تحديات الردع السيبراني في الإستراتيجية الأمنية الصينية

م.د. علي حسن هويدي

جامعة بغداد - كلية العلوم السياسية- قسم الدراسات الدولية

ali.h@copolicy.uobaghdad.edu.iq

https://doi.org/10.61884/hjs.v14i56.661

ملخص :

يتناول هذا البحث موضوع صعوبات الردع الإلكتروني في الإستراتيجية الأمنية للصين، حيث يُعَد من أبرز التغيرات في العقيدة الأمنية خلال القرن الحادي والعشرين، الهدف من الدراسة هو تحليل أدوات الردع الإلكتروني التي تستخدمها الصين، مثل القدرات التقنية، والهياكل التنظيمية، والقوانين، والدبلوماسية الرقمية، مع توضيح العلاقة بين هذا الردع والسياسة الخارجية للصين، خاصة في ظل التحديات القانونية والتقنية والمحلية التي تؤثر على فعاليته، وقد توصلت الدراسة إلى أن الردع الإلكتروني أصبح وسيلة أساسية في السياسة الأمنية والخارجية الصينية، لكنه لا يزال يواجه صعوبات تتعلق بتعقيد النسب، وتداخل الأدوار المؤسسية، وافتقار إطار قانوني دولي ملزم ينظم سلوك الدول في الفضاء السيبراني، وانتهت الدراسة بمجموعة من الاقتراحات لتعزيز فعالية الردع الإلكتروني الصيني على الصعيدين الداخلي والدولي.

الكلمات المفتاحية: الردع السيبراني، الأمن القومي الصيني، الإستراتيجية الأمنية، التهديدات الإلكترونية، السيادة الرقمية.

Challenges of Cyber Deterrence in China's Security Strategy

Dr. Ali Hasan Howidy

University of Baghdad / College of Political Science / Department of International Studies

ali.h@copolicy.uobaghdad.edu.iq

ABSTRACT:

This study examines the challenges of cyber deterrence within China's security strategy, as one of the most significant transformations in its security doctrine in the twenty-first century. The objective of the research is to analyze the instruments of cyber deterrence employed by China—such as technological capabilities, organizational structures, legal frameworks, and digital diplomacy—while clarifying the relationship between cyber deterrence and China's foreign policy. The study particularly focuses on the legal, technical, and domestic challenges that influence the effectiveness of this deterrence. The findings indicate that cyber deterrence has become a central tool in China's national and foreign security policies. However, it continues to face obstacles related to the complexity of attribution, overlapping institutional roles, and the absence of a binding international legal framework governing state behavior in cyberspace. The study concludes with a set of recommendations aimed at enhancing the effectiveness of China's cyber deterrence at both the domestic and international levels.

KEYWORDS: Cyber deterrence, Chinese national security, security strategy, cyber threats, digital sovereignty.

المقدمة:

في زمن تتسارع فيه التغيرات التكنولوجية، لم تعد القوة التقليدية لوحدها كافية لضمان سلامة الدولة، بل أصبحت الفضاءات الرقمية تمثل ساحة أساسية للصراع الجيوسياسي، ومع زيادة التهديدات الإلكترونية، ظهر مفهوم الردع الرقمي كعنصر أساسي في الإستراتيجية الأمنية للدول الكبرى، مثل الصين، التي تعيش نمواً اقتصادياً وعسكرياً مرتبطاً بتحول رقمي قوي، يدرس هذا البحث فكرة الردع الرقمي، وأنواعه، وتأثيره في تقوية الإستراتيجية الأمنية الصينية، مع تحليل واقعي للأدوات التي تستخدمها الصين لمواجهة التهديدات الإلكترونية.

إشكالية البحث:

كيف ساعد الردع الرقمي في بناء وتحديث خطة الأمن لجمهورية الصين الشعبية، وما هي الوسائل والتحديات الحقيقية التي يواجهها في السياق الدولي المتغير؟ والبحث ينطلق من اهمية تقرن بالنقاط التالية:

١. تسليط الضوء على كيفية تغير مفاهيم الأمن القومي لتشمل الفضاء الإلكتروني.
٢. دراسة التجربة الصينية كنموذج في مجال الردع الرقمي على مستوى العالم.
٣. وضع إطار لفهم القوانين والإستراتيجيات المتعلقة بالردع في الفضاء الإلكتروني.

فرضيات البحث:

١. تطورت الخطة الأمنية في الصين بسبب زيادة المخاطر المتعلقة بالإنترنت.
٢. تستخدم الصين مزيجاً من الأساليب الدفاعية والهجومية في إستراتيجياتها الإلكترونية.
٣. تجعل الظروف العالمية المضطربة من الصعب تحقيق فعالية الردع السيبراني في الصين.

منهجية البحث:

يستند البحث إلى منهج تحليلي ومقارن، حيث يستخدم مراجع أكاديمية وتقارير أمنية عالمية لفهم مواقف الصين وتصرفاتها في الفضاء السيبراني.

هيكلية البحث:

تنظم هيكل هذا البحث إلى قسمين، القسم الأول: الإطار النظري لمفهوم الردع السيبراني وينقسم إلى نقطتين، النقطة الأولى بعنوان: دراسة جوانب الردع السيبراني وأنواعه، بينما النقطة الثانية: تطور الإستراتيجية الأمنية الصينية في المجال السيبراني، أما القسم الثاني: فقد تناول تأثير الردع السيبراني على الإستراتيجية الأمنية الصينية، ويقسم الى: أدوات الردع السيبراني الصينية، بينما الثانية تطرقت إلى التحديات التي تواجه الردع السيبراني في الصين ، بالإضافة إلى ذلك، هناك خاتمة ومصادر.

المبحث الأول

الإطار النظري لمفهوم الردع السيبر اني

يشير مفهوم الردع في مجال الأمن السيبراني إلى استغلال قدرات التكنولوجيا الرقمية، سواء كانت هجومية أو دفاعية، لمنع أو تقليل فرص تنفيذ هجوم إلكتروني من قِبَل خصم ، وذلك يتم عن طريق إظهار القدرة على الرد أو إبطال آثار الهجوم المتوقع. هذا المفهوم هو امتداد لفكرة الردع التقليدي، لكنه يواجه تحديات خاصة بالفضاء السيبراني، مثل الغموض وصعوبة تحديد الفاعلين وسرعة تطور التكنولوجيا، ينقسم الردع السيبراني إلى ثلاثة أنواع رئيسية:

١. الردع بالعقوبة: التهديد بإطلاق هجمات إلكترونية مضادة أو تقليدية للإضرار بالخصم.

٢. الردع بالحرمان: تعزيز الدفاعات لمنع المهاجم من تحقيق أهدافه.

٣. الردع بالغموض والشك: خلق حالة من عدم اليقين لدى الخصم حول قدرات الدولة وإجراءاتها، مما يقلل من فرص المخاطرة بالهجوم.

يشمل الردع السيبراني جوانب متعددة، مثل التقنية والقانونية والعسكرية والسياسية، ويتطلب تعاونًا بين المؤسسات الحكومية والشركات التقنية والنظم القانونية المحلية والدولية.

المطلب الأول

دراسة جو انب الردع السيبر اني و أنواعه:

يعد الردع السيبراني مجموعة من السياسات والإستراتيجيات الرامية إلى منع أو تقليل فرص التعرض لهجمات إلكترونية ضد دولة أو مؤسسة أو بنية تحتية رقمية، من خلال توضيح القدرة على الدفاع أو الرد أو الانتقام من هجوم محتمل، يعتمد الردع السيبراني على ثلاثة عناصر رئيسية:

مصداقية الدفاع: إظهار كفاءة الدولة في حماية أصولها الرقمية

١. مصداقية الدفاع: إظهار كفاءة الدولة في حماية أصولها الرقمية.

٢. القدرة على الانتقام: توفر أدوات هجومية إلكترونية أو تقليدية لمواجهة المعتدي.

٣. الرغبة في الردع: وجود نية سياسية واضحة للرد على أي تهديد سيبراني.

في عصر يتسم بسرعة التحول الرقمي، أصبح الردع السيبراني أمرًا حيويًا للدول والمؤسسات التي تعتمد بشكل كبير على البنية التحتية الرقمية. ينطلق الردع السيبراني من الجانب التقني، حيث تظهر المعركة من خلال أدوات غير مرئية ولكنها فعالة للغاية، الدول التي

تسعى لبناء نظام ردع سيبراني قوي لا تكتفي باستخدام جدران نارية تقليدية أو أنظمة للكشف عن الاختراق، بل تسعى لتطوير تقنيات تعتمد على الذكاء الاصطناعي والتعلم الآلي، والتي يمكنها توقع الهجمات قبل حدوثها وتحليل سلوك المعتدين المحتملين، علاوة على ذلك، أصبح تشكيل فرق للاستجابة للحوادث السيبرانية (مثل فرق CERT وSOC) جزءًا أساسياً من الدفاع، حيث تعمل هذه الفرق على مدار الساعة لمراقبة التهديدات والتعامل معها بسرعة.،في المقابل، لا تتجاهل الدول تحسين قدراتها الهجومية بتطوير برمجيات ، قادرة على تعطيل أنظمة حساسة مثل الكهرباء والمياه والاتصالات، مما يجعل الردع السيبراني سلاحًا ذو حدين.

أصبح الردع السيبراني أمرًا حيويًا للدول والمؤسسات التي تعتمد بشكل كبير على البنية التحتية الرقمية

أما من الناحية القانونية، لا يزال المجال السيبراني يحتاج إلى إطار قانوني دولي موحد يعرف الهجمات الإلكترونية بدقة ويحدد كيفية الرد عليها، تعد مشكلة تحديد الجهة المنفذة للهجوم من أكبر التحديات، وذلك لأن المهاجمين يستخدمون تقنيات متقدمة لإخفاء هويتهم، مثل الشبكات الافتراضية الخاصة (VPN) والبوتات ،حتى اتفاقية بودابست للجريمة الإلكترونية، والتي تعد أول محاولة دولية لتنظيم هذا المجال، لم تحظَ بقبول عالمي، حيث لم تنضم إليها دول كبرى مثل روسيا والصين، مما يضعف من فعاليتها ، وهذا يضع البحث امام تساؤل هل يعد الهجوم السيبراني استخدامًا للقوة وهل يبرر الرد العسكري؟

في الجانب السياسي، يصبح الردع السيبراني وسيلة دبلوماسية فعالة، فالدول لا تستخدمه فقط لحماية أمنها، بل أيضًا لنقل رسائل سياسية، وتقديم ضغط على خصومها ، فعلى سبيل المثال، قد تقوم دولة ما بتسريب معلومات استخباراتية حول قدراتها السيبرانية أو حول نجاحاتها في الاختراق، بهدف إثارة الخوف لدى الخصم نفسيًا وسياستياً. كما يُستخدم الردع السيبراني كجزء من العقوبات الاقتصادية أو طرد الدبلوماسيين أو إيقاف التعاون الاستخباراتي، مما يجعله جزءًا من أدوات السياسة الخارجية، وفي بعض الأحيان، يُظهر الردع السيبراني بشكل استعراضي حيث تُنشر أخبار عن قدرات الدولة في هذا المجال، بهدف تعزيز صورتها كقوة رقمية قوية.

أما البُعد الإستراتيجي، فهو الأساس الذي يعتمد عليه الردع السيبراني، حيث تُبنى الإستراتيجيات على ثلاثة محاور رئيسية: الردع بالإنكار، والردع بالانتقام، والردع بالاستيعاب،

فالردع بالإنكار يعتمد على تقوية الدفاعات بحيث لا ينجح الهجوم في المقام الأول، بينما يعتمد الردع بالانتقام على تهديد الخصم برد مؤلم سواء كان هذا الهجوم سيبرانيًا أو عسكريًا، أما الردع بالاستيعاب، فيتمثل في تعزيز الأنظمة لتستطيع التعافي السريع بعد الهجوم، مما يُفقد المعتدي فعاليته، وتتعزز هذه الإستراتيجيات عبر التعاون الدولي، وتبادل المعلومات الاستخباراتية، وإنشاء تحالفات سيبرانية مثل «Cyber NATO» التي تهدف إلى تنسيق الجهود بين الدول المتحالفة ، كما أن الردع السيبراني لا يُمارس في فراغ، بل يحتاج لفهم عميق لخصائص الخصم، وقدراته، ونواياه، لذلك يعد التحليل الاستخباراتي أساسيًا في تطوير الإستراتيجيات.

وأخيرًا، يأتي البُعد النفسي والإعلامي، الذي يعد من أكثر الأبعاد تأثيرًا على الرغم من كونه الأقل وضوحًا ، فالحرب النفسية الرقمية تستخدم لإرباك الخصم، وزرع الشك في أمانه، وخلق حالة من عدم اليقين داخل مؤسساته ، كما يعد استخدام الإعلام لتضخيم القدرات السيبرانية أو تهديد الخصم بالانتقام وسيلة فعالة لردعهم دون الحاجة للقوة، وتفيد وسائل التواصل الاجتماعي كمنصات لنشر الرسائل المستهدفة، واستهداف النخب وصانعي القرار، مما يجعل عملية الردع السيبراني شاملة تشمل التقنية، والقانون، والسياسة، والإستراتيجية، والنفسية.

تُبنى الإستراتيجيات على ثلاثة محاور رئيسية: الردع بالإنكار، والردع بالانتقام، والردع بالاستيعاب

كما أن الردع السيبراني يُفهم كمفهوم إستراتيجي يهدف إلى منع الهجمات الإلكترونية قبل حدوثها، من خلال إقناع الخصم بأن الهجوم لن يحقق أهدافه أو أن العواقب ستكون صعبة، تتنوع أنواعه وأساليبه، ولكل نوع أمثلة حقيقية تظهر تطبيقه في الواقع ، و يُعتدالردع بالإنكار نوعًا رئيسيًا من الردع السيبراني، ويرتكز على تعزيز الدفاعات السيبرانية بحيث يصبح الهجوم غير مجدٍ ، فعلى سبيل المثال، تعتمد شركة Microsoft على بنية تحتية تعتمد تقنيات «Zero Trust» التي تفترض أن كل محاولة وصول غير موثوقة، حتى من داخل الشبكة، مما يصعب عملية الاختراق ، كذلك، قام الكيان الاسرائيلي بتطوير نظام دفاع سيبراني يعتمد على التكرار والتشفير المتقدم، مما يجعل حتى الهجمات الجزئية غير فعالة.[1].

أما الردع بالعقاب، فيقوم على تهديد الخصم برد مؤلم في حال تنفيذ الهجوم ، الولايات المتحدة طبّقت هذا النوع من الردع عندما أعلنت في ٢٠١٨ عن إستراتيجية

(1) Herbert Lin & Amy Zegart (Eds.)،Bytes، Bombs، and Spies: The Strategic Dimensions of Offensive Cyber Operations، 2019، Brookings Institution Press، Washington، D.C.m P. 252.

"Cyber Deterrence Initiative"، والتي تتضمن الرد على الهجمات السيبرانية بهجمات مضادة أو عقوبات اقتصادية [1].

الردع القانوني والدبلوماسي يقوم على استخدام القوانين الدولية والضغط السياسي، و أنشأ الاتحاد الأوروبي نظامًا يسمى "EU Cyber Diplomacy Toolbox" حتى يتمكن من فرض عقوبات على الدول التي تقوم بالهجمات الإلكترونية. أيضًا، و تعد اتفاقية بودابست أول اتفاق عالمي لمكافحة الجرائم الإلكترونية، على الرغم من عدم انضمام دول مثل روسيا والصين، مما يعكس الصعوبات القانونية المتعلقة بهذا النوع من الردع.

الردع النفسي والإعلامي يرتكز على زراعة الشك والخوف في عقول الأعداء عن طريق إبراز القدرات السيبرانية للدولة. فعلت كوريا الشمالية، مثلاً، ذلك عن طريق نشر أخبار عن اختراقات ناجحة، مما يخلق شعورًا بالردع دون الحاجة لتنفيذ هجوم حقيقي ، كذلك، استخدمت إيران الإعلام لنشر معلومات عن قدرتها على اختراق أنظمة خصومها، مما ساعد على بناء صورة قوية للردع.

أما الردع الاستباقي، فهو يتجسد من خلال القيام بعمليات سيبرانية ضد الأعداء المحتملين قبل حدوث أي هجوم. الهجوم السيبراني المعروف بـ "Stuxnet"، والذي يُعتقد أن الولايات المتحدة وإسرائيل قامتا به ضد المنشآت النووية الإيرانية في ٢٠١٠، هو مثال بارز على هذا النوع، حيث تم تعطيل أجهزة الطرد المركزي قبل استخدامها في تخصيب اليورانيوم.

وأخيرًا، يوجد النوع الهجين من الردع، الذي يجمع بين أنواع عدة ، فنأخذ الصين مثالًا على ذلك، حيث تمزج بين الردع عن طريق بناء دفاعات قوية، واستخدام أساليب نفسية بإبراز قدراتها السيبرانية، والردع القانوني من خلال عدم قبول بعض الاتفاقيات الدولية التي لا تخدم مصالحها، أيضًا، يعتمد حلف الناتو على مزيج من الردع بالعقوبات

ان زيادة وعي الدولة بمكونات الردع السيبراني يجعل قدرتها على تحقيق الأمن الرقمي الوطني أعلى وأكثر كفاءة.[2].

(1) Joseph S. Nye Jr،Deterrence and Dissuasion in Cyberspace، 2017، Belfer Center for Science and International Affairs، Harvard University، P.20.

(2) Thomas Rid،Cyber War Will Not Take Place، 2013، Oxford University Press، Oxford، UK، P.240.

المطلب الثاني

تطور الإستر اتيجية الأمنية الصينية في المجال السيبر اني

شهدت الإستراتيجية الصينية الأمنية في المجال السبراني تغيرًا كبيرًا خلال العقدين الاخيرين، نتيجة لزيادة التهديدات الرقمية والاعتماد المتزايد على الفضاء الإلكتروني في جوانب الحياة المختلفة ، ومن موقف الحذر والرد في البداية، تحولت الصين تدريجيًا إلى تبني طريقة هجومية ودفاعية معًا، تعمل على تعزيز الأمن الرقمي الداخلي وتوسيع قدرتها على الردع السيبراني ضد الأعداء الخارجيين.

تشير قوانين الأمن السيبراني التي وضعتها الصين في عام ٢٠١٧، وإنشاء هيئات مثل مكتب الفضاء السيبراني، إلى دخول الصين في مرحلة جديدة تُعنى بالأمن السيبراني بشكل منظم ، كما أصبحت الإستراتيجية السيبرانية جزءًا رئيسيًا من إستراتيجيتها الدفاعية العامة، التي تهدف إلى السيطرة على المعلومات، والسيادة الرقمية، واستخدام التأثير السيبراني كوسيلة ضغط في السياقات الجيوسياسية.، ومع ازدياد الاعتماد على الإنترنت في المجالات الاقتصادية والعسكرية والسياسية، بدأت القيادة تدرك أن الفضاء السيبراني قد يصبح ساحة صراع حقيقي، مما جعلها تعيد ترتيب أولوياتها الأمنية.

بدأت القيادة تدرك أن الفضاء السيبراني قد يصبح ساحة صراع حقيقي، مما جعلها تعيد ترتيب أولوياتها الأمنية

في عام ٢٠١٠، تبنت الصين فكرة «السيادة السيبرانية»، التي تتيح للدولة التحكم الكامل في الفضاء الرقمي الخاص بها، بما في ذلك المحتوى والبيانات والبنية التحتية، كان هذا المفهوم نقطة تحول، فقد أطلقت الحكومة مجموعة من السياسات التي تهدف إلى تنظيم استخدام الإنترنت، وزيادة الرقابة، وتطوير قدرات دفاعية وهجومية في العالم الرقمي، ومن أبرز هذه السياسات «جدار الحماية العظيم»، الذي يُعد من أكبر أنظمة الرقابة على الإنترنت في العالم، ويهدف إلى منع الوصول إلى المحتوى الخارجي الذي ترى الحكومة أنه يشكل تهديدًا للاستقرار الداخلي.

في عام ٢٠١٣، تم إنشاء «اللجنة المركزية لأمن الإنترنت والمعلومات» في الصين، برئاسة الرئيس شي جين بينغ، لتكون المسؤولة عن وضع وتنفيذ السياسات الخاصة بالأمن السيبراني، هذا التحول يعكس كيف أن الأمن السيبراني قد أصبح قضية إستراتيجية تتعلق بأعلى مستويات صنع القرار ، منذ ذلك الحين، بدأت الصين بإدماج الأمن السيبراني في إستراتيجياتها العسكرية، حيث عد جيش التحرير الشعبي الفضاء السيبراني ساحة قتال خامسة بجانب البر والبحر والجو والفضاء.

في عام ٢٠١٧، أصبح قانون الأمن السيبراني الصيني ساري المفعول، وهو أول قانون شامل ينظم هذا المجال، و ينص القانون على ضرورة تخزين البيانات داخل الصين، ويُلزم الشركات الأجنبية والمحلية بجملة من المعايير للامتثال في حماية المعلومات، كما يمنح السلطات صلاحيات واسعة لمراقبة الأنشطة الرقمية، مما أثار جدلًا دوليًا حول تأثيره على حرية الإنترنت وخصوصية المستخدمين، و لم يكن هذا القانون مجرد أداة تنظيمية، بل كان أيضًا إعلانًا سياسيًا يُظهر أن الصين تعدُ الأمن السيبراني جزءًا لا يتجزأ من سيادتها الوطنية.

استثمرت الصين مليارات الدولارات في تطوير تقنيات الذكاء الاصطناعي، وتحليل البيانات الكبيرة، وإنشاء مراكز متقدمة للأمن السيبراني، كما أطلقت برامج لتدريب الأفراد، وأقامت شراكات مع القطاعين العام والخاص لتعزيز الابتكار في هذا المجال، و بدأت الجامعات الصينية في تقديم تخصصات أكاديمية متقدمة في الأمن السيبراني، مما ساعد في تشكيل جيل جديد من المختصين القادرين على التعامل مع التهديدات المعقدة.

على المستوى العالمي، اتبعت الصين سياسة مزدوجة؛ فهي تدعو لإنشاء نظام عالمي لإدارة الفضاء الإلكتروني، بينما ترفض في نفس الوقت الانضمام إلى معاهدات مثل اتفاقية بودابست بدعوى أنها لا تأخذ في الاعتبار احتياجات الدول النامية ، وهذا دفع الصين الى تطوير قدراتها السبرانية حيث تعتبر الصين نموذجًا فريدًا يدمج بين الأمن القومي والرقابة السياسية والتحول الرقمي، فأصبح الأمن السيبراني في الصين ليس مجرد وسيلة للدفاع، بل جزءًا أساسيًا من خطة الهيمنة الرقمية الجيوسياسية، و هذا النموذج يعتمد على فكرة «السيادة السيبرانية المطلقة»، مما يجعله موضوع نقاش عالمي بين من يرونه ضرورة للأمن الداخلي ومن يعدونه تهديدًا للحرية الرقمية حول العالم.

تلعب مجموعة من المؤسسات الصينية أدوارًا مهمة في صياغة وتنفيذ سياسات الأمن السيبراني، وتتضمن هذه الجهات مؤسسات حكومية وعسكرية وتنظيمية وأكاديمية، مما يعكس التعقيد والتشابك في هذا المجال في الصين، في مركز الهيكل التنظيمي، تأتي اللجنة المركزية لأمن الإنترنت والمعلومات، التي يرأسها الرئيس الصيني، والتي تُعد الهيئة العليا المسؤولة عن وضع السياسات السيبرانية وتنسيق الجهود بين الجهات المختلفة ، و تمثل هذه اللجنة تحولًا إستراتيجيًا في التعامل مع الأمن السيبراني، حيث أصبحت المسألة ليست مجرد تقنية بل قضية أمن قومي على أعلى المستويات، بجانبها، تساهم وزارة الأمن العام في مراقبة الأنشطة الرقمية في البلاد، وتطبيق القوانين المتعلقة بالجرائم الإلكترونية، كما تشرف على التحقيقات في الهجمات الإلكترونية التي تستهدف البنية التحتية الوطنية.

بينما تتولى وزارة الصناعة وتكنولوجيا المعلومات مسؤوليات مثل وضع المعايير التقنية وتنظيم قطاع الاتصالات وتعزيز أمن الشبكات والبنية التحتية الرقمية، كما تشرف على تطوير المجالات المرتبطة بالأمن السيبراني، بالإضافة إلى ذلك، يبرز دور جيش التحرير الشعبي الصيني في الأمن السيبراني، حيث يمتلك وحدات متخصصة في الحروب السيبرانية، ويعد الفضاء الرقمي ساحة قتال خامسة إلى جانب اليابسة والبحر والجو والفضاء، و تعمل هذه الوحدات على تحسين القدرات الهجومية والدفاعية، وتشارك في أنشطة التجسس الإلكتروني وجمع المعلومات الاستخبارية.

توجد هيئات تنظيمية مثل مكتب إدارة التشفير الخاص بأمن الدولة، الذي يتولى مسؤولية تطوير وتنفيذ تقنيات التشفير، مع ضمان حماية المعلومات الحساسة، خصوصًا تلك المتعلقة بالأمن القومي ، إضافة إلى ذلك، تسهم الجامعات والأكاديميات في تدريب الأفراد وإجراء أبحاث متقدمة في مجال الأمن السيبراني، مثل جامعة الدفاع الوطني وجامعة تشينغهوا، اللتين تعدان من أبرز المؤسسات التعليمية في هذا المجال، و كذلك، تشارك شركات كبيرة مثل هواوي وعلي بابا وتينسنت في تطوير حلول أمنية متطورة، وتعمل بالتعاون مع الحكومة في مشاريع إستراتيجية تهدف إلى تعزيز الأمن السيبراني للدولة.

يبرز دور جيش التحرير الشعبي الصيني في الأمن السيبراني، حيث يمتلك وحدات متخصصة في الحروب السيبرانية، ويعد الفضاء الرقمي ساحة قتال خامسة إلى جانب اليابسة والبحر والجو والفضاء

هذا التعاون بين الجهات الحكومية والعسكرية والأكاديمية والتجارية يعكس النموذج الفريد للصين، الذي يدمج الأمن السيبراني في إطار شامل يتعلق بالسيادة الرقمية، والنمو الاقتصادي، والاستقرار السياسي، مما يجعل كل مؤسسة فعالة جزءًا من شبكة متكاملة تهدف إلى حماية الفضاء السيبراني في الصين ضد التهديدات الداخلية والخارجية، يتميز النموذج الصيني في مجال الأمن السيبراني بأنه مركزي ومنظم بدقة، حيث يرتبط الأمن القومي ارتباطًا وثيقًا بالسياسات التكنولوجية ومراقبة المجتمع ، و تعمل كل هيئة ضمن رؤية الحزب الشيوعي لتحقيق "السيادة السيبرانية"، والقدرة على مواجهة التهديدات الرقمية من الداخل والخارج، وخلق نموذج عالمي ينافس أساليب إدارة الإنترنت الغربية.

المبحث الثاني

أثر الردع السيبراني على الإستراتيجية الأمنية الصينية

أدى تزايد المخاطر الإلكترونية في العالم إلى جعل الردع السيبراني جزءًا أساسيًا في وضع الإستراتيجية الأمنية للصين. مع تزايد الهجمات الرقمية والاختراقات التي تتعرض لها الصين من دول أخرى، عملت بكين على إنشاء نظام شامل للردع السيبراني ، هذا النظام يساعدها في حماية أمنها الرقمي وزيادة قدرتها على مواجهة التهديدات أو منعها قبل حدوثها ، وقد ساعد هذا التوجه في تعديل المفهوم الأمني للصين، بحيث يتم التعامل مع الفضاءات السيبرانية وفقًا لأسلوب أمني صارم، يمزج بين الدفاع الاستباقي، والهجمات الإلكترونية، والتحكم في البيانات، وتطوير ردع رقمي وطني كجزء من الأمن الشامل للبلاد.

المطلب الأول

أدوات الردع السيبراني الصيني

تتكون أدوات الردع السيبراني في الصين من مجموعة متكاملة من المهارات التقنية، والهياكل التنظيمية، والإستراتيجيات غير الشائعة، التي تهدف إلى حماية الفضاء الرقمي الوطني، وصد المخاطر من الخصوم المحتملين، وتحقيق التفوق في مجال القتال الرقمي ، وتعتمد الصين على مزيج من الردع التقليدي والردع الرمادي، حيث لا تكتفي بعرض قوتها التقنية، بل تستخدم أيضًا الغموض في إستراتيجياتها، والإنكار الذي يبدو مقبولاً، والعمليات غير المباشرة، من بين أهم تلك الأدوات، تطوير وحدات هجوم خاصة داخل جيش التحرير الشعبي، مثل الوحدة ٦١٣٩٨، التي يعتقد أنها مسؤولة عن تنفيذ عمليات اختراق ضخمة ضد أهداف خارجية، بما في ذلك الحكومات والشركات التقنية في أمريكا وأوروبا ، ولا تقتصر تلك الوحدات على جمع المعلومات الاستخباراتية، بل تستخدم كوسيلة لإظهار القدرة على الإضرار بالبنية التحتية الرقمية للخصوم، مما يسهم في إنشاء توازن يمنع التصعيد.

كما تقوم الصين ببناء مهارات دفاعية متطورة تشمل أنظمة لمراقبة وتحليل حركة البيانات، وتقنيات الذكاء الاصطناعي لرصد الأنشطة المشبوهة، وتطوير برامج حماية محلية، مما يقلل من الاعتماد على الشركات الأجنبية ويعزز من سيادتها الرقمية ، أيضًا، تعد سياسة

تخزين البيانات داخل الصين، وإجبار الشركات الأجنبية على الالتزام بالمعايير المحلية، جزءًا من إستراتيجية الردع، حيث تمنح السلطات القدرة على إدارة تدفق المعلومات بشكل كامل. بالإضافة إلى ذلك، تلعب الصين على القوانين مثل قانون الأمن السيبراني لعام ٢٠١٧، الذي يعطي الحكومة سلطات كبيرة في مراقبة الإنترنت، ويعد بمثابة تحذير واضح بأن أي نشاط رقمي سيخضع لرقابة دقيقة.

من ضمن الإستراتيجيات غير التقليدية التي تستخدمها الصين في الردع السيبراني، هي استهداف البنية التحتية الرقمية العالمية، مثل الكابلات البحرية التي تنقل أكثر من ٩٥٪ من بيانات الإنترنت والاتصالات المالية والعسكرية. وقد تم تسجيل العديد من الحوادث التي تشير إلى تورط الصين في تعطيل هذه الكابلات، كما حدث في جزر ماتسو التايوانية، حيث أدى قطع الكابلات إلى عزل الآلاف عن الإنترنت لأسابيع ، هذا النوع من العمليات يُعتد جزءًا من إستراتيجية هجينة تهدف إلى اختبار ردود فعل المجتمع الدولي دون الدخول في أي مواجهة مباشرة، وتستغل الصين أيضًا أدوات اقتصادية وتقنية، مثل السيطرة على المعادن النادرة، التي تعد ضرورية لصناعة الشرائح الإلكترونية، مما يمنحها قوة للتأثير على سلاسل الإمداد العالمية، ويستخدم كورقة ضغط في النزاعات السيبرانية.

بشكل عام، تعكس أدوات الردع السيبراني الصينية فلسفة إستراتيجية ترى في الفضاء الرقمي ساحة قتال شاملة، تُستخدم فيها القوة التقنية، والسيطرة التنظيمية، والعمليات الرمادية، والتأثير الاقتصادي، للوصول إلى أهداف الأمن القومي، وحماية نفسها من الخصوم، وتعزيز مكانة الصين كقوة رئيسية في الفضاء السيبراني العالمي ، توضح أدوات الردع السيبراني الصينية توازنًا بين الردع بالعقوبات، والردع بالحرمان، والردع عبر الغموض ، و يتميز النموذج الصيني بدمج الأدوات التقليدية للدولة (القوات المسلحة، الأمن، التشريع) مع التكنولوجيا المتقدمة (الذكاء الاصطناعي، البيانات الضخمة)، في إطار إستراتيجية شاملة تهدف إلى حماية الفضاء السيبراني للصين، ومنع التدخلات أو الهجمات، مما يضمن بقاء الصين في موقع آمن ومسيطر ضمن النظام الرقمي العالمي.

المطلب الثاني

التحديات التي تواجه الردع السيبراني الصيني

على الرغم من التقدم الكبير في إنشاء أساليب للردع في الفضاء الإلكتروني، لا تزال البيئة الرقمية الحالية تواجه مجموعة من الصعوبات المعقدة التي تؤثر على فعالية هذا الردع' إن طبيعة الفضاء السيبراني، المليئة بالغموض والتداخل بين الفاعلين الحكوميين وغير الحكوميين، تجعل من الصعب تحقيق ردع كامل أو مؤكد ، علاوة على ذلك، فإن مشكلات تحديد المصدر، تفاوت القدرات بين الدول، وعدم وضوح الأطر القانونية تؤثر على إمكانية استخدام الردع السيبراني بوصفها أداة إستراتيجية ثابتة وموثوقة، هذه الصعوبات تسلط الضوء على الحاجة المستمرة إلى تطوير أدوات تقنية وقانونية وأمنية تتناسب مع تعقيدات البيئة الرقمية المتغيرة[1].

التحديات السياسية والدولية التي تواجه الردع السيبراني:

يواجه الردع الإلكتروني مشكلات سياسية ودولية معقدة، حيث تتداخل المصالح الجيوسياسية والمتطلبات القانونية والتوازنات الإستراتيجية، مما يجعل إنشاء نظام ردع ثابت وفعال في العالم الرقمي أمرًا صعبًا' من أهم هذه المشكلات هو عدم وجود قانون دولي موحد ينظم استخدام القوة الإلكترونية، إذ لا توجد حتى الآن اتفاقية عالمية واضحة تُحدد ما هو الهجوم السيبراني، وما هي الردود القابلة للتطبيق، وما هي حدود المسؤولية القانونية للدول ، هذا الغياب القانوني يمنح الدول حرية تفسير الهجمات الإلكترونية بناءً على مصالحها، مما يصعب عملية الردع، لأن الخصوم قد لا يعرفون الحدود أو النتائج المحتملة لأفعالهم.

كذلك، فإن طبيعة الهجمات الإلكترونية التي لا تُنسب إلى جهة معينة تعتبر تحديًا كبيرًا، إذ يمكن تنفيذ هجمات اختراق وتخريب دون وجود أدلة واضحة على الجهة المسؤولة، مما يقلل من فعالية الردع المبني على التهديد بالعقاب. الدول التي تتعرض للهجمات قد تتردد في اتخاذ إجراءات إذا لم تستطع إثبات المسؤولية بشكل قاطع، مما يشجع الجهات الفاعلة على الاستمرار في تلك الأنشطة دون خوف من العواقب ، هذا الغموض يُستغل أحيانًا كوسيلة إستراتيجية، كما تفعل الصين في الكثير من الحالات، حيث تنكر تدخّلها في الهجمات رغم وجود أدلة تقنية تشير إلى ذلك، مما يربك الخصوم ويجعل من الصعب بناء ردع فعّال.

هناك أيضًا مشكلات تتعلق بضعف الحماية القانونية للبنية التحتية الرقمية العالمية، مثل الكابلات البحرية التي تنقل أكثر من ٩٥٪ من بيانات الإنترنت والاتصالات المالية

(١) رائد العلي، قراءات في الردع السيبراني ،مصدر سبق ذكره،ص٢١١.

والعسكرية، هذه الكابلات تعد أهدافًا سهلة للهجمات، وقد تم تسجيل حوادث تشير إلى تورط الصين في تخريبها، كما حدث في جزر ماتسو التايوانية، حيث أدى قطع الكابلات إلى عزل آلاف الأشخاص عن الإنترنت لأسابيع ، هذه الأنواع من الهجمات تعقّد من عملية الردع، لأنها تحدث في مناطق قانونية رمادية، ولا توجد آليات دولية قوية لحمايتها أو عقاب المعتدين عليها.

أيضًا، فإن الاختلاف في المفاهيم السياسية بين الدول يشكلChallenge إضافي، حيث تدعو بعض الدول إلى حرية الإنترنت والتعاون الدولي، بينما تتبنى الصين مفهوم "السيادة السيبرانية"، الذي يعطيها الحق في السيطرة الكاملة على فضائها الرقمي ويرفض التدخل الخارجي ، هذا الاختلاف يعوق تطوير قواعد مشتركة للردع، ويزيد من الانقسامات السياسية، ويقلل من فعالية المبادرات الدولية مثل اتفاقية بودابست، التي ترفض الصين الانضمام إليها بحجة أنها لا تراعي خصوصيات الدول النامية.

بشكل عام، يواجه الردع الإلكتروني تحديات سياسية ودولية متعددة تشمل الغموض التقني، والفراغ القانوني، والتنافس الجيوسياسي، والاختلاف في المفاهيم، مما يجعل إنشاء نظام ردع فعال في الفضاء الرقمي مهمة بالغة التعقيد، تتطلب تعاونًا دوليًا عميقًا وصياغة قواعد جديدة تتناسب مع طبيعة هذا المجال المتغير والسريع.

تظهر القضايا القانونية والدولية أن الدفاع السيبراني، على عكس الدفاع النووي أو العسكري العادي، ليس له أساس قانوني متماسك يضمن فعاليته وثباته ، لذلك، لا يمكن إنشاء دفاع سيبراني عالمي حقيقي إلا من خلال تعاون دولي شامل يخلق قواعد واضحة، وآليات للتوثيق والمحاسبة بشكل محايد، وتوافق على المبادئ الأساسية للسلوك المسؤول في عالم الإنترنت.

التحديات التقنية والداخلية في الردع السيبر اني

١- صعوبة النسبة الفنية

على الرغم من تحسين أدوات تتبع الهجمات الإلكترونية، إلا أن التعرف بدقة على المهاجمين لا يزال بعيدًا عن الكمال.

يستخدم المهاجمون أساليب مثل:

- تغيير عناوين IP
- نقل الهجمات عبر دول مختلفة
- أدوات لإخفاء الهوية (مثل TOR وVPNs العسكرية)
- الأثر: يضعف القدرة على اتخاذ ردود فعل صحيحة أو استباقية؛ لأن الردع الفعّال يحتاج إلى معرفة دقيقة عن الخصم.

٢- تسارع تطور أدوات الهجوم

- الفترة الزمنية بين ظهور ثغرة جديدة وإصدار التحديث الأمني لا تزال مقلقة.
- دائمًا ما يتفوق المهاجمون على الدفاع بسبب:
- استخدام تقنيات الذكاء الاصطناعي لاكتشاف الثغرات
- الاعتماد على السوق السوداء لشراء أدوات هجومية متطورة
- الأثر: يجعل الدفاع السيبراني دائمًا في موقف رد الفعل، مما يحد من فعالية الردع بالحرمان.

٣- تعقيد الذكاء الاصطناعي في تحليل السلوكيات

- تعتمد الصين على الذكاء الاصطناعي لتحليل التهديدات، ولكن هذه الأنظمة:
- تواجه صعوبات في تمييز بين الأنشطة العدوانية والطبيعية.
- يمكن أن تنتج إنذارات خاطئة تؤثر على سرعة الاستجابة.
- الأثر: قد يؤدي إلى عدم القدرة على توقع الهجمات أو فهمها بشكل صحيح، مما يخفف من الاستعداد الدفاعي.

الأثر: قد يؤدي إلى عدم القدرة على توقع الهجمات أو فهمها بشكل صحيح، مما يخفف من الاستعداد الدفاعي

٤- تحديات حماية البنية التحتية المهمة

- أصبحت القطاعات مثل الطاقة والنقل والاتصالات والمالية رقمية، لكن:
- العديد من الأنظمة لا تزال تعتمد على برمجيات قديمة.
- هناك صعوبة في الدمج بين أمان الشبكات التشغيلية وأمان تكنولوجيا المعلومات.
- الأثر: يشكل نقطة ضعف يمكن أن يستغلها العدو لضرب الأمن القومي، مما يقلل من فاعلية الردع الاستباقي.

التحديات الداخلية (السياسية، المؤسساتية، الاجتماعية)

١. تتداخل السلطات وتختلط المهام بين المؤسسات السيبرانية في الصين، رغم وجود أجهزة متطورة مثل CAC وMSS وPLA، إلا أن هناك تداخلًا في الوظائف بين الجهات الأمنية والمدنية والعسكرية. التنسيق في حالات الطوارئ السيبرانية ضعيف، مما يؤخر اتخاذ القرارات الحاسمة في الأوقات الحرجة ويقلل من فاعلية الردع.

٢. وعي المجتمع بأهمية الأمن السيبراني ضعيف، حيث لا يدرك المواطنون والشركات الصغيرة المخاطر المرتبطة بالأمان الرقمي ، استخدام برمجيات غير مصرح بها، وعدم تحديث الأنظمة، وسوء إدارة كلمات المرور كلها تمثل نقاط ضعف داخلية، فهذا الأمر

يفتح المجال للاختراق ويؤثر سلبًا على ثقة الناس في فاعلية الحماية السيبرانية.

٣. تعتمد الصين على شركات خاصة في تطوير بنيتها الرقمية مثل Huawei وAlibaba و Tencent وZTE، ورغم أن هذه الشركات تحت رقابة الدولة، إلا أن طبيعتها التجارية قد تؤخر إبلاغ الحكومة عن الثغرات أو الهجمات، فمصالحها الاقتصادية قد تتعارض مع احتياجات الأمن القومي، مما يؤدي إلى وجود ثغرات في الأمن السيبراني الداخلي.

٤. تعتمد بعض البنى التحتية الصينية على تكنولوجيا أجنبية على الرغم من السياسات التي تدعو للاكتفاء الذاتي، مثل استخدام شرائح إلكترونية أجنبية وبرامج حماية خارجية ، فهذا يعرض البنية الرقمية للاختراق أو التلاعب من قبل الأعداء، مما يقلل من قدرة البلاد على تنفيذ ردع شامل.

تظهر التحديات التقنية والداخلية أن بناء إستراتيجية فعالة للردع السيبراني لا يقتصر فقط على القدرات الهجومية والدفاعية، بل يحتاج أيضًا إلى تكامل بين المؤسسات، ورفع مستوى الوعي التكنولوجي بين الأفراد، وتوفير تنظيمات متجددة ومنسقة، فإن أي خلل في هذه العناصر، سواء كان تقنيًا أو إداريًا ؛ يهدد فعالية الردع ويجعل من السهل على الأعداء اختراق النظام.

النتائج:

١- تعتمد الصين طريقة متكاملة للقيام بالردع السيبراني، تتضمن وسائل عسكرية وقانونية وتقنية ومؤسساتية، لحماية مصالحها الرقمية والسياسية.

٢- أصبح الردع السيبراني جزءًا مهمًا من سياسة الصين الخارجية، سواء كان ذلك ضمن تحالفات دولية أو في حالات النزاع غير التقليدية مثل موقفها من تايوان أو بحر الصين الجنوبي.

٣- هناك نقص في القوانين الدولية التي تعيق تنظيم فعّال للهجمات السيبرانية، مما يقلل من فعالية الردع كوسيلة لضبط سلوك الفاعلين المتهورين.

٤- تواجه الصين بعض التحديات الداخلية المتعلقة بالهياكل المؤسسية والتكنولوجيا، بما في ذلك تداخل السلطات بين الأجهزة، واختلاف مستويات الوعي في القطاع الخاص والمجتمع، بالإضافة إلى اعتمادها النسبي على التقنية الأجنبية.

٥- بالرغم من تقدم الردع السيبراني، إلا أنه لا يزال أقل استقرارًا من الردع التقليدي العسكرية أو النووية، بسبب صعوبة تحديد النسب والردود المناسبة وأحيانًا غياب الردود الرسمية.

التوصيـات:

١- يجب أن يكون هناك إطار قانوني دولي ملزم لتنظيم سلوك الدول في الفضاء الرقمي، يوضح بشكل دقيق ما يعنيه الهجوم الرقمي ويعطي الشرعية للردود السيبرانية القانونية.

٢- ينبغي على الصين تحسين الشفافية في مؤسساتها وتنسيق الأعمال بين أجهزتها في المجال السيبراني (مثل CAC وMSS وPLA) لضمان استجابة سريعة وتقليل التعقيدات الإدارية.

٣- يجب دعم برامج التوعية بالأمن السيبراني في المجتمع، مع تحديث البنية التحتية التقنية للمؤسسات المدنية، لتقليل الثغرات الداخلية التي قد يستفيد منها الخصوم.

٤- من المهم الاستثمار في تحقيق الاكتفاء الذاتي الرقمي من خلال تصنيع شرائح إلكترونية محلية، وتطوير برمجيات أمنية وطنية مستقلة، مما يساعد في تقليل الاعتماد على التكنولوجيا الأجنبية.

٥- ينبغي توسيع وسائل الردع السيبراني من خلال دمج القوة الناعمة الرقمية مثل الدبلوماسية السيبرانية والحرب المعلوماتية، لتعزيز الردع غير المباشر وتحقيق توازن بدون تصعيد.

٦- يجب تعزيز التعاون مع القوى الرقمية الناشئة مثل روسيا والهند وبعض دول آسيا الوسطى لبناء نظام سيبراني دولي بديل يوازن النفوذ الغربي ويدعم فكرة «السيادة الرقمية».

الخاتمة

لم يعد ردع الفضاء الإلكتروني مجرد خيار ثانوي ضمن صياغة الأمن الوطني للدول، بل أصبح أحد العناصر الأساسية في هيكل الأمن القومي، لاسيما لدولة مثل الصين التي تسعى لتصبح واحدة من القوى العظمى ، وقد أظهر البحث أن الصين تتبنى إنموذجاً متعدد الأبعاد لتعزيز قدراتها على الردع في الفضاء السيبراني، يجمع بين الهجمات والدفاع، والتشريعات والرقابة، والتكنولوجيا والدبلوماسية ، في الوقت نفسه، تواجه هذه الإستراتيجية تحديات كبيرة تتعلق بالبيئة القانونية الدولية، والتطورات التقنية المستمرة، والقيود الداخلية التي يمكن أن تضعف فاعلية هذا الردع أو تؤثر على استقراره.

المصادر

مصادر باللغة العربية:

١- رغدة البهي–الردع السيبراني: المفهوم والإشكاليات والمتطلبات ، المركز الديمقراطي العربي – برلين، ألمانيا – مجلة العلوم السياسية والقانون، العدد الأول، ١٧٢ ..

٢- رائد العلي، قراءات في الردع السيبراني ،المركز العربي الاستراتيجي، دمشق، ٢٠٢٢.

٣- بوغازي عبد القادر–الردع السيبراني: مقاربة للطبيعة، الفواعل وقيود القانون الدولي ،المجلة الجزائرية للحقوق والعلوم السياسية ،الجزائر ، المجلد ١٠، العدد ١،٢٠٢٥

مصادر باللغة الانكليزية:

1. Joseph S. Nye Jr،Deterrence and Dissuasion in Cyberspace ، Belfer Center for Science and International Affairs ، Harvard University.2017،
2. Martin C. Libicki،Cyberdeterrence and Cyberwar ، RAND Corporation ، Santa Monica, California.2009،
3. Thomas Rid،Cyber War Will Not Take Place ، Oxford University Press ، Oxford, UK.2013،
4. Brandon Valeriano & Ryan C. Maness، Cyber War versus Cyber Realities: Cyber Conflict in the International System ، Oxford University Press ، New York.2015،
5. Herbert Lin & Amy Zegart (Eds.) ،Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations ،Brookings Institution Press ، Washington.2019،
6. Richard J. Harknett & Emily Goldman،The Cyber Deterrence Problem، Strategic Studies Quarterly – Air University Press .2011،
7. Jasper L. Tran ،Cybersecurity Law: A Legal Arsenal for Cyber Deterrence ، Harvard Journal of Law & Technology ، Cambridge.2016،
8. Michael N. Schmitt (Ed.) ،Tallinn Manual on the International Law Applicable to Cyber Warfare ، Cambridge University Press ، Cambridge.2019،

9. David Sanger،The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age ، Crown Publishing ، New York.2018،
10. Ben Buchanan،The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations ،Oxford University Press ، New York .2019،
11. P.W. Singer & Allan Friedman–Cybersecurity and Cyberwar: What Everyone Needs to Know ، Oxford University Press.2017،
12. Jason Healey (Ed.) ،A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 – ،Cyber Conflict Studies Association، Washington.2013،
13. Myriam Dunn Cavelty،Cyber-Security and Threat Politics: US Efforts to Secure the Information Age ،Routledge ، London.2008،