

قائمة المصادر والمراجع :

- 1- إدزارد ، د ؛ بوب، م ه ؛ رولينغ ، ف : قاموس الآلهة والأساطير ، تعريب : محمد وحيد خياطة ، دار الشرق العربي ، بيروت، لبنان و حلب، سورية ، د . ت .
- 2 - اسماعيل ، عز الدين : الشعر العربي المعاصر قضاياها و ظواهره الفنية و المعنوية، دار الفكر العربي ، ط 3، د.ت.
- 3 - باقر ، طه ، مقدمة في أدب العراق القديم ، كلية الآداب جامعة بغداد - دار الحرية للطباعة ، بغداد ، 1976 م .
- 4 - بلحاج ، كاملي : أثر التراث الشعبي في تشكيل القصيدة العربية المعاصرة ، منشورات اتحاد الكتاب العرب ، دمشق ، 2004 م .
- 5 - الجبوري ، كامل سلمان : معجم الأدباء من العصر الجاهلي حتى سنة 2002 م ، دار الكتب العلمية ، بيروت لبنان ، ط1، 2002 م .
- 6 - داود ، أنس : الأسطورة في الشعر العربي الحديث ، مكتبة عين شمس ، دار الجيل للطباعة ، الفجالة ، 1975 م .
- 7 - السواح ، فراس، الأسطورة والمعنى ، دراسة في الميثولوجيا و الديانات المشرقية ، دار علاء الدين للنشر و التوزيع و الترجمة ، ط 2 ، 2001 م .
- 8 - السواح ، فراس : لغز عشتار الألوهة المؤنثة و أصل الدين و الأسطورة ، دار علاء الدين ، دمشق سورية ، ط 8 ، 2002 م .
- 9 - السواح ، فراس : مغامرة العقل الأولى - دراسة في الأسطورة سوريا و بلاد الرافدين : ، دار الكلمة ، بيروت لبنان ، د . ت .
- 10 - علي ، فاضل عبد الواحد : عشتار و مأساة تمّوز ، الأهالي للطباعة والنشر والتوزيع ، دمشق سورية ، ط1، 1999 م .
- 11 - فضل ، صلاح : أساليب الشعرية المعاصرة ، دار الآداب ، بيروت ، ط 1 ، 1995 م .
- 12 - مطلق ، شاكر : ديوان تجليات النور البرّي : ، دار الذاكرة ، حمص سورية ، ط1 ، 1997م.
- 13 - مطلق ، شاكر : ديوان تجليات عشتار : ، دار الكتاب للنشر ، حمص سورية ، ط1 ، 1988م.
- 14 - مطلق ، شاكر : ديوان ذاكرة القصب : ، دار الذاكرة ، حمص سورية ، ط1 ، 1993 م .
- 15 - مطلق ، شاكر : ديوان معلقة كلكاش على أبواب أوروك :. دار الإرشاد للنشر ، حمص سورية ، ط 1 1984 م .

العقيدة الأمنية للصين في مجال الفضاء السيبراني

أ.د. لؤي صيوح* د. رامي لايقة** رمضان الهوشي***

(الإيداع: 27 تشرين الثاني 2024، القبول: 5 شباط 2025)

الملخص:

تعد العقيدة الأمنية من الركائز الهامة في السياسة العامة للدولة ، وخاصةً في مجال الفضاء السيبراني حيث إن العلاقات الدولية تطورت من حيث الفواعل والمواضيع والأدوات المستخدمة في إدارة مختلف التفاعلات، وفي ظل القفزة النوعية التي تزامنت مع ثورة التكنولوجيا الرقمية والتي اقتحمت شتى مجالات الحياة الإنسانية والتفاعلات الدولية، ظهر نوع جديد من التهديدات والمتمثل في التهديدات السيبرانية، ومع بروز القوة السيبرانية كركيزة أساسية في بناء الأمن القومي، سارعت الدول لتشكيل الهيئات والمؤسسات المدنية والعسكرية ، وسن التشريعات القانونية ووضع إستراتيجية خاصة لمواجهة التهديدات السيبرانية الحالية والمستقبلية والدفاع عن أمنها، إضافة إلى العمل على المستويين الإقليمي والدولي من أجل فضاء سيبراني آمن وسلمي، يهدف البحث إلى دراسة أهم المفاهيم في الفضاء السيبراني (cyber space)، ودراسة العقيدة الأمنية للصين في مجال الفضاء السيبراني، ودور التقدم التكنولوجي السيبراني في تطوير هذه العقيدة على المستوى الوطني والدولي. يعتمد البحث على المنهج الوصفي التحليلي، توصلت الدراسة إلى نتائج أهمها: تنوع صور التهديدات السيبرانية من (تجسس سيبراني، قرصنة سيبرانية، هجمات سيبرانية، إرهاب سيبراني). ومن أهم التوصيات: ضرورة تنمية القدرات السيبرانية ودمجها في مختلف المجالات، وضرورة المراقبة الكاملة للتطور التقني والتكنولوجي.

الكلمات المفتاحية: السيبرانية، الفضاء السيبراني، القوة السيبرانية، الهجمات السيبرانية، الأمن السيبراني، التهديدات الأمنية.

* أستاذ في قسم الاقتصاد والتخطيط، اختصاص علاقات دولية، كلية الاقتصاد، جامعة تشرين، اللاذقية، سورية.
** أستاذ مساعد في قسم الاقتصاد والتخطيط، اختصاص علاقات دولية، كلية الاقتصاد، جامعة تشرين، اللاذقية، سورية.
*** طالب دكتوراه في قسم الاقتصاد والتخطيط، اختصاص علاقات دولية، كلية الاقتصاد، جامعة تشرين، اللاذقية، سورية.

China's Cybersecurity Doctrine

Prof. Dr. Louay Sayyounh* Dr. Rami Laika** Ramadan Al Houshi***

(Received: 27 November 2024, Accepted: 5 February 2025)

Abstract:

Security doctrine is one of the important pillars of the state's public policy, especially in the field of cyberspace, as international relations have developed in terms of actors, topics and tools used to manage various interactions. In light of the qualitative leap that coincided with the digital technology revolution, which has invaded various areas of human life and international interactions, a new type of threat has emerged, namely cyber threats. With the emergence of cyber power as a fundamental pillar in building national security, countries have rushed to form civil and military bodies and institutions, enact legal legislation and develop a special strategy to confront current and future cyber threats and defend their security, in addition to working at the regional and international levels for a safe and peaceful cyberspace. The research aims to study the most important concepts in cyberspace, study China's security doctrine in the field of cyberspace, and the role of cyber technological progress in developing this doctrine at the national and international levels. The research is based on the descriptive analytical approach. The study reached the most important results: the diversity of cyber threats from (cyber espionage, cyber hacking, cyber attacks, cyber terrorism). The most important recommendations include: the necessity of developing cyber capabilities and integrating them into various fields, and the necessity of fully keeping pace with technical and technological development.

Keywords: cyber, cyberspace, cyber force, cyber-attacks, cyber security, security threats.

* Professor in the Department of Economics and Planning, specializing in International Relations, Faculty of Economics, Tishreen University, Latakia, Syria.

** Assistant Professor in the Department of Economics and Planning, specializing in International Relations, Faculty of Economics, Tishreen University, Latakia, Syria.

*** PhD student in the Department of Economics and Planning, specializing in International Relations, Faculty of Economics, Tishreen University, Latakia, Syria.

المقدمة:

أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، حيث تزداد المخاطر السيبرانية في غالب الأحيان كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الإنترنت، وأجهزة الحاسوب بأشكال متعددة مثل: الهجمات والقرصنة السيبرانية، باعتبارها الجرائم الأكثر شيوعاً في العالم الرقمي.

يعد الفضاء السيبراني مجال جديد وبيئة جديدة مؤثرة في حركة التفاعلات والتحويلات في العلاقات الدولية، والذي أصبح جزءاً أصيلاً من عمل الدول ومن بنيتها التحتية.

حيث إن الدول تستخدم القدرات التي يوفرها هذا الفضاء، من أجل الأمن والقوة العسكرية، نظراً لأن زيادة الاعتماد على الفضاء السيبراني، في جميع القطاعات العامة والخاصة وكذلك العمليات الحكومية.

وتزداد العلاقة بين الأمن السيبراني والأمن القومي، كلما ازداد الاعتماد على الوسائل التي يوفرها الفضاء السيبراني، خاصة مع التسارع في تبني الحكومات الإلكترونية والمدن الذكية في العديد من الدول.

حيث توجهت الصين إلى وضع إستراتيجية دفاعية شاملة من أجل ضمان الأمن السيبراني، لأن الأمن السيبراني يعد ضمن الأمن الوطني الشامل، فأجهزة الأمن السيبرانية الصينية تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي إلى خلق تهديدات ليست بالسهلة، نظراً للتهديدات السيبرانية المتعاقبة عليها فما كان عليها إلا إتباع طرق للهجوم أو الدفاع، وذلك بوضع إستراتيجيات أمنية جديدة، لحماية فضاءها السيبراني وفقاً لقدراتها السيبرانية.

مشكلة البحث:

يؤدي التطور والتقدم التكنولوجي، إلى تغير وظهور أشكال جديد من التهديدات المتمثلة بالتهديدات السيبرانية، الأمر الذي استدعى تنمية القدرات التكنولوجية والسيبرانية في وضع استراتيجيات في مجال الفضاء السيبراني.

استناداً لما سبق يمكن صياغة السؤال الرئيسي: كيف أثر الفضاء السيبراني في تطور العقيدة الأمنية للصين؟

يتفرع عن السؤال الرئيسي عدة أسئلة فرعية:

1- ما هو مفهوم السيبرانية؟

2- ماهي أهم المفاهيم في الفضاء السيبراني؟

3- ماهي أهم ركائز العقيدة الأمنية الصينية في مجال الفضاء السيبراني؟

أهمية البحث:

تكمن أهمية البحث في أهمية علمية كونه يناقش موضوع حديث على الساحة الدولية، وهو موضوع القوة السيبرانية وتطور العقيدة الأمنية بما يتناسب مع الشكل الجديد للقوة، وأهمية هذا الموضوع على الساحة الدولية من خلال استخدام القوة في مجال الحرب السيبرانية، إضافة إلى دراسة المفاهيم الأساسية المرتبطة بالفضاء السيبراني، وأهمية عملية تتمثل في تزايد تأثير التهديدات والهجمات السيبرانية على الأمن القومي للدول، وخاصة الصين التي تعد من الدول المتطورة في المجال التقني والتكنولوجي، ومن الدول الرائدة في مجال القوة السيبرانية وتوظيفها في مختلف المجالات.

أهداف البحث: يهدف البحث إلى:

1- زيادة الوعي حول أهمية القوة السيبرانية في ظل التحول في أشكال القوة على الساحة الدولية من القوة الصلبة إلى القوة السيبرانية.

2- دراسة المفاهيم الأساسية النظرية المرتبطة بالفضاء السيبراني مثل (السيبرانية، القوة السيبرانية، الأمن السيبراني).

3- دراسة العقيدة الأمنية للصين في مجال الفضاء السيبراني، ودور التقدم التكنولوجي السيبراني في تطوير هذه العقيدة على المستوى الوطني والدولي.

فرضيات البحث:

- 1- هنالك علاقة ذات دلالة معنوية بين التقدم الذي حققته الصين في المجال التقني ومواجهتها للهجمات السيبرانية.
- 2- هنالك علاقة ذات دلالة معنوية بين الفضاء السيبراني والتحول في مفهوم القوة، وظهور القوة السيبرانية.

منهج البحث:

المنهج الوصفي التحليلي: يقوم المنهج الوصفي التحليلي، على وصف وتحليل ماهية القوة السيبرانية بتحليل واقعي، والتعرف على الإستراتيجية الصينية في مجال السيبراني، للوصول إلى النتائج واقتراح التوصيات.

الدراسات السابقة:

1-دراسة (صالح، 2021) بعنوان: القوة الذكية التنافس العالمي على قوة الفضاء الإلكتروني والقدرات السيبرانية، مقال علمي محكم منشور في مجلة دفا تر السياسة و القانون ، جامعة عباس لغرور خنشلة، الجزائر ،هدفت هذه الدراسة إلى تسليط الضوء على تأثير تكنولوجيا الاتصالات والمعلومات، في التفاعل بين الفواعل الأساسية في السياسة الدولية (الدول)، وتأثيره في تحول القوة ، وهذا أدى إلى ظهور مبادئ جديدة في النظام الدولي (الفضاء السيبراني) ، وأشكال جديدة من أشكال القوة (القوة السيبرانية)، ونوع جديد من التهديدات (التهديدات السيبرانية) ، واستخدمت الدراسة المنهج الوصفي التحليلي.

توصلت الدراسة إلى أن ثورة المعلومات والاعتماد على التقنيات المتطورة ساهم في تغير العديد من المفاهيم التقليدية المتعلقة بالعلاقات الدولية، بدءاً من وحدات التفاعل في العلاقات الدولية، حيث لم تعد الدولة الفاعل الوحيد في ظل قدرات فواعل أخرى، وسعي الدول إلى تنمية القدرات السيبرانية، ووضع إستراتيجيات لمواجهة التهديدات السيبرانية في المستقبل.

2-دراسة (سيدهم، 2020) بعنوان: الأمن الفضائي السيبراني التحديات والحلول، بحث علمي محكم منشور في المجلة الجزائرية للأمن الإنساني، جامعة سطيف، الجزائر .

من خلال هذه الدراسة تم تسليط الضوء على أهم التحديات التي تواجه الأمن السيبراني، وإيجاد الحلول المناسبة التي يمكن استخدامها للوقاية ولمواجهة الأخطار التي تهدد الأمن السيبراني.

اعتمدت الدراسة على المنهج الوصفي التحليلي لتحليل ودراسة الأخطار التي تواجه الأمن السيبراني وإيجاد الحلول المناسبة.

توصلت الدراسة إلى أن الجرائم السيبرانية ذات طبيعة خاصة وهذا يفرض وجود جهاز تحقيق ذو كفاءة وخبرة، إضافة إلى ضرورة التعاون القضائي وتسليم المجرمين مرتكبي الجرائم السيبرانية.

3-دراسة (رشاد، 2022) بعنوان: التهديدات الهجينة في العلاقات الدولية (السيبرانية والذكاء الاصطناعي)، بحث علمي منشور في مجلة وادي النيل للدراسات والبحوث الإنسانية، جامعة 6 أكتوبر .

هدفت الدراسة إلى دراسة التهديدات الأمنية، في العلاقات الدولية طبيعتها وخصائصها، إضافة إلى مفهوم السيبرانية والذكاء الاصطناعي، وانعكاساتها على العلاقات الدولية، واعتمدت الدراسة على المنهج الوصفي التحليلي.

توصلت الدراسة إلى نتائج أهمها: إن التقدم التكنولوجي والتقنيات الحديثة فرض وسائل جديدة على العمليات العسكرية وبالتالي زيادة التهديدات على الأمن القومي للدول.

4-دراسة (الجليل، 2023) بعنوان: استراتيجيات الأمن السيبراني كتحدى للتحول الرقمي بالمنظمات الحكومية تجربة الامارات.

بحث علمي محكم منشور في مجلة الرسالة للدراسات الاعلامية.

تهدف الدراسة إلى التعرف على استراتيجيات الأمن السيبراني في ظل التهديدات الأمنية السيبرانية، وخاصة في ظل التحول الرقمي والتقدم التكنولوجي.

اعتمد البحث على المنهج الوصفي التحليلي.

توصل البحث إلى نتائج أهمها: نجاح التجربة الاماراتية في تبني استراتيجية سيبرانية، وذلك لاعتمادها على وسائل حديثة وتنمية القدرات السيبرانية.

5-(Sharma,2016): China's Emergence as a Cyber Power.

ظهور الصين كقوة سيبرانية.

هدفت الدراسة إلى إبراز أهمية الفضاء السيبراني كوسيلة جديدة في الصراع الدولي وتوصلت إلى أن التفوق في المجال السيبراني يمكن الدولة من ممارسة قوتها السيبرانية لتحقيق أهدافها وسعت الدراسة إلى إبراز الدوافع والأهداف التي تدفع الصين إلى تنمية قوتها السيبرانية وتحديد العوامل الأساسية لصنع القوة السيبرانية.

توصلت الدراسة إلى نتائج أهمها أن الفضاء السيبراني أصبح جزءاً جوهرياً من مكونات قوة الدولة وأثر في كل المجالات، وأصبح له دور في العمليات العسكرية والأمنية، طورت الدول بنيتها التحتية من أجل تسهيل الحصول على القوة السيبرانية وتوظيفها لتطوير وحماية مصالحها وتحقيق أهدافها.

تتميز الدراسة الحالية عن الدراسات السابقة في أنها ستقدم جانب تطبيقي مع ذكر العقيدة الأمنية الصينية في مجال الفضاء السيبراني، على المستوى الوطني والدولي، ومعرفة أهم الهجمات السيبرانية التي تعرضت لها الصين.

متغيرات البحث:

المتغير المستقل: الفضاء السيبراني.

المتغير التابع: العقيدة الأمنية للصين سواء على المستوى الوطني والدولي.

حدود البحث:

الحدود الزمانية: الفترة من 2015 إلى 2024.

الحدود المكانية: الصين.

1- مفهوم السيبرانية:

يطلق العديد من المصطلحات والمفاهيم على الهجمات السيبرانية، فقد أطلق مصطلح الحرب الافتراضية، أو الحرب السيبرانية، أو الحرب الإلكترونية على الهجمات السيبرانية، التي يتم من خلالها قيام القرصنة بمهاجمة الملفات والمواقع التي تخص الآخرين، كمهاجمة المواقع الإلكترونية للمنشآت المهمة، أو مهاجمة الحواسيب التابعة للوحدات العسكرية، أو الوحدات الاقتصادية لدول معينة بقصد تدميرها، والسيطرة عليها والإضرار بها (العيسى وعناب، 2019).

ترتبط نشأة الهجمات السيبرانية بحدثين مهمين هما (فرحات، 2019):

الأول: استخدام أجهزة الكمبيوتر في منتصف خمسينيات القرن الماضي، كأداة لحفظ المعلومات رقمياً حيث أصبح للحاسب دور أساسي في عمل الشركات والأفراد.

الثاني: ظهور الشبكة العنكبوتية (الإنترنت) التي أحدثت انقلاباً في حياة الأفراد من خلال التواصل وسرعة نقل المعلومات.

1-2- تعريف السيبرانية لغةً:

الهجمات السيبرانية مصطلح حديث ظهر في العقود الأخيرة، نتيجة لثورة التكنولوجيا والمعلومات ولم تكن الهجمات السيبرانية معروفة إلا في وقت قريب مما يشكل أحد أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام، فيما يخص تحديد طبيعتها، أو تعريفها، أو الكشف عن عناصرها خاصة أنها تستهدف جميع الحواسيب والمعلومات التي بداخلها، والأنظمة، والبرامج، والشبكات المفتوحة لاستعمال الجمهور العام، أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستخدمين والمفصلة عن شبكة الإنترنت العامة، فالهجمات السيبرانية يكتنفها غموض كبير، مما ينتج عن

ذلك صعوبات واجهها المختصون في القانون الدولي العام والإنساني على وجه الخصوص، وذلك من حيث تحديد تعريف محدد ومتفق عليه للهجمات السيبرانية (حطيط، 2020).

حيث أن السيبرانية مصطلح يوناني الأصل وترجع إلى مصطلح (kybemetes) الذي ورد في مؤلفات الخيال العلمي ويعني القيادة والتحكم عن بُعد، فقد ورد في قاموس المورد تعريف للسيبرانية حيث عرّفها بأنها: علم الضبط، مصدرها (Cybernetics) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها، بينما قاموس مصطلح الأمن المعلوماتي فقد عرف السيبرانية بقوله: هي هجوم عبر الفضاء السيبراني يهدف إلى السيطرة على المواقع الإلكترونية، أو البنى التحتية إلكترونياً لتعطيلها أو تدميرها، أو الإضرار بها (العيسى وعناب، 2019).

إن أول من استخدم مصطلح السيبرانية هو أحد علماء الرياضيات في عام 1948، في أثناء دراسته موضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية أما في اللغة العربية فنجد أن مصطلح السيبرانية، هو مصطلح مستخدم في اللغة الإنجليزية (Cyber) ولا يوجد مصطلح يناظره، أو يقابله في اللغة العربية لهذا واجه المتخصصون في اللغة العربية صعوبات في اختيار مصطلح مقارب لمصطلح (cyber) في اللغة الإنجليزية (حطيط، 2020).

وفي القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبير إلى مصدرها بل عرفت السيبرانية في نطاق استخدامها الفعلي أي العسكري، وهذا ما أشار إليه قاموس المصطلحات العسكرية الأمريكية بقوله: السيبرانية هي أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو تعطيل برامج إلكترونية أخرى (التميمي، 2021).

2- الفضاء السيبراني ومفهوم القوة:

تعد القوة من المفاهيم الأساسية في العلاقات الدولية، ومن ثم فإن هناك العديد من التعريفات لمفهوم القوة الفيلسوف الصيني (سان تزو) يعرفها بأنها: القدرة على شن الحروب حيث أن العمليات العسكرية مهمة للأمم والشعوب، وهي أساس الحياة أو الموت، أما ميكافلي فيعرفها بأنها: من العناصر الأساسية لقيام الدولة، وإن وجود الدولة وبقائها يعتمد بالدرجة الأولى على القوة (عوامر، 2018).

القوة هي امتلاك القدرة على التأثير في أطراف أخرى لتحقيق أهداف محددة، ومن ثم القوة وفقاً لهذا التعريف لها بعدين وهما: امتلاك مصادر القوة، والقدرة على توظيف هذه المصادر لتحقيق أهداف محددة.

هناك تعريف عديدة لمفهوم القوة فنجد أن مفهوم القوة الصلبة مرتبطاً بالمفهوم التقليدي للقوة الذي يعرف بالقدرة على فرض السيطرة على الآخرين عن طريق الإكراه، والإرغام ومن المصادر الأساسية للقوة الصلبة هي: القوة العسكرية، والقوة الاقتصادية، أما القوة الناعمة فهي: استخدام الجاذبية بدلاً من الإرغام وهي تنشأ من ثقافة أي بلد، أو حضارته، أو تقاليد الدول، أما القوة الذكية فهي قدرة الفاعلين الدوليين على الجمع بين عناصر القوة الصلبة والقوة الناعمة، بطريقة تضمن تحقيق أهداف الفاعلين الدوليين بكفاءة وفعالية. (صالح، 2021)

فقد عرف جوزيف س ناي القوة السيبرانية: بأنها مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات، والمعلومات، والشبكات الإلكترونية، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل.

والقوة السيبرانية أعطت دفعا للقوة الناعمة حيث إن الفضاء السيبراني أصبح مصدراً لشن هجمات من خلال نشر معلومات مضللة، ومن خلال الحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط، ومن ناحية أخرى يتعلق بتبني الدول للإنفاق في سياسات الدفاع السيبراني، وحماية شبكاتها الوطنية من خطر التهديدات وبناء مؤسسات وطنية للحماية من الهجمات السيبرانية. (عوامر، 2018) وهذا يثبت صحة الفرضية الثانية أن الفضاء السيبراني ساهم في تحول القوة من شكلها التقليدي إلى شكلها السيبراني.

وتعد الولايات المتحدة الأمريكية وروسيا والصين من أكبر القوى في مجال الاستحواذ على القوة السيبرانية القادرة على توظيف هذه القدرات لتحقيق الأمن السيبراني، وقد ظهرت قوى جديدة في مجال القوة السيبراني مثل إيران وتركيا. (صالح، 2021)

وبالتالي أدى الفضاء السيبراني والتقدم التكنولوجي إلى التحول في المفاهيم الأساسية في العلاقات الدولية مثل مفهوم القوة، فظهرت القوة السيبرانية والأمن السيبراني، والحرب السيبرانية والتي تعد من حروب الجيل الخامس للحروب التي تعتمد على تفجير الدول من الداخل.

3- مفاهيم في الفضاء السيبراني:

3-1- الحرب السيبرانية:

تعد الحرب السيبرانية من الحروب الحديثة والغير واضحة حيث يكتنفها الغموض، لأنها كانت مختلطة مع الحروب النفسية والدعائية، في حين أن انتشار شبكة الإنترنت وثورة المعلومات فتح آفاق كبيرة للدول في استغلال هذه الشبكة في حروبها الدولية، والتغلغل في أي شبكة من شبكات الإنترنت، والسيطرة على هذه الشبكة وتعطيلها، أو تغيير البيانات عليها، أو إتلافها، أو التحكم فيها من خلال الضغط على بضعة أزرار (العبودي، 2019).

يمكن تعريف الحرب السيبرانية (cyber war) على أنها: هجوم متعدد بغرض تعطيل عمل، أو خداع، أو إضعاف أو تدمير أنظمة الكمبيوتر وشبكات الاتصالات والمعلومات والبرامج الموجودة في تلك الأنظمة، أو الشبكات التي تمر من خلالها (منصور، 2019).

3-2- مفهوم الفضاء السيبراني:

يعد الفضاء السيبراني مجالاً حيويًا وجيوستراتيجيًا، حيث فرضت الثورة التكنولوجية مجموعة من التحديات والتهديدات الأمنية الجديدة، وبرز في النظام الدولي ما يعرف بالفضاء السيبراني، الذي أثر بدوره على التفاعلات السياسية والدولية الحاصلة بين مختلف الفاعلين في العلاقات الدولية المعاصرة، وحتى على المستوى الوطني. (حسين، 2021) تم تعريف الفضاء السيبراني بأنه مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المضمنة، كما يشار إليه بوصفه مكاناً مادياً، فهو مصطلح مختصر يشير إلى البيئة التي يتم إنشاؤها عن طريق النقاء الشبكات التعاونية من أجهزة الكمبيوتر وأنظمة المعلومات والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية (فرحات وعمر، 2021).

ويُخاض فيه العديد من الحروب والهجمات الرقمية، وهو مجال مركّب يشمل عدداً من العناصر وهي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات وحوسبة المعلومات ونقل وتخزين البيانات، ومستخدمو كل هذه العناصر وعليه فمسألة تحديد مفهوم الفضاء السيبراني، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي. (فرحات، 2019).

وعرفته وكالة الأمم المتحدة في تكنولوجيا المعلومات والاتصالات على أنه الحيز المادي وغير المادي ومعلومات محوسبه ، وشبكات، أجهزة ، الذي ينشأ أو يتكون من جزء أو من كل العناصر التالية: حواسيب وبرامج ومضامين ومعدات مرور ورقابة، والفضاء السيبراني يعد بيئة المعلومات وعلى نطاق عالمي يشكل من خلال استخدام الأجهزة الإلكترونية. وهناك من يرى أن الفضاء السيبراني ساحة حرب خامسة من ضمن المجالات السبع في الجو والبر والبحر والفضاء الخارجي والفضاءين الإلكترونيين المغناطيسية (سلمان وجاسم، 2023).

3-3- مفهوم الأمن السيبراني:

تسعى الدول إلى زيادة قدرتها في مجال الفضاء السيبراني، لذلك عليها تنمية قدراتها التكنولوجية ومواكبة التقدم التقني، الأمر الذي استدعى تحقيق الأمن السيبراني من أجل حماية المعلومات السرية، وبالتالي يعرف الأمن السيبراني: أمن

الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالإنترنت، فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات أو على الأقل الحد من أثارها (زرزوقة، 2018).

4- وسائل الهجمات السيبرانية (الأسلحة السيبرانية):

سيتم توضيح أبرز الوسائل التي تعد أسلحة للحرب السيبرانية والتي تُعد الأكثر استخداماً على الساحة الدولية وذلك على النحو الآتي:

1- استخدام البرامج الخبيثة:

تعد بمثابة برنامج ينفذ في لحظة محددة، أو في فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف، أو حالة مضمون النظام بغية تسهيل تنفيذ العمل غير المشروع، كإدراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محلاً للاعتداء، كأن يسعى البرنامج إلى البحث عن حرف في أي سجل يتضمن أمراً بالدفع، أو القيام بإجراء معين وعندما تكتشفه تعمل على إزالة هذا الحرف من السجل أو عدم إمكانية القيام بإجراء معين، ومن الأمثلة عن هذه البرامج برنامج سوتر (suter) وهو برنامج خبيث يستهدف البيانات الموجودة على الأنظمة الإلكترونية ويعمل على تشفير البيانات والمعلومات واختراق أجهزة الرادار. (التميمي، 2021).

2- هجمات الحرمان من الخدمة:

تعد هجمات الحرمان من الخدمة هجمات سيبرانية تتم بإغراق المواقع بسيل من البيانات غير اللازمة، التي يجري إرسالها ببرامج متخصصة تعمل على نشرها فتؤدي إلى بطء في الخدمات، أو صعوبة وصول المستخدمين إلى المواقع المطلوبة (عوامر، 2018).

3- الهجوم السيبراني:

يتم الهجوم السيبراني من خلال التشويش والخداع السيبراني، والقيام بالتجسس على الهدف لسرقة معلومات سرية، بغض النظر عن الأهداف والتي قد تكون اقتصادية كالتجارة بين الشركات، أو إستراتيجية أو عسكرية بين دول معينة، ومن تلك العمليات أيضاً التعدي على الملكية الفكرية، وقرصنة المعلومات كسرقة البرامج الحاسوبية، وتوزيع مواد مكتوبة، أو مصورة بدون إذن المالك الشرعي خاصة وأن وجود شبكة الإنترنت قد أدى إلى توسيع انتشار مثل تلك العمليات لسهولة النشر والتوزيع على هذه الشبكة (دحماني، 2018).

ومن الأمثلة على ذلك الهجوم السيبراني بفيروس (Stuxnet) وهو برنامج فيروسي يهاجم أنظمة التحكم المستخدمة في مراقبة الوحدات التي تعمل ألياً (حكيم وصبرينة، 2020).

5- الفواعل الرئيسية في ممارسة الهجمات السيبرانية:

حدد جوزيف س ناي أربعة أنواع من الفواعل الذين يمتلكون القوة السيبرانية وهي: الدول، الفواعل من غير الدول والأفراد.

1- الدولة: تعد الدولة فاعلاً محورياً في تسيير الفضاء السيبراني، انطلاقاً من إمكاناتها المادية، والبنوية والبشرية، والقانونية وتجدر الإشارة هنا إلى الاحتكار القانوني للدولة للفضاء السيبراني، بواسطة أجهزتها المختلفة، ولذلك لا بد لها من التحكم في مجال الفضاء السيبراني، وهو الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى التي قد تصل إلى تهديد مصالحها. (nayi, 2010).

2- الشركات متعددة الجنسيات:

تعد من الفواعل من غير الدول التي لها دور كبير في الفضاء السيبراني، لامتلاكها موارد للقوة تفوق قدرة بعض الدول، ولا ينقصها سوى شرعية ممارسة القوة، التي هي حكراً على الدول فمثلاً نجد شركات: جوجل Google وميكروسوفت Microsoft و أبل Apple المنتشرة في مختلف دول العالم التي تمتلك قواعد من البيانات العملاقة حيث إن معظم الدول

تتجه إلى جذب مثل هذه الشركات الدولية لخلق استثمارات جديدة ولأن العائد الاقتصادي من تصديرها للتكنولوجيا مرتفع جداً (زروقة، 2018).

3- حركات التحرر الوطني:

تعد من أبرز الفواعل الدولية من غير الدول والتي تضم عدد كبير من الأفراد بصفاتهم الشخصية، ويقومون بإرسال هجمات سيبرانية ضد أهداف العدو على الإنترنت بغية اختراق مواقعهم الأمنية وتعطيل عملها (عوامر، 2018).

4- الأفراد:

يعد الأفراد فاعلاً مهماً، وهم الذين يملكون معرفة إلكترونية ويستطيعون توظيفها ولكن تصعب ملاحظتهم والكشف عن هويتهم، حيث أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية حيث إن له القدرة على إحداث الثورة المعلوماتية كما أن هناك أفراداً مختصين في أعمال القرصنة، أو الجرائم السيبرانية، وسرقة المعلومات والبيانات الشخصية والتلاعب بها أو استغلالها لتحقيق مصالحهم (naye, 2010).

إن الفضاء السيبراني يساعد في انتشار القوة بين مختلف الفاعلين على الساحة الدولية، الأمر الذي أدى إلى زيادة المخاطر والتهديدات التي تواجهها الدول عبر الفضاء السيبراني، وأصبح من الضروري امتلاك مصادر التكنولوجيا الحديثة، ومواكبة التقدم التقني والرقمي التي تمكن الدول من مواجهة هذه المخاطر، وذلك من أجل امتلاك الأسلحة السيبرانية التي يتم استخدامها لحماية مصالح الدول.

6- مفهوم العقيدة الأمنية والاستراتيجية الأمنية.

تعد العقيدة الأمنية من الركائز الأساسية التي تساهم في صنع السياسة العامة والأمنية للدولة داخلياً وخارجياً. وتعد استراتيجية الأمن القومي والتطور التكنولوجي والتهديدات الحقيقية أو المحتملة من أهم العوامل المؤثرة في صناعة وصياغة العقيدة الأمنية.

تعرف العقيدة الأمنية بأنها: الاستراتيجية العليا للدولة حيث تعبر عن فن وعلم تطوير واستخدام القوى السياسية والاقتصادية والعسكرية للدولة، أثناء السلم أو الحرب لتحقيق الغايات والأهداف العامة للدولة.

أما الاستراتيجية الأمنية: هي الطريق أو الأسلوب الذي تستطيع الدولة من خلاله توظيف كافة الإمكانيات والقدرات والطاقات، لتحقيق الأمن وتحقيق الأهداف والغايات المرجوة (قسايسة، 2021).

يرى الباحث أن مفهوم العقيدة الأمنية يتوافق إلى حد كبير مع مفهوم الاستراتيجية، لأن المفهومين يتفقان في الجوهر وهو توظيف الطاقات المختلفة في تحقيق الغايات العليا للدولة.

7- أهمية القوة السيبرانية في تطوير الاقتصاد الصيني.

تعد مخاطر وتهديدات الفضاء السيبراني من العوامل المهمة لتصاعد وبروز التنافس بين شركات عاملة في مجال الأمن السيبراني لتعزيز سوق الانفاق العالمي وتأمين للبنى التحتية السيبرانية، مع بروز فواعل آخرين لشبكات القرصنة وشبكات الجريمة السيبرانية، إذ انتهجت الصين من خلال سياستها على الصعيد الدولي في التركيز على التعاون والانفتاح على آلية السوق العالمي وأهميتها ورغبة الصين في السيطرة والتحكم في الأسواق العالمية. ومن الأبعاد المهمة والرئيسية للفضاء السيبراني وهو البعد الاقتصادي الذي أصبح جاذب لكافة قطاعات المجتمع وبنات تكنولوجيا المعلومات والمعرفة بهذا المجال محرك للنمو الاقتصادي وهو من العوامل الأساسية لهذه المعلومات والتكنولوجيا هو النهوض بالاقتصاد الوطني مما دفع الصين في الآونة الأخيرة لزيادة الاستثمار في التكنولوجيا الحديثة (سلمان وجاسم، 2023).

وتسعى الصين إلى تطوير المنتجات والخدمات في سوق الأمن السيبراني، الأمر الذي ينعكس إيجاباً على الاقتصاد الصيني، حيث تؤثر الزيادة في الطلب على السلع والخدمات في مجال الأمن السيبراني، على شركات إنتاج الأسلحة والخدمات العسكرية وتؤدي إلى ظهور ما يعرف بسوق الأمن السيبراني، ويتضمن سوق الأمن السيبراني تطوير المنتجات

والخدمات للتطبيقات الهجومية والدفاعية، حيث تركز هذه التطبيقات على النشاط الحكومي والعسكري، ويشار إليها أيضاً باسم الأسلحة السيبرانية كما يتكون قطاع الأمن السيبراني من الشركات التي توفر المنتجات والخدمات للاستخدام الهجومي والدفاعي، عبر تكنولوجيا المعلومات والاتصالات والمجال الصناعي (قوادة وكحلوش، 2021).

8- دور القوة السيبرانية في العقيدة الأمنية الصينية:

لقد وضعت الصين القوة السيبرانية أحد أولوياتها على غرار باقي دول العالم، التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها آليات جديدة تعني بهذه المسائل، بالموازرة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية الصينية المعاصرة، ولهذا فإن السلطات الصينية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم والهجمات السيبرانية (الميموني، 2020).

ولامتلاك قوة سيبرانية لا بد من وجود عناصر تدعم هذه القوة منها: (دحماني، 2018)

1-بنية تكنولوجية:

هي البنية الأساسية لتكنولوجيا المعلومات، والإطار المتكامل الذي تعمل عليه الشبكات الرقمية، وتتضمن هذه البنية مراكز البيانات وأجهزة الحاسوب، وشبكات الحاسوب، وأجهزة إدارة قواعد البيانات، ونظام للوائح التنظيمية.

2-أسلحة سيبرانية (الفيرسات): هي برامج تم تصميمها لإلحاق الضرر بقواعد البيانات، أو سرقتها وتخريبها أو قطع الاتصال بالشبكة، علماً أنه يصعب التعرف أو اكتشاف هذه الأسلحة، وهي برامج صنعت عمداً لتغيير خصائص الملفات.

3-الردع السيبراني: يكون الردع السيبراني من خلال خلق مجموعة من المحفزات التي تمنع قيام أحد أطراف الصراع من القيام باعتداء، أو الهجوم مستقبلاً، مع العلم أنه لايسطيع أحد الأطراف القضاء على الخصم الآخر كلياً.

4-بنية مؤسسية وتشريعية: مهمتها تحقيق استخدام القوة السيبرانية في ظل تحقيق إستراتيجية الدولة، وتدريب الجيوش والكتائب السيبرانية لتحقيق الأمن السيبراني للدولة والأفراد، وأن يكون هناك هيئة تشريعية تهتم بتعريف الجرائم السيبرانية وتحديد جزاء مرتكبيها.

5-العنصر البشري: هو المدرب على استخدام أجهزة الفضاء السيبراني، وقادر على اختراعها وتطويرها، وهذا يعتمد على جودة التعليم المقدم وولاء هذه العناصر للدول.

8-1-العقيدة الأمنية الصينية على المستوى الوطني:

بالنسبة إلى الصين فإن الأمن السيبراني جزء من السيادة السيبرانية ويرتبط مفهوم السيادة السيبرانية بالحاجة إلى التحكم في أي نشاط يرتبط بالدولة فالحكومة الصينية تعمل على تركيز الرقابة والتحكم في الانترنت ومحتواه وبذلك فإن الأمن السيبراني يعتبره الصينيون وسيلة للحفاظ على السيادة السيبرانية ويستند مفهوم السيادة السيبرانية في الصين على مبدئين رئيسين (شرايطية، 2020).

لا بد من حظر أي تأثير غير مرغوب فيه في الدولة عبر فضاء المعلومة ومنع مواطنيها من التعرض للأفكار والآراء التي تعتبرها الدولة غير مقبولة.

تحويل حوكمة الانترنت من البيئات الحالية التي تشمل الأكاديميين والشركات إلى منتدى دولي مثل الأمم المتحدة هذه الخطوة تستلزم أيضاً نقل السلطة من الشركات والأفراد إلى الدول وحدها.

أطلقت الوثائق الصينية على الإستراتيجية الصينية حرب الوخز بالإبر وهي تشير إلى القدرة على شل العدو من خلال مهاجمة نقاط الضعف لديه وأنظمة التحكم والقيادة والاتصالات والمعلومات التابعة للدولة كما قام جيش التحرير الصيني بتطوير عقيدة عسكرية سيبرانية تم بمقتضاها تدريب القوات الصينية على آليات الهجوم السيبراني من خلال برامج المحاكاة للحروب السيبرانية. وهذا يثبت صحة الفرضية الأولى، وفي عام 2012م بدأت الحكومة الصينية في بذل جهود للتوصل إلى استراتيجية شاملة في إعداد هيكل تنظيمي لأمن الشبكات فقد تم إنشاء لجنة الأمن القومي ومجموعة قيادية مركزية

لأمن المعلومات والانترنت يترأسها الرئيسي الصيني فكانت استراتيجية الصين للأمن السيبراني تؤكد على دعم البنية التحتية لأمن الشبكات والمعلومات لكن تعدد الهيئات والقطاعات وتداخلها في هذا المجال أدى إلى تداخل وتضارب المصالح فيما بينها (غيدان والربيعي، 2020).

كما أصدرت الصين (قانون الأمن السيبراني الصيني) المعمول به منذ 2017 شددت من خلاله على أنه من حق الدول ذات السيادة وضع قوانين وقواعد لتنظيم الفضاء السيبراني طبقاً لما تقتضيه مصلحة البلاد وإتباعاً للممارسات الدولية المعمول بها في هذا الصدد يمكن فهم قانون الأمن السيبراني في الصين كتأثير لمفهوم السيادة السيبرانية فجاء هام من هذا القانون يشترط أن تقوم الشركات التي تساهم في البنية التحتية الحيوية للمعلومات بتخزين بياناتها داخل الحدود الصينية وبمقتضاه يكون محظوراً على مقدمي خدمات الانترنت إفشاء سرية البيانات (بيرم، 2019).

8-2- العقيدة الأمنية الصينية على المستوى الدولي:

حماية الأمن الدولي ضرورة حتمية تفرضها مقتضيات العصر لذلك كان على الدول أن تسعى للحد من الهجمات السيبرانية وأيضاً نتيجة لحوادث الأمن السيبراني العالمي انطلقت فكرة حماية الفضاء السيبراني، بإنشائها مجموعات عمل لمكافحة الجريمة السيبرانية كما اتخذت قرارات بخصوص الأمن في الفضاء السيبراني والقرارات الصادرة عنها بينت للدول الأعضاء أهمية التحديات السيبرانية (دحماني، 2018).

في عام 2012 قام كل من الصين والبرازيل وجنوب أفريقيا وروسيا بعقد اتفاقية تنظيم مشترك في المسائل المتعلقة بإدارة الانترنت والتنمية والفضاء السيبراني وتبادل الانترنت والتعاون في مجال الأمن السيبراني وأبرمت اتفاقية بين الصين وكوريا الجنوبية حيث أعرب الجانبان عن الحاجة إلى تعزيز وتنسيق المواقف الدولية لإدارة الانترنت (شرايطية، 2020).

كما تسعى الصين لتعزيز أهدافها من خلال الدعوة إلى مفهوم السيادة السيبرانية في المحافل الدولية باحتواء جدول الأعمال العالمي، أفضل مثال على ذلك هو اجتماع فريق هندسة كما الانترنت لعام 2015 حيث أرسلت الصين 40 ممثلاً ومعظم الدول الغربية واحداً أو اثنين على الأكثر، ويتضمن الجزء الأخير من هذه الاستراتيجية بناء تحالفات وشراكات لمواجهة الهيمنة المتصورة للولايات المتحدة في هذا المجال (بيرم، 2019).

دافعت الصين عن فكرتها التي تستند إلى وجود فضاء سيبراني آمن وسلمي بعيداً عن استخدام الفضاء السيبراني في أعمال عدوانية، في مختلف المجالات الدبلوماسية في محاولة لإنشاء تحالف واسع من الدول يوافق على هذا المبدأ فقد أكدت قمة البريكس لعام 2016 على أولوية الدول في وضع جدول الأعمال كما دافعت الصين عن نفس الفكرة في إطار أعمال منظمة شنغهاي للتعاون التي تتألف من الصين وروسيا والعديد من دول آسيا الوسطى الموقف الرئيسي الذي اتخذته هذه الدول هو أولوية الدولة وإمكانية تطبيقها في مجال الفضاء السيبراني أيضاً (شرايطية، 2020).

9- العلاقة بين الأمن السيبراني والذكاء الاصطناعي:

هنالك ارتباط وثيق بين الأمن السيبراني والذكاء الاصطناعي فالذكاء الاصطناعي له ارتباط بالعلوم الأخرى مثل علم الرياضيات وعلم النفس واللغات وله دور مهم ورئيسي في تطور لغة الكمبيوتر وأنظمة الحاسوب، والغرض هو الوصول إلى دقة أكثر في الحواسيب والذكاء من الإنسان وهناك اتجاه حديث في توظيف تكنولوجيا الحواسيب والتي تكون خواصها أكثر وأدق ذكاء من الذكاء البشري في مجالات عديدة ولاسيما الاقتصادية في العالم.

حيث تسعى الصين إلى توظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني، من خلال التطبيقات التي يوفرها الذكاء الاصطناعي سواء في الجانب السياسي أو الاقتصادي أو العسكري.

ويعرف الذكاء الاصطناعي بأنه: عملية محاكاة للذكاء البشري بواسطة الآلات وخاصة أنظمة الكمبيوتر.

أضحت الصين في الوقت الحالي منافس تكنولوجي قوي لها نظام تكنولوجي مدعم ومجهز بالموارد ومصمم لغرض الفوز بهذه المنافسة وإعادة شكل النظام في العالم لصالحها، ويعد الذكاء الاصطناعي العديد من التكنولوجيات المهمة في توسع

نفوذ الصين ومنافسة القوة العسكرية والاقتصادية للولايات المتحدة الأمريكية وتأمين استقرارها المحلي، وتسعى لتمويل المشاريع الضخمة التي تتعلق بالبنى التحتية الرقمية داخل الصين وخارجها (سلمان وجاسم، 2023).

10-الاستنتاجات: من خلال هذه الدراسة تم التوصل إلى عدد من النتائج وهي:

1. أحدث الفضاء السيبراني تغييراً في مفاهيم العلاقات الدولية كمفهوم القوة فظهر مصطلح القوة السيبرانية، والحرب السيبرانية.
2. تنوع صور التهديدات السيبرانية من (تجسس سيبراني، قرصنة سيبرانية، هجمات سيبرانية، إرهاب سيبراني) .
3. أكدت الصين على أهمية التحول إلى القوة السيبرانية، والعمل على توظيفها في كل المجالات العسكرية والاقتصادية.
4. تعد التكنولوجيا من أهم الركائز الاستراتيجية لدولة الصين وتخصص موارد هائلة لتطوير الجانب السيبراني والتكنولوجي.

11-التوصيات: بناء على نتائج البحث يوصي الباحث بالتوصيات التالية:

- 1- ضرورة تنمية القدرات السيبرانية ودمجها في مختلف المجالات، وضرورة المواكبة الكاملة للمفاهيم الحديثة في المجال التقني والتكنولوجي على المستوى الدولي.
- 2- الاستفادة من التجارب الدولية الناجحة في مجال الفضاء السيبراني، وخاصة التجربة الصينية الرائدة في مجال الفضاء السيبراني.
- 3- ضرورة العمل على تحقيق الأمن السيبراني وذلك من خلال التعاون بين الدول والشركات المتخصصة في مجال الأمن السيبراني والتكنولوجي لمواجهة مختلف التهديدات السيبرانية.
- 4- ضرورة وضع قواعد قانونية دولية موحدة تحكم حالات الحرب والنزاع في الفضاء السيبراني.

12-المراجع:

- 1- العيسى، طلال، عناب، عدي (2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي. مجلة الزرقاء للبحوث والدراسات الإنسانية. مجلد 19، العدد 1.
- 2- بيرم، فاطمة (2019). السيادة الوطنية في ظل الفضاء السيبراني والتحول الرقمي الصين نموذجاً. المجلة الجزائرية للأمن الإنساني. مجلد 5، العدد 1، ص 789-816.
- 3- دحماني، سليم (2017). أثر التهديدات السيبرانية على الأمن القومي للدول أمريكا نموذجاً. رسالة ماستر في العلاقات الدولية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة: الجزائر.
- 4- فرحات، علاء الدين، عمرو، عمارة (2021). الفضاء السيبراني وتأكل مفهوم السيادة الوطنية. المجلة الجزائرية للدراسات السياسية، مجلد 8، العدد 1، ص 162-183.
- 5- حسين، حياة (2021). الفضاء الإلكتروني وتحديات الأمن العالمي. مجلة العلوم القانونية والسياسية. مجلد 12، العدد 1، ص 1066-1089.
- 6- حطيط، رولا (2020). السيبرانية الحرب الخفية في المنطقة المظلمة. مجلة السياسة الدولية. مجلد 7، عدد 3.
- 7- شرايطية، سميرة (2020). السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي. مجلة العلوم السياسية والعلاقات الدولية. المجلد 9، العدد 16.
- 8- شلوش، نورة (2017). القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول. مجلة بابل للدراسات الإنسانية، مجلد 8، عدد 2.
- 9- عوامر، فاطمة (2018). أثر القوة السيبرانية في الاستراتيجيات الأمنية للدول الكبرى دراسة حالة الصين. رسالة ماجستير في الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة: الجزائر.