استراتيجيـة الشـؤون السيبرانيـة الصينيـة

سهيـر حسـن سعـدون
الجامعة المستنصرية / كلية العلوم السياسية

البريد الإلكتروني Email : Suhaira26alhassan@gmail.com

الكلمات المفتاحية: الصين، الأمن السيبراني، الفضاء الإلكتروني، التنافس الأمريكي الصيني، الحزام والطريق الرقمي.

كيفية اقتباس البحث

سعـدون ، سهيـر حسـن، استراتيجيـة الشـؤون السيبرانيـة الصينيـة،مجلـة مركز بابـل للدراسـات الانسانية، أيلول ٢٠٢٥،المجلد:١٥ ،العدد:٥ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

China's Cybersecurity Strategy

Suhair Hassan Saadoun
Al-Mustansiriya University / College of Political Science

Keywords : China, Cybersecurity, Cyberspace, US-China Competition, Digital Silk Road.

How To Cite This Article
Saadoun, Suhair Hassan, China's Cybersecurity Strategy,Journal Of Babylon Center For Humanities Studies, September 2025,Volume:15,Issue 5.

Abstract:

This research aims to examine China's cyber strategy as one of the rising major powers in the international system, which has successfully utilized cyberspace as a strategic tool for national security and global competition. The study explores China's motivations for prioritizing cyber power, the main components that have placed it at the forefront internationally, and analyzes the tools, objectives, and means of its cyber strategy. It also highlights the dimensions of cyber competition with the United States, as the world's two largest economic and technological powers, and investigates areas of cyber cooperation between China and Russia. Furthermore, it addresses the "Digital Silk Road" as an extension of China's global influence in cyberspace. The research concludes that cyber power is a core pillar of China's foreign policy, employed through a dual approach that combines intense competition with adversaries and strategic cooperation with allies.

In an environment where cybercrime is thriving, the law is lax, and there is inconsistent enforcement of its mechanisms, the Chinese government has been working tirelessly to build an effective technical system for "network security." Therefore, China's enactment of the "Cybersecurity Law" represents an important step to address this sensitive issue and its significant impact on the country's national

security. This law reflects a broad global trend to regulate cyberspace activities and combat cyber threats that could undermine the national security of various countries around the world.

الملخص:

يهدف هذا البحث إلى دراسة الاستراتيجية السيبرانية للصين بوصفها إحدى القوى الكبرى الصاعدة في النظام الدولي، والتي استطاعت توظيف الفضاء الإلكتروني كأداة استراتيجية للأمن القومي والتنافس الدولي. يتناول البحث دوافع الصين للاهتمام بالقوة السيبرانية، ومقومات هذه القوة التي جعلتها في موقع متقدم عالميًا، بالإضافة إلى تحليل أدوات وأهداف ووسائل استراتيجيتها السيبرانية. كما يسلط الضوء على أبعاد التنافس السيبراني مع الولايات المتحدة الأمريكية، باعتبارهما أكبر قوتين اقتصاديتين وتقنيتين، ويبحث في مجالات التعاون السيبراني بين الصين وروسيا، وصولًا إلى مشروع "الحزام والطريق الرقمي" بوصفه امتدادًا للنفوذ الصيني في الفضاء الإلكتروني العالمي ، بالتالي فأن القوة السيبرانية تمثل ركيزة أساسية في السياسة الخارجية الصينية، وأن بكين توظفها بأسلوب مزدوج يجمع بين التنافس الحاد مع خصومها والتعاون الاستراتيجي مع حلفائها.

ان الأمر الذي دفع السلطات الحكومية الصينية إلى السعي الحثيث لبناء منظومة تقنية فعالة ل " أمن الشبكات " ، في بيئة تزدهر فيها الجريمة الإلكترونية وتراخي القانون وتطبيق غير متكافئ لآلياته ، لذا مثل تشريع الصين ل " قانون الأمن السيبراني " خطوة مهمة لمعالجة هذه القضية الحساسة وتأثيرها الكبير على الأمن الوطني للدولة ، ويعكس هذا القانون اتجاها عالميا واسع النطاق لتنظيم أنشطة الفضاء السيبراني ومكافحة التهديدات السيبرانية التي يمكن أن تقوض الأمن الوطني لدول العالم المختلفة .

المقدمة:

شهدت البشرية منذ سنوات تقدما تكنولوجيا، قلما عرفه عصر من العصور السابقة من قبل، حتى بات هذا التقدم ثورة قائمة بذاتها في عالم الاتصالات والعلاقات الدولية، كما أصبح العالم بفضلها بمثابة قرية كونية فعلا، بحيث أصبح للفضاء السيبراني دور في حركة التفاعلات والتحولات البنيوية كمجال جديد في العلاقات الدولية وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات في النظام الدولي حتى أصبح العالم اليوم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي والانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف، وبذلك أصبحت قضية أمن الفضاء الالكتروني من عمليات القرصنة الالكترونية والهجمات السيبرانية والتي بدوها تؤثر على أمن الدول تلقى اهتماما

متصاعدا على أجندة الأمن الدولي وتتخذ محلا كبيرا في صياغة استراتيجيتها القومية العليا ، وباتت العلاقة بين والتكنولوجيا وامن الدول علاقة طردية فبتطور التكنولوجيا تتزايد إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الالكترونية إلى أخطار الكترونية في الفضاء السيبراني الذي يمثل التهديد الأكبر لأمن الدول خاصة وانه غدا وسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف والمزود الأول لتغذية التوترات الدولية، لذا اصبح الامن السيبراني يدخل ضمن اولويات استراتيجيات الدول وسياساتها الخارجية

اهمية البحث:

تعد الصين احد اهم الدول التي استخدمت الفضاء السيبراني واستحدثت استراتيجيات سيبرانية للتعامل مع الهجمات والتهديدات الالكترونية التي قد تهددها وكذلك اعتماد الاساليب التي ترد بها بأعتبارها قوة كبرى صاعدة تنافس القوة العظمى الاولى في العالم وهي الولايات المتحدة الامريكية حيث تعد التهديدات والاتهامات المتبادلة بينها وبين الولايات المتحدة من ابرز انواع المشاكل على الصعيد السيبراني في الوقت الحاضر، كما تعد الصين ثاني دولة اقتصاديا وسكانيا بعد الولايات المتحدة كذلك تعتبر دولة متطورة تقنيا وتمتلك العديد من مقومات القوة الاخرى ما يؤهلها ان تلعب دورا استراتيجيا كبيرا في العالم مستقبلا ، اذا فان الاهمية الكبيرة للصين وتأثيرها البالغ في النظام الدولي يتطلب منا دراسة عميقة لكل مقومات قوة هذ الدولة والتي من ضمن هذه المقومات هي القوة الالكترونية (السيبرانية) محل البحث .

اشكالية البحث:

ينطلق البحث من تساؤل جوهري مفاده :ما هي الاستراتيجيات والآليات التي تتبعها الصين في شؤنها السيبرانية؟ وتندرج ضمن هذه الإشكالية الرئيسية مجموعة من الأسئلة الفرعية تتمثل أساسا في التالي :

١.ما هي دوافع الصين للاهتمام بالقوة السيبرانية؟

٢.ماهي مقومات القوة السيبرانية الصينية؟

٣.ما هي الاستراتيجية السيبرانية الصينية ؟ ما هي اهدافها، ادواتها ووسائلها؟

٤.كيف تتعامل الصين سيبرانياً تجاه التنافس الامريكي معها ؟

٥.ما هي مجالات التعاون الروسي الصيني في الشؤون السيبرانية؟

٦.ما هو مشروع طريق الحرير الرقمي ؟

فرضية البحث:

للأجابة على الاشكاليات السابقة تم صياغة فرضية مفادها : ان للصين من مقومات القوة السيبرانية ما يجعلها تحتل مكانة مهمة في هذا المجال كذلك لها استراتيجيات في الشؤون السيبرانية متعددة او ثنائية الجانب منها ما يكون بصيغ تنافسية كما تفعل في تنافسها السيبراني مع الولايات المتحدة الامريكية ، والجانب الاخر ما يكون تعاونياً كما هو الحال في تعاونها السيبراني مع روسيا.

منهجية البحث:

تم الاعتماد في كتابة هذا البحث على المنهجين الاستقرائي والاستنباطي بالاضافة الى عدة مقتربات منها المقرب التحليلي والوصفي والتاريخي .

هيكلية البحث:

تم تقسيم هذا البحث وفق هيكلية منهجية الى مقدمة وخاتمة وخمسة محاور كالتالي :

المحور الاول : دوافع الصين للاهتمام بالقوة السيبرانية.

المحور الثاني: مقومات قوة الاستراتيجية السيبرانية الصينية.

المحور الثالث: استراتيجية السيبرانية الصينية" الادوات ، الاهداف ، الطرق"

الحور الرابع: التنافس الامريكي الصيني في المجال السيبراني.

المحور الخامس: التعاون الصيني الروسي في المجال السيبراني.

المحور السادس: مشروع الحزام والطريق الرقمي.

المحور الاول : دوافع الصين للاهتمام بالقوة السيبرانية

لقد شهد النظام الدولي العديد من التغييرات في اغلب مقوماته ومجالاته لا سيما بعد الثورة الصناعية والعلمية الحديثة اذ كان احد ابرز هذه المجالات اهتمام الدول بالتقنيات الحديثة مثل الذكاء الاصطناعي والامن السيبراني وغيرها من المجالات الاخرى[١]. من ثم لدراسة استراتيجة دولة ما لا بد من التعرف على اهم مقومات قوة تلك الدولة لا سيما مقومات القوة الالكترونية "السيبرانية" التي تعد احد ابرز مقومات القوة واهمها نظراً للتطور الكبير الذي شهده المجال السيبراني حديثاً. حيث في الصين تفسر السياسة الخارجية بما فيها المجال السيبراني في ضوء سياستها الداخلية والمتمثلة بحماية وديمومة سيطرة الحزب الشيوعي حيث يضمن ذلك ضمان استقرار الصين الداخلي والخارجي في كافة المستويات والصعد ومن ثم تتمثل دوافع الصين في المجال السيبراني بعدة اشكال (اقتصادية، سياسية، عسكرية وغيرها).

اولاً: الدوافع الاقتصادية

تشمل الدوافع الاقتصادية للاستراتيجية الصينية السيبرانية هدفين رئيسيين هما ضمان استمرار النمو الاقتصادي وردع الجرائم الالكترونية المحلية ، وفيما يتعلق بالتجسس الالكتروني والصناعي والذي يرتبط بالحصول على المعلومات الاقتصادية الصناعية بما في ذلك الاسرار التجارية الخاصة بالبحث والتطوير والانتاج ، حيث يحدث ذلك على نطاق واسع في الصين بالتالي فقد وصف مكتب الولايات المتحدة لمكافحة التجسس (NCIX) في تقرير له بأن الجهات الالكترونية الصينية هم " الجناة الاكثر نشاطاً واستمرارية في مجال التجسس الاقتصادي" ، ونظرا لصعوبة قياس الاثار المترتبة على هذه الجرائم فأنه من الصعب معرفة المدى الحقيقي للجريمة الالكترونية والتجسس الالكتروني الصيني اما الصين فأنها تستمر في الرد على هذه الاتهامات مصرة الى ان الدولة لا تدعم اي نشاطات لها علاقة بالقرصنة[٢].

ثانياً: الدوافع السياسية

فيما يتعلق بالدوافع السياسية ، فأن الحكومة الصينية تخشى من إتاحة استخدام الإنترنت دون قيود ، ومن عدم السيطرة على عملية تدفق وانتشار المعلومات خاصة من قبل المعارضة ، الأمر الذي قد يشكل خطرا كبيرا على استقرار النظام الشيوعي الصيني وعلى السلطة الحاكمة ، لذلك قامت الصين بتطبيق تدابير وقائية في إطار تبني مفهوم " احترام السيادة الصينية في مجال القضاء الإلكتروني " . والذي من شأنه أن يسمح للصين بالسيطرة على الإنترنت داخل حدود الدولة ، في حين أن المفهوم الغربي للفضاء الإلكتروني يتبنى نجا منفتحا من خلال التدفق الحر للمعلومات عبر الحدود . وفيما يتعلق بالشؤون الخارجية ، تقوم الحكومة الصينية بتوليف جهات غير حكومية أو على الأقل لا تمنعها للقيام بأنشطة إلكترونية ضد الخصوم ، تشمل التجسس الإلكتروني في المجالات المختلفة الاقتصادية والصناعية والعسكرية ، ونظرا لعدم إمكانية إثبات وجود علاقة بين المؤسسات الحكومية والجهات الفاعلة التي ترعاها الدولة في هذا المجال ، لذلك فمن الصعب إلقاء اللوم على الحكومة الصينية ومقاضاتها وفقا للقانون الدولي في هذا الشأن[٣].

ثالثاً: الدوافع العسكرية

تكمن نقطة التحول الرئيسية في النسيج الصيني بعد استلام الولايات المتحدة للتكنولوجيا العسكرية المتقدمة في حرب الخليج ، فمنذ ذلك الحين ركزت الصين على تكنولوجيا المعلومات والاتصالات من أجل توظيفها في الحروب المستقبلية ، وتطمح في احتلال موقع متقدم في هذا المجال بحلول عام ٢٠٥٠ أن الصين قد عملت على ترسيخ أسس استراتيجية الأمن الإلكتروني في العلوم والأدبيات العسكرية الصينية ، مثل المبادئ التوجيهية للاستراتيجية العسكرية ، وعلم

الاستراتيجية العسكرية ، فضلا عن المبادرات الحكومية ، مثل مبادرة " المهام التاريخية الجديدة " ل " هو جين تاو " ، والأوراق البيضاء للدفاع الوطني ومن خلال هذه العلوم والأدبيات العسكرية ، بحث العسكريون في استراتيجيات تمكنهم من استغلال المجال الإلكتروني في مختلف السيناريوهات الهجومية والدفاعية وتشير الكاتبة إلى أنه بسبب اختلاف الثقافات الاستراتيجية ، فإن العلوم والأدبيات العسكرية لا تميز بوضوح في هذا المجال بين التدابير الدفاعية والهجومية ، وبالتالي فإن ما قد نعتبره الصين آليات دفاعية ، قد يتم تأويله على أنه اليات هجومية في الولايات المتحدة وغيرها من الدول الغربية . وتتوقع الكاتبة أن تلعب العمليات العسكرية الإلكترونية دورا هاما في السيناريوهات العسكرية المتعلقة بتايوان ، والنزاعات الإقليمية والبحرية الأخرى ،وكذلك ضد الولايات المتحدة ، وقد أشارت العديد من التقارير الخاصة بالتهديدات المتقدمة المستمرة الصادرة عن شركات الأمن الإلكتروني الأمريكية إلى تطور مستوى الهجمات الإلكترونية الصينية ضد الحكومة والمؤسسات الصناعية والتجارية الأمريكية ، على الرغم من استمرار في الصين لهذه الاتهامات[٤] .

المحور الثاني : مقومات قوة الاستراتيجية السيبرانية الصينية

ان عملية صنع القرار في الدول المقدمة يتميز بالتعقيد والتشابك مما يتطلب توظيف ادوات وتكنلوجيا حديثة لتحليل البيانات واتخاذ قرارات صحيحة[٥]، لدراسة الصين كقوة كبرى يجب أن نبين ان هناك عناصر للقوة في الاستراتيجية السيبرانية للصين تتعدد وتتنوع اشكالها حيث لولا هذه العناصر لما كانت هناك قوة سيبرانية صينية حيث ان القوة السيبرانية هي قدرة الدولة القومية على السيطرة والتأثير داخل وعبر الفضاء الالكتروني لدعم عناصر المجالات الأخرى للسلطة الوطنية حيث يعتمد تحقيق القوة السيبرانية على قدرة الدولة على تطوير موارد العمل في الفضاء السيبراني والتي تختلف عن القوة البحرية ، البرية والجوية أو حتى الفضائية ، فبدلا من الدبابات والسفن والطائرات تحتاج الدولة إلى أجهزة الكمبيوتر المتصلة بالشبكة ، والاتصالات السلكية واللاسلكية والبنية التحتية والبرامج والأشخاص ذوي القدرات الخاصة في المجال السيبراني، بالتالي مع ادراكها أن تفوق الدولة في المجال السيبراني يزيد من قوتها ويعزز مكانتها الدولية ، فان الصين ومن المؤتمر الثامن عشر للحزب الشيوعي الصيفي تولي أهمية بالغة للأنترنت ، حيث عملت اللجنة المركزية للحزب على تطويره وفي نفس الوقت حوكمته ، وقامت بتنسيق القضايا المتعلقة بالإعلام والأمن السيبراني في المجالات السياسية ، الاقتصادية ، الثقافية

والاجتماعية والعسكرية ، بما يضمن توجه الصين نحو بناء قوة سيبرانية[٦]. حسب "لي تشانغ" مدير معهد دراسات المعلومات والتنمية الإجتماعية في الصين ، أن مفهوم القوة السيبرانية يشير الى قدرة اتخاذ إجراءات وممارسة التأثير في الفضاء السيبراني " ، فان القوة السيبرانية الصينية تقوم على العوامل التالية :[٧]

١.قدرات الانترنت و تكنولوجيا المعلومات : قدرة الدولة على اجراء البحوث وتطوير تكنولوجيا المعلومات وتعزيز الابتكار وتطبيق البحوث في الصناعة ، بحيث يمكن لهذه التقنيات تحويل العمليات الصناعية والتجارية وتزيد من انتاجيتها .

٢.قدرات صناعة تكنولوجيا المعلومات : وجود دولة تسيطر على صناعة تكنولوجيا المعلومات العالمية ، يعتبر معيارا للقوة السيبرانية ، فالولايات المتحدة الأمريكية في موطن لرواد صناعة تكنولوجيا المعلوماتية العالمية مثل Appel BN , Microsoft , Intel, Google, Cisco وهو ما يجعلها قوة سيبرانية عظمى.

٣. قدرات سوق الانترنت : تعتبر البنية التحتية عامل دفع رئيسي للقوة السيبرانية ، والتي تتكون من عدد مستخدمي الانترنت ، وعدد الأجهزة ، والبنية التحتية للانترنت متكاملة.

٤. تأثير ثقافة الانترنت ومدى انتشارها ، ودورها في تغيير سلوكيات عامة المجتمع ، كون الانترنت تستخدم في الاتصالات ، الشبكات والتعلم ، فانه يجب الاهتمام بدرجة التأثير على السلوك الذي تمارسه ثقافة الإنترنت بما يظهر دمج المجتمع معها.

٥. الدبلوماسية الرقمية "القدرات السياسة الخارجية" : ويشير الى القوة التفاوضية لدولة قومية وقدرتها على التأثير على المنصات الإلكترونية الحديثة والمتعددة الأطراف والمشتركين.

٦.القوة العسكرية السيبرانية تتكون من القدرة على الدفاع على البنية التحتية لتكنولوجيا المعلومات الوطنية العسكرية الهامة من الهجمات ، قدرة الردع والقدرة على اجراء عمليات هجومية في الفضاء الالكتروني والقدرة على منع الشبكات الخاصة من التجسسي.

٧.المصلحة الوطنية في المشاركة في استراتيجية الفضاء الإلكتروني ، بالترتيب لتكوين قوة سيبرانية فانه ليس كافيا الدولة امة مجرد امتلاك جزء او كل الفدرات . وانما لابد من وجود الدافع او الرغبة في استخدام تلك القوة ، حيث يجب على الدولة القومية ان تكون قادرة على استخدام الفضاء الإلكتروني من اجل تحقيق الأهداف الاقتصادية ، والضروريات السياسية ، والحاجات الأمنية.

إن صناعة المعلومات الإلكترونية في الصين قد شهدت نموا سريعا في عام ٢٠١٦ مع توسع في القيمة المضافة لإنتاج الصناعة بنسبة ١٠ % على أساس سنوي ، و كان أقل بقيمة ٠.٥

% عام ٢٠١٥ لكن فاق نمو الناتج المحلي ب ٤ % وفقا لوزارة الصناعة والتكنولوجيا . وشهدت الصناعة تطورا سريعا بفضل تعزيز الإبتكارات القائمة على الأنترنت ، وجهود الحكومة لتحسين البنية التحتية ، في الصين اكثر من ٧٠٠ مليون مستخدم للانترنت و ٣.١ مليار مستخدم لاجهزة الذكية بمختلف اشكالها بالتالي فأنها تحتل المرتبة الاولى في العالم من هذه الناحية ، اما بالنسبة للصناعة والانتاج فان الصين عام ٢٠١٦ انتجت ٢.١ مليار هاتف محمول[٨]، بالتالي فأن ذلك دليلا واضحا على قوة البنية التحتية للصين في المجال الالكتروني وينعكس ذلك على قوتها السيبرانية ككل باعتبار البنية التحتية احد اهم مقومات القوة السيبرانية الصينية، كذلك تمتلك الصين العديد من البرامج الخبيثة ولكن بالنظر إلى أن الصين تضفي قدرا من السرية ، على قدراتها السيبرانية ، مما يصعب إدراك إمكانياتها السيبرانية ، كما أنها دائما ما تنكر صلتها بأي هجوم ، إلا أنها من برمجت كل من فيروس :[٩]

١.فيروس تيتان راين : " مطر العمالقة " و الذي يتم إستخدامه لإنتزاع معلومات من خلال أجهزة خادمة .

٢. فيروس وانا كراي : والذي يتم عمله بتشفير بيانات الحواسيب ثم إرسل رسالة يطالب بالفدية بعملة البيتي كوين الإلكترونية مقابل الإفراج عن البيانات إلا أن الصين تنفي صلتها هذا الفيروس .

كما تتم العمليات السيبرانية الصينية بهذه الفايروسات بثلاث طرق : مهاجمة شبكات الحاسب الآلي ، و الدفاع عن شبكات الحاسب الآلي ، و إستطلاع شبكات الحاسب الآلي.

كذلك تشير الدراسات الى ان مساعي الصين لبناء قوة سيبرانية موجهة بشكل اساسي لتحقيق ثلاث اهداف قد تكون مرتبطة بشكل كبير بالامن القومي حيث تتمثل هذه الاهداف بما يلي :[١٠]

١.الحفاظ على بقاء نظام الحكم المتمثل بالحزب الشيوعي الصيني .

٢.الحفاظ على السيادة الوطنية ووحدة الاراضي " منع استقلال تايوان".

٣.الحفاظ على التنمية الاقتصادية والاجتماعية وتحديث الجيش بما يضمن لها ان تكون قوة عالمية.

المحور الثالث :الاستراتيجية السيبرانية الصينية

تبنت الصين في السنوات القليلة الماضية سياسة صارمة وأكثر اتساقا تجاه الفضاء السيبراني ، وفي هذا الصدد يعتبر عام ٢٠١٤ عاما فاصلا حيث تم استحداث " مجموعة من الانترنت المركزي " و " مجموعة المعلومات الرائدة " ، كلاهما تحت رئاسة الرئيس الصيني تشي جين بينغ " ، وهو ما يرسل إشارة قوية على التزام الصين القوي بهذه القضية ، تنظر الصين إلى

الفضاء السيبراني في الوقت نفسه على أنه تهديد كبير للاستقرار الصيني وضروري لأهداف التنمية الصينية ، وبالتالي فإن تحقيق التوازن الصحيح بين الانفتاح والقمع هو مسألة حساسة .

ان إحدى الطرق الرئيسية التي حاولت الصين تحقيق التوازن بين هاذين الشاغلين فيها كانت من خلال تشجيع الشركات المحلية ومنحها حصة في النظام ، لقد تم إعطاء رجال الأعمال البارزين ، دور في تشكيل وتعزيز السياسات الصينية ، حيث في عام ٢٠١٥ أطلقت الصين أكبر عملية إعادة تنظيم على مستوى القوات المسلحة(جيش التحرير الشعبي) حيث شملت الإصلاحات جميع صنوف وفروع الجيش البرية والبحرية والجوية، وكان من ضمن الاصلاحات المهمة استحداث فرع جديد يسمى " قوات الدعم الاستراتيجي" من بين مهامها الأساسية هي تأمين الفضاء الكهرومغناطيسي والفضاء الالكتروني، والتحكم في العمليات السيبرانية إدارتها إلى مستويات عليا، بما يضمن تحقيق السيادة السيبرانية عبر قوة سيبرانية فعالة، كما عملت الصين على ترسيخ أُسس استراتيجية الأمن الإلكتروني في العلوم والأدبيات العسكرية الصينية، مثل: المبادئ التوجيهية للاستراتيجية العسكرية The Military Strategic Guidelines ، وعلم الاستراتيجية العسكريةThe Science of Military Strategy ، فضلاً عن المبادرات الحكومية، مثل مبادرة "المهام التاريخية الجديدة" لـ"هو جين تاو Hu Jintao's New Historic Missions"، والأوراق البيضاء للدفاع الوطني The National Defiance White Papers. ومن خلال هذه العلوم والأدبيات العسكرية، بحث العسكريون في استراتيجيات تُمكنهم من استغلال المجال الإلكتروني في مختلف السيناريوهات الهجومية والدفاعية[١١] .

كما أصدرت الصين " قانون الأمن السيبراني الصيني " المعمول به منذ عام ٢٠١٧ ، شددت من خلاله على أنه من حق الدول ذات السيادة وضع قوانين وقواعد لتنظيم الفضاء السيبراني طبقا لما تقتضيه مصلحة البلاد وإتباعا للممارسات الدولية المعمول بها في هذا الصدد . يمكن فهم قانون الأمن السيبراني في الصين ، كتأثير لمفهوم السيادة السيبرانية ، فجزء هام من هذا القانون يشترط أن تقوم الشركات التي تساهم في البنية التحتية الحيوية للمعلومات بتخزين بياناتها داخل الحدود الصينية .[١٢]

وبمقتضاه يكون محظورا على مقدمي خدمات الانترنت جمع وبيع المعلومات الشخصية للمستخدمين ، كما أنه ينبغي عليهم التعامل مع هذه المعلومات بما يتماشى مع القانون والقواعد الخاصة بالدولة ، ويعطي القانون الحق لمستخدمي الانترنت أن يطلبوا من مقدمي الخدمات حذف معلوماتهم إذا ما تم إساءة استخدامها ، كما يطلب القانون بامتثال الشركات المساعدة التحقيقات الصينية ، وأخيرا يستلزم المفهوم أيضا استمرار الرقابة الحالية على المواقع التي تعتبر

ضـارة بالصـين ، ومـن التطـورات الأخيـرة قـرار الحكومـة اتخـاذ إجـراءات صـارمة ضـد مـزودي الشبكات الافتراضية الخاصة ، حيث تمكنت هذه الشبكات حتى الآن من تجنب الرقابة ، مما يسمح لمستخدمي الانترنت بالوصول إلى المواقع الأجنبية المحجوبة ، كما تمت الاستجابة الصينية من خلال تبني إستراتيجية شاملة عام ٢٠١٦ لتحقيق اكتفاء تكنولوجي ذاتي بحلول عام ٢٠٢٥ من خلال تخصيص مئات المليارات سنويا لأغراض تطوير القدرات الوطنية الصينية ، خاصة وأنها تعتمد بشكل كامل على استيراد الرقائق الالكترونية التي تؤدي عمليات المعالجة الدقيقة ، والتي تدخل في معظم الصناعات الالكترونية لأجهزة الاستخدام الشخصية والتجارية مثل الهواتف النقالة والكمبيوتر وأجهزة التلفزيون ... الخ ، وهي صناعات تحتل في مجملها ثلث الصادرات الصينية إلى العالم ، وأخطر ما في هذا الموضوع هو الاعتماد شبه الكامل على المجهزين الأمريكيين ، وقد واجهت الصين انكشافا استراتيجيا كبيرا في نيسان ٢٠١٨ حين قامت إدارة " ترامب " بفرض عقوبات ضريبية على شركة ZTE عملاق الصناعات الالكترونية ومعدات الاتصالات " الرابع عالميا " ، مما أدى إلى توقفها بسبب إحجام المجهزين عن إمدادها باحتياجاتها ، وقد تم رفع العقوبات بعد اتصالات سياسية بين البلدين ، إثر ذلك قام الرئيس الصيني بتوجيه نداء خاص إلى علماء بلاده للعمل لبذل جهود استثنائية للخروج من هذا الموقف[١٣] .

علاوة على ذلك تبذل الصين جهودا كبيرة وتنفق الكثير لتطوير قدراتها الذاتية في ميدان حوسبة الكم ، التي تستخدم ميكانيكا الكم وتوفر القدرة على إجراء عدة عمليات حساب في آن واحد ، وهو حقل يحتاج إلى نوع خاص من أجهزة الحاسوب . إن إحراز التقدم في هذا المجال يؤمن للصين القدرة على تأمين قنوات اتصال مشفرة ، كما يوفر القدرة على فك شفرات الآخرين ، وفي المجال الاقتصادي يمكن لهذه الحواسيب أن توفر منافع هائلة وخاصة في مجال تحليل المعلومات والمعطيات في معظم المجالات الصناعية . ففي ٢٠١٦ أطلقت الصين أول قمر صناعي يمكنه نقل اتصالات مشفرة من خلال هذه الوسيلة ، كما أنجزت الصين مد أطول كابل لهذا النوع من الاتصالات المشفرة بين بكين وشنغهاي . كما أعلنت الصين عام ٢٠١٧ أنها تخطط لتبوأ موقع الريادة العالمية في ميدان الذكاء الاصطناعي بحدود عام ٢٠٣٠ ، وذلك بتشجيع الاستثمار والابتكار في هذا الميدان ، حيث بادرت بإنشاء بعض الهيئات والشركات المتخصصة في هذا المجال ، مثل : Baido شركة صينية عابرة للحدود متخصصة بخدمات الانترنت والذكاء الاصطناعي ، و Tencent شركة عابرة للحدود متخصصة بالأنترنت والعاب

الفيديو ، وعملاق الانترنت Alibaba وشركة Flytex المتخصصة بجوانب دقيقة ذات صلة بالانترنت[١٤].

كما تبذل الصين أيضا جهودا مضنية من أجل التعامل مع الموجة الجديدة من الاكتشافات وخاصة في مجال تقنيات شبكات الجيل الخامس من الهواتف النقالة ، تلك التقنية الثورية الجديدة التي تعتبرها الصين العمود الفقري الاستراتيجية " صنع في الصين ٢٠٢٥ " ، التي ستحول بكين إلى " قوة تقنية كبرى " ، فيما تعتبر الولايات المتحدة تلك الاستراتيجية مصدر قلق بالغا وتهديد مباشرة لأمنها القومي ، خاصة من طرف الشركة الرائدة عالميا " هواوي " التي تعد ثاني أكبر شركات إنتاج أجهزة الهواتف المحمولة في العالم بعد " سامسونغ " الكورية ، بحصة سوقية تصل إلى ١٧ % بحسب بيانات الربع الأول ٢٠١٩ ، حيث ازدادت مبيعات هواوي عام ٢٠١٨ بنسبة ٢٠ بالمئة مقارنة مع ٢٠١٧ لتصل إلى ١٠٧ مليارات دولار ، بعد أن كانت ١٢ مليار دولار في ٢٠٠٨ ، وبذلك انتقلت إلى مصاف شركتي جوجل ومايكروسوفت الأمريكيتين للتكنولوجيا[١٥].

بالإضافة الى ذلك بدأت الصين بتطوير تقنية شبكة الجيل الخامس الخاصة بها في أوائل ٢٠٠٩ ، كما تصدرت تقنيات الشركة اللاسلكية لشبكة " 5G " المرتبة الأولى في اختبارات تقييم الأداء التي تتم من قبل جهات مستقلة ، وفازت مؤخرا بجائزة " أفضل تقنية لشبكة الجيل الخامس " في قمة الجيل الخامس العالمية سنة ٢٠١٩، الأمر الذي أدى إلى تصعيد حدة الصراع بين الصين والولايات المتحدة التي أعلنت مقاطعتها لشركة " هوواوي " ومنعتها من التنافس للفوز بعقود أمريكية ، كما ضغطت على حلفائها الاستشائها من المشاركة في شبكات الجيل الخامس فيها ، وقد استجاب بعض الحلفاء لطلبها على غرار نيوزيلندا وأستراليا ، فيما لا يزال حلفاء آخرون يدرسون هذه الخطوات ، وأبرزهم ألمانيا وفرنسا وبولندا وبريطانيا ، والسبب في ذلك حسب أمريكا يكمن في العلاقات الوطيدة التي تربط مؤسس " هواوي " بالجيش الصيني ، مما يمكنه من اعتراض الاتصالات في أمريكا ، كما يمكنه شن هجمات الكترونية على البنية التحتية..الخ ، وقد بلغ الصراع ذروته بين الطرفين حين اعتقلت السلطات الكندية ابنة مؤسس " هواوي " المديرة المالية " منغ وانزو " ، وذلك بطلب أمريكي بتهمة الاحتيال وانتهاك العقوبات الأمريكية المفروضة على إيران ، مما وتر العلاقات بين الأطراف الثلاثة خاصة بعد قبول تسليم كندا " وانزو " لأمريكا في حال ثبوت إدانتها ، حيث استخدمت الصين كل إمكاناتها الدبلوماسية ، وضغطت على حلفائها ومنافسيها على حد سواء ، واتخذت الصين إجراءات غير اعتيادية ،

وانتهجت " دبلوماسية الرهائن " حيث اعتقلت مواطنين كنديين بتهمة التجسس ، في محاولة لإنجاز نوع من تبادل السجناء مع كندا ، ومنع تسليم " وانزو " للحكومة الأمريكية .[١٦]

تشير قضية " هواوي " إلى تصاعد حدة التوترات بين الولايات المتحدة والصين ، ومن غير الواضح بعد إن كان البلدان سيتجنبان المزيد من التصعيد أم أنه قد يحدث ما هو أسوأ بكثير ، خاصة أن هناك العديد من التهم الموجهة إليها بالتحايل وسرقة أسرار تكنولوجية من الشركات الأمريكية والغربية ، تحاول من خلالها الصين استدراك ما فاتها لتقليص الفجوة بينها وبين الدول الغربية المتقدمة ، ليس فقط للحاق بها ولكن لكسب السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية لا يمكن تجاوزها . كذلك ارتبط اسم " هواوي " بفضيحة قريبة من هذا الملف الشائك ، حين اتهم أحد مهندسيها بسرقة المعلومات من روبوت لاختبار الهاتف طورته شركة T– Mobile الأمريكية ، كما تسعى الصين لتعزيز أهدافها من خلال الدعوة إلى مفهوم السيادة السيبرانية في المحافل الدولية ، باحتواء جدول الأعمال العالمية في المجالات الالكترونية ، أحسن مثال على ذلك هو اجتماع فريق هندسة الانترنت لعام ٢٠١٥ ، حيث أرسلت الصين ٤٠ ممثلا لمعظم الدول الغربية واحدة أو اثنين على الأكثر ، وتتضمن الإستراتيجية بناء تحالفات وشراكات لمواجهة الهيمنة المتصورة للولايات المتحدة في هذا المجال . حيث دافعت الصين عن فكرتها في مختلف المجالات الدبلوماسية في محاولة لإنشاء تحالف واسع من الدول يوافق على هذا المبدأ ، فقد أكدت قمة " البريكيس" لعام ٢٠١٦ 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 أيضا ، إضافة إلى ذلك وفي إطار إنجاز أهدافها بتقييد نشاطات الشركات الغربية وهيمنتها على الفضاء السيبراني ، فقد بادرت الصين إلى خطوات عملية من جانبها لتحقيق ذلك ، حيث شرعت في إنشاء بنية تحتية هائلة لربط الصين بالمحيط الهندي والخليج العربي وأوروبا بما سماه الخبراء الصينيون " طريق الحرير الرقمي " إلى جانب مشروعها العملاق المعروف بطريق الحرير الاقتصادي ، إلى جانب ذلك الطرق والجسور وخطوط السكك الحديد والمطارات فقد تم مد خطوط الألياف البصرية وشبكات الهواتف النقالة ومحطات الاتصال بالأقمار الصناعية ومراكز تجميع المعطيات والمدن الذكية ... الخ كجزء من الاستراتيجية السيبرانية الصينية [١٧] .

المحور الرابع: التنافس الامريكي الصيني في المجال السيبراني.

تعد روسيا والصين والولايات المتحدة من أكبر القوى في مجال الاستحواذ على القوة الإلكترونية القادرة على توفير أقصى درجات الأمن الإلكتروني security cyber ، وهو ما فرض على الدول وجود إجراءات حماية عبر تبني سياسات دفاعية تتضمن عمليات الحماية والتطوير لإجراءات الدفاع ضد الأخطار المحتملة وحماية نظم المعلومات ومنع تعرضها لعمليات هجومية معادية، وتعزيز الأمن الالكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحتية، ايضا من أجل ضمان امن وسلامة الفضاء الالكتروني ، إلى جانب تبني سياسات هجومية في الفضاء الإلكتروني عبر اتخاذ إجراءات لمهاجمة مصادر التهديد وتعقب الفاعليين في الهجوم على منشآت البنية التحية الحيوية ويتم استخدام نظم إلكترونية متقدمة كتطوير استخدام أسلحة إلكترونية في الحروب . ويشهد العالم تطورا حذرا وسريا في هذا الشأن[١٨].

اتسمت العلاقة بين الولايات المتحدة الامريكية والصين بأنها مزيج معقد يجمع ما بين التعاون تارة والتنافس والصراع تارة اخرى، فبعد انتهاء الحرب الباردة وظهور الصين كقوة صاعدة في النظام الدولي وعلى وجه الخصوص بروزها اقتصاديًا اذ اصبحت ثاني اكبر دولة اقتصاديًا بعد الولايات المتحدة الامريكية من ناحية الناتج المحلي الاجمالي وتعادل القوة الشرائية بالاضافة الى كونها دولة عضو دائم في مجلس الامن الدولي وسعيها الى الصعود بطريقة سلمية كل ما تقدم جعلها تقف بشكل مباشر بمقابل الولايات المتحدة الامريكية بمختلف الجوانب التي تعد الجوانب السيبرانية من اهمها[١٩] .

حيث كانت نتيجة للمتغيرات التي أحدثتها ثورة المعلومات والتكنولوجيا ، ظهر ما يعرف بحرب المعلومات الإستراتيجية ، التي عرفها البعض بأنها أعمال تقوم بها دول تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى ، بهدف تحقيق أضرار بالغة أو تعطيلها أو سرقة المعلومات » ، لذلك أصبحت حرب المعلومات شكلا من اشكال الصراع ، لذا فإن سلاح المعلومات اصبح أحد أهم الأسلحة التي تستخدمها الدول ، ولاسيما الدول المتقدمة ، لتحقيق أهدافها الإستراتيجية ، وفق ما أكده ديفيد جومبرت بقوله : « إن أحد الآثار المهمة الثورة المعلومات هو احتمال الوقوع الوشيك لحرب المعلومات ، أي الحرب التي يتم خوضها بالمعلومات بوصفها سلاحا أو هدفا رئيسا ترى الولايات المتحدة الأمريكية أن أكبر التهديدات التي يواجهها الأمن القومي الأمريكي في القرن الحادي والعشرين ، هو قضية الأمن الإلكتروني ، وهذه التهديدات متأتية من الصين ، إذ تعمل الأخيرة على سرقة معلومات التجارة الأمريكية ومعلومات و أسرار عسكرية ، مع توجيه هجمات الكترونية تعمل على تعطيل المنظومة

الإلكترونية الشبكات الدفاع والاستخبارات الأمريكية [٢٠]. لذلك تعد قضية أمن الانترنت من أبرز القضايا المؤثرة في العلاقات بين الصين والولايات المتحدة الأمريكية ، ولاسيما عام ٢٠١٣ .

إذ اتهمت الولايات المتحدة الأمريكية الصين بالقيام بأعمال تجسس السرقة معلومات عسكرية وتجارية سرية ، وقامت شركة مانديانت الأمريكية للأمن الإلكتروني بتقديم تقرير اتهمت فيه الجيش الصيني بشن هجمات الكترونية واسعة النطاق على مؤسسات أمريكية ، وإن الاتهامات المتبادلة بين الصين والولايات المتحدة الأمريكية تدلل على وجود تنافس دولي على ما يعرف بالذكاء الاصطناعي والقوة الالكترونية ، وبالتالي استخدام هذه الإمكانيات في تنفيذ هجماتها ، وسعي الدولة المستهدفة للحصول على التطور التكنولوجي واستخدامه ، وهذا ما أكدته ريفا جوجون كبيرة المحللين بمعهد سترانفورد الأمريكي للدراسات الأمنية والإستراتيجية بقولها : « إن التنافس بين اقطاب العالم ودوله الصغيرة على امتلاك أحدث برمجيات الذكاء الاصطناعي ، سيؤدي الى صراعات جديدة بسبب تخوف الأطراف الدولية من بعضها » ، وبالتالي فإن تقنية الذكاء الاصطناعي والحصول عليها أصبحت تحديا للدول الكبرى[٢١].

بالاضافة لما سبق فأن هناك العديد من الهجمات السيبرانية التي قام بها العديد من القراصنة الصينيون او تنسب الى الصين حيث تعتداهم اوجه التنافس السيبراني الصيني الامريكي ، نذكر منها الاتي[٢٢] :

١.في عام ١٩٩٩ قام عدد من القراصنة الصينيون بمهاجمة مواقع الكترونية رسمية تابعة للولايات المتحدة الامريكية وتحديدا باختراق موقع البيت الابيض والاستحواذ على الاف المعلومات الرقمية عالية السرية.

٢.عام ٢٠٠٣ تم القيام بسلسلة من الهجمات السيبرانية ضد كبرى الشركات الصناعية الامريكة بواسطة تيتان راين "مطر العمالقة ".

٣.في عام ٢٠١٣ ووفقا لتقرير مانديات ، هاجمت الصين على الاقل ١٤١ مؤسسة صناعية امريكية بداية عام ٢٠٠٦ حيث ترتب على ذلك سرقة العديد من البيانات وبراءات الاختراع وحقوق الملكية الفكرية ونتائج بحث علمية وغيرها العديد من السرقات السيبرانية الاخرى .

٤.خلال عام ٢٠١٩ تمكن مهاجمون صينيون من الوصول لأدولت تابعة لوكالة الأمن القومي الأميركية باستخدام ثغرات خطيرة، حيث تم استخدام هذه الثغرات، التي كشفها تسريب لمجموعة "Shadow Brokers" في عام ٢٠١٧ ، بواسطة مجموعة القرصنة الإلكترونية الصينية المعروفة باسم "APT3" الصينية في عام ٢٠١٦.

٥.في اذار ٢٠٢١ قامت مجموعة قرصنة صينية تعرف باسم هافنيوم بأختراق شركة مايكروسوفت والاضرار بعشرا الالاف من الشركات والعملاء المستخدمين لبريد الكتروني مرتبط بمايكروسوفت.[٢٣]

استنادا الى ما تقدم ، فإن الأمن الالكتروني يعد من أهم المتغيرات الجديدة المؤثرة في التنافس الأمريكي – الصيني ، لأن امتلاك القوة التقنية والمعرفية هو قوة إضافية لعناصر قوة الدولة الشاملة في القرن الحادي والعشرين ، حيث تشكل عمليات القرصنة لغايات جمع المعلومات الاستخبارية والاطلاع على معطيات خاصة، جزء التجسس في الهجمات السيبرانية حيث لفت تقرير سنوي صدر عن مكتب المخابرات الوطنية الأمريكية(DNI) ، في كانون الثاني ٢٠٢٤ إلى تصاعد أنشطة التجسس السيبراني التي تقوم بها الصين في الآونة الأخيرة، وادعى التقرير أن الحكومة الصينية "طورت" قدراتها في الهجمات السيبرانية، بما في ذلك توجيه آراء المواطنين الأمريكيين، ان تصاعد الدور الصيني في المجال السيبراني هذا يعني التأثير في النطاقين الإقليمي والدولي للصين ، وهو الذي لا ترغب الولايات المتحدة به في سياق رغبتها المستمرة بالسيطرة والهيمنة على النظام الدولي .

المحور الخامس: التعاون الصيني الروسي في المجال السيبراني.

تسعى روسيا إلى إقامة علاقة دفاعية أكثر مؤسسية مع الصين من خلال المشاورات والتبادلات والمناورات والاتفاقيات المنتظمة التي تقنن التعاون الدفاعي التقني المتزايد. وبالكاد كان هذا التطور الأخير، فقد انبثقت سياسة التقارب هذه من الأيام الأخيرة للاتحاد السوفييتي، الأمر الذي أعاد صياغة علاقات روسيا مع الصين. وبناء على الاتفاقات التي تم التوصل إليها في التسعينيات وأوائل العقد الأول من القرن الحادي والعشرين لترسيم الحدود وتجريدها من السلاح، أمضت القوتان سنوات في الاستثمار في تدابير بناء الثقة، وآليات التشاور، وأطر التعاون الدفاعي، ومواءمة توقعاتهما للسياسة الخارجية.

وفي عملية تدريجية، عملت موسكو وبكين على الحد من تلك التي من شأنها أن تدفع القوتين إلى النظر إلى كل منهما على أنها تهديدات محتملة، مع زيادة التعاون العسكري تدريجيا. في اجتماع في أكتوبر ٢٠١٩، أعلن فلاديمير بوتين أن روسيا تساعد الصين في تطوير نظام إنذار مبكر بالصواريخ الباليستية. ومن دون تقديم تفاصيل ، اشار بوتين الى ان " هذا مسعى جاد للغاية سيزيد بشكل جوهرى وجذرى من القدرة الدفاعية لجمهورية الصين الشعبية لان الولايات المتحدة وروسيا فقط لديهما مثل هذا النظام فى الوقت الحالى " .[٢٤]

فيما يخص التعاون السيراني الروسي الصيني نجد ان في عام ٢٠١٥، وقع الرئيس الصيني شي جين بينغ والرئيس الروسي فلاديمير بوتين اتفاقية "حول التعاون في ضمان أمن المعلومات الدولي"، بالتالي فأنه من الأكثر واقعية أن نرى أن الاتفاق يعكس تصورات التهديد المشتركة بين الصين وروسيا، كما وفرت إطارا للتعاون المستقبلي في مجال مراقبة الإنترنت، يتضمن الاتفاق قائمة طويلة من التهديدات للاستقرار المحلي، وفي السنوات التي تلت توقيعه، يبدو أن غالبية التبادلات مصممة لتبادل التكنولوجيات والمعلومات والعمليات المتعلقة بمراقبة الإنترنت. ففي حزيران ٢٠١٩، على سبيل المثال، شارك وفد صيني في المؤتمر الدولي الروسي لأمن المعلومات وناقش مناورات قطع الشبكة الروسية. وبعد شهر سافر وفد من إدارة الفضاء الإلكتروني الصينية إلى موسكو واجتمع مع الهيئة التنفيذية الاتحادية الروسية المسؤولة عن الرقابة في وسائل الإعلام والاتصالات السلكية واللاسلكية للبحث في القضايا الهامة لا سيما السيبرانية منها، حيث وعلى مدى هذه السنوات، أدخلت موسكو سلسلة من القوانين الأكثر تقييدا للإنترنت. تطلب تشريعات مكافحة الإرهاب، المعروفة باسم قانون ياروفايا، من مقدمي خدمات الإنترنت ومشغلي الهواتف المحمولة ومحركات البحث وغيرها من خدمات الويب تخزين جميع حركة المرور الروسية، وافادت الانباء ان شركة الاتصالات الصينية العملاقة هواوى عقدت محادثات مع شركة بولات الروسية لصناعة معدات الاتصالات لتوفير اجهزة للمساعدة في التخزين . يمنح قانون الإنترنت السيادي، الذي دخل حيز التنفيذ في نوفمبر ٢٠١٩ ، السلطات الروسية القدرة على التحكم في حركة البيانات و – من الناحية النظرية – إغلاق الإنترنت الروسي عن بقية العالم. يتطلب القانون من مشغلي الاتصالات تركيب بعض الأجهزة والبرامج والمعدات الروسية المنشأ التي تقدمها Roscomnadzor لمواجهة التهديدات السيبرانية، بما في ذلك معدات فحص الحزم العميقة، ويساعد على إنشاء بنية تحتية للإنترنت تبدو أكثر تشابها مع الصين[٢٥].

كما ان هناك تعاون متزايد بين روسيا والصين على الجيل الخامس، الجيل القادم من شبكات الاتصالات السلكية واللاسلكية. ومع مواجهة هواوي مقاومة في الولايات المتحدة وأستراليا وبعض الدول الأوروبية، وسعت عملياتها في روسيا، وتزايدت عمليات البحث والتطوير ووقعت اتفاقيات تعاون مع الجامعات الروسية. ووقعت هواوي صفقة مع شركة الاتصالات MTS لتطوير شبكات الجيل الخامس، وأطلق الاثنان منطقة اختبار الجيل الخامس في موسكو في أكتوبر ٢٠١٩، وتتوقع الشركة مضاعفة عدد موظفيها في مجال البحث والتطوير أربع مرات في روسيا بحلول عام ٢٠٢٤، ليصل العدد الإجمالي إلى ٢٠٠٠ مهندس كما أفادت التقارير أن هواوي أعلنت

عن توظيف مهندسين ذوي خبرة في المهارات الهجومية مثل استغلال الضعف واختبار الاختراق بالاضافة لما سبق تتعاون الصين مع روسيا في مختلف المجالات منها وتسعى كلا الدولتين لتطوير هذه القدرات بواسطة التعاون المشترك بهدف تطوير الجوانب الالكترونية والتقنية بالضد من الولايات المتحدة الامريكية[٢٦].

ولكن على الرغم من التصور والمصالح المشتركة للتهديد، هناك حدود لمدى التعاون الوثيق بين الجانبين الروسي والصيني ومن المرجح أن تظل بكين وموسكو حذرتين من القدرات السيبرانية للآخر، ونظرا للصلة القوية للقدرات السيبرانية بأجهزة الاستخبارات الخاصة بكل بلد، فمن غير المرجح أن يتقاسم الجانبان القدرات الهجومية ويبدو أن هذا النقص في تبادل التقنيات الهجومية ينعكس على جماعات القرصنة الإجرامية وغير الحكومية أيضا وتفيد شركات الأمن السيبراني عن القليل من التبادل أو التعاون بين القراصنة المجرمين الروس والصينيين حيث من المتوقع ان سيظل الدفاع هو محور التعاون الرئيسى للجانبين[٢٧] .

المحور السادس: مشروع الحزام والطريق الرقمي

تتكون " مبادرة الحزام والطريق" من مجموعة كبيرة من الممرات والطرق البرية والبحرية و خطوط الانابيب وشبكات الاتصالات وتكنلوجيا المعلومات وغيرها والتي تنطلق من الصين وصولا الى قارة اوروبا مارة بجميع المناطق الواقعة ضمن هذا المسار ، حيث يعد مشروع الحزام والطريق الرقمي احد اهم هذه المسارات الذي وضع حديثا حيث تولى رئاسة برنامج «الحزام والطريق الرقميّ» Digital Belt and Road Program (DBAR) الذي دشّنه في عام ٢٠١٦ علماء صينيون بالتعاون مع خبراء من ١٩ دولةً و٧ منظمات دولية.

يتمثّل الهدف من هذا البرنامج في تحسين عمليات الرصد البيئيّ، وتعزيز مشاركة البيانات، ودعم صنع السياسات، وذلك باستخدام البيانات الضخمة الناتجة عن عمليات رصد كوكب الأرض. وتستثمر الأكاديمية الصينية للعلوم (CAS) أكثر من ٢٠٠ مليون يوان (ما يعادل ٣٢ مليون دولار أمريكيّ) على مدار الأعوام الخمسة القادمة لدعم برنامج «الحزام والطريق الرقميّ»، حيث سيرصد البرنامج أنواعًا مختلفة من النظم البيئية وتطوّرها، بما في ذلك الأراضي العشبية، والغابات، والأنهار الجليدية، والمناطق الحضرية، والأراضي الزراعية، والمناطق الساحلية. وستتم مشاركة المعلومات البيئية والاجتماعية والاقتصادية من خلال منصة للبيانات الأرضية الضخمة، من المقرر إطلاقها في الفترة ما بين عامي ٢٠١٦ و٢٠٢٦. ستتيح هذه البوابة – التي ستعمل بنظام "الوصول المفتوح" – للباحثين وصنّاع السياسات والجمهور تتبُّع التغيّرات، وحركات

التنمية، والاتجاهات السائدة. كما سيتحقق البرنامج من المقاييس والمؤشرات من أجل توفير البيانات والمعلومات لأهداف التنمية المستدامة لمنظمة الأمم المتحدة لعام ٢٠٣٠[٢٨].

يتضمن هذا المشروع انشاء شبكة متطورة من البنية التحتية الالكترونية والتي تستكمل مهمة ربط الصين بالعالم الخارجي في عصر التكنلوجيا حيث بدأت فكرة انشاء هذا المشروع عام ٢٠١٥ لدى انعقاد "ورشة عمل الصين _ الاتحاد الاوربي للتعاون الرقمي" في بروكسل، حيث كان التصور آنذاك ان يتكون المشروع من كابلات ضوئية وشبكات للهاتف المحمول فضلا عن تطوير التجارة الالكترونية بين الصين والدول الاعضاء في المبادرة حيث اعلن الرئيس الصيني عن البداية الفعلية لهذا المشروع عام ٢٠١٨ ، والذي اكد على ان المشروع سوف يساعد الدول الاخرى على تطوير بنيتها التحتية الرقمية وتعزيز الامن السيبراني ، حيث اوضح "تشن تشاو شيونج "نائب وزير الصناعة وتكنلوجيا المعلومات الصيني ان الهدف من هذا المشروع خلق " مجتمع ذي مصير مشترك في الفضاء السيبراني" ، وتعتبر مدينة شيان احدى العواصم القديمة للصين ، واحدى اهم المدن التي تمد الجيش الصيني بالخبراء الفنيين ، هي مركز هذا المشروع حيث تسعى الصين الى تحويل هذه المدينة الى احدى مراكز التكنلوجيا المتقدمة[٢٩].

يستهدف هذا المشروع فتح اسواق جديدة للتجارة الالكترونية اما المنتجات الصينية ، لا سيما ان هناك فرصا كبيرة لنمو التجارة الالكترونية حيث تأتي في مقدمة هذه الفرص الاستثمارات الصينية واسعة النطاق في مختلف دول العالم كذلك توسعها (الصين) في انشاء مشروعات قائمة على التكنلوجيا الامر الذي سوف يزيد من عدد مستخدمي الانترنت لا سيما بين فئة السباب بالتالي المساعدة في ايجاد اسواق رائجة لتصريف المنتجات عبر التسويق الالكتروني لها [٣٠].

خلاصة لما سبق يمكننا ان نعد مشروع الحزام والطريق الرقمي احد اهم النماذج التطبيقية للاستراتيجية السيبرانية الصينية ، لما له من اهمية كبيرة في استخدام وتوظيف الجانب المعلوماتي والتكنلوجي لأغراض سياسية واقتصادية وغيرها حيث يدخل الجانب السيبراني بشكل كبير في تطوير وانجاح هذا المشروع .

الخاتمة

إن تطور وسائل الاتصالات ووسائطها ساهم في زعزعة الوظيفة التوجيهية للدولة في كل ما يتعلق بالتحكم في الفضاء السيبراني ، بحيث أضحى مفهوم الحدود السياسية والجغرافية وكذلك مفهوم السيادة ومفهوم الاستقلال عن الآخرين من المفاهيم التي لا يمكن الاعتداد بها . إذ أثرت المتغيرات الدولية التي رافقت تطور الفضاء السيبراني على مفهوم السيادة الوطنية ونطاق تطبيقه في المجالين الداخلي والخارجي على حد سواء ، وقد أثارت تلك المتغيرات تحديات طالت

كل أنماط الدول وطرحت نفسها بأشكال مختلفة على تلك الأنماط ، بالنسبة للصين بعد أن اتخذت في البداية موقفًا دفاعيًا وتفاعليًا نسبيًا بشأن الحوكمة العالمية للفضاء الإلكتروني ، تبنت الصين في عهد الرئيس شي جين بينغ استراتيجية إلكترونية أكثر نشاطًا، لهذه الاستراتيجية ثلاثة أهداف أساسية: الحد من التهديد الذي قد يشكله الإنترنت وتدفق المعلومات على الاستقرار الداخلي وشرعية النظام ؛ تشكيل الفضاء الإلكتروني لتوسيع نفوذ بكين السياسي والعسكري والاقتصادي؛ ومواجهة مزايا الولايات المتحدة في الفضاء الإلكتروني مع زيادة مساحة الصين للمناورة ، يعد المبدأ الأول المدرج في الاستراتيجية الإلكترونية الوطنية لعام ٢٠١٦ هو "احترام وحماية السيادة في الفضاء السيبراني". المهمة الإستراتيجية الأولى هي "الدفاع بحزم عن السيادة في الفضاء السيبراني" و "معارضة جميع الأعمال التي تهدف إلى تقويض النظام الوطني لبلدنا أو تدمير سيادة بلادنا من خلال الشبكة".

ان الأمر الذي دفع السلطات الحكومية الصينية إلى السعي الحثيث لبناء منظومة تقنية فعالة ل " أمن الشبكات " ، في بيئة تزدهر فيها الجريمة الإلكترونية وتراخي القانون وتطبيق غير متكافئ لآلياته ، لذا مثل تشريع الصين ل " قانون الأمن السيبراني " خطوة مهمة لمعالجة هذه القضية الحساسة وتأثيرها الكبير على الأمن الوطني للدولة ، ويعكس هذا القانون اتجاها عالميا واسع النطاق لتنظيم أنشطة الفضاء السيبراني ومكافحة التهديدات السيبرانية التي يمكن أن تقوض الأمن الوطني لدول العالم المختلفة .

فالصين ترى أن نطاق الفضاء السيبراني يجعل من المستحيل على ممثل واحد أن يديرها في إشارة واضحة إلى الهيمنة الأمريكية ، والنتيجة هي وجود العديد من المصالح والجهات الفاعلة والإيديولوجيات التي تتصادم بشكل متكرر ، قد تكون النتيجة هي منافسة متبادلة المنفعة أو يمكن أن يتحول الاحتكاك إلى صراع مدمر خاصة بين الولايات المتحدة والصين . لذلك تسعى الصين إلى توسيع نطاق سيادتها السيبرانية وتخصص من أجل ذلك موارد هائلة خاصة في ميدان الصناعات الالكترونية ، وذلك لإنشاء فضاء تتحكم فيه وطنيا الأمر الذي يخرجها شيئا فشيئا من دائرة الهيمنة والاحتكار الذي تمارسه الشركات الأمريكية في هذا المجال ، وهو مجال حيوي ويمثل أفقا مستقبليا يرسم الكثير من ملامح العلاقات الدولية في العقود القادمة ، ويحدد بشكل كبير نظام توازنات القوة الدولية ، وبالتالي لا يمكن إرجاع دوافع تبني الصين لسيادتها في الفضاء السيبراني إلى بعد واحد فقط ، بل هي أبعاد : سياسية ، اقتصادية ، أمنية ، ثقافية ، وأخرى مرتبطة أساسا بالتطلعات العالمية الصينية .

الهوامش

مجلة مركز بابل للدراسات الإنسانية ٢٠٢٥ المجلد ١٥/ العدد ٥

[1] هبة نصير عبد الرزاق ، الذكاء الاصطناعي: تهديدات القرن الحادي والعشرين وكالة DARPA انموذجًا، مجلة المستنصرية للدراسات العربية ولدولية ، الجامعة المستنصرية ، العدد ٨٧، ٢٠٢٤، ص١٣٥.

[2] علي زياد العلي، الصراع والامن الجيوسبراني في السياسة الدولية ، دار امجد للنشر والتوزيع ، ط١، الاردن، ٢٠١٩، ص١٦٦.

[3] المصدر نفسه ، ص١٦٧_١٦٨.

[4] علي زياد العلي ، مصدر سبق ذكره ، ص١٦٨.

[5] سما طاهر مسلم ، تأثير الذكاء الاصطناعي على صنع القرارات السياسية: نماذج مختارة ، المجلة السياسية والدولية ، الجامعة المستنصرية ، العدد ٦٢، ٢٠٢٥، ص٣٩٥.

[6] فاطمة عوامر، تأثر القوة السيبرانية على الاستراتيجيات الامنية للدول الكبرى ، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية ، ٢٠١٨،ص٥٥-٥٨. رسالة ماجستير منشورة على الرابط التالي: https://dspace.univ-ouargla.dz/jspui/handle/123456789/19660

[7] سميرة شرايطية، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية المجلد ٩، العدد ١٦ ،٢٠٢٠، ص٤٠٠_٤٠٢.

[8] فرح عصام ، استراتيجية تشي الثورية ..كيف تغير الصين مستقبل الانترنت في العالم ، مقالة منشورة على شبكة المعلومات الدولية ،على الرابط التالي : https://www.aljazeera.net/midan/reality/politics/2020/7/2/%D8%A7%D9%84%D8%B5%D9%8A%D9%86-%D9%88%D8%AD%D9%83%D9%85-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%87%D9%84-%D9%8A%D9%86%D8%AA%D9%87%D9%8A-%D8%B9%D8%B5%D8%B1

[9] إيهاب خليفة ، القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت الولايات المتحدة الأمريكية نموذجا " ، العربي للنشر و التوزيع ، مصر ، ٢٠١٧. ٢٥٦ .

[10] سميرة شرايطية ، مصدر سبق ذكره، ص٤٠١.

[11] اكرم حسام فرحات، حوائط الردع ..الجدار السيبراني الصيني في مواجهة مشروع العقل الامريكي، مقالة منشورة على شبكة المعلومات الدولية على الرابط التالي: https://tahreersr.com/reports/%D8%AD%D9%88%D8%A7%D8%A6%D8%B7-%D8%A7%D9%84%D8%B1%D8%AF%D8%B9-%D8%A7%D9%84%D8%AC%D8%AF%D8%A7%D8%B1-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D8%B5%D9%8A%D9%86%D9%8A-%D9%81/

[12] حرب الانترنت ..او حين تتحد ايران والصين ضد امريكيا، مقالة منشورة على شبكة المعلومات الدولية على الرابطالتالي : https://www.aljazeera.net/news/politics/2019/7/7/%D9%87%D9%8A%D9%85%D9%86%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%AD%D8%B1%D8%A8-%D8%A8%D9%83%D9%8A%D9%86-%D8%B7%D9%87%D8%B1%D8%A7%D9%86-%D9%88%D8%A7%D8%B4%D9%86%D8%B7%D9%86

[١٣] نسيمة طويل ، الاستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا : دراسة لمرحلة ما بعد الحرب الباردة ، جامعة باتنة ، كلية الحقوق والعلوم السياسية ،اطروحة دكتوراه منشورة ، ٢٠٠٩، ص١١١،١١٣.

[١٤] فائز السعدون ،الصين .. تحديات السيادة التكنلوجية ، مقال منشور على شبكة المعلومات الدولية على الرابط التالي : https://bit.ly/2XQmCF6

[١٥] تشين يانغ وان، لماذا يتهيب الغرب من شركة هواوي الصينية للاتصالات ، مقال منشور على شبكة المعلومات الدولية على الرابط التالي: https://bbc.in/2Ns75cH .

[١٦] محمد وائل ، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو_معلوماتية والفضاء السيبراني ، مجلة دراسات اقليمية ، العدد ٤٤، ٢٠٢٠، ص١٤٨.

[١٧] محد يوسف كيطان ،"استراتيجية الأمن الوطني السيبراني للصين : قراءة في قانون الأمن السيبراني الصيني"، مقالة منشورة على بكة المعلومات الدولية على الرابط التالي : http://www.alnahrain.iq/post/2422018/05/8.

[١٨] نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني " التهديد المتصاعد لامن الدول" ، مجلة مركز بابل للدراسات الانسانية ، مجلد٨، العدد ٢، ٢٠١٨، ص١٩٩-٢٠٠.

[١٩] هناء عبدالغفار حمود ، النزاع التجاري الامريكي- الصيني : الدوافع والانعكاسات الاقتصادية عالميًا، مجلة الادارة والاقتصاد، الجامعة المستنصرية ، العدد ١٢٩ ، ٢٠٢١، ص١٨٤.

[٢٠] باهر مردان ،العلاقات الامريكية الصينية دراسة في الحوار الاقتصادي والاستراتيجي، انكي للنشر والتوزيع ، ط١، بغداد ٢٠٢٠، ص٩٥.

[٢١] باهر مردان، مصدر سبق ذكره، ص٩٧.

[٢٢] تقرير يكشف معلومات عن الهجمات السيبرانية الصينية ضد أميركا، على الرابط التالي ، https://www.alhurra.com/

[٢٣] "عشرات الآلاف" من عملاء مايكروسوفت ضحايا حملة قرصنة مرتبطة بالصين، مقالة منشورة على شبكة المعلومات الدولي على الرباط التالي: https://www.alhurra.com/tech/2021/03/06/%D8%B9%D8%B4%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%A2%D9%84%D8%A7%D9%81-%D8%B9%D9%85%D9%84%D8%A7%D8%A1-%D9%85%D8%A7%D9%8A%D9%83%D8%B1%D9%88%D8%B3%D9%88%D9%81%D8%AA-%D8%B6%D8%AD%D8%A7%D9%8A%D8%A7-%D8%AD%D9%85%D9%84%D8%A9-%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D9%85%D8%B1%D8%AA%D8%A8%D8%B7%D8%A9-%D8%A8%D8%A7%D9%84%D8%B5%D9%8A%D9%86

[24] MICHAEL KOFMAN ،THE EMPERORS LEAGUE: UNDERSTANDING SINO-RUSSIAN DEFENSE COOPERATION، https://warontherocks.com/ .

[25] ADAM SEGAL ،PEERING INTO THE FUTURE OF SINO-RUSSIAN CYBER SECURITY COOPERATION، https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

[٢٦] تيموثي آر هيث ، كريستين غانيس ، كورتيز إي كوبر، اعادة تطوير الصين وجيش التحرير الشعبي، مؤسسة راند البحثية، نيويورك ٢٠١٦ ، ص٥٨.

[27] Adam Segal ،Chinese Cyber Diplomacy in a New Era of Uncertainty ،A Hoover Institution Essay ،Stanford University،p25.

[٢٨] جوو هوادونج، نحو انشاء طريق الحرير الرقمي، مقالة منشورة على شبكة المعلومات الدولية على الرابط التالي: https://arabicedition.nature.com .

[٢٩] علي صلاح، عبدالوهاب منصور، كيف تربط الصين اقتصادها بالعالم الخارجي، ملحق لمجلة اتجاهات الاحداث ،مركز المستقبل للابحاث والدراسات، العدد ٢٦، الامارات ،٢٠١٨، ص٦.

[٣٠] المصدر نفسه ، ص٧.

قائمة المصادر:

1.Adam Segal ،Chinese Cyber Diplomacy in a New Era of Uncertainty ،A Hoover Institution Essay ،Stanford University.

2.ADAM SEGAL ،PEERING INTO THE FUTURE OF SINO-RUSSIAN CYBER SECURITY COOPERATION، https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

3.MICHAEL KOFMAN ،THE EMPERORS LEAGUE: UNDERSTANDING SINO-RUSSIAN DEFENSE COOPERATION، https://warontherocks.com/ .

٤.اكرم حسام فرحات، حوائط الردع ..الجدار السيبراني الصيني في مواجهة مشروع العقل الامريكي، مقالة منشورة على شبكة المعلومات الدولية على الرابط التالي: https://tahreersr.com/reports/%D8%AD%D9%88%D8%A7%D8%A6%D8%B7-%D8%A7%D9%84%D8%B1%D8%AF%D8%B9-%D8%A7%D9%84%D8%AC%D8%AF%D8%A7%D8%B1-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9/%8A-%D8%A7%D9%84%D8%B5%D9%8A%D9%86%D9%8A-%D9%81

٥.إيهاب خليفة ، القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت الولايات المتحدة الأمريكية نموذجا " ، العربي للنشر و التوزيع ، مصر ، ٢٠١٧.

٦.باهر مردان ،العلاقات الامريكية الصينية دراسة في الحوار الاقتصادي والاستراتيجي، انكي للنشر والتوزيع ، ط١، بغداد ٢٠٢٠.

٧.تشين يانغ وان، لماذا يتهيب الغرب من شركة هواوي الصينية للاتصالات ، مقال منشور على شبكة المعلومات الدولية على الرابط التالي: https://bbc.in/2Ns75cH .

٨. تقرير يكشف معلومات عن الهجمات السيبرانية الصينية ضد أميركا، على الرابط التالي ، https://www.alhurra.com/

٩.تيموثي آر هيث ، كريستين غانيس ، كورتيز إي كوبر، اعادة تطوير الصين وجيش التحرير الشعبي، مؤسسة راند البحثية، نيويورك ٢٠١٦ .

١٠.جوو هوادونج، نحو انشاء طريق الحرير الرقمي، مقالة منشورة على شبكة المعلومات الدولية على الرابط التالي: https://arabicedition.nature.com .

١١.حرب الانترنت ..او حين تتحد ايران والصين ضد امريكيا، مقالة منشورة على شبكة المعلومات الدولية على الرابط التالي: https://www.aljazeera.net/news/politics/2019/7/7/%D9%87%D9%8A%D9%85%D9%86%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-

%D8%AD%D8%B1%D8%A8-%D8%A8%D9%83%D9%8A%D9%86-%D8%B7%D9%87%D8%B1%D8%A7%D9%86-%D9%88%D8%A7%D8%B4%D9%86%D8%B7%D9%86

١٢.سما طاهر مسلم ، تأثير الذكاء الاصطناعي على صنع القرارات السياسية: نماذج مختارة ، المجلة السياسية والدولية ، الجامعة المستنصرية ، العدد ٦٢، ٢٠٢٥.

١٣.سميرة شرايطية، السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي، المجلة الجزائرية للأمن والتنمية المجلد ٩، العدد ١٦ ،٢٠٢٠.

١٤.عشرات الآلاف من عملاء مايكروسوفت ضحايا حملة قرصنة مرتبطة بالصين، مقالة منشورة على شبكة المعلومات الدولي على الرابط التالي:
https://www.alhurra.com/tech/2021/03/06/%D8%B9%D8%B4%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%A2%D9%84%D8%A7%D9%81-%D8%B9%D9%85%D9%84%D8%A7%D8%A1-%D9%85%D8%A7%D9%8A%D9%83%D8%B1%D9%88%D8%B3%D9%88%D9%81%D8%AA-%D8%B6%D8%AD%D8%A7%D9%8A%D8%A7-%D8%AD%D9%85%D9%84%D8%A9-%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D9%85%D8%B1%D8%AA%D8%A8%D8%B7%D8%A9-%D8%A8%D8%A7%D9%84%D8%B5%D9%8A%D9%86

١٥.علي زياد العلي، الصراع والامن الجيوسبراني في السياسة الدولية ، دار امجد للنشر والتوزيع ، ط١، الاردن، ٢٠١٩

١٦.علي صلاح، عبدالوهاب منصور، كيف تربط الصين اقتصادها بالعالم الخارجي، ملحق لمجلة اتجاهات الاحداث ،مركز المستقبل للابحاث والدراسات، العدد ٢٦، الامارات ،٢٠١٨.

١٧.فاطمة عوامر، تأثر القوة السيبرانية على الاستراتيجيات الامنية للدول الكبرى ، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية ، ٢٠١٨،ص٥٥-٥٨. رسالة ماجستير منشورة على الرابط التالي: https://dspace.univ-ouargla.dz/jspui/handle/123456789/19660

١٨. فائز السعدون ،الصين .. تحديات السيادة التكنلوجية ، مقال منشور على شبكة المعلومات الدولية على الرابط التالي : https://bit.ly/2XQmCF6

١٩.فرح عصام ، استراتيجية تشي الثورية ..كيف تغير الصين مستقبل الانترنت في العالم ، مقالة منشورة على شبكة المعلومات الدولية ،على الرابط التالي :
https://www.aljazeera.net/midan/reality/politics/2020/7/2/%D8%A7%D9%84%D8%B5%D9%8A%D9%86-%D9%88%D8%AD%D9%83%D9%85-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%87%D9%84-%D9%8A%D9%86%D8%AA%D9%87%D9%8A-%D8%B9%D8%B5%D8%B1

٢٠. محد يوسف كيطان ،"استراتيجية الأمن الوطني السيبراني للصين : قراءة في قانون الأمن السيبراني الصيني"، مقالة منشورة على بكة المعلومات الدولية على الرابط التالي :
.http://www.alnahrain.iq/post/2422018/05/8

٢١. محمد وائل ، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو_معلوماتية والفضاء السيبراني ، مجلة دراسات اقليمية ، العدد ٤٤، ٢٠٢٠.

٢٢.نسيمة طويل ، الاستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا : دراسة لمرحلة ما بعد الحرب الباردة ، جامعة باتنة ، كلية الحقوق والعلوم السياسية ،اطروحة دكتوراه منشورة ، ٢٠٠٩.

٢٣. نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني " التهديد المتصاعد لأمن الدول" ، مجلة مركز بابل للدراسات الانسانية ، مجلد٨، العدد ٢، ٢٠١٨.

٢٤.هبة نصير عبد الرزاق ، الذكاء الاصطناعي: تهديدات القرن الحادي والعشرين وكالة DARPA انموذجًا، مجلة المستنصرية للدراسات العربية والدولية ، الجامعة المستنصرية ، العدد ٨٧، ٢٠٢٤.

٢٥.هناء عبدالغفار حمود ، النزاع التجاري الامريكي– الصيني : الدوافع والانعكاسات الاقتصادية عالميًا، مجلة الادارة والاقتصاد، الجامعة المستنصرية ، العدد ١٢٩ ، ٢٠٢١.

List of sources:

1.Adam Segal ،Chinese Cyber Diplomacy in a New Era of Uncertainty ،A Hoover Institution Essay ،Stanford University.

2.ADAM SEGAL ،PEERING INTO THE FUTURE OF SINO-RUSSIAN CYBER SECURITY COOPERATION، https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

3.MICHAEL KOFMAN ،THE EMPERORS LEAGUE: UNDERSTANDING SINO-RUSSIAN DEFENSE COOPERATION، https://warontherocks.com/ .

4.Akram Hossam Farahat, Walls of Deterrence... The Chinese Cyber Wall in the Face of the American Mind Project, an article published on the International Information Network at the link Next: https://tahreersr.com/reports/%D8%AD%D9%88%D8%A7%D8%A6%D8%B7-%D8%A7%D9%84%D8%B1%D8%AF%D8%B9-%D8%A7%D9%84%D8%AC%D8%AF%D8%A7%D8%B1-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D8%B5%D9%8A%D9%86%D9%8A-%D9%81/

5.Ihab Khalifa, Electronic Power: How Can Countries Manage Their Affairs in the Internet Age? The United States of America as a Model, Al-Arabi Publishing and Distribution, Egypt 2017.

6.Baher Mardan, US-China Relations: A Study in Economic and Strategic Dialogue, Anki Publishing and Distribution, 1st ed., Baghdad 2020.

7.Chen Yang Wan, Why the West is Afraid of the Chinese Telecommunications Company Huawei, an article published online at the following link: https://bbc.in/2Ns75cH.

8.A Report Reveals Information on Chinese Cyber Attacks Against America, available at the following link: https://www.alhurra.com/

9.Timothy R. Heath, Christine Gunness, and Cortez E. Cooper, The Re-Development of China and the People's Liberation Army, RAND Corporation, New York, 2016.

10.10. Guo Huadong, Towards the Establishment of a Digital Silk Road, an article published online at the following link: https://arabicedition.nature.com.

11.Cyber War... or When Iran and China Unite Against America, an article published online at the following link: Next: https://www.aljazeera.net/news/politics/2019/7/7/%D9%87%D9%8A%D9%85%D9%86%D8%A9-%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%AD%D8%B1%D8%A8-%D8%A8%D9%83%D9%8A%D9%86-%D8%B7%D9%87%D8%B1%D8%A7%D9%86-%D9%88%D8%A7%D8%B4%D9%86%D8%B7%D9%86

12.Sama Taher Muslim, The Impact of Artificial Intelligence on Political Decision-Making: Selected Models, Political and International Journal, Al-Mustansiriya University, Issue No. 62, 2025.

13.Samira Sharaitia, "Cyber Sovereignty in China: Between Power Requirements and National Security Necessities," Algerian Journal of Security and Development, Volume 9, Issue 16, 2020.
14.Tens of Thousands of Microsoft Customers Victims of a Hacking Campaign Linked to China, an article published on the Internet at the following link: https://www.alhurra.com/tech/2021/03/06/%D8%B9%D8%B4%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%A2%D9%84%D8%A7%D9%81-%D8%B9%D9%85%D9%84%D8%A7%D8%A1-%D9%85%D8%A7%D9%8A%D9%83%D8%B1%D9%88%D8%B3%D9%88%D9%81%D8%AA-%D8%B6%D8%AD%D8%A7%D9%8A%D8%A7-%D8%AD%D9%85%D9%84%D8%A9-%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D9%85%D8%B1%D8%AA%D8%A8%D8%B7%D8%A9-%D8%A8%D8%A7%D9%84%D8%B5%D9%8A%D9%86
15. Ali Ziad Al-Ali, Conflict and Geo-Cyber Security in International Politics, Dar Amjad for Publishing and Distribution, 1st ed., Jordan, 2019.
16. Ali Salah, Abdul Wahab Mansour, How China Links Its Economy to the Outside World, Supplement to the Journal of Events Trends, Future Center for Research and Studies, Issue 26, UAE, 2018.
17. Fatima Awamer, The Impact of Cyber Power on the Security Strategies of Major Powers, University of Kasdi Merbah, Ouargla, Faculty of Law and Political Science, 2018, pp. 55-58. Master's thesis published at the following link: https://dspace.univ-ouargla.dz/jspui/handle/123456789/19660
18. Fayez Al-Saadoun, China... Challenges of Technological Sovereignty, an article published on the Internet at the following link: https://bit.ly/2XQmCF6
19. Farah Essam, Xi's Revolutionary Strategy... How China is Changing the Future of the Internet in the World, an article published on the Internet at the following link: https://www.aljazeera.net/midan/reality/politics/2020/7/2/%D8%A7%D9%84%D8%B5%D9%8A%D9%86-%D9%88%D8%AD%D9%83%D9%85-%D8%A7%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%87%D9%84-%D9%8A%D9%86%D8%AA%D9%87%D9%8A-%D8%B9%D8%B5%D8%B1
20. Mohamed Youssef Keitan, "China's National Cybersecurity Strategy: A Reading of the Chinese Cybersecurity Law," an article published on the International Information Network at the following link: http://www.alnahrain.iq/post/2422018/05/8.
21. Muhammad Wael, The Future of Global Strategic Security in Light of Techno-Information Challenges and Cyberspace, Journal of Regional Studies, Issue 44, 2020.
22. Nasima Tawil, The American Security Strategy in Northeast Asia: A Study of the Post-Cold War Era, University of Batna, Faculty of Law and Political Science, published doctoral dissertation, 2009.
23. Noura Shaloush, Electronic Piracy in Cyberspace: The Rising Threat to State Security, Journal of the Babylon Center for Humanities Studies, Volume 8, Issue 2, 2018.
24. Hiba Nasir Abdul Razzaq, Artificial Intelligence: Threats of the 21st Century: DARPA as a Model, Al-Mustansiriya Journal of Arab and International Studies, Al-Mustansiriya University, Issue 87, 2024.
25. Hana Abdul Ghaffar Hamoud, The US-China Trade Dispute: Motives and Global Economic Implications, Journal of Administration and Economics, Al-Mustansiriya University, Issue 129 2021.