دور الامن السيبراني في الامن العالمي في القرن الحادي والعشرين

م.د. سرى موفق مقصود

جامعة النهرين _ كلية العلوم السياسية

The Role of Cyber Security in the Global Century in the Twenty-First Century[1]

Sura Mwafak Maqsoud

Al-Nahrain University, Political Science, Iraq

DOI:10.37648/ijrssh.v13i02.071

Received: 06 May 2023; Accepted: 20 June 2023; Published: 26 June 2023

ABSTRACT

This study focuses on the concept of cybersecurity and its role in global security and the extent of changes that occurred in the concept of global security, especially in the twenty-first century and the competition between major powers for supremacy in cyberspace (the United States of America, China) and aims to demonstrate the importance of having an infrastructure in space This study concludes that cyberspace has become the most important field for these countries and the appropriate environment for settling inter-conflicts between the major powers.

الملخص:

تركز هذه الدراسة على مفهوم الامن السيبراني ودوره في الامن العالمي ومدى التغييرات التي طرأت على مفهوم الامن العالمي لاسيما في القرن الحادي والعشرين والتنافس بين القوى الكبرى على التفوق في الفضاء السيبراني (الولايات المتحدة الامريكية، الصين) وتهدف الى بيان مدى اهمية وجود بنية تحتية في الفضاء السيبرانية لتحقيق الاهداف والرؤيا الاستراتيجية للدول وحماية مصالحها وامنها القومي، **وتستنتج هذه**

[1] How to cite the article: Maqsoud S.M. (June 2023) The Role of Cyber Security in the Global Century in the Twenty-First Century; *International Journal of Research in Social Sciences and Humanities*, Vol 13, Issue 2, 842-857, DOI: http://doi.org/10.37648/ijrssh.v13i02.071

الدراسة ان الفضاء السيبراني اصبح المجال الاكثر اهمية لهذه الدول والبيئة الملائمة لتصفية النزاعات البينية للقوى الكبرى.

المقدمة:

ظهر الامن السيبراني نتيجة للتطور التقني والتكنولوجي الذي شهد العالم منذ اواخر القرن العشرين وشكل نقطة تحول في مفهوم الامن على المستوى العالمي، كما ان ظهور الامن السيبراني ادى الى اعادة ترتيب مقومات القوة للدول، كما ظهرت أداوات جديد اخذت دور واضح واهمية حقيقة فيما يخص الشأن الامني للدول ومنها (الحروب السيبرانية، الجيوش السيبرانية، الدفاع السيبراني، الارهاب السيبراني، الجريمة السيبرانية)، لذا نجد ان دول العالم عملت على تأسيس مؤسسات بحثية وامنية تهتم بدراسة الفضاء السيبراني وتعمل على توفير بنية تحتية في الفضاء السيبراني قادرة على تحقيق مصالحها السياسية والاقتصادية والامنية، لذا سنتطرق من خلال هذا البحث الى التغيرات التي طرأت على مفهوم القوة في النظام الدولي وكيف تم اعادة هيكلة مفهوم الامن القومي ليتضمن (الامن السيبراني) للمنظومة مقومات القوة للدول، وسيتم اخذ نماذج عالمية متمثلة بـ(الولايات المتحدة الامريكية، الصين) بأعتبارها القوى الفاعلة والمؤثرة بشكل اساسي في النظام الدولي وبأعتبارها القوة الضالعة في مجال الامن السيبراني.

الكلمات المفتاحية: الولايات المتحدة الامريكية، الصين، الامن السيبراني، الفضاء السيبراني.

اهداف البحث:

1- توضيح مفهوم الامن السيبراني ودوره في تحقيق مصالح الدول وحمايتها على المستوى السياسي والامني والاقتصادي.
2- بيان مدى اهمية وجود بنية تحتية في الفضاء السيبرانية لتحقيق الاهداف والرؤيا الاستراتيجية للدول وحماية مصالحها وامنها القومي.
3- بيان دور الامن السيبراني في العلاقات الدولية وكيفية استخدام الفضاء السيبرانية كمجال لتحقيق الاهداف في العلاقات الدولية.

مشكلة البحث:

تتمثل مشكلة البحث بالاتي:

1- ما هو الامن السيبراني على الامن السياسي والاقتصادي والامني للدول؟
2- هل بالامكان الاستعاضة عن الحروب التقليدية بالحروب السيبرانية لتحقيق اهداف الدول؟
3- مدى قدرة الدول النامية على توفير استراتيجية فعالة في مجال الفضاء السيبراني لترتقي الى مصاف الدول المتقدمة؟
4- هل الفضاء السيبراني اصبح بالفعل من اهم مقومات القوة للدول اضافة الى المقومات التقليدية للقوة (السياسي، الاقتصادية،الامنية)؟

فرضية البحث:

ينطلق البحث من فرضية مفادها " ان مجال الفضاء السيبراني له دور اساسي وفعال في تحقيق الامن القومي للدول بشكل خاص والامن العالمي للنظام الدولي بشكل عام، اي ان كلما كانت الدولة لديها بنية تحتية في مجال الفضاء السيبراني كلما كانت قادرة على حماية امنها القومي وتحقيق اهدافها الامنية والسياسية والاقتصادية".

المطلب الاول: الاطار النظري للامن السيبراني:

اولاً: مفهوم الامن السيبراني: جاء مصطلح "السيبرانية" (Cybernetic) مشتقاً من المصطلح الاغريقي (kybernetes) ويعني الطيار او قائد الدفة او الحاكم، والسيبرانية مأخوذة من من كلمة (cyber) وتعني صفة لاي شئ مرتبط بثقافة الحواسيب او تقنية المعلومات او الواقع الافتراضي، ويعد (وليام جيبسون- William Gibson) اول من استخدم كلمة (cyber) لتصبح في مفهوم الفضاء السيبراني (cyber Space) في كتابة الكلاسيكي عام (1984)[1] .

ظهر مفهوم (الامن السيبراني) بعد الحرب الباردة نتيجة للابتكارات التكنولوجية والتغيرات الجيوسياسية التي طرأت على النظام الدولي والتحول نحو الاعتماد على اجهزة الكمبيوتر في العديد من

(1) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الانسانية، مجلد(8)، العدد (2) جامعة بابل، بابل، 2018، ص200.

المجالات، وتم استخدامه لاول مرة من قبل علماء الكمبيوتر في اوائل التسعينات للتأكيد على حالات الاختراق المرتبطة بأجهزة الكمبيوتر، وتجاوز النطاق التقني عندما اتضح ان التهديدات التي تحدث بسبب التقنيات الرقمية من شأنها ان تؤدي الى اثار اجتماعية مدمرة[1]، ويقصد بـ(الامن السيبراني): أتخاذ اجراءات ووضع معايير لمنع وصول المعلومات الخاصة او لحماية تلك المعلومات بأن تكون في ايدي جهة معادية اشخاص غير مخولين بها عبر الشبكة المعلوماتية)، فالفضاء السيبراني هو مجال مفتوح ومنتفي السيادة ويعد مصدر لادوات جديدة للصراع الدولي، فتصبح الحكومة الالكترونية عرضة للعديد من التهديدات الداخلية والخارجية لاهداف مختلفة من خلال (الهاكرز)، بأختراق النظام الامني المعلوماتي للحكومة، لذا تطلب الامر وضع استراتجيات جديدة للامن القومي للدولة[2].

ومن الجلي الغني عن البيان ان مصادر القوة في العلاقات الدولية تتغير، فبالاضافة الى القوة الصلبة التي تتمثل بـ(القوة العسكرية) اخذت مصادر القوة الاخرى تأخذ دور واضح في مقومات القوة للدول مثل (القوة الاقتصادية)، ومن ثم ظهرت القوة الناعمة كأحد اهم مصادر القوة للدول، ومع ثورة المعلومات ظهر مصدر اخر من مصادر القوة وهو ما يعرف بـ(قوة السايبر) (Power Cyber)، ويعرف جوزيف ناي القوة السيبرانية بأنها: (القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، اي انها القدرة على استخدام الفضاء السيبراني لايجاد مزايا للدولة، والتأثير على الاحداث المتعلقة بالبيئات التشغيلية الاخرى، وذلك من خلال ادوات سيبرانية)[3].

وان الامن السيبراني اصبح يمتد من داخل الدولة الى النظام الدولي ليشكل جزء من الامن الجماعي العالمي، لا سيما مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي، لذا اصبحت هناك حاجة حقيقية ومصالح وطنية اقليمية دولية للحفاظ على امن الفضاء السيبراني، على اساس ان الفضاء السيبراني اصبح جزء لا يتجزء من الامن العالمي لاسيما مع التقدم التقني الذي يشهد العالم اليوم وتزايد التهديدات السيبرانية على البنية التحتية للمعلومات.

(1) تغريد معين حسن المشهدي، الاثر العسكري للامن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، جامعة الكوفة، كلية الاداب، المجلد الثاني، العدد (30)، 2019، ص240.

(2) محمود محارب، اسرائيل والحرب الالكترونية، الدوحة، المركز العربي للابحاث ودراسة السياسات، 2011، ص6.

(3) Joseph S.Nye JR, Cyber Power, Harvard Kennedy School, 2010, P.30.

ثانياً: المفاهيم المقاربة:

1- **الفضاء السيبراني:** يتمثل بأنه فضاء رمزي افتراضي وتصويري موجود في نطاق الإنترنت, وان أي شيء يتم عبر الإنترنت، يحدث داخل حدود الفضاء السيبراني، سواء أكان ذلك بإرسال بريد إلكتروني أو موقع ويب أو ممارسة لعبة، فكل هذه الأشياء موجودة داخل الإنترنت –الفراغ ، ويمكن القول إنّ (الفضاء السيبراني) هو مجال شامل متكون من شبكة تضم المنشآت التكنولوجية للإعلام بما فيها الإنترنت وشبكات الاتصال السلكي واللاسلكي, كما يفهمه الأمريكيون على أنه, "مجال شامل على مستوى البيئة الرقمية يتشكل من شبكات مرتبطة ومتواصلة بينياً بالمنشآت وتكنولوجيات الإعلام بما فيها الإنترنت, شبكات الإتصال, الحواسيب, وسائل الرقابة وغيرها"[(1)].

2- **الصراع السيبراني:** يمثل احد اوجه الصراع الدولي ويعني نوع من انواع الصراع المتقدم القائم على استخدام التكنولوجيا وومن خلاله يتمكن احد اطراف الصراع ان يوقع خسائر فادحة بالطرف الاخر ويتسبب في فشل البنية المعلوماتية والاتصالاتية الخاصة به وهو ما يسبب خسائر عسكرية واقتصادية فادحة من خلال قطع انظمة الاتصال بين الوحدات العسكرية او تضليل معلوماتها او تغيير المسار لبعض الهجمات العسكرية[(2)].

3- **الحروب السيبرانية:** هي مستوى من التسلح العسكري المتقدم والذي من شأنه ان يتفوق على الخصم بأستخدام وسائل عديدة كتقنية الاخفاء في الطائرات المقاتلة الحديثة ومنظومة الرصد الجوي (S400) ومنظومة (Thad) الامريكية وهي تكتيك يهدف الى تعطيل فاعلية منظومات الدفاع والهجوم عن طريق التشويش والاعاقة الالكترونية[(3)].

ثانياً: الفواعل في مجال القوة السيبرانية:

يعد (جوزيف ناي) من اوائل المهتمين بالشؤون الخاصة بالامن السيبراني وعرف القوة السيبرانية بأنها: (القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، اي انها القدرة على استخدام الفضاء السيبراني لايجاد مزايا للدولة،

(1) يوسف بوغرارة، الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبري، مجلة الدراسات الأفريقية وحوض النيل–المركز الديمقراطي العربي، المجلد الأول، العدد الثالث، جامعة مستغانم، الجزائر، أيلول 2018، ص103.

(2) تغريد معين حسن المشهدي،مصدر سابق، ص242.

(3) اسراء شريف جيجان، الامن السيبراني الصيني: دراسة في الواقع والتحديات، جامعة النهرين، مجلة قضايا سياسية، العدد (65)، 2022، ص37.

والتأثير على الاحداث المتعلقة بالبيئات التشغيلية الاخرى وذلك من خلال ادوات سيبرانية[1]، وحدد (جدوزيف ناي) ثلاث انواع من الفاعلين الذين يمتلكون القوة السيبرانية[2]:

1- **الدول:** تمتلك قدرة كبيرة على تنفيذ هجمات سيبرانية وأنشاء بنية تحتية وتطويرها وتكوين سلطة داخل حدودها، وتمثل الفاعل الاكثر قوة في مجال الفضاء السيبراني.

2- **الفاعلون من غير الدول:** وتضم (المنظمات الدولية، الشركات المتعددة الجنسية)، ولديهم القدرة على احداث الاختراقات الالكترونية وتعطيل انظمة الاتصال الدفاعية وتنفيذ هجمات سيبرانية، وبالرغم من عدم امتلاكهم مقومات الدول نفسها في الهجمات السيبرانية، الا انهم يشكلون خطراً كبيراً على البيئة الدولية نتيجة امتلاكهم مقومات القوة السيبرانية التي تفوق قدرة بعض الدول، الا انها تنقصها شرعية ممارسة القوة التي لا زالت حكراً على الدول، وطالما تدخل هذه الشركات في ازمات سيبرانية نتيجة تعرضها لهجمات سيبرانية ومن ثم تؤثر في اقتصاديات الدول وثقافة مجتمعاتها، ومن ابرز الامثلة على ذلك تسريبات (Wikileaks)، اذ تم نشر ملايين الوثائق السرية للادارة الامريكية وقنصلياتها، وادى ذلك الى مشاكل دبلوماسية بين الولايات الماحدة وحلفائها.

3- **الافراد:** ويمثلون الافراد الذين يمتلكون مهارات تكنولوجية عالية ولديهم القدرة على توظيفها، ومن الصعب معرفة هوياتهم أو ملاحقتهم.

ثالثاً: علاقة الامن السيبراني بالامن العالمي:

بعد ظهور "الفضاء السيبراني" تغيرت مفاهيم الامن القومي والعالمي، واصبح هناك ادوات اخرى وأليات اخرى للصراع ولعب الفضاء السيبراني دور اساسي في تعظيم القوة واضافة بعد اخر لمقومات القوة للدول، واصبح بدوره معياراً لمدى قوة الدولة وقدرتها على خوض صراع مع دول او فواعل دولية اخرى، كما اصبح الفضاء السيبراني مجالاً لحرب العصر الحقيقة من خلال استخدام الادمغة والتكنولوجيا ودخول عدة فواعل او اطراف في الصراع وينعكس ذلك على مدى توفر قدرات ومهارات وتقنيات عالية، واصبح التفوق في مجال الفضاء السيبراني يعد عنصراً حيوياً لتفوق الدولة في المجالات الاخرى في حال خوض صراع خارجي[3]،

(1) Joseph S. Nay, Cyber Power , Harvard Kennedy School, 2010, p.3.

(2) لامية طالة، التهديدات والجرائم السيبرانية (تأثيرها على الامن القومي للدول واستراتيجيات مكافحتها)، مجلة معالم للدراسات القانونية والسياسية، المجلد (4)، العدد (2)، 2022، ص60.

(3) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الامن والسلم الدوليين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، مجلد 57، 2019، ص96.

المبحث الثاني: الامن السيبراني للقوى العظمى (الولايات المتحدة الامريكية انموذجاً):

اصبح للفضاء السيبراني دور واضح وفعال ومؤثر في العلاقات الدولية في القرن الحادي والعشرين، وبالتالي اصبح التهديد السيبراني يشكل احد اهم التحديات التي تشغل كل دولة في النظام الدولي، اذ اثر الفضاء السيبراني في طبيعة وخصائص القوة، لاسيما مع تزايد فرص تعرض الدول لاخطار تهدد المصالح الاستراتيجية للدول بشكل مباشر وانعكس ذلك على العلاقات الاقتصادية والسياسية الدولية، ومع تزايد العلاقة بين الامن والتكنولوجيا وترابطهما بشكل واضح، ادى ذلك الى وجود حاجة ماسة الى اعادة صياغة مفهوم "الامن القومي للدولة"، كما ان الفضاء السيبراني اصبح ساحة عالمية عابرة لحدود الدول اي لا يتقيد بالحدود الجغرافية للدول، مما ادى ذلك الى وجود ترابط بين الامن السيبراني الداخلي للدول وبين أمن الفضاء السيبراني، وهو ما يشكل بالنتيجة الامن الجماعي العالمي، لذا نجد ان الدول الكبرى اخذت تعمل على تحديث عقيدتها الامنية، ومثال ذلك (حلف الشمال الاطلسي) الذي عمل على تحديث العقيدة الامنية نظراً للتغيرات الحاصلة في طبيعة التمخاطر والتهديدات الدولية، وكذلك ان العقيدة الروسية الجديدة تضمنت بند جديد يخص تهديدات الامن السيبراني في المجالين الاقتصادي والعسكري، كما ان كل من (الصين، واسرائيل، وبريطانيا، وفرنسا، والولايات المتحدة الامريكية، وايران، وكوريا الشمالية) طورت عقيدتها الامنية بما يتلائم مع التطورات التي طرأت على المنظومة الامنية العالمية واضافة بعد اخر يتثمل بـ(الامن السيبراني)[1].

وفي ظل الصراع الدولي القائم على عوامل الصراع التقليدية اصبح هناك عامل اخر او أداة اخرى للتنافس والصراع بين القوى العظمى والتي ترتبط بعلاقة تنافسية مثل الولايات المتحدة والصين لذا سنحاول ان نوضح مقومات القوة السيبرانية لكل منهما وكيفية تأثيرها على أمن مجتمع المعلومات العالمي.

اولاً: الاستراتيجية السيبرانية الامريكية: تعد الولايات المتحدة الامريكية من اوائل الدول التي عملت على الاهتمام بالجانب التقني والمعلوماتي وتطوير البنية التحتية للفضاء السيبراني كأحد وسائل تدعيم القوة الناعمة للدولة، وتجنباً لاي تهديدات للاقتصاد او الامن او الملكية الفكرية او التجارة او غيرها من المجالات الاخرى التي تعد معرضة لمخاطر الاختراق السيبراني، لذا بدأت الولايات المتحدة الامريكية الاهتمام بمجال الفضاء السيبراني منذ عام (1993)، وبعد احداث (11/سبتمبر/2001) اولت اهتماماً اكبر واخذت في عام (2003) بصياغة استراتيجية خاصة بالامن السيبراني عرفت **بـ(الاستراتيجية الوطنية لحماية الفضاء السيبراني)**، وفرت

(1) كريستوفر س. تشسفيس واخرون، التوصل الى اتفاق مع الصين بشأن الفضاء الالكتروني، مؤسسة راند، 2016، ص8.

هذه الاستراتيجية مظلة الحماية المعلوماتية لشبكات الحاسوب في الولايات المتحدة الامريكية، وفي عام (2006) صدرت "الاستراتيجية الامريكية لادارة الفضاء السيبراني" وفي عام (2007) وفي ظل ادارة اوباما دعت الادارة الامريكية وكالة الامن القومي للتنسيق مع وزارة الامن الداخلي لحماية الحكومة وشبكة الاتصالات المدنية من الاختراق السيبراني وتم تخصيص نحو (144) مليون دولار من ميزانية الدفاع الامريكي لضمان تحقيق اهداف خطة تعزيز الامن السيبراني للمؤسسات الحكومية[1]، وفي عام (2008) بدأت مرحلة انتقالية جديدة في تطوير نظام الامن السيبراني وتم تطوير (استعراض سياسة الفضاء السيبراني)، ومن خلال هذه الاستراتيجية تم الاعتماد على مبدأ التقييس والمبادئ التوجيهية العامة والتي بموجبها توجب على رأس المال الخاص ضمان أمنها السيبراني وتطوير الإمكانات البشرية، الا ان الهدف الاهم تمثل بتطوير التعاون في قضايا الأمن السيبراني على المستوى الدولي والذي أصبح العنصر المركزي لسياستها وضع" الاستراتيجية الدولية للفضاء السيبراني" في عام (2011)، لانشاء منصة موحدة للتفاعل الدولي بشأن قضايا الفضاء الإلكتروني لتعزيز سياسة الأمن السيبراني[2].

نجد ان الولايات المتحدة عملت على اساس مبدأ (حرية الانترنت) كأحد الادوات الناعمة للسياسة الخارجية للدولة، حاولت من خلالها احكام سيطرتها والاحتفاظ بدورها في ادارة الانترنت ومركزها العالمي في مجال الشركات التكنولوجية الكبرى الخاصة بالخدمات والتطبيقات والصناعات الالكترونية، ونتيجة توالي الهجمات السيبرانية ضد المنشأت الحيوية للولايات المتحدة الامريكية ولعل اهمها محاولة روسيا التدخل في انتخابات (2016) ودعم (ترامب) مقابل (هيلاري) نجد ان الولايات المتحدة علملت على استخدام نمطين للامن السيبراني[3]:

اولاً: النمط الاول: توظيف "القوة الناعمة" في الفضاء السيبراني بأستخدام الحرب المعلوماتية مثل شن الحرب النفسية ونشر المعلومات المضللة وتوظيف المعلومات لصالحها.

ثانياً: النمط الثاني: توظيف "القوة الصلبة" في الفضاء السيبراني من خلال شن هجمات سيبرانية وفيروسات تخريبية وتطوير استخدام الاسلحة السيبرانية ومن خلال تهديد الامن السيبراني للمنشأت الحيوية للدول.

(1) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العدد (2)، 2015، ص93.

(2) علي محمود سلمان النداوي، الفضاء السيبراني ودوره في صياغة وتوجيه مسار القوة في العلاقات الاقتصادية الدولي، (اطروحة دكتوراه)، جامعة النهرين، كلية العلوم السياسية، قسم العلاقات الدولية، 2021، ص188.

(3) عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والامريكية، المركز العربي لابحاث الفضاء الالكتروني، متوفر على الرابط الاتي: https://accronline.com/print_article.aspx?id=32528، تم الاطلاع عليه بتاريخ: 2022/9/18.

ونظراً لما سبق نجد ان وزارة الدفاع الأمريكية عملت على وضع استراتيجية الفضاء السيبراني الجديدة لعام (2018) تسمى بـــ(الاستراتيجية الإلكترونية الوطنية لعام 2018)، لتكون بديلاً عن الإستراتيجيات السابقة التي صدرت في عام (2015), هذه الاستراتيجية تحدد نهج الحكومة الأمريكية لتأمين الفضاء الإلكتروني، وتركز الاستراتيجية على حماية البنية التحتية الحيوية للولايات المتحدة، وتعزيز معايير الأمن السيبراني الدولية، وتقوية الدفاعات الإلكترونية للحكومة الأمريكية ، وتتركز رؤية هذه الإستراتيجية على كيف تخطط وزارة الدفاع الأمريكية لتنفيذ إستراتيجيات الأمن والدفاع في الفضاء السيبراني, مع الاخذ بنظر الاعتبار وجود قوى اخرى منافسة في المجال السيبراني مثل (الصين، روسيا، كوريا الشمالية، ايران) ، ونجد ان هذه الدول قد وجهت العديد من الهجمات الالكترونية للولايات المتحدة الامريكية، وبالوقت ذاته تتبع الولايات المتحدة استراتيجية السلوك الجيد في الفضاء الالكتروني لذا فهي تتجنب الرد من قبل قراصنة الولايات المتحدة الامريكية على الهجمات التي تتعرض لها من قبل قراصنة مرتبطين بهذه الدول [(1)].

كما أصدرت في مارس 2023 استراتيجية وطنية لتعزيز الأمن السيبراني وتخفيف الأنشطة السيبرانية غير المشروعة من قبل جهات فاعلة، وتدعو تلك الاستراتيجية إلى بذل جهود للدفاع عن "البنية التحتية الحيوية" للبلاد و"تعطيل وتفكيك الجهات التي تشكل تهديداً للامن السيبراني للولايات المتحدة، ووفقاً للتقرير الذي تم اعداده من قبل "المعهد الدولي للدراسات الاستراتيجية" والذي يستعرض القدرات الإلكترونية لـ 15 دولة في العالم، وتتمثل هذه الدول بـ(الولايات المتحدة والمملكة المتحدة وكندا وأستراليا وفرنسا وإسرائيل واليابان والصين وروسيا وإيران وكوريا الشمالية والهند وإندونيسيا وماليزيا وفيتنام)[(2)].

ووضع التقرير هذه الدول في ثلاث مستويات، الأول: هو للدول التي تتمتع بنقاط قوة رائدة في جميع الفئات المذكورة. وفي هذه الفئة، وضع الولايات المتحدة فقط وقال إنها "تستحق" هذا اللقب.

أما المستوى الثاني: فهو للدول التي لديها نقاط القوة في بعض الفئات، وهي بدون ترتيب، أستراليا، كندا، والصين وفرنسا وإسرائيل وروسيا والمملكة المتحدة.

(1) نافل العتيبي, ملخص الإستراتيجية الأمريكية للفضاء السيبراني, مؤسسة عسير للصحافة والنشر, صحيفة الوطن، ايلول: 2018، متوفر على الرابط الاتي: https://www.alwatan.com.sa/article/37651 تم الاطلاع عليه بتأريخ: 2023/5/29.

(2) تقرير تعزيز الامن السيبراني والحفاظ على الامن الوطني، ترينذز للبحوث والدراسات، متوفر على الرابط الاتي: ، تم الاطلاع عليه بتأريخ: https://trendsresearch.org/ar/insight/enhance-cyber-security-and-maintain-national-security/ 2023/5/29.

والمستوى الثالث: خاص بالدول التي لديها نقاط قوة في بعض الفئات ولكنها تملك نقاط ضعف كبيرة في الأخرى، وهي الهند وإندونيسيا وإيران واليابان وماليزيا وكوريا الشمالية وفيتنام.

وبالتأكيد تمتع الولايات بـ"النفوذ الجيوسياسي لأنها موطن للعديد من الشركات المهيمنة"، لكن الدولة الوحيدة التي تنافس هذا الوضع هي الصين، التي ينمو سوقها من تكنولوجيا المعلومات والاتصالات بشكل ملحوظ، كما تتمتع الولايات المتحدة الامريكية بقدرة "متانة التفوق الرقمي الصناعي الأميركي" الذي يقوم على عوامل منها التحالفات الدولية، على مدى السنوات العشر القادمة على الأقل، لذا تعد الولايات المتحدة الدولة الرائدة الاولى في مجال الامن السيبراني[1].

كما تتمتع الولايات المتحدة الامريكية بتقنيات سيبرانية متقدمة وتعمل على استغلالها للأغراض الاقتصادية والقوة العسكرية ما جعل الولايات المتحدة متقدمة على الصين، وأن اتفاق الولايات المتحدة ودول غربية أخرى على تقييد وصول الصين إلى بعض التقنيات الغربية هو ما عطل قدرتها على تطوير التكنولوجيا المتقدمة الخاصة بها.

ثانياً: الاستراتيجية السيبرانية الصينية:

تعد الصين من اهم واخطر الدول في مجال الفضا السيبراني وتأتي بعد الولايات المتحدة الامريكية، ومن اكبر الدول في عدد مستخدمي الانترنت في العالم، وتعمل الصين في هذا المجال من خلال مفهوم (الانترنت السيادي) اي فرض سيطرة مطلقة من جانب الدولة على شبكة الانترنت والتحكم ومراقبة تبادل المعلومات وذلك من خلال وجود (مشروع جدار الحماية العظيم) الذي بدأت بتنفيذه عام (1998) وانجزت مراحله كافة عام (2008)، ومهام هذا المشروع تتمثل بحجب المحتوى ومراقبة الفيديو والتعرف على الوجوه، وفي عام (2013) تم تشكيل مجموعة القيادة المركزية لامن المعلومات وبأشراف مباشر من الرئيس الصيني (شي جين بينغ)[2]، وبدأ هدف الصين الاساس بالتحول الى قوة سيبرانية عظمى، ان عبارة (القوة السيبرانية العظمى) تشكل مفهوما رئيسياً يوجه الاستراتيجية الصينية في مجال الاتصالات السلكية واللاسلكية وتكنولوجيا المعلومات على نطاق واسع تعاني الصين من الهجمات السيبرانية المتكررة، اذ ان (80%) من المواقع الحكومية الصينية تتعرض لهجمات سيبرانية تأتي معظمها من الولايات المتحدة الامريكية.

(1) علي محمود سلمان النداوي، الفضاء السيبراني ودوره في صياغة وتوجيه مسار القوة في العلاقات الاقتصادية الدولي، مصدر سابق، ص190.
(2) اسراء شريف جيجان، الامن السيبراني الصيني:دراسة في الواقع،مجلة قضايا سياسية، جامعة النهرين ، كلية العلوم السياسية، العدد (65)، 2021، ص41.

ومن وجهة نظر الحكومة الصينية أن البرمجيات المصنعة من قبل الشركات الغربية تشكل تهديداً للأمن القومي, لذا نجد ان الصين عملت على ابتكار وتنظيم برمجيات خاصة بها، فسياسة الأمن السيبراني الصينية بشكل عام, لديها القدرة على تغيير السوق العالمية من ناحية المنتجات وخدمات تكنولوجيا المعلومات, لذا, تتخذ الحكومة الصينية خطوات ملموسة لتعزيز الأمن السيبراني, ففي عام (2014)، أسست "المجموعة القيادية لأمن الفضاء الإلكتروني والمعلوماتية"[1].

وتعد السياسية الخارجية للصين في مجال الامن السيبراني كأنعكاس لسياستها الداخلية التي تتمثل بحماية واستمرار قوة الحزب الشيوعي الصيني، لذا فأن ضمان استقرار الصين داخياً وخارجياً واستمرار تحقيق النمو الاقتصادي والتأثير بالمنظومة الدولية والتهيؤ لاحتمال نشوب نزاع سيبراني عسكري كلها اهداف تدعم استمرار حكم الحزب الشيوعي الصيني، وهناك العديد من المحفزات الاقتصادية والسياسية والعسكرية التي تدعم التفوق الصيني في مجال الفضاء السيبراني[2].

ومن ناحية أخرى، نلاحظ محاولة الصين التي تدرك تفوق الولايات المتحدة السيبراني، القيام بأنشطة دبلوماسية لتأكيد نفوذها في مجال الفضاء الإلكتروني، من خلال حصول مسؤول صيني على منصب أمين عام الاتحاد الدولي للاتصالات، والقيام بمبادرات الحزام والطريق الرقمية وإنشاء شركات اتصالات كبيرة تتمتع بنفوذ عالمي، **ومن المحتمل ان تتمتع** الصين بمكانة اكثر تأثيراً في مجال الامن السيبراني العالمي من خلال سياستها التجارية والاستثمارية ومبادرتها العالمية (الحزام والطريق) والتي تم طرحها عام (2013)[3]، والتي تتضمن (طريق حرير رقمي)، يتمثل بمشروعات سلكية ولاسلكية وكاميرات مراقبة وكوابل بحرية واقمار صناعية، وتم اضافة (طريق الحرير الرقمي) الى مبادرة الحزام والطريق في عام (2015)، وذلك انعكاساً لرغبة الصين لتكون قوة تكنولوجة عظمى، وبعد اطلاق طريق الحرير الرقمي عملت الصين على اطلاق برنامج

(1) V.T. Tsakanyan, The Role Of Cyber security In World Politics, Peoples' Friendship University of Russia (RUDN University), Moscow, Russia. 339-340. http://journals.rudn.ru/international_relations

(2) Ronald Deibert, Canadian International Council, China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy, China Papers No. 7, February 2010, P. 5.

(3) تشاو لي، مبادرة الحزام والطريق الصينية من منظور الاقتصاد الثقافي العالمي، ترجمة: محمد بيج -شيه يانغ، منشورات ضفاف، ط1، بيروت، 2018، ص20.

(تحالف بيانات الارض الكبيرة للحزام والطريق) محاولة بذلك الاستغناء عن النظام الامريكي (GPS)، وقررت تسميته (بيدو) (Beiduo) وتتم ادارته من قبل وزارة الدفاع الصينية[1].

ووفقاً لـ(غريج أوستن) خبير الأمن السيبراني لواشنطن بوست" :لقد أحرزت الصين تقدما كبيرا في تعزيز قدراتها منذ عام 2014، ولكن لم تكن قريبة بما يكفي لسد الفجوة مع الولايات المتحدة، ونجد ان السبب الرئيسي هو المكانة النسبية للاقتصادات الرقمية للبلدين، حيث تظل الولايات المتحدة متقدمة جداً على الرغم من التقدم الرقمي الصيني[2].

ويوضح تقييم التهديد السنوي لعام 2023 لمكتب مدير الاستخبارات الوطنية التهديد السيبراني الذي تشكله جمهورية الصين الشعبية (PRC): "ربما تمثل الصين حالياً التهديد الأوسع والأكثر نشاطاً واستمراراً للتجسس السيبراني للحكومة الأمريكية والقطاع الخاص، تزيد مساعي الصين السيبرانية وتصدير صناعتها للتقنيات ذات الصلة من تهديدات العمليات السيبرانية العدوانية ضد الولايات المتحدة. . . يكاد يكون من المؤكد أن الصين قادرة على شن هجمات إلكترونية يمكن أن تعطل خدمات البنية التحتية الحيوية داخل الولايات المتحدة ، بما في ذلك ضد خطوط أنابيب النفط والغاز وأنظمة السكك الحديدية وغيرها، فالصين اليوم تسابق الزمن لتطويع الذكاء الاصطناعي للاغراض العسكريةبما في ذلك حشود الدرونز الاوتوماتيكية وبرنامج يمكنه الدفاع عن نفسه ضد الهجمات السيبرانية، وبرنامج ينقب وسائل التواصل الاجتماعي بغرض رصد اي تحركات سياسية محتملة وذلك من خلال وضع خطط واستراتيجيات لتتحول الصين الى (مركز عالمي اساسي لابتكارات الذكاء الاصطناعي) بحلول عام (2030)[3].

نجد ان كلل من الولايات المتحدة والصين في تنافس مستمر في مجالات متعددة ومن ضمنها الفضاء السيبراني وتحاول الاخيرة وضع استراتجيات امنية سيبرانية لتتفقوق على الولايات المتحدة الامريكية رغم اختلاف الرؤى تجاه الامن السيبراني لكل منهما، وسنوضح فيما يلي اختلاف الرؤى الخاص بكل من الولايات المتحدة والصين.

(1) محمد الساعدي، الابعاد السياسية لطريق الحرير الرقمي، مركز النهرين للدراسات الاستراتيجية، متوفر على الرابط الاتي: https://www.alnahrain.iq/post/743، تم الاطلاع عليه بتأريخ: (2023/6/1).

(2) China Cyber Threat Overview and Advisories, Americas Cyber Defense Agency, Available on: **https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.**

([3]) Rohan Goswami, Aggressive' China cyberattacks are the 'defining threat' of our time, top U.S. cyber official says, Available on: https://www.cnbc.com/2023/06/13/china-cyberattacks-are-a-defining-threat-top-us-cyber-official.html .

شكل (1) اختلاف الرؤى حول الفضاء السيبراني

اختلاف الرؤى حول الفضاء السيبراني		
البلد	الولايات المتحدة الامريكية	الصين
الفضاء السيبراني	فوضوي	فضاء سيادي
التنظيم	دور مركزي للقطاع الخاص و لاحاجة لتدخل الحكومات	دور مركزي للدولة وضرورة التدخل الحكومي
حوكمة الانترنت	مشاركة كافة اصحاب المصلحة (حكومات، قطاع خاص، اكاديمي،مجتمع مدني)	دور اساسي للدول ووضع قواعد ومنظمات جديدة للتعامل مع الظاهرة المستحدثة

المصدر: عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والامريكية، المركز العربي للفضاء الالكتروني، متوفر على الرابط الاتي: https://accronline.com/article_detail.aspx?id=32528 ، تم الاطلاع عليه بتأريخ 2023/6/1.

الخاتمة:

في القرن الحادي والعشرين تغير مفهوم الامن العالمي وطرأ عليه العديد من التغييرات واصبح يشمل ابعاد عدة ومن اهمها الامن السيبراني، اذ انتشرت القوة بين الفاعلين لا سيما القوى العظمى والفاعلة في هذ المجال وانتقل الصراع من مادي الى افتراضي، وبدأت الدول تتجه نحو عسكرة الفضاء السيبراني، فكلما زاد التحدي، زادت التهديدات السيبرانية واثر ذلك على الامن القومي للدول وعلى الامن العالمي للمنظومة الدولية، اذ في عالم اليوم نلاحظ ان الامن السيبراني اصبح على رأس اوليات قضايا الامن القومي للدول، وتوجه الدول الى وضع استراتيجيات ومبادرات عالمي في مجال الامن السيبراني بل وتشريع القوانين المختصة بهذا المجال، وعقد اتفاقيات للتعاون في الامن السيبراني، اذ كلفت الجرائم الالكترونية الاقتصاد العالمي مايزيد عن (6) تريليونات دولار لعام (2021) ومن المتوقع ان تصل كلفة هذه الجرائم والهجمات السيبرانية الى (10.5) تريليون دولار عام (2050)، ومما سبق يتوصل البحث الى النتائج الاتية:

1- ان الامن السيبراني اصبح البعد الخامس لابعاد الامن القومي للدول.

2- اصبح الفضاء السيبراني المجال الاكثر اهتماماً من قبل القوى الكبرى (الولايات المتحدة الامريكية، الصين).

3- تعمل الصين على وضع الخطط والاستراتيجيات العالمية الخاصة بتفوقها في مجال الفضاء السيبراني.

4- يعد الفضاء السيبراني مجال لتسوية الصراعات بين القوى الكبرى وادارة صراعاتها البينية بالرغم من صعوبة تهديد هوية المهاجمين عبر الفضاء السيبراني.

5- ان التنافس بين القوى الكبرى اصبح يشمل جانب اخرى ويتمثل بجانب (الامن السيبراني) بأعتباره جزء من منظومة الامن العالمي، ولعل اصبح يتسقطب الاهتمام الاكبر من هذه القوى الكبرى.

المصادر:

اولاً: المصادر العربية:

1- اسراء شريف جيجان، الامن السيبراني الصيني: دراسة في الواقع والتحديات، جامعة النهرين، مجلة قضايا سياسية، العدد (65)، 2022.

2- اسراء شريف جيجان، الامن السيبراني الصيني:دراسة في الواقع،مجلة قضايا سياسية، جامعة النهرين ، كلية العلوم السياسية، العدد (65)، 2021.

3- تشاو لي، مبادرة الحزام والطريق الصينية من منظور الاقتصاد الثقافي العالمي، ترجمة: محمد بيج - شيه يانغ، منشورات ضفاف، ط1، بيروت، 2018.

4- تغريد معين حسن المشهدي، الاثر العسكري للامن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، جامعة الكوفة، كلية الاداب، المجلد الثاني، العدد (30)، 2019.

5- سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العدد (2)، 2015.

6- علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الامن والسلم الدوليين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، مجلد 57، 2019.

7- علي محمود سلمان النداوي، الفضاء السيبراني ودوره في صياغة وتوجيه مسار القوة في العلاقات الاقتصادية الدولي، (اطروحة دكتوراه)، جامعة النهرين، كلية العلوم السياسية، قسم العلاقات الدولية، 2021.

8- كريستوفر س. تشسفيس واخرون، التوصل الى اتفاق مع الصين بشأن الفضاء الالكتروني، مؤسسة راند، 2016.

9- لامية طالة، التهديدات والجرائم السيبرانية (تأثيرها على الامن القومي للدول واستراتيجيات مكافحتها)، مجلة معالم للدراسات القانونية والسياسية، المجلد (4)، العدد (2)، 2022.

10- محمود محارب، اسرائيل والحرب الالكترونية، الدوحة، المركز العربي للابحاث ودراسة السياسات، 2011.

11- نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الانسانية، مجلد(8)، العدد (2) جامعة بابل، بابل، 2018.

12- يوسف بوغرارة، الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبري، مجلة الدراسات الأفريقية وحوض النيل–المركز الديمقراطي العربي، المجلد الأول، العدد الثالث، جامعة مستغانم، الجزائر، أيلول 2018.

Financial support and sponsorship: Nil

Conflict of Interest: None

ثانياً: المصادر الانكليزية:

1- China Cyber Threat Overview and Advisories, Americas Cyber Defense Agency, Available on: https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.
2- Joseph S.Nye JR, Cyber Power, Harvard Kennedy School, 2010, P.30.
3- Rohan Goswami, Aggressive' China cyberattacks are the 'defining threat' of our time, top U.S. cyber official says, Available on: https://www.cnbc.com/2023/06/13/china-cyberattacks-are-a-defining-threat-top-us-cyber-official.html
4- Ronald Deibert, Canadian International Council, China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy, China Papers No. 7, February 2010, P. 5.
5- V.T. Tsakanyan, The Role Of Cyber security In World Politics, Peoples' Friendship University of Russia (RUDN University), Moscow, Russia. 339-340. http://journals.rudn.ru/international_relations

ثالثاً: الانترنت:

1- تقرير تعزيز الامن السيبراني والحفاظ على الامن الوطني، ترينذز للبحوث والدراسات، متوفر على الرابط الاتي: ، تم الاطلاع عليه بتأريخ: https://trendsresearch.org/ar/insight/enhance-cyber-security-and-maintain-national-security/ 2023/5/29.

2- عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والامريكية، المركز العربي لابحاث الفضاء الالكتروني، متوفر على الرابط الاتي: https://accronline.com/print_article.aspx?id=32528، تم الاطلاع عليه بتاريخ: 2022/9/18.

3- عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والامريكية، المركز العربي للفضاء الالكتروني، متوفر على الرابط الاتي:

https://accronline.com/article_detail.aspx?id=32528 ، تم الاطلاع عليه بتأريخ 2023/6/1.

4- محمد الساعدي، الابعاد السياسية لطريق الحرير الرقمي، مركز النهرين للدراسات الاستراتيجية، متوفر على الرابط الاتي: https://www.alnahrain.iq/post/743، تم الاطلاع عليه بتأريخ: (2023/6/1).

5- نافل العتيبي, ملخص الإستراتيجية الأمريكية للفضاء السيبراني, مؤسسة عسير للصحافة والنشر, صحيفة الوطن، ايلول: 2018، متوفر على الرابط الاتي: https://www.alwatan.com.sa/article/37651 تم الاطلاع عليه بتأريخ: 2023/5/29.