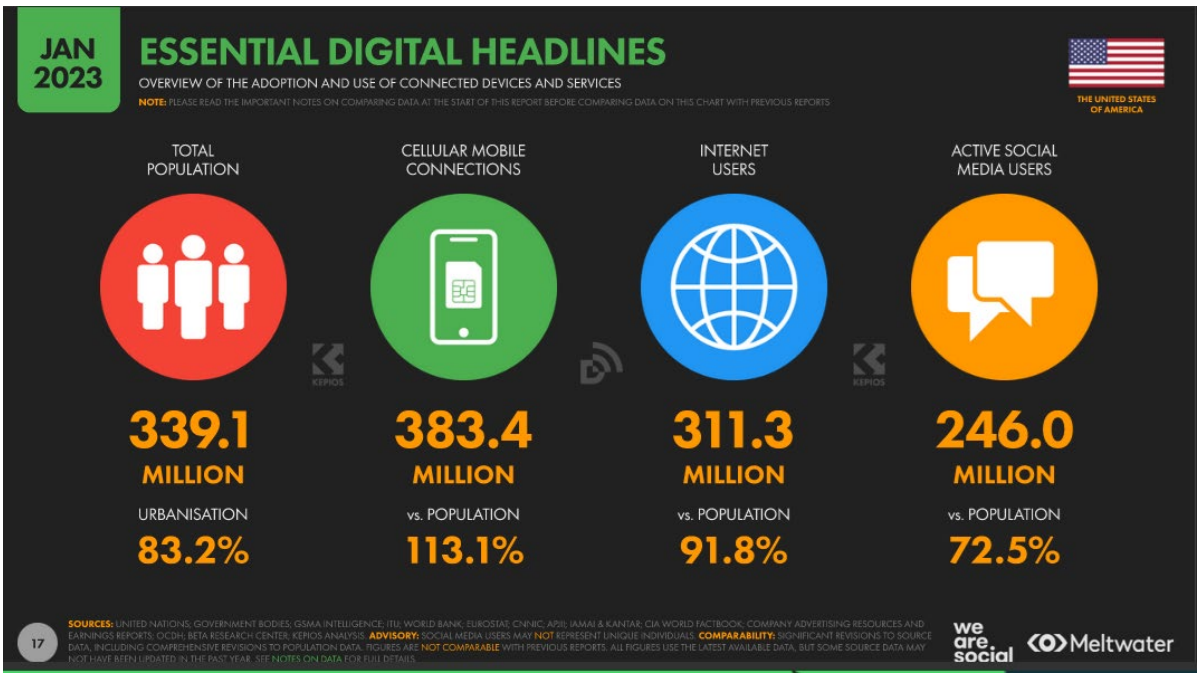
[4]- Ibid. Accessed: (18/9/2023).

[5]- هدى النعيمي، الهجمات السيبرانية وتصاعد المنافسة الدولية، مرجع سبق ذكره، تاريخ الزيارة في:(2023/9/21)

الكبرى، وحوالي 2.9 مليار دولار إلى وكالة الأمن السيبراني الأمريكية وأمن البنية التحتية([1])، وفي المقابل طلبت إدارة الرئيس جو بايدن من الكونجرس زيادة التمويل السيبراني بمبلغ 26.6 مليار دولار في السنة المالية 2024([2]).

وتمتلك الولايات المتحدة مجموعة من العوامل والمميزات التي تجعلها قوة بارزة في هذا المجال من خلال امتلاكها قدرات سيبرانية متقدمة سواء بالتعاون مع القطاع الخاص، والاستثمار في البحث والتطوير المتعلق بالأمن السيبراني، وقدرتها على تنفيذ هجمات سيبرانية[3]. كما لديها قوة عاملة مختصة في المجال السيبراني، وتعاون وثيق مع شركات التكنولوجيا العملاقة (غوغل، فيسبوك، مايكروسوفت...) التي تتخذ من الولايات المتحدة مقراً لها.

الشكل رقم (1): عدد مستخدمي الإنترنت في الولايات المتحدة (2015 – 2023):



[1]- Mark Stone, How much is the U.S. investing in cyber (and is it enough)?, Security Intelligence, January 20, 2023, https://urlz.fr/q0NP , Accessed: (21/9/2023).

[2]- Sean Carberry, White House Asks for $842 Billion in 2024 DOD Funding, 3.2 Percent Above 2023 Budge,National defense magazine, 3/9/2023, https://urlz.fr/q0NU , Accessed: (22/9/2023), See Also:

Biden's 2024 Budget Impacts IT Modernization Across Government, Government CIO Media, (15/3/2023). https://urlz.fr/q0OO , Accessed: (21/9/2023).

[3]- Denise E. Zheng, 2015 DOD Cyber Strategy ,CSIS, April 24, 2015, https://urlz.fr/q0OW , Accessed: (22/9/2023).

Source: Number of internet users in the United States from 2015 to 2023, Feb 22, 2023, https://urlz.fr/q0PB ,Accessed: (22/9/2023).

ويوضح الشكل رقم (1) أن عدد الأشخاص الذين وصلوا إلى الانترنيت في الولايات المتحدة الأمريكية قد تجاوز 311 مليون شخص منذ يناير 2023، مما يجعلها واحدة من أكبر الأسواق عبر الإنترنت في العالم. وتحتل الولايات المتحدة الأمريكية حالياً المرتبة الثالثة بعد الصين والهند فيما يتعلق بحجم الجمهور المتصل بالإنترنت.

وحسب المعطيات، كانت الولايات المتحدة الأمريكية موطنًا لـ 246.0 مليون مستخدم لوسائل التواصل الاجتماعي في يناير 2023، أي ما يعادل 72.5 %من إجمالي السكان. وكان ما مجموعه 383.4 مليون اتصال محمول خلوي نشط في الولايات المتحدة في أوائل عام 2023، وهذا الرقم يعادل 113.1% من إجمالي السكان. وهناك 246.0 مليون مستخدم لوسائل التواصل الاجتماعي.

وتزداد أهمية النجاح في المجال السيبراني بشكل ملحوظ بكونه أصبح ضرورياً لتعزيز المصالح القومية الأمريكية. وفي الوقت الحالي تحدد التكنولوجيات الرقمية عدد العمليات التي تصف عمل المجتمعات الحديثة والتي تمتد من الاتصال إلى التمويل ومن الكهرباء إلى النقل ومن التجسس إلى الأمن القومي. وتركز جهود الولايات المتحدة الأمريكية في تعزيز قدراتها السيبرانية استناداً إلى هذه الحقائق، مع المنافسة الشرسة مع دول أخرى مثل الصين وروسيا.

وتسعى الولايات المتحدة الأمريكية، التي اخترعت الإنترنيت إلى ضمان استمرارية دور الإنترنيت في تعزيز قوتها ونفوذها وحريتها وأمنها الإليكتروني. فمن وجهة نظر الولايات المتحدة الأمريكية فإن الفضاء السيبراني يجب أن يُعزز التفوق العسكري وممارسة الأنشطة الاستخبارية لحماية الأمن القومي والعمل على ردع القوى الدولية المنافسة ومواجهة التهديدات المعلوماتية وحماية النظام الانتخابي الديمقراطي عبر كسب الحروب في أي مجال، بما في ذلك الفضاء السيبراني وشن هجمات سيبرانية استباقية والتعاون مع الحلفاء لتحقيق هذه الأهداف([1]).

انطلاقاً مما سبق، فإن الولايات المتحدة تتمتع بقدرات سيبرانية متقدمة تعكس التزامها القوي بحماية أمنها ومصالحها في الفضاء السيبراني. يتجلى هذا الالتزام عبر ممارسة التوسع الأمريكي نحو تحقيق سيادة الفضاء السيبراني من خلال مجموعة من السياسات والاستراتيجيات الرئيسية أهمها ممارسة السيطرة على منظمة "آيكان" (ICANN)، وهي المنظمة المسؤولة عن إدارة أسماء النطاقات على الإنترنت، وهذا يساهم في تعزيز تأثير الولايات المتحدة في الهياكل العالمية للإنترنت وضمان استدامتها.

[1]- شريفة كلاع، الأمن السيبراني وأشكال التهديد: تحديات عالمية، ط 1، ألفا للوثائق، الأردن، 2023، ص 220.

بالإضافة إلى ذلك تعبر زيادة الولايات المتحدة الأمريكية لميزانيتها في المجال السيبراني عن التزامها بمكافحة التهديدات السيبرانية وتعزيز القدرات الدفاعية والهجومية في هذا المجال، فالاستثمار المستمر في هذا القطاع، الذي يقدر بمليارات الدولارات، يسهم في تطوير تكنولوجيا سيبرانية متقدمة ويوظف قوة عاملة متخصصة ومدربة لمواجهة التهديدات بفعالية، إضافة إلى الاستثمار المستمر في الأمن السيبراني الذي يُسهم في حماية البنية التحتية الحيوية.

ويشير تقرير مركز بيلفر للعلوم والشؤون الدولية التابع لجامعة هارفارد لعام 2022([1])، وقبله مؤشر المعهد الدولي للدراسات الاستراتيجية لعام2021([2]) الذي يستعرض القدرات السيبرانية لـ 15 دولة في العالم)، إلى تصدر الولايات المتحدة الأمريكية للمرتبة الأولى على مستوى العالم كدولة تتمتع بنقاط قوة رائدة في الفضاء السيبراني، حيث تمتلك قدرة استخبارات سيبرانية عالية الجودة، وقاعدة أكاديمية وصناعية سيبرانية قوية، إضافة إلى استراتيجية وعقيدة متقدمة، والحكم والقيادة والاعتماد السيبراني، والأمن السيبراني والمرونة، والريادة العالمية في شؤون الفضاء السيبراني، والقدرة الهجومية السيبرانية.

كما احتلت الولايات المتحدة في عام 2020، المرتبة الأولى في مؤشر الأمن السيبراني العالمي Global Cybersecurity Index (GCI) الذي يصدر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة برصيد 100 نقطة مؤشر من بين الدول ذات أعلى التزام بالأمن السيبراني([3]).

وبهذا، يرى الباحث أن القدرات السيبرانية الأمريكية تعتمد على تقنيات متطورة وتكنولوجيا عالية الدقة في وضع سياستها واستراتيجياتها على الصعيدين الوطني والدولي، وتقوم الولايات المتحدة بالاستفادة من أسس علمية متقدمة سبقت بها العديد من الدول في مجال السيبرانية بفترة زمنية. هذا التفوق يمكّن الولايات المتحدة من تحقيق السيطرة والقيادة في هذا المجال، خاصة مع توظيفها وتطويرها للتكنولوجيا السيبرانية واستخدامها بفعالية، لا سيما أنها تسعى جاهدة إلى تطوير وتعزيز قدراتها السيبرانية بهدف تحقيق أهدافها الاستراتيجية، والتي من ضمنها الهيمنة على الفضاء السيبراني في ظل التنافس مع الدول الأخرى لا سيما مع الصين وروسيا؛ مما يعكس أهمية الفضاء السيبراني كبيئة استراتيجية حيوية وضرورة لضمان الأمن القومي والاقتصادي والعسكري.

[1]- National Cyber Power Index 2022, https://urlz.fr/mMqt, Accessed: 22/9/2023

[2]- Cyber Capabilities and National Power: A Net Assessment, IISS, 28th June 2021, https://urlz.fr/q0U7, Accessed: 22/9/2023

[3]- Global Cybersecurity Index 2020 ,International Telecommunication Union, https://urlz.fr/q0Yd, Accessed: 22/9/2023

ثانياً: القدرات السيبرانية للصين

تعود ارهاصات الصين للتحول لقوة سيبرانية عظمى إلى سنة 2014 حيث قدَّم الرئيس الصيني (شي جين بينغ Xi Jinping) مفهوم "القوة السيبرانية العظمى"، وذلك عند إنشائه المجموعة القيادية المركزية من أجل الأمن السيبراني وتكنولوجيا المعلومات بالحزب الشيوعي الصيني[1]، وطرح عدة مفاهيم لاتزال تحدد أهمية الفضاء السيبراني لطموحات الصين الدولية مسلطاً الضوء على تأثير ثورة تكنولوجيا المعلومات في التطورات في الشؤون السياسية والاقتصادية والعسكرية الدولية([2]).

وقد بدأت الصين بالاهتمام ببناء استراتيجية سيبرانية عام 2016، خلال المؤتمر العاشر للحزب الشيوعي الصيني، حيث أكدت السلطات العليا على أهمية المجال السيبراني. وتم دعم هذه الاستراتيجية من خلال أول قانون صيني للأمن السيبراني في 2017 ([3]). حددت الاستراتيجية تسع مهام أساسية، مع التركيز على السيادة وتقوية الدفاع الإلكتروني، وعملت اللجنة المركزية للحزب على تطويره وفي الوقت نفسه حوكمته، وقامت أيضاً بترتيب القضايا ذات الصلة بالإعلام والقوة السيبرانية في جميع المجالات، مما يتيح للصين ببناء وتطوير استراتيجية سيبرانية قادرة على المنافسة في الساحة الدولية[4].

إنّ التحسينات التي حققتها الصين على مدار السنوات الماضية وخبرتها في تطوير قدرات الهجمات السيبرانية وبناء المؤسسات ذات الصلة، والقدرة الهجومية وتوظيف أدواتها السيبرانية في العمليات العسكرية، جعل مؤشر القوة السيبرانية الوطني لعام 2022 الصادر عن مركز بيلفر للعلوم والشؤون الدولية التابع لجامعة هارفادر يصنف الصين على أنها ثاني أكبر قوة سيبرانية شمولاً بعد الولايات المتحدة([5]).

توافق هذه التقديرات إلى حد كبير مع ما استعرضه المعهد الدولي للدراسات الاستراتيجية (IISS) في تقريره الصادر في يوليو 2021 الذي وضع ترتيباً للقوى السيبرانية الكبرى في العالم، معتمداً على سبعة معايير هي: الاستراتيجية والعقيدة، والإدارة والقيادة والسيطرة، وقدرات الاستخبارات السيبرانية، والاعتمادية على

---

[1]- شريفة كلاع، مرجع سبق ذكره، ص 227.

[2]- المرجع نفسه، ص 227.

[3]- Lyu Jinghua, What Are China's Cyber Capabilities and Intentions?, Carnegie Endowment for International Peace, April 01, 2019, https://urlz.fr/q0Y7, Accessed, (23/9/2023)

[4]- عبد الكريم زهير عطية الشمري وحازم موسى الجنابي، "مطارحات هيمنة الاستراتيجية الأميركية السيبرانية"، مجلة تكريت للعلوم السياسية، جامعة تكريت - كلية العلوم السياسية، العراق، العدد 24، 2021، ص 17.

[5]-Biswarup Baidya, Cyberwarfare: Growing Chinese Cyber Threats and Implications for India, May 5, 2023, https://urlz.fr/q0Vf , Accessed: 22/9/2023, See Also:

National Cyber Power Index 2022, Belfer Center for Science and International Afiairs, https://urlz.fr/mMqt , Accessed: (22/9/2023).

الفضاء السيبراني، والأمن السيبراني، والريادة العالمية في الفضاء السيبراني والقدرات السيبرانية الهجومية([1]).

كان إدراج "قوة الدعم الاستراتيجي" في جيش التحرير الشعبي الصيني في عام 2015 سبباً في تعزيز حلم الصين في التحول إلى قوة عظمى سيبرانية مهيمنة بحلول عام 2025. وتنظر المؤسسة العسكرية الصينية إلى الحرب السيبرانية باعتبارها تدبيراً وقائياً للعمليات العسكرية التقليدية.

كما أنها تستخدم تقنيات التجسس الإلكتروني للتعرف على نقاط الضعف في البنى التحتية الحيوية لخصمها والتي يمكن التلاعب بها في زمن الحرب. ومع وضع هذا الهدف في الاعتبار، أدخلت الصين العديد من المجالات السيبرانية إلى قواتها المسلحة، وهي الإدارة الثالثة لجيش التحرير الشعبي المسؤولة عن الدفاع عن شبكات الكمبيوتر، واستخبارات الإشارة، واستغلال شبكات الكمبيوتر، والقسم الرابع مسؤول عن الحرب الإلكترونية للشبكة المتكاملة، وهجمات شبكات الكمبيوتر، ودمج قوة الدعم الاستراتيجي مع الاستخبارات والاتصالات لبناء قوة حرب معلومات متكاملة.

وتتبع الصين نهج "الأمة بأكملها" في بناء النظام البيئي للمجال السيبراني، بما في ذلك العديد من مجموعات القراصنة الوطنية، وطلاب الجامعات كمحاربين سيبرانيين، وشركات الاتصالات الخاصة مثل هواوي وZTE بالتعاون مع جيش التحرير الشعبي الصيني([2]).

وتنقسم الوحدات الصينية المسؤولة عن تنفيذ أنشطة سيبرانية إلى مجموعتين: الهاكرز المحترفين داخل الجيش الشعبي الصيني والهاكرز "الوطنيين" الذين يعملون من وقت لآخر لصالح الحكومة ويدعمون عمليات مختلفة في الفضاء السيبراني. وبالرغم من أن الهيكل الصيني للإشراف على العمليات السيبرانية ليس موجوداً بوضوح كما هو الحال في الولايات المتحدة، إلا أن معظم الخبراء يعتقدون أن معظم العمليات السيبرانية تجرى تحت إشراف القسم الثالث التابع لإدارة الأركان العامة للجيش الشعبي الصيني([3]).

ويشبه هذا الهيكل إلى حد ما وكالة الأمن القومي الأمريكية، ويركز جهوده على استخبارات الإشارات وكسر الشفرات وأمان الاتصالات السيبرانية للجيش الشعبي الصيني. حيث كان هناك حوالي 130,000 شخصاً يعملون في هذا القسم. والعنصر الأهم فيه هو مركز الحاسوب الشمالي ببجين، الوحدة PLA 61539 الذي

---

[1]-Cyber Capabilities and National Power: A Net Assessment, IISS, 28th June 2021, https://urlz.fr/q0U7 , Accessed: (22/9/2023).

[2]- Biswarup Baidya, op. cit, (22/9/2023).

ZTE Corporation is a Chinese partially state-owned technology company that specializes in telecommunication. Founded in 1985, ZTE is listed on both the Hong Kong and Shenzhen Stock Exchanges.

[3]- Andrzej Kozłowski, The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan, Wydawnictwo Uniwersytetu Łódzkiego, 2015, p.164, https://urlz.fr/q0Xo , Accessed, (22/9/2023).

يشرف على عشرة أقسام تعمل على "تصميم وتطوير أنظمة الدفاع والهجوم واستغلال الشبكات الحاسوبية".

وأيضاً تُركز الصين كثيراً على التدريب، فهناك 12 مرفقاً تدريبياً خاصاً بالقدرات السيبرانية موجوداً في جميع أنحاء الصين، وتلعب وحدة متخصصة في الأمن السيبراني موجودة في أكبر قاعدة عسكرية في الصين، وتغطي مساحة 1066 كيلومتراً مربعاً تسمى Zhurihe دوراً خاصاً حيث تحاكي سلوك الولايات المتحدة وحلفائها في الفضاء السيبراني وتستخدم لتدريب الوحدات السيبرانية الصينية وزيادة قدراتها([1]).

أما وحدة الهجمات السيبرانية الصينية "السرية" الأكثر شهرة فهي "الوحدة 61398" التابعة للفرقة الثالثة من الجيش الشعبي الصيني، والتي تتألف من أكثر الخبراء والمتخصصين في تكنولوجيا المعلومات ومهندسي الإلكترونيات والرياضيين واللغويين (معظمهم يتحدثون اللغة الإنجليزية) ويقع مقرها الرئيسي في شنغهاي، وهي تلعب دوراً ليس فقط كوحدة تقليدية، بل تشكل مركزاً تشغيلياً ينفذ القرارات التي اتخذت في بكين بشأن النشاط في الفضاء السيبراني([2]).

ويلعب القسم الرابع (السيبراني) أيضاً دوراً في إدارة العمليات السيبرانية والتدابير المضادة الإلكترونية التابعة لهيئة الأركان العامة لجيش التحرير الشعبي، حيث يتولى مهمة الهجمات السيبرانية الهجومية والتدابير الإلكترونية المضادة (التشويش ومكافحة التشويش)، والتصدي للتهديدات السيبرانية وتعزيز أمن المعلومات والبنية التحتية([3]).

وتحت هذا القسم يعمل ثلاثة معاهد بحثية، وأربعة مراكز تشغيلية، واثني عشر مكتباً تشغيلياً، والتي تراقب اتصالات الهاتف والراديو والأقمار الصناعية والكمبيوتر، حيث يوجد مجتمع كبير يسمى بالقراصنة الوطنيين في الصين، الذين يقومون بعمليات بسيطة في الفضاء السيبراني مثل، هجمات منع الوصول من الخدمة وتشويه "الويب" وتفجير البريد الإلكتروني.

وينتمي إلى هذه المجموعات أعضاء أقسام تكنولوجيا المعلومات بالجامعات، والموظفون في أقسام تكنولوجيا المعلومات في المؤسسات المملوكة للدولة، واللاعبون عبر الإنترنت الذين يتعاونون مع الحكومة أو يعملون تحت توجيهها لتنفيذ مهام سيبرانية محددة([4]).

---

[1]- Ibid, p. 165.

[2]- Adam Jourdan, China-U.S. cyber spying row turns spotlight back on shadowy Unit 61398, Reuters, May 20, 2014, https://urlz.fr/q0X1 , Accessed, (22/9/2023).

[3]- Mark Clayton, US indicts five in China's secret 'Unit 61398' for cyber-spying on US firms, The Christian Science Monitor, May 19, 2014, https://urlz.fr/q0Xd , Accessed, (22/9/2023.)

[4]- Andrzej Kozłowski, op. cit, p.165.

وقد أصبح قطاع التكنولوجيا الرقمية للصين مقياساً لقوتها ونفوذها في الخارج، وجبهة رئيسية في الصراع الذي تخوضه مع الولايات المتحدة. وعلى الرغم من وجود عدد كبير من السياسات المعمول بها في الصين في المجال السيبراني والتكنولوجي والرقمي، فإن إستراتيجية الصين الرقمية (الشاملة) التي نشرت في فبراير 2023، تهدف إلى دفع التنمية الرقمية في الصين إلى الأمام تحت عنوان "إستراتيجية الصين الرقمية"([1]).

وتقترح الاستراتيجية تحوُّل الصين إلى الرقمنة كلياً بحلول عام 2025، لتصبح بكين رائدة عالمياً في المجال الرقمي في غضون عام 2035. وجرى العمل على تطوير إستراتيجية الصين الرقمية وفقاً لإطار عمل رسمي يُعرَف باسم "2522"، ويمثل كل رقم واحداً من البنود الرئيسة للاستراتيجية، وأحد الأهداف والطرق والوسائل "للصين الرقمية"، بما في ذلك المكون الدولي([2]).

كما تسعى الصين إلى تعزيز التطور الرقمي في بناء البنية التحتية السيبرانية ونظام موارد البيانات، بالإضافة إلى زيادة دمج التقنيات الرقمية مع قطاعات البنى التحتية، وتسريع بناء شبكة الجيل الخامس، والتطبيق الواسع النطاق للإصدار السادس لبروتوكول الإنترنت، ونظام "بي دو" (BeiDou) للملاحة عبر الأقمار الصناعية، بالإضافة إلى تطوير إنترنت الأشياء (IoT)([3]).

وتستخدم الصين القدرات السيبرانية في المقام الأول لتحقيق الاحتياجات والمصالح المحلية، لتوليد الرخاء والحفاظ على النمو الاقتصادي والاستقرار الاجتماعي، وينصب التركيز الرئيسي على "تطهير" شبكة الإنترنت في الصين من الأفكار والمعلومات التي قد تُشكل تحدياً لسلطة الحزب الشيوعي الصيني، مما يجعل تكنولوجيات المراقبة والرقابة أمراً حيوياً([4]).

إنّ ظهور الصين كقوة عالمية كبرى يعمل على إعادة تشكيل المجال السيبراني، لاسيما وأن الصين تتمتع بأكبر مجتمع لمستخدمي الإنترنت في العالم، وتُبين احصائيات عام 2023، أن حوالي 884 مليون شخصاً يستخدمون الإنترنت للتسوق والتعليم والتجارة، أي ما يمثل حوالي نسبة 82 % من مستخدمي الإنترنت في

---

[1]- خالد وليد محمود، ماذا وراء الإعلان عن إستراتيجية الصين الرقمية؟، الجزيرة نت، 2023/4/15، تاريخ الزيارة https://cutt.us/D5UNY ، في: (2023/9/22).

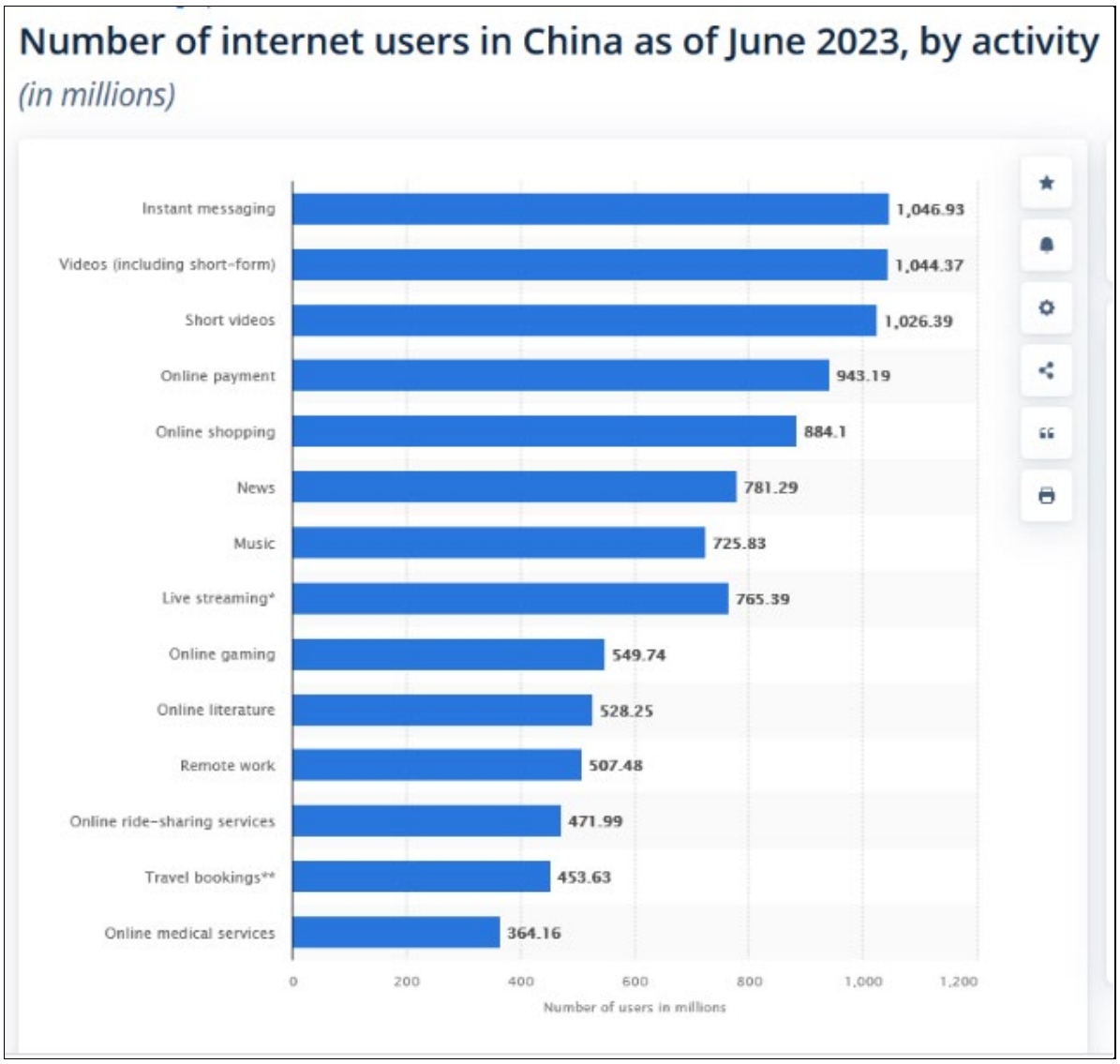
[2]- David Dorman, The Digital China "Plan" is New, but "Digital China" is Not, Digital china wins the future, (27/2/2023), https://urlz.fr/q0Xw

[3]- Sarah Sewall, Tyler Vandenberg, Kaj Malden, China's BeiDou, New Dimensions of Great Power Competition, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, US, Feb. 2022, https://urlz.fr/q0Xz , Accessed: (22/9/2023).

[4]- Helene Pleil, Being a Cyberpower – China's Ambitions in Cyberspace, Tech Policy Press, 30/3/2023, https://urlz.fr/q0XE , Accessed, (22/9/2023).

الصين([1]). وكان إجمالي 1.69 مليار اتصال محمول خلوي نشطاً في الصين في أوائل عام 2023، وهذا الرقم يعادل 118.6 % من إجمالي السكان([2]).

الشكل رقم (2): عدد مستخدمي الإنترنت في الصين (يونيو 2023)



Source: Number of internet users in China as of June 2023, by activity, statista, Sep 14, 2023, https://urlz.fr/q0W5 , Accessed, (22/9/2023).

تتميز القدرات السيبرانية الصينية بشيوع ثقافة الإنترنت وتغلغلها، والتي تعد الركن الرئيسي في تطور الاستراتيجية السيبرانية، نظراً للعدد الكبير من مستخدمي الإنترنت، وكذلك لتوافر عدد كبير من الأجهزة

[1]- Number of internet users in China as of June 2023, by activity, statista, Sep 14, 2023, https://urlz.fr/q0W5 , Accessed: (22/9/2023).

[2]- Digital 2023: China, Data Reportal, Feb.2023, https://urlz.fr/q0XK , Accessed: (22/9/2023).

الإلكترونية والبنية التحتية([1])، بالإضافة إلى ذلك، تمتلك الصين قدرات مميزة في صناعة التكنولوجيا والمعلومات، وتمتاز وبقدرات بحثية تكنولوجية في مجال الذكاء الاصطناعي، فضلاً عن القدرات العسكرية والاستخبارية السيبرانية.

ويدعم هذا المشهد محفزات اقتصادية وسياسية وعسكرية، حيث رؤية الرئيس الصيني، تمثل السيادة السيبرانية حق كل دولة باختيار طريقها الخاص إلى التنمية السيبرانية، وأسلوبها في التنظيم السيبراني وتنظيم السياسات العامة للإنترنت، والمشاركة في حكم عالمي للفضاء السيبراني بحيث تكون على قدم المساواة مع الدول الأخرى([2]).

بناء على ما سبق، تعكس القدرات السيبرانية الصينية نمواً سريعاً وتقدماً تكنولوجياً واقتصادياً يضعها في صدارة المؤشرات الدولية في هذا المجال، وتمتلك الصين أسساً تكنولوجية قوية وموارد اقتصادية تدعم تطوير الأمن السيبراني، ومع ذلك، هناك تحديات تشمل استخدام محتمل للقدرات السيبرانية في الجانب العسكري واتهامات بشن أو تسخير هذه القدرات لشن هجمات سيبرانية لا سيما على صعيد الاختراقات والخصوصية والرقابة.

خاتمة:

إن تحليل القدرات السيبرانية الأمريكية والصينية والتنافس بينهما يشكل جزءًا حيويًا من المشهد الدولي الحديث. إذ يتسارع التطور التكنولوجي في مجال الفضاء السيبراني، مما يعكس تأثيره في عنصري القوة والأمن الوطنيين. فالولايات المتحدة الأمريكية تمتلك اليوم قوة سيبرانية هائلة، مدعومة بالابتكار التكنولوجي والاستراتيجيات السيبرانية الدفاعية والهجومية. بينما تعزز الصين بشكل متزايد من قدراتها السيبرانية، وتعدل استراتيجياتها العسكرية لتشمل الأبعاد الرقمية، فالقطاع التكنولوجي الصيني يشهد تقدمًا سريعًا، ويُعد تحديث التشريعات وتعزيز الابتكار دليلاً على هذه القدرة في تحقيق تفوق سيبراني عالمي ومنافس للولايات المتحدة الأمريكية.

---

[1]- على الرغم من ان الصين تتجه نحو وضع أهداف لزيادة دمج اقتصادها وصناعاتها وتقنياتها العسكرية بالفضاء السيبراني، إلا أنها تحاول أن تبقى زمام الأمور تحت سيطرتها قدر الإمكان، وبالنسبة لها؛ فإن حماية الفضاء السيبراني مسألة دفاع قومي هذا يعني أن الحكومة تتحكم كلياً بهذا الفضاء وتمارس الرقابة عليه لا بل تفصل شبكة الإنترنت الداخلية عن العالم الخارجي أو تعطلها نهائياً. ووضعت الصين تشريعات سيبرانية مكنتها من أن تحصن البنى التحتية السيبرانية بما يسمى جدار النار الصيني العظيم. انظر: أنديرا عراجي، مرجع سبق ذكره، ص 167.

[2]- إستراتيجية "شي جين بينغ" الثورية.. كيف تغير الصين مستقبل الإنترنت في العالم؟، الجزيرة نت، (2020/7/2)، https://cutt.us/3XYZa ، تاريخ الزيارة في: (2023/9/22)، أنظر أيضاً:

RUSH DOSHI, EMILY DE LA BRUYÈRE,NATHAN PICARSIC, AND JOHN FERGUSON, CHINA AS A "CYBER GREAT POWER", Foreign Policy at Brookings, APRIL 2021, https://urlz.fr/q0Yq , Accessed: (22/9/2023)

ومن المرجح أن يتسارع هذا التنافس في مجالات مثل الذكاء الاصطناعي والتكنولوجيا السيبرانية، مما يؤدي إلى تطورات هائلة في هذه القدرات. إذ يُظهر التحليل والاستشراف بهذا الجانب أن التنافس بين القدرات السيبرانية الأمريكية والصينية سيستمر في تحديد المشهد الدولي الذي تعززه التطورات والتحولات الهائلة في الديناميات الجيوسياسية والتكنولوجية السيبرانية المتقدمة التي ستمثل عامل محوري يحدد القواعد الجديدة للقوة والتأثير العالمي مستقبلاً.