

جيوبوليتيكا الأمن السيبراني؛ دراسة حالة الصراع الصيني الأمريكي في

الفضاء السيبراني

The geopolitics of cybersecurity: Case Study of the Sino-American Cyber rivalry

الغنجة هيشام داود*، المدرسة الوطنية العليا للعلوم السياسية

hichemdadoud.el-ghandja@enssp.dz

تاريخ إرسال المقال: 2024 /09 /14 تاريخ قبول المقال: 2025 /04 /28 تاريخ نشر المقال: 2025 /05 /13

الملخص:

استهدفت هذه الدراسة تحليل تطور مفاهيم الجيوبوليتيكا والأمن، ودراسة آثار ذلك في بروز مفهوم الأمن السيبراني وتطوره. كما سعت الدراسة إلى استكشاف حالة الصراع الجيوبوليتيكي بين الولايات المتحدة الأمريكية والصين في الفضاء السيبراني. ركز الباحث في بداية دراسته على تحديد استراتيجيات كل من البلدين في مجال الأمن السيبراني، ثم عرض أبرز مظاهر هذا الصراع وأهم أمثلته. تشير النتائج المتوصل إليها أن الأمن السيبراني يعد مكوناً أساسياً في التنافس بين الدولتين، ويشكل جانباً محورياً من جوانب الأمن القومي على نطاق واسع. كما تُعتبر الصين أكبر تهديد سيبراني للولايات المتحدة، حيث تستهدف بنيتها التحتية الاقتصادية والعسكرية بطريقة تتماشى مع أهدافها الاستراتيجية بعيدة المدى. بالمقابل، تسعى الولايات المتحدة إلى تقويض القوة الصينية من خلال إضعاف بنيتها التحتية، مما يحول دون صعودها كقوة عظمى في مجالات مثل الذكاء الاصطناعي، والرقائق الإلكترونية، والصناعات العسكرية. وقد تجلت هذه التوجهات في توجيه السياسات السيبرانية وغير السيبرانية لكلا البلدين نحو تقليل نفوذ الآخر في هذه المجالات الحيوية.

الكلمات المفتاحية: جيوبوليتيكا، صراع، أمن سيبراني، فضاء سيبراني.

Abstract:

This study aimed to analyze the evolution of the concepts of geopolitics and security and to examine the implications of this in the emergence and development of the concept of cybersecurity. The study also sought to explore the state of the geopolitical conflict between the United States and China in cyberspace. At the beginning of the study, the researcher focused on identifying the strategies of both countries in the field of cybersecurity, and then presented the most prominent manifestations and examples of this conflict. The findings indicate that cybersecurity is a key component of the rivalry between the two countries and constitutes a pivotal aspect of national security on a large scale. China is the biggest cyber threat to the United States, targeting its economic and military infrastructure in a manner consistent with its long-term strategic goals. In turn, the United States seeks to undermine Chinese power by weakening its infrastructure, preventing its rise as a superpower in areas such as artificial intelligence, chips, and military industries. These trends have

manifested themselves in directing the cyber and non-cyber policies of both countries toward minimizing the influence of the other in these vital areas.

Key words: Geopolitics, Rivalry, Cybersecurity, Cyberspace.

المقدمة:

تعتبر التهديدات والحروب السيبرانية من أبرز التهديدات غير التماثلية التي أصبحت تواجه الدول والفواعل غير الدول، سواء كانت هذه التهديدات آتية من دول أو من مجموعات مدعومة من قبل دول أخرى، أو من طرف جماعات مستقلة نسبياً أو تماماً عن الدول. وصار كثير من الدارسين يربطون بين الأمن السيبراني ومفاهيم أخرى كالجيوبوليتيكا، من حيث أنه يمكن استخدام أدوات التحليل الجيوبوليتيكية في تحليل مختلف التفاعلات في الفضاء السيبراني.

وتكمن أهمية هذا الموضوع، في أن التهديدات السيبرانية لم تساهم في تغيير مفهوم الأمن وتوسيعه فحسب، بل وأصبح كثير من الدارسين يربطون المجال السيبراني بأنه شكل جديد من أشكال تظهر الصراع الجيوبوليتيكي بين الدول العظمى خاصة، بل وبين كل الدول التي أصبحت الكثير منها تتبنى استراتيجيات محددة تهدف إلى تحقيق أقصى قدر من الأمن في الفضاء السيبراني، بما فيها الصين والولايات المتحدة الأمريكية اللتان أصبحتا تعيشان منافسة وصراعا شديدين في هذا الفضاء.

لذلك تكمن إشكالية هذه الدراسة في محاولة تحديد العلاقة بين مفهومي الجيوبوليتيكا والأمن السيبراني، وما هي علاقات التلاقي والتأثير المتبادل بين المفهومين. ونهدف من وراء ذلك خصوصا إلى دراسة درجة امتداد المفاهيم الجيوبوليتيكية التقليدية لتصبح كأدوات تحليل لما يحدث من صراع سيبراني، خاصة بين الولايات المتحدة الأمريكية والصين كدراسة حالة. وما أبرز مظاهر هذا الصراع السيبراني الصيني الأمريكي، بناء على استراتيجيتي الدولتين في هذا الفضاء؟

ومن أجل معالجة الإشكالية السابقة، اتبعنا في هذه الدراسة منهج دراسة الحالة، باعتبارنا ركزنا على حالة صراعية واحدة في الفضاء السيبراني، بين الولايات المتحدة الأمريكية والصين، بشكل قد يسهل فهم طبيعة مختلف الصراعات الأخرى الحادثة في هذا الفضاء.

لذلك بناء على ما سبق، فإننا سنحاول في القسم الأول من المقال دراسة العلاقة بين مفهومي الجيوبوليتيكا والأمن السيبراني، وأوجه التداخل والتلاقي بينهما. في حين سنعالج في القسم الثاني مظاهر الصراع الجيوبوليتيكي في الفضاء السيبراني، بين الصين والولايات المتحدة الأمريكية خصوصا، بداية من إعطاء أمثلة لاستراتيجيات الدولتين فيما يخص الأمن السيبراني، ثم دراسة أبرز مظاهر هذا الصراع السيبراني الصيني الأمريكي.

1- الجيوبوليتيكا والأمن السيبراني، تحديد المفهومين وبيان العلاقة بينهما.

يعتبر مفهوم الجيوبوليتيكا من المفاهيم التي عرف مضمونها تغيرا كبيرا، وانعقد هذا المفهوم نسبيا من المفاهيم التقليدية التي كانت مرتبطة به، فأصبح كثير من الدارسين لا يربطونه بالجغرافيا فحسب، بل بكافة

مظاهر الصراع والتنافس على النفوذ والقوة مهما كان المجال. ومن هذه المجالات التي صار يتجلى فيها هذا التنافس واضحا؛ الفضاء السيبراني.

1.1- الجيوبوليتيكا: تعريف المفهوم ودراسة تطوره.

إن الجيوبوليتيكا في مفهومها التقليدي الذي اتفق حوله المنظرون المؤسسون في هذا العلم، استخدمت في تبرير وتفسير التنافس الكبير بين الدول الذي كان حاصلا سابقا، سواء من حيث التنافس على الموارد، الأقاليم، الصراع من أجل القوة، أو الصراع من أجل التأثير على توازن القوة.¹

ويعرف إيف لاكوست Yves Lacoste الجيوبوليتيكا بأنها صراع قوة على، أو من أجل إقليم محدد. ويعتبر أن ليس كل صراع على إقليم معين هو صراع جيوبوليتيكي بالضرورة، ولكن إذا كان هذا الصراع من أجل السيطرة أو بسط النفوذ على هذه الأقاليم، فيمكن توصيفه حينئذ بأنه صراع جيوبوليتيكي.²

غير أن هذا التعريف، الذي يتفق معه كثير من الدارسين، يحصر الجيوبوليتيكا في معناها التقليدي المرتبط بالجغرافيا تحديدا، في حين أن العديد من الدراسات الجيوبوليتيكية والأمنية المعاصرة تعتبر أن مفهوم الجيوبوليتيكا ليس مرتبطا بالأرض أو الإقليم فحسب، بل يتعداه إلى مجالات أوسع، لعاملين أساسيين: أن الصراع الدولي الحالي قد تعدى الجانب الصراع التقليدي الذي كان مهيمنا سابقا، والذي تميز بالتنافس والصراع الجيوبوليتيكي المرتبط بالجغرافيا، والأمر الثاني أن مفهوم الأمن والإقليم قد أصبح واسعا وغير قابل للتحديد، وغير مرتبط بالحدود الجغرافية التقليدية وبمفهوم الأمن التقليدي. إضافة إلى أن الجيوبوليتيكا ليست مرتبطة بالدولة فحسب، بل بفواعل أخرى كذلك، باعتبار أن المفهوم الأبرز في الجيوبوليتيكا هو الصراع Rivalry وليس الجغرافيا.³

من جهة أخرى، يرى ألكسندر دوغين Alexandre Douguine، أن الجيوبوليتيكا هي علم السلطة ومن أجل السلطة، وهي علم الفئات السياسية العليا، ولا يمكن فهم الجيوبوليتيكا المتعلقة بالدول دون فهم توجهات الدولة واستراتيجياتها في علاقاتها الصراعية مع الدول الأخرى، باعتبار أن الجيوبوليتيكا هي قيادة إمكانيات الدولة لتحقيق أهداف الطبقات الحاكمة. وبالتالي لا يمكن فهم مظاهر الصراع الجيوبوليتيكي مهما كان شكله دون الإحاطة باستراتيجيات الدول المتعلقة بفضاءات الصراع المختلفة.⁴

لذلك نخلص مما سبق أن مفهوم الجيوبوليتيكا المعاصر لا يزال مرتبطا بالدول كفواعل مركزية ولكن غير وحيدة في النظام الدولي، إضافة إلى أن الجيوبوليتيكا غير مرتبطة بالصراع على الفضاءات الجغرافية بمفهومها الجغرافي التقليدي، بل يمكن كذلك إسقاط أهم أداة تحليل جيوبوليتيكية والمتمثلة في الصراع أو التنافس Rivalry، على فضاءات أخرى عابرة للحدود، ومن أبرزها الفضاء السيبراني.

2.1- مفهوم الأمن السيبراني وارتباطه بالجيوبوليتيكا.

بعد تحديد مفهوم الجيوبوليتيكا وبيان تطوره، ننتقل إلى الحديث عن مفهوم الأمن السيبراني، كمفهوم جديد في العلاقات الدولية، الجيوبوليتيكا، والدراسات الأمنية في آن.

1.2.1- الأمن السيبراني ومفهوم الأمن الموسع.

يمكن تعريف الفضاء السيبراني كبيئة افتراضية عالمية لأنظمة المعلومات التي يجري تداولها فيه. وهو عالم افتراضي بشكل كامل، غير أنه يتشابه مع عالمنا المادي في بعض الخصائص، ويتباين معه في خصائص أخرى من أبرزها خاصيته العابرة للحدود، إذ لا توجد حدود مادية أو افتراضية لما يتم تداوله داخل الفضاء السيبراني، ومن ثم فإن التهديدات الموجودة في هذا الفضاء هي تهديدات عابرة للحدود.⁵ ويمكن اعتبار الفضاء السيبراني أو الإلكتروني بمثابة فضاء خامس، يضاف إلى الفضاءات الأربعة التقليدية: الإقليم البري، الإقليم البحري، الإقليم الجوي، والفضاء الخارجي. وتتنافس القوى الكبرى على السيطرة وبسط النفوذ في هذا الفضاء مثل تنافسها على الفضاءات الأربعة سائلة الذكر.⁶ لذلك يمكن إسقاط العديد من المفاهيم المتداولة في العالم المادي، والمرتبطة بالأمن السيبراني والجيوبوليتيكا على الفضاء السيبراني كذلك. من أمثلة ذلك مفاهيم مثل: القوة السيبرانية، الإرهاب السيبراني، الجريمة السيبرانية، الصراع السيبراني، الدفاع السيبراني، الاستراتيجية السيبرانية، وجيوبوليتيكا الفضاء السيبراني، وغيرها.⁷

من ناحية أخرى، وفي الدراسات الأمنية تحديداً، شهدت العقود الأخيرة تصاعد الحديث في الوسط الأكاديمي عن توسيع مفهوم الأمن، وفك ارتباطه عن المفهوم التقليدي الذي عرف به لعقود طويلة، والمرتبطة خاصة بالجانب العسكري وغيرها من الجوانب ذات الطبيعة المادية المحضة. ولعل من أبرز الإسهامات التي ساعدت في مسار توسيع مفهوم الأمن؛ إسهامات مدرسة كوبنهاغن، وعلى رأسهم المنظر باري بوزان Barry Buzan، إذ في خضم سعيه -بمعنية باحثين آخرين في معهد كوبنهاغن لدراسات السلام Conpenhagen Peace Research Institution- لتغيير مفهوم الأمن وتوسيعه، بحيث لم يعد يشمل البعد العسكري فحسب، بل أبعاداً أخرى، كالبعد السياسي، الاقتصادي، المجتمعي، والبيئي.⁸

وعكس النظريات الأمنية التقليدية، فإن مفهوم الأمن الموسع حسب باري بوزان لا يتعلق بالدولة كفاعل مركزي في العلاقات الدولية، أي أن الدولة ليست هي الغاية الوحيدة للعمليات الهادفة لتحقيق الأمن، بل إن هناك فواعل أخرى تؤخذ بعين الاعتبار في ذلك، وعلى رأسها الفرد والنظام الدولي ككل. ولعل التهديدات السيبرانية -بهذا المعنى- من التهديدات التي تستهدف الدولة، والفرد، بل والنظام الدولي برمته، ويكون مصدرها الدولة، الأفراد، وفواعل أخرى كذلك.⁹

2.2.1- تطور مفهوم الأمن السيبراني.

بناء على ما تم ذكره سابقاً، فإن مفهوم الأمن السيبراني أصبح جانبا مركزيا ومهما من جوانب أمن الدول كفواعل مركزية، بل أمن الأفراد وفواعل أخرى كذلك. بالإضافة إلى ذلك، فإن تعريف الأمن السيبراني هو الآخر ليس محل إجماع من قبل الخبراء والدارسين، بل يمكن القول أن مفهومه يتغير باستمرار بتغير وتطور التفاعلات الدولية. فبداية من ظهور أول برنامج مضاد للفيروسات عام 1987، أين كان مفهوم الأمن السيبراني لا يخرج

عن إطار حماية أجهزة الكمبيوتر فحسب من الاختراقات؛ وصولاً إلى تطور شبكة الأنترنت وعالميتها مما أدى إلى ظهور تهديدات سيبرانية جديدة، كالجريمة المنظمة والإرهاب وغيرها، حتمت على الدول تغيير استراتيجياتها ومفاهيمها المتعلقة بالأمن السيبراني، بشكل جعل الدول تضع الأمن السيبراني في أولويات أجندها المتعلقة بالأمن القومي.^{10 11}

كما يمكن القول إنه هناك العديد من الفواعل التي تؤدي إلى تطور مفهوم الأمن السيبراني باستمرار، إذ يمكن اعتبار التفاعل بين ثلاثية: التكنولوجيا، السياسة، والعلم؛ بمثابة المحرك المركزي لمفهوم الأمن السيبراني. فالتكنولوجيا تشمل تطور التكنولوجيات الرقمية من جهة، وتطور الأحداث السيبرانية من جهة أخرى، كظهور تهديدات جديدة مثلاً لم تكن موجودة من قبل. أما السياسة فتشمل السياسة الدولية وارتباط الصراع السيبراني بها من ناحية، ومن ناحية أخرى التفاعلات السياسية الداخلية بين مختلف الأجهزة البيروقراطية وتصورها للتهديد السيبراني واستراتيجيات التعامل معه. أما العلم فيشمل تطور الدراسات الأمنية والسياسية ومختلف الاتجاهات النظرية المرتبطة بمفهوم الأمن السيبراني.¹²

وتتفاعل هذه المفاهيم الثلاثة مع بعضها البعض، فمثلاً تؤثر التطورات في مجال التكنولوجيا وظهور تهديدات سيبرانية جديدة على استراتيجيات الدول السيبرانية وسياساتها. كما ترسم سياسات الدول المتعلقة بالأمن السيبراني معالم التعامل مع الفضاء السيبراني والتحكم في مساراته وتفاعلاته. وتؤثر التطورات التكنولوجية على توسيع أكثر لمفهوم الأمن من الناحية النظرية، وهكذا.¹³

وتتقاطع هذه العوامل المؤثرة في تطور مفهوم الأمن السيبراني إلى حد ما مع طرح الباحثين باري بوزان وهانسن Hansen، في حديثهما عن أهم العوامل التي تساهم في تطور وتوسيع مفهوم الأمن، والمتمثلة حسبهما في: سياسات الدول العظمى، التكنولوجيا، الأحداث الكبرى، النقاشات الأكاديمية في حقل العلاقات الدولية والدراسات الأمنية، والمأسسة.¹⁴

وإذا أردنا تقديم تعريف تقني، شامل، وحديث لمفهوم الأمن السيبراني، فإن تعريف الباحث في معهد الدفاع الأسترالي فرانسيسكو شيليرو: Francesco Schilero قد يفي بالغرض:¹⁵

"الأمن السيبراني هو جمع وتنسيق الموارد بما في ذلك الأفراد والبنية التحتية والهياكل والعمليات لحماية الشبكات وأنظمة الكمبيوتر التي تدعم الإنترنت من الأحداث التي تهدد النزاهة وتتداخل مع حقوق الملكية، مما يؤدي إلى حد ما من الخسارة."¹⁶

ويعتبر هذا التعريف شاملاً إلى حد ما من الناحية التقنية، غير أنه يفتقد إلى الإشارة إلى مصادر التهديد مثلاً، وعلى رأسها الصراعات الجيوبوليتيكية، وعوامل أخرى كذلك. فمن الأمثلة البارزة على ذلك التدخل الروسي المزعوم في الانتخابات الأمريكية عام 2016، والهجوم السيبراني الكوري الشمالي على شركة سوني بيكتشرز Sony Pictures في عام 2014، والحرب السيبرانية غير المتوقعة بين الولايات المتحدة وإيران، وبين الولايات المتحدة والصين من جهة أخرى.¹⁷ أي أن الأمن السيبراني لا يتعلق بتطوير أنظمة أمن سيبراني فحسب، بل

يجب الأخذ بعين الاعتبار مشهد التهديدات العالمية من قبل الدول، ومن قبل الفواعل الأخرى كالشركات والأفراد كذلك، أي أن كل قرار يتم اتخاذه في الفضاء السيبراني له آثار أمنية، والعكس صحيح.¹⁸

2- الصراع الأمريكي الصيني في الفضاء السيبراني.

من أبرز تجليات الصراع على بسط النفوذ في الفضاء السيبراني على المستوى الدولي، الصراع السيبراني الجاري بين الولايات المتحدة الأمريكية والصين، الذي سنحاول تبين مظاهره، بداية من تحديد معالم استراتيجيتي الدولتين في الفضاء السيبراني أولاً، ثم وصولاً إلى تحليل بعض مظاهر الصراع بينهما في هذا الفضاء.

1.2- قراءة في الاستراتيجية الأمريكية للأمن السيبراني.

يعتبر كثير من الدارسين أن الولايات المتحدة الأمريكية لا زالت تلك الدولة الباحثة عن الهيمنة، بل أن نظرية الاستقرار الهيمني لا تزال تعتبر أهم نظرية جيوبوليتيكية مرتبطة ارتباطاً مباشراً بصانع القرار الأمريكي. ومضمون هذه النظرية أن الولايات المتحدة الأمريكية فقط من بإمكانها الحفاظ على الهيمنة الجيوبوليتيكية ومن ثم استقرار العالم.¹⁹

يمكن ملاحظة نوايا الهيمنة الأمريكية بداية بدراسة وثيقة إستراتيجية الأمن القومي، التي تعتبر من أهم الوثائق التي ينشرها صانع القرار الأمريكي، والتي تسمح لنا بالاطلاع على أهم معالم استراتيجية الأمن القومي للولايات المتحدة الأمريكية. ورجوعاً إلى آخر وثيقة تم نشرها في أكتوبر 2022، فإننا يمكن أن نستشف أمرين أساسيين فيما يتعلق بدراستنا:

1.1.2- الصين كأكبر مصدر تهديد للولايات المتحدة الأمريكية.

تعتبر القيادة الأمريكية الصين أكبر تهديد للأمن القومي الأمريكي بكل جوانبه: الاقتصادي، العسكري، الثقافي، وغيرها. إذ أن الصين التي تم ذكرها 14 مرة في وثيقة استراتيجية الأمن القومي الأمريكي، تقود عالماً موازياً من الأنظمة التسلطية التي تسعى إلى مراجعة النظام العالمي وأأسسه:

"إن نطاق الدول التي تدعم رؤيتنا لعالم حر ومنفتح ومزدهر وآمن واسع وقوي، تشمل حلفاءنا

الديمقراطيين في أوروبا ومنطقة المحيطين الهندي والهادئ، فضلاً عن الشركاء الديمقراطيين الرئيسيين في

جميع أنحاء العالم."²⁰

"إن التحدي الاستراتيجي الأكثر إلحاحاً الذي يواجه رؤيتنا هو من القوى التي تربط الحكم الاستبدادي بسياسة خارجية رجعية. إن سلوكهم هو الذي يشكل تحدياً للسلام والاستقرار الدوليين - وخاصة شن الحروب العدوانية أو الاستعداد لها، وتقويض العمليات السياسية الديمقراطية في البلدان الأخرى... ومن المؤسف أن روسيا وجمهورية الصين الشعبية تعلان ذلك."²¹

أي بناء على ما سبق، يمكن أن نستشف أن الصين تمثل أكبر تهديد مستدام وحقيقي لمصالح الولايات المتحدة الأمريكية، أي أن صانع القرار الأمريكي لا يرى في الصين ذلك المنافس على الأسواق، أو تلك الدولة

النامية الهادفة إلى رفع مستويات النمو، بل كدولة تسعى إلى تغيير قواعد لعبة المنظومة الدولية، وإعادة تشكيل النظام الدولي وفق قواعد قيمية ومادية مختلفة عن تلك التي تتبناها الولايات المتحدة الأمريكية.

2.1.2- الصين كأكبر مصدر تهديد سيبراني للولايات المتحدة الأمريكية.

من جهة أخرى، فإن الأمن السيبراني للولايات المتحدة الأمريكية مرتبط في ذهن صانع القرار بالتهديد القادم من روسيا والصين أساساً، إذ تم الإشارة إلى ذلك مباشرة في وثيقة الأمن القومي، بأن الشركات والاقتصاد الأمريكيين، بما فيها تلك الناشطة في قطاع التكنولوجيا وقطاعات أخرى، قد أصبحت هدفاً للهجمات السيبرانية القادمة من هذين البلدين تحديداً، إضافة إلى هجمات قادمة من فواعل غير الدول، كالجماعات الإرهابية، ومجموعات شبه مستقلة مدعومة من قبل دول معادية لمصالح الولايات المتحدة الأمريكية.²²

فبالإضافة إلى كوريا الشمالية، إيران، وروسيا؛ تعتبر الصين أكبر تهديد للقطاعين العام والخاص الأمريكيين، لأنها الدولة الوحيدة التي تهدف إلى إعادة هيكلة ورسم النظام العالمي، ومن الناحية السيبرانية، ترى الولايات المتحدة الأمريكية أن الصين تسعى إلى نشر ودعم ما تسميه بالتسلطية الرقمية، وذلك عن طريق ممارسة رقابة شديدة على هذا الفضاء، خاصة من ناحية المنصات التي تملكها، وكذلك تسعى الصين إلى سرقة الملكية الفكرية لعدد المنتجات الأمريكية الخالصة.²³

ومن بين أهم المجالات التي تشكل فيها الصين خطراً على الولايات المتحدة الأمريكية سيبرانياً:

أولاً: تمارس الصين -حسب الولايات المتحدة الأمريكية- الجوسسة السيبرانية، ونقوم بشكل ممنهج بسرقة معلومات حساسة ذات علاقة مباشرة بوزارة الدفاع الأمريكية مثلاً؛

ثانياً: تحاول الصين بأي شكل من الأشكال السيطرة على أهم شركات التكنولوجيا والأمن السيبراني ليس في الصين فحسب، بل خارج الصين كذلك بما فيها الولايات المتحدة الأمريكية؛

ثالثاً: تصدر الصين كذلك مقدراتها السيبرانية من برمجيات متطورة وغيرها إلى دول معادية للولايات المتحدة الأمريكية؛

رابعاً: تطور الصين بشكل مخيف قدراتها السيبرانية خاصة فيما يتعلق بأنظمة الأمن السيبراني ومكافحة الجوسسة، وتدعم العديد من الشركات التي تطور برمجيات خبيثة تستخدم في الهجمات السيبرانية.²⁴

وحسب وثيقة الأمن السيبراني المنشورة من قبل وزارة الدفاع الأمريكية عام 2023، فإن الصين تهدف من كل ما تم ذكره سابقاً إلى شن حروب سيبرانية مستقبلية تهدف إلى تقويض القطاع التكنولوجي الأمريكي، بالإضافة إلى القطاعين الاقتصادي والعسكري، بشكل يشكل أكبر تهديد سيبراني يواجه الولايات المتحدة الأمريكية.²⁵

2.2- الاستراتيجية الصينية للأمن السيبراني.

إذا كانت الصين تعتبر بمثابة أكبر تهديد لمصالح الولايات المتحدة الأمريكية، في الفضاء السيبراني خصوصاً، فقد يطرح تساؤل حول معالم الاستراتيجية الصينية بشكل عام، والسيبرانية بشكل خاص، وهل يمكن توصيفها بالهادفة إلى الهيمنة، كاستراتيجية الولايات المتحدة الأمريكية.

1.2.2- الصين، كقوة غير مهيمنة.

تدعي القيادة في الصين أنها دولة لن تسعى أبداً إلى الهيمنة أو التوسع أو أي نوع من البحث عن مجالات بسط النفوذ. علاوة على ذلك، تلتزم الحكومة الشيوعية الصينية بأن تكون لاعبا سلميا في كافة مناطق العالم. والصين الحديثة؛ منذ تأسيسها عام 1949، لم تبدأ حرباً أو تشن هجمات عدائية ضد الآخرين، بل تعطي بدلا من ذلك الأولوية للنمو الاقتصادي والازدهار على حساب الحرب والصراعات.²⁶

بالإضافة إلى ذلك، يزعم المسؤولون الصينيون أن العقيدة العسكرية للصين عقيدة دفاعية، ويمكن إظهار النقاط الرئيسية للاستراتيجية الصينية من خلال المبادئ التالية:

أولاً: ردع ومقاومة أي نوع من العدوان؛

ثانياً: حماية الأمن السياسي الوطني والسيادة الوطنية والوحدة والسلامة الإقليمية؛

ثالثاً: حماية حقوق الصين ومصالحها البحرية، والدفاع عن مصالح الصين في الخارج؛

رابعاً: دعم التنمية المستدامة للبلاد.²⁷

لذلك، ورغم الادعاءات الأمريكية بأن الصين لديها أهداف هيمنية خفية، فإن الصين دائماً ما تعتبر نفسها دولة من الدول النامية، ذات استراتيجية عسكرية دفاعية، لا تهدف بأي شكل من الأشكال إلى الهيمنة على مختلف الفضاءات، بما فيها الفضاء السيبراني.

2.2.2- التصور الصيني للأمن السيبراني.

أصبح الأمن السيبراني مفهوماً ذا أولوية قصوى بالنسبة للقيادة الصينية. في عام 2014، أعلن الرئيس الصيني شي جين بينغ أن الصين ستصبح "قوة إلكترونية"، وهو هدف يشمل العناصر الاقتصادية والتكنولوجية ومجالات أخرى. وسيكون الأمن السيبراني عاملاً تمكينياً رئيسياً لهذه الأجندة الطموحة.²⁸

وجاء الإعلان عن هذا الهدف الطموح، عاماً بعد إعلان مبادرة "حزام واحد طريق واحد" 'One Belt One Road' (OBOR) أو مبادرة الحزام والطريق التي أطلقها الرئيس الصيني شي جين بينغ Xi Jinping في عام 2013. وعلى الرغم من الطبيعة الاقتصادية لهذه المبادرة، فيمكن القول إن الصين تسعى وراءها إلى تعزيز موقفها وأن تصبح محددًا للتفاعلات الجيوسياسية في عديد مناطق العالم. يمكن اعتباره ذلك نوعاً من "التوازن الناعم"، وهو شكل غير عسكري من التوازن يهدف إلى فرض تكاليف إضافية على الدولة المهيمنة التي، بسبب رجحان قوتها، لا يمكن معارضتها بطريقة صلبة تقليدية.²⁹

وبحلول نهاية عام 2017، نشرت بكين استراتيجية وطنية للأمن السيبراني، واستراتيجية تعاون سيبراني دولية، وقانون الأمن السيبراني، وأصبحت هذه الوثائق بمثابة حجر الزاوية التي توضح الإطار التنظيمي للفضاء السيبراني في الصين، وتوضح معالم الأمن السيبراني بالنسبة لكل الفواعل التي تنشط في هذا الإطار.³⁰ وبالإطلاع على استراتيجية الأمن السيبراني الصينية المنشورة سنة 2017 من قبل إدارة الفضاء السيبراني في الصين، فإنه يمكن استنتاج النقاط الآتية:

أولاً: تؤكد الصين أن الفضاء السيبراني مثله مثل الفضاءات الأخرى، وبأن "السيادة في الفضاء السيبراني هي جانب مهم من جوانب السيادة الفعلية للصين"؛

ثانياً: الصين لا تسعى أبداً إلى الهيمنة على الفضاء السيبراني، وفي المقابل سوف تقوم الصين بردع كل محاولة لتقويض أمنها في الفضاء السيبراني؛

ثالثاً: تبني استراتيجية للأمن السيبراني من قبل الصين، لا يعني بأي شكل من الأشكال إغلاق السوق الصينية أمام الشركات والفواعل الأجنبية، بل مرافقة الفواعل الصينية الداخلية والخارجية في الاستراتيجيات والسياسات التي تسعى الصين إلى تحقيقها.³¹

أي يمكن القول أن أهداف الصين في ميدان الأمن السيبراني، لا تختلف عن أهدافها في ما يتعلق باستراتيجيتها للأمن القومي. أي أن الصين تسعى إلى تحقيق أهدافها الاقتصادية وتوسيع مجالات قوتها الناعمة عن طريق استخدام الفضاء السيبراني، وهذا المثال، إضافة إلى أمثلة أخرى، من أبرز تجليات الصراع بين الصين والولايات المتحدة الأمريكية سيبرانياً، والذي سندرسه في المطلب اللاحق.

3.2- بعض تجليات الصراع الأمريكي الصيني في الفضاء السيبراني

تعتقد الإدارة الأمريكية أن لدى الصين قدرات هائلة مرتبطة بالفضاء السيبراني، خاصة من حيث الجوسسة والقرصنة. إذ حسب مدير مكتب التحقيقات الفيدرالي الأمريكي كريستيان واي Chris Wray، فإن قدرات الصين السيبرانية تفوق كل الدول العظمى مجتمعة. وحسبه "إذا ركز كل واحد من عملاء ومحلي الاستخبارات في مكتب التحقيقات الفيدرالي على الصين حصرياً، فسيظل عدد القرصنة الصينيين يفوق عدد موظفينا السيبرانيين بنسبة 50 مقابل 1 على الأقل".³²

وتدعي الولايات المتحدة الأمريكية بمعية حلفائها أن أول وحدة مسؤولة عن الهجمات السيبرانية وحروب المعلومات القادمة من الصين تتمثل في قسم أنظمة شبكة قوة الدعم الاستراتيجي التابع لوزارة الدفاع الصينية، مع مجموعة مهام تشمل الحرب النفسية والإلكترونية، تشويه، سرقة المعلومات ونشر الأخبار الكاذبة والإشاعات. فعلى سبيل المثال، تشير التقديرات إلى أن تايوان -التي تعتبر أبرز حليف للولايات المتحدة الأمريكية في جوار الصين- تتعرض لهجمات من هذه الشاكلة تصل إلى 2400 قطعة من المعلومات المضللة يومياً. وتهدف هذه الحرب إلى الإطاحة؛ أو على الأقل زعزعة أسس النظام الحاكم في تايوان الموالي للولايات المتحدة الأمريكية حسب السلطات الصينية.³³

ومنذ عام 2000، وفي دراسة محينة لمعهد الدراسات الاستراتيجية والدولية الأمريكي Center for Strategic and International Studies، يمكن إحصاء حوالي 224 حالة تجسس صينية موجهة ضد الولايات المتحدة الأمريكية، وحوالي 1200 قضية سرقة ملكية فكرية رفعتها شركات أمريكية ضد كيانات صينية داخل الولايات المتحدة أو في الصين.³⁴

وقدمت نفس الدراسة إحصائيات متعددة، توضح توزيع مصادر الهجمات الصينية:

49% من الهجمات مصدرها المباشر الجيش الصيني أو موظفون في الحكومة الصينية؛

41% من القرصنة كانوا مواطنين صينيين عاديين، يتعاونون بطريقة مباشرة أو غير مباشرة مع الحكومة

الصينية؛

10% كانوا أشخاصا غير صينيين (عادة أشخاص أمريكيون تم تجنيدهم من قبل المسؤولين الصينيين).³⁵

أما أهداف هذه الهجمات السيبرانية فيمكن ذكر بعضها فيما يأتي:

29% من الحوادث سعت للحصول على التكنولوجيا العسكرية الأمريكية؛

54% من الحوادث سعت للحصول على تقنيات تجارية ومعلومات اقتصادية أمريكية.³⁶

سعت 17% من الحوادث إلى الحصول على معلومات عن الوكالات المدنية أو السياسيين الأمريكيين.

ومن أبرز هذه الهجمات التي تهدف إلى تقويض البنية التحتية الأمريكية، واستخدام الجوسسة من أجل

الحصول على معلومات حساسة وسرية في ميادين الدفاع والاقتصاد خصوصا؛ هجمات أورورا Aurora

السيبرانية التي شنتها مجموعات مرتبطة بالحكومة الصينية -حسب الولايات المتحدة الأمريكية- من أولى

الهجمات التي استهدفت أكثر من 100 شركة تكنولوجية أمريكية منها شركات Yahoo, Adobe, Morgan

Stanley, Google، تدخل بعضها في إطار سلسلة إمداد وزارة الدفاع الأمريكية. واتهمت الولايات المتحدة

مجموعات Sneaky Panda. The Elderwood Gang. The Beijing Group، بقيادة عملية القرصنة،

والأخطر حسب الولايات المتحدة أن هذه الجماعات تنشط بصفة غير رسمية، أي لا تتبع وزارة الدفاع الصينية

مباشرة، بل تتكون من حوالي 50000 إلى 100000 هكر موالى للحكومة، ينشطون بطريقة شبه مستقلة، في

شكل جديد ومبتكر من أشكال الحروب السيبرانية.^{37 38}

أما بالنسبة للولايات المتحدة الأمريكية، فإنها لا تركز على ترتيب هجمات سيبرانية ضد المصالح الصينية

بالأساس، بل الأهم بالنسبة لها هو حرمان الصين من أن تصبح قوة تكنولوجية، خاصة في قطاعي الرقائق

الإلكترونية وأشباه الموصلات، والذكاء الاصطناعي. فالولايات المتحدة الأمريكية تفرض عقوبات على أكثر

من 2000 شركة وكيان صينيين لمكافحة التجسس الصناعي/الاقتصادي الصيني من جهة، ومن جهة أخرى

منع الصين من الحصول على التكنولوجيات المتطورة في ميادين الذكاء الاصطناعي، الصناعات العسكرية،

والرقائق الإلكترونية. لذلك اعتمدت الولايات المتحدة قانون "الرقائق والعلوم" عام 2022 بميزانية تقرب من 53

مليار دولار، يحظر على الشركات الأمريكية المدعمة من الحكومة التوسع داخل الصين. وفي 7 أكتوبر

2022، أصدرت الولايات المتحدة حزمة قيود جديدة على صادرات التكنولوجيا إلى الصين شملت أنواعاً محددة من الرقائق المتقدمة، ومعدات تصنيعها، والمركبات الكيميائية الخاصة بتصميمها وتصنيعها. تعرقل حزمة القيود هذه قدرة الصين على بناء القوة الحاسوبية المطلوبة لتطوير قدراتها في مجال الذكاء الاصطناعي والفضاء السيبراني ككل.³⁹

الخاتمة:

حاول الباحث في هذه الدراسة دراسة الإشكالية التي تتعلق بمحاولة تحديد العلاقة بين مفهومي الجيوبوليتيكا والأمن السيبراني، وما هي علاقات التلاقي والتأثير المتبادل بين المفهومين. وهدف من وراء ذلك خصوصاً إلى دراسة درجة امتداد المفاهيم الجيوبوليتيكية التقليدية لتصبح كأدوات تحليل لما يحدث من صراع سيبراني، خاصة بين الولايات المتحدة الأمريكية والصين كدراسة حالة. وما أبرز مظاهر هذا الصراع السيبراني الصيني الأمريكي، بناء على استراتيجيتي الدولتين في هذا الفضاء؟

ولمعالجة الإشكالية سابقة الذكر قام الباحث أولاً بتسليط الضوء على العلاقة بين ثنائية الجيوبوليتيكا والأمن السيبراني، بداية من الحديث عن تطور مفهوم الجيوبوليتيكا، وصولاً إلى محاولة تحديد مفهوم الأمن السيبراني ومدى ارتباطه بأدبيات الجيوبوليتيكا. لينتقل في القسم الثاني من الدراسة إلى دراسة حالة الصراع الجيوبوليتيكي الصيني الأمريكي في الفضاء السيبراني، بذكر بعض تجلياته وأمثله، ولكن قبل ذلك محاولة فهم استراتيجيتي الولايات المتحدة الأمريكية والصين للأمن القومي، واستراتيجيتي الدولتين للأمن السيبراني كذلك.

وللإجابة على الإشكالية سابقة الذكر، خلص الباحث إلى النتائج البحثية الآتية:

أن مفهوم الجيوبوليتيكا قد تطور ليشمل الصراع في فضاءات أخرى غير الفضاء الجغرافي التقليدي، أي أن مفهوم الجيوبوليتيكا لم يعد متعلقاً بالجغرافية فحسب، بل يتعداه إلى فضاءات افتراضية أخرى. أن الفضاء السيبراني من أبرز مجالات الصراع الجيوبوليتيكي، وأن الجيوبوليتيكا بمفهومها المعاصر تشمل الفضاء السيبراني بكافة المظاهر الصراعية التي نجدها فيه.

أن الأمن السيبراني من مجالات مفهوم الأمن الموسع، ولا يمكن حسب الباحث الاكتفاء بالتقسيم التقليدي لمفهوم الأمن الموسع كما قدمه باري بوزان، بل إن الدراسات الحديثة توفر تقسيمات أوسع وتشمل الأمن في الفضاء السيبراني.

لا يمكن فهم الصراع السيبراني الصيني الأمريكي، دون فهم استراتيجيتي الدولتين للأمن القومي، إذ أن الاستراتيجيتين توفر فهم المعالم العامة التي تركز عليها كل دولة في الفضاء السيبراني، وما هي أهداف الدولة، ما هي المخاطر ومصادر التهديد، وكيف ستتعامل الدولة مع هذه التهديدات.

أن الصين -عكس مبادئها المعلنة في استراتيجياتها الأمنية والسيبرانية- تمارس حرباً سيبرانية ذات طابع هجومي في بعض أمثلتها على الولايات المتحدة الأمريكية، وتستهدف الصين قطاعات محددة في هذه الهجمات، خاصة القطاع الدفاعي، وبعض القطاعات التي تعاني فيها الصين من تأخر مقارنة بالولايات المتحدة الأمريكية. تعتبر الولايات المتحدة الأمريكية الصين، كأكبر تهديد سيبراني وجيوبوليتيكي، ويتضح بشكل جلي من خلال ما سبق أن الولايات المتحدة الأمريكية لها استراتيجية ذات طابع هيمني، بما فيها استراتيجيتها في الفضاء السيبراني. وتعمل الولايات المتحدة الأمريكية في هذا الفضاء أساساً على منع الصين من الحصول على التكنولوجيا في بعض القطاعات الحساسة التي تهم الصين، كالرقائق الإلكترونية، الذكاء الاصطناعي، قطاع الدفاع والصناعات العسكرية، وغيرها.

وفي الأخير، مثل هذه الدراسات، تستدعي دراسات أخرى عابرة للتخصصات، باعتبار أن الأمن السيبراني له علاقة بالعديد من الميادين البحثية الأخرى، كالدراسات الأمنية، الاقتصاد والجيواقتصاد، دراسات الكمبيوتر، وغيرها، من أجل فهم أكبر لهذا الموضوع، وتبني استراتيجيات توفر فهم وإدراك واضحاً للتهديدات السيبرانية، وبشكل يجعل من هذا الموضوع كذلك موضوعاً خصباً وحديثاً نسبياً في الميدان الأكاديمي، خاصة مع التكنولوجيات الحديثة الآخذة في التطور في السنوات الأخيرة، والتي اقتحمت المجال السيبراني ومجالات أخرى، كالذكاء الاصطناعي، أنترنت الأشياء، البلوكتشين، وغيرها.

الهوامش:

¹ Merje Kuus, **Critical Geopolitics**, Published in print: 01 March 2010, Published online: 30 November 2017, <https://doi.org/10.1093/acrefore/9780190846626.013.137>

² Yves Lacoste, **Définir la géopolitique**, 9 décembre 2019, <https://www.vie-publique.fr/parole-dexpert/277002-definir-la-geopolitique-par-yves-lacoste#:~:text=de%20la%20g%C3%A9opolitique-.Qu'est%2Dce%20que%20la%20g%C3%A9opolitique%20%3F,la%20souverainet%C3%A9%20d'un%20territoire.>

³ Leonhardt van Efferink, **The Definition of Geopolitics – The Classical, French and Critical Traditions**, 05/01/2009, https://exploringgeopolitics.org/publication_efferink_van_leonhardt_the_definition_of_geopolitics_classical_french_critical/

⁴ ألكسندر دوغين، **أسس الجيوبوليتيكا**، تعريب وتقديم: عماد حاتم، بيروت: دار الكتاب الجديد المتحدة، 2004. ص. 59.

⁵ تغريد معين حسن المشهدي، **الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة**، الكوفة: مجلة البحوث الجغرافية، العدد 30، 2019. ص. 241.

⁶ ايهاب خليفة، **القوة الإلكترونية وابعاد التحول في خصائص القوة**، مصر: مكتبة الإسكندرية، 2014. ص. 7، 8.

⁷ تغريد معين حسن المشهدي، مرجع سابق، ص. 242.

⁸ عمار بالة، إسهامات مدرسة كوبنهاغن في توسيع مفهوم الأمن، من الأمن العسكري إلى الأمن المجتمعي، مجلة الحقوق والحريات، المجلد 10، العدد 02، 2022. ص 1161-1167.

⁹ نوال بومليك، البعد الإقليمي للأزمة الليبية وفق منظور مدرسة كوبنهاغن، مجلة العلوم القانونية والسياسية، المجلد 12، العدد 02، سبتمبر 2021. ص. 656.

¹⁰ Davies, Vikki, **The history of cybersecurity**, October 04, 2021. <https://cybermagazine.com/cyber-security/history-cybersecurity>

¹¹ Myriam Dunn Cavelty & Andreas Wenger, **Cyber security meets security politics: Complex technology, fragmented politics, and networked science**, Contemporary Security Policy, VOL. 41, NO. 1, 5–32 2020. <https://doi.org/10.1080/13523260.2019.1678855> p. 7.

¹² Ibid. pp. 9, 10.

¹³ Ibid. pp. 9, 10.

¹⁴ Ibid. pp. 8, 9.

¹⁵ قدم الباحث تعريفه هذا، بعد دراسة مستفيضة تناولت العديد من التعريفات المختلفة لمفهوم الأمن السيبراني بالنقد والتحليل، ليخلص في الأخير إلى هذا التعريف الإجرائي. مع الإشارة أن هذا التعريف يفتقد إلى الإشارة إلى الأمن السيبراني بوصفه جانباً من جوانب الأمن القومي للدول من جهة، ومن جهة أخرى الفواعل الأخرى التي تتعرض كذلك للتهديدات السيبرانية.

¹⁶ Francesco Schiliro, **Towards a Contemporary Definition of Cybersecurity**, 21 November 2022. P. 11. <https://arxiv.org/ftp/arxiv/papers/2302/2302.02274.pdf>

¹⁷ Tom Donovan, **The Geopolitics of Cybersecurity: A New Frontier in International Relations**, July 8, 2023, <https://www.thefinalhop.com/the-geopolitics-of-cybersecurity-a-new-frontier-in-international-relations/>

¹⁸ Paul Proctor, **How Geopolitics Impacts the Cyber-Threat Landscape**, June 10, 2022. <https://www.gartner.com/en/newsroom/press-releases/2022-06-10-how-geopolitics-impacts-the-cyber-threat-landscape>

¹⁹ Jeffrey D. Sachs, **The New Geopolitics**, Center for International Relations and Sustainable Development, Serbia, <https://www.cirsd.org/en/horizons/horizons-winter-2023--issue-no22/the-new-geopolitics>

²⁰ The White House, **National Security Strategy**, Washington: October 2022. P. 8.

²¹ Ibid. S.P.

²² Ibid. P. 34.

²³ The White House, **National Cybersecurity Strategy**, Washington, March 2023. P. 3.

²⁴ U.S. Department of Defense, **Cyber strategy of the DOD**, 2023. P. 4.

²⁵ Ibid. P. 4.

²⁶ Ministry of National Defense of China, Defense Policy: **China's Defensive National Defense Policy in the New Era**, <http://eng.mod.gov.cn>

²⁷ Ibid.

²⁸ Rogier Creemers, **The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy**, Journal of Contemporary China, Published online: 30 Mar 2023. <https://doi.org/10.1080/10670564.2023.2196508>

²⁹ Raviprasad Narayanan, **One Belt, One Road: Changing Asian Geo-Politics and India**, Institute for Security and Development Policy, Stockholm, November, 2022. P8.

³⁰ Rogier Creemers, Op.cit.

³¹ The State Council, The People's Republic of China, **China announces cybersecurity strategy**, China: Xinhua, Updated: Dec 27, 2016 9:12 PM, https://english.www.gov.cn/state_council/ministries/2016/12/27/content_281475526667672.htm

³² Raphael Satter, **FBI chief says China has bigger hacking program than the competition combined**, Reuters, September 18, 2023 10:05 PM GMT+1, <https://www.reuters.com/world/fbi-chief-says-china-has-bigger-hacking-program-than-competition-combined-2023-09-18/>

³³ Matthew Becerra, **The Battle for Reality: Chinese Disinformation in Taiwan**, August 24, 2022. <https://www.geopoliticalmonitor.com/the-battle-for-reality-chinese-disinformation-in-taiwan/>

³⁴ Center for Strategic and International Studies, **Survey of Chinese Espionage in the United States Since 2000**, Washington: March 2023. <https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000>

³⁵ Ibid.

³⁶ Ibid.

³⁷ Mara Hvistendahl, **China's Hacker Army**, MARCH 3, 2010, 9:58 PM. <https://foreignpolicy.com/2010/03/03/chinas-hacker-army/>

³⁸ Mark Clayton, **Stealing US business secrets: Experts ID two huge cyber 'gangs' in China**, September 14, 2012. <https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China>

³⁹ مركز الإمارات للسياسات، الاجتثاث والانتقام: حرب الرقائيق الإلكترونية بين الصين والولايات المتحدة، أبو ظبي: 19 سبتمبر 2023. <https://epc.ae/ar/details/featured/alijitithath-waliantiqam-harb-alraqayiq-al-ilikturunia-bayn-alsiyn-walwilayat-almutahida>