العدد ٣٢
السنة ٢٠٢٦

مجلة كلية القانون والعلوم السياسية
The College of Law and Political Science Journal

الاستراتيجية السيبرانية لجمهورية الصين الشعبية

هالة خالد حميد(*) ، هدى خلف علي(**)

(*) مدرس دكتور - جامعة بغداد Huda.ali2201@copolicy.uobaghdad.edu.iq

(**)جامعة بغداد dr.halakh@copolicy.uobaghdad.edu.iq

المستخلص

أدركت الصين منذ عام (١٩٩١) بعد حرب الخليج الثانية التحول الجوهري الكبير في طبيعة الصراعات الدولية، لاسيما الدور الحاسم للتكنولوجيا في الفضاء السيبراني لتحقيق التفوق العسكري على المستوى العالمي، بعد أن أظهرت حرب الخليج الفجوة الواضحة بين القدرات الصينية ونظيرتها الأمريكية، وقد أسهمت الدراسة التي تقدم بها ضباط من جيش التحرير الشعبي في ترسيخ القناعة الكاملة ومفادها أن المواجهة التقليدية مع الولايات المتحدة بشكل مباشرة لم يعد خيارًا واقعيًا، مما دفع الصين إلى تبني استراتيجيات بديلة تقوم على تطوير القدرات الهجومية والدفاعية في المجال السيبراني، وعلى اثر ذلك، عملت القيادة الصينية على إنشاء قيادة متخصصة بالأمن السيبراني، وتطوير وتحديث بنيتها المعلوماتية، ودمج الحرب السيبرانية ضمن عقيدتها العسكرية الشاملة، وتعتمد الاستراتيجية السيبرانية الصينية على مفهوم الحرب الشبكية التي تشمل المراقبة المتكاملة والسيطرة والحماية والهجوم، وتركز على شل قدرات الخصوم وإضعافهم في المراحل الأولى للمواجهة، ما يحقق لها التفوق الاستراتيجي ويعزز طموحاتها في الوصول إلى مكانة عسكرية متقدمة عالميًا.

الكلمات المفتاحية

الاستراتيجية السيبرانية الصينية، التنافس الامريكي الصيني، توظيف الفضاء السيبراني

للاستشهاد بهذا البحث:

حميد، هالة خالد، و علي، هدى خلف. "الاستراتيجية السيبرانية لجمهورية الصين الشعبية" . مجلة كلية القانون والعلوم السياسية، عدد ٣٢، ص ٣٥١-٣٦٧، https://doi.org/10.61279/1czndk56.

تاريخ الاستلام: ١٤ حزيران ٢٠٢٥ تاريخ القبول: ٢٠ أب ٢٠٢٦ تاريخ النشر ورقيا: ٢٥ نيسان ٢٠٢٦

متوفر على الموقع الالكتروني: ٢٥ نيسان ٢٠٢٦

متوفر على: https://jlps.edu.iq/index.php/jlps/ar/article/view/598

متوفر على: https://iasj.rdd.edu.iq/journals/journal/view/253

ترميز رقمي: https://doi.org/10.61279/1czndk56

مفهرسة على: https://doaj.org/toc/2664-4088

Issue 32
Year 2026

مجلة كلية القانون والعلوم السياسية
The College of Law and Political Science Journal

The Cyber Strategy of the People's Republic of China

Halah Khalid Hameed(*), Huda Khalaf Ali Ahmed(**)

(*)Lecturer Dr. - Baghdad University dr.halakh@copolicy.uobaghdad.edu.iq (**) Baghdad University Huda.ali2201@copolicy.uobaghdad.edu.iq

Abstract

The escalating cyber competition between the United States and China has become a crucial arena for conflict and influence within the international system. Amidst the rapid scientific and technological advancements in digital technology, big data, and artificial intelligence, the tremendous development of global information infrastructure at the dawn of the 21st century has led to the emergence of cyberspace as a new strategic field for competition among major powers, a vital arena for reshaping patterns of influence and power in international relations.

The cyber competition between China and the United States represents one of the most prominent manifestations of the nature of international conflicts. It is no longer limited to economic and military aspects but has expanded to include protecting cyberspace, controlling information, influencing the global digital economy, and securing critical infrastructure. Furthermore, China's rise as a cyber and technological power rivaling the United States, and its pursuit of developing unconventional military capabilities and achieving strategic parity, have contributed to redefining bilateral relations between the two powers and intensifying the competition between them. The two countries.

This thesis examines the digital and technological foundations upon which both the United States and China rely to build their technological and cyber capabilities. It analyzes the mechanisms of cyber deployment in both countries, including the application of technology in the fields of economics, defense, and security; the management of cyberspace; data protection; and the struggle for control over major technology companies. The thesis argues that cyberspace has become a decisive factor in managing conflict and competition between the two countries, and a fundamental element in reshaping the international order and the foundations of global power in the 21st century, making cyber technology a strategic resource no less important than traditional military and economic power.

Key Words

China's cyber strategy, US-China rivalry, use of cyberspace

Recommended citation

حميد، هالة خالد، و علي، هدى خلف. "الاستراتيجية السيبرانية لجمهورية الصين الشعبية" . مجلة كلية القانون والعلوم السياسية، عدد ٣٢، ص ٣٥١-٣٦٧، https://doi.org/10.61279/1czndk56.

Received 14 June 2025; accepted 20 Aug. 2025

published 25 April 2026 ; published online: 25 April 2026

Available online at: https://jlps.edu.iq/index.php/jlps/ar/article/view/598
Online archived copy can be found at: https://iasj.rdd.edu.iq/journals/journal/view/253
Indexed by: https://doaj.org/toc/2664-4088
Crossref DOI: https://doi.org/10.61279/1czndk56
This article has been reviewed under the journal's double-blind peer review policy.

المقدمة

خلال حرب الخليج الثانية في عام (١٩٩١) أدركت الصين ضعف قدراتها العسكرية مقارنة بمتطلبات الحروب الحديثة، وبالخصوص بعد توتر علاقتها مع تايوان حين هددت الولايات المتحدة الأمريكية بالرد على أي هجوم من الصين، وذلك بإرسال البوارج الحربية الأمريكية إلى بحر الصين الجنوبي، ما دفع الصين إلى إعادة النظر في خططها وتحديث قدراتها القتالية البحرية[١].أما التحول الذي حدث في العقيدة العسكرية الصينية، فجاء بعد ما نشر العقيدين في الجيش الصيني (وانغ شيان سوي وتشياو لينغ) تقريراً بعنوان (حرب غير مقيدة)، والذي أشار واوضح الفجوة الكبيرة بين الجيشين الأمريكي والصيني التي ظهرت بوضوح في حرب الخليج عام (١٩٩١)، حيث تمكنت الولايات المتحدة الأمريكية من حسم المعركة ضد العراق خلال (٤٢) يوم فقط باستخدام حرب التكنولوجيا المتقدمة والمعلومات، حيث لاحظا العقيدان أن الجيش العراقي والذي كان مجهز بأسلحة مشابهة لتلك التي يمتلكها الجيش الروسي والصيني، لم يصمد أمام تلك القدرات التكنولوجية الحديثة، وقد شكل هذا التقرير أساسًا لإصلاحات عميقة في الفكر العسكري والاستراتيجية العسكرية الصينية، إذ أصبح التركيز على تطوير قدرات هجومية متطورة تستهدف البنية التحتية للعدو، كالأنظمة المالية وشبكات الطاقة، كما أن روسيا والصين استخلصتا من التجربة الأمريكية في حرب الخليج أهمية المعلومات والتكنولوجي افي الحروب الحديثة، وبدأت الصين في بناء قدرات دفاعية وهجومية متقدمة على هذا الأساس، وقد لخّص الجنرال السوفيتي (س. بوغانوف جوهر) هذه التحولات بقوله: "لقد خسر صدام الحرب قبل أن تبدأ... كانت حرب استخبارات ومعلومات،، وتحكم وسيطرة، وهذا هو مستقبل الحروب"[٢]. ومن اجل توفير حماية أمنية لها من الأخطار المحتملة، مثل تفكك الإتحاد السوفيتي، وبداية الهيمنة الامريكية كقوة أحادية في النظام الدولي، إذ كانت حرب الخليج (١٩٩١) أول اختبار فعلي لهذه الهيمنة[٣].

ومع تغير الاستراتيجيات الدولية على وفق تغير أولويات السياسة الخارجية للدول الكبرى تجاه مناطق العالم بسبب التغير في احوال البيئة الدولية المؤثرة في مسار حركة الهيمنة فالثابت بان هذه الاستراتيجيات لن تخرج من هذه الاولويات لان المنافسة بين الولايات المتحدة

1 Thomas A. Johnson, CYBERSECURITY Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, p 159، Cybersecurity : protecting critical infrastructures from cyber attack and cyber warfare 9781482239225, 1482239221 - DOKUMEN.PUB

2 Quoted from : Thomas A. Johnson, aforementioned source , p 158

٣ صبا هاشم كمر، هالة خالد حميد، تأثير التحالفات الأمنية على ديناميات الصراع في منطقة الخليج العربي بعد ٢٠٠٣، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٧٠، ٢٠٢٥ , ص٣

والدول الكبار مثل الصين وروسيا سيعملون على ملئ الفراغ لأنها مركز الارتقاء الى الريادة العالمية لتتمتع بميزات جيواقتصادية وجيوستراتيجية فريدة[٤]. وبما ان الصفة العامة في العلاقات الدولية هي التغير المستمر بسبب التطورات الاقتصادية والعسكرية والسياسية والتكنولوجية ما ادى الى تحول في مفهوم القوة فقد تحول مفهوم القوة من القوة الصلبة الى الناعمة الى الذكية[٥].

وبعدما نشر العقيدان في جيش التحرير الشعبي الصيني دراستهما في عام (١٩٩٩)، خلصت الدراسة إلى أن مواجهة الولايات المتحدة الأمريكية في حرب (تقليدية) لم تعد ممكنة، ودعت الدراسة إلى تطوير قدرات الصين الدفاعية والهجومية في مجالات (غير تقليدية)، خاصة الفضاء السيبراني، وأشارت الدراسة إلى ضعف هيمنة الولايات المتحدة الأمريكية في هذا المجال (السيبراني)، وحثت الدراسة على تطوير هذا المجال لتحقيق مصالح الصين الوطنية، ويربط (ريتشارد كلارك) خبير الأمن السيبراني في الولايات المتحدة هذا التوجه بالعقيدة الصينية المعروفة بـ(شاشو جيان)، التي تعتمد على أسلحة (غير تقليدية) لاستهداف نقاط ضعف الخصوم، هذا وقد ارتبطت هذه العقيدة بوحدات سيبرانية صينية مثل (٦١٣٩٨ و٧٨٠٢٠)، التي وُجهت لها اتهامات من الإدارة الأمريكية منذ عام (٢٠١٣) بالتجسس وسرقة أسرار اقتصادية وعسكرية، ويعتبر الخبراء الغربيون، ومنهم (كلارك وهاريس وبرينر)، أن الحرب السيبرانية باتت سلاحًا رئيسًا في الحرب (غير المقيدة)، وتعد تهديدًا مباشرًا للاقتصاد العالمي وللأمن القومي[٦].

وقامت مجموعة القيادة المعلوماتية الصينية في عام (٢٠١٢)، بتحديث معاييرها التوجيهية من اجل مراجعة المخاوف التي تتعلق بالبنية التحتية الحيوية، إلا أن تركيز النخب الصينية ظل متذبذبًا، وأعلنت الصين في أعقاب قضية (إدوارد سنودن عام ٢٠١٤)، عن تأسيس "مجموعة قيادة الأمن السيبراني والمعلوماتية" برئاسة الرئيس الصيني (شي جين بينغ)، وتضم ٢١

٤ محمود فاضل حمود، عباس هاشم عزيز، تأثير المتغير العسكري الأمريكي في الواقع الامني لمنطقة الخليج العربي بعد عام ٢٠٠٣، مجلة العلوم السياسية، العدد ٦٤، كانون الاول، ٢٠٢٢، ص ١٦٦ – ١٦٧. لمزيد من المعلومات ينظر: https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/620/499

٥ إسراء شريف الكعود، أحمد كامل الخفاجي، تطبيق القوة الذكية في صراع القوى الاقليمية في الشرق الاوسط بعد ٢٠١١، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٦٢، ٢٠٢١،ص، لمزيد من المعلومات ينظر : https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/589/442

6 George Lucas, Ethics and Cyber Warfare, Ethics and Cyber Warfare The Quest for Responsible Security in the Age of Digital Warfare, 2016, p 5-8, Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare [1 ed.] 0190276525, 9780190276522 - DOKUMEN.PUB

عضواً من قيادات الحزب الشيوعي الصيني والدولة، بهدف التصدي للتهديدات السيبرانية وتنسيق السياسات السيبرانية وتعزيز الانضباط الحزبي، وأقرت الهيئة التشريعية العليا قانون الأمن السيبراني الصيني، في تشرين الثاني (٢٠١٦) الذي دخل حيز التنفيذ عام (٢٠١٧)، ليعكس جهود الصين في حماية أمنها القومي وتنظيم الفضاء السيبراني، ويركز القانون على حماية المعلومات الحيوية والبيانات الشخصية، ويلزم بتجميع البيانات داخل الصين وتنظيم استخدامها[٧]. وتسعى الصين، بوصفها ثالث اقوى دولة في العالم من حيث القوى العسكرية بعد الولايات المتحدة الامريكية وروسيا، وهي تعمل على تحديث قوتها المسلحة وفق توجيهات الرئيس الصيني (شي جين بينغ)، بهدف تحقيق التفوق العسكري العالمي بحلول عام ٢٠٤٩، وهذا السعي مدعومة بإنفاق عسكري كبير يعد الثاني عالمياً[٨] . لذلك انطلقت الصين تحت تأثير مرتكزات إيديولوجيا وسياسية من اجل السيطرة الاقتصادية والتكنولوجية[٩].

ولأول مرة أصدر مكتب معلومات شبكة الإنترنت الصيني في عام (٢٠١٢)، "الاستراتيجية الوطنية لأمن الفضاء السيبراني"، التي حددت موقف جمهورية الصين من حمايته الفضاء السيبراني وتنميته، وأشارت الوثيقة إلى تصاعد التهديدات السيبرانية بفعل التطور التقني، وهي تؤكد على أن التدخلات الخارجية والتجسس السيبراني يضر بالأمن الاقتصادي والسياسي وسلامة المعلومات، وأبرزت الاستراتيجية مهام وأهداف الصين في هذا المجال، وهي تدعوا إلى التعاون الدولي المبني على الثقة المتبادلة في مواجهة التهديدات المشتركة، ويؤكد الباحث الصيني (تشانغ لي) أن عدة دول كانت تنتظر صدور هذه الاستراتيجية من اجل توضيح موقف الصين في الجانب السيبراني[١٠] . وتعتمد الحرب السيبرانية في العقيدة الصينية على شبكة حرب سيبرانية متكاملة، تنسق العمليات الجوية

٧ **احمد يوسف كيطان**، استراتيجية الأمن الوطني الإلكتروني للصين: قراءة في قانون الأمن الإلكتروني الصيني، مركز النهرين للدراسات الاستراتيجية، ٢٠١٨/٤/١، منشور من خلال الرابط : مركز النهرين للدراسات والابحاث الإستراتيجية(alnahrain.iq) ، متوفرة على شكل ملف بصيغة pdf.

٨ أحمد عبد الأمير الأنباري، تعزيز فرص التنافس للقوى الفاعلة في النظام الدولي: دراسة في تأثير المتغيرين الاقتصادي والعسكري، جامعة بغداد/ كلية العلوم السياسية، مجلة تكريت للعلوم السياسية، ٢٠٢٢/٩/٣٠، ص ١٢.

٩ مرتضى جبار مكي، يسرى مهدي صالح، دور الهوية في التنافس والصراع بين الصين والهند، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٧٠ كانون الاول، ٢٠٢٥، ص ٢٦٠، لمزيد من المعلومات ينظر: https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/810/589

١٠ yang mu، الصين تصدر الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، خبر منشور على وكالة أنباء CCTV.COM العربية، ٢٠١٦/١٢/٢٧، شبكة الانترنت من خلال الرابط : الصين تصدر الإستراتيجية الوطنية لأمن الفضاء الإلكتروني CCTV.com_Arabic، تاريخ آخر زيارة في يوم ٣٠ / ٥ / ٢٠٢٥.

والبرية والبحرية عبر السيطرة على الطيف الكهرومغناطيسي، وهي تدمج القدرات التقنية الحديثة مع البنية العسكرية التقليدية، وأكد (بو شيونغ) قائد جيش التحرير الشعبي على ضرورة تطوير القدرة والانتصار باستخدام التكنولوجيا المتقدمة لمواجهة الهيمنة الأمريكية، ويصنف المحلل الأمريكي توماس القدرات السيبرانية الصينية في ثلاث مهام:

- المراقبة: لجمع المعلومات واستهداف البنى التحتية
- الهجوم: لتعطيل شبكات العدو
- الحماية: للوقاية من الهجمات المضادة.

وتركز العقيدة العسكرية على هزيمة العدو قبل بدء القتال وذلك من خلال هجمات منسقة وتفوق معلوماتي يستهدف البنية التحتية ونظم الحاسوب، فيما تسميه الصين حرب الوخز بالإبر، عبر استهداف نقاط الضعف لإرباك الخصم المتفوق تقنياً(١١).

وأصدر المكتب الوطني الصيني للمعلومات والإنترنت في (٢٧ / ١٢ / ٢٠١٦)، "الاستراتيجية الوطنية لأمن الفضاء السيبرانية"، التي أُقرت من قبل "القيادة المركزية للأمن الإلكتروني والمعلوماتية" تنفيذًا لتوجيهات الرئيس الصيني (شي جين بينغ)، تناولت الاستراتيجية الجديدة التحديات الأمنية المتزايدة بفعل التطور التكنولوجي والتقني، وأكدت أن الإنترنت بات أداة للتدخل في شؤون الدول الداخلية، وتهديدًا للأمن القومي وذلك من خلال سرقة المعلومات عبر الهجمات السيبرانية، ودعت الوثيقة إلى بناء فضاء سيبراني مستقر وآمن، وبالتعاون الدولي لاحترام سيادة الفضاء السيبراني(١٢). كما كشفت تقارير لجنة المراجعة الاقتصادية والأمنية الأمريكية-الصينية في الكونغرس الأمريكي عام (٢٠١١) عن تعزيز الصين لقدراتها في الحرب السيبرانية، معتبرة إياها بأنها جزءًا من تحقيق التفوق في المجال العسكري، ووسيلة لمواجهة خصوم أقوى، وذكر تقرير اخر منفصل من أن (١٢) مجموعة صينية مدعومة من الحكومة الصينية متورطة في هجمات سيبرانية ضد مؤسسات وشركات أمريكية، وتوصلت تحقيقات أمريكية، استناداً إلى مصادر من بينها وثائق (ويكيليكس)، إلى أن أبرز هذه الهجمات تنطلق من مكتب الاستطلاع الفني الأول في ولاية (تشنغدو)، أحد أبرز مراكز الحرب السيبرانية التابع للجيش الصيني، رغم نفي الصين بشكل

١١ سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص ٩٦.

12 可可, 国家网络安全战略发布提出九大战略任务, 新华社, 27/12/2016 ,https://www.infzm.com/contents/121860.

-Keke, "National Cybersecurity Strategy Released, Proposing Nine Strategic Tasks," Xinhua News Agency, December 27, 2016,

-كيكي، "إصدار استراتيجية الأمن السيبراني الوطنية، واقتراح تسع مهام استراتيجية"، وكالة أنباء شينهوا، ٢٧ ديسمبر/كانون الأول ٢٠١٦

مستمر لهذه الاتهامات، وهي تستخدم المتسللين المدنيين لغرض دعم عملياتها السيبرانية(١٣).

واتهمت الولايات المتحدة في عام (٢٠١٤)، خمسة ضباط من الوحدة (٦١٣٩٨) التابعة لجيش التحرير الشعبي الصيني بسرقة أسرار عسكرية وتجارية، من بينها معلومات عن طائرة (*F*-35) الهدف من اتهامهم لم يكن المحاكمة، بل لغرض إرسال رسالة مفادها أن التنصل من الهجمات السيبرانية لم يعد مقبولاً، وفي نهاية نفس العام، اتُهمت الولايات المتحدة كوريا الشمالية باختراق شركة (*Sony Pictures*) ردًا على فيلم ساخر عن زعيمها الذي يصور المحاولة الفاشلة لاغتيال (كيم جونغ أون)، وفي عام (٢٠١٥)، نسب هجوم سيبراني واسع إلى الصين، حيث أدى إلى سرقة بيانات حساسة تخص (٢١ مليون) موظف أمريكي، بما فيها بصمات الأصابع لموظفين، ما تسبب في استقالة "مدير المكتب الخاص بإدارة شؤون الموظفين" في الولايات المتحدة الأمريكية(١٤).

ويرى الخبير الأمريكي (آدم سيغال) أن الصين تفترض أن الولايات المتحدة الأمريكية تتجسس عبر منتجات شركاتها مثل (سيسكو ومايكروسوفت)، ولهذا تحظر الصين العديد من المنصات الأمريكية مثل (تويتر، ويوتيوب، وفيسبوك... إلخ) (١٥) وتطور نسخًا مخصصة من البرامج، مثل (*Windows* 10). للمستخدمين الحكوميين(١٦)، وأنشأت الصين في عام (٢٠١١)، الجيش الأزرق المختص في الحروب السيبرانية، بهدف تعزيز أمن الشبكات، واعتبرت هذا الجيش جزءًا من التدريب العسكري وتُتهم الصين أيضا باستخدام المدنيين والمتسللين من ضمن عملياتها السيبرانية لغرض سرقة التكنولوجيا، واستهداف البنى التحتية، وجمع معلومات استخباراتية، ووفقًا لتقارير أمريكية، فأن الصين تعمل على تطوير قدرات هجومية سيبرانية، وتجهّز قوات فضائية عسكرية تضم وحدات حرب سيبرانية، واستخبارات فضائية، وصواريخ نووية وقد أجرت سلسلة تجارب على تطوير أسلحة متقدمة، وصواريخ مضادة للأقمار الصناعية وغارات صوتية، مثل

13 JASON ANDRESS STEVE WINTERFELD LILLIAN ABLON, CYBER WARFARE Techniques, Tactics and Tools for Security Practitioners SECOND EDITION ,2013 , p 66 , Cyber Warfare [2nd edition] 9780124166721 - DOKUMEN.PUB

14 George Lucas , aforementioned source , p 5-8 .

١٥ علاء الجبالي، شركة Microsoft تطور نسخة خاصة من Windows 10 للحكومة الصينية، خبر منشور على مجلة TGTV الالكترونية، على شبكة الانترنت من خلال الرابط : شركة Microsoft تطوّر نسخة خاصة من Windows 10 للحكومة الصينية (tgtv.tn)، أخر زيارة في يوم ٢٠٢٥/٥/٣٠

١٦ **وكالة أنباء الشرق الأوسط المصرية**، الصين تستحدث ما يسمى بالجيش الأزرق لحماية شبكتها من القرصنة الإلكترونية، خبر منشور على شبكة الانترنت من خلال الرابط : الصين تستحدث ما يسمى بالجيش الأزرق لحماية شبكتها من القرصنة الإلكترونية - موقع الصين بعيون عربية(chinainarabic.org) ، أخر زيارة في يوم ٢٠٢٥/٥/٣٠.

الأسلحة الكهرومغناطيسية، والهدف من ذلك هو مواجهة التفوق العسكري الأميركي، بالخصوص في حال نشوب صراع حول (تايوان)[١٧].

وتشير تقارير رسمية من البنتاغون ولجان أمنية أميركية إلى تورط الصين في عمليات تجسس سيبراني واسعة استهدفت أسراراً عسكرية وتجارية، ضمن استراتيجية لخلق تفوق استراتيجي واقتصادي، وأنشأت الصين في عام (٢٠١٥)، (قوات الدعم الاستراتيجي) لتطوير قدراتها المعلوماتية والفضائية، ودمجها في عقيدتها العسكرية، ويرى الخبراء أن الصين تسعى لتأمين ردع استراتيجي، وتمكين جيشها من خوض حروب معلوماتية، إضافة إلى حماية مصالحها في الخارج، كما تؤكد الوثائق الغربية أن الصين تعتبر الفضاء السيبراني ساحة صراع أساسية، ما يفسر ارتفاع إنفاقها العسكري بشكل كبير، وسط مساعٍ لفرض نفسها كقوة عالمية كبرى[١٨].

ويرى جيمي ميتزل نائب الرئيس التنفيذي لجمعية آسيا, أن الصين واستناداً إلى تقارير رسمية، تُعد من أبرز الدول المتورطة في التجسس السيبراني والقرصنة السيبرانية، وهو ما أكده (البنتاغون عام ٢٠١٠)، مشيراً إلى أن الصين تطور قدراتها السيبرانية لاستهداف معلومات استراتيجية، كما أوضحت لجنة المراجعة الأمريكية / الصينية أن الحزب الشيوعي والحكومة الصينية ينفذون هجمات سيبرانية على أنظمة ومؤسسات أمريكية، وذكرت تقارير أخرى أن الصين تمارس التجسس التجاري كأداة استراتيجية لغرض تعزيز تفوقها العسكري والاقتصادي[١٩].

وأنشأت الصين (قوات الدعم الاستراتيجي) في عام (٢٠١٥)، باعتباره جزءً من إصلاحات واسعة في جيشها، لتطوير قدراته في الفضاء السيبراني ودمجها بالعمليات العسكرية، وتعد هذه القوات أداة رئيسية للردع الاستراتيجي، وتمكين الجيش في الحروب المعلوماتية، من حماية المصالح الصينية العالمية، وتتكون من وحدات متخصصة في إدارة الحروب السيبرانية وإطلاق وتشغيل الأقمار الصناعية، والاتصالات، والاستطلاع، والمراقبة من دون أن تكون قيادة

١٧ مي خلف، الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟، الخليج أونلاين، ٢٠١٦/١/٣، شبكة الانترنت من خلال الرابط : الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟ | الخليج أونلاين (alkhaleejonline.net) ، أخر زيارة يوم ٢٠٢٥/٥/٣٠.

١٨ مي خلف، الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟، الخليج أونلاين، ٢٠١٦/١/٣، شبكة الانترنت من خلال الرابط : الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟ | الخليج أونلاين (alkhaleejonline.net) ، أخر زيارة يوم ٢٠٢٥/٥/٣٠.

19 Jamie F. Metzl , China's Threat to World Order ,ASIA SOCIETY ,August 17, 2011 ,pdf ,Jamie Metzl: China's Threat to World Order - WSJ.

مستقلة كحال مثيلاتها في الولايات المتحدة الأمريكية[٢٠].

وتعد الصين (أول دولة) تنشئ وحدة متخصصة في الحرب السيبرانية، تركز على تطوير أسلحة النبض الكهرومغناطيسي هذه الأسلحة تشبه أشعة نبض (جاما) التي تحدث عندما يتم تفجير نووي، مما تسبب في تعطيل الأجهزة، ومن ضمن ها أجهزة الحاسب الآلي وغيرها من الأجهزة الالكترونية [٢١]. وبالخصوص في حال نشوب صراع حول (تايوان) وتُعرف هذه الأسلحة بمشروع (الورقة الرابحة)، وتطور الصين هذه الأسلحة بسرية تامة وباستخدام أحدث التقنيات[٢٢].

وتسعى الصين لضم (تايوان) بعدما تم دمج (هونغ كونغ وماكاو) [٢٣]. وقد رفعت إنفاقها العسكري من (١١٩ مليار دولار في عام ٢٠١١) إلى (٢٤٨ مليار دولار في عام ٢٠١٨)[٢٤]. رغم نفيها الدخول في سباق تسلح، وأثارت هذه التحركات قلق الولايات المتحدة الأمريكية، التي وصفت الدمج المدني/العسكري الصيني بأنه تهديد أمن ي، وقد أدرج الرئيس الصيني (شي جين بينغ) هذا الدمج ضمن خطته الإصلاحية لعام (٢٠١٦)، وشكل لجنة لتطوير تقنيات الاستخدام المزدوج، مما يعزز ترسانة الجيش الشعبي الصيني، ورداً على الهجمات السيبرانية الصينية المتزايدة، تتجه الولايات المتحدة الأمريكية لاتخاذ إجراءات صارمة، بعدما تبن تورط وحدات من جيش التحرير الشعبي في عمليات القرصنة والتجسس بشكل واسعة على مؤسسات وشركات أمريكية[٢٥].

وتواجه الولايات المتحدة منذ عقود هجمات صينية متطورة وأصبحت أكثر شبحية وتعقيداً العالم[٢٦] .ويصعب تعقبها الأميركية وقد أكد خبراء أن

٢٠ كيفين إل. بولبيترKevin. L. Pollpeter ،مايكل أس. تشيس Michael S. Chase ،إريك هيجينبوثام Eric Heginbotham، إنشاء قوات الدعم الاستراتيجي بجيش التحرير الشعبي الصيني وتداعياتها على العمليات الفضائية العسكرية الصينية، منشور من مؤسسةRAND ،سانتا مونيكا، كاليفورنيا، أعد لصالح القوات الجوية الأمريكية، ٢٠١٧، ix.

٢١ حياة حسين، الفضاء الإلكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية، المجلد ١٢، العدد ١، ٢٠٢١، ص ١٠٨٣.

٢٢ عادل عبد الصادق، مؤتمر حروب الفضاء السبراني، مصدر سبق ذكره.

٢٣ صامويل هنتنجتون، صدام الحضارات أعادة صنع النظام العالمي، ط٢، ترجمة طلعت الشايب، simon schustr &, Rockefeller center , نيويورك ١٩٩٦ , ص ٢٨٣ .

٢٤ احمد عبد الأمير الأنباري، قضايا دولية معاصرة، مصدر سبق ذكره .متوفرة على شكل ملف بصيغة pdf.

25 Anja Manuel and Kathleen Hicks , Can China's Military Win the Tech War? How the United States Should—and Should Not—Counter Beijing's Civil-Military Fusion , Can China's Military Win the Tech War? | Foreign Affairs

٢٦ نيويورك تايمز، تحولت الى التهديد الإلكتروني الأول.. كيف تستخدم الصين هجمات الشبح المعقدة ضد الولايات المتحدة؟، مقال منشور على قناة البسالة الالكترونية، شبكة الانترنت من خلال الرابط : تحولت الى التهديد الإلكتروني الأول.. كيف تستخدم الصين هجمات الشبح المعقدة ضد الولايات المتحدة؟(albasalh.com) ، أخر زيارة في يوم ٢٠٢٥/٦/١.

الاختراق الصيني لمكتب إدارة شؤون الموظفين عام (٢٠١٤) أدى إلى أضرار بالغة[٢٧]. وسط انتقادات لفشل الحماية الأمريكية للمعلومات الحساسة[٢٨]. وقد علق (مايكل هايدن) الرئيس السابق لوكالة الأمن الوطني، قائلاً: "التعليق المناسب هنا ليس (العار على الصين)، وإنما (العار علينا) لعدم توفيرنا الحماية المناسبة لهذا النمط من المعلومات"[٢٩].

وتعتبر الصين خصما رئيسًا للولايات المتحدة الأمريكية في المجالات التقليدية العسكرية وفي الفضاء السيبراني، وقد أظهرت الصين بوضوح طموحاتها للتفوق الاقتصادي والعسكري، وهي تستخدم الفضاء السيبراني كوسيلة لتحقيق هذه الأهداف، ففي الفترة ما بين (٢٠١٠ و٢٠١٥)، نفذ قراصنة صينيون هجمات سيبرانية ممنهجة على شركات صناعية أوروبية وأميركية، لسرقة معلومات عن تصنيع الطائرات المقاتلة وتجارية، وقد استُخدمت هذه البيانات في وقت لاحق في تطوير طائرات صينية تجارية[٣٠].

وازدادت المخاوف في الغرب والولايات المتحدة من قدرات الصين السيبرانية، وسط اتهامات للحكومة الصينية برعاية هجمات سيبرانية متكررة على مؤسسات وشركات وجامعات أميركية كبرى ونشر مركز الأمن الأميركي الجديد في هذا السياق دراسة بعنوان (الدولة المقاتلة)، وتناولت استراتيجية الأمن السيبراني الصيني دوافعها السياسية والعسكرية والاقتصادية، بالإضافة إلى رؤيتها للأنشطة الأميركية في الفضاء السيبراني[٣١].

ووفقاً لتقرير (البنتاغون)، أصبح الجيش الصيني يعطي أهمية كبرى للفضاء السيبراني، وخاصة مع تزايد اعتماد

---

٢٧ خطة أميركية للرد على "القرصنة الصينية"، خبر منشور على Sky News عربية، شبكة الانترنت من خلال الرابط: خطة أميركية للرد على "القرصنة الصينية" | "سكاي نيوز عربية (skynewsarabia.com) ، أخر زيارة يوم ٢٠٢٥/٦/١.

28 Anja Manuel and Kathleen Hicks , Can China's Military Win the Tech War? How the United States Should—and Should Not—Counter Beijing's Civil-Military Fusion , Can China's Military Win the Tech War? | Foreign Affairs

٢٩ هال براندز، حول الصراع الإلكتروني الروسي ـ الصيني ـ الأميركي، جريدة الشرق الأوسط، العدد ١٥٣٦٦، الأربعاء ٢٠٢٠/١٢/٢٣، منشورة من خلال الرابط : حول الصراع الإلكتروني الروسي ـ الصيني ـ الأميركي | الشرق الأوسط (aawsat.com)،متوفرة على شكل ملف بصيغة pdf.

٣٠ ديمتري ألبروفيتش، من أجل واقعية الكترونية لا توجد حلول تقنية لمشاكل جيوسياسية، مقال منشور على قناة اندبندنت عربية، ٢٠٢١/١٢/٢٥، شبكة الانترنت من خلال الرابط : من أجل واقعية الكترونية | اندبندنت عربية (independentarabia.com)، موعد أخر زيارة في٢٠٢٥/٦/١.

٣١ أسراء احمد إسماعيل، السيادة الإلكترونية :عناصر الإستراتيجية الصينية للأمن الإلكتروني، بحث منشور على مركز Future ، ٢٠١٥/٢/٥، من خلال الرابط : Future Center - عناصر الإستراتيجية الصينية للأمن الإلكتروني(futureuae.com) ، متوفر على شكل ملف بصيغة pdf.

الصين على الاقتصاد الالكتروني الرقمي، وتشير وزارة الدفاع الأميركية(البنتاغون) إلى أن الصين تعمل على تعزيز قدراتها السيبرانية من خلال تطوير التدريب والابتكار المحلي، بهدف سد الفجوة مع الولايات المتحدة الامريكية وقد وثّق التقرير عدداً من الهجمات والاختراقات الصينية على الشبكات الأميركية، وأكد أن الصين تستخدم تلك القدرات من اجل دعم جمع المعلومات الاستخباراتية والاقتصادية والدفاعية، مما يمكنها من بناء صورة واضحة عن البنية الدفاعية في الولايات المتحدة الأميركية لتستغلها في أوقات الأزمات[٣٢].وتركز الصين في عقيدتها السيبرانية على الحروب المستقبلية، التي تُستخدم فيها تقنيات الطيف الكهرومغناطيسي لتعطيل أنظمة العدو، خصوصاً مع إدراكها لاعتماد الغرب على بنى تحتية سيبرانية معقدة، ويُشتبه بأن اغلب القراصنة الصينيين أما مرتبطين بالجيش أو أنهم يحصلون على دعم من الاستخبارات الصينية والروسية [٣٣]. وعرضت الصين في السنوات الأخيرة (طائرتين شبح)، يُقال إنهما تشبهان الطائرتين الأميركيتين (*F*-22 و*F*-35)، التي تصنعها (شركة لوكهيد مارتن)[٣٤]. مما يعكس تفوق الصين وقفزتها التكنولوجية[٣٥]. ويرى مسؤولون أميركيون أن الفضاء السيبراني قد يتحول إلى ساحة للحرب بين البلدين، لأن التشابك الاقتصادي بينهما يجعل من الحرب التقليدية غير مربحة[٣٦].

كما وتستثمر الصين بكثافة في الدفاع السيبراني باعتباره وسيلة لتقليل الفجوة مع الولايات المتحدة وروسيا في القدرات التقليدية، ولا تقتصر جهودها على الوحدات العسكرية المختصة كالوحدة (٦١٣٩٨)، بل تشمل أيضاً تنظيم ميليشيات سيبرانية من المدنيين تجمع الأسرار التجارية والصناعية لغرض دعم الشركات الصينية، وتعد الولايات المتحدة بأن أكبر تهديد لها في مجال الحرب السيبرانية هي الصين، وتدرك الصين بدورها أن الولايات المتحدة الأمريكية خصم سيبراني لا يُستهان به ابدًا، مما يعزز احتمالية اندلاع صراع سيبراني في المستقبل، وبالخصوص في ظل الاعتماد الكامل

32 Steve Ranger, , China aims to narrow cyber warfare gap with US While US blames China for cyber attacks on networks, August 17, 2018 ,China aims to narrow cyberwarfare gap with US | ZDNet .

33 Steve Ranger, , China aims to narrow cyber warfare gap with US While US blames China for cyber attacks on networks, August 17, 2018 ,China aims to narrow cyberwarfare gap with US | ZDNet .

٣٤ اختراق شبكات الكمبيوتر الأمريكية يتيح كنزا ثمينا للمتسللين، مقال منشور على قناة وكالة النبأ الإخبارية، ٧/حزيران/٢٠١٥، شبكة الانترنت منشور من خلال الرابط : اختراق شبكات الكمبيوتر الامريكية يتيح كنزا ثمينا للمتسللين(annabaa.org) ، أخر زيارة في يوم ٢٠٢٥/٦/١.

35 Christopher White and Brian Mazanek, Understanding cyber warfare: politics, policy and strategy ,2019, p 84.

36 Thomas A. Johnson, aforementioned source, p 177.

للدولتين على الفضاء السيبراني في إدارة قطاعات الدولة والاقتصاد(٣٧).

واتهم تقرير الاستخبارات الأمريكية لعام (٢٠٢٣) بأن الصين تشكل أخطر تهديد سيبراني بشكل مستمر، بسبب تطورها الكبير في تنفيذ هجمات سيبرانية متقدمة، تشمل استغلال هجمات سلسلة التوريد، وثغرات (اليوم صفر)(*) إلى جانب استخدام أدوات شرعية لأغراض خبيثة من الصعب كشفها، كما تستعين الصين بالذكاء الاصطناعي من اجل تعزيز هجماتها من خلال تطوير أدوات رصد متقدمة وتحليل البيانات الضخمة، وتسعى الصين لتكون رائدة في الذكاء الاصطناعي بحلول عام (٢٠٣٠)، وفي هذا المجال من المرجح أنها تلجأ لسرقة التكنولوجيا الغربية والامريكية، كما فعلت في قطاعات أخرى مثل أشباه الموصلات، الفضاء بهدف دعم أمنها القومي وتسريع نموها التكنولوجي(٣٨).

وركزت الصين في السنوات الأخيرة على تعزيز أمنها السيبراني من خلال توجيهات عليا من قيادات في الحزب الشيوعي، وإنشاء مجموعات استراتيجية لتطوير هذا المجال، عسكريًا ومدنيًا وتشمل استراتيجية الصين ثلاثة محاور رئيسة:

١- سياسيًا: حماية السلطة عبر السيطرة على المعلومات والدعاية
٢- اقتصاديًا: حماية النمو من خلال التجسس الصناعي والتجاري.
٣- عسكريًا: الاستعداد لصراعات سيبرانية وتحقيق تفوق تقني عبر تحديث القدرات وبناء الكوادر.

كما وتسعى الصين لترويج رؤيتها حول (سيادة الدولة على الإنترنت)، دوليًا ومحليًا، لتبرير الرقابة الداخلية ومقاومة الهيمنة الأمريكية على الفضاء السيبراني، وعلى الرغم من الأولوية التي تحظى بها هذه الاستراتيجية، إلا أنها ما تزال تعاني من ضعف التنسيق وتضارب المصالح بين الجهات المختصة، ولا يتوقع من أن يتغير السلوك الصيني في الجانب السيبراني دون تغير في الحسابات الاستراتيجية أو تحولات سياسية كبرى، لذا تحتاج الولايات المتحدة إلى فهم أهداف الصين،

---

٣٧ فريق تحرير مجلة ن بوست، حروب الفضاء الإلكتروني، خبر منشور على قناة ن بوست الالكترونية، ٢٢ / ٢ / ٢٠١٥، منشور من خلال الرابط : حروب الفضاء الإلكتروني | نون بوست(noonpost.com) ، أخر زيارة في يوم ٢٠٢٥/٦/١، متوفر على شكل ملف بصيغة pdf.

* هي هجمات تستغل ثغرات أمنية غير مكتشفة أو غير معروفة من قبل مطوري البرامج أو الشركات المنتجة لها، مما يمنح المهاجمين نافذة زمنية قبل أن يتم إصدار تحديث أو تصحيح (Patch) لسد الثغرة، لمزيد من المعلومات ينظر : https://www.broadcom.com/company/newsroom/press-releases?filtr=zero-day ، أخر زيارة في يوم ٢٠٢٥/٦/١.

38 By Mercy A. Kuo , China's Cybersecurity and Statecraft Insights from Timothy Flannery, February 20, 2024, https://thediplomat.com/2024/02/chinas-cybersecurity-and-statecraft/?utm_source=chatgpt.com

والعمل باستراتيجية شاملة وتعاونية بين القطاعين الخاص والعام لضبط التوازن السيبراني(٣٩).

وتعد الاستراتيجية الصينية في الجانب السيبراني امتدادًا لفكر المفكر العسكري (صن تزو)، الذي ركز على تحقيق النصر من دون قتال(٤٠). وهو ما يظهر في التوجه الصيني نحو الحرب السيبرانية وقد شكلت حرب الخليج الثانية عام (١٩٩١) وتعد نقطة التحول في التفكير العسكري الصيني، إذ أدركت الصين أهمية التكنولوجيا الحديثة في الصراعات الجديدة، ما دفعها للتركيز على تطوير قدراتها السيبرانية في المعلومات والاتصالات لاستخدامها في الحروب المستقبلية، مستهدفة الريادة في هذا المجال بحلول عام (٢٠٥٠) ومنذ ذلك الحين، عملت الصين على ترسيخ أسس استراتيجية سيبرانية متكاملة عبر مبادراتها الحكومية وأدبياتها العسكرية مثل (المهام التاريخية الجديدة)، والورقة البيضاء للدفاع الوطني، وهي تولي أهمية خاصة للحرب السيبرانية في النزاعات المرتبطة (بتايوان والبحر الجنوبي)، حيث تسعى إلى توظيف الفضاء السيبراني لأغراض دفاعية وهجومية(٤١). وتتجلى رؤية الرئيس (شي جين بينغ) في تعزيز الدفاع النشط وتسريع تحديث الجيش الصيني(٤٢)، ما دفع جيش التحرير الشعبي لتطوير بنيته السيبرانية، وإطلاق طائرات إلكترونية مثل (CSA-003) للتجسس ومراقبة النشاطات السيبرانية للخصوم(٤٣). وتواصل استثمارها في تقنيات الإنترنت والمعلومات لتعزيز أمنها القومي وتأمين سيادتها الوطنية، استنادًا إلى مبدأ (الدفاع النشط) وتحقيق الجاهزية لمواجهة أي تهديد سيبرانية(٤٤).

ولقد وضع الزعيم الصيني (شي جين بينغ) في عام (٢٠١٣)، الأسس الإستراتيجية لمشروع (الحزام والطريق)، الذي يُنظر إليه كأداة لهيمنة الصين العالمية بحلول عام (٢٠٤٩)، ويهدف هذا المشروع لأن

39 Amy Chang, CNAS Releases Report on China's Cyber Strategy, December 03, 2014, https://www.cnas.org/press/press-release/cnas-releases-report-on-chinas-cyber-strategy?utm_source=chatgpt.com

٤٠ سون أتزو، فن الحرب، أعداد وترجمة رؤوف شبايك، ٢٠٠٧،ص ٢١،الفصل الثالث، الهجوم بالخداع (التخطيط للهجوم) المقولة الثانية، منشور من خلال الرابط : http://www.dawahmemo.com/image/2012-08-04-09_37_57figh.pdf، متوفر على شكل ملف بصيغة pdf.

٤١ علي زياد العلي، مصدر سبق ذكره، ص ١٦٨.

٤٢ إسراء شريف جيجان، مصدر سبق ذكره، ص٤٠.

٤٣ عمر حامد شكر، مصدر سبق ذكره، ص ٦.

٤٤ فريدة طاجن، تأثير القوة الإلكترونية على الاستراتيجيات الأمنية للدول الكبرى دراسة حالة الصين، مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، ٢٠١٨، ص ٦، متوفرة على شكل ملف بصيغة pdf .

يكون النسخة المتطورة والحديثة لطريق الحرير التاريخي، وذلك عبر إنشاء شبكة بنى تحتية برية، وبحرية، وجوية ضخمة، بل وحتى رقمية، تمتد عبر آسيا وأوروبا وإفريقيا، ويستهدف المشروع الدول الفقيرة بشكل خاص أو الدول التي تعاني من أزمات اقتصادية، لتكون أكثر قابلية للاندماج في هذا النظام الجديد بقيادة الصين، وقد كان من المتوقع أن تتربع جمهورية الصين الشعبية على عرش الاقتصاد العالمي بحلول عام (٢٠٣٢)، لكن (جائحة كورونا) ساهمت في تسريع هذا التقدم بشكل كبير، حيث توقعت المؤسسات المالية العالمية أن الصين ستحقق هذا الإنجاز بحلول عام (٢٠٢٨)، هذا التسارع وضع الولايات المتحدة الأمريكية في موقف محرج، قد يدفعها في المستقبل إلى تقبل صعود الصين كقوة منافسة لها، على غرار ما حدث مع الاتحاد السوفيتي السابق إبان الحرب الباردة، وبالتالي قد يشهد العالم عودة إلى نظام القطبية الثنائية: قطب تقوده الولايات المتحدة وحلفاءها في الغرب وبعض دول الشرق الأوسط، وقطب أخر تقوده الصين ويضم دول (مبادرة الحزام والطريق)، وفي هذه المرحلة، قد يلعب العالم العربي والشرق الأوسط دوراً محورياً يُرجّح كفة التوازن الدولي[٤٥].

الخاتمة

مما تقدم تبين أن الصين تسير بشكل ثابت نحو تحقيق أهدافها الاستراتيجية، وقد فهمت الصين أن التفوق على الولايات المتحدة الأمريكية لا يكون من خلال المواجهة العسكرية أو عبر التنافس على النفوذ في مناطق النفوذ مثل الشرق الأوسط، بل تكون من خلال القوة الاقتصادية والتكنولوجيا، فالصراع القادم سيكون على من يتمكن من الصمود ماليًا سيكون المنتصر، فأن الدول الكبرى تدرك تماما أن أي حرب مباشرة بين دولتين كبيرتين (قوتين عظيمتين) ستتجه بشكل سريع نحو السلاح النووي، ما يعني دمارًا متبادلاً لكلا الطرفين ولا توجد مصلحة فيه لأي طرف من الأطراف، وهو ما يجعل الحرب خيارًا غير عقلانيًا، وتضح أن الصين توظف الفضاء السيبراني باعتباره أداة استراتيجية من اجل دعم قوتها العسكرية والاقتصادية، عبر التجسس والاختراقات الصناعية التي تستهدف المؤسسات الغربية، وقد طورت الصين بنيتها السيبرانية وذلك بدمج القدرات المدنية والعسكرية، مما يعكس إدراكها لأهمية الحرب السيبرانية، وعلى الرغم من مشاركتها في الاتفاقيات الدولية، تتمسك الصين بمبدأ (السيادة السيبرانية) لحماية نظامها السياسي والاقتصادي، ما يشكل تحدياً مباشراً للولايات المتحدة والغرب ويستدعي استراتيجيات ردع متزنة لحماية أمنها القومي.

٤٥ عز الدين قداري الإدريسي، استراتيجية الصين في الهيمنة على العالم، مركز حمورابي للبحوث والدراسات الاستراتيجية، ٧ كانون الأول ٢٠٢١، ص ٣ – ٦.

إقرار تضارب المصالح

يُقر المؤلف بعدم وجود أي تضارب محتمل في المصالح فيما يتعلق بالبحث أو التأليف أو نشر هذا المقال.

التمويل

لم يتلقَ المؤلف أي دعم مالي لإجراء هذا البحث أو تأليفه أو نشره.

البيان الأخلاقي

هذا البحث يتوافق مع المعايير الأخلاقية لإجراء الدراسات العلمية. وقد تم الحصول على موافقة خطية من جميع المشاركين الأفراد المشمولين في الدراسة.

بيان توفر البيانات

البيانات متاحة عند الطلب من المؤلف المراسل.

الشكر والتقدير

لا يوجد شكر وتقدير أفصح به الباحث

المصادر

قائمة المصادر العربية

١- احمد عبد الأمير الأنباري، تعزيز فرص التنافس للقوى الفاعلة في النظام الدولي: دراسة في تأثير المتغيرين الاقتصادي والعسكري، جامعة بغداد/ كلية العلوم السياسية، مجلة تكريت للعلوم السياسية، ٣٠ / ٩ / ٢٠٢٢.

٢- اسراء شريف الكعود، أحمد كامل الخفاجي، تطبيق القوة الذكية في صراع القوى الاقليمية في الشرق الاوسط بعد ٢٠١١، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٦٢، ٢٠٢١، لمزيد من المعلومات ينظر: https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/589/442

٣- محمود فاضل حمود، عباس هاشم عزيز، تأثير المتغير العسكري الأمريكي في الواقع الامني لمنطقة الخليج العربي بعد عام ٢٠٠٣، مجلة العلوم السياسية ، العدد ٦٤، كانون الاول، ٢٠٢٢. لمزيد من المعلومات ينظر: https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/620/499

٤- مرتضى جبار مكي، يسرى مهدي صالح، دور الهوية في التنافس والصراع بين الصين والهند، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٧٠ كانون الاول، ٢٠٢٥، لمزيد من المعلومات ينظر: https://jcopolicy.uobaghdad.edu.iq/index.php/jcopolicy/article/view/810/589

٥- صبا هاشم كمر، هالة خالد حميد، تأثير التحالفات الأمنية على ديناميات الصراع في منطقة الخليج العربي بعد ٢٠٠٣، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٧٠، ٢٠٢٥ .

٦- عز الدين قداري الإدريسي، استراتيجية الصين في الهيمنة على العالم، مركز حمورابي للبحوث والدراسات الاستراتيجية، ٧ كانون الأول ٢٠٢١.

٧- فريق تحرير مجلة ن بوست، حروب الفضاء الإلكتروني، خبر منشور على قناة ن بوست الالكترونية، ٢٠١٥/٢/٢٢، منشور من خلال الرابط : حروب الفضاء الإلكتروني | نون بوست (noonpost.com) ، أخر زيارة في يوم ٢٠٢٥/٦/١، متوفر على شكل ملف بصيغة pdf.

٨- احمد عبد الأمير الأنباري، قضايا دولية معاصرة، مصدر سبق ذكره .متوفرة على شكل ملف بصيغة pdf.
٩- احمد يوسف كيطان، استراتيجية الأمن الوطني الإلكتروني للصين: قراءة في قانون الأمن الإلكتروني الصيني، مركز النهرين للدراسات الاستراتيجية، ١ / ٤ / ٢٠١٨، منشور من خلال الرابط : مركز النهرين للدراسات والابحاث الإستراتيجية (alnahrain.iq) ، متوفرة على شكل ملف بصيغة pdf.
١٠- اختراق شبكات الكمبيوتر الأمريكية يتيح كنزا ثمينا للمتسللين، مقال منشور على قناة وكالة النبأ الإخبارية، ٧/ حزيران/ ٢٠١٥، شبكة الانترنت منشور من خلال الرابط : اختراق شبكات الكمبيوتر الامريكية يتيح كنزا ثمينا للمتسللين (annabaa.org) ، أخر زيارة في يوم ١ / ٦ / ٢٠٢٥ .
١١- اسراء احمد إسماعيل، السيادة الإلكترونية :عناصر الاستراتيجية الصينية للأمن الإلكتروني، بحث منشور على مركز Future ، ٥ / ٢ / ٢٠١٥، من خلال الرابط : Future Center - عناصر الإستراتيجية الصينية للأمن الإلكتروني (futureuae.com) ، متوفر على شكل ملف بصيغة pdf.
١٢- حياة حسين، الفضاء الإلكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية، المجلد ١٢، العدد ١، ٢٠٢١ .
١٣- خطة أميركية للرد على "القرصنة الصينية"، خبر منشور على Sky News عربية، شبكة الانترنت من خلال الرابط : خطة أميركية للرد على "القرصنة الصينية" | سكاي نيوز عربية (skynewsarabia.com) ، أخر زيارة يوم ١ / ٦ / ٢٠٢٥ .
١٤- ديمتري ألبروفيتش، من أجل واقعية الكترونية لا توجد حلول تقنية لمشاكل جيوسياسية، مقال منشور على قناة اندبندنت عربية، ٢٥ / ١٢ / ٢٠٢١، شبكة الانترنت من خلال الرابط : من أجل واقعية الكترونية | اندبندنت عربية (independentarabia.com) ، موعد أخر زيارة في١/ ٦/٢٠٢٥.
١٥- سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص ٩٦ .
١٦- عادل عبد الصادق، مؤتمر حروب الفضاء السبراني، مصدر سبق ذكره .
١٧- علاء الجبالي، شركة Microsoft تطور نسخة خاصة من Windows 10للحكومة الصينية، خبر منشور على مجلة TGTV الالكترونية، على شبكة الانترنت من خلال الرابط : شركة Microsoft تطوّر نسخة خاصة من Windows 10للحكومة الصينية (tgtv.tn) ، أخر زيارة في يوم ٣٠ / ٥ / ٢٠٢٥
١٨- علي زياد العلي، مصدر سبق ذكره.
١٩- عمر حامد شكر، مصدر سبق ذكره .
٢٠- فريدة طاجن، تأثير القوة الإلكترونية على الاستراتيجيات الأمنية للدول الكبرى دراسة حالة الصين، مذكرة تخرج لاستكمال متطلبات نيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، ٢٠١٨، متوفرة على شكل ملف بصيغة pdf .
٢١- كيفين إل. بولبيترKevin. L. Pollpeter ،مايكل أس. تشيس Michael S. Chase ،إريك هيجينبوثام Eric Heginbotham، إنشاء قوات الدعم الاستراتيجي بجيش التحرير الشعبي الصيني وتداعياتها على العمليات الفضائية العسكرية الصينية
٢٢- مؤسسةRAND ،سانتا مونيكا، كاليفورنيا، أعد لصالح القوات الجوية الأمريكية، ٢٠١٧، ix .

٢٣- مي خلف، الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟،الخليج أونلاين، ٣ / ١ / ٢٠١٦، شبكة الانترنت من خلال الرابط : الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟ | الخليج أونلاين (alkhaleejonline.net) ، أخر زيارة يوم ٣٠ / ٥ / ٢٠٢٥.

٢٤- مي خلف، الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟،الخليج أونلاين، ٣ / ١ / ٢٠١٦، شبكة الانترنت من خلال الرابط : الصين تستعد لحرب الفضاء ضد أمريكا.. ماذا يريد الصينيون؟ | الخليج أونلاين (alkhaleejonline.net) ، أخر زيارة يوم ٣٠ / ٥ / ٢٠٢٥.

٢٥- نيويورك تايمز، تحولت الى التهديد الإلكتروني الأول.. كيف تستخدم الصين هجمات الشبح المعقدة ضد الولايات المتحدة؟، مقال منشور على قناة البسالة الالكترونية، شبكة الانترنت من خلال الرابط : تحولت الى التهديد الإلكتروني الأول.. كيف تستخدم الصين هجمات الشبح المعقدة ضد الولايات المتحدة؟ (albasalh.com)، أخر زيارة في يوم ١ / ٦ / ٢٠٢٥ .

٢٦- هال براندز، حول الصراع الإلكتروني الروسي ـ الصيني ـ الأميركي، جريدة الشرق الأوسط، العدد ١٥٣٦٦، الأربعاء ٢٣ / ١٢ / ٢٠٢٠، منشورة من خلال الرابط : حول الصراع الإلكتروني الروسي ـ الصيني ـ الأميركي | الشرق الأوسط (aawsat.com) ،متوفرة على شكل ملف بصيغة pdf.

٢٧- وكالة أنباء الشرق الأوسط المصرية، الصين تستحدث ما يسمى بالجيش الأزرق لحماية شبكتها من القرصنة الإلكترونية، خبر منشور على شبكة الانترنت من خلال الرابط : الصين تستحدث ما يسمى بالجيش الأزرق لحماية شبكتها من القرصنة الإلكترونية - موقع الصين بعيون عربية(chinainarabic.org) ، أخر زيارة في يوم ٣٠ / ٥ / ٢٠٢٥ .

٢٨- yang mu، الصين تصدر الاستراتيجية الوطنية لأمن الفضاء الإلكتروني، خبر منشور على وكالة أنباء CCTV.COM العربية، ٢٧ / ١٢ / ٢٠١٦، شبكة الانترنت من خلال الرابط : الصين تصدر الإستراتيجية الوطنية لأمن الفضاء الإلكتروني_CCTV.com Arabic، تاريخ آخر زيارة في يوم ٣٠ / ٥ / ٢٠٢٥.

٢٩- إسراء شريف جيجان، مصدر سبق ذكره.

٣٠- كيكي، "إصدار استراتيجية الأمن السيبراني الوطنية، واقتراح تسع مهام استراتيجية"، وكالة أنباء شينهوا، ٢٧ ديسمبر/كانون الأول ٢٠١٦

المصادر الانكليزية المترجمة

١- سون أتزو، فن الحرب، أعداد وترجمة رؤوف شبابيك، ٢٠٠٧،ص ٢١،الفصل الثالث،الهجوم بالخداع (التخطيط للهجوم) المقولة الثانية، منشور من خلال الرابط : http://www.dawahmemo.com/image/2012-08-04-09_37_57figh.pdf، متوفر على شكل ملف بصيغة pdf .

٢- صامويل هنتنجتون، صدام الحضارات أعادة صنع النظام العالمي، ط٢، ترجمة طلعت الشايب، simon schustr , &, Rockefeller center نيويورك ١٩٩٦ .