المجلة العلمية
لكلية الدراسات الاقتصادية والعلوم السياسية

https://esalexu.journals.ekb.eg
دورية علمية محكمة
المجلد العاشر (العدد العشرين، يوليو 2025)

تأثير القوة السيبرانية على الاستراتيجية الأمريكية في مواجهة الاستراتيجية الصينية [1]

The American Strategy The Impact of Cyber Power on in Confronting the Chinese Strategy

رباب إبراهيم سلومة
باحث دكتوراه العلوم السياسية
كلية الدراسات الاقتصادية والعلوم السياسية
جامعة الإسكندرية
rababsluma1@gmail.com

[1] تم تقديم البحث في 2024/9/4، وتم قبوله للنشر في 2025/7/1.

الملخص

أعادت التطورات التكنولوجية إلى السطح مرة أخرى دراسة الاستراتيجية خاصة، التأثير المحتمل للقدرات السيبرانية على الاستراتيجية المستقبلية. خاصة في ظل غياب السيادة في الفضاء الإلكتروني وانتشار الفوضى تماما مثل النسق الدولي على أرض الواقع، حيث أعطي الفضاء الإلكتروني معنى جديد لأدوات القوة، وخاصة أداة العنف الممثلة بشكل جديد للحرب. حيث يمكن لأي شخص مهاجمة الجميع تقريبًا من أي مكان وفي أي وقت، نظرًا لطبيعة الفضاء السيبراني الافتراضية، أدى التسارع هذا في تطورات التكنولوجيا إلي تسارع صعود الكيانات القوي في النسق الدولي وإحداث تأثير كبير في قرارات القوي بالنسق، نتيجة لذلك تساءلت القوى الكبرى مثل الصين والولايات المتحدة حول مدى كفاية الفكر الاستراتيجي، مما دفع تلك القوي إلي تحديث في استراتيجيتها بما يتوافق مع مكانتها وسرعة التطور التكنولوجي، أدى ذلك إلى وجود مستوى آخر من التنافس والصراع بين الصين والولايات المتحدة، كانت أبرز أدواتها أولاً، الهجمات السيبرانية والتجسسية وتبادل الاتهامات بينهما. وثانياً، دخول سباق التطور في آليات الأسلحة الموجهة عبر تطبيقات الذكاء الاصطناعي، مما انعكس على اقتصاد كليهما وأليات قوتهما العسكرية وتبعاً لها آليات الاستراتيجية خاصة في منطقة الإندوباسيفيك ومسار مبادرة الحزام والطريق الصينية ومن ثم القرار السياسي والدبلوماسي لكلا القوتين بشأن القضايا الاستراتيجية مثل الأزمة التايوانية.

كلمات مفتاحية: الحرب السيبرانية / الاستراتيجية السيبرانية /القوة الأمريكية / مبادرة الحزام والطريق الصينية/الذكاء الاصطناعي.

Abstract

Technological Developments Have Once Again Resurfaced The Study Of Strategy, In Particular, The Potential Impact Of Cyber Capabilities On Future Strategy. Especially In Light Of The Absence Of Sovereignty In Cyberspace And The Spread Of Chaos, Just Like The International Format On The Ground, Cyberspace Has Given A New Meaning To The Tools Of Power, Especially The Tool Of Violence Represented In A New Form Of War. Since Anyone Can Attack Almost Everyone From Anywhere And At Any Time, Due To The Virtual Nature Of Cyberspace, This Acceleration In Technology Developments Has Accelerated The Rise Of Powerful Entities In The International Format And Made A Significant Impact On The Decisions Of The Powerful In The Format, As A Result, Major Powers Such As China And The United States Wondered About

The Adequacy Of Strategic This Has Led To Another Level Of Competition And Conflict Between China And The United States, The Most Prominent Tools Of Which Were, First, Cyber-Attacks, Espionage And The Exchange Of Accusations Between Them. Secondly, The Entry Into The Race Of Development In The Mechanisms Of Guided Weapons Through Artificial Intelligence Applications, This Was Reflected In The Economy Of Both Countries And The Mechanisms Of Their Military Power, Followed By Strategic Mechanisms, Especially In The Indo-Pacific Region And The Course Of The Chinese Belt And Road Initiative, And Then The Political And Diplomatic Decision Of Both Powers On Strategic Issues Such As The Taiwanese Crisis.

Keywords: Cyber Warfare / Cyber Strategy / American Power / China's Belt and Road Initiative / Artificial Intelligence.

مقدمة

تطورت قدرات الدول بالفضاء الإلكتروني بصورة سريعة في السنوات الأخير، ليصبح مجالاً هاماً في العلاقات الدولية، قد تكتسب أولوية لدى العديد من الدول نظراً، لأن الفضاء السيبراني يتميز بالعالمية، ولا يقتصر مجاله على المجالات المحلية أو الدولية فقط. بل، يتقاطع تقريباً في كافة مجالات النشاط البشري، حيث لا يقتصر الأمر على قدرات الدول، ولكن أصبح الأفراد والجماعات والشركات، بالإضافة إلى الدول يعتمدون عليه بشكل متزايد، ومع تشابك العلاقات بين الدول سواء على مستوى القوى الكبرى أو الإقليمية، خاصة في ظل وجود تحركات في سلم القوي للعديد من الدول الكبرى، والتي تتقاطع مصالحها وتتضارب في صورة نزاعات إقليمية أو اختلالات بالقوة، نتيجة ذلك التنافس لكل دولة. تسعى الدول الكبرى في إدارة ترتيبها في سلم القوة والتنافس على قيادة العالم وإدارة العلاقات الدولية وفقاً لمصالحها الوطنية عبر العديد من الآليات والأبعاد التي تقاس بها قوة الدول، إلا أن التفوق الاقتصادي والعسكري وحتى السياسي وحده لم يعد كافياً، ولكن التطور وزيادة القوة السيبرانية لدى الدول أصبح أمراً في غاية الأهمية، وبالرغم من أن الولايات المتحدة كانت في الطليعة الثورة الإلكترونية في كافة أنظمتها إلا شهدت هذه الثورة تراجعاً نسبياً. في مقابل ذلك تصاعدت قدرات الصين في العقدين الأخيرين، في العديد من المجالات سواء اقتصادياً وعسكرياً أو اقتصادياً ومؤخرا سيبرانياً أو إلكترونياً، والتي بدورها ترجمت العديد من التطلعات للرؤساء الصينين وفقاً لاستراتيجية صينية واعية، مركزة ومُلبية لمتطلبات الواقع الجديد، حيث بذل الرئيس "**شي جين بينغ**" جهداً كبير في إقرار العديد من التطورات وهيكلة المؤسسات الصينية والتشريعية، في

إطار رغبة الصين بأن تصبح " **قوة إلكترونية عظمي**"، إلي جانب التحدث عن رؤيته خاصة لتطوير الاقتصاد الرقمي وتعزيز التكامل العميق بين الإنترنت والبيانات الضخمة، والذكاء الصناعي، وغيرها من رقمنة القطاعات التقليدية من قطاعات التصنيع والزراعة، كل هذه الجهود في الفضاء الإلكتروني، والتي منها تنطلق الصين في إضافة جديدة لترساناتها العسكرية، وجود ترسانة سيبرانية تدعم وتضاعف جهدها في تحقيق تفوقها الاقتصادي والعسكري بصورة خاصة، حيث طورت العديد من القدرات الإلكترونية الهجومية، مع فرض العديد من التشريعات التي تدعم تلك التوجهات الاستراتيجية المبنية علي الأفعال التجسسية من اختراقات وغيرها، مما مثل هذا الأمر تهديداً هائلاً للولايات المتحدة في الفضاء الإلكتروني الذي لطالما سيطرت عليه في عقود سابقة، إلا أن السياسة الإلكترونية للصين تخطت تلك الهيمنة الأمريكية، وأصبحت أكثر تعقيداً عن ذي قبل، عما تمثله التفاعلات ومسارات التنافس الدولي للقوي الكبرى التقليدية بالنسق الدولي، إلا أن الأمر اختلف في الفضاء الإلكتروني، شكلت أنشطة الصين في الفضاء الإلكتروني تحدياً مختلفاً وجوهرياً وأصبح أكثر إلحاحاً في دراسته وإيجاد بدائل للتعاطي مع مستجداته من قبل الولايات المتحدة . خاصة في ظل توجيه سلوك الدولة نحو معايير أكثر مسؤولية في حالة السلم، في حين أن الصين لديها رغبة في عدم الالتزام بنفس القواعد الدولية، الأمر الذي مثل وجود علاقات بين البلدين في صورة أكثر ديناميكية، خاصة في الآونة الأخيرة، عملت تشريعات الصين بصورة واضحة على تشريعات الأمن السيبراني في الصين، القائم على أولوية تسليح صناعة الأمن السيبراني، وخاصة بعد تأكيد الأمين العام للحزب الشيوعي "شي جين بينغ" في 5 مارس 2018 على أن مسؤولي الحزب الشيوعي المنفذين للسياسات الإلكترونية يجب أن يكون لديهم وجهة نظر "**صحيحة** " للفضاء السيبراني لأن " **الأفكار تحدد الإجراءات** " ومن ثم **مكانة القوة العظمى، وأولوية الأمن القومي، والفضاء السيبراني كمكان للمنافسة الاستراتيجية الدولية**. ونظراً لهذا التوجه المعلن واجهت الولايات المتحدة العديد من الهجمات السيبرانية، ورصدت العديد من الاختراقات والتجسس الإلكتروني وغيرها من الآليات التي تستغلها الصين تحت ما يعرف بالسيادة الإلكترونية لها. في مقابل ذلك تنشأ الصين العديد من المؤسسات والمنظمات الجديدة، لتحل محل آليات الحوكمة السيبرانية الموضوعة من قبل الولايات المتحدة والغرب عموماً، وبما يتماشى مع المعايير الصينية في تحقيق مكانتها العظمى، وتحقيقاً لأمنها القومي عموماً، وفي الفضاء السيبراني بصورة خاصة كمكان جديد وفعال في إدارة المنافسة الاستراتيجية الدولية، خاصة مع رصدت العديد من التقارير الأمريكية الرسمية طموحات خطط ومبادرات الصين في السيطرة على الفضاء الإلكتروني. وطرحت عبر

هذه التقارير العديد من التساؤلات حول مدى كفاية الموارد للقوات الأمريكية الإلكترونية العسكرية أو حتى بصورة عامة، حول مدى كفاية الحماية الحالية للبنية التحتية الحيوية للولايات المتحدة، ونطاق التعاون في مجال الأمن السيبراني بين القطاعين العام والخاص، في ظل تطور وتعقد أنشطة الصين التجسسية واستخدام الصين تقنيات وإجراءات متقدمة ومعقدة في السنوات الأخيرة، ومدى اختلالات القوة الأمريكية في مواجهة تزايد التصاعد الصيني في إيجاد بدائل للمعايير الأمريكية وتأثيرها على النسق الدولي.

مشكلة الدراسة

تأتي القوة السيبرانية كمحدد رئيس بالفترة الحالية في قياس قوة الدول بالنسق الدولي، بل أصبح تأثيرها يتضاعف عند بناء الاستراتيجيات للدول الكبرى مؤخراً، فكرة التوجيه عن بعد أو الاختراق عن بعد وتعطيل أو إضعاف أدوات القوة للدول الأخرى، مثلما يحدث مؤخرا من قبل الصين وروسيا في الاختراقات السيبرانية للمصالح الاقتصادية والعسكرية الأمريكية والتسبب في تغيير استراتيجيات القوة لديها وتطوير البرامج المختلفة. ومن هنا، يمكن صياغة المشكلة البحثية في سؤال رئيس مفاده: **ما هو تأثير القوة السيبرانية على الاستراتيجية الأمريكية في مواجهة الاستراتيجية الصينية؟**، وينبثق منه تساؤلات فرعية محل الدراسة **كالتالي:** هل تراجعت قدرات الصين في تهديدها للمصالح الأمريكية في ظل التطور التكنولوجي للذكاء الاصطناعي وتطبيقاته المختلفة؟، مدى تأثير المعلومة أو فكرة الاختراقات السيبرانية على قوة ومكانة الدول بالنسق الدولي، خاصة الولايات المتحدة؟

أهمية موضوع الدراسة

1. تتضح أهميتها الأكاديمية والعلمية خاصة في الدراسات الأمنية الدولية من خلال التعريف بالموضوع، مما يجعلها جديرة بالدراسة والتحليل. وذلك بتقديم إضافة للمكتبة العربية ومحاولة لسد الفجوة المعرفية حول التطورات في نظرية الردع الجديدة، بالإضافة إلى تحليل التنافس التكنولوجي وأثره سواء على الابتكارات أو التطور السيبراني بشكل خاص في العلاقات الدولية.
2. تعزز هذه الدراسة التفكير الأكاديمي حول بناء الاستراتيجيات الحديثة، وفهم تحولاتها خاصة بدراسة ميزان القوة وتأثير القوة السيبرانية في ميزان القوة الدولي، في إطار تقديم فهم أو دراسة لبعض أبعادها، مثل تعزيز الأمن القومي الأمريكي باستخدام القوة السيبرانية في حماية البنية التحتية الأمريكية من التدمير أو الاختراق في ظل إدارة تنافسها مع الصين، حيث يعتبر المجال السيبراني ساحة الصراع

الجديدة بين الدول، وتبعًا لذلك يؤثر على الاقتصاد العالمي خاصة في ظل السيطرة الأمريكية على الابتكار وسلاسل التوريد العالمية.

3. تقديم صورة واضحة عن التفاعلات الأمريكية وآلية الحفاظ على تفوقها العسكري وتعزيز الأمن القومي الأمريكي وإدارة مصالحها وأهدافها الاستراتيجية في أوراسيا وتداعياتها اللاحقة على ميزان القوى بالنسق الدولي سواء كان اقتصاديًا أو سياسيًا أو عسكريًا، خاصة مع دخول القوة السيبرانية واقتصادياتها.

فرضية الدراسة

تلعب القوة السيبرانية دوراً محوريًا في تعزيز الاستراتيجية الأمريكية وإحداث تغييرات جوهرية فيها لمواجهة التحديات التي تفرضها الاستراتيجية الصينية. في ظل امتلاك الصين لمشروعات شاملة بالمبادرة خاصة بتطور القدرات السيبرانية، والتي ينعكس تأثيرها بصورة جذرية ممثلة في إعادة تكوين النسق الدولي بشكل يهدد الأمن القومي الأمريكي وموقعه بالنسق كقوة مهيمنة عليه، وتشير الفرضية إلى حدوث الكثير من التغييرات الاستراتيجية كانعكاس لتلك الاختلالات في صورة صراعات قادمة، مما سيدفع الاستراتيجية الأمريكية من محاولة تصحيح الوضع الراهن والمستقبلي من خلال التأثير على موازين القوة المختلفة اقتصادية وسياسية وعسكرية بصورة خاصة، حيث سيكون الجيش الأمريكي بشكل كبير أكثر تركيزًا في التحضير لمعارك مستقبلية عالية التقنية، فضلاً عن كونها قوة منخرطة بشكل مركزي في التعاون الأمني في الخارج مما يسهم في تحقيق التفوق الأمريكي في ظل التنافس الجيوسياسي والجيو استراتيجي الذي فرضته الصين بالنسق الدولي .

منهج الدراسة

تقع أهمية اختيار " المنهج الواقعي " كمنهج يعطي إطاراً تحليلياً مناسبا لدراسة تأثير القوة السيبرانية على الاستراتيجية الأمريكية في مواجهة الاستراتيجية الصينية لأن أهم أدواته المفاهيمية هي مفهوم القوة والصراع والمصلحة الوطنية في النسق الدولي في ظل فوضوية النسق الدولي، حيث يظهر القوة السيبرانية وسيلة لتحقيق التفوق الاستراتيجي لكل من الصين والولايات المتحدة، والذي بضرورة الحال يؤدي هذا التنافس إلي سباق الهيمنة فيما بينهم، وهذا يفسر تصاعد الهجمات السيبرانية والتجسس الإلكتروني كأدوات لإدارة الصراع، ومن ثم نجد أن القوى الكبرى الصين والولايات المتحدة تسعى للتركيز على مصلحتها الوطنية بتوظيف القوة السيبرانية بحماية مصالحها الحيوية ضد بعضهما البعض، عبر التفوق العسكري

وحماية البنية التحتية الحيوية، لذا جملة القول يحلل المنهج الواقعي استراتيجيات الولايات المتحدة والصين وتقييم الأهداف السيبرانية في إطار إدارة التنافس بينهما في ظل ساحة الصراع الجديدة الممثلة بالمجال السيبراني، حيث يعطي تفسيراً للهجمات السيبرانية أو الابتكار التكنولوجي الذي تسعى إليه القوى الكبرى كالولايات المتحدة لتحقيق واستمرارية هيمنتها، في ظل فوضوية النسق وغياب السلطة العليا التي تنظم المجال السيبراني .

الإطار الزمني والمكاني للدراسة

تستهدف الدراسة نطاق زمني من 2009-2022، ونطاقها المكاني في الدراسة منطقة الإندوباسيفيك بصورة مركزة، لأن بداية مواجهة الولايات المتحدة لمبادرة الحزام والطريق فعلياً بخطوات فعلية جاءت من خلال إدارة أوباما مع إعلان استراتيجية التوجه نحو آسيا مع العديد من المبادرات التي سبقتها في ذات الإطار المكاني وتمثل نهاية النطاق الزمني 2022، لأنها جاءت بها إعلان إدارة بايدن لاستراتيجية الأمن القومي الأمريكي المركزة في أغلبها على آليات وتوجهات الولايات المتحدة في مواجهة الحزام والطريق وبصورة خاصة منطقة الإندوباسيفك، تعد كلا الاستراتيجيتين امتداد لنفس التوجهات الأمريكية خط ثابت يمكن الاعتماد عليه في فهم ودراسة الاستراتيجية الأمريكية وتطورها في مواجهة المبادرة الصينية خاصة في المجال السيبراني .

دراسات سابقة

1. **غراي، كولن س. (2015). مستقبل الاستراتيجية، بوليتي برس.**

Gray,Colin S.(2015.(Future Of Strategy ,Polity Press.

تدور أغلب أفكار كولن فكرة رئيسة هدفها "إظهار الصفات العالمية للاستراتيجية، يركز على ماذا يقصد جراي بالاستراتيجية ومناقشة حججه حول أهمية الاستراتيجية والحاجة إليها، إلى جانب ذلك يركز على الفرق بين النظرية الاستراتيجية والممارسة الاستراتيجية فالأولي كانت وستظل دون تغيير عبر التاريخ، والثانية تتغير حسب الوقت والتكنولوجيا والموقع وغيرها من العوامل الأخرى المؤثرة تأكيد جراي في أغلب كتاباته حول الاستراتيجية ليست بالضرورة تكون الأداة العسكرية فقط، ولكنه يري أن هناك ما يعرف باستراتيجية الجسر وهي أي أداة للقوة، يمكن أن تتضمن أدوات غير عسكرية وفي الاستراتيجية بشكل عام مع ذلك تحقق أهدافاً سياسية. طرحه لمفهوم " **البنيات الفكرية** " للعصور النووية يجدها البعض أنها غير

كافية في طريقة عرضها للأدلة. ولكنها، استطاعت أن توجه النقاشات النظرية والمفاهيمية لإيجاد صيغة يمكن بها فهم التغيرات التي حدثت في النسق النووي العالمي، فهو يسمح عبر ذلك المفهوم للمفكر الاستراتيجي بالتمييز ما بين أسباب وأعراض تغيير السياسة. والتي لاحقاً خرج لنا بتعريف الاستراتيجية "كوسيلة لتحقيق الأهداف السياسية والتي إذا ترجمت إلى وسائل عملية تصبح وسيلة لضمان السلام والأمن" (Cséfalvay،2023)، **وتأتي الاستفادة البحثية:** من خلال كتابات جراي خاصة ذلك الكتاب مستقبل الاستراتيجية حول استكشاف للاستراتيجية الحديثة كيف تتغير سياقات الاستراتيجية باختلاف العوامل وغيرها، إضافة إلى العلاقة بين الاستراتيجية والسياسة وتفريقه بين النظرية الاستراتيجية والاستراتيجيات المعروفة باسم الخطط.

2. مور، دانيال.(2022). العمليات السيبرانية الهجومية: فهم الحرب غير الملموسة. المملكة المتحدة: مطبعة جامعة أكسفورد.

Moore, Daniel. (2022) **Offensive Cyber Operations: Understanding Intangible Warfare.** United Kingdom: Oxford University Press**.**

يتناول الكتاب في مجمله العديد من الموضوعات الخاصة بمجال الحرب السيبراني ومن أسس ومعايير ودراسات حالة خاصة بمجال الفضاء السيبراني الأمريكي والصيني والروسي، وأيضاً أمثلة على التهديدات الإيرانية المحتملة، ناهيك عن عرض لأهم ما توصلت إليه الثورة التكنولوجية في المال السيبراني، تكمن أهمية الكتاب في تقديم الكاتب دانييل إلى تقديم فهم حول كيف تدمج الدول العمليات السيبرانية الهجومية في استراتيجيتها، بالإضافة إلى عن فهم دورة حياة وتعقد استهداف شبكات الخصم هو أمر أساسي للقيام بذلك بفعالية في الصراع. يسعى التحليل بالأخذ بالأسباب الواقعية في الفهم من خلال الجمع بين دراسات الحالة التشغيلية والاستراتيجية العسكرية والتحليل الفني، حيث تمثل الحرب السيبرانية جزء من الحرب التقليدية بأهدافها ولكن بوسائل غير ملموسة، فالصراع ينشأ ويدار بوسائل غير مادية مثل فضاء المعلومات وغيرها. **لذا تأتي الاستفادة البحثية في مناقشة الكتاب لطبيعة** العمليات السيبرانية الهجومية واختلافات حجمها من تسلل، من تخريب، من جمع معلومات استخباراتية وقت السلم أو تعطيل موارد وقت الحرب عبر هجمات قصيرة الأمد، تهدف إلى إحداث اضطرابات تكتيكية مؤقتة يقدم الكتاب في أغلب فصوله فهم للاحتمالات، قبل أن يتحول إلى إلقاء النظرة على بعض الجهات الفاعلة بالحرب السيبرانية

والأكثر إنتاجاً للهجمات أو الأثر تعرضاً لها مثل الولايات المتحدة وروسيا والصين وإيران. ولكل منها وجهة ولكل منها وجهة نظره ومزاياه وتحدياته الفريدة عند مهاجمة الشبكات من أجل التأثير.

3. إيريكا دي لونيرجان، جاكلين شنايدر. (2023)، قوة المعتقدات في الاستراتيجية السيبرانية الأمريكية: الدور المتطور للردع والمعايير والتصعيد، مجلة الأمن السيبراني، المجلد 9، العدد 1، 2023،

Lonergan ,Erica D, Schneider ,Jacquelyn.(2023), **The Power Of Beliefs In US Cyber Strategy: The Evolving Role Of Deterrence, Norms, And Escalation**, Journal Of Cybersecurity, Volume 9, Issue 1, 2023

يقدم الكاتب ملخصاً حول "الدور الذي يلعبه الفضاء الإلكتروني في القوة العسكرية محل نقاش حاد. ولكن كيف تتجلى هذه الأفكار في الاستراتيجية السيبرانية؟ في هذه المقالة، نتتبع تطور الأفكار حول القوة السيبرانية العسكرية، مع التركيز على الولايات المتحدة الأمريكية. وعلى وجه الخصوص، نستخدم عقداً من الاستراتيجيات السيبرانية الدفاعية الأمريكية كعدسة لاستكشاف كيف تغيرت الأفكار حول دور المؤسسة العسكرية في تعزيز المعايير السيبرانية، وجدوى الردع السيبراني، ومخاطر التصعيد بمرور الوقت. ومن خلال ذلك نحدد مصادر الاستمرارية والانقطاع. ننتقل بعد ذلك إلى الأدبيات الأكاديمية لتقييم تلك الأفكار وتقييم استراتيجيات الدفاع الأمريكية السيبرانية، وتحديد الثغرات والتوترات." **تأتي الاستفادة البحثية: يوفر لمحة حول تطور الأفكار الاستراتيجية السيبرانية الدفاعية الأمريكية**، خاصة توضيح ثلاثة استراتيجيات دفاعية إلكترونية أمريكية تم تطويرها في الأعوام 2011 و2015 و2018، وتأثرهم بنسق الفضاء الإلكتروني على الصعيد الدولي وتوازن القُوى، خاصة أن الأفكار التي تناولها الكتاب تقدم مقترحات، وأفكار لوضع استراتيجيات الدفاع الأمريكية الإلكترونية المستقبلية بصورة ناجعة.

4. فيشركيلر، مايكل بي، وآخرون(2022). نظرية الثبات السيبراني: إعادة تعريف الأمن القومي في الفضاء السيبراني. الولايات المتحدة، مطبعة جامعة أكسفورد.

(Fischerkeller, Michael P., Et Al.) 2022 (**Cyber Persistence Theory: Redefining National Security In Cyberspace.** United States, Oxford University Press)

يقوم الكتاب بشرح وتسليط الضوء ويناقش العديد من الأفكار منها آلية وضع تصورات جريئة ومتقدمة للأساسيات التي تحرك السلوك و الديناميكيات في الفضاء السيبراني، تنظر للعمليات والحملات السيبرانية إنها مجرد أفعال لا ترقي لمستوي الصراعات المسلحة، يتناقش الكتاب "نظرية الثبات السيبراني"

وتدور حول سوء فهم الفضاء السيبراني أدي لتطبيق نظريات الصراع في بيئة مختلفة عن البيئة التي نشأت فبها تلك الاستراتيجيات، مما تسبب بخسائر استراتيجية ويوضح المؤلفين كيف أن نموذج نظرية الردع لا يستطيع تفسير أو إدارة غلبة النشاط السيبراني للدولة" . **لذا تأتي الاستفادة البحثية بما يمثله الكتاب بإضافته** الجديدة أهمية كبرى، حيث يقدم الكتاب نظرية جديدة تسليط الضوء على الديناميكيات الاستغلالية وليست القسرية، للمنافسة السيبرانية، بمعنى من يمتلك المعلومة يستطيع أن يساوم بصورة أكبر لا أن يفرض فقط حقيقة واقعية بالقوة، حيث يقدم الكتاب إطاراً تحليلاً يمكن أن يكون بمنزلة الأساس لاستراتيجيات جديدة، بالإضافة إلى تقديم الكتاب بعض التوجيهات التي قد تفيد صناع السياسات الاستراتيجية بصورة خاصة يمكنهم من خلالها تأمين فضاء إلكتروني أكثر استقراراً وأمناً

مفاهيم رئيسية:

- **الاستراتيجية السيبرانية** هي مجموعة من الخطط والسياسات التي تضعها الدول أو المؤسسات بهدف تنظيم وحماية البنية التحتية الرقمية، والدفاع عن الفضاء السيبراني من الهجمات الإلكترونية، وتعزيز القدرات التكنولوجية لضمان الأمن القومي والمصالح الاستراتيجية في البيئة الرقمية. تشمل الاستراتيجية السيبرانية جوانب متعددة مثل الردع الإلكتروني، الحماية من التهديدات السيبرانية، وتعزيز التعاون الدولي في هذا المجال. (Executive Office Of The President. ,September 2018)
- **الحرب السيبرانية** هي الصراع الذي يتم بين الدول أو الجهات الفاعلة باستخدام الوسائل الإلكترونية بهدف تعطيل، تدمير، أو السيطرة على أنظمة الحواسيب وشبكات الإنترنت التابعة للخصم. تُستخدم في هذه الحرب تقنيات القرصنة، البرمجيات الضارة، والهجمات على البنية التحتية الحيوية مثل شبكات الكهرباء والاتصالات، بهدف تحقيق أهداف عسكرية، سياسية، أو اقتصادية (Clark& Landau. ,2010).

خطة الدراسة

تتكون الدراسة من مبحثين: **المبحث الأول:** القوة السيبرانية الصينية وتأثيرها على الاستراتيجية الأمريكية، **المبحث الثاني:** استراتيجيات الأمن السيبراني للولايات المتحدة في مواجهة الاستراتيجية السيبرانية الصينية.

المبحث الأول

القوة السيبرانية الصينية وتأثيرها على الاستراتيجية الأمريكية.

تعد تسارع التكنولوجيا من أهم المؤثرات على مسارات أدوات القوة في النسق الدولي والإقليمي، وعلى مدار العقود السابقة شهدت تطبيقات الذكاء الاصطناعي زيادة علي ذلك التأثير على القُوَى الكبرى خاصة الصين والولايات المتحدة، بطبيعة الحال تطوير تطبيقات الذكاء الاصطناعي مرت بعدة مراحل حتى تصل لذلك التأثر القُوَى في القوة والنفوذ للوحدات السياسية المتفاعلة بالأنساق المختلفة سواء على المستوى الإقليمي أو الدولي، تأتي تلك الاستراتيجية السيبرانية في إطار التصور الصيني حول ضرورة وجود قوة غير متكافئة مع الغرب، تسمح لها بالخروج من إطار الهيمنة الخاص بالغرب إلى النسق الخاص بها، زيادةً على ذلك فالصين تسعى إلي تحقيق السيادة الرقمية والتي تسمح لها بتنظيم الفضاء الإلكتروني كيفما شاءت، فإن النظام الصيني على دراية تامة بمعلومات التهديد المحتمل التي تشَكَّلها عندما تُترك خارج نطاق السيطرة لذلك تشَكَّل جملة القوانين CSL و DSL و PIPL، جنباً إلى جنب مع لوائح الصناعة المختلفة والمعايير الوطنية، إطاراً قانونياً شاملاً ومفصلاً لحماية البيانات والأمن السيبرانى في الصين.

المطلب الأول

تطور القوة السيبرانية في الاستراتيجية الصينية

يأتي تفوق الصين في الذكاء الاصطناعي أساس واقعي في التأثير على القوة الأمريكية واختلالها من خلال رصد الاختراقات التي تمت من قبل الصين وأثرت بصورة مباشرة على قدرة الولايات المتحدة في التعامل معها، لم تأتي فكرة اكتساح الصين من فراغ خاصة في مجال مثل التنمية الرقمية ومجالات إدارة البيانات والأمن السيبراني، لذا جاء التأثير على المجال السيبراني الدولي والاختراقات السيبرانية المؤثرة على العديد من القوي بالنسق الدولي والإقليمي، وتطوير الذكاء الاصطناعي بصورة عشوائية، بل عملت الصين على تطويرها الرقمي على قدم وساق على مدار العقد الماضي. عملت الاستراتيجية الصينية لتوجيه وتعزيز السوق الرقمي واستمرارية تدفق البيانات العميقة والسائلة إلى دمج توليد البيانات – وعلى نطاق أوسع، والنظام الإيكولوجي الصناعي لتكنولوجيا المعلومات – في نسيج الاقتصاد الصيني باعتباره "**عامل إنتاج**" جديد متكامل (Dasgupta, 2023)، جاء ذلك رداً على عسكرة وزارة الدفاع الأمريكية للعالم مع إنشاء القيادة الإلكترونية الأمريكية عام 2009، رأي القادة الصينيين ضرورة وجود نسخة صينية من القيادة

الإلكترونية فيما يعرف بسباق حرب المعلومات التي دخلت فيها كلا القوتين، وذلك في إطار ما أعلنه الرئيس "هو جين تاو' مع خمسة من كبار جنرالات جيش التحرير الشعبي في مديرية الأركان العامة (GSD) في عام 2010، وتفسيراً لذلك الأمر نجد كتابة "جريج أوستين " تفسير نفس النقطة لضرورة امتلاك أمل الانفتاح في تبني التكنولوجيا الحديثة، ففي عام 2010، توصل المحللون الصينيون إلى استنتاج مفاده أن "ظل البلد – مجرد – مقلداً للابتكار التقني... ولم يقدم البيئة التمكينية " (Austin, 2014, P110)، **في ظل** امتلاك منافسيهم تلك البيئة التي أدت تقدمهم، مما أدى إلى خنق التغير الثقافي التكنولوجي الحقيقي. وفي ذات السياق في 20 يوليو 2010 صدر الأمر الرئاسي الصيني في "التعامل مع التهديدات الإلكترونية مع دخول الصين عصر المعلومات، وتعزيز البنية التحتية الإلكترونية للبلاد، بالإضافة إلي ما سبق نجد أنه في 8 نوفمبر 2012 في إطار نقل القيادة الرئاسية الصينية من جين تاو إلي الرئيس شي جين بينغ " صرح بان جيش التحرير الشعبي الصيني "ستسرع الصين تطبيقات تكنولوجيا المعلومات العسكرية الكاملة بحلول عام 2020".(Paganini, 2015) عملت الصين على تطوير استراتيجياتها بشكل عام على فكرة " **الدفاع النشط أو الهجوم الدفاعي** (Patton, 2016) "، فقد أعلنت مجموعة استشارية تابعة للكونجرس تصريح حول اعتبار الصين كأكبر خطر منفرد على أمن التقنيات، حيث اتهمت الولايات المتحدة الأمريكية الصين بشن هجمات حرب إلكترونية استهدفت شبكات منظمات أمريكية عسكرية وتجارية وبحثية وصناعية مهمة. (Claburn،2010)، **استكمالاً لما سبق** صدرت في عام 2015 وثيقة من وزارة الدفاع الوطني الصيني بعنوان "**استراتيجية الصين العسكرية**". حيث عدلت الوثيقة الأخيرة النقطة الأساسية **(Preparations For Military Struggle (PMS**.– النضال العسكري للجيش الصيني إلى "كسب الحروب المحلية المعلوماتية "، وجدير بالذكر تناولت هذه الوثيقة العسكرية الرسمية أول مرة " الأمن السيبراني " حيث عرفت "**الفضاء الإلكتروني**" : بأنه "ركيزة جديدة للتنمية الاقتصادية والاجتماعية، ومجال جديد للأمن القومي" وفي ذات السياق أوضحت بهذه الوثيقة أن "الصين تواجه تهديدات أمنية شديدة الخطورة لبنيتها التحتية السيبرانية"، حيث أن "**المنافسة الاستراتيجية الدولية في الفضاء السيبراني آخذة في التحول على نحو متزايد، تقوم دول قليلة بتطوير قواتها العسكرية الإلكترونية**".(Jinghua,2019) ويأتي ذلك في إطار تطبيقي يظهر في الاستثمارات الصينية في مجال الذكاء الاصطناعي مؤكدة على أهمية حيث شهدت الفترة من 2015–2017 زيادة كبيرة في الاستثمار بالذكاء الاصطناعي حيث وصلت ل 11.52 مليار دولار (Mcnally 2021,)، إضافة إلى ذلك تخطط

وزارة الصناعة وتكنولوجيا المعلومات (MIIT) أيضاً لتعزيز التنمية والطلب بالنسبة لمنتجات الأمن السيبرانى لاعتبارها قطاع هام والتقصير فيه يمثل جزء كبير من التهديدات التي تواجهها الصين، بلغت تقريباً قيمة القطاع أكثر من 38.6 مليار دولار بحلول عام 2023، تفسراً لتلك الزيادة في الاستثمارات وتنمية الطلب على الأمن السيبراني، جاء خلال إلزام الصناعات الرئيسة بتخصيص 10٪ من ميزانية تكنولوجيا المعلومات الخاصة بها للأمن السيبرانى بداخلها العامين المقبلين، ويمثل ذلك الأمر تعزيز مصطنع من وزارة الاتصالات وتكنولوجيا المعلومات الصينية (***Borak,2021***)، **ويلاحظ أن اعتراف الصين بوجود تهديدات وإدراكها أن الوسائل السيبرانية ضرورية للحرب المعلوماتية.** انعكس ذلك على عقيدة الصينيين الاستراتيجية، ونتيجة لذلك الأمر ترتبط الصين في وثائقها وتصريحاتها الرسمية بمراجعة دورية لتطورات الواقع للأمن القومي الصيني سواء محلياً أو خارجياً. وفقاً لذلك، تحدد العقيدة الصينية " موقع الإنترنت ضمن المفهوم التشغيلي الأكبر لعمليات المعلومات (*IO*)، الذي يتضمن أيضاً الحرب الإلكترونية والفضائية والنفسية" (...) وتجدر الإشارة إلى قول" **الاستراتيجيين الصينيين إن هذه هي القدرات الأساسية التي يجب تنسيقها كأسلحة استراتيجية "لشل نظام أنظمة التشغيل للعدو" و "تخريب نظام قيادة حرب العدو**". بمعنى آخر: يعتقد جيش التحرير الشعبي أن المعلومات هي المورد الحاسم في ساحة المعركة الحديثة وأن النصر يتحقق من خلال ضمان وصول المرء إلى هذا المورد بينما يحرمه العدو" (Kitchen,2021)، **لذا تعتمد الحكومة الصينية آلية مراقبة الإنترنت بصورة متداخلة.** عبر زيادة الاستثمارات بالذكاء الاصطناعي خاصة بين عامي 2010-2017 بلغت إجمالي الاستثمارات الصينية في الذكاء الاصطناعي ما يقرب من 1.3 مليار دولار إلى حوالى 2.1 % من الناتج المحلي الإجمالي الصيني المخصص للبحث والتطوير(Mcnally ,2021)، قد يكون النسق للنظام الشيوعي الصيني في فترات له يعطي إطار إنه متجه إلي الانفتاح على آليات السوق التي لا تتحكم فيه الدولة كاملة، خاصة في مجالات فتح باب الاستثمار الأجنبي في الصين أو العولمة، إلا إنه في واقع الأمر وضعت الصين استراتيجيات وآليات تهدف إلى وقف الأزمات السيبرانية الكبرى، وضمان الشبكة المحلية وأن المعلومات المختلفة عبر مواد وقوانين صينية. **ووفقاً لما رصدتها بعض التقارير الأمريكية الرسمية مثل تقرير لجنة المراجعة الاقتصادية والأمنية الأمريكية الصينية في الجلسة 117 لعام 2022**، ولكن في الحالة الصينية تستخدم تلك البيانات في تحقيق أهداف تجسسية استخباراتية – الأمر فعلياً ينطبق على كافة الدول الكبرى، ولكن حالة الصينية هي مثار التركيز _ ولكن الصين تخترق تلك القوانين الخاصة بحماية المعلومات بكل

روتيني، حيث تلزم الشركات خاصة العاملة في المجال التكنولوجي على تسليم كود المصدر في القضايا المدنية. بل، في كثير من الحالات يلاحظ إلزام ومطالبة الشركات والباحثين بتقديم جميع الثغرات للبرامج والأجهزة المكتشفة إلى الحكومة الصينية قبل تقديمها إلى البائعين، بمعني تعمل الحكومة الصينية على تكوين ثغرات تسمح لها بالاطّلاع التجسس على كافة البرامج والأجهزة بصورة قانونية، (U.S.CONGRESS,November2022)

المطلب الثاني

تأثير الهجمات السيبرانية الصينية على الاستراتيجية الأمريكية

قد أتت الاختراقات الصينية كمسار داعم للتطور التكنولوجي وبصور خاصة وتطورها السريع في أغلب المجالات الاقتصادية والعسكرية عبر العديد من الاختراقات، ساهمت في حصول الصين على تدفق هائل من المعلومات ودعمت بها استراتيجياتها كقوة كبرى صاعدة، وفي إطار تعريف هل تعتبر الهجمات حربا سيبرانية أم هجمات تخريبية فنجد أن "**توماس ريد** " في عرض رؤيته بمضمون تلك الهجمات الإلكترونية القديمة أو الحديثة، إنها لا تشكل الصورة النمطية للأعمال الحربية التي اعتادها المحللين، إنها ترقى إلى كونها "نسخ معقدة من ثلاثة أنشطة... قديمة قدم الحرب نفسها: التخريب والتجسس والتخريب "(Rid , 2012,P6) ولاحظ أن هجمات رفض الخدمة الموزعة الهائلة (Ddos) على إستونيا في عام 2007 لا يمكن وصفها بأنها عمل حرب لأن "مجرد" حصار "المواقع الإلكترونية ليس فعلاً عنيفاً بذاتها".(Rid , 2012,P13) إلا إنها تتم بصورة حديثة مستخدمة أدوات العصر الحديث عبر الفضاء الإلكتروني أو السيبراني. ويؤكد أن الهجمات الإلكترونية تختلف عن الحرب التقليدية لأنها لا تفي بتعريف كلاوزفيتز للحرب على أنها استخدام عنيف وفعال وسياسي للقوة (Rid , 2012,P7). ويؤكد "**ريد**" أيضاً مجازية كلمة "**حرب**" في مصطلح "**الحرب الإلكترونية أو السيبرانية** " أكثر من كونها وصفية لحال واقعي كما في الحروب التقليدية المادية. لذا نستعرض بعض هذه الهجمات الصينية على سبيل المثال لا الحصر:

1- الهجمات الإلكترونية على مستوى البنية التحتية المدنية

ووفقاً لتقرير DTIC لعام 2009 بعنوان "**قدرة جمهورية الصين الشعبية على الحرب السيبرانية واستغلال شبكة الكمبيوتر**" الذي تم إعداده للجنة المراجعة الاقتصادية والأمنية الأمريكية الصينية، أشار إلى أن قدرات الصين المتزايدة في الحرب الإلكترونية تمثل تهديدات ناشئة للمصالح الوطنية للولايات المتحدة. (Krekel. 2009)، **جاء هذا الأمر بمنزلة إنذار تلته العديد من الخروقات تسببت في كثير من**

الخسائر المادية والمعرفية للولايات المتحدة والدول المرتبطة بها خاصة في سلاسل التوريد أو مستخدمي التكنولوجيا الأمريكية منها: في 8 أبريل 2010، أعلنت شركة China Telecom المملوكة للدولة عن طريق شبكة خاطئة أمرت "بكميات هائلة" من حركة الإنترنت الأمريكية والأجنبية الأخرى بالمرور عبر الخوادم الصينية استغرقت 18 دقيقة. في حين نفت لاحقاً الشركة الصينية التهم التي وجهت إليها من قبل الولايات المتحدة باختطاف حركة مرور الإنترنت بالولايات المتحدة على إثر خروج متحدث باسم وزارة الدفاع الأمريكية يؤكد حدوث هذا الأمر ولكن لا زالوا لا يعرفون حدوث هذا الفعل عن قصد خبيث أم لا. (Wolf ,2010,). **وتماشياً مع ما تم ذكره** نجد تصريح وتحذير مدير وكالة المخابرات المركزية السابق "ليون بانيتا "، في عام 2011، من أن "***هجوم بيرل هاربور القادم يمكن أن يكون هجوماً إلكترونياً.***" (Drake,2013)، في تقرير صادر في يونيو 2022 يؤكد قيام الجهات الفاعلة السيبرانية التي ترعاها الدولة في جمهورية الصين الشعبية بحملات واسعة النطاق لاستغلال الثغرات الأمنية التي تم تحديدها علناً بسرعة، والمعروفة أيضاً باسم الثغرات الشائعة ونقاط الضعف منذ عام 2020 **(Consider The Cves-Vulnerabilities And Exposures Common)**

زيادةً على ذلك سمحت هذه التقنية للجهات الفاعلة لتحقيق مكاسب الوصول إلى حسابات الضحايا باستخدام أكواد الاستغلال المتاحة للعامة ضد الخصوصية الافتراضية **VPN** . (Cybersecurity Advisory, JUN 2022,Pp 22:25)، **ووفقاً لتقرير مناقشة صادر عن الكونجرس في 20 يوليو 2021 استعرضت المناقشة** بعض الهجمات شديدة الخطورة التي كانت ستؤثر على المواطنين وبالتالي تهديد الأمن القومي الأمريكي داخلياً بصورة مباشرة " ففي فبراير 2021، تضمن هجوم إلكتروني على منشأة لمعالجة المياه في أولدسمار بولاية فلوريدا زيادة مستويات هيدروكسيد الصوديوم من 100 جزء في المليون إلى 11100 جزء في المليون في مياه الشرب. ومع ذلك، فقد ارتفعت مستويات هذه المادة الكيميائية في المياه التي تنتجها شركة أولدسمار بولاية فلوريدا إلى مستويات من شأنها أن تسبب ضرراً للناس إذا شربوها أو استخدموها" (U.S.Congress 20 July ,2021)، **وفي ذات الإطار**، قدمت **CISA** و FBI أدلة على حملة صينية تستهدف النفط الأمريكي وشركات خطوط أنابيب الغاز الوطنية من 2011 إلى 2013 "لغرض عقد خط أنابيب أمريكي". (CISA.Gov. 21 July , 2021) الهجمات الصينية ضد التكنولوجيا التشغيلية، وبطبيعة الحال عند تتبع المكتب الفيدرالي بنشاط الهجمات الصينية ضد ما يقرب من 23 خط أنابيب غاز طبيعي مختلف. أسفرت عن وجود 16 هجوماً أدت لوجود ثغرات مؤكدة في تلك

الأنظمة (Mesich,2022)، وأشار التقرير إلى أن النشاط "كان يهدف في النهاية إلى المساعدة تطور الصين قدرات هجوم إلكتروني ضد خطوط الأنابيب الأمريكية لإلحاق الضرر المادي بخط الأنابيب أو تعطل عمليات خطوط الأنابيب ". كما اتهم مسؤولو الحكومة الأمريكية الجهات الفاعلة التي تعمل لمصلحتها استخدام المخابرات الصينية لبرامج الفدية لابتزاز الشركات الأمريكية "(The U.S.–China Economic And Security Review Commission,2022,Pp65:83).

2- الجانب الاستخباراتي

أما بشأن أمن شبكات المعلومات في عام 2015 عندما أدى خرق بيانات مكتب إدارة شؤون الموظفين(**OPM**) إلى سرقة الملايين من سجلات الموظفين الحساسة للموظفين الفيدراليين حوالي 22 مليون سجل. إن الهجمات ضد الحكومات الفيدرالية وحكومات الولايات والحكومات المحلية والإقليمية والقبلية، فضلاً عن التهديدات التي تتعرض لها أنظمة المعلومات الخاصة وأنظمة البنية التحتية الحيوية، (U.S. Congress, 20 July,2021))، وفي ذات الإطار في 2017 كشفت الولايات المتحدة لائحة اتهام للمقاولين أو جواسيس الإنترنت الصينيين المتورطين بشكل مباشر في سرقة الأعمال الأمريكية (BING,2017)، وتجدر الإشارة إلى ألية الهجمات الإلكترونية تتم من قبل المهاجمين عبر أدوات مسح للشبكات مفتوحة المصدر بشكل روتيني للبحث عن أنظمة غير مُصححة وتمييزها كهدف. وبطبيعة الحال يؤدي هذا إلى زيادة كفاءة عملياتهم إلى الحد الأقصى، بينما يلغي أيضاً الحاجة إلى استخدام تكتيكات أكثر. (Mesich, 2022)، **بالإضافة إلى ما سبق ذكره جاء البيان الافتتاحي للمفوضة "كارولين بارثولوميو"** في إطار جلسة الاستماع بالكونجرس إلى "قدرات الصين السيبرانية: الحرب والتجسس والتداعيات على الولايات المتحدة"، ذكرت إنه في مايو 2020، بالإضافة إلى الاكتشافات السابقة من مكتب التحقيقات الفيدرالي (FBI) كشف عن تحقيقه في "استهداف وتسوية الولايات المتحدة. المنظمات التي تجري أبحاثاً متعلقة بـ *COVID*-19 من قبل الجهات الفاعلة الإلكترونية المنتسبة إلى جمهورية الصين الشعبية والجامعيين غير التقليديين ". حيث تم الإبلاغ عن الانتهاكات لشركة التأمين الصحي *Anthem Inc.*، *Equifax*، ماريوت" (The U.S.–China Economic And Security Review Commission,2022,Pp 5-7)، وسابقاً في مايو 2014، اتهمت وزارة العدل الأمريكية خمسة ضباط عسكريين صينيين بالسرقة السيبرانية. وردت وزارة الخارجية الصينية بغضب وبسرعة غير مسبوقة، مطالبة الولايات المتحدة بسحب القضية (Menn,2014). **ويأتي تأثير ذلك على القوة الأمريكية في أن** سرقة تلك

البيانات يكمن فيما أشار إليه "خبراء التكهن بأن الجمع بين البيانات المكتسبة من خلال اختراق *OPM* مع البيانات المسروقة من الآخرين كيانات مثل الفنادق ومكاتب الائتمان يمكن أن تؤدي إلى التعرف على عملاء المخابرات الأمريكية والأصول التي يتم تداولها أو الانتقال عبرها" (GRAFF,2020)، ووفق ما صرح به مدير مكتب التحقيقات الفيدرالي جيمس كومي: "إنها صفقة كبيرة جدًا من منظور الأمن القومي ومن منظور مكافحة التجسس. إنها كنز دفين من المعلومات حول كل شخص عمل أو حاول العمل أو يعمل لمصلحة حكومة الولايات المتحدة.". (Washington Post, 9 July2015).

3- الجانب الاقتصادي الرقمي أو السيبراني

في إطار الاستخدام المتواصل للدول الأجنبية كالصين للهجمات الإلكترونية لسرقة المعلومات، والتأثير على السكان وإلحاق الضرر بالصناعة، بما في ذلك البنية التحتية المادية والرقمية الحيوية. يلاحظ العديد من المحللين أن الكم الهائل من المعلومات التي حصلت عليها الجهات الصينية أثرت في تطور اقتصادها الرقمي بشكل طورت الصين أقوى بنية تحتية الرقمية في العالم نافست بها الولايات المتحدة **فوفقاً للبيانات التي ذكرها داس جوبتا** Dasgupta**، في دراسته** : " أنهت الصين عام 2021 بـ 1.425.000 محطة قاعدية *G5*، 60٪ من الإجمالي العالمي، و 455 مليون مستخدم *G* . 5 أما بالنسبة لإجمالي عدد مستخدمي الإنترنت، فقد نما من 564 مليوناً في عام 2012 إلى 772 مليوناً في عام 2017 إلى 1.032 ملياراً في عام 2021 – بمعدل انتشار الإنترنت بنسبة 73٪. " (Dasgupta,2023)، انعكست تلك التطويرات على سوق الاقتصاد الرقمي وانتقال التطور الرقمي إلى الشرق، **ومنها الشركات المصنعة للتكنولوجيا وبرامج الكمبيوتر وغيرها من التقنيات لتوفر البنية التحتية المساعدة إلى جانب حدوث طفرة في الشركات التكنولوجية الناشئة في المجال الرقمي في صورة متزايدة:** " نمو الاقتصاد الرقمي بنفس القدر من الازدهار. ارتفع إجمالي القيمة السنوية، من حيث تصنيع أجهزة ومعدات تكنولوجيا المعلومات والاتصالات وكذلك تطوير البرمجيات والإيرادات، من 27.2 تريليون يوان صيني تمثل 32.9 في المئة من الناتج المحلي الإجمالي في عام 2017 إلى 45.5 تريليون يوان صيني يمثل 39.8 في المائة من الناتج المحلي الإجمالي في عام 2021 (دولار أمريكي) / يوان = 1 / 6.4 في ديسمبر 2021). **وفي أساس** هذه التطورات كانت الطبيعة المتفجرة المتنامية لتوليد البيانات. قفز إنتاج البيانات الخام في المجال السيبراني الصيني من 2.3 زيتابايت (*ZB*) في عام 2017 إلى 6.6 زيتابايت في نهاية عام 2021، وهو ما يشكل أكثر من 10 في المئة من إجمالي البيانات في جميع أنحاء العالم". (Dasgupta,2023)، مع

أنّ هناك عدد متزايد من الدول والجهات الفاعلة التي تمتلك مثل هذه القدرات إلا إنه لا زالت تلك الدول تستخدم مجرمي الإنترنت أو المخترقين الأجانب ذوي المهارة العالية في مجال الاختراقات السيبرانية، **ووفقًا لتقرير مراجعة المخاطر السنوية في أبريل 2021** (U.S. Office Of The Director Of National Intelligence. 2021,Pp 20:21)، إن احتمال تأثر حوالي 18 ألف عميل حول العالم بهذه البرمجيات قد أثار قلق الحكومة الأمريكية، حيث أن هناك كيانات وشبكات أمريكية رسمية تم استهدافها بواسطة هذه البرمجيات، بما في ذلك شبكات المؤسسات في جميع أنحاء الحكومة الفيدرالية، وحكومات الولايات، والحكومات المحلية في الولايات المتحدة؛ بما في ذلك بعض وكالات الحكومة الأمريكية، **في 13 مايو 2021**، تم الإبلاغ عن أن قسم شرطة العاصمة تعرض لأسوأ هجوم إلكتروني تم الإبلاغ عنه ضد قسم شرطة في الولايات المتحدة. وأطلقت العصابة، المعروفة باسم مجموعة بابوك–Pabuk، آلاف الوثائق الحساسة الخاصة بإدارة شرطة العاصمة على الويب المظلم **DARK WEB** لأن الإدارة لم تدفع. لا تقتصر التهديدات السيبرانية على المعلومات المتعلقة بموظفي الحكومة (U.S.Congress 20 July ,2021)، **لم تكن تلك الاختراقات هي الأولى من نوعها** ولكن كانت اختراقات سولار ويند والهافيوم هي الأبرز، ومقدمة لاختراقات وتطوير الذكاء الاصطناعي الصيني في مجالات عدة، **فوفقًا لتقرير الكونجرس الصادر 29 سبتمبر 2021 بعنوان" الأمن السيبراني الفيدرالي: الخلفية والقضايا":** (Jaikaran, 2021,P3)، وتعد من أخطر الهجمات الإلكترونية إلى سمحت للحكومات مثل الصين وروسيا في فهم الكثير من ثغرات والحياة الأمريكية بتفاصيل كبيرة ومن ثم تغذية برامج الذكاء الاصطناعي في التحليلات، مثل هجمات سولار ويند – Solarwinds والهافنيوم –Hafnium.، ففي هجمات سولار ويند **Solarwinds** أحد أكثر الهجمات تطوراً التي تم اكتشافها في الولايات المتحدة على الإطلاق، وسولار ويند هي شركة تصنيع منتجات إدارة تكنولوجيا المعلومات لعملاء الأعمال، تسمح منتجات Solarwinds لكبار مسؤولي المعلومات (Cios– Chief Information Security Officers) بأتمتة بعض الأنشطة مثل إدارة عناوين بروتوكول الإنترنت (IP)، ومراقبة الأجهزة على شبكتها، ونشر التحديثات(Solarwinds Official Website) ، تم تنفيذ محاولة الاختراق من قبل جهاز المخابرات الرئيسي في روسيا لتسليم التعليمات البرمجية إلى برامج إدارة الشبكات المستخدمة على نطاق واسع، مع تعرض ما يقرب من 18000 عميل من الشركات والحكومة الفيدرالية والبحث من بين أكثر من 300000 عميل للخطر. **اعتبارًا من 17 فبراير 2021**، تم اختراق العديد من العروض الرسمية، بما في ذلك الشركة

نفسها وست وكالات فيدرالية وحوالي 100 وكالة من القطاع الخاص. استخدم المتسللون الكأس لتوزيع البرامج الضارة عند التشغيل، مما قد يؤدي إلى إزالة العملاء وتوقف العملاء الدوليين عن التعامل مع شركة الإنترنت Solar Wind. – Solar Wind. **إلى جانب ذلك** فمنذ توقيع مايكروسوفت 10 ووكالة الأمن السيبراني والبنية التحتية حول هذه الاتفاقية في مارس 2021، لم تكن الصين تنوي بذل أي جهد للاختراق مثل Solar Wind Four، استغلت ثغرة سيادية لم يكتشفها الفنيون، وبفضلها تمكنت من إجراء عمليات تجسس وإحداث أضرار ذات آثار عالمية، تمكنت من الوصول إلى رسائل البريد الإلكتروني الأربعة الخاصة بهم – يوم الصفر – 0–يوم ضد Microsoft Exchange Server (خدمة البريد الإلكتروني) Microsoft Exchange السحابية .(CISA, 3 March,2021) و **في عام 2021، تم** إصدار تنبيهات وإرشادات مشتركة مع الجهات الرسمية المتعلقة بالأمن السيبراني مع شركاء الولايات المتحدة في الداخل والخارج، بما في ذلك مكتب التحقيقات الفيدرالي **(FBI)**، ووكالة الأمن القومي **(NSA)**، والفضاء الإلكتروني الأسترالي مركز الأمن **(ACSC)** المركز الوطني للأمن السيبراني في المملكة المتحدة **(NCSC)**. وصدرت تلك النشرات والإرشادات لتغطي العديد من الموضوعات حول التهديدات المستمرة للبيئات السحابية والبنية التحتية وسلاسل التوريد للجهات الفاعلة المهددة والضارة البرامج (Infrastructure & Cybersecurity Security Agency– Cisa, 1september 2021,Pp 19:20)،

4– على المستوى العسكري

وفقاً لتقرير المراجعة الصادر عن ممثل البنتاجون" في 30 يوليو عام 2019 مستعرضاً بعض ما جاء فيه، حيث يعد التقرير نافذة على جزء من مشكلة أكبر موثقة جيداً في وزارة الدفاع تتعلق بالأمن السيبراني متضمنة العديد من الاختراقات الضارة التي أسفرت عن حدوث خروقات كبيرة فقدت عبرها كم من المعلومات العسكرية، فضلاً على استمرار ضعف العديد من أنظمة الكمبيوتر العسكرية الأمريكية. **نجد المراجعة التي نشرها المفتش العام للبنتاجون في سبتمبر عام 2019** تأكيد على أثر تلك الاختراقات على القوة الأمريكية من خلال شراء موظفو وزارة الدفاع لآلاف الطابعات والكاميرات وأجهزة الكمبيوتر التي تحمل مخاطر أمنية إلكترونية معروفة، وفي إطار ذلك ذكر التقرير حصر تقريبي حول شراء ما يقرب من 9000 منتج من منتجات تكنولوجيا المعلومات المتاحة تجارياً في السنة المالي 2018، وأشار التقرير حول مدى خطورة عدم تحديد معيار أو الإشراف على عمليات الشراء هنا الكثير من المخاطر التي ستواجه

المنظمة الأمنية تتعلق بإمكانية استخدامها للتجسس أو اختراق الأفراد والمنشآت العسكرية الأمريكية. (Donnelly 2019).

انعكست تلك الاختراقات السابقة والاضطلاع على تطوير البرامج والبيانات، بل برامج القوات الأمريكية البحرية على تقييم صيني لقوتها ومقابل ومنافس لأخر تحديثات أمريكية. بل، ومنافسة خاصة في مسار تطبيقات الذكاء الاصطناعي الصيني في مجال البحرية الصينية وتطويرها المعدات لإضافة خدمات تصنيع قائم على الذكاء الاصطناعي منافس من قِبل الصين. بل، نجد أن تطورها السريع في تطوير العديد من الأسلحة يمثل وسيلة للردع الاستراتيجي ضد الولايات المتحدة خاصة في منطقة بحر الصين الجنوبي والشرقي أو فيما يتعلق بمسألة الأزمة التايوانية، **وكشف تقرير البنتاجون الصادر في سبتمبر 2020** أن جيش التحرير الشعبي يركز جهده بشكل خاص على تطوير الأسلحة المستقلة وأنظمة C2 الآلية. دون تقديم تفاصيل، يزعم التقرير أنه تم إحراز تقدم كبير في تطوير السفن السطحية غير المأهولة والدبابات غير المأهولة، بالإضافة إلى "الطائرات دون طيار المسلحة" التي تستخدم الذكاء الاصطناعي "لأداء التوجيه المستقل، وتحديد الأهداف، وتنفيذ الهجوم". وفي إطار تقدير الأثر الذي ستحدثه تلك الأنظمة **وفقاً لتقرير البنتاجون:** *"إن النصر في الحرب المستقبلية، وفقاً للاستراتيجيين في جيش التحرير الشعبي، سيعتمد على الجانب الذي يمكنه المراقبة والتوجيه واتخاذ القرار والتصرف بسرعة وفعالية أكبر في بيئة تشغيل ديناميكية بشكل متزايد". "ونتيجة لذلك، تسعى الصين إلى تطوير تقنيات جديدة مثل الذكاء الاصطناعي لدعم القدرات العسكرية المستقبلية، مثل أنظمة القيادة والسيطرة المستقلة (C2)، والتخطيط العملياتي الأكثر تطوراً وتنبؤياً، ودمج الاستخبارات والمراقبة والاستطلاع"* (ISR)). (OFFICE OF THE SECRETARY OF DEFENSE – DOD ,2020)، **والأثر من تلك التقنيات السابق ذكرها بإضافة الذكاء الاصطناعي لها سيلعب دوراً حاسماً بشكل خاص في التخطيط العسكري الصيني خاصة** إحراز الصين تقدماً في تطوير أنظمة C2 المتقدمة التي تستخدم الذكاء الاصطناعي "لجمع ودمج ونقل البيانات الضخمة لإدارة ساحة المعركة بشكل أكثر فعالية، وإنشاء مسارات عمل مثالية" من قبل القادة في الميدان. **وفي ذات السياق نجد أن الأثر المباشر** على دخول مثل تلك الدفاعات الصينية هي قيام شركة تحاول شركة Lockheed Martin شراء طائرة Aerojet Rocketdyne.في ديسمبر 2021، في صفقة قيمتها 4.4 مليار دولار. **على الرغم من وجود تخوفات أمريكية بالضرر الذي ينتج من احتكار الناعة ووقف لمنافسة عند تركيزها في يد شركة واحدة مثل لوكهيد إلا أن** الرئيس التنفيذي للوكهيد مارتن

"جيمس تيكليت "له راي آخر أن ذلك سيزيد من تطوير أنظمة الدفاع الأمريكية ومحاولة جعلها أشبه بأنظمة الدفاع الصينية وزيادة قدرات الدفاع الأمريكية (NAUGHTON, 2021).، نجد أن الصين دخلت سباق التسلح الفضائي عبر تقنيات الذكاء الاصطناعي فوفق تقرير أمريكي استخباراتي مسرب تقوم الصين ببناء أسلحة سيبرانية متطورة "للسيطرة" على أقمار العدو الصناعية، مما يجعلها عديمة الفائدة لإشارات البيانات أو المراقبة أثناء الحرب، **وذلك وفق استعراض صحيفة الفايننشيال تايمز لذلك التقرير المسرب**، تهدف الهجمات السيبرانية الأكثر طموحاً التي تشنها الصين إلى تقليد الإشارات التي تتلقاها أقمار العدو(المنافس الاستراتيجي) الصناعية من مشغليها، مما يؤدي إلى خداعها إما للاستيلاء عليها بالكامل أو تعطلها في أثناء اللحظات الحاسمة في القتال. وتعد الصين بتلك التقنيات قد قطعت شوط كبير وتقدم ملحوظ يمكنها من السيطرة على الفضاء وأقمار الاتصالات، **وقال الجنرال "بي تشانس سالتزمان"، قائد قوة الفضاء الأمريكية، للكونجرس في مارس 2023**، بتطوير قدرات مضادة للفضاء لتحقق حلماً لتصبح القوة الأولى خارج الغلاف الجوي، إضافة إلى ذلك نشر الجيش الصيني 347 قمراً صناعياً، بما في ذلك حوالي 35 قمراً تم إطلاقها في الفترة من بداية من أكتوبر 2022 إلى يونيو 2023 بهدف مراقبة وتتبع واستهداف ومهاجمة القوات الأمريكية في أي صراع مستقبلي. (Schwartz&Sevastopulo, 2023 & Srivastava)

إلى جانب الأُثر في الاختلال بالقوة الأمريكية السابق ذكره نجد أن هناك تأثير أخر مثل التأثير على خدمات الموانئ المتخصصة: فنجد أنها إضافة للترسانة التجارية والبحرية الصينية خاص العامة بالمحيطين الهندي والهادئ، حيث تطور الجيش الصيني قدراته في مجال الذكاء الاصطناعي باستخدامها فيما يتعلق بتحسين عمليات الاستحواذ والصيانة خاصة في مسار مبادرة الحزام والطريق البحرية حتى تلك الصين عقود الموانئ وتطويرها **إضافة إلى أسطول خدماتها عبر تلك الموانئ فيما يلي: (** Morgan,.Et Al ,2020)

أولاً: زيادة قدراتها بدراسة استخدام تطبيق جديد للتعرف على الصور لتحديد الشقوق في شفرات المروحيات، بتكليف من جيش التحرير الصيني لقواته البحرية، **ثانياً:** ذلك تفعيل نظام قادر على تحليل ما يقرب من 300 معدة من المعدات، وأيضاً من سجلات الصيانة لتمكين الصيانة التنبؤية، لاسيماً تساعد تلك الأنظمة في توفير نظام تحذيرات من الفشل الوشيك في الأنظمة الكهروميكانيكية"، **ثالثاً:** قامت القوات البحرية الصينية بمشروع لإنشاء "**نظام تصنيع ذكي للبيانات الضخمة** " للسفن الحربية، **إضافة إلى ذلك** يمكن

استخدامه في التعرف على الصور لتحديد أعطال الهيكل والنمذجة الثلاثية الأبعاد لتصميم السفن. **رابعاً:** إطلاق جيش التحرير الشعبي الصيني مشروعات لاستخدام البيانات الضخمة وتحليلات البيانات لتحسين محاكاة سلسلة التوريد وإدارتها، ودعم أقسام الأعمال في جيش التحرير الشعبي الصيني بمعلومات عن صناعاتهم ". إضافة إلى ذلك تستخدم الصين حاويات الشحن بالموانئ التي تتبعها، كمنصات إطلاق للصواريخ، وتعتبر بمنزلة حصان طروادة تستطيع بها تنفيذ هجمات في أي مكان بالعالم، عبر نظم التوجيه الذكية بالأقمار الصناعية (Congressional Research Service, 2023,P14)، **إجمالاً يمكن اختصار مجمل الاختراقات الصينية ومحورها في التأثير الحاضر والمستقبلي على القوة الأمريكية في المجال السيبراني إن لم يتم تحديثها:** في تصريح" تسنغ بيسو"، الزميل الباحث في معهد تايوان للدفاع الوطني و أبحاث الأمن (INDSR)، "إن موجة الحرب المعرفية خلال التدريبات العسكرية الحية الأخيرة في الصين لم تكن فريدة من نوعها. ووصف ذلك بأنه عرض أولي لـ "خطة الحرب الإلكترونية للصين" (CHAU And TING-FANG ,2022)، **فضلاً عن ذلك،** لا يعني استعراضنا لسجل الاختراقات وربطه بالتطوير الصيني بشكل عام، أن الصين لا تمتلك القدرة على التطوير والابتكار. على العكس لديها القدرة على إضافة ابتكارات وتحديثات متقدم، عبر تطوير أسلحة مختلفة معتمدة على الذكاء الاصطناعي ذاتية التوجيه أو إضافة ميزات أخرى لها تضعف من تأثير السلاح القابل لدي القوات الأمريكية وعلى الجانب السيبراني توفرت لدى الصين من هذه الخروقات للأمن السيبراني الأمريكي تدفقات معرفية ومعلوماتية في صورة بيانات خام ساهمت في تطورها في السوق الرقمي العالمي، لأن النموذج الصيني يكون متطرف وواضح في حالة دخول حرب تتعلق بسيادته القومية أو ما يعدّه جزء من سيادتها القومية لا يقبل فيه المساومة.

المبحث الثاني

استراتيجيات الأمن السيبراني للولايات المتحدة في مواجهة الاستراتيجية السيبرانية الصينية

تسعي الاستراتيجية الأمريكية دومًا في الحفاظ عي هيمنتها ومكانتها بالنسق الدولي، مؤخراً في ظل تصاعد بيئة المنافسة السيبرانية بين القوي المختلفة، وخاصة ما بين الصين والولايات المتحدة كفاعلين رئيسيين في هذا المجال، تهدف الاستراتيجية السيبرانية الأمريكية إلي حماية أمنها القومي، بناء تحالفات

دولية، والاستثمار في القدرات التقنية دوليًا وداخليًا، بدعم القدرات الدفاعية والهجومية عبر تعزيز التعاون بين القطاعين العام والخاص، في مقابل ذل سعي الصين لتعزيز نفوذها الجيوسياسي، وتنفيذ الهجمات السيبرانية وتطوير وتحديث صناعتها التقنية المحلية عبر شركاتها الوطنية ، ودعمها في بيئة المنافسة العالمية .

المطلب الأول

استراتيجية الأمن السيبراني من المنظور الأمريكي

يأتي تطوير الاستراتيجيات الأمريكية الخاصة بمجالات الأمن السيبراني ومواكبة التطورات التي تحدث بصورة سريعة في مسارات ومجالات تطوير أنظمة الأسلحة الفتاكة أو ما يعرف بأسلحة الجيل السادس المعتمدة على الذكاء الاصطناعي، وذلك في إطار الهدف الثابت من كافة الاستراتيجيات الأمريكية، هي معالجة القصور والحفاظ على مصالح الأمن القومي والدفاع عن الولايات المتحدة، بشكل شامل في ظل التنافس الدولي ووجود محاولات لمنافسة الولايات المتحدة. لذا كان هناك تساؤل يطرح حول ما المنظور الذي ترى به الولايات المتحدة قدراتها السيبرانية أو التحديات التي تمثلها القُوَى الآخرين خلال استراتيجيتها السيبرانية ؟، يصف مكتب الإدارة والميزانية – (The Office Of Management And Budget OMB)، ومع أنّ طرح الذكاء الاصطناعي في وزارة الدفاع الأمريكية لم يكن بجديد فقد روجها وزير الدفاع "تشاك هاجل" بدعم من خليفته "أشتون كارتر" تحت عنوان استراتيجية **الأوفست الثالثة**، ويقف وراء تقديم أو تشكيل فريق البنتاجون الخوارزمي أو السيبراني للحرب المتعددة هي المنظمة المسؤولة عن مشروع "**مافن**"، وتتلخص نهج الحرب السيبرانية التي تم طرحها على" آلية قائمة على تسخير وتفعيل الأنظمة الخوارزمية التي تدعم الذكاء الاصطناعي وتوظيفه في إدارة النزاعات طويلة الأمد. " Morgan، (Et.Al,2020)، لذا تتولى الوكالات الفيدرالية " **الأمن السيبراني**" ويتم تعريفه بأنه " منع الضرر وحمايته واستعادته أجهزة الكمبيوتر، أنظمة الاتصالات الإلكترونية، خدمات الاتصالات الإلكترونية، الأسلاك الاتصالات والمراسلات الإلكترونية، بما في ذلك المعلومات الواردة فيها، لضمان توافرها وسلامتها وتوثيقها وسريتها وعدم إنكارها. " (Office Of Management And Budget, 2016,P28).

أولاً، في إطار الاستراتيجية الأمريكية في الفترة من 2011-2019

- **استراتيجية 2011:** وفق لشهادة لجاكلين شنايدر، زميل هوفر، معهد هوفر، بجامعة ستانفورد، جلسة استماع بالكونجرس في 22 فبراير 2022 : تمثل استراتيجية 2011 أو استراتيجية إلكترونية حقيقية لوزارة الدفاع، حددت بها أولويات الدفاع في المجال السيبراني، وجدير بالذكر أن تلك الاستراتيجية لم تحدد أو تسمي أية خصوم كما في الاستراتيجيات اللاحقة، إنما نتيجة جاءت فيها تحديد لعدد من التهديدات غير الحكومية والتهديدات السيبرانية، عمومًا تلك التي يمكن تهدد أن الدولة القومية في صورتها العامة، ويرجع البعض أن ذلك نتيجة عدم اليقين حول طبيعة وحدود الدور الذي يجب أن تمثله الولايات المتحدة أو بشكل أخر ما هي طبيعة الدور المنوط بالجيش الأمريكي أن يلعبه في الفضاء الإلكتروني. (The U.S.-China Economic And Security Review Commission,2022) ، **جاء المنظور الأمريكي** بهذه الاستراتيجية في التأكيد على الأمن للمعلومات وضرورة ربطه بفكرة الحرية الشخصية دون عوائق حكومية وعدم تغذية **وهم الأمن** أو خنق التدفق للمعلومات المعيق للتعاون الدولي، حيث تؤكد على إن الانغلاق أو الرقابة المتشددة على المعلومات أو وسائل التواصل لا توفر الأمن، وإنما تغذي هواجس فكرة الأمن الوهمي وتقوض المبادئ الديمقراطية الأمريكية مع أنّ الصعوبات التي تواجه الدول في تطوير تدابير أمنية قوية، ويأتي في إطار التأكيد على ذلك تناول الولايات المتحدة نهج في بناء استراتيجياتها على فكرة الانفتاح في المعلومات كامتداد لديموقراطياتها (The White House, 2011,P3:P5).، حيث كانت إدارة أوباما تعمل على نهج الردع الدبلوماسي ودعم القوات العسكرية في بناء وتعزيز التحالفات العسكرية، في ظل احتفاظها بجميع الخيارات والوسائل للرد المناسب وفق للقانون الدولي المعمول به. وضعت إدارة أوباما والمبادئ المعيارية المفصلة حول السلوكيات المناسبة في الفضاء السيبراني مثل القاعدة ضد الهجمات على البنية التحتية الحيوية، والتركيز على نشر هذه المعايير داخل الأمم المتحدة والعلاقات بالحلفاء (Kerry,2015)، وتلك القواعد التي تعمل حالياً روسيا والصين على تغييرها لأنها تُرسي أساس قوي للهيمنة الأمريكية على الفضاء الإلكتروني وفقًا للمنظور الأمريكي ومصالحه.
- **استراتيجية 2015:** استكمالاً للاستراتيجيات تركز استراتيجية عام 2015 على استخدام بين الرد استخدام القوة العسكرية بين الرد على تهديد الدولة والتهديد من غير الدول، ويؤكد على أهمية

التعامل مع الجهات الفاعلة في الدولة، إضافة إلى ذلك نرى تركيز أهداف الاستراتيجية المتمثلة في تدريب القُوَى العاملة السيبرانية، بناء القدرات التقنية، وتقييم جاهزية قوة المهمة السيبرانية هي خطوة نحو تحسين منهجي للوعي السيبراني والمعلوماتي في العقيدة العسكرية. DEFENSE TECHNICAL INFORMATION CENTER) (DTIC., 2015,Pi-، وتعد هذه الاستراتيجية محددة لقدرات وزارة الدفاع وواقعها في مسألة الردع والدفاع بالفضاء الإلكتروني، حيث شهدت نمواً في تطوير فرق جيدة للمهام السيبرانية حوالي 133 فريقاً متخصصاً مكون من حوالى 6000 فرداً، بجانب بدأت أربعة ألوية أو وحدات في التجهيز للخدمة الإلكترونية أو الدفاع الإلكتروني، بالإضافة إلي ذلك تدريب القوات السيبرانية وتشغيلها لدعم العمليات الجوية والبرية والبحرية. U.S Department Defense), (2018 ، وتعد هذه الاستراتيجية الأولي لتحديد الخصوم ذوي الأولوية هم روسيا والصين وإيران والشمال كوريا، بالإضافة إلي تحديد الجهات الفاعلة غير الحكومية، ومن ثم توضيح مسؤوليات وزارة الدفاع داخل الحكومة الفيدرالية ؛ وأبرزها الردع والدفاع من أجل الحفاظ على الهيمنة الأمريكية خاصة في المجال السيبراني. -The U.S.) China Economic And Security Review(Commission,2022,P205، واستمرت الاستراتيجية في إتباع نهج أوباما في العمل على ضبط النفس وخلق مجال إلكتروني ذو مرونة يمكن العمل، إلا أن الإفراط في الاعتماد على التكنولوجيا يجعلها عرضة لأن تكون دومًا في حالة خصومة يمكن عبرها تحييدها وأنظمتها المتقدمة، لذا فضلت إدارة أوباما أسلوب القيادة من الخلف أو بالوكالة (Department Of Defense- DOD, 2018)، أي تصدير الحلفاء والشركاء للولايات المتحدة في التصدر لمواجهة مثل تلك الهجمات دون إحداث اصطدام أو مواجهة مباشرة قائمة على الردع الدبلوماسي، لأن إدارة أوباما كانت تفترض أن الهجمات كانت تتم في صورة تصعيدية وفُعِلَت في الاستراتيجيات السابقة ركز على ردع الأحداث السيبرانية والاستجابة لها، لكل حدث على حِدَةٍ، لأن كانت التركيز في فترتي أوباما على بالأساس على "نهج فيدرالي للفضاء السيبراني "، حيث حدد الأدوار والمسؤوليات الأساسية لـ وزارة الدفاع، وزارة الأمن الوطني، وزارة الخارجية، ومكتب التحقيقات الفدرالي / وزارة العدل (Committee On Armed Services,2017).

- **استراتيجية 2018** : جاءت إدارة ترامب وقد تسلمت قدر من تخوفات إدارة أوباما في ظل تصاعد حملات التضليل لانتخابات 2018 والاختراقات المختلفة، كانت هناك حوافز ودوافع خاصة من خلال القطاع الخاص ووزارة الدفاع من أجل تفعيل استراتيجية سيبرانية أكثر نشاطاً وفاعلية عن السابقة، إلا أن إدارة دونالد ترامب اختارت مسار آخر قائم على إعادة كتاب الاستراتيجيات الإلكترونية، أسفرت في تركيزها على الصين وروسيا كمحور لتخطيط ودفع بالجهود السيبرانية، أدى ذلك إلى إيجاد استراتيجية نشطة عرفت باسم "**المشاركة النشطة**"، وقائمة على المخاطرة أو إدارة المخاطر عبر مفهوم الدفاع من الأمام Defend Forward ، ومواجهة الخصوم قبل حدوث الهجمات الإلكترونية، والعمل على تعطيل وقف النشاط السيبراني الضار من منبعه، بما في ذلك النشاط الذي يقع دون المستوى الصراع المسلح، **ووفقاً لمجلس علوم الدفاع (DSB) فرقة العمل المعنية بالردع السيبراني، وزارة الدفاع، فبراير " :2017 ولا** تحتاج الولايات المتحدة إلى الثقة بنسبة 100% لتوفير الردع الفعّال. ومن الأفضل للقادة التركيز أولاً على تقليل ثقة الخصم في قدرته على تعطيل أنظمتنا أو حرمانها منها. وفي إنشاء مجموعة من البرامج لتعزيز الأمن السيبراني ومرونة الأنظمة العسكرية وغير العسكرية الرئيسة، يشكل الشعور بالأولويات والشعور أو إدراك بما هو ومدي" القدر الكافي" ضرورة أساسية". (Defense Science Board (DSB), 2017) ، لأن اعتقاد إدارة ترامب بقدر ما توفر لديها من تقارير أن مخاطر الهجمات تفوق مخاطر التصعيد، وأسفر ذلك عن تفويض إدارة ترامب لمزيد من الصلاحيات للجيش الأمريكي، بالإضافة إلي ذلك صياغة الهدف الرئيسي لوزارة الدفاع للعمليات السيبرانية الهجومية والدفاعية على إنها مشكلات ما قبل الصراع وغير جغرافية، أسفر ذلك عن توفير مساحة للتخطيط وتنفيذ الحملات السيبرانية من قبل القوات الأمريكية (The U.S.-China Economic And Review Security Commission,2022,Pp205-221).، نتيجة لذلك ركزت الاستراتيجية الأمريكية -استراتيجية 2018 الوطنية- على المنافسة الاستراتيجية بين الدول، وليس الإرهاب، هي الآن الشغل الشاغل للأمن القومى الأمريكي. فالصين منافس استراتيجي يستخدم الاقتصاد المفترس لتخويف جيرانه بينما يقوم بعسكرة السمات في بحر الصين الجنوبي، **وفي إطار تقييمي** من قبل الولايات المتحدة جاءت نتائج تقرير نشر دراسة في 2018 من قبل منظمة وزارة الدفاع المسؤولة عن " نشر التكنولوجيا التجارية وتوسيع نطاقها "وتوسيع نطاقها" لأغراض الأمن القومى والأغراض

العسكرية، (DIU)، دراسة عن استراتيجية نقل الصين للتكنولوجيا، محفزة أو منبه للوضع القائم لاستراتيجيات أو بصورة أدق تقيم التطور الصيني مقابل الأمريكي في مجال التكنولوجيا والذكاء الاصطناعي، تركزت أهم النتائج حول زيادة الاستثمارات الصينية في تقنيات المستقبل الحاسمة والتي ستكون أساس الابتكارات المستقبلية لكل من التطبيقات التجارية والعسكرية للذكاء الاصطناعي، ذلك بالإضافة لتوقع ذات التقرير أن تلك التقنيات المستقبلية قائمة بالأساس في نسبة غير قليلة منها على سرقات الملكية الفكرية الأمريكية مقدرة ب 300 مليار دولار سنويا، وترجع نتائج التقرير إلي إنه ليس لدى الولايات المتحدة سياسة شاملة، أو وجود أدوات لمعالجة هذا النقل الضخم للتكنولوجيا في الصين، فضلاً عن عدم وجود النظرة الشاملة لدى حكومة الولايات المتحدة عن مدى وسرعة حدوث نقل التكنولوجيا الأمريكية في ذلك التوقيت أو ما هي التقنيات التي يجب على الحكومة الأمريكية حمايتها(Mcnally,2021)، **بالرغم من أن القيادة الأمريكية السيبرانية** تعد نموذجاً يحتذي به عالميًا، إلا إنها تواجه تحديات سيبرانية متزايدة من الصين، لتفوق الصين بتطويرها لمبادرة الحزام والطريق التي تتنوع تحتها المبادرات والمشاريع متفوقة بذل علي مشروع مارشال الأمريكي فعند قياس القدرات السيبرانية للصين مقارنة بالولايات المتحدة يصبح الأمر معقداً حيث لا تمتلك أمريا أكبر قوة بشرية في المجال السيبراني، مقارنة بما تمتلكه الصين حيث يعمل في جيش التحرير الشعبي الصيني حوالي 50 ألف فرد مقابل 6 آلاف فرد في الجيش الأمريكي.(Schneider Et.Al,2020)، إلا أن تلك المعضلة قد حلتها الصين بتفعيل استراتيجية الدمج العسكري– المدني، إلا أن لازالت الإدارات الأمريكية تجد صعوبة في تحقيق ذلك الدمج بين وزارة الدفاع القطاع الخاص، نظراً لصعوبة بناء الثقة في إعطاء تصريحات للاطلاع على المعلومات ذات السرية وغير متاحة للعامة، ولكن تم إيجاد صيغة أخرى في أتمتة المعلومات وتبادل التعاون بين الوكالات المختلفة بالحكومة الأمريكية. (Schneider, 2022)، وعليه قدمت استراتيجية 2018 مفهوم " الدفاع من الأمام forward defense" أو المشاركة المستمرة كأفضل نهج في إدارة الصراع أو المنافسة مع الصين، حيث ركزت على الاستراتيجية الأمريكية على إتباع نهج مرن وفعال في مواجهة القدرات الصينية، عبر تعزيز القدرات السيبرانية الدفاعية والهجومية الأمريكية.

ثانياً، إطار الاستراتيجية الأمريكية في الفترة من 2020-2022.

ناهيك عن النهج الأمريكي السابق إلا إنه وفقاً لواشنطن بوست إن كثير من الغموض يجري حول النشاطات التجسسية الأمريكي ضد بكين في إطلاق إدارة بادين في مطلع 2021 موجة من التدابير لتحييد بعض معارضيه، وزيادةً على ذلك نجد أن بعض تلك التدابير تصب في عمق العلاقات التجارية المعقدة ما بين واشنطن وبكين (سليمان والجعفري، 2023)، إلا إدارة بايدن أن استمرت في نفس النهج للاستراتيجية السيبرانية الأمريكية 2018 مع إزالة بعض القيود كما فعل ترامب على تنفيذ هجمات تجسسية مضادة، إلا أن الإطار العام **للاستراتيجية السيبرانية لترامب جاءت قائمة على 4 ركائز رئيسة: أولاً:** تعزيز الأمن القومي الأمريكي من خلال تنسيق المعلومات ما بين الوكالات الفيدرالية، **ثانياً:** تعزيز الاقتصاد الأمريكي الرقمي، بتشجيع الابتكار في قطاع التكنولوجيا، **ثالثاً:** مكافحة التهديدات السيبرانية، من خلال استخدام كافة أدوات القوة الأمريكية، رابعاً: تزويد حلفاء الولايات المتحدة بقدرات سيبرانية؛ للتعامل مع التهديدات السيبرانية التي تستهدف المصالح المشتركة والدعوة إلى حرية الإنترنت في جميع أنحاء العالم. إجمالاً، نجد الاستراتيجية الأمريكية للأمن القومي 12 أكتوبر لعام 2022 تتلخص في التالي: (The White House, 12 October. 2022).

جاءت الاستراتيجية كتلخيص فعلى لما عملت عليه إدارة بايدن على تنفيذها خلال العامين السابقين من مواجهة المنافسة الاستراتيجية على المكانة والهيمنة الأمريكية بالنسق الدولي **جاءت بعض النقاط لمواجهة التحديات الجديدة التي تواجهها عبر رؤيتها** : من استمراريتها للحفاظ على المصالح الحيوية الأمريكية والتغلب على المنافسين الجيوسياسيين على رأسهم الصين وروسيا بكافة الوسائل والأدوات المتاحة من خلال تحسين ومعالجة المشاكل الداخلية الأمريكية **أولاً** عبر تعزيز القدرات الأمريكية الاقتصادية والتكنولوجية العسكرية، **ثانياً** من خلال الرؤية الأمريكية التي تهدف إلى التعاون مع الحلفاء، إلى جانب مواصلة العمل على تعزيز قدرات الردع والسعي إلى الحفاظ على استقرار النظام الدولي مع الحلفاء بخلق نسق دولي مستقر وآمن بعيداً عن سيطرة النظم أوتوقراطية، والتوجه نحو تعزيز مكانة الولايات المتحدة العالمية ومصداقيتها عبر استخدام الأدوات الدبلوماسية مع الدول التي تتشارك نفس الرؤية مع الولايات المتحدة، بالإضافة إلي تكريس الترتيبات الاقتصادية مع الحلفاء والشركاء عبر الحفاظ على قواعد التجارة العالمية وغيرها. مثال على ذلك الشراكة الأمريكية مع منظمة الآسيان أو رابطة جنوب شرق آسيا والولايات المتحدة في إطار الشراكة الاستراتيجية في إطار التعاون ما بينها خاصة في التنمية الرقمية والأمن السيبراني

وغيرها من المجالات خاصة إعلان إدارة بايدن عن تقديم ما يصل عن 102 مليون دولار أمريكي لتوسيع الشراكة الاستراتيجية بين دول جنوب شرق آسيا في المحيطين الهادي والهندي والولايات المتحدة وفي القمة الخامسة بواشنطن أعلن الرئيس بايدن عن 150 مليون دولار أمريكي في برامج رابط الآسيان أمم جنوب شرق آسيا التي تم دمجها مع أكثر من 800 مليون دولار أمريكي مطلوبة في السنة المالية 2023 للبرامج الثنائية في الدول الأعضاء في رابطة أمم جنوب شرق آسيا، وأكثر من 12 مليار دولار أمريكي في المساعدات التنموية والاقتصادية والصحية والأمنية منذ عام 2002، كل هذا الدعم في مقابل تطويق الخطر الاستراتيجي الصيني، وبصورة خاصة ومواجهة مبادرة الحزام والطريق في شقها التكنولوجي بصورة خاصة.(The White House , 12 November,2022)، **وتأتي عبر** تعزيز الأمن السيبراني وحماية الشبكات، حتى إعلان الاستراتيجية الجديدة للأمن السيبراني في مارس 2023 صرح الرئيس جو بايدن أن إدارته أنفقت على البنية التحتية للإنترنت باستثمار 65 مليار دولار للتأكد من أن كل أمريكي لديه إمكانية الوصول إلى الإنترنت الموثوق به عالي السرعة. (The White House,1 March،2023)، إلى جانب تعيينه في أغسطس 2022 إعلان الرئيس بايدن تعيين قادة صناعيين وحكوميين مؤهلين تأهيلاً عالياً متنوعين كأعضاء في المجلس الاستشاري الوطني للبنية التحتية (NIAC) التابع للرئيس، الذي يقدم المشورة للبيت الأبيض حول كيفية الحد من المخاطر المادية والإلكترونية وتحسين الأمن والبنية التحتية. مرونة قطاعات البنية التحتية الحيوية في البلاد. (The White House, 31 August, 2022)، ولا تزال إدارة بايدن تعتبر الصين وروسيا وكوريا الشمالية أسوأ المنتهكين للأمن السيبراني الأمريكي وتمثل تلك النقطة استمرارية لما ذكرته إدارة ترامب أيضاً لازالت إدارة بايدن تعتبر الأمر ذاته عبر التصريحات المختلفة من عام 2020 حتى عام 2023 لازالت إدارة بايدن تؤكد على الأمر نفسه عبر التصريحات الرسمية المختلفة، حيث جاءت استراتيجية مارس 2023 بشكل واضح " تشير الاستراتيجية إلى أن الصين وروسيا وإيران وكوريا الشمالية هم أسوأ المنتهكين عندما يتعلق الأمر "**بالاستخدام العدواني للقدرات السيبرانية المتقدمة**" ضد الولايات المتحدة. ومع ذلك، فإن الصين هي التي تعتبرها حكومة الولايات المتحدة أخطر تهديد، مدعية: "تمثل جمهورية الصين الشعبية الآن التهديد الأوسع والأكثر نشاطاً والأكثر استمراراً لكل من شبكات الحكومة والقطاع الخاص وهي الدولة الوحيدة التي لديها نية لإعادة تشكيل النظام الدولي، وبشكل متزايد، على الصعيد الاقتصادي والدبلوماسي. والقوة العسكرية والتكنولوجية للقيام بذلك "" (The White House,1 March 2023,P3).

المطلب الثاني

توازن القوى بالنسق عبر تعاون مشترك بين الولايات المتحدة وحلفائها في مواجهة القوة الصينية

جاءت العديد من الإجراءات الاستراتيجية لمواجهة التفوق الصيني السيبراني المؤثر على القوة الأمريكية بالنسق الدولي سواء كانت على مستوي التطوير الداخلي أو مستوي التحالفات الدولية بالنسق.

أولاً، على المستوى التطوير الداخلي للقوة السيبرانية التي تدعم الاستراتيجية الأمريكية:

بعد أحداث إغلاق خط أنابيب كولونيال بايبلاين–Colonial Pipeline، أشار إلى استعداده للعمل مباشرة للرد على المهاجمين وتلك الخطوة التي ترددت إدارة أوباما في اتخاذها خلال اختراقات الانتخابات عام 2016، وجدير بالذكر قد صرح بايدن بصورة واضحة: « سنتخذ أيضاً إجراءً لتعطيل قدرتهم على العمل»، وهي عبارة تشير على ما يبدو إلى أن القيادة السيبرانية للولايات المتحدة، وهي قوة الحرب السيبرانية العسكرية (U.S.Congress , 20 July, 2021)، **وفي ذات الإطار** استكمالاً للإجراءات التطويرية التي اتخذها الكونجرس في 2018، وجدير بالذكر أن مركز الذكاء الاصطناعي المشترك (JAIC) الذي تتمثل مهمته في تنسيق وتطوير ونشر الذكاء الاصطناعي المتعلق بوزارة الدفاع عبر تنشيط استراتيجية تسريع تبني الذكاء الاصطناعي وإنشاء قوة مناسبة لعصرنا، **عبر إتباع نهج ثلاثي الأبعاد لتطوير الذكاء الاصطناعي** قائم على: **أولاً،** المؤسسات التكنولوجية، **ثانياً،** دعم المهام، **ثالثاً،** الذكاء الاصطناعي التشغيلي، تعد أهم مهام ذلك المركز في تحسين الاختلالات بالقوة الأمريكية التي تحدثها مؤسسات تكنولوجيا الذكاء الاصطناعي الصيني على سبيل المثال دعم لمهام الذكاء الاصطناعي تُعلق أي نظام من تطوير العمليات القتالية، إلى جانب ذلك تحليل كميات ضخمة من البيانات والمعلومات في ثواني تساعد في دعم القرارات التطبيقات الصناعية سواء مدنية كانت أو عسكرية" (Mcnally,2021)، **وفي ذات السياق** قد سمح **قانون "جون.س. ماكين"** عام 2019، بإنشاء لجنة الأمن القومي للذكاء الاصطناعي (CCAI)، وتتمثل مهام هذه اللجنة في تعزيز وتطوير الذكاء الاصطناعي وغيرها من التقنيات المختلفة، إلى جانب مراجعة سياسات الذكاء الاصطناعي من قدرة الولايات المتحدة على التطوير والبحث العلمي في ذات المجال إلى تقييم المخاطر والأخلاقيات المرتبطة بالمجال، وذلك بالإضافة إلي مهمتها الرئيسة في الدفاع عن الولايات المتحدة والحفاظ على تفوقها في مجال الذكاء الاصطناعي . (Schmidt, Et Al ,2021)

ثانيًا: على مستوى التنسيق مع الحلفاء بالنسق الدولي:

تم اقتراح في تقرير لجنة لمراجعة تعريف جديد وفي إطار التحديث بعد عدد كبير من هجمات الفدية على منشئات البنية التحتية، اقترحت لجنة Cyberspace Solarium أيضاً أن يقوم الكونجرس بتدوين مفهوم "البنية التحتية الهامة بشكل منهجي" (SICI) حيث "الكيانات المسؤولة عن الأنظمة والأصول التي تدعم الوظائف الحيوية الوطنية مضمونة الدعم الكامل من الولايات المتحدة. الحكومة وتتحمل متطلبات أمنية إضافية تتوافق مع وضعها الفريد والأهمية. كيانات SICI هي الأجزاء الأكثر أهمية في بنيتنا التحتية الحيوية." (The U.S.-China Economic And Security Review Commission. 2022, Pp65:83)، وتبعًا لذلك تطرقت الاستراتيجية إلى تعزيز آليات وسائل والدفع بالاستثمارات العالمية لتعزيز الأمن السيبرانى، بالإضافة إلى العمل على بناء بنية تحتية رقمية قوية، والتي يترتب عليها حماية الشبكة الرقمية لسلاسل التوريد، وسد الفجوة الرقمية ما بين البلدان المختلفة بدرجات اقتصادها من الغنية إلى المتوسطة إلى الفقيرة في دخلها، مع الحفاظ عند تطبيق ذلك الأمر على القيم الأمريكية من حماية الديموقراطية وحماية حقوق الإنسان وعدم انتهاك الخصوصيات، إلى جانب وضع إطار لمحاسبة مجرمي الإنترنت. **وتعقيباً على تلك النقطة**، بالقطع لا ينطبق تطبيقه مع المخترقين أو المنتهكين للخصوصيات أو الشبكات الأخرى التابعين للولايات المتحدة وحلفاؤها، فكل دولة ترى منظور حماية أمنها القومي وفق متطلباتها ومعاييرها تختلف عندما يتعلق الأمر بأمنها القومي أو مصلحتها. ويمكن تفسير ذلك فقد جاءت الاستراتيجية الأمريكية لإدارة بايدن استمرارية لها كمبادئ عامة وفي ذلك الإطار **وتفسيرا لذلك فيما يلي: فوفقاً للفريق تشارلز مور، نائب قائد القيادة السيبرانية الأمريكية، لمجلة يونيباث- Unipath- Magazine (مور، 2022):**

وفي إطار استمرارية العمل بالركيزة الأخرى، وهي تزويد حلفاء الولايات المتحدة بقدرات سيبرانية؛ جاءت مساعدة القيادة السيبرانية الأمريكية عبر تطوير شراكات ضمن إطار عمل الدفاع الجماعي مع حلفاء الولايات المتحدة عبر ما يعرف باستخدام "**عمليات البحث المتقدم**" ويتم ذلك عبر فرق الكشف عن الأنشطة السيبرانية الخبيثة ثم يتم نشر الوعي عنها وإبلاغ الدول الشريكة مع ملاحقة هذه الأنشطة عبر شبكات هذه الدول، ناهيك عن جمع المعلومات الاستخباراتية القيمة وتحييد التهديدات المحتملة لشبكات الولايات المتحدة والبلدان الشريكة لها إلي جانب ذلك عبر الفرق السيبرانية والمعلومات التي تم جمعها يتم تزويد الدول الشريكة بها ورفع قدراتها السيبرانية وتعريف المجتمع السيبراني العالمي بالثغرات والاستراتيجيات

والأساليب والإجراءات. التي تتخذها الجهات المعادية، بالإضافة إلى أدلة على محاولة البرامج الخبيثة اختراق الأنظمة. **جاء التركيز** من إدارة بايدن على إحراز الأهداف الاستراتيجية وعملاً بالركيزة لاستراتيجية السيبرانية القائمة على مكافحة التهديدات السيبرانية، من خلال استخدام كافة أدوات القوة الأمريكية، التالية حيث عملت الوكالات الحكومية الأمريكية العزم في انتخابات 2020 على منع الأنشطة السيبرانية التي تسبت في اختراقات للانتخابات الأمريكية عامي 2016 و 2018 و2020، حيث شكلت خلالها فريق تعاوني بناء على استراتيجية 2018 القائمة على الركائز الاستراتيجية القائمة على تعزيز الأمن القومي الأمريكي من خلال تنسيق المعلومات ما بين الوكالات الفيدرالية عبر: " تشكيل فريقاً تعاونياً متعدد المهام لتحديد التهديدات وتبادل المعلومات وتنسيق الإجراءات؛ وهذه الوكالات هي وكالة الأمن السيبراني وأمن البنية التحتية، ومكتب التحقيقات الفيدرالي، ووكالة الأمن القومي، والقيادة السيبرانية الأمريكية"(مور، 2022)، **وفي ذات السياق** أطلقت الإدارة الأميركية مشروع "**مراجعة الأمن**" :وفي إطار الجدل بأن منصة تيك توك الصينية تراجع بايدن مثل ترامب عن اتخاذ أي إجراءات عقابية ضدها، نظراً لأنها كانت في فترة الانتخابات وخشيت إدارة بايدن من خسارة قطاع كبير من الأجيال الشابة المستخدم لتيك توك." (سليمان والجعفري، 2023)، بالإضافة إلى تحسين الشراكات الدفاعية الجماعية التي تقودها الولايات المتحدة والتي هدفها رفع القدرة على التوافق العملياتي والاستعداد في حال حدوث هجوم سيبراني لاكتشاف أية ثغرات في العمل الجماعي، جاء تطبيق ذلك في استضافة القيادة السيبرانية الأمريكية في نوفمبر 2021 أكبر تمرين سيبراني مشترك ومتعدد الجنسيات، حيث يتضمن ذلك التدريب حوالى 23 دولة عبر تدريب 200 محارب سيبراني من تلك الدول، وبطبيعة الحال تهدف هذه الترتيبات على اختبار، وتنمية المهارات والقدرات الدفاعية لتلك الدول عبر متدربيها. (مور، 2022)، **وفي ذات السياق** ومع زيادة الاختراقات كانت هناك زيادة ملحوظة في الاختراقات الإلكترونية التي تنشأ في الصين وتستهدف أنظمة الكمبيوتر الأمريكية والدفاع ذات الصلة خاصة في تحييد وغلق محطات الكهرباء الأمريكية (Gorman,2009,)، وخطوط أنابيب النفط المركزية وغيرها يُظهر حجم الهجمات السيبرانية، وهجمات برامج الفدية في عام 2021 وحده أنه لا يوجد أحد محصن ضد الجهات الفاعلة السيبرانية التابعة للدولة أو مجرمي الإنترنت. **لذا، لزيادة صلابة الدفاع الأمريكي في الفضاء السيبراني،** عملت إدارة بايدن عبر القيادة السيبرانية على إقامة شراكة متينة مع القطاع الخاص، عبر برنامجين أساسيين: " "أندر أدفايزمنت" و "دريم بورت"، أما "أندر أدفايزمنت" فهو برنامج من برامج القطاع الخاص لتبادل المعلومات يتصف بأنه علني وتطوعي ويخدم الطرفين. وأما

"دريم بورت" فهو مركز ابتكار غير سري يسمح للقيادة السيبرانية بالتفاعل مع أعضاء القطاع والأوساط الأكاديمية لتبادل الأفكار وتقديم حلول مبتكرة لمشكلات الأمن السيبراني. وكلا البرنامجين إسهام مباشر في قدرة القيادة السيبرانية على الدفاع عن وطننا في الفضاء السيبراني ومواصلة النمو نطاقاً وحجماً. (مور،2023) . **واستكمالاً** للإجراءات الداعمة للاستراتيجية السيبرانية في أبريل 2022، أطلقت الولايات المتحدة و60 دولة إعلان مستقبل الإنترنت (DFI)، الذي يجمع تحالفاً واسعاً ومتنوعاً من الشركاء – وهو الأكبر من نوعه – حول رؤية ديمقراطية مشتركة لمجتمع منفتح وحر. مستقبل رقمي عالمي وقابل للتشغيل البيني وموثوق وآمن. وإجمالاً تأتي الاستراتيجيات السيبرانية الأمريكية مكملة لأهدافها بغض النظر عن الانتماء الحزبي للإدارة من جمهوري أو ديموقراطي إلا أن العامل المشترك من خلال الاستمرارية في تحقيق أهداف الأمن القومي الأمريكي، وذلك نراه لاحقاً عند الإعلان عن الاستراتيجية الأخيرة للأمن السيبراني في مارس 2023 (The White. House 1 March,2023,P29)، **نجد أنها تمثل تلخيص** ذلك أيضاً بالخطوات السابقة والتي تم استكمال أكثر من 60% منها عبر الاستراتيجيات السابقة، ولكن بأدوات محدثة أكثر وبشراكات أوسع استراتيجية وطنية جديدة للأمن السيبراني تهدف إلى "تأمين الفوائد الكاملة لنظام بيئي رقمي آمن لجميع الأمريكيين ". وفيما يلي أهم النقاط " نهجنا: الطريق إلى المرونة في الفضاء الإلكتروني سيكون التعاون العميق والدائم بين أصحاب المصلحة عبر نظامنا البيئي الرقمي هو الأساس الذي نجعله أكثر قابلية للدفاع عنه ومرونة ومتوافقاً مع القيم الأمريكية. تسعى هذه الاستراتيجية إلى بناء وتعزيز التعاون حول خمس ركائز: (1) الدفاع عن البنية التحتية الحيوية، (2) تعطيل وتفكيك الجهات التهديدية، (3) تشكيل قِوَى السوق لتعزيز الأمن والمرونة، (4) الاستثمار في مستقبل مرن، و (5) إقامة شراكات دولية لتحقيق الأهداف المشتركة. ويتطلب كل جهد مستويات غير مسبوقة من التعاون بين مجتمعات أصحاب المصلحة المعنيين، بما في ذلك القطاع العام والصناعة الخاصة والمجتمع المدني والحلفاء والشركاء الدوليين." (The White House 1 March,2023,P4)

الخاتمة

تسعى الدول الكبرى إلي تعظيم قوتها لزيادة هيمنتها على النسق الدولي، هي نتاج لتصعيد الذي قاده الرئيس شي جين بينغ في الخطاب الصيني بشكل كبير عبر ضرورة تطوير وتقوية قدرات الصين السيبرانية، الفضاء ليس أرضاً يمكن التحكم بها و بأبعادها المختلفة و لكن كافة الكيانات من دول ومؤسسات رسمية وغير رسمية والجماعات والأفراد وكل من له وصول بالإنترنت في ظل الاقتصاد الخاضع للعولمة

الذي يمتلك الجميع ممارسة لسلطة التحكم بالإنترنت نجد أن أكبر مزودي الخدمات السيبرانية أو البنية التحتية للإنترنت هم من القطاعات الخاصة أو العابرة للقوميات وغيرها. نظراً لرؤية الصين الاستراتيجية أن الحرب الإلكترونية أداة مفيدة للغاية ورخيصة وفعالة من حيث التكلفة لتغيير ديناميكيات العالم، أدى الاستثمار في القدرات السيبرانية الهجومية للصين بمنحها سلاحاً رئيساً في ترسانتها لممارسة نفوذها في النسق العالمي. وانعكس ذلك على زيادة الجهود التي تبذلها الدول في جميع أنحاء العالم لتعزيز قدراتها الإلكترونية نتيجة تزايد تهديد الحرب الإلكترونية مع تصاعد كثافة الاستثمار في قدرات الحرب الإلكترونية بين القُوَى الكبرى. ففي عام 2019 فقامت تايوان عبر المعهد الأمريكي في تايوان – الذي يمثل المصالح الأمريكية في الجزيرة – وليس الجيش الأمريكي، فضلاً عن استخدام قطاعاتهم الخاصة للعمليات السيبرانية والتنصل من أي إسناد للهجمات التي تتم برعاية الحكومة الصينية بشكل قاطع، إلا أن الصين استطاعت أن تمكن روافع مجتمعية غير رسمية ترعاها عبر تمكين مقاولو الأمن الهجوميين من القطاع الخاص والمؤسسات الأكاديمية، حيث قامت بإنشاء القيادة السيبرانية الأمريكية والتي قامت بتدريب شامل لحوالي 60 دولة في 2021 لتحسين قدرات الاستعداد والاستجابة السيبرانية للدول في حالة حدوث هجوم سيبراني كبير، من المرجح أن يكون الصراع وخاصة العسكري منه بنفس الأسباب التي أدت للحروب سابقاً ولكن الطرق التي تشن بها تلك الحروب وتدار بها الصراعات سوف تتغير مع ظهور التقنيات والتطبيقات والمبادئ الجديدة حيث الجميع ما بين أجهزة الاستشعار المحسنة والذكاء الاصطناعي والأتمتة مع الأسلحة التي تفوق سرعتها سرعة الصوت وغيرها من التقنيات المتقدمة عبر العمليات السيبرانية لتنفيذ هجمات إلكترونية بغرض سرقة المعلومات والتأثير على صانعي القرار الرسمي عبر إلحاق الضرر بالبنية التحتية المادية والرقمية الحيوية، يأتي ذلك من تزايد مخترقي الإنترنت المهرة الذين يستهدفون الولايات المتحدة، في ذات الوقت بينهم عِلاقة منفعة متبادلة مع هذه الدول مثل مجموعات منفذي برامج الفدية وسولار ويند وغيرهم، هي مصدر قلق متزايد للدول في جميع أنحاء العالم، خاصة مع تزايد القدرات السيبرانية الصينية الهجومية والدفاعية الفائقة. مادامت الدول والقوى الكبرى تسعى إلى السلطة والنفوذ بالنسق الدولي دوماً. **إجمالاً** ستظل التهديدات السيبرانية من الدول القومية وعملائها في صورة تصاعدية طالما تحقق منها أهدافها الاستراتيجية، من المرجح أن يكون الصراع وخاصة العسكري منه بنفس الأسباب التي أدت للحروب سابقاً، ولكن الطرق التي تُشن بها تلك الحروب وتدار بها الصراعات سوف تتغير مع ظهور التقنيات والتطبيقات والمبادئ الجديدة ختاماً تسعى الدول الكبرى أيا كانت طبيعة نظمها إلي الوصول إلي القوة سواء كان نظام ليبرالي

أو حتى شمولي ذو نسق مغلق، تسعى الدول الكبرى إلي تعظيم قوتها لزيادة هيمنتها على النسق الدولي، لاشك أن القُوَى الكبرى ممثلة في الصين والولايات المتحدة في حالة تنافس قوي وسريع التطور، حيث سيكون مستقبل الاستراتيجية في القرن الحادي والعشرين في ضوء التغيرات التكنولوجية على إنه تفاعل مستمر بين الأضداد، سيلعب فيه الأمن السيبراني دوراً مهيمناً على استراتيجيات الأمن القومي لكلا القوتين، حيث بدخول الأسلحة السيبرانية أو التكنولوجيا السيبرانية أعلنوا بها انتهاء حقبة الحرب الباردة، وبداية نسق جديد تحاول القوة التعديلية الصينية – كما وصفها ترامب – في تغيير أسس وقواعد اللعبة بالنسق الدولي.

الآفاق المستقبلية:

بصورة مركزة تتصدر مسارات وتطور وتأثير القوة السيبرانية الأجندة الجيوسياسية والاستراتيجية مؤخراً. نركز بعض منها في النقاط التالية:

1- **تعزيز الاستثمار في القوة السيبرانية** من قبل كلاً من الصين والولايات المتحدة حيث ستعمل كلاً منهم على زيادة وتحسين وتطوير البنية التحتية للقدرات السيبرانية الدفاعية والمدنية الحيوية، مما يزيد من سيطرتهم على التجارة والاقتصاد الرقمي بصورة متزايدة.

2- **بروز القوة السيبرانية المستقبلية كأداة من أدوات القوة والهيمنة للولايات المتحدة والصين**، حيث الاعتمادية المتزايدة على تكنولوجيا وتطبيقات الذكاء الاصطناعي خاصة في تطبيقاتها الاستخباراتية والعسكرية. والاقتصادية ... وغيرها.

3- **التأثير على الشراكات والتحالفات الدولية**، من خلال تكتلات القوى التي تحشد لها الولايات المتحدة وحلفاؤها لحماية مصالحهم المشتركة ضد النفوذ والتهديد السيبراني الصيني المتزايد.

4- **التأثير على الاقتصاد العالمي وارتباط سياساته بالأمن السيبراني**، حيث ستؤدي الهجمات السيبرانية إلى تعطيل شبكات التجارة من بورصة وسلاسل الإمداد العالمية، مما ستزيد الاهتمام بتطوير وسائل آمنة للتبادل التجاري الرقمي بصورة خاصة مثل تحويلات البنوك التجارية وغيرها، مع توقع زيادة نشاط الهجمات السيبرانية المتبادل بين الطرفين، للتأثير على معدلات النمو الاقتصادي للدول الكبرى عبر وكلاء أو بصورة مباشرة سينعكس ذلك إيجابًا في زيادة الاستثمارات من القوى المختلفة في تطوير سياستها الأمنية السيبرانية.

5- **نشاط ساحة جديدة للتنافس بالنسق الدولي افتراضياً**، ممثلة سباق التسلح السيبراني، حيث ستصبح الهجمات السيبرانية أحد المحاور الرئيسية في بناء وتطوير استراتيجيات الأمن القومي. ووجود تفاوض وفرض سيطرة تتعلق بالمصالح للطرفين المتنافسة بشأن تنظيم مفاوضات أو معاهدات تمنع تلك الاختراقات المتبادلة قد تلح ولكن في إطار تنظيم أو وضع إطار حاكم وقواعد اللعبة في الحرب السيبرانية ولكن الأمر غير متوقع تحديده، وإن تم فسيكون متعلق بتعارض المصالح وتضاربها لذا نجاح مثل ذلك الاتفاق سيكون محدود.

قائمة المراجع

أولاً: المراجع العربية

- **التقارير**

1- منذر سليمان وجعفر الجعفري، (2023)، منطاد **صيني تقليدي "متجوّل" يكشف ثغرات التقنية الأميركية**، مركز المرصد -للدراسات العربية الأمريكية Center For American And Arab Studie-، 12 فبراير.

- **المصادر الإلكترونية**

1- تشارلز مور، **(2022)، الدفاع المشترك: رؤية القيادة السيبرانية الأمريكية**، لمجلة يونيباث- Unipath- Magazine، 15 ديسمبر. /Https://Unipath-Magazine.Com/Ar * يونيباث هي مجلة عسكرية مهنية ربع سنوية ينشرها قائد القيادة المركزية الأمريكية بوصفها منبراً دولياً للعسكريين في منطقة الشرق الأوسط وآسيا الوسطى والجنوبية.

ثانياً المراجع الأجنبية:

- **Books**

1- Moore, Daniel. (2022) **Offensive Cyber Operations: Understanding Intangible Warfare.** United Kingdom: Oxford University Press**.**

2- Gray, Colin S. (2015).**Future Of Strategy**, Polity Press.

3- Clark, David. D., & Landau, Suzan. (2010), **Proceedings of a Workshop on Deterring Cyberattacks: Chapter: Untangling Attribution in Cyber-Attacks**, National Academies Press.

- **Periodicals:**

1- Austin, Greg. (2014), **Cyber Policy in China**. Cambridge, Uk: Polity Press.

2- Rid, Thomas (2012), '**Cyber War Will Not Take Place'**, *Journal Of Strategic Studies* Vol. 35, No 1.

3- Schneider, Jacquelyn G &Goldman,Emily O.&Warner,Michael&Nakasone,Paul M. U.S. Army& Demchak,Chris C.(2020),**Ten Years In: Implementing Str Ears In: Implementing Strategic Appr Ategic Approaches To Cyberspace**,U.S. Naval War College U.S. Naval War College Digital Commons,Newport Papers. No.45.

4- Lonergan ,Erica D, Schneider ,Jacquelyn.(2023), **The Power Of Beliefs In Us Cyber Strategy: The Evolving Role Of Deterrence, Norms, And Escalation**, Journal Of Cybersecurity, Volume 9, Issue 1, 2023

- **Theses And Dissertations:**

1- Mcnally, Brandon Tyler)2021(,**United States Artificial Intelligence Policy: Building Toward A Sixth-Generation Military And Lethal Autonomous Weapon Systems**, Master Thesis, Johns Hopkins University In Conformity With The Requirements For The Degree Of Master Of Arts In Global Security Studies Baltimore, Maryland, December **.**

2- Patton,Diane E.(2016(**Assess Cybersecurity Strategies In The United States And China Within A Cultural Framework** ,A Research Report Submitted To The College In Partial Fulfillment Of Graduation Requirements For The Degree Master Of Arts And Operational Sciences Adviser: Wing Commander Graeme Corfield, Raf Maxwell Air Force Base, Alabama,.**Air Command And Staff College, Air University**,April

- **Reports**

1- Bing,Chris.(27 November. 2017),**Doj Reveals Indictment Against Chinese Cyberspies That Stole U.S. Business Secrets**,Cyber Scoop,

2- Cybersecurity Advisory (Jun 2022).**People's Republic Of China State-Sponsored Cyber Actors Exploit Network Providers And Devices**,Defense, Ver 1.0 , U/Oo/160405-22 , Pp-22- 25,

3- Chau, Thompson And Ting-Fang ,Cheng (2022) .**Cyber Warfare: China Attacks Force Taiwan To Bolster Defenses Power Plants Hospitals And Other Essential Facilities Seen As Possible Targets**, Nikkei Staff Writer , 13 September.

4- Claburn, Thomas.(2010), **China Cyber Espionage Threatens U.S., Report Says,**Informationweek. 27 February

5- Drake ,Bruce) 11 February, 2013(,**China And Cyber Attacks: A Top Concern Of U.S. Experts**, Pew Research Center.

6- Jinghua, Lyu (1april, 2019),**What Are China's Cyber Capabilities And Intentions?**, Carnegie Endowment .

7- Donnelly , John (M Cq-Roll Call). (2019), **Pentagon Workers Bought Thousands Of Chinese-Made Electronics Vulnerable To Hacks And Spying** Task And Purpose**,** Published Jul 30.

8- Morgan, Forrest E., Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly , Klima, And Derek Grossman)2020)**, Military Applications Of**

Artificial Intelligence: Ethical Concerns In An Uncertain World. Santa Monica, Ca: Rand Corporation .

- **Official Documents :**

1- The White House .(12 October.2022),**Us National Security Strategy**,Washington D.C.

2- The White House (12 November ,2022) **,Asean-U.S. Leaders' Statement On The Establishment Of The Asean-U.S. Comprehensive Strategic Partnership**, Briefing Room ,Statements And Releases,

3- The White House (1 March 2023),**National Cybersecurity-Strategy 2023** , Washington .

4- The White House (31 August, 2022**), President Biden Announces Appointments To The President's National Infrastructure Advisory Council** , Briefing Room, Statements And Releases,

5- The U.S.-China Economic And Security Review Commission . (2022) ,**China's Cyber Capabilities: Warfare, Espionage, And Implications For The United State Hearing Befor**e ,One Hundred Seventeenth Congress,Second Session,Thursday, February 17.Pp65-83

6- Office Of Management And Budget,(2016), **Managing Information As A Strategic Resource**, Circular No. A-130, Washington, Dc, A130,A130 Revised.

7- The White House (2011).**International Strategy For Cyberspace: Prosperity, Security, And Openness In A Networked World**. Washington, Dc.

8- Kerry,John.(2015),**Remarks:An Open And Secure Internet: We Must Have Both,** The Office Of Website Management, Bureau Of Public Affairs, U.S. State Department.,Korea University Seoul, South Korea, 18 May.

9- Defense Technical Information Center-Dtic.(2015), **The United States Military's Contribution To National Security**,Washington, D.C. June 2015.

10- Department Of Defense-Dod. (2018)**. Cyber Strategy Summary ,** Washington, 18 September.

11- Committee On Armed Services.(2 March, 2017), **Cyber Strategy And Policy**, , United States Senate, One Hundred Fifteenth Congress, First Session, ,

12- Defense Science Board (Dsb).(2017), **Task Force On Cyber Deterrence**, Department Of Defense , February . * **Dsb** Is A Federal Advisory Committee

13- Schneider,Jacquelyn G.(2022) **, U.S. Military Strategy And Domestic Policy Coordination Testimony Before The U.S.-China Economic And Security Review Commission Hearing On China's Cyber Capabilities: Warfare, Espionage, And Implications For The United State**s,U.S.-China Economic And Security Review Commission One Hundred Seventeenth Congress Second Session Thursday, February 17

14- The White House(1 March,2023),**National Cybersecurity-Strategy 2023** , 1 March 2023

15- White House (1 March ,2023),National Cybersecurity-Strategy March 2023 Washington, Dc.

16- Krekel . Bryan .(2009), **Capability Of The People's Republic Of China To Conduct Cyber Warfare And Computer Network Exploitation**, Dtic Document.

17- Cisa.Gov.(21 July , 2021),**Chinese Gas Pipeline Intrusion Campaign**, 2011 To 2013,Official Website Of The U.S. Department Of Homeland Security,Alert Code 21-201a

18- Jaikaran,Chris.(2021) ,**Federal Cybersecurity: Background And Issues For Congress**,Congressional, Research Service, September 29.

19- Cisa.(3 March,2021), **Emergency Directive : Ed 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities**,U.S. Department Of Homeland Security.

20- Cybersecurity & Infrastructure Security Agency- Cisa (1 September 2021), **Cisa Year In Review 2021**

21- Congressional Research Service (2023),**China Naval Modernization: Implications For U.S. Navy Capabilities**—Background And Issues For Congress, Updated15 May .

22- Executive Office of the President. (September 2018). **National cyber strategy of the United States of America**. The White House.

23- Schmidt ,Eric Et Al. (2021):, **Final Report: National Security Commission On Artificial Intelligence**, National Security Commission On Artificial Intelligence

24- Office Of The Secretary Of Defense -Dod (2020)**Annual Report To Congress: Military And Security Developments Involving The People's Republic Of China** ,1september.

25- U.S.Congress.(November ,2022) ,**2022 Report U.S.-China Economic And Security Review Commission**, One Hundred Seventeenth Congress Second Session 2022,Printed For The Use Of The U.S.-China Economic And Security Review Commission.

26- U.S.Congress(20july, 2021). **H3696 Congressional Record** — House

27- U.S.Joint Chief Of Staff .(2012), **Joint Publication 3-13: Information Operations,**27 November 2012 ,Incorporating Change 1, 20 November 2014. ;**Seealso** : U.S. Government Accountability Office-Gao (2011) **,Gao-11-865t :Cybersecurity: Continued Attention Needed To Protect Our Nation's Critical Infrastructure,** July 26.

28- U.S. Office Of The Director Of National Intelligence.(2021) ,**2021 Annual Threat Assessment** , April 9.

- **Electronic Resources :**

1- Borak,Masha.(2021),**China Drafts Three-Year Plan To Boost Its Cybersecurity Industry Amid Increasing Concerns For Data Safety** ,Scmp,13 July.

2- Dasgupta,Saibal (2022),**China Boosts Military Spending Amid Ukraine Uncertainties**, March 05, 2022 .

3- Gorman,Siobhan (2009),**Electricity Grid In U.S. Penetrated By Spies**, Wall Street Journal ,8 April .

4- Graff,Garrett M.(2020**),China's Hacking Spree Will Have A Decades-Long Fallout**,Wired ,11 February.

5- Kitchen, Klon (2021) , **Informatized Wars: How China Thinks About Cyber**, Aei, 21 April

6- Menn, Joseph. (2014). **Private U.S. Report Accuses Another Chinese Military Unit Of Hacking**. Reuters.

7- Mesich, Mathias (2022).**China Is Targeting America's Critical Infrastructure**. **Here's What You Can Do About It**.Industrial Defender, 29 June.

8- Naughton,Hank (2021).**Biden Should Shoot This Acquisition Down**, Defense One, 25 March

9- Solarwinds Official Website . Https://Www.Solarwinds.Com

10- Srivastava,Mehul & Schwartz,Felicia, And Sevastopulo Ft , Demetri,)2023(,**China Building Cyber Weapons To Hijack Enemy Satellites, Says Us Leak**, Ars Technica, 21 April

11- Paganini,Pierluig (2015), **China And Its Cyber Capabilities, Are You Really Surprised?**, Security Affairs, March 20, 2015

12- Washington Post.(9 July , 2015),**Hacks Of Opm Databases Compromised 22.1 Million People, Federal Authorities Say**,

13- Wolf, Jim (2010). **Pentagon Says "Aware" Of China Internet Rerouting**". Reuters. 19 November