التهديدات السيبرانية وأثرها على العلاقات الأمريكية الصينية

Cyber threats and their impact on U.S.China relations

اسم الباحث: م.م هناء رشيد محيسن كزار
جهة الإنتساب: الجامعة العراقية ــ كلية القانون والعلوم السياسية

Auther's name: Assistant teacher Hanaa Rashid Muhaisen kazar
Affiliation: Iraq University/College of Law and political Science
E-mail:**hana.r.muhaisen@aliraqia.edu.iq**

نوع العمل العلمي: بحث
مجال العمل: سياسة - السياسة الدولية

work type: research paper
discipline: Politic, International Politics

https://doi.org/10.61279/785r2648

رقم العدد وتاريخه: العدد الثامن والعشرون - نيسان ٢٠٢٥
تاريخ الاستلام:٢٠٢٤/١١/٢٠
تاريخ القبول: ٢٠٢٤/١٢/١
تاريخ النشر: ٢٥ نيسان ٢٠٢٥

Issue No. & date: Issue 28 -April2025
Received: 20/11/2024
Acceptance date: 1/12/2024
Published Online: 25 April. 2025

تاريخ التقديم ١١/٢٠ تاريخ القبول ١٢/١
تاريخ النشر ٢٠٢٥/٤/٢٥

التهديدات السيبرانية وأثرها على العلاقات الأمريكية الصينية

Cyber threats and their impact on U.S.China relations

م.م هناء رشيد محيسن كزار
الجامعة العراقية ـ كلية القانون والعلوم السياسية
Assistant teacher Hanaa Rashid Muhaisen kazar
Iraq University/College of Law and political Science
hana.r.muhaisen@aliraqia.edu.iq

المستخلص

يمثل التطور التكنولوجي الذي شهده القرن الحالي من التطورات المهمة التي أثرت على الفرد والمجتمع وكذلك العلاقات الدولية ، فالدول لم تعد منعزلة كالسابق بل انفتحت الدول على بعضها ليصبح العالم قرية صغيرة ، وعلى الرغم من أن التطور التكنولوجي كان إيجابيا في كثير من الاحيان بل أنه عزز التواصل بين الدول ، ألا أنه اصبح تهديداً يواجه الكثير من الدول ، لاسيما بين الولايات المتحدة والصين وما تواجهه الولايات المتحدة من عمليات تجسس وقرصنة واختراقات سيبرانية صينية على البنية التحتية, واتهام الصين بسرقة معلومات عسكرية وتجارية سرية, وشن هجمات سيبرانية واسعة النطاق على مؤسسات أمريكية, ومدى تأثير وانعكاس التهديدات السيبرانية على مستقبل العلاقات الأمريكية ـــــ الصينية .

الكلمات المفتاحية: التهديدات السيبرانية، الولايات المتحدة الأمريكية، الصين، مستقبل

Abstract

The technological development witnessed in the current century represents one of the important developments that have affected the individual, society, as well as international relations. Countries are no longer isolated as before, but countries have opened up to each other, to make the world a small village, and Although technological development has often been positive, but it has strengthened communication between countries, but it has become a threat facing many countries, especially between the United States and China and the United States faces espionage and piracy Chinese cyber breaches on infrastructure, accusing China of stealing classified military and commercial information, launching large-scale cyberattacks on U.S. institutions, and the impact and reflection of cyber threats on the future of U.S.-China relations.

Key words; Cyber threats, United States, China, Future.

المقدمة

في ظل التطور السريع في مجال التكنولوجيا والاتصالات, أصبح مجال الفضاء السيبراني امراً حيوياً وحاسماً في العالم الحديث, تسعى الدول والمنظمات حول العالم الى مواجهة المخاطر التي تهدد سياستها واستراتيجياتها , مما يتعين عليها حماية الأنظمة والبيانات الحساسة , والتهديدات السيبرانية لم تعد قضية تهم فقط القطاع التقني , بل أصبح يمثل تحديات تؤثر على الاقتصاد والامن الوطني والعلاقات الدولية, وكلما تزداد المخاطر السيبرانية كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات , فأصبحنا امام جرائم حقيقية ومتكاملة تتم عن طريق شبكة الأنترنت بأشكال مختلفة , كسرقة الأموال , النصب والاحتيال ,التخطيط لعمليات إرهابية , القرصنة, باعتبارها الجريمة الأكثر شيوعا في العالم الرقمي.

تعتبر التهديدات السيبرانية مصدر قلق الأول لدى الدول حول العالم مثلا روسيا، والولايات المتحدة الامريكية، والصين في ظل العصر الرقمي الذي نعيشه اليوم، فمع زيادة التقدم والتطور بالتقنية والنمو المستمر لحجم التعاملات ونقل البيانات الحساسة التي تتم عبر الشبكات، يعمل المجرمون الإلكترونيون بشكل دائم على تطوير أساليب جديدة من الهجمات السيبرانية،

باعتبار أن الولايات المتحدة الأمريكية والصين تمثلان إحدى أهم الدول الرائدة عالمياً في مجال القدرات السيبرانية، فالولايات المتحدة تحتل مكانة ريادية بسبب قوتها السياسية والاقتصادية والعسكرية والتكنولوجية؛ حيث تمتلك إمكانيات وقدرات كبيرة في مجال الفضاء السيبراني. من جهة أخرى تنمو الصين بسرعة كقوة اقتصادية ناشئة، وتستثمر بشكل كبير في تطوير قدراتها السيبرانية بشكل ملحوظ.

كما تتصدر كل من الولايات المتحدة الأمريكية والصين التقارير العالمية لقياس القدرات السيبرانية ومؤشرات الأمن السيبراني العالمية، وذلك بفضل قدرتهما على التأثير والسيطرة في الفضاء السيبراني ومواجهة التحديات السيبرانية، والتكيف مع المتطلبات المتزايدة في هذا المجال على صعيد البنية الرقمية.

اهمية البحث:

تكمن اهمية التهديدات السيبرانية التي تمثل التقييم الشامل للقدرة على التأثير والتحكم في الفضاء السيبراني، يمكن تصور القدرات السيبرانية كوسائل وأدوات تستخدم لتحقيق القوة السيبرانية. الدول والكيانات السياسية يسعون لزيادة قدراتهم السيبرانية لضمان أمنهم السيبراني وتعزيز تأثيرهم في العالم الرقمي.

حيث تسعى العديد والكثير من الدول خاصة الولايات المتحدة الأمريكية والصين لتعزيز قوتها السيبرانية والاستثمار في القدرات السيبرانية لمواجهة التهديدات السيبرانية،

وفي الوقت الحاضر، نشهد كيف تأثير تلك الهجمات السيبرانية على مستقبل العلاقات بين البلدين.

اشكالية البحث:

ينطلق البحث من سؤال مركزي هو كيف يؤثر التهديد السيبراني بين الولايات المتحدة والصين في تعزيز نفوذهما العالمي، وكيف يمكن ان يتجلى ذلك التهديد في الاستراتيجيات السيبرانية لكل منهما؟ وكيف ستحافظ كل من الولايات المتحدة الأمريكية والصين على أمنها السيبراني في ظل التحديات الراهنة لاسيما مع التطور التكنولوجي السريع الذي يشهده العالم، ما يجعل الولايات المتحدة ان تكون على اهبة الاستعداد دائماً لمواجهة أي خرق لأمنها الفضائي السيبراني.

فرضية البحث:

وينطلق البحث من فرضية مفادها: « ان التهديدات السيبرانية اصبحت مصدر قلق في العلاقات الدولية لاسيما دولة الولايات المتحدة والصين، لما لها من طبيعة مختلفة عن التهديدات التقليدية خاصة مع التطور التكنولوجي السريع في المجال السيبراني.

منهجية البحث:

منهجية: قد تم توظيف في البحث المنهج التحليلي من خلال دراسة العوامل والمسببات التي أدت الى تطور الهجمات والتهديدات السيبرانية التي حدثت في العلاقات بين الدولتين وتتبع الأثر الذي احدثته هذه التهديدات على مستقبلهم، وايضا تم استخدام المنهج المقارن يعتمد هذا المنهج على المقارنة بين ظاهرتين وأثر التهديد السيبراني من منظور الولايات المتحدة والصين، واستخدم المنهج المستقبلي او الاستشرافي للاستشراف على مستقبل التهديدات في العلاقات بين امريكا والصين.

هيكلية البحث:

يتضمن هذا البحث فضلاً عن مقدمة والخاتمة على ثلاث مباحث، تناول المبحث الاول دراسة مفهوم التهديدات السيبرانية ونشأتها وأنماطها، وتناول المبحث الثاني طبيعة التهديدات السيبرانية بين الولايات المتحدة الامريكية والصين، تضمن المطلب الأول المنظور الأمريكي من التهديد الصيني، وفي المطلب الثاني المنظور الصيني من التهديد الأمريكي، والمبحث الثالث ما إثر هذه التهديدات على مستقبل العلاقات بين البلدين.

المبحث الأول
مفهوم التهديدات السيبرانية

في ظل التسابق الالكتروني الذي نعيشه، نرى ان هناك العديد من المفاهيم الجديدة بدأت بالظهور على الساحة الالكترونية وبدأت بالانتشار من أبرزها مصطلح السيبرانية الذي ارتبط بعدة مصطلحات من ضمنها التهديدات السيبرانية، والحرب السيبرانية، والقوة السيبرانية.

من أجل الوقوف على مفهوم السيبرانية سنبحث في نطاق تعريفها لغة واصطلاحاً في ضوء المفاهيم اللغوية، وما أدرجه خبراء التكنولوجيا المعلومات والمختصون.

المطلب الأول: السيبرانية (لغة واصطلاحاً)

جاءت بدايات السيبرانية من ارتباط الأنترنيت ببناء فضاء جديد ألا وهو الفضاء السيبراني الافتراضي « أو السيبرسبيس pace" "Cypressإذ ظهر هذا المفهوم لأول مرة في ثمانينات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الأمريكي الكنديWilliam Gibson " «، الذي ألف عدة روايات تضمنت هذا المفهوم ليتخذ مع الأنترنيت معنى الفضاء الجديد للاتصال.[1]

اولاً: السيبرانية (لغة)

كلمة سايبر (Cyber) يونانية الأصل، وترجع الى مصطلح (Kybernetes) الذي ورد بداية في مؤلفات الخيال العلمي، ويعني القيادة أو التحكم عن بعد او بمعنى الشخص الذي يدير دفة السفينة حيث تستخدم مجازاً للمتحكم « governor «٢.والسيبرانية في القاموس (المورد) هي علم الضبط، ومصدرها (Cybernetics) وهي علم التحكم الأوتوماتيكي، وهو يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها. ٣ وأشار بعض المؤرخين الى أن أصلها يرجع الى ان اول من استخدم مصطلح السيبرانية هو عالم الرياضيات الأمريكي نورب رت وينر (Norbert wiener)، في العام ١٩٤٨, في أثناء دراسته موضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية.

تطلق كلمة « سيبراني «(Cyber)، لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد، وشبكة الانترنت.٤

١. يحيى ياسين سعود ، الحروب السيبرانية :في ضوء القانون الدولي الإنساني ، المجلة القانونية , جامعة القاهرة , العدد٤, المجلد ٢٠١٨, السودان, ٢٠١٨, ص ٨٤

2. Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference. Online, Oxford University Press, 2010,p4.

٣. منير البعلبكي , المورد : قاموس انكليزي ـــ عربي , دار العلم للملايين , بيروت , ٢٠٠٤, ص ٢٣٤.

٤. احمد عبيس الفتلاوي, الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر, مجلة المحقق الحلي للعلوم القانونية والسياسية, كلية القانون / جامعة بابل ، المجلد ٨ , العدد الرابع, ٢٠١٦, ص ٦١٤.

وبالرجوع الى المختصين في اللغة العربية، نجد ان ثمة تحدياً يوجههم في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الانكليزية، لعدم وجود مصطلح مناظر له في اللغة العربية، لكون ان الترجمة العربية لعنوان اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية كانت ترجمة صائبة، اذ ترجم العنوان (Cybercrime on Conven) الى اللغة العربية: (اتفاقية المتعلقة بالجريمة الإلكترونية) ٥

ثانياً: السيبرانية (اصطلاحاً)

عرف قاموس مصطلحات الأمن المعلوماتي السيبرانية بـ: هجوم عبر الفضاء الإلكتروني يهدف الى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونياً، لتعطيلها أو تدميرها أوالاضرار بها.

يرتبط مفهوم السيبرانية بالعديد من المصطلحات، فنجد مصطلح الهجمات السيبرانية (CyberAttack)، المقصود بها الأفعال الصادرة من أجهزة الحاسوب وشبكات المعلومات التابعة لدولة ما بشكل منظم ومدروس على أجهزة حاسوب وشبكات معلومات لدولة أخرى بغرض التجسس او التخريب او التوجيه. ٦ وقد عرف (Michael N. Schmitt) الهجمات السيبرانية بأنها « تلك الإجراءات التي تتخذها الدولة من اجل الهجوم على نظم المعلومات للعدو وبهدف التأثير والاضرار فيها، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة.٧

يرتبط مفهوم السيبرانية ايضاً بمفهوم اخر يطلق علية القوة السيبرانية ((Cyber power،اذعرفها «جوزيف ناى» بأنها مجموعة الموارد المتعلقة بالتحكم في والسيطرة على أجهزة الحاسبات والمعلومات، والشبكات الالكترونية،والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل.٨وتبنى اخرون مصطلح الحرب السيبرانية (Cyber Warfare)، اذ عرفها عبد القادر محمد فهمي بأنها ((هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة، او الفاعلين من غير الدول، لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الأخرين من الدول وغير الدول، او تقليلها، او حتى تدميرها، سواء كان ذلك على مستوى البنية التحتية للدولة، او مستوى منظومات قوتها العسكرية،

٥. اتفاقية مجلس أوروبا المتعلق بالجريمة الإلكترونية, مجموعة المعاهدات الأوروبية رقم ١٨٥, مجلس أوروبا , بودابست, ٢٠٠١ .
٦. رولا حطيط, السيبرانية: الحرب الخفية في المنطقة المظلمة, مركز باحث للدراسات الفلسطينية والاستراتيجية, بيروت, ٢٠٢٠, ص٤.
٧. أميرة عبد العظيم محمد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام , مجلة الشريعة والقانون , العدد ٣٥ ، كلية القانون /جامعة الإمارات العربية المتحدة، ٢٠٢٠ , ص ٣٩٤.
٨. عادل عبد الصادق , الفضاء الالكتروني والرأي العام : تغير المجتمع والأدوات والتأثير» ,المركز العربي لأبحاث الفضاء الإلكتروني : استراتيجية , العدد ٢٤٥٩, ٢٠١٣, ص٣٥ .

وبالشكل الذي يعرض الأمن القومي الى تهديد جسيم)). ٩

المطلب الثاني: التهديدات السيبرانية (Threats Cyber): النشأة والأنماط

يشير مصطلح التهديدات السيبرانية الى استخدام جملة من الممارسات والاجراءات التي تسعى لألحاق الخلل والعطل والوسائل الالكترونية الخاصة بالعدو, بالإضافة الى تحقيق الحماية للذات من الاستطلاع الالكتروني المعادي ومقاومته, وتحقيق الاستقرار للنظم الالكترونية الصديقة, ويعتبر استخدام الطاقة الكهرومغناطيسية في نطاق الحرب الالكترونية ضرورياً, وذلك لغايات تعطيل حركة العدو, ومنعها من استغلال المجال الكهرومغناطيسي, ان(الحرب الالكترونية) تتخذ من شبكة الانترنت حلبة صراع لها, وتأتي الهجمات التي تشن فيها بسبب دوافع سياسية, وتوجه الضربات الالكترونية على مواقع الانترنت الرسمية للعدو, وكل ما يتعلق بشبكاته وخدماته الاساسية, وتكون الضربات بقرصنة وتعطيل المواقع, وسرقة البيانات السرية وتخريبها, واختراق الانظمة المالية, ١٠ والتهديدات السيبرانية تولد مخاطر التي هي عبارة عن الضرر الذي يهدد أمن الأفراد والبيئة والجماعات البشرية ويمكن احتواءه أن لم يتفاقم , وتلك المخاطر تشمل على كل تهديد يستهدف مؤسسات الدولة باستخدام الأيديولوجيات أو استخدام مكونات القدرة لدولة ضد دولة أخرى حيث يمكن أن يكون إقليم الدولة أو استقلالها أو أمنها مهدداً بضرر ويمكن أن تأتي التهديدات من الخارج أو من الداخل الدولة, وفي هذه الحالة لابد للدولة أن يكون لها استراتيجيات تستطيع من خلالها مواجهة تلك التحديات التي تتعرض لها. ١١

ولمواجهة التهديدات السيبرانية تعمل الدول بوضع خطط واستراتيجيات وتكشف قدرتها لمواجهة التهديدات السيبرانية كجزء لا يتجزأ من استراتيجيتها الشاملة، ومع ضعف وانهيار بعض الدول ظهرت أنماط جديدة من النزاعات والصراعات مما زاد من خطورة التهديدات السيبرانية وهذا ما دعا وتوجب على الأنظمة الدولية الى اخذ احتياطات ووضع رؤى استراتيجية للحد وتفويض تلك الهجومات. ١٢

---

٩. عبد القادر محمد فهمي , الحروب التقليدية وحروب الفضاء الإلكتروني : دراسة مقارنة في المفاهيم وقواعد الاشتباك , مجلة العلوم القانونية والسياسية , المجلد١٦,العدد ٢ـ القاهرة , ٢٠١٨, ص ٢٢ .

١٠. يونس مؤيد يونس مصطفى, استراتيجية الولايات المتحدة الامريكية للأمن السيبراني, مجلة قضايا سياسية, العدد ٥٥, كلية العلوم السياسية / جامعة النهرين ، ٢٠١٨, ص١٢٤ .

١١. تيري ديبيل , استراتيجية الشؤون الخارجية منطق الحكم الأمريكي , ترجمة : وليد شحادة , دار الكتاب العربية , مؤسسة محمد بن آل راشد آل مكتوم , بيروت , ٢٠٠٩, ص٢٥٨ .

١٢. اسراء شريف الكعود , التأثير السيبراني في الأمن القومي للدول الفاعلة (الولايات المتحدة الأمريكية) انموذجا, مجلة العلوم السياسية , العدد ٦٤ ، كلية العلوم السياسية / جامعة بغداد ، كانون الاول ٢٠٢٢ , ص ٤.

أن التهديدات السيبرانية ستكون المشهد الصراعي المستقبلي في البيئات الاستراتيجية الاقليمية والدولية على مستوى التنافس والتماس القوة من قبل القوى المسيطرة في النظام الدولي والقوى الاقليمية الساعية الى ايجاد مكان لها في البيئة الاستراتيجية، ولكن بصورة رقمية وتكنولوجية، وهي صراعات قديمة جديدة، بدأت منذ الوقت الذي ابتكر فيه الانسان أدوات تواصله الأولى، منذ الحربين العالميتين الأولى والثانية، وما سبقهما من حروب وثورات وقعت في عقدي الثورة الفكرية والصناعية.١٣ فضلا عن ذلك، ادى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلفته من حروب سيبرانية الى مزيد من التهديدات والتداعيات على تفاعلات السياسة الدولية،١٤ منها تحديث القدرات الهجومية والدفاعية، اذ سعت الدول الى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية والاستثمار في البنية التحتية المعلوماتية وتأمينها وتحديث القدرات العسكرية. ١٥ الاستعداد لتهديدات المستقبل، حيث تبنى العديد من الدول استراتيجية حرب المعلومات بحسبانها حرب للمستقبل، بهدف التشتيت، واثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم.

ولمعرفة الانواع المختلفة من الهجمات السيبرانية، تقسم التهديدات السيبرانية التي تواجهها الدول الى أربعة أنماط رئيسية هي: ١٦

١. هجمات الحرمان من الخدمة: حيث يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم او الجهاز على معالجتها والاستجابة لها، مما يؤدي الى توقفه بصورة جزئية او كلية او ابطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي، وهي تستعمل كثيرا ضد مواقع الانترنيت او البنوك او المؤسسات من أجل التأثير عليها أو لدفع فدية مالية.
٢. اتلاف المعلومات أو تعديلها: ويقصد به الوصول الى المعلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي الى نتائج كارثية خاصة إذا كانت خطط عسكرية او مواعيد او خرائط سرية.
٣. التجسس على الشبكات: ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير او تغيير في البيانات. والهدف منه الحصول على المعلومات قد

١٣. يونس مؤيد مصطفى, مصدر سبق ذكره, ص ١٢٤ .
١٤. عادل عبد الصادق, الفضاء الإلكتروني والعلاقات الدولية : دراسة في النظرية والتطبيق, المكتبة الأكاديمية , القاهرة , ٢٠١٦, ص٢٢- ٢٦ .
١٥. عادل عبد الصادق, القوة الإلكترونية : أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني, مجلة السياسية الدولية ، العدد ١٨٨, مركز الاهرام للدراسات السياسية والاستراتيجية ، ابريل ٢٠١٢, ص ٢٧ .
١٦. اسماعيل زروقة, الفضاء السيبراني والتحول في مفاهيم القوة والصراع, مجلة العلوم القانونية والسياسية, المجلد ١٠, العدد ٠١, جامعة الوادي ، الجزائر ، ٢٠١٩, ص١٠٢٢ .

تكون خطط عسكرية أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلباً على مهام الخصم، ١٧ وايضاً الدخول الى الانظمة الخاصة للدول لإضعافها وضرب المصالح القومية لها، من قبل الدول التي تريد للقوى العظمى زوال مكانتها غي النظام الدولي سواء كانت دول منافسة مثل الولايات المتحدة الامريكية، روسيا، الصين، كوريا الشمالية. ١٨

٤. تدمير المعلومات: يتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، ويصطلح عليه « تهديد لسلامة المحتوى « ويعني بها إحداث تغيير في البيانات سواء بالحذف أو تدمير من قبل أشخاص غير مخولين.

نستنتج في نهاية البحث، لقد تنبه إلى هذا الموضوع الكثير من المختصين والمفكرين، فركزوا عليه بالبحث والتحليل في نطاق النزاعات والهجمات السيبرانية عموماً، واصبحت التهديدات السيبرانية مصدر قلق لكثير من الدول، وتأثيرها على استراتيجية الدول وانعكاساتها على العلاقات الدولية، وهو ما سنتعرض اليه فيما يلي في المبحث الثاني.

١٧. سليم دحماني, أثر التهديدات» السيبرانية «على الأمن القومي الولايات المتحدة الأمريكية ـــآنموذجاـــ ، رسالة ماجستير, جامعة محمد بوضياف ـــــ المسيلة, الجزائر, ٢٠١٨, ص ٢٢ .

١٨. اسراء شريف جيجان, مصدر سبق ذكره, ص ١٠ .

المبحث الثاني
طبيعة التهديدات السيبرانية
بين الولايات المتحدة الامريكية والصين

تزايدت العلاقة بين الأمن والتكنولوجيا خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول الى أخطار وتهديدات، مما دعا حماية قيم المجتمع الأساسية وابعاد مصادر التهديد، وغياب الخوف من خطر تعرض هذه القيم للهجوم.

كتنت المنافسة على القوة بين القوى الكبرى في العالم تعتمد دائما على المشهد الأمني الاستراتيجي وعلى مر السنيين , تطورت العمليات العسكرية والحروب مع تطور أسلحة ومعدات وتقنيات جديدة وقد شهد نشأ القرن الحادي والعشرين ثورة أخرى في الشؤون العسكرية عندما تم تحديث الحرب الإلكترونية وبرزت التهديدات السيبرانية والحرب السيبرانية ,في القرن الحالي , نشأت أقطاب قوى جديدة, حيث بدأت الصين وأمريكا في التنافس على جميع مستويات وفي جميع المجالات , وتسببت الاختلافات في وجهات النظر السياسية وبعض المنافسة لكسب نفوذ أكبر في مناطق مختلفة في ان تصبح الولايات المتحدة الأمريكية والصين دولتين متنافسة , لذا تدهورت العلاقات الثنائية الى درجة أن كلا البلدين لا يثقان في نوايا وأفعال وأهداف بعضهم البعض .

المطلب الاول: المنظور الأمريكي لصعود التهديد السيبراني الصيني

ان الهيمنة السيبرانية الصينية يشكل خطراً مباشراً ووخيماً على نسيج الأمن القومي الأميركي. فالبنية الأساسية المخترقة قد تشل الاستعداد العسكري، وتعطل العمليات الاستخباراتية، وتقوض بشدة قدرة الولايات المتحدة على الدفاع عن نفسها والوفاء بالتزاماتها الاستراتيجية العالمية. وتمتد هذه الثغرة إلى ما هو أبعد من الجيش، مما قد يؤدي إلى تآكل التحالفات وتشجيع الجهات الفاعلة العالمية المعادية. ١٩

من منظور الولايات المتحدة الأمريكية تمثلت الشكوى الأساسية في اختراقات الصين المتكررة لأنظمة الولايات المتحدة عبر الفضاء الإلكتروني لأغراض التجسس تتعلق بالأمن القومي، واحتمال أن تكون الصين مستعدة لهدم البنى التحتية الأساسية للولايات المتحدة في حال نشوب أزمة، كما عربت الولايات المتحدة عن مخاوفها تجاه معاملة الصين للشركات الأمريكية بذريعة حماية أمنها. ٢٠

---

19. Jason Collins, Us Firm Launches Effort To Fight Chinese Cyber Espionage, Warrior Contributoroc ,4,2023, Aviribal At: Https://Warriormaven.Com/Author/Jason-Collins-Warrior-Contributo .

٢٠. سكوت وارين هارلد , مارتن سي .ليبيكي , التوصل الى اتفاق مع الصين بشأن الفضاء الإلكتروني , مؤسسة RAND, سانتا مونيكا , كاليفورنيا, ٢٠١٦, ص ٦ــ ٩ .

اتهمت الولايات المتحدة الامريكية الصين عدة مرات بالاهتمام بالقضايا السيبرانية مثل أنشطة التجسس السيبراني التجارية والحوادث السيبرانية الضخمة، بينما نفت الصين واحتجت بشدة ذلك الاتهام في الوقت نفسه. وفي مارس عام ٢٠١٤، اتهمت وزارة العدل الأمريكية، سبعة مواطنين صينيين يعتقد أنهم أعضاء في مجموعة القرصنة ((APT٣١، التي تم تسميتها في عدد من الهجمات على المنظمات الأمريكية منذ عام ٢٠١٤. قدم الحادث إضاءة جديدة لنطاق استخدام الحكومة الصينية لجماعات القرصنة الخاصة للتجسس ضد المنافسين الأجانب ، ويبدو أن حملة القرصنة تستهدف مجموعة واسعة من الصناعات ، بما في ذلك: شبكة الاتصالات, محطات معالجة المياه, وشبكات الكهربائية , وخطوط أنابيب النفط والغاز الطبيعي , وأنظمة النقل «.٢١

وفي تحذير مباشر من احتمال تعريض البنية التحتية للخطر بسبب التهديدات والهجمات السيبرانية من الصين,من حيث ان المتسللين الصينيين يكمنون استعداداً لإحداث فوضى والتسبب بضرر حقيقي للمواطنين والمجتمعات الأمريكية, ولم يكتف التهديد السيبراني باتخاذ إجراءات في البنية التحتية الحيوية بل تسلل ببساطة وحفر فيها, حيث اصبح التهديد السيبراني الصيني وغيره من الجهات الفاعلة المماثلة أكثر جرأة في استكشاف أنظمة البنية الأساسية الحيوية . ٢٢

لقد تصاعدت التوترات بين الولايات المتحدة والصين بسبب قلق الولايات المتحدة المتزايد بشأن القدرات العسكرية الصينية وتحديثها , وقضايا تتراوح من تايوان وبحر الصين الشرقي الى بحر الصين الجنوبي ,وقد تزايدت مخاوف الولايات المتحدة من ان الصين تجهز لضربات معلوماتية على شبكاتهم الالكترونية لتحقيق اغراض عسكرية, كما ان لدى الصين مخاوف مماثلة نابعة من التحديث العسكري للولايات المتحدة والسياسات التي تبنتها الولايات المتحدة بدءاً من اعادة التوازن في منطقة اسيا والمحيط الهادي الى استراتيجية المحيطين الهندي والهادي . ٢٣

ان تركيز الأنشطة السيبرانية الصينية الخبيثة التي تستهدف البنية التحتية الحيوية من خلال تحالف استخباراتي إلكتروني شامل ومنسق سيجعل الأمر أكثر صعوبة وتكلفة بالنسبة لبكين لمواصلة مسارها الحالي. وبنفس القدر من القيمة، فإن هذا من شأنه أن يرسل إشارة واضحة إلى العالم بأن الولايات المتحدة وحلفاءها وشركائها الإقليميين على استعداد لمنافسة بكين في الفضاء الإلكتروني لتأمين الحرية الدائمة للنظام البيئي الرقمي

٢١. الصين تحتج بشدة على اتهامها بالقرصنة الإلكترونية , صحيفة العرب الشرق الاوسط ,٢٦ مارس ٢٠٢٤ .

22. Scott Ikeda, More Warnings From Us And on Officials On Chinese Cyber Threat: "Epoch-Defining Challenge"CPO Magazine, Rezone Pte. Ltd., Singapore May 2024 , p.3.

23. Jon Lindsay,China And Cybersecurity Political, Economic, And Strategic Dimensions, IGCC Workshop Report on China and Cybersecurity, 2012, P2.

العالمي. ٢٤

المطلب الثاني: المنظور الصيني للتهديد السيبراني الأمريكي

تسعى الصين الى الحصول على أحدث التقنيات التي لها تأثير كبير على عمليات التجسس السيبراني, وضمان النمو الاقتصادي والاستقرار والسيطرة على الانترنت للحفاظ على حكم الحزب الشيوعي الصيني ودعم القدرة العسكرية من خلال التقنيات المتقدمة في الفضاء السيبراني ووضع خطط للبنية التحتية الحيوية للقوات العسكرية التي يحتمل ان تكون معادية وهذه السياسات واللوائح هي استراتيجيات الحكومة الصينية للتعامل مع التهديدات السيبرانية وتعزيز الأمن السيبراني ويمكن ان تكون هذه السياسات في الصين هي الأساس لوضع خارطة طريق لتحسين أمنها في العالم السيبراني . ٢٥

بدأت الولايات المتحدة منذ أكثر من عقدين بالقلق ازاء نقاط الضعف في المجال السيبراني وذلك بالبحث عن طريق للحد منه، وفي الوقت نفسه بدأت بشكل سري في تطوير واستخدام العمليات السيبرانية الهجومية لأغراض عسكرية مع ضمان تعديل وكالات الاستخبارات التابعة لها لتكييف أنشطة جمع المعلومات الخاصة بها ليشمل استحواذ على شبكة الإنترنت. ٢٦

تنظر الصين الى الولايات المتحدة بمزيج حذر من الشك والشراكة والمنافسة، يعتقد الصينيون أن الولايات المتحدة هي قوة رجعية تسعى إلى الحد من النفوذ السياسي للصين والإضرار بمصالح الصين، إحدى الطرق لمواجهة التفوق الأمريكي هي أن تشارك الصين في عمليات الكترونية في محاولة لانتزاع المعلومات من « الدبلوماسية والاقتصادية والدفاعية «. ٢٧

نتيجة عمليات التجسس الصينية ونظرا للحوادث السيبرانية الضخمة , اتهمت أمريكا الصين بالتهديدات من جانب القراصنة الصينيين , وارتكاب تجسس الكتروني ضد شركات امريكية, وهددت الصين بفرض عقوبات سيبرانية وفرض عقوبات على الكيانات التي استفادت من أنشطة التجسس التجاري, لكن تشجب الصين اتهامات الولايات

24. Victor Atkins, to combat Chinese cyber threats, the US must spearhead a new Indo-Pacific intelligence coalition, Atlantic Council (Adrienne Arsht Latin America Center) , Washington, February 2024 , p.2,
25. Nadia Dian Ardita & others, Op. Cit P.22
26. James A. Lewis, "A Necessary Contest: An Overview of U.S. Cyber Capabilities." Asia Policy, vol. 27 no. 2020 ,2, P. 84.
27. Emilio Iasiello, China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities, Journal of Strategic Security, USF Libraries at Scholar Commons, Volume 9, Number 2 Article2016) ,4): p 47.

المتحدة لها بالقرصنة وتدعي بأنها هي ضحية للهجمات السيبرانية الصادرة من الولايات المتحدة , ويشكو المسؤولون والمحللون الصينيون من القيود المفروضة من الولايات المتحدة على شركات الاتصالات الصينية الى الاسواق مثل شركة هواوي (Huawei) وشركة زت تي اي(ZTE Corporation) , ٢٨ وكذلك يدين المراقبون الصينيون ما يصفونه « بالهيمنة الامريكية على الانترنت ويشيرون الى العديد من الموجهات والخوادم والبرامج المستخدمة لدعم البنية التحتية للإنترنت في الصين إما تصنعها أو تتحكم فيها الشركات الامريكية, ٢٩ خاصة ان الولايات المتحدة تعمل على الاستثمار المستمر في البحث والتطوير من خلال الزيادة في تقنيات واستراتيجيات الأمن السيبراني لتعزيز قدراتها الدفاعية وضمان بقاء بنيتها التحتية الحيوية أمنة ضد التهديدات المستقبلية, وبالرغم من سعي الولايات المتحدة والصين الى التوصل الى أتفاق عبر المفاوضات او أيجاد طريقة أخرى للاتفاق على الأعراف والسلوكيات المتعلقة بالفضاء الإلكتروني, ومنها «اتفاقية الأمن السيبراني» (٣٠) في ٢نوفمبر لعام ٢٠١٥ على الرغم من فرصة التعاون ضئيلة بين الدولتين, كان هناك عدم ثقة بين الممثلين لان الاهداف التي حاول تحقيقها مختلفة في ما يتعلق بمصالحهما, حاولت الولايات المتحدة وقف الأنشطة السيبرانية غير القانونية للصين من خلال حملها على الحوار اولاً من ناحية أخرى لم تعترف الصين أبداً بأي عمل تجسس يمكن اعتباره تهديداً لواشنطن , وكان لكل الطرفين مطالبات مختلفة لم يرغب كل طرف في الاعتراف به على انه الطرف الذي بدأ الاحتكاك .

يشكو مراقبو جمهورية الصين الشعبية بمرارة من «هيمنة» الإنترنت الأمريكية، مشيرين إلى أن معظم أجهزة التوجيه والخوادم والبرامج المستخدمة لدعم العمود الفقري للإنترنت في الصين تنتجها شركات أمريكية.٢٣ ويلاحظ آخرون، مثل جيانغ تشونغ، مدير مركز أبحاث الأمن الاقتصادي في المعاهد الصينية للعلاقات الدولية المعاصرة (CICIR)، «المزايا الاحتكارية» للولايات المتحدة في مجالات مثل المعايير التكنولوجية. المرافق الأساسية وموارد الملكية الفكرية ودقة اسم النطاق، بحجة أن هذه تشكل شكلا من أشكال «الهيمنة السيبرانية». ٣١

٢٨. صلاح حيدر عبد الواحد , حروب الفضاء الإلكتروني : دراسة في مفهومها وخصائصها وسبل مواجهتها , رسالة ماجستير, جامعة الشرق الأوسط , كلية الآداب والعلوم قسم العلوم السياسية , ٢٠٢١, ص ٥٩ .

29. Nicole Perlroth, "China Is Said to Use Powerful New Weapon to Censor the Internet," New York Times, April 2015 ,10; "China Behind Cyberattack on US Sites, Report Says," San Francisco Chronicle, May 2015 ,8.

٣٠. تعد اتفاقية الأمن السيبراني بين الولايات المتحدة الامريكية والصين خطوة أولية, ولكنها ليست فعالة في حد ذاتها من حيث تحقيق التعاون في الفضاء السيبراني ووقف التجسس الاقتصادي , اذ جاء فيها: عدم قيام الطرفين بالقرصنة او سرقة الأسرار التجارية او الانخراط او دعم شبكات التجسس التجارية , وهي تساعد على جعل الحوار بينهما حول أمن الشبكات أقل تصادماً من جهة وهي أقوى دليل على جهود الحكومة للحد من أنشطة التجسس السيبراني .

31. Jiang Chong, "Cyber: The Invisible New Battlefront [Wangluo: Kanbujian de xin zhanxian]," Seeking Truth [Qiu Shi], No. 2010 ,13, pp. 55–53 .

بسبب استمرار الهجمات الالكترونية ضد البنية التحتية الاساسية فرضت الولايات المتحدة عقوبات اقتصادية وقيود على السفر على الحكومة الصينية الذي يعتقد انهم وراء الهجمات السيبرانية، وهناك احتمال من انهيار المحادثات الثنائية نظراً للانقسام الواضح بين اصحاب المصلحة في الولايات المتحدة. بالرغم هناك اختلافات جوهرية بين الصين والولايات المتحدة بقضايا حوكمة الانترنت , وقانون مكافحة الارهاب الجديد , والعلاقات العسكرية في الفضاء الالكتروني وتواصل كل من الصين والولايات المتحدة بناء ترسانات الاسلحة السيبرانية الخاصة بكل منهما واستكشاف شبكات كل منهما , اذ تعهد الرئيس لبصين « يشي جين بينج « بتحسين قدرات الصين في الحرب السيبرانية وتعزيز» قدرات الدفاع والردع السيبراني» ونشرت وزارة الدفاع الامريكية دليلا جديداً لقانون الحرب , حيث يتم الترويج لـ «القنابل المنطقية « في شبكات وأنظمة معلومات دولة معادية , وهذا من شأنه ان يزيد من تأجيج المنافسة ويولد انعدام الثقة «٣٢

أن التهديدات السيبرانية ليست سوى أداة واحدة من أدوات القوة الناعمة التي تستخدمها الصين ولكنها تمنح البلاد نفوذاً واسع النطاق على البلدان المدينة. اذ تهدف كلا الدولتين الى ان تصبح قوة عظمى عالمية مهيمنة من خلال الاستعداد مبكرا للتهديدات والتحديات.

32. Franz-Stefan Gadym, China-US Relations in Cyberspace: A Half-Year Assessment, china) focus, Jun 2016 , 16, Available At: https://www.chinausfocus.com/peace-security/china-us-relations-in-cyberspace-a-half-year-assessment?gad_source=1&gclid=CjwKCAjw4_K0BhBsEiwAfVVZ_1p6hRpUhnTMmJsd4QSONBCAKgIBZW_BksBhMpwPNAjrpF9jWvd0hhoCXxQQAvD_BwE, time of Visit: 10 August 2024..

المبحث الثالث

مستقبل التهديدات السيبرانية الأمريكية ــ الصينية

تعد العلاقات بين الولايات المتحدة والصين من بين العلاقات الاكثر اهمية في العالم، ويستفيد الجانبان بشكل كبير من الانترنت واستخدام التكنولوجيا، لكن مسألة التهديدات السيبرانية والاتهامات المتكررة بالقرصنة والتجسس في حلقة لانهاية لها من الفرص الضائعة للمصالحة من قبل الدولتين، سنتطرق في هذا المبحث على كيفية انعكاس التهديدات السيبرانية على مستقبل العلاقات الأمريكية ـــ الصينية، وحماية مستقبل أمريكا وتخفيف من أثار السيطرة الصينية على البنية التحتية الحيوية في الولايات المتحدة، بما تفرضه من تحديات معقدة على الاستقرار والسلام العالميين.

المطلب الأول: زيادة حدة التهديدات

لذا أعربت الوكالات الفيدرالية الأمريكية عن قلقها من المجموعات التي ترعاها الصين والتي تحاول الوصول إلى أنظمة تكنولوجيا المعلومات الخاصة بخطوط الأنابيب الأمريكية وشركات الاتصالات وغيرها، من المرجح أن تكافح السلطات الأمريكية لردع العمليات السيبرانية الصينية الهجومية. ٣٣

لا تزال الصين والولايات المتحدة بحاجة إلى معالجة قضايا الأمن السيبراني، بما في ذلك التعاون في مجال إنفاذ القانون. وضع قواعد دولية في الفضاء السيبراني؛ الوصول إلى الأسواق؛ والثقة بين جيوشهم. وتمثل القضية الرابعة تتعلق بالجيش الخطر الأكبر، من حيث أن الولايات المتحدة كانت تضغط من أجل عسكرة الفضاء الإلكتروني والدعوة إلى العمليات السيبرانية الهجومية، مما يزيد من خطر نشوب صراعات إلكترونية بين البلدين. ٣٤

يمكن فهم أن قضايا الأمن السيبراني بين الصين والولايات المتحدة لا تقتصر فقط على سياق الدفاع ولكنها مرتبطة بالسياق الاقتصادي بين الدولتين وان التهديدات السيبرانية مرتبطة بالتهديدات التجارية ويعتبر كلا الطرفين الطرف الاخر منافساً بل ويميل الى أن يشكل تهديداً للسلع التجارية لكل بلد.

ثانياً: انخفاض حدة التهديدات

إن الطبيعة العالمية للتهديدات السيبرانية تتطلب من الولايات المتحدة اتباع نهج دولي تعاوني في الدفاع السيبراني وتعزيز تدابير الأمن السيبراني في جميع قطاعات البنية

٣٣. مستقبل الأمن السيبراني , مقالة منشورة في الانترنت أغسطس ٢٠٢٣, https://search.app/dD٦NgNv٢yfbmPAHp٧ .

34. Lena Allen, America's Future: Mitigating the Implications of Chinese Control Over U.S. Critical Infrastructure, April 2024 ,12.

التحتية الحيوية من خلال تبادل المعلومات الاستخباراتية حول التهديدات، وتنسيق جهود الاستجابة، والوعي الشامل بالتهديدات، والمشاركة في الجهود الدبلوماسية الرامية إلى إرساء المعايير السيبرانية، وبذلك تستطيع الولايات المتحدة تعزيز دفاعاتها وتعزيز مجال رقمي أكثر استقراراً وأمناً. ٣٥

لأداره القضية السيبرانية في أطار علاقة ثنائية , واقناع جمهورية الصين الشعبية برؤية المفاوضات كوسيلة لتقليل من احتمال حدوث مزيداً من التهديدات و التدهور في العلاقات الثنائية يجب على الولايات المتحدة والصين ايجاد طريقة للتوصل الى تسوية مؤقتة باتفاق تفاوضي, للوصول الى وضع حد وتخفيف من خطر التهديد ووضع حد للقرصنة التي ترعاها الدولة واي شكل من اشكال الهجمات الإلكترونية بما في ذلك التجسس الإلكتروني, بل وضع أطار عمل من شأنه ان يساعد ليس فقط في منع الخلافات من الانتشار الى أجزاء أخرى من العلاقات الثنائية , بل ومساعدة الدولتين على الاقتراب من فهم ما يشكل الاستقرار الاستراتيجي, أي السلام في الفضاء الإلكتروني.

اجراء مناقشات رسمية بين الطرفين حول معايير السلوك المقبولة والشفافية الحوار، وتقليل احتمالية تحول الصراع في الفضاء الإلكتروني الى حركية، بالإضافة الى ان كلا الطرفين لديهم مصلحة مشتركة في منع المتطرفين والجماعات الإرهابية والأطراف الثالثة الأخرى من مهاجمة البنية التحتية الحيوية،ولمواجهة التهديد الذي تتعرض له البنية التحتية الحيوية من قبل «فولت تايفون» وغيرها من الجهات الفاعلة السيبرانية الصينية التي ترعاها الدولة، يجب على الولايات المتحدة إطلاق تحالف جديد متعدد الأطراف لتبادل المعلومات الاستخباراتية حول التهديدات السيبرانية في منطقة المحيطين الهندي والهادئ. يجب أن يستفيد هذا التحالف من بعض الدروس المستفادة من تحالف العيون الاستخباراتية الخمسة،. ومن شأن توسيع نطاق وموارد مثل هذا التحالف أن يساعد في تعطيل التهديدات السيبرانية، والإشارة إلى العالم بأن الولايات المتحدة وشركائها ملتزمون بحماية البنية التحتية السيبرانية والمادية من الجهات الفاعلة الخبيثة، والمساعدة بشكل مثالي في ردع التهديدات السيبرانية المستقبلية من الصين. ٣٦

ثالثاً: بقاء الوضع الحالي

ان العلاقات بين البلدين ساءت بسبب قضية الانترنت ولا تزال الدولتان تواجهان عقبات كبيرة في تطوير الجهود التعاونية ونحسين التفاهم المتبادل بشأن قضية التهديدات

35.) Lena Allen Op.Cit.
36. Adam Segal, A brief for the U.S.-China Relations in Strategic Domains Project, the national bureau of Asian research, Washington, 2015, p.3.

والفضاء السيبراني، ونتيجة للدرجة العالية من عدم الثقة بين البلدين والضغوط السياسية المتزايدة في الولايات المتحدة لفرض العقوبات على الصين بسبب الاختراقات والقرصنة، أقصى ما يمكن توقعه هو أن واشنطن وبكين ستبديان استعدادهما لمواصلة المناقشات الموضوعية لإدارة الخلافات ومنع تصعيد الأحداث في المجال السيبراني إلى أحداث فعلية.

ان الشكوك المتزايدة وعدم الثقة بينن البلدين يدفع علاقتهما في اتجاه سلبي وبقاء الوضع، وبالرغم لما له هذا الاتفاق من أهمية سياسية، لا يزال غير واضح إذا كان هذا الاتفاق والتعاون سيساعد في خفض عدد التهديدات السيبرانية الصينية ضد الولايات المتحدة الأمريكية. ٣٧ تنكر الصين انها لم تفعل انتهاكات ضد الولايات المتحدة ولا عمليات تجسس ولا عمليات قرصنة، لذا من الصعب التوصل الى أتفاق بين البلدين، تنفي جمهورية الصين الشعبية على الجانب الآخر من العالم مزاعم القرصنة باعتبارها خاطئة، وهكذا، اتهامات متكررة بالقرصنة من قبل دولة ضد أخرى في حلقة لا نهاية لها من الوهم والفرصة الضائعة للمصالحة من قبل الدولتين القوميتين.

يوجد ثلاث خيارات سياسية أساسية للولايات المتحدة في التعامل مع الصين حول هذه القضية: التركيز بشكل أساسي على تحسين الدفاعات السيبرانية الأمريكية، أو محاولة إقناع الصين بتغيير سلوكها من خلال الدبلوماسية، أو التفاوض على المعايير والسلوك، أو إجبار الصين على تغيير ممارساتها السيبرانية من خلال الإكراه. تعزيز الدفاعات الأمريكية هو أحد خيارات السياسة الرئيسية, على سبيل المثال يمكن للولايات المتحدة أن تحاول إحراج الصين لتغيير سلوكها بينما تعرض عليها أيضا نوعا من الترتيب التفاوضي. وبالمثل، يمكن للولايات المتحدة أن تسعى إلى تحسين دفاعاتها (الردع عن طريق الإنكار) مع الضغط أيضا على الصين للتفاوض. ٣٨

وعلى المدى الطويل، سوف يقرر عاملان ما إذا كانت الصين والولايات المتحدة ستتعاونان أو تتنافسان مع بعضهما البعض في الفضاء الإلكتروني. الأول هو إزالة الاقتصاد من خلال الاقتصاد الرقمي والأمن الجغرافي التقليدي من خلال الأمن السيبراني, سيكون لها تأثير مهم على علاقات الفضاء الإلكتروني، والعلاقات الثنائية بشكل عام. وينطوي العامل الثاني على بناء الثقة المتبادلة في المجالين العسكري والاستخباراتي. ومن المحتمل أن يؤدي أي نقص في الثقة المتبادلة إلى صراعات منخفضة الشدة.

---

٣٧. فريدة طاجين, تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى دراسة حالة ــ الصين ـــرسالة ماجستير, جامعة قاصدي مرباح ورقلة, كلية الحقوق والعلوم السياسية, ٢٠١٨, ص ٧٧ ــ ٧٨ .

38. Scott Warren Harold, Cyber Problem" in U.S.-China Relations,: RAND Corporation Stable URt, 03 Aug 2024: https://www.jstor.org/stable/10.7249/j.ctt1cx3vfr.. 6

الخـــاتـمة

أتسم عالم اليوم، والذي اضفى عليه التقدم التقني سمة عصر السرعة والمعرفة، لينتقل الأمر من العصر الإنساني الى العصر الآلي، وهو خلاصة معبرة عن تدخل التكنولوجيا في مجمل نواحي الحياة العامة للشعوب والدول ان تطور المجتمعات والثورة التكنولوجية في المعلومات والاتصال، والتوجه نحو مجتمع المعلومات والمعرفة

نظرا لطبيعة التهديدات السيبرانية المتجددة هناك تغير واستمرار في السياسات والعلاقات بين الولايات المتحدة الامريكية والصين، فيما يخص الأمن الفضائي السيبراني، وهي استراتيجيات استباقية وقائية لردع الهجمات الفضائية يشمل كل الابعاد السياسية والاقتصادية والعسكرية والمدنية،

إن إمكانية سيطرة الصين على البنية التحتية الحيوية للولايات المتحدة تمثل تهديدًا كبيرًا للأمن القومي الأمريكي، والاستقرار الاقتصادي، والرفاهة المجتمعية. ويتطلب التصدي لهذا التحدي استراتيجية شاملة ومتعددة الأوجه تشمل تعزيز الدفاعات السيبرانية، وتعزيز المرونة والتكرار، والتعاون الدولي، والابتكار المستمر في تقنيات الأمن السيبراني.

وعلى الرغم من الاحتياطات المستمرة من قبل الولايات المتحدة الامريكية نلاحظ عمليات قرصنة واختراقات وتسريبات المعلومات، لأن مجال التهديدات السيبرانية مجال حيوي ومتجدد ما ان تتوصل الى طرق لمعالجة الاختراقات وترصين الشبكات حتى يظهر نوع ونمط جديد للتهديدات وهذا يعتمد على فعالية وحيوية الوحدات الدولية لاكتشاف الثغرات التي من خلالها الوصول الى الاهداف الساعية الى تحقيقها.

الاستنتاجات

١. دفعت الحرب السيبرانية الحالية دولا في العالم إلى تطوير قواتها العسكرية وغير العسكرية في الفضاء الإلكتروني. إحداها هي الصين، التي تعتبر أنه من خلال زيادة قوتها في الفضاء الإلكتروني، ستكون هناك زيادة متسارعة في القدرات في المجالات الاقتصادية والعسكرية. على الرغم من أن الحكومة الصينية نفت أن القرصنة لم تكن عملا تم تنفيذه تحت قيادة جيش التحرير الشعبي، إلا أن التحقيق الذي أجرته الحكومة الأمريكية أظهر أدلة قوية من خلال تتبع موقع وهوية المتسللين الخمسة.
٢. يمكن فهم أن الحرب السيبرانية بين الصين الولايات المتحدة هي حالة معقدة. زعمت كل من الصين والولايات المتحدة أن أفعالهما كانت تعتبر إجراءات دفاعية. المشكلة هي أن الصين بدأت خطوتها الأولى بمهاجمة البنية السيبرانية الإمريكية, علاوة على ذلك، كانت علاقة الصين والولايات المتحدة عالية التوتر في السنوات الأخيرة أدنى شيء لا يزال التحليل حول هذه المسألة مستمرا، حيث ستستمر المنافسة بين البلدين في المستقبل، مما يخلق إمكانيات لمزيد من الأبحاث والدراسات.

المراجع

اولاً: الكتب العربية

١. ايهاب خليفة، القوة الالكترونية: كي يمكن ان تدير الدول شؤونها في عصر الانترنت، دار العربي للنشر والتوزيع، بيروت, ٢٠١٧, ص٢٧.

٢. عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، القاهرة، المكتبة الأكاديمية , ٢٠١٦, ص٢٢ــ ٢٦

٣. منير البعلبكي، المورد: قاموس انكليزي ـــ عربي، دار العلم للملايين، بيروت , ٢٠٠٤, ص ٢٣٤.

ثانياً: بحوث ومجلات

٤. أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، العدد الرابع , ٢٠١٦, ص١٨

٥. اسراء شريف الكعود، التأثير السيبراني في الأمن القومي للدول الفاعلة (الولايات المتحدة الأمريكية) انموذجا، مجلة العلوم السياسية/ جامعة بغداد، العدد (٦٤) كانون الاول (٢٠٢٢)، ص ٤.

٦. اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، المجلد ١٠, العدد ٠١, ٢٠١٩, ص١٠٢٢.

٧. أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد ٣٥، كلية القانون /جامعة الإمارات العربية المتحدة، ٢٠٢٠, ص ٣٩٤.

٨. تيري ديبيل، استراتيجية الشؤون الخارجية منطق الحكم الأمريكي، ترجمة: وليد شحادة، دار الكتاب العربية، مؤسسة محمد بن آل راشد آل مكتوم، بيروت , ٢٠٠٩, ص٢٥٨.

٩. رولا حطيط، السيبرانية: الحرب الخفية في المنطقة المظلمة، مركز باحث للدراسات الفلسطينية والاستراتيجية، بيروت , ٢٠٢٠, ص ٤.

١٠. عبد القادر محمد فهمي،الحروب التقليدية وحروب الفضاء الإلكتروني: دراسة مقارنة في المفاهيم وقواعد الاشتباك، مجلة العلوم القانونية والسياسية، المجلد١٦,العدد ٢ـ القاهرة ٢٠١٨, ص ٢٢.

١١. عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسية الدولية، العدد ١٨٨, مركز الاهرام للدراسات السياسية

والاستراتيجية، ابريل ٢٠١٢, ص ٢٧
١٢. عادل عبد الصادق، الفضاء الالكتروني والرأي العام: تغير المجتمع والأدوات والتأثير»، المركز العربي لأبحاث الفضاء الإلكتروني: استراتيجية، العدد ٢٤٥٩, ٢٠١٣, ص٣٥
١٣. عادل عبد الصادق، انماط الحرب السيبرانية وتداعيتها على الأمن العالمي، مجلة السياسة الدولية، العدد ٢٠٨, المجلد ٥٢, مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، ابريل ٢٠١٧ , ص ٣٢
١٤. علي عبد الخضر محمد أثر التقدم التكنولوجي على المشهد الجيوسياسي بين الولايات المتحدة والصين، مجلة مركز بابل للدراسات الإنسانية، المجلد ١٣, العدد٢, ٢٠٢٣, ص١٠٧٧.
١٥. يحيى ياسين سعود، الحروب السيبرانية: في ضوء القانون الدولي الإنساني، المجلة القانونية، جامعة القاهرة، العدد٤, المجلد ٢٠١٨, السودان، ٢٠١٨, ص ٨٤
١٦. يونس مؤيد يونس مصطفى، استراتيجية الولايات المتحدة الامريكية للأمن السيبراني، مجلة قضايا سياسية، العدد ٥٥, كلية العلوم السياسية / جامعة النهرين، ٢٠١٨, ص١٢٤.

ثالثاً: الرسائل والاطروحات

١٧. سليم دحماني، أثر التهديدات» السيبرانية «على الأمن القومي الولايات المتحدة الأمريكية ـــآنموذجا ـــرسالة ماجستير، جامعة محمد بوضياف ـــــ المسيلة، الجزائر, ٢٠١٨, ص
١٨. فريدة طاجين، تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى دراسة حالة ـــ الصين ـــ رسالة ماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية, ٢٠١٨, ص ٧٧ ـــ ٧٨
١٩. صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، جامعة الشرق الأوسط، كلية الآداب والعلوم قسم العلوم السياسية , ٢٠٢١, ص ٥٩.

خامساً: الأنترنت

٢٠. ستيفن روتش، طبول الحرب السيبرانية بين الولايات المتحدة والصين، مقالة، ٢٧فبراير , ٢٠٢٤, على الموقع الالكتروني
project Syndicate " https://www.project syndicate.org
٢١. سكوت وارين هارلد، مارتن سي. ليبيكي، التوصل الى اتفاق مع الصين بشأن الفضاء الإلكتروني، مؤسسة RAND, سانتا مونيكا، كاليفورنيا, ٢٠١٦, ص ٦ـــ ٩.

٢٢. الصبن تحتج بشدة على اتهامها بالقرصنة الإلكترونية، صحيفة العرب الشرق الاوسط ,٢٦ مارس ٢٠٢٤.

٢٣. مستقبل الأمن السيبراني، مقالة منشورة في الانترنت أغسطس ٢٠٢٣, الرابط الإلكتروني .https://search.app/dD٦NgNv٢yfbmPAHp٧

References

1. Adam Segal, A brief for the U.S.-China Relations in Strategic Domains Project, the national bureau of Asian research, Washington, 2015, p.3
2. Jennie M. Williamson. Information Operations: Computer Network Attack in the 21 Century. Strategy Research Project (Pennsylvania:U.S. Army War College. Carlisle Barracks 22 (2002 .
3. Jon R.Lindsay,The Impact of China on Cybersecurity, International Security December ,2015,p15-14.
4. Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference. Online, Oxford University Press, 2010,p4.
5. Jason Collins, Us Firm Launches Effort to Fight Chinese Cyber Espionage, Warrior Contributor ,4,2023, Aviribal At : Https://Warriormaven.Com/Author/Jason-Collins-Warrior-Contributo . 11. Scott Ikeda, More Warnings from US And UK Officials on Chinese Cyber Threat: "Epoch-Defining Challenge" , CPO Magazine, Rezone Pte. Ltd, Singapore , May 2024 , p.3 .
6. Jon Lindsay, China and Cybersecurity Political, Economic, And Strategic Dimensions, IGCC Workshop Report on China and Cybersecurity, 2012, P2
7. US Chinese cyber threat to critical infrastructure, Geopolitical & Security Insights, May 2024 , https://dragonflyintelligence.com.
8. James A. Lewis, "A Necessary Contest: An Overview of U.S. Cyber Capabilities." Asia Policy, vol. 27 no. 2020 ,2, P. 84.
9. Emilio Iasiello, China's Three Warfare's Strategy Mitigates Fallout from Cyber Espionage Activities, Journal of Strategic Security, USF Libraries at Scholar Commons, Volume 9, Number 2 Article2016) ,4): p 47.
10. Nadia Dian Ardita & others, Cyberwarfare between the United States and China 2022 -2014
11. Victor Atkins, to combat Chinese cyber threats, the US must spearhead a new Indo-Pacific intelligence coalition, Atlantic Council (Adrienne Arsht Latin America Center) , Washington, February 2024 , p.2,
12. Jiang Chong, "Cyber: The Invisible New Battlefront [Wangluo: Kanbujian de xin zhanxian]," Seeking Truth [Qiu Shi], No. 2010 ,13, pp. 55–53 .
13. Franz-Stefan Gadym, China-US Relations in Cyberspace: A Half-Year Assessment, China US focus, Jun 2016 , 16, Available
14. Nicole Perlroth, "China Is Said to Use Powerful New Weapon to Censor the

Internet," New York Times, April 2015 ,10; "China Behind Cyberattack on US Sites, Report Says," San Francisco Chronicle, May 2015 ,8.
15. Lena Allen, America's Future: Mitigating the Implications of Chinese Control Over U.S. Critical Infrastructure, April 2024 ,12

First: Books Arabic

16. Ihab Khalifa, Electronic Power: So that States Can Manage Their Affairs in the Internet Age, Dar Al-Arabi for Publishing and Distribution, Beirut, 2017, p.7
17. Adel Abdel Sadek, Cyberspace and International Relations: A Study in Theory and Practice, Cairo, Academic Library, 2016, p 26 22
18. Minbar Al-Baalbaki, Al-Mawrid: English-Arabic Dictionary, Dar Al-Ilm Li Malayoun, Beirut, 2004, p. 234.

Second: Research and Journal

19. Ahmed Issa Nima Al-Fatlawi, Cyber-attacks: their concept and the international responsibility arising from them in the light of contemporary international organization, Al-Muhaqqiq Al-Hilli Journal for Legal and Political Sciences, University of Babylon, Fourth Issue, 2016, p 18
20. Esraa Sharif Al-Kaoud, The Cyber Impact on the National Security of Active States (United States) as a Model, Journal of Political Science / University of Baghdad, Issue (64), December (2022), p. 4.
21. Ismail Zarrouka, Cyberspace and the Transformation in the Concepts of Power and Conflict, Journal of Legal and Political Sciences, Volume 10, Issue 2019 ,01, p. 1022.
22. Amira Abdel Azim Mohamed, Cyber Risks and Ways to Confront Them in Public International Law, Journal of Sharia and Law, No. 35, Faculty of Law / U.A.E. University, 2020, p. 394.
23. Terry Debelle, Foreign Affairs Strategy: The Logic of American Governance, translated by: Walid Shehadeh, Dar Al-Kitab Arabic, Mohamed bin Rashid Al Maktoum Foundation, Beirut, 2009, p. 258.
24. Rola Hoteit, Cyber: The Hidden War in the Dark Zone, Researcher Center for Palestinian and Strategic Studies, Beirut, 2020, p. 4.
25. Abdel Qader Mohamed Fahmy, Conventional wars and cyber wars: a comparative study in concepts and rules of engagement, Journal of Legal and Political Sciences, Vol. 16, No. 2, Cairo, 2018, p. 22.
26. Adel Abdel Sadek, Cyber Power: Weapons of Mass Proliferation in the Cyber Age, International Political Magazine, Issue 188, Al-Ahram Center for Political and Strategic Studies, April 2012, p. 27
27. Adel Abdel Sadek, Cyberspace and Public Opinion: Community Change, Tools and Impact", Arab Center for Cyberspace Research: Strategy, Issue 2013 ,2459, p 35
28. Adel Abdel Sadek, Patterns of Syrian-Israeli warfare and its repercussions

on global security, Journal of International Politics, Issue 208, Volume 52, Al-Ahram Center for Political and Strategic Studies, Cairo, April 2017, pp. -32

29. Ali Abdel Khader Mohamed Al-Mamouri, The Impact of Technological Progress on the Geopolitical Scene between the United States and China, Journal of the Babylon Center for Humanitarian Studies, Volume 13, Issue 2023 ,2, p. 1077
30. Mona Abdel Allah Al-Samhan, Requirements for achieving cybersecurity for management information systems at King Saud University, Journal of the College of Education, Mansoura University, Issue 111 July 2020, p. 11.
31. Yahya Yassin Saud, Cyber Wars: In the Light of International Humanitarian Law, Legal Journal, Cairo University, Issue 4, Volume 2018, Sudan, 2018, p. 84
32. Younis Muayad Younis Mustafa, The United States Strategy for Cybersecurity, Journal of Political Issues, Issue 55, College of Political Science / Al-Nahrain University, 2018, p. 124.

Third: Theses and Dissertations

33. Salim Dahmani, The Impact of "Cyber" Threats on National Security United States as a Model Master Thesis, Mohamed Boudiaf University Messila, Algeria, 2018, p.
34. Farida Tagine, The Impact of Cyber Power on the Security Strategies of Major Countries: A Case Study of China, Master Thesis, Kasdi Merbah Ouargla University, Faculty of Law and Political Science, 2018, pp. 78 77
35. Salah Haider Abdul Wahid, Cyber wars: a study in their concept, characteristics and ways to confront them, Master Thesis, Middle East University, Faculty of Arts and Sciences, Department of Political Science, 2021,

Fifth: Internet

36. Stephen Roach, Drums of Cyber War between the United States and China, article, February 2024 ,27, at the project Syndicate website, https://www. project syndicate.org
37. Scott Warren Harald, Martin C. Libicke, Reaching an agreement with China on cyberspace, RAND Foundation, Santa Monica, California, 2016, pp. 9-6.
38. Al-Sabin strongly protests against accusations of electronic piracy, Al-Arab Al-Sharq Al-Awsat newspaper, March 2024 ,26.
39. The Future of Cybersecurity, article published in the Internet August 2023, link https://search.app/dD6NgNv2yfbmPAHp7.