Tikrit Journal For Political Sciences

: https://doi.org/10.25130/tjfps.v2i32.195

TJFPS

ISSUE 32

IRAQI Academic Scientific Journals

العراقية المجلات الاكاديمية العلمية

ISSN: 2663-9203 (Electronic)
ISSN: 2312-6639 (print)

Contents lists available at:
http://tjfps.tu.edu.iq/index.php/poiltic

Tikrit Journal For Political Science

Tikrit Journal For Political Science
SINCE 2014

التهديدات السيبرانية وانعكاسها على الامن القومي الامريكي

"Cyber Threats and Their Impact on the U.S. National Security"

Lect.Jasim Muhammed Taha [a]
University of Al Mosul/ College of Political Science [a]

م. جاسم محمد طه [a] *
جامعة الموصل/ كلية العلوم السياسية [a]

Article info.

Article history:
- Received: April 22, 2023
- Accepted: 12 May . 2023
- Available online: June 30, 2023

Keywords:
- Cyber Threats
- Cyberspace
- Cyber Force

US National Security

Abstract: The cyberspace has been turned into a new arena for the international struggle between the major powers in order to impose hegemony and influence on cyberspace, and these developments imposed a rethinking of the structure and the concept of national security of the state. As a result, the issue of cyberspace security became part of the national security strategies of many developed countries in order to prevent the exposure of their vital infrastructure to cyber threats and risks, and the United States is one of the first global powers to realize the importance of the impact of cyberspace on the global balance of power, as it considered it an essential element of the comprehensive forces of the state. Therefore, the United States focused on technological and information superiority in cyberspace in order to increase its strategic capabilities and deprive opponents of it within its national strategy for the twenty-first century. Since the cyberspace is one of the sources of threats facing the United States of America, it is necessary to develop several strategies to deal with threats and risks poses by cyberspace that threaten US national security.

*Corresponding Author: Jasim Muhammed Taha, E-Mail: jasim1967b@uomosul.edu.iq
Tel: +964774871105 , Affiliation: University of Al Mosul/ College of Political Science

معلومات البحث :

تواريخ البحث:
- الاستلام : 22/ نيسان /2023
- القبول : 12/ أيار /2023
- النشر المباشر: 30/ حزيران /2023

الكلمات المفتاحية :
- التهديدات السيبرانية
- الفضاء السيبراني
- القوة السيبرانية
- الامن القومي الامريكي

الخلاصة : تحول الفضاء السيبراني الى ساحة جديدة للصراع الدولي بين القوى الكبرى من اجل فرض الهيمنة والنفوذ على الفضاء السيبراني ، وفرضت تلك التطورات اعادة التفكير في بنية ومفهوم الأمن القومي للدولة، وأصبحت مسألة أمن الفضاء السيبراني تدخل في استراتيجيات الأمن القومي للعديد من الدول المتقدمة من أجل منع تعرض بنيتها التحتية الحيوية للتهديدات والمخاطر السيبرانية، وتعد الولايات المتحدة الامريكية من أوائل القوى العالمية التي ادركت اهمية تأثير الفضاء السيبراني في توازنات القوى العالمية، اذ اعتبرته عنصرا أساسياً من عناصر القوى الشاملة للدولة، ومن هنا ركزت على التفوق التكنلوجي والمعلوماتي في الفضاء السيبراني من اجل زيادة قدراتها الاستراتيجية وحرمان الخصوم منه ضمن استراتيجيتها القومية للقرن الحادي والعشرين، ولما كان الفضاء السيبراني أحد مصادر التهديدات التي تواجه الولايات المتحدة الأمريكية، كان لابد من ضرورة وضع عدة استراتيجيات للتعامل مع التهديدات والمخاطر التي يطرحها والتي تعمل على تهديد الأمن القومي الأمريكي.

المقدمة:

مما لا ريب فيه ان تزايد العلاقة بين مفهومي التكنلوجيا والأمن القومي أفضى الى زيادة التهديدات والمخاطر على المصالح الاستراتيجية للدول من خلال مخاطر الفضاء السيبراني، ومن ثم تحول الفضاء السيبراني الى ساحة جديدة للصراع الدولي بين القوى الكبرى من اجل فرض الهيمنة والنفوذ على الفضاء السيبراني، وفرضت تلك التطورات اعادة التفكير في بنية و مفهوم الامن القومي للدولة، والذي يعنى بحماية قيم المجتمع الاساسية وابعاد مصادر التهديد عنها، وأصبحت مسألة أمن الفضاء السيبراني تدخل في استراتيجيات الأمن القومي للعديد من الدول المتقدمة من أجل منع تعرض بنيتها التحتية الحيوية للخطر.

وتعد الولايات المتحدة الامريكية من أوائل القوى العالمية التي ادركت اهمية تأثير الفضاء السيبراني في توازنات القوى العالمية، اذ اعتبرته عنصرا أساسياً من عناصر القوى الشاملة للدولة، ومن هنا ركزت على التفوق التكنلوجي والمعلوماتي في الفضاء السيبراني من اجل زيادة قدراتها الاستراتيجية وحرمان الخصوم

منه ضمن استراتيجيتها القومية للقرن الحادي والعشرين ، واتسع الهدف الامريكي ليشمل مجمل الامكانات والقدرات السيبرانية في مجال المعلومات والاتصالات مع تزايد التنافس العالمي على فرض الهيمنة والنفوذ في الفضاء السيبراني، فضلاً عن صعود مفهوم القوة الذكية الذي عبر عن التلاقي بين القوتين الصلبة والناعمة بهدف تحقيق اهداف السياسة الامريكية ، وحماية امنها القومي.

ولما كان الفضاء السيبراني أحد مصادر التهديدات التي تواجه الولايات المتحدة الامريكية، كان لابد من ضرورة وضع عدة استراتيجيات للتعامل مع التهديدات و المخاطر التي يطرحها والتي تعمل على تهديد الامن القومي الامريكي، اذ تكمن خطورة الفضاء السيبراني في اعتماد الولايات المتحدة عليه بشكل كبير جداً من خلال ربط بنيتها التحتية بهذا الفضاء ، سيما في محطات الطاقة، والقطاع التجاري و المالي، و أنظمة النقل والمواصلات، وأنظمة الاتصالات والدفاع وهو الامر الذي يعني ان تهديد احدى هذه القطاعات أو النظم هو تهديد للأمن القومي الامريكي..

اولاً: اهمية الدراسة: تنبع اهمية الدراسة من كونها تهتم بدراسة موضوع استراتيجي يدخل ضمن موضوعات الدراسات الاستراتيجية والامنية للولايات المتحدة الامريكية ، كما تأتي اهمية الدراسة من تزايد تأثير التهديدات والمخاطر السيبرانية على الامن القومي الامريكي، اذ تكمن خطورة الفضاء السيبراني في اعتماد الولايات المتحدة الامريكية عليه بشكل متزايد في مختلف القطاعات سيما في انظمة النقل والمواصلات، والمؤسسات المالية والتجارية، وانظمة الدفاع والقيادة والسيطرة، والبنية التحتية الاستراتيجية، ومن ثم فان اي تهديد لأحد هذه النظم والقطاعات هو بمثابة تهديد للأمن القومي الامريكي، ومن هنا انبثقت اهمية الدراسة.

ثانياً: أهداف الدراسة : تسعى الدراسة الى تحقيق مجموعة من الأهداف لعل أهمها الاتي:

1- التعرف على تداعيات التهديدات السيبرانية على الأمن القومي الأمريكي.

2- التعرف على المفاهيم الجديدة في الفضاء السيبراني والمفاهيم المرتبطة بها(القوة السيبرانية ، الحرب السيبرانية، الامن السيبراني، الارهاب السيبراني)

3- التعرف على طبيعة المصالح والمخاطر السيبرانية التي تؤثر على الامن القومي الامريكي.

4- التعرف على الاستراتيجيات الوطنية السيبرانية الامريكية التي اعتمدتها الولايات المتحدة الامريكية لمواجهة التهديدات السيبرانية.

ثالثاً: مشكلة الدراسة وتساؤلاتها الرئيسة: للولايات المتحدة الامريكية مصالح وأهداف استراتيجية في الفضاء السيبراني على مختلف المستويات الاقتصادية والسياسية والامنية والعسكرية، مما افضى الى تعرضها للعديد من الهجمات السيبرانية في مختلف القطاعات الاستراتيجية ، ومن ثم اصبح الفضاء السيبراني أحد مصادر التهديدات الخطيرة التي تواجه الأمن القومي الامريكي، الأمر الذي تطلب صياغة عدة خطط واستراتيجيات لمواجهة هذه التهديدات والمخاطر السيبرانية . ومن هنا انبثقت المشكلة البحثية والتي يمكن صياغتها بالتساؤل البحثي الرئيس الاتي: ما طبيعة التهديدات السيبرانية وما أثرها على الامن القومي الامريكي؟

ومن هذا التساؤل الرئيس انبثقت عدة تساؤلات فرعية لعل اهمها الاتي:

1- ما المقصود بمفهومي التهديدات السيبرانية والفضاء السيبراني؟

2- ما سمات الفضاء السيبراني، وما طبيعة المفاهيم الجديدة المرتبطة ببيئة الفضاء السيبراني (القوة السيبرانية، الصراع السيبراني، الأمن السيبراني، الردع السيبراني، الارهاب السيبراني) ؟

3- ماهي مصالح الولايات المتحدة في الفضاء السيبراني، وماهي أبرز مصادر التهديدات الاقتصادية والعسكرية لتلك المصالح؟

4- ماهي ملامح استراتيجية الفضاء الوطنية الامريكية في عهد الرؤساء (اوباما، ترامب، جون بايدن)؟ وهل تغيرت الاستراتيجية السيبرانية بتغير الإدارات الأمريكية المتعاقبة؟

5- ما مستقبل الصراع ومحاولات الهيمنة السيبرانية الامريكية في الفضاء السيبراني؟

رابعا: فرضيات الدراسة: تستند الدراسة على اختبار صحة الفرضيات الأتية:

الفرضية الاولى: هناك علاقة طردية موجبة بين زيادة الاعتماد من قبل الولايات المتحدة الامريكية على الفضاء السيبراني وبين زيادة حجم التهديدات والمخاطر للأمن القومي الامريكي، اذ تعتمد الولايات المتحدة الامريكية بدرجة كبيرة على الفضاء السيبراني ومن ثم اصبحت اكثر عرضة للتهديدات السيبرانية، ولعل من أخطر تلك التهديدات ما يتعلق بسرقة معلومات اقتصادية وعسكرية وسياسية وسرقة براءات الاختراع والتكنلوجيا المتطورة والتلاعب بالبيانات المالية والاقتصادية.

الفرضية الثانية: كما تستند الدراسة على فرضية مفادها: ان امتلاك القدرات السيبرانية لم تعد تقتصر او تبقى حكراً على فاعل محدد، بل اصبح بمقدور الدول الصغيرة والمتوسطة والفاعلين من غير الدول مهما تواضعت امكانياتهم الاستفادة القصوى من القدرات السيبرانية ، بسبب انخفاض كلفتها المادية ، ومن ثم

اصبح بإمكان الافراد والجماعات حيازة نفوذ سيبراني في الفضاء السيبراني ، الامر الذي جعل هذا الفضاء مجالاً للصراعات المختلفة لكل الفاعلين من الدول وغير الدول من اجل تحقيق مكاسب استراتيجية وحيازة اكبر قدر من التأثير والنفوذ السيبراني.

خامساً: الإطار الزماني والمكاني:

يبدأ الاطار الزماني للدراسة منذ عام 2001 ولغاية الانتهاء من الدراسة عام 2023، ويعود السبب بالانطلاق من عام 2001 ، لأنه بدأ التركيز على الفضاء السيبراني بعده تهديد امني جديد للأمن القومي للدول بفعل احداث دولية لعل من ابرزها استخدام تنظيم القاعدة الارهابي لهذا الفضاء بمثابة ساحة قتال ضد الولايات المتحدة بعد احداث ايلول 2001، كما برز دور الفضاء السيبراني في عام 2007 كمجال جديد في العمليات القتالية بين استونيا وروسيا ، ثم الحرب بين روسيا وجورجيا ،فضلا عن احداث اخرى كثيرة وقعت في هذه الفترة تم توظيف الفضاء السيبراني كساحة قتال ، كما شهدت مدة الدراسة صياغة العديد من الاستراتيجيات الوطنية السيبرانية الامريكية المهمة لمواجهة التهديدات والمخاطر السيبرانية على الامن القومي الأمريكي في عهد الإدارات الأمريكية المتعاقبة على الحكم سيما (فترة ادارة الرؤساء اوباما – ترامب – جون بايدن).

اما فيما يتعلق بالاطار المكاني للدراسة فانه يشمل كل التفاعلات التنافسية والتعاونية والصراعية التي تجري في الفضاء السيبراني من قبل الولايات المتحدة الامريكية والقوى الاخرى المنافسة لها سيما روسيا والصين فضلا عن الفاعلين من غير الدول، سيما ان امتلاك القدرات السيبرانية لم يعد حكراً على فاعلاً بعينه، اذ اصبح بمقدور الدول الصغيرة والمتوسطة والفاعلين من غير الدول الاستفادة من القدرات السيبرانية من اجل بسط النفوذ وتحقيق مأرب ومكاسب استراتيجية وسياسية ومالية وتهديد مصالح الولايات المتحدة في الفضاء السيبراني، وسوف يتم التركيز في هذه الدراسة على التهديدات السيبرانية ذات البعد الاقتصادي والعسكري التي تتعرض لها الولايات المتحدة الامريكية.

سادساً: منهجية الدراسة: من اجل الاجابة على التساؤلات التي تبنتها الدراسة تم الاعتماد على المنهج التحليلي والوصفي من اجل تحليل التهديدات والمخاطر السيبرانية ورصد وتحليل تداعياتها على الامن القومي الامريكي ومناقشة ملامح الاستراتيجية الوطنية السيبرانية الامريكية خلال الادارات المتعاقبة على الحكم سيما ادارة الرئيس اوباما والرئيس ترامب ثم ادارة الرئيس الحالي جون بايدن.

سابعاً: التقسيم المقترح للدراسة: بناء على تحديد اهمية الدراسة وتساؤلاتها الرئيسة وفرضياتها، فقد توزعت الدراسة الى ثلاثة مباحث ومقدمة وخاتمة، تضمن المبحث الاول تأصيل مفاهيمي لمصطلح التهديدات السيبرانية والفضاء السيبراني من خلال مطلبين، تضمن الاول التهديد السيبراني والفضاء السيبراني ، بينما تناول المطلب الثاني المفاهيم الجديدة في بيئة الفضاء السيبراني والمفاهيم المرتبطة بها، بينما تناول المبحث الثاني طبيعة التهديدات والمخاطر السيبرانية وتداعياتها على الامن القومي الامريكي من خلال مطلبين، ناقش المطلب الاول التهديدات الاقتصادية السيبرانية التي تواجه الولايات المتحدة الامريكية في الفضاء السيبراني، بينما ناقش المطلب الثاني التهديدات العسكرية السيبرانية التي تواجه الولايات المتحدة الامريكية في الفضاء السيبراني، بينما ناقش المبحث الثالث استراتيجيات الولايات المتحدة للأمن السيبراني خلال الادارات المتعاقبة على الحكم، من خلال ثلاثة مطالب، حلل المطلب الاول ملامح استراتيجية الفضاء الوطنية الامريكية في عهد باراك اوباما، وناقش المطلب الثاني استراتيجية الفضاء الوطنية السيبرانية في عهد الرئيس ترامب، بينما حلل المطلب الثالث الاستراتيجية الوطنية السيبرانية في عهد الرئيس جون بايدن.

المبحث الأول: تأصيل مفاهيمي لمصطلح التهديدات السيبرانية والفضاء السيبراني

ان البحث في قضايا التحديات الامنية و التهديدات السيبرانية يقتضي توصيف بيئة هذه التحديات، ومعرفة مفهوم الفضاء السيبراني والمفاهيم المرتبطة به (الامن السيبراني، القوة السيبرانية ، الصراع السيبراني) في بيئة سيبرانية تتداخل فيها الحسابات الانسانية والتكنلوجية وتتشابك فيها طبيعة، واهداف، وهويات الاطراف من الدول وغير الدول كالأفراد والشركات، وجماعات القرصنة وغيرها من الفواعل، ومن ثم فان اي محاولة بحثية لفهم طبيعة التهديدات والمخاطر في الفضاء السيبراني تستلزم مساراً ونمطاً من المقاربات العابرة للتخصصات الانسانية والتقنية بسبب التمازج بين اهداف البيئتين الافتراضية والواقعية، لذا برزت الحاجة الى مداخل ورؤى نظرية اكثر قدرة على تفسير طبيعة التغيرات والتهديدات التي الحقتها الحقائق التكنلوجية بهذه المفاهيم، و من هنا تسعى الدراسة في هذا المبحث الى التعرف على مفهوم التهديدات السيبرانية ومناقشة ظاهرة الفضاء السيبراني من حيث ماهيته ، وسماته، ومعرفة طبيعة علاقته بالمفاهيم الاخرى المرتبطة بالفضاء السيبراني .

المطلب الاول : مفهوم التهديد السيبراني و الفضاء السيبراني

تبلورت مصالح قومية للدول في الفضاء السيبراني بسبب تزايد الاعتماد على ربط البنى التحتية لها بالفضاء السيبراني من خلال بيئة عمل سيبرانية تشابكية واحدة، تعرف ب (البنية التحتية القومية للمعلومات، مثل قطاعات النفط والطاقة والنقل والاتصالات، فضلاً عن الخدمات الحكومية والمالية والتجارة الإلكترونية، وغيرها من المصالح الاستراتيجية الاخرى في بيئة الفضاء السيبراني، ومن ثم اصبح اي تهديد أو هجوم على هذه المصالح الاستراتيجية للدولة قد يفضي الى حدوث عدم توازن استراتيجي ، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول، ومما عزز على تنامي التهديدات السيبرانية لمصالح الدول وبروز حروب سيبرانية هو قلة تكاليف الحروب السيبرانية مقارنة بنظيراتها التقليدية ، فضلاً عن تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية لصالح القطاع الخاص[1]، تسعى الدراسة في هذا المطلب الى محاولة التأصيل النظري لمفهوم حديث نسبياً وهو مفهوم التهديد السيبراني وكيفية استخدامه في مجال العلاقات الدولية وفق ادبيات العلوم السياسية.

[1] – عادل عبد الصادق، انماط الحرب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، مصدر سبق ذكره، ص31–32.

اولاً: مفهوم التهديد السيبراني:

يعرف التهديد على انه اعلان للتعبير عن نية التدخل أو الايذاء أو معاقبة الطرف الاخر، وبموجب هذا التعريف فان التهديد الصريح والضمني للدولة يعد من التهديدات الامنية، وهناك من يعرف التهديد على انه النية لإلحاق الضرر بالطرف الاخر أو القيام بعمل عدائي ضده.[1]

اما التهديد السيبراني يعرف بانه مجموعة المخاطر التي تواجه المستخدمين سواء كانوا فواعل من الدول او من غير الدول على الانترنيت، وتهدف هذه الفواعل الى الحاق الاذى والتدمير والتخريب على الهدف الذي تم استهدافه[2]، كما يعرف بانه أي ممارسة عدوانية توظف فيها الحواسب او عناصر نظمها السيبرانية والبنية التحتية لنسيجها الشبكاتي، من اجل أحداث ضرر أو تخريب في نظم وحواسب الخصم على مستوى المكونات والموارد السيبرانية أو الأداء، اذ اضحت الهجمات السيبرانية جزءاً لا يتجزأ من استراتيجية المواجهة بين المتخاصمين في الفضاء السيبراني والذي فرض حضوره قبالة مجالات المواجهة البرية والبحرية والجوية على حد سواء[3]، ومن ثم اصبح الصراع على النفوذ في البيئة السيبرانية مصدراً لظهور تهديدات امنية جديدة لا تقل في خطورتها عن التهديدات الامنية التقليدية، ولعل من ابرز انواع الاسلحة السيبرانية واكثرها استخداماً على الساحة الدولية هو سلاح الحرمان من الخدمة القادرة على شل حركة الانظمة الالكترونية وتعطيل مصالح الدول والافراد والشركات والمصارف المالية وغيرها من الشركات[4].

وفي هذا السياق يتزايد معدل التهديدات والمخاطر وفرص الحروب السيبرانية مع توظيف القدرات السيبرانية في تحقيق المصالح الاستراتيجية، و مع اتساع نطاق مخاطر الصراعات السيبرانية ، ومع زيادة

---

[1] – فوزي حسن الزبيدي، منهجية تقييم مخاطر الامن القومي، مجلة رؤى استراتيجية، مركز المنظار للتدريب والدراسات الاستراتيجية، دبي، يوليو 2015، ص 19.

[2] –مخاطر الامن السيبراني، شركة سايبر للأمن السيبراني، على الرابط: https://cyberone.co/%D8%A7%D84%9

[3] – حسن مظفر الرزو، التهديد السيبراني الايراني، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية ، برلين ، ط1، 2020، ص 242.

[4] – نوران شفيق، اشكال التهديدات الالكترونية ومصادرها، المركز الاوربي لدراسات مكافحة الارهاب، على الرابط: https://www.europarabct.com/?p=34807

عدد الاطراف في هذا الصراع ، اضحى الصراع ذا طبيعة سياسية متخذاً شكلاً عسكرياً من حيث طبيعة الاضرار وتدمير الثروة المعلوماتية في البنية التحتية للدولة [1].

ثانيا: مفهوم الفضاء السيبراني: اختصر الفضاء السيبراني حاجز الزمان والمكان وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة، وانماط جديدة تختلف عن الصراعات التقليدية[2]، سيما ان الفضاء السيبراني هو وطن جديد لا ينتمي الى الجغرافيا ولا الى التاريخ، وهو وطن دون حدود، ودون ذاكرة، ودون تراث، انه الوطن الذي تبنيه شبكات الاتصال المعلوماتية الالكترونية في بيئة الفضاء السيبراني[3]، تلك البيئة السيبرانية التي تمتاز بغياب الحدود والقيود الجغرافية أو السياسية أو الاقليمية، وغياب الحكم القاهر لعنصر الزمن، وغياب السلطة المسؤولة عن بيئة الشبكات، مما يعني غياب ممارسات الرقابة الدينية أو الأخلاقية أو الاجتماعية في البيئة السيبرانية[4]

وقد عرفت البشرية في صراعها من اجل البقاء بيئات طبيعية سعت لاستكشافها واستغلالها ومحاولة فرض نفوذها عليها، بداية من الأرض أو الاقليم البري والاقليم البحري، ومع التطور التكنلوجي أمكن القفز الى بيئة طبيعية أخرى وهي الاقليم الجوي ثم الانتقال الى بيئة الفضاء الخارجي من خلال الصواريخ والأقمار الصناعية ، وبفضل ثورة المعلومات والتكنلوجيا ومع ظهور شبكات الانترنيت ومواقع الويب ظهرت لدينا بيئة الفضاء السيبراني الذي اضحى احد العناصر الرئيسة التي تؤثر في النظام الدولي بما يحمل من ادوات تكنلوجية تلعب دوراً مهماً في عملية التعبئة والحشد في العالم ، فضلاً عن التأثير في القيم الاستراتيجية والسياسية، وتجدر الإشارة الى أن مسألة تحديد مفهوم الفضاء السيبراني هي مسألة نسبية، تتوقف على

---

[1] – عبد الغفار عفيفي ، استراتيجية الردع السيبراني.. التجربة الامريكية، مجلة السياسة الدولية، مركز الاهرام للدراسات الاستراتيجية، القاهرة، العدد 213، يوليو 2018، ص 196

[2] – سماح عبد المنصور، الصراع السيبراني ، طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية ، ملحق اتجاهات نظرية ، الصراع السيبراني ، التنازع العالمي على قوة الفضاء الالكتروني، العدد 208، مركز الاهرام للدراسات الاستراتيجية، ابريل 2017، ص 5.

[3] – علاء الدين فرحات، الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 10، العدد3، الجزائر، 2019، ص 90.

[4] – حسن مظفر الرزو، الفضاء المعلوماتي، مركز دراسات الوحدة العربية، ط1، بيروت، 2007، ص 323.

طبيعة ادراك وفهم كل من الدول والهيئات كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في الفضاء السيبراني[1].

يعرف الفضاء السيبراني بانه مصطلح حديث، ظهر نتيجة لثورة تكنلوجيا المعلومات، ويشمل جميع الحواسيب والمعلومات التي بداخلها والانظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الانترنيت العامة[2]، كما يعرف الفضاء السيبراني نسبة الى علم (السيبرنيتيك) وهو العلم الذي يدرس طرق سيلان المعلومات ومراقبتها عند الكائنات الحية، وداخل الاجهزة الالية والمنظومات الاجتماعية والاقتصادية[3]، ومصطلح السيبرانية مأخوذ من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب، أو تقنية المعلومات، أو الواقع الافتراضي[4].

أما الوكالة الفرنسية لأمن انظمة الاعلام وهي(وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي) فقد عرفته بانه فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الالية للمعطيات الرقمية[5]، وتجدر الاشارة بان اول من استخدم مصطلح السيبرانية هو عالم الرياضيات (نوربرت وينر)(Norbert Wiener) عام 1948 اثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان والهندسة الميكانيكية.[6]

أما الاتحاد الدولي للاتصالات يعرف الفضاء السيبراني بانه المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي (أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات

---

[1] – اسماعيل زروقة ، الفضاء السيبراني والتحول في مفهوم القوة والصراع، مصدر سبق ذكره، ص 1017.

[2] – محمود محارب، اسرائيل والحرب الالكترونية ، قراءة في كتاب حرب في الفضاء الالكتروني، اتجاهات وتأثيرات على إسرائيل، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2011، ص 1.

[3] – علاء الدين فرحات، مصدر سبق ذكره ، ص 90.

[4] – صالح بن علي بن عبد الرحمن، الأمن الرقمي وحماية المستخدم من مخاطر الانترنيت، رؤية 2030، هيئة الاتصالات وتقنية المعلومات، الرياض ، 2017، ص 6.

[5] – قادير اسماعيل ، ادارة الحروب النفسية في الفضاء الالكتروني، الاستراتيجية الامريكية الجديدة في الشرق الاوسط، الندوة الدولية عولمة الاعلام السياسي وتحديات الامن القومي للدول النامية ، قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، الجزائر، 2007، ص4.

[6] – احمد عبيس الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد4،جامعة بابل، 2016، ص615.

النقل والتحكم، ومستخدمو كل هذه العناصر)[1]،أما قاموس مصطلحات الأمن المعلوماتي عرف السيبرانية بأنها هجوم عبر الفضاء الإلكتروني، يهدف الى السيطرة على مواقع الكترونية، أو بنى محمية إلكترونيا لتعطيلها، أو تدميرها، أو الأضرار بها[2]، وفي الجانب العسكري يعرف الفضاء السيبراني بانه الذراع الرابعة للجيوش الحديثة، وأنه يمثل البعد الخامس بالحرب، وهذا التعريف يحصر الفضاء السيبراني في المجال العسكري فقط دون التطرق للمجالات الاخرى[3] .

وفي هذا الاطار بات المجتمع الدولي في العصر الحديث يواجه عدداً كبيراً من التهديدات والمخاطر الأمنية, التي تتسم بتغيرها وتطورها المستمر، واتساع نطاق تأثيرها اذ لا يقتصر على الإضرار بأمن فواعل بعينها، وإنما يمتد ليؤثر في الأمن العالمي بشكل عام، ولعل أبرز هذه التهديدات الأمنية المعاصرة وأكثرها حداثة وأوسعها انتشارا هي التهديدات السيبرانية (Cyber threats)، التي بات من الصعب حصرها أو تطوير استراتيجيات محكمة لمواجهتها بشكل كامل، سيما مع تعدد أشكالها ومساراتها ومصادرها، وتطورها المتسارع، ولذا باتت مواجهة هذه التهديدات على قمة أولويات الامن القومي و السياسات الأمنية للدول والمنظمات الدولية، وسيما مع توقع إمكانية حدوث طفرة في التطورات التكنولوجية في الفضاء السيبراني في السنوات القادمة، تتعاظم معها خطورة هذه التهديدات[4]، وفي هذا الاطار شهد القرن العشرين وبدايات القرن الحادي والعشرين ثورة معلوماتية كان لها انعكاساتها على مسار السياسة الدولية، اذ افرزت تلك الثورة ثلاثة عناصر أساسية هي المعلومات، والفضاء السيبراني، والطابع الرقمي[5] .

وخلاصة القول ان الفضاء السيبراني هو مجال افتراضي من صنع الانسان، يعتمد على تكنلوجيا المعلومات والاتصالات، وأن من يمتلك القدرة والكفاءة على توظيف القدرات السيبرانية من اجل تحقيق مأرب

---

[1] - The International Telecommunication Union, ITU Toolkit for Cybercrime, Legislation Geneva, 2010, p12.

[2] – احمد عبيس الفتلاوي، الهجمات السيبرانية، مصدر سبق ذكره، ص 613.

[3] – اسماعيل زروقة ، الفضاء السيبراني والتحول في مفهوم القوة والصراع، مصدر سبق ذكره، ص 1017.

[4] – نوران شفيق، اشكال التهديدات الالكترونية ومصادرها، المركز الاوربي لدراسات مكافحة الارهاب والاستخبارات، المانيا، وحدة الدراسات و التقارير، على الرابط: https://www.europarabct.com/?p=34807

[5]– عادل عبد الصادق ، الارهاب الالكتروني ، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة ، مؤسسة الاهرام ، مركز الدراسات الاستراتيجية ، القاهرة، 2009، ص39.

ومكاسب استراتيجية وتعظيم الاستفادة من الفضاء السيبراني سوف يصبح اكثر قدرة على تحقيق اهدافه بفرض الهيمنة والنفوذ في هذا الفضاء، والتأثير على سلوك الفاعلين المستخدمين لهذه البيئة.

ثانياً: سمات الفضاء السيبراني:

تعود اسباب اهتمام الفاعلين سواء أكانوا من الدول أم غيرها، بهذا الفضاء، كمجال لتحقيق الهيمنة والنفوذ، وادارة الصراعات، الى امتلاكه عدة سمات اساسية، لعل اهمها الاتي[1]:

1- ساحة صراع افتراضية: فيما انه ليس مساحة جغرافية، لذلك يتخطى الفضاء السيبراني العديد من الثنائيات التي تظهر في الصراعات التقليدية، اذ يشارك في الصراعات ذات الطبيعة السيبرانية المدنيون والعسكريون، كما ترتبط ايضاً بالتطورات المادية السياسية والعسكرية على الارض، بخلاف انها اقل كلفة من حيث الخسائر المادية، واكثر تحديداً للهدف مقارنة بنظيرتها التقليدية.

2- زيادة الاعتماد التكنلوجي: اذ باتت الدول الحديثة تربط بنيتها التحتية بالفضاء السيبراني، سيما شبكات الكهرباء، والمياه، والبنوك، والبورصة، والاتصالات، وغيرها، فضلاً عن انظمة السيطرة والتحكم العسكرية، وجمع المعلومات، مثل الاقمار الصناعية، والطائرات دون طيار في الحروب، ومن ثم اصبح استهداف تلك البنى التحتية للدولة ذات الطابع الالكتروني احد عوامل الصراع السيبراني.

3- تماهي حدود الداخل والخارج: أي وجود حالة من التأثير الشبكي المتزايد داخل الدول وخارجها، اذ اتسع استخدام الافراد، والجماعات، والدول، للتكنلوجيا الحديثة المرتبطة بالفضاء السيبراني.

4- غياب الشفافية الالكترونية، فمع عدم القدرة على معرفة هويات القائمين على هجمات القرصنة، نشبت معضلة غياب الشفافية والقوانين المقيدة للصراعات في المجال السيبراني .

5- الفضاء السيبراني لا يقتصر على شبكة الانترنيت فقط، وانما شبكات عالمية وخاصة أخرى مثل، GPS, ACARS,SWIFT, PSTN [2]

6- القدرة على التشبيك وبناء روابط افتراضية، اذ تتيح الأدوات السيبرانية للأفراد قدرة أكبر على التواصل، والتشبيك، وبناء مجتمعات افتراضية بأشكال مختلفة للتأثير في القضايا عبر وسائل التواصل الاجتماعي[1] .

---

[1] – سماح عبد الصبور، الصراع السيبراني، طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، التنازع العالمي على قوة الفضاء السيبراني، مصدر سبق ذكره، ص5-6 .

[2] – صالح بن علي بن عبد الرحمن، الأمن الرقمي، مصدر سبق ذكره، ص 7.

7- انخفاض الكلفة الاقتصادية والسرعة في تبادل المعلومات، فضلاً عن سهولة استخدامه، وامكانية تخفي الفاعلين الذين يستخدمونه وعدم الكشف عن هويتهم الحقيقية.[2]

8- صعوبة الردع الالكتروني: يهدف الردع التقليدي الى خلق حزمة من المحفزات المانعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم في المستقبل ، لكن هذا الهدف يختلف في حالة الردع الالكتروني[3]، على اساس ان الفضاء السيبراني ساحة افتراضية، فيصعب بالتالي على الدول وضع حدود لسيادتها عليه، ومع ضعف القوانين الدولية للسيطرة على هذا الفضاء، يغيب الردع في ظل امكانية التخفي على شبكة الانترنيت، ومجهولية مصدر الهجمات السيبرانية، وسهولة ان يقوم بها الافراد وليس الدول فقط، اذ زادت خبرات القراصنة بشكل متطور دون الحاجة الى لنظم معقدة كانت تملكها الدول وحدها في الصراعات التقليدية[4].

المطلب الثاني: المفاهيم الجديدة في بيئة الفضاء السيبراني والمفاهيم المرتبطة بها

أمسى الفضاء السيبراني مجالاً حديثاً للفعل والتأثير والتغيير في النظام الدولي ، ومع الاستخدام المكثف لتكنلوجيا المعلومات والاتصالات اصبحت قضية امن الفضاء السيبراني تلقى اهتماماً متزايداً على اجندة الأمن الدولي، اذ ازدادت العلاقة بين الأمن والتكنلوجيا مع امكانية تعرض المصالح الحيوية الاستراتيجية الى مخاطر باتت تهدد بتحول الفضاء السيبراني الى ساحة للصراع الدولي المتعدد الاطراف، ومن ثم يفرض واقع هذه البيئة السيبرانية الجديدة تحديات تتعلق بإعادة تعريف القوة السيبرانية وتحديد عناصرها، وتعريف الصراع السيبراني و الأمن السيبراني، فضلاً عن الارهاب السيبراني، وهو ما سيتناوله هذا المطلب.

اولاً: القوة السيبرانية: استطاعت بعض الدول أن تحقق قفزة كبيرة في توظيف وتطويع التكنلوجيا الحديثة في زيادة قوتها وتعظيمها، وظهر لدينا نوع جديد من القوة اطلق عليها (القوة السيبرانية)(Cyber

---

[1] – ابتسام علي حسين، فرص وقيود الأطراف المتنازعة على المجال العام السيبراني ، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، مصدر سبق ذكره، ص 12.

ولمزيد من التفاصيل حول المجتمعات الافتراضية ، ينظر الى : علي محمد رحومة ، علم الاجتماع الالي، مقاربة في علم الاجتماع العربي ، سلسلة عالم المعرفة، العدد، 347، يناير 2008.

[2] – ايهاب خليفة ، القوة الالكترونية، مصدر سبق ذكره، ص 64.

[3] -Martin C.Libicki, Cyber deterrence and Cyber war, Santa Monica: Rand, 2009, p28.

[4] – سماح عبد الصبور، الصراع السيبراني ، طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، مصدر سبق ذكره، ص6.

(Power[1]، ويعرفها (جوزيف ناي) (Joseph s. Nye) بأنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا و للتأثير في الاحداث في البيانات الواقعية الأخرى عبر ادوات الكترونية، وقد حدد (جوزيف ناي) مصادر التهديد في عصر الفضاء السيبراني الى أربعة تهديدات تضمنت التخريب الاقتصادي و الجرائم الالكترونية والحرب الالكترونية ، والإرهاب الالكتروني[2].

وكان لظهور الفضاء السيبراني والشبكة العنكبوتية أثر مهم في الحياة البشرية ، فسهولة استخدامها ورخص تكلفتها ساعد على قيامها بمهام متعددة في الحياة البشرية، في مختلف الصعد الاقتصادية والتجارية والمعلوماتية و العسكرية و السياسية و حتى الأيديولوجية ، ومن ثم ظهر مفهوم اطلق عليه (القوة السيبرانية) (Cyber power)، و بات جلياً ان من يمتلك أدوات واليات توظيف البيئة السيبرانية فانه سيكون الأكثر قدرة على تحقيق اهدافه الاستراتيجية، و التأثير في سلوك الفاعلين المستخدمين لهذه البيئة السيبرانية.[3]

ومن ثم فان الثورة المعلوماتية التي افرزت القوة السيبرانية كشكل جديد من اشكال القوة أفضت بأن يكون لهذه القوة الافتراضية تأثير كبير في علاقات القوى على مستوى السياسة الدولية ، فمن ناحية ادت الى توزيع القوة بين عدد أكبر من الفاعلين، مما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك، مقارنة بالمجالات الأخرى للقوة، ومن ناحية اخرى جعلت القوة الافتراضية السيبرانية الفاعلين الاصغر في السياسة الدولية لديهم قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني ، وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية[4] ، وفي هذا السياق فان امتلاك القدرات السيبرانية لم يعد حكراً على فاعل بعينه اذ اصبح في مقدور الدول الصغيرة، والمتوسطة، والفاعلين من غير الدول، مهما صغر حجمهم، وتواضعت امكانياتهم، الاستفادة من القدرات السيبرانية بما فيها تطوير اسلحة رقمية، وتهديد الخصوم بها، سيما انه في الوقت الحالي، تتسع باطراد قائمة الدول ذات القدرات السيبرانية المتطورة.

---

[1] – ايهاب خليفة، القوة الالكترونية، المصدر السابق ، ص 7.

[2] Joseph S Nye. Jr.Cyper power (Cambridge: Harvard Kennedy school . Belfer center for Science and International Affairs .2010, pp.12-16.

[3]– ايهاب خليفة، القوة الالكترونية ، كيف يمكن ان تدبر الدول شؤونها في عصر الانترنيت(الولايات المتحدة انموذجاً) ، العربي للنشر والتوزيع، ط1، القاهرة، 2017، ص 5.

[4] – سعاد محمود ابو ليلة ، المصدر السابق، ص 16.

وفي هذا السياق لعب الفضاء السيبراني دوراً اساسياً في تعظيم القوة، او الاستحواذ على عناصرها الأساسية في العلاقات الدولية، اذ اصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فاعلية على الارض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في الفضاء السيبراني على نظم التحكم والسيطرة التكنلوجية، ومن هنا برزت القوة السيبرانية، التي تضمنت، مجموعة من الموارد المتعلقة بالتحكم والسيطرة على اجهزة الحاسبات والمعلومات ، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل[1] .

وانطلاقاً من هذه المعطيات يمكن القول بان الفضاء السيبراني هو مجال اخر لاستعراض القوى، وممارسة النفوذ وتحقيق التفوق والتنافس الدولي، فلم تعد ترسانات الاسلحة التقليدية وأسلحة الدمار الشامل هي المعيار الاساس لقياس القوة بعد الثورة المعلوماتية، اذ وفرت تكنلوجيا المعلومات والاتصالات اسلحة من نوع جديد تفضي الى احراز النصر وكسب المعركة، متجاوزة الفواعل بذلك الحدود الجغرافية ، والتقليل من الخسائر البشرية والمادية[2] .

عناصر القوة السيبرانية: يتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية والاقتصادية والسياسية والثقافية والاعلامية وغيرها، وحتى تتمكن الدولة من ممارسة النفوذ داخلياً او خارجياً عبر القوة السيبرانية، يجب ان تتضمن مجموعة عناصر لعل اهمها الاتي[3] :

1- وجود بنية تحتية سيبرانية : وتشمل اجهزة الكمبيوتر وشبكات الاتصالات والبرمجيات وقواعد البيانات، لمختلف الأنظمة والقطاعات.

2- وجود بنية مؤسسية: تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة.

3- وجود بنية تشريعية: تكون ضامنة ومحددة لاستعمال القوة السيبرانية.

4- وجود استراتيجية تتضمن أهداف واضحة: تحدد طرق واليات العمل والأهداف المرجوة.

---

[1] – عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العلمي، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، مصدر سبق ذكره، ص 33.

[2] – لبنى خميس مهدي، اثر السيبرانية في تطور القوة، مجلة حمورابي، العدد 33-34، السنة الثامنة، بغداد، 2020، ص152.

[3] – اسماعيل زروقة، الفضاء السيبراني والتحول في مفهوم القوة والصراع، مصدر سبق ذكره، ص118.

ثانياً: الصراع السيبراني: مع تحول الفضاء السيبراني الى ساحة للتفاعلات الدولية، برز العديد من الانماط التوظيفية له سواء على صعيد الاستخدامات ذات الطبيعة العسكرية او المدنية، الامر الذي جعل هذا الفضاء بمثابة مجالاً للصراعات المختلفة سواء للفاعلين من الدول او غير الدول من اجل حيازة اكبر قدر من النفوذ والتأثير السيبراني، ويمكن تعريف الصراع السيبراني بأنه استخدام تكنلوجيا الحاسوب في الفضاء السيبراني لأغراض التدمير من اجل التغيير، أو التأثير، أو التعديل في التفاعلات الدبلوماسية والعسكرية بين فواعل مختلفة، كما يعرف الصراع السيبراني بانه نموذج للحرب غير المتكافئة تسعى من خلاله كل اطراف الصراع المختلفة الى تعظيم الاستفادة من الفضاء السيبراني وبسط النفوذ والهيمنة وحماية امنها القومي فضلاً عن تحقيق مكاسب استراتيجية واقتصادية وسياسية ومالية لم تكن لتحققها عبر الوسائل العسكرية التقليدية، سيما ان امتلاك القدرات السيبرانية لم يعد حكراً على فاعل بعينه، اذ اصبح في مقدور الدول الصغيرة والمتوسطة والفاعلين من غير الدول الاستفادة من القدرات السيبرانية بما فيها تطوير اسلحة رقمية وتهديد الخصوم بها[1]، كما ساعد الفضاء السيبراني على انتشار القوة بين مختلف الفاعلين ، واعطى مساحة متزايدة للفواعل من غير الدول للتأثير في التفاعلات الاقليمية والدولية ، وافضى ذلك الى زيادة التهديدات والمخاطر التي تواجهها الدول من خلال الفضاء السيبراني[2].

وفي هذا السياق تتسع قائمة الدول ذات القدرات السيبرانية المتطورة، اذ لم تعد القائمة تقتصر على القوى السيبرانية العظمى (الولايات المتحدة الاميركية ، الصين، بريطانيا، روسيا)، فضلا عن (اسرائيل)، اذ ظهرت في اقاليم مختلفة قوى سيبرانية يعتد بها مثل(استراليا، الهند، إندونيسيا، كوريا الجنوبية، في اسيا، البرازيل والمكسيك والارجنتين في امريكا الجنوبية والوسطى، وفي منطقة الشرق الاوسط بزغت قوى اقليمية سيبرانية (ايران، تركيا، وفاعلون من غير الدول) يحاولون توظيف القدرات السيبرانية من اجل تحقيق اهداف استراتيجية .[3]

---

[1] – احمد زكي عثمان، تأثير القدرات السيبرانية في الصراعات الاقليمية، ملحق مجلة السياسة الدولية، اتجاهات نظرية ، الصراع السيبراني، مركز الاهرام للدراسات الاستراتيجية، القاهرة، العدد 208، ابريل 2017، ص 17.

[2] – ايهاب خليفة، القوة الالكترونية، العربي للنشر والتوزيع، ط1 القاهرة، 2017، ص 62.

[3] – احمد زكي عثمان، المصدر السابق، ص 17.

وفي هذا الاطار شكلت القفزات التكنلوجية الهائلة في مجال الاتصال والمعلومات في اواخر القرن العشرين وبدايات القرن الحادي والعشرين مسارات جديدة لنشوب صراعات حول النفوذ السيبراني في الفضاء السيبراني، اذ عد هذا الاخير ساحة واسعة للتفاعلات العالمية تضمنت في الاساس على شبكات رقمية ذات صلة كبيرة بين اجهزة الحاسوب وانظمة الاتصال والتكنو معلوماتية والانترنيت بغرض تدفق المعلومات، وتكتنف ظاهرة الصراع السيبراني حالة من الغموض وعدم اليقينية وهو الاقرب الى ما كان يسمى بالغموض النووي اثناء الحرب الباردة.[1]

وانطلاقا من هذه المعطيات فان الصراع في الفضاء السيبراني اضحى يمثل نمطاً جديداً من الظواهر قيد التبلور في التفاعلات العالمية ، نتاجاً لتزايد الاعتماد عليه، سواء من قبل الافراد أو الجماعات أو الدول، وتطرح هذه الظاهرة في بعض جوانبها خصوصية من حيث طبيعة معنى الصراعات السيبرانية وأدواتها وفواعلها، ومن جانب اخر تشتبك مع نظيرتها التقليدية لتصبح احدى ادواتها في التنافس على النفوذ والهيمنة في العالم، و هنا من المهم الاشارة الى أن هناك اربعة اسلحة رئيسية في الصراعات السيبرانية هي: تخريب ومهاجمة مواقع الانترنيت، الحرمان من الخدمة، الاقتحام الفيروسي، عمليات التسلل[2].

ثالثاً: الأمن السيبراني: تزايدت العلاقة بين بين الامن والفضاء السيبراني سيما مع امكانية تعرض المصالح الاستراتيجية للدول الى اخطار وتهديدات ، الأمر الذي افضى الى تحول الفضاء الالكتروني الى وسيط ومصدر لأدوات جديدة للصراع الدولي[3]، اذ يعرف الامن السيبراني بأنه أمن وحماية الشبكات والانظمة المعلوماتية والبيانات والاجهزة المتصلة بالأنترنيت، وهو المسار الذي يتعلق بإجراءات ومعايير الحماية التي ينبغي اتخاذها والالتزام بها عند استشعار الخطر لمواجهة التهديدات والمخاطر السيبرانية والحد من تأثيرها[4].

---

[1] – عبد الغفار عفيفي ، استراتيجية الردع السيبراني.. التجربة الامريكية، مجلة السياسة الدولية ، مركز الاهرام للدراسات الاستراتيجية، القاهرة، العدد 213، يوليو 2018، ص 196.

[2] – سماح عبد الصبور، مصدر سبق ذكره، ص 7، ص10.

[3] – عادل عبد الصادق، انماط الحرب السيبرانية ، مصدر سبق ذكره، ص 32.

[4] – منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية، بيروت، 2017، ص35.

رابعاً :الردع السيبراني: هو مجموعة من الاجراءات التي تفضي الى خلق عدد من المحفزات التي تمنع قيام احد أطراف الصراع باعتداء او هجوم مستقبلاً على الطرف الاخر، ويتطلب الردع السيبراني مصداقية الدفاع عن انظمة المعلومات وردع اي محاولة لاختراقها، كما يتطلب القدرة على الانتقام ، وتكبيد المهاجم ضرراً يفوق ما وقع على المدافع من أضرار[1].

خامساً :الارهاب السيبراني: شكلت ظاهرة الارهاب السيبراني احدى ابرز الظواهر التي نتجت عن اتساع استخدام الفاعلين من غير الدول للفضاء السيبراني ، وعلى الرغم من القيم الايجابية والتعاونية التي ارتبطت ببزوغ الفضاء السيبراني فانه سرعان ما ظهرت استخدامات غير سلمية كشفت وجهاً سلبياً لتلك التطورات الكبيرة ، لاسيما مع تصاعد استغلال الجماعات الارهابية للتكنلوجيا الحديثة ليس فقط على المستوى الميداني، وانما على صعيد التواصل والاعلام وبث الافكار وتجنيد المتعاطفين وساهم ذلك في افراز جدالات نظرية بشأن ما سمي بالإرهاب السيبراني[2].

ومن هنا صعد مفهوم الارهاب السيبراني ليعبر عن العلاقة بين الجماعات الارهابية وأدوات الفضاء السيبراني ، وهو المصطلح الذي صكه لأول مرة الباحث الامريكي (باري كولين) (Barry C. Collin) في منتصف ثمانينات القرن العشرين ، بحسبانه يمثل حالة من الاندماج بين العالمين الواقعي والافتراضي من اجل تحقيق اهداف ارهابية ضد المصالح العامة[3]، ومن ثم يعرف الارهاب السيبراني بأنه استخدام التنظيمات الارهابية وبعض المنظمات والدول لشبكات التواصل (الانترنيت) للتواصل والدعاية والتضليل ، من اجل تحقيق مكاسب استراتيجية من خلال الهجوم أو التهديد بالهجوم على اجهزة الحاسوب والشبكات وانظمة المعلومات لتدمير البنية التحتية وترهيب الحكومة او المواطنين واجبارهم على تحقيق أهداف سياسية واقتصادية واجتماعية بعيدة المدى، وتعد هذه التنظيمات الارهابية الاحدث والاكثر خطورة على الأمن الدولي.[4]

---

[1] -Joseph S. Nye JR, Cyber power, (London: Harvard Kennedy School, 2010) P.10.

[2] – فاطمة الزهراء عبد الفتاح، تطور توظيف جماعات العنف للإرهاب السيبراني، ملحق مجلة السياسة الدولية العدد،208، ص25، مصدر سبق ذكره.

[3] – المصدر نفسه ، ص 25.

[4] – محمد اكرم محسن ، التهديد السيبراني للأمن الاقليمي في القرن الحادي والعشرين (اسرائيل انموذجا) ، رسالة ماجستير ، جامعة الموصل، كلية العلوم السياسية،2022، ص28.

المبحث الثاني: طبيعة التهديدات والمخاطر السيبرانية وانعكاساتها على الأمن القومي الأمريكي:

يحتل الفضاء السيبراني اهمية كبيرة للولايات المتحدة الامريكية بسبب ارتباط معظم البنى التحتية المدنية والعسكرية بالفضاء السيبراني، وفي نفس الوقت تواجه تهديدات كبيرة في البيئة السيبرانية، سيما ان هناك تغير في طبيعة التهديدات السيبرانية التي واجهتها الولايات المتحدة من اختراق مواقع الكترونية الى سرقة معلومات اقتصادية وعسكرية فضلاً عن تسريب وثائق سياسية، وسرقة انظمة حربية .

ويزداد الامر خطورة مع ربط معظم البنى التحتية الامريكية بالفضاء السيبراني، مثل انظمة المواصلات والاتصالات، وادارة المحطات النووية ، ومنشآت توليد الطاقة الكهربائية ، وأنظمة ادارة السدود المائية ، بالإضافة الى أنظمة توجيه الصواريخ عن بعد والطائرات بدون طيار ، والسيطرة على الاقمار الصناعية وغيرها من المصالح الاستراتيجية، ومن هنا فان الحفاظ على هذه البنية التحتية من اي هجمات سيبرانية يدخل في صميم اهتمامات الامن القومي الامريكي[1] .

وانطلاقاً من هذه المعطيات احتل الفضاء السيبراني أهمية كبيرة في المدرك الاستراتيجي الأمريكي بسبب ارتباط معظم البنى التحتية المدنية والعسكرية بالفضاء السيبراني، بما أفرز مصالح قومية ترتبط بأمنها، وبسبب هذ الارتباط والتشابك مع الفضاء السيبراني تواجه الولايات المتحدة الامريكية تهديدات ومخاطر جمة مصدرها الفضاء السيبراني[2]، ومن هنا يسعى هذا المبحث الى تحديد طبيعة وانواع هذه التهديدات وتداعياتها على الامن القومي الامريكي، وسيتم التركيز على التهديدات الاقتصادية والتهديدات العسكرية بشكل كبير من خلال مطلبين ، يناقش الاول انواع التهديدات السيبرانية الاقتصادية المؤثرة على الامن القومي الامريكي، اما المطلب الثاني سوف يناقش التهديدات العسكرية السيبرانية المؤثرة على الامن القومي الأمريكي.

[1] – ايهاب خليفة، القوة الالكترونية، العربي للنشر والتوزيع ، القاهرة، ط1، 2017، ص239.

[2] – المصدر نفسه ، ص239.

المطلب الاول : التهديدات السيبرانية الاقتصادية التي تواجها الولايات المتحدة وتداعياتها على الأمن القومي الأمريكي

أحدثت تكنلوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، مما افضى الى زيادة التحديات و التهديدات والمخاطر السيبرانية مع زيادة هيمنة تكنلوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية متكاملة الاركان تحصل عن طريق شبكات الانترنيت بأشكال ومسارات متعددة مثل سرقة الاموال، النصب والاحتيال، التخطيط لعمليات ارهابية، الترويج لأخبار كاذبة، الابتزاز الإلكتروني، فضلاً عن جريمة القرصنة الالكترونية بعدها الجريمة الاكثر انتشاراً في العالم الافتراضي[1].

ازدادت التهديدات السيبرانية ذات الطابع الاقتصادي للنظام المالي ، ففي شهر فبراير 2016 استهدف القراصنة بنك بنغلاديش المركزي واستغلوا مواطن الضعف في نظام سويفت، وهو نظام رسائل الدفع الالكترونية الرئيسي للنظام المالي العالمي في محاولة لسرقة مليار دولار، وعلى الرغم من حظر معظم المعاملات فقد اختفى مبلغ قدره (101) مليون دولار، وكانت عملية السطو بمثابة جرس انذار لعالم التمويل في الولايات المتحدة ، بان المخاطر السيبرانية في النظام المالي قد تم التهوين من شأنها بشكل كبير، ومع ذلك لا تزال الحكومات والمؤسسات المصرفية تكافح من اجل احتواء التهديدات الاقتصادية السيبرانية، ففي فبراير من عام 2020 حذرت (كرستين لا غارد) الرئيس السابق لصندوق النقد الدولي من أن حدوث هجمة سيبرانية على المؤسسات المصرفية سيفضي الى نشوء ازمة مالية خطيرة، وفي ابريل من عام 2020 حذر مجلس الاستقرار المالي في الولايات المتحدة انه اذا لم يتم احتواء اي اعتداء سيبراني اقتصادي فقد تفضي الى اضطرابات خطيرة في الانظمة المالية مما يؤدي الى مخاطر اوسع على الاستقرار الاقتصادي العالمي[2]، لا سيما ان الولايات المتحدة الامريكية تخشى من امكانية تكرار سيناريو الهجمات السيبرانية الروسية على استونيا في 2007 والذي تسبب في توقف التعاملات البنكية والمصرفية فضلاً عن تدمير الكثير من

[1] – اسماعيل زروقة، الفضاء السيبراني والتحول في مفهوم القوة والصراع، مجلة العلوم القانونية والسياسية، الجزائر، المجلد 10، العدد 1، 2019 ص117..

[2] – تيم نيلسون، التهديد السيبراني العالمي، مكتب التمويل والتنمية، معهد كارنيغي للسلام الدولي ، أذار 2021، ص 24.

المؤسسات المصرفية وشل معظم القطاعات الاقتصادية في استونيا[1]، ومن هنا امست مواجهة هذه التهديدات والمخاطر الاقتصادية في البيئة السيبرانية على قمة اولويات الامن القومي السيبراني الامريكي.

وفي هذا السياق تعد التهديدات السيبرانية ذات الطابع الاقتصادي من اخطر التهديدات التي يمكن ان تتعرض لها الولايات المتحدة ، بسبب ان النظم التجارية والمالية والمصرفية تعمل الكترونياً، بالإضافة الى شركات التكنولوجيا العملاقة بما تتضمنه انظمتها السيبرانية من براءات اختراع ومشاريع تطوير سرية وحقوق الملكية الفكرية هي عرضة للاختراق السيبراني وسرقة المعلومات التجارية لصالح الدول المنافسة ، مما يضع الاقتصاد الامريكي امام خسائر ضخمة سواء نتيجة سرقة معلومات اقتصادية او تجارية او سرقة براءات الاختراع التي تضعف قدرة المنتج الامريكي على المنافسة في السوق العالمية، وتعد الصين وروسيا من اهم الدول التي قد تلحق بالولايات المتحدة خسائر اقتصادية عبر البيئة السيبرانية.[2]

وفي هذا الاطار نشرت مجلة التايم تقريراً مفاده تعرض كبريات شركات الصناعة الامريكية الى حزمة من الهجمات السيبرانية مصدرها الصين والموسومة ب (هجمات مطر العمالة) بدأت منذ 2003، وبين تقرير (مانديات) وهي احدى شركات الامن السيبراني الامريكية لعام 2013، ان الصين قد هاجمت (141) مؤسسة تجارية وصناعية امريكية في عام 2006 من اجل سرقة البيانات الاقتصادية وبراءات الاختراع الصناعية ونتائج ابحاث اقتصادية علمية ، مما ادى الى الحاق خسائر اقتصادية كبيرة بهذه الشركات الامريكية صبت في مصلحة الاقتصاد الصيني على حساب الاقتصاد الامريكي، وفي عام 2011 اشار تقرير صادر عن شركة (مكافي)المتخصصة في برامج مكافحة الفيروسات الى تعرض شركات النفط الامريكية وشركات الطاقة والبتروكيمياويات الى هجمات سيبرانية ترجع الى IP جهاز كمبيوتر يوجد بالصين عام 2009.[3]

كما اظهرت دراسة في العام 2018 اقرها مجلس المستشارين الاقتصاديين للبيت الابيض ان الاقتصاد الامريكي يخسر سنوياً بين 57 و 109 مليار دولار بسبب الهجمات السيبرانية على قطاع الخدمات المالية

[1] - Rebecca Grant, victory in cyberspace, An Air force Association special Report, October 2007. https://www.airandspaceforces.com/1025threat

[2] – ايهاب خليفة، القوة الالكترونية ، مكتبة العربي للنشر والتوزيع، القاهرة، ط1، 2017، ص 115.

[3] – المصدر نفسه ، ص 222.

وشبكات الطاقة[1]، وذكرت صحيفة (نيويورك تايمز) الامريكية ، ان الحكومة الامريكية تتهم الصين بمحاولة سرقة معلومات عن ابحاث بخصوص لقاح كورونا واستغلال وقت الوباء لعمل هجمات على البنية التحتية والمؤسسات المالية الامريكية[2]، ويؤكد تقرير صادر من مجلس السياسة الخارجية الامريكية، ان اجهزة الاستخبارات الصينية تعمل على استغلال الاشخاص ذوي الاصول الصينية داخل الشركات الامريكية من اجل سرقة المعلومات الاقتصادية من خلال البريد الالكتروني، وفي عام 2014 تم الحكم في سبعة قضايا تجسس اقتصادي ذات صلة بالصين ،وفي عام 2015 افرجت محكمة امريكية عن استاذ يعمل في الجامعة بعد اتهامه بالتجسس الاقتصادي، وكان "تشانج هاو" احد ستة صينيين نسبت لهم الحكومة الامريكية تهمة التجسس الاقتصادي [3].

وفي عام 2021 تعرضت نحو 200 شركة امريكية لهجوم سيبراني حسب تقرير مؤسسات الامن الالكتروني بالولايات المتحدة الاميركية، واستهدف الهجوم شركة تكنلوجيا المعلومات (كاسيا) في ولاية فلوريدا قبل ان ينتشر في بقية الشركات التي تستخدم نفس البرمجيات[4]، وفيما يتعلق بالهجمات السيبرانية على انابيب النفط، تعرضت الولايات المتحدة الى هجوم سيبراني استهدف خط انابيب النفط (كولونيا باي بلاين) في الساحل الشرقي للولايات المتحدة في عام 2021 وادى الى نقص كبير في امدادات الطاقة بجميع انحاء الولايات المتحدة[5].ولما كانت الولايات المتحدة فاعلا أساسياً في بنية النظام الاقتصادي العالمي، ومحرك رئيس في تطوير تكنلوجيا المعلومات والاتصالات الحديثة، ومن ثم فان اقتصادها سيبقى دوماً في موضع الخطر وعرضة للاختراق والقرصنة من قبل القوى المنافسة لها، من اجل جمع المعلومات الاقتصادية والصناعية التي تتحكم في الأسواق العالمية.

---

[1] - The cost of Malicious Cyber Activity to The U.S. Economy, The Council of Economic Advisers , February 2018,p 1

[2] – محمد هيكل، زيادة وتيرة الهجمات السيبرانية بالتزامن مع جائحة كورونا ، نيويورك تايمز تقرير منشور على الرابط: .https:covid – 19. Ecsstudies. Com

[3] – امريكا تفرج عن استاذ جامعي، صحيفة الشرق، العدد 103، 2015 على الرابط: https://al-2015/07/30/sharq.com/article

[4] – القرصنة الالكترونية على الرابط: 2015/07/30/https://al-sharq.com/article

[5] – داليا السيد، الهجمات السيبرانية، مجلة درع الوطن، الامارات، 2021،على الرابط: https://www.nationshield.ae/index.php/home

المطلب الثاني: التهديدات العسكرية السيبرانية وتداعياتها على الامن القومي الامريكي

بدأ التركيز على الفضاء السيبراني كتهديد امني جديد بفعل أحداث دولية لعل من ابرزها استخدام تنظيم القاعدة له كميدان قتال ضد الولايات المتحدة الامريكية بعد احداث ايلول 2001، وفي عام 2007 برز بشكل اكبر دور الفضاء السيبراني كساحة جديدة في الصراع بين استونيا وروسيا، وفي عام 2008 في الحرب بين روسيا وجورجيا ، ثم جاء الهجوم الالكتروني بفيروس "ستاكس نت" على برنامج ايران النووي عام 2010 ليكون بمثابة نقلة مهمة في تطور مجال الاسلحة السيبرانية ، و خلال العقد الاخير حدثت موجة انتشار كبيرة جداً لتكنلوجيا المعلومات والاتصالات ، اذ وصل عدد المتصلين بخدمة الانترنيت الى اكثر من 2 مليار شخص، وعدد مشتركي الشبكات الاجتماعية الى اكثر من 2 مليار ، ومن ثم افضت علاقة الفضاء السيبراني بعمل المنشأت الحيوية الى امكانية تعرضها لهجمات سيبرانية تستهدف الشبكة كوسيط وحامل للخدمات، او بشل عمل انظمتها المعلوماتية ، ومن هنا اصبحت القدرة على تنفيذ الهجمات السيبرانية أداة سيطرة ونفوذ استراتيجية بالغة الاهمية في زمن السلم والحرب، ترتب على ذلك دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء السيبراني دوراً اساسياً في تعظيم القوة ، اذ اصبح التفوق في البيئة السيبرانية عنصرا مهماً في تنفيذ عمليات ذات فاعلية كبيرة في الارض ، والبحر ، والجو ، والفضاء من خلال نظم التحكم والسيطرة.[1]

كما افضى تراجع سيادة الدولة مع تصاعد دور الفاعلين من غير الدول في العلاقات الدولية مثل الشركات التكنلوجية العابرة للحدود وشبكات الجريمة والقرصنة الالكترونية والجماعات الارهابية وغيرها، الى فرض تحديات عديدة في الحفاظ على الامن السيبراني العالمي، و دفع ذلك الى بروز اتجاهات تعددية لتحقيق الامن عبر التنسيق بين اصحاب المصلحة من الحكومات والمجتمع المدني والشركات التكنلوجية ووسائل الاعلام والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني[2].

[1] – عادل عبد الصادق ، القوة الالكترونية اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد 188، ابريل ، مركز الاهرام للدراسات الاستراتيجية، 2012، ص28.

[2] – عادل عبد الصادق، انماط الحرب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية ، ملحق اتجاهات نظرية ، الصراع السيبراني، مصدر سبق ذكره، ص32.

لا سيما ان المجتمع الدولي في العصر الحديث بات يواجه عدداً كبيراً من التهديدات الأمنية التي تتسم بتغيرها وتطورها المستمر، واتساع نطاق تأثيرها بحيث لا يقتصر على الإضرار بأمن فواعل بعينها، وإنما يمتد ليؤثر في الأمن العالمي بشكل عام، ولعل أبرز هذه التهديدات الأمنية المعاصرة وأكثرها حداثة وأوسعها انتشارا هي التهديدات السيبرانية Cyber threats، ذات الطابع العسكري، اذ أصبحت التهديدات السيبرانية ذات الطابع العسكري معقدا جداً، و اصبح من الصعب حصرها أو تطوير استراتيجيات محكمة لمواجهتها بشكل كامل، سيما مع تعدد مصادرها وانماطها، فضلاً عن تطورها المستمر، وفى إبريل 2001، حدث توتر في العلاقات الأمريكية الصينية بسبب إرسال الولايات المتحدة الامريكية طائرة تجسس على الساحل الجنوبي للصين، وهو ما ردت عليه الصين بإرسال طائرة حربية اصطدمت مع الطائرة الأمريكية مما أدى إلى هبوط الطاقم الأمريكي اضطراريًا على الأراضي الصينية واحتجاز الصين له، وهي الأزمة التي انتهت بجهود دبلوماسية من الطرفين، في تلك الفترة، وفي ظل توتر العلاقات ما بين البلدين، تعرضت المواقع السيبرانية الخاصة بالجيش الأمريكي لهجمات الحرمان من الخدمة من قبل عدة جماعات صينية كان من بينها جماعة أطلق عليها ((Honker Union، وفى يوليو 2008، تعرضت الولايات المتحدة إلى سلسلة من هجمات الحرمان من الخدمة التي استهدفت عدداً من المواقع والمؤسسات العسكرية.[1]

ولعل من اخطر ما تعانيه الولايات المتحدة الامريكية في مجال التهديدات السيبرانية ذات البعد العسكري هو تعرضها المستمر لسرقة البيانات والمعلومات العسكرية أو التلاعب بها، والسيطرة على نظم الدفاع الجوي والطيران، سيما ان المؤسسات العسكرية الامريكية وادارة الاقمار الصناعية والصناعات الحربية والغواصات النووية ونظم الدفاع الجوي والطيران كلها مرتبطة بأنظمة الكترونية حديثة .

وفي هذا الاطار انطلقت عام 2008 واحدة من اخطر الهجمات الموجهة ضد انظمة حواسب الجيش الأمريكي من خلال حزمة USB) متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية متواجدة في منطقة الشرق الأوسط، مما شكل ما يشبه جسراً رقمياً تم من خلاله نقل الاف الملفات من البيانات الى

[1] – التهديدات الالكترونية ،الاشكال والمصادر، المركز الاوربي لدراسات مكافحة الارهاب، 2020، على الرابط: https://www.europarabct.com/

خوادم خارجية ، فضلا عن استهداف اكثر من 72 شركة من بينها 13 مكتباً من مقاولي قوات الدفاع من اجل سرقة معلومات حول الخطط والمباني العسكرية[1].

وفي تقرير مقدم إلى الكونجرس الأمريكي سربت أجزاء منه إلى صحيفة الواشنطن بوست، ذكر أن قراصنة صينيين ، قاموا بسرقة معلومات عسكرية أمريكية تتعلق بمنظومات مضادة للصواريخ من طراز PAC–3) ونظام (THAAD) ، وهذا مكن الحكومة الصينية من استخدام هذه المعلومات لتطوير تقنياتها العسكرية، وفي الوقت الذي أعلنت فيه الصين عن إنشاء وحدات حرب الفضاء الإلكتروني عام 2003 تعرضت الولايات المتحدة في نفس العام لواحدة من أسوأ حزم التجسس الإلكتروني، ويطلق عليها اسم Titan Rain))، اذ تم سحب ما يتراوح بين (10 و20) تيرابايت من المعلومات من شبكة البنتاجون ، كما قام قراصنة صينيون بشن هجمات اخرى على المواقع الإلكترونية لشركة (لوكهيد مارتين) الأمريكية وسرقوا معلومات عن تكنولوجيا حديثة لصناعة مقاتلة (أف– 35)التي استخدمتها الصين لدى تصميم وتصنيع مقاتلة (تي 20 الصينية)[2]، وفق تقرير لشبكة فوكس نيوز فان الصين نجحت في تصنيع طائراتها المقاتلة من الجيل الخامس عن طرق التجسس السيبراني وقيامها بنسخ التكنلوجيا العسكرية الامريكية .[3]

وفي عام 2011 اعلنت القيادة المركزية الامريكية بان ايران نجحت في السيطرة سيبرانياً على طائرة استطلاع بدون طيار امريكية فوق مياه مضيق هرمز ، وارغمتها على النزول[4]، وفي 19 ديسمبر من عام 2020، اتهم وزير الخارجية الامريكي(مايك بومبيو) روسيا بالوقوف وراء شن اسوء هجوم تجسس سيبراني على الحكومة الامريكية، واعلنت الولايات المتحدة عن تعرضها لهجمات سيبرانية وقرصنة معلوماتية ضخمة استهدفت مؤسسات امريكية حساسة من بينها المكتب الحكومي الذي يدير الاسلحة النووية التابع لوزارة الطاقة الامريكية[5].

---

[1] – ايهاب خليفة، القوة الالكترونية، مصدر سبق ذكره، ص 198.

[2] – التطبيقات الامنية لقوة الفضاء الالكتروني، دورية اتجاهات الاحداث، مركز المستقبل ، العدد الاول، اغسطس 2014، على الرابط: https://futureuae.com/m/Mainpage/Item/851/cyber–power

[3] – بندر الدوشي، امريكا والصين، على الرابط: 10/03/2023/https://www.alarabiya.net/arab–and–world

[4] – ايران اسقطت بلا مبرر طائرة استطلاع امريكية، على الرابط: https://www.bbc.com/arabic/middleeast–48700382

[5] – الهجوم الالكتروني على الولايات المتحدة، على الرابط: https://www.bbc.com/arabic/world–55377723

وفي عام 2021 كشفت شبكة (بالو التو) الامنية بان قراصنة يشتبه بانهم اجانب تمكنوا من اختراق تسعة منظمات حساسة في قطاعات الدفاع والطاقة والتكنلوجيا في الولايات المتحدة الامريكية، وبينت الشبكة الامنية انه بمساعدة من وكالة الامن القومي الامريكي وهيئة الابحاث الامنية السيبرانية تم الكشف عن اختراق القراصنة والذين كانوا يهدفون الى سرقة معلومات حساسة من شركات متعاقدة مع وزارة الدفاع الامريكية [1] .

وفي 20 ابريل من عام 2023 تعرضت مطارات الولايات المتحدة الامريكية الى عطل غامض في انظمة القيادة والحاسوب، مما افضى الى تأخير رحلات الطيران في جميع انحاء الولايات المتحدة ، وعلى الرغم من نفي الرئيس الامريكي "جون بايدن" تعرض المطارات لهجوم سيبراني، لكن ذلك لا ينفي هذا الاحتمال، سيما ان الولايات المتحدة سبق ان تعرضت في منتصف عام 2022 الى هجوم سيبراني افضى الى تعطل عدة مواقع الكترونية لمطارات امريكية تبنت مسؤوليته مجموعة من القراصنة الروس، وفي الانتخابات الامريكية التي فاز بها ترامب على خصمه الديمقراطي هيلاري كلنتون ، اتهمت الاخيرة روسيا بالوقوف وراء تزوير الانتخابات من خلال تنفيذ هجمات سيبرانية على النظام الانتخابي ، ومنذ اندلاع الحرب الروسية–الاوكرانية، ازدادت التحذيرات الدولية من نشوء حرب سيبرانية بين روسيا من جهة ، والولايات المتحدة و اوربا من الجهة الاخرى، سيما ان هذه الهجمات السيبرانية تعد واحدة من سيناريوهات الحرب الحديثة[2] .

وفي هذا السياق تجري الولايات المتحدة سنوياً محاكاة التعرض لحرب سيبرانية ، يطلق عليها (عاصفة الحواسب)، (cyber Storm) ، تخصص ميزانية ضخمة قدرت عام 2012 ب (500) مليون دولار، لمواجهة التهديدات السيبرانية وتطوير اسلحة وادوات الحرب السيبرانية[3]، ومن ثم اصبح الأمن السيبراني من اهم التحديات التي تواجه البشرية في زمن الثورة الصناعية الرابعة، سيما ان القرصنة و الجرائم السيبرانية قد

---

[1] – قراصنة يخترقون تسعة منظمات حساسة، على الرابط:
https://arabic.cnn.com/world/article/2021/11/08/hackers-defense-contractors-energy-health-care-nsa

[2] – جيهان فوزي، الحرب السيبرانية هل تتطور الى نووية، على الرابط:
/14/01/2023/https://www.alarabiya.net/politics

[3] – ايناس عبد الهادي، صراع القوى في الفضاء السيبراني، مركز وطن الفراتين للدراسات الاستراتيجية، على الرابط:
17/https://watan-alfuratain.iq/articles/details

كلفت الاقتصاد العالمي اكثر من 6 تريليونات دولار عام 2021، ومن المتوقع ان تصل كلفة هذه الجرائم السيبرانية على الاقتصاد العالمي على نحو 10 ونصف ترليون دولار سنوياً بحلول عام 2050 حسب ما ذكرت مجلة الجرائم الالكترونية (cybercrime magazine) في تقريرها مستندة على احصائيات رسمية[1].

وبينت الازمة الاوكرانية الاخيرة، والاستعراض النووي في كوريا الشمالية وايران، ان الاسلحة النووية لم تتلاشى، بل اصبحت اجندتها تتضافر مع صعود الاسلحة السيبرانية ، سيما ان احد الاحتمالات السلبية المرتبطة بتطورات الثورة التكنو معلوماتية هو ظهور الاسلحة السيبرانية كتهديد للعمليات النووية على المستويات الرقمية والمادية ، اذ ان الاسلحة السيبرانية يمكنها تعطيل او اضعاف اداء الانظمة المادية المرتبطة بالبنية التحتية للأسلحة النووية ، مثل اقمار الانذار المبكر أو ايقاف اداء وظائف السيطرة والقيادة النووية على جميع المستويات[2] .

المبحث الثالث: استراتيجيات الولايات المتحدة الامريكية للأمن السيبراني خلال الادارات المتعاقبة.

نتيجة لزيادة حجم التهديدات والهجمات السيبرانية اتجهت العديد من الدول الى تحديث قدراتها الهجومية والدفاعية لمواجهة تهديدات ومخاطر الحرب السيبرانية فضلاً عن الاستثمار في البنية التحتية التكنو معلوماتية ورفع كفاءة الجاهزية والاستعداد للحرب السيبرانية[3]، كما حفزت المزايا الاستراتيجية لهجمات الفضاء السيبراني الى امكانية توظيفها عسكرياً في ظل اعتماد الدول على الانظمة الالكترونية في جميع منشأتها الحيوية ، فضلاً عن العمل على توظيف الفضاء السيبراني في تعظيم قوة الدول، ومن ثمة ظهر ما يعرف ب الاستراتيجية السيبرانية للدول، ومن جهة اخرى افضت عملية تصاعد المخاطر الى تصاعد دور الشركات العاملة في مجال الامن السيبراني في ظل اتساع نطاق مخاطر الانشطة العدائية التي يمارسها الفاعلون سواء كانوا من الدول او من غير الدول[4]، ومن ثم ادى اتساع علاقة الدول بالفضاء السيبراني الى ظهور جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية ، ولعل من أبرز تلك التداعيات الاتي[5]:

---

[1] – جيهان فوزي، الحرب السيبرانية هل تتطور الى نووية، مصدر سبق 1كره .

[2] – المصدر نفسه .

[3] – عبد الغفار عفيفي ، استراتيجية الردع السيبراني.. التجربة الامريكية ، مجلة السياسة الدولية ، مركز الاهرام للدراسات الاستراتيجية، القاهرة، العدد 213، يوليو 2018، ص 196.

[4] – المصدر نفسه ، ص 200.

[5] – عادل عبد الصادق ، مصدر سبق ذكره ، ص35.

1- تصاعد المخاطر السيبرانية، سيما مع قابلية المؤسسات الحيوية سواء كانت ذات طبيعة عسكرية أو مدنية في الدول للهجوم السيبراني عليها عبر وسيط وحامل للخدمات السيبرانية، او شل عمل انظمتها التكنو معلوماتية، ومن ثم فان التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية مهمة في زمن السلم أو الحرب.

2- تعزيز القوة وانتشارها، ادى الفضاء السيبراني الى اعادة تشكيل قدرة الاطراف المؤثرة، مثل الولايات المتحدة الامريكية، لطالما كانت الاخيرة تمتلك الاحتكار لمصادر القوة ، ولكن سرعان ما برزت مسألة انتشار القوة بين فواعل متعددة من الدول وغير الدول.

3- عسكرة الفضاء السيبراني، وذلك من اجل درء تهديداته على امن الفضاء السيبراني، وادت عسكرة الفضاء الى تصاعد القدرات في سباق التسلح السيبراني، فضلا عن تبني استراتيجيات دفاعية وهجومية سيبرانية لدى المؤسسات المعنية بالأمن السيبراني في الدول.

4- ادماج الفضاء السيبراني ضمن الامن القومي للدول، وذلك عبر انشاء وحدات متخصصة في الحروب السيبرانية، واجراء المناورات لتعزيز الدفاعات السيبرانية ، فضلاً عن القيام بالتدريب وانشاء مشروعات وطنية للأمن السيبراني.

5- الاستعداد لحروب المستقبل، اذ تعتمد العديد من الدول على استراتيجية حرب المعلومات بعدها حرباً للمستقبل، وترى الدول الكبرى ان من يحدد نتائج ومألات تلك المعارك المستقبلية ليس من يمتلك القوة فقط، وانما القادر على التشويش على المعلومات وشل القوة للخصم.

واستدعت تلك التهديدات تارة اجراءات حكومية دفاعية لحماية هذه المصالح، وتارة أخرى هجومية من أجل التأثير في سلوك الاطراف المتنافسة ، سيما ان القوة السيبرانية أخذت طابعاً انتشارياً واسعاً بين فواعل من غير الدول وأصبح بإمكان الأفراد والجماعات حيازة نفوذ سيبراني في البيئة الافتراضية السيبرانية، الأمر الذي خلف حروباً سيبرانية اختلفت أدواتها ومضامينها عن نظيرتها التقليدية[1]، ومن ثم اصبح الفضاء الإلكتروني يستخدم للقيام بحروب غير تقليدية عبر هجمات الارهاب السيبراني، واطلاق فايروسات الحاسب،

[1] – خالد حنفي علي، اشكاليات تداخل الصراعات السيبرانية والتقليدية، مصدر سبق ذكره، ص3.

والتجسس الالكتروني، وعن طريق الاختراق المباشر لشبكة المعلومات مما افضى الى ظهور مصادر جديدة غير تقليدية للتهديدات على الأمن القومي الامريكي[1] .

وربما ادركت الولايات المتحدة الامريكية (كقوة عالمية باحثة عن استمرار هيمنتها)، اهمية تأثير العامل التكنلوجي والمعلوماتي في بنية موازين القوى العالمية ، اذ وضعت التفوق المعلوماتي في الفضاء السيبراني كمجال لزيادة قدراتها و حرمان الخصوم منه ضمن استراتيجيتها القومية للقرن الحادي والعشرين، واتسع هذا الهدف الامريكي ليشمل معظم القدرات السيبرانية في مجال المعلومات والاتصالات مع تزايد الصراع العالمي على حيازة النفوذ في الفضاء السيبراني[2]، سيما ان التهديدات السيبرانية ستكون بمثابة المشهد الصراعي المستقبلي في البيئات الاستراتيجية الاقليمية والدولية على مستوى التنافس والصراع من قبل القوى المهيمنة على النظام الدولي والقوى الاقليمية الطامحة الى ايجاد مكان لها في البيئة الاستراتيجية بمسارات تكنلوجية ورقمية[3].

وفي هذا السياق تحتل الهيمنة على الفضاء السيبراني واستخدامه كوسيلة لكبح جماح الاستراتيجيات الصاعدة للقوى المنافسة لها، مكانة متقدمة جداً في اجندة الاستراتيجية الامريكية وسيما في حقب الرؤساء (باراك اوباما، دونالد جون ترامب، جون بايدن)، ففي هذا الفضاء السيبراني تتنافس وتتطارح الاستراتيجية الامريكية مع الاستراتيجيات الدولية والاقليمية التي تسعى للخروج من نطاق الهيمنة الامريكية مثل(الصين، روسيا، المانيا، كوريا الشمالية) وغيرها من الاستراتيجيات والتي تنذر بحرب سيبرانية مستقبلية.

وفي هذا السياق شهد العالم تحولات واضحة في مسارات الاستراتيجية الامريكية تجاه الفضاء السيبراني نتيجة التفوق عالمياً، فالانفراد بكفة التوازن الاستراتيجي والقدرة على الاستقطاب الاقليمي والعالمي حفزها

---

[1] – سعاد محمود ابو ليلة ، دورة القوة، ديناميكيات الانتقال من الصلبة الى الناعمة الى الافتراضية، مجلة السياسة الدولية ، ملحق اتجاهات نظرية ، كيف يمكن فهم تحولات القوة في السياسة الدولية، مركز الاهرام للدراسات الاستراتيجية، العدد 188، ابريل ، القاهرة، 2012، ص 16.

[2] – خالد حنفي علي ، اشكاليات تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208، مركز الاهرام للدراسات السياسية والاستراتيجية، ابريل 2017، ص3.

[3] – وليد غسان سعيد، دور الحرب الالكترونية في الصراع العربي الاسرائيلي، اطروحة دكتوراه غير منشورة، كلية الدراسات العليا ، جامعة النجاح الوطنية، فلسطين، 2013، ص 81.

لاستكمال الهيمنة السيبرانية[1]، لذلك تنوعت الاستراتيجيات الامريكية السيبرانية ما بين الهجوم والدفاع من خلال الادارات المتعاقبة على حكم البيت الابيض[2]، وقد مثل اعلان الرئيس الامريكي (دونالد جون ترامب) انشاء فرع عسكري جديد في الفضاء نقطة تحول فارقة بهذا الشأن، ونستعرض فيما يلي ابرز ملامح التحولات في استراتيجيات الفضاء السيبراني الامريكي.

المطلب الاول: ملامح استراتيجية الفضاء الوطنية الامريكية في عهد باراك اوباما:

اكد الرئيس الامريكي (باراك اوباما) في خطاب له اثناء حملته الانتخابية ان التهديدات السيبرانية تعد من اخطر التحديات التي تواجه الامن القومي الامريكي ، واكد بان رفاهية الاقتصاد الامريكي في القرن الحادي والعشرين سوف تعتمد على الامن السيبراني[3]، واتخذت الادارة الامريكية في حقبة الرئيس(باراك اوباما) حزمة من التدابير الاستباقية والوقائية لمواجهة التهديدات والمخاطر السيبرانية ، ولعل من اهم تلك التدابير اعلان وزارة الدفاع الامريكية في 22 يونيو 2009 تشكيل قيادة عسكرية للفضاء السيبراني لحماية شبكات الجيش الامريكي والرد على الهجمات السيبرانية التي ينفذها قراصنة المعلوماتية للقوى المنافسة للولايات المتحدة الامريكية، لتبرز اهمية الفضاء السيبراني كقضية تتعلق بالأمن القومي الامريكي في ظل تزايد الاعتماد الدولي عليه[4].

وفي عام 2010 اصدرت ادارة الرئيس (باراك اوباما) سياسة وطنية للفضاء، وركزت هذه السياسة على اهم التهديدات ومنها الهجمات السيبرانية والارهاب السيبراني و الكوارث الطبيعية والاوبئة وسبل مواجهتها[5] ، ثم تلاها في عام 2011 اصدار اول استراتيجية وطنية للأمن الوطني السيبراني، والتي كانت بمثابة نهجاً براجماتياً يهدف الى الحفاظ على المزايا المستمدة من الفضاء السيبراني، مع مواجهة تحيات البيئة

---

[1] – عبد الكريم زهير، الاستراتيجية الأمريكية للهيمنة على الفضاء السيبراني العالمي، رسالة ماجستير غير منشورة، كلية العلوم السياسية، جامعة الموصل، 2021، ص 162.

[2] – ايهاب خليفة، القوة الالكترونية، مصدر سبق ذكره، ص 242.

[3] – president Obama, Speech at Purdue University, July 17th , 2008,. على الرابط: https://www.spokesman.com/stories/2008/jul/17/obama-outlines-national-security-strategy–

[4] – عادل عبد الصادق، الفضاء الالكتروني وتهديدات جديدة للأمن القومي، المركز العربي لأبحاث الفضاء الالكتروني، على الرابط: https://accronline.com/article_detail.aspx

[5] – National Security Strategy 2010, The White House ,May 2010, p9.

الاستراتيجية السيبرانية المتطورة، وجمع المعلومات الاستخبارية والانشطة ذات الصلة ، ولعل من اهم اهداف الاستراتيجية الامريكية للأمن الوطني السيبراني في عهد اوباما هي الاتي[1] :

1- تعزيز السلامة والاستقرار والامن في الفضاء، والحفاظ على مزايا الامن القومي الاستراتيجي الممنوحة للولايات المتحدة في الفضاء السيبراني المتنازع عليه.

2- تنشيط القاعدة الصناعية الفضائية التي تساهم في دعم الامن القومي الامريكي.

3- تعزيز الاستخدام السلمي للفضاء السيبراني والتعاون مع الحلفاء والدول الاخرى والمنظمات الدولية بهذا الشأن.

4- منع وردع الاعتداء على البنية التحتية الفضائية التي تدعم الامن القومي الامريكي.

وفي هذا السياق نظرت ادارة اوباما الى الفضاء السيبراني بعده احد مصادر الرخاء والتقدم الاقتصادي للولايات المتحدة، اذ اكدت معظم الاستراتيجيات على ضرورة بناء شراكات مع القطاع الخاص والافراد فضلاً عن تعزيز التعاون الدولي من اجل مكافحة مخاطر الهجمات السيبرانية[2]، واتجهت ادارة الرئيس اوباما نحو برنامج يركز على الاستخدامات التجارية والمدنية بشكل عام من خلال الاستراتيجيات السابقة، ففي البداية نأت خطط الفضاء السيبرانية الامريكية في عهد اوباما عن ادخال قدرات هجومية لبرامجها، ولكن يبدو ان هذا الاتجاه كان مرهوناً بتحركات القوى الدولية الاخرى ، اذ بدء الحديث حول ضرورة التحول حول هذا النهج في عام 2013، عندما اطلقت الصين صاروخ وصف بانه مهمة بحثية حسب تصريحات المسؤولين في الصين، الا انه كان في الحقيقة اختباراً لسلاح جديد مضاد للأقمار الصناعية ، سيما ان الاختبار الصيني جاء عقب مجموعة اختبارات اخرى اجرتها كل من روسيا والصين للأقمار الصناعية المناورة في مدارات ارضية منخفضة، الأمر الذي افضى الى قلق ومخاوف امريكية حول امن الفضاء السيبراني، وتم رفع هذه المخاوف من حتمية نشوء حرب سيبرانية الى الرئيس اوباما ، الامر الذي أدى الى مراجعة الاستراتيجية التي يقودها مجلس الامن القومي في عام 2014.[3].

---

[1] – عزة هاشم: رهانات التوجه الامريكي لتسليح الفضاء، ملحق مجلة السياسة الدولية، مركز الاهرام للدراسات الاستراتيجية، القاهرة، العدد 216، ابريل 2019، ص 5.

[2] –ايهاب خليفة، القوة الالكترونية ، مصدر سبق ذكره، ص 160.

[3] – عزة هاشم، مصدر سبق ذكره، ص 6.

المطلب الثاني : ملامح استراتيجية الفضاء الوطنية الامريكية في عهد الرئيس ترامب:

تصاعدت خلال عام 2018، مخاوف كبيرة من انخراط القوى الكبرى في النظام الدولي وتحديداً الولايات المتحدة الامريكية وروسيا والصين في سباق تسلح خطير في الفضاء السيبراني، كان ابرز ما اثار تلك المخاوف اعلان الرئيس الامريكي دونالد ترامب في عام 2018 عن عزم ادارته تأسيس قوة عسكرية فضائية لتحل محل قيادة الفضاء، وتصبح قوة مستقلة تمثل الفرع السادس من افرع القوات المسلحة الامريكية، الى جانب القوات البحرية والبرية والجوية والمارينز وحرس السواحل، واشار الى انه في ظل هذه القوة الفضائية الجديدة ستعمل الولايات المتحدة على تطوير عقيدة قتال وتكتيكات، واستخدام احدث التقنيات للحرب في الفضاء السيبراني، فضلاً عن اعداد فيلق عسكري من رواد الفضاء يمثل نخبة مقاتلة تستخدم خطط الحرب المشتركة في الفضاء[1]، وتهدف القوة الفضائية الامريكية الى حماية الاقمار الصناعية الامريكية من اي اعتداء مادي او اي محاولة قرصنة او تشويش من جانب الخصوم، وكذلك تهدف الى تطوير القدرات العسكرية الدفاعية والهجومية في الفضاء السيبراني، وقيادة المعركة وعمليات النقل الفضائي فضلاً عن حماية اكثر من 100 قمر صناعي امريكي يخدمون وكالات الاستخبارات والامن القومي الامريكي[2]، واعترف قانون تفويض الدفاع الوطني بالقوة الفضائية بعدها فرعاً مستقلاً ضمن القوات المسلحة الامريكية يوم 20 ديسمبر 2019، ولعل من ابرز واجبات القوة الفضائية التي تم تأسيسها في عهد ترامب هو حماية مصالح الولايات المتحدة الامريكية وحلفائها في الفضاء السيبراني و ردع اي عدوان او هجمات موجهة ضد المصالح الامريكية الاستراتيجية في البيئة السيبرانية، فضلاً عن تنفيذ العمليات العسكرية السيبرانية[3]، وضمان هيمنة الولايات المتحدة المهددة من قبل الصين وروسيا في الفضاء السيبراني[4]، اذ تواجه الهيمنة الامريكية في الفضاء السيبراني تهديداً من جانب روسيا والصين اللتين طورتا قدراتهما التكنلوجية، وتتراوح

[1] – مالك عوني، حرب نجوم جديدة، ملحق مجلة السياسة الدولية، العدد 216، ابريل 2019، ص 3.

[2] – قوة الفضاء الامريكية، طبيعتها ومهامها، على الرابط: https://www.alhurra.com/choice-alhurra

[3] – القوة الفضائية للولايات المتحدة، على الرابط: https://ar.wikipedia.org/wiki/

[4] – صراع الكبار، الجزيرة ، على الرابط: https://www.aljazeera.net/politics

التهديدات من التشويش على الاقمار الصناعية لنظام تحديد المواقع الى استهداف قمر صناعي بصاروخ ارض جو ، وهو ما اختبرته الصين بنجاح في عام 2007، وفقاً للبنتاغون[1].

وحذرت الصين بان الولايات المتحدة تسعى الى تحويل الفضاء الى ساحة معركة جديدة ، بعدما اعلن الرئيس (ترامب) تأسيس ذراع عسكرية جديدة تحت مسمى القوة الفضائية، وقال المتحدث باسم وزارة الخارجية الصينية (غينغ شوانغ) ان المسارات الامريكية تنتهك بقوة الاجماع الدولي بشأن الاستخدام السلمي للفضاء الخارجي، وتشكل تهديداً مباشراً للأمن والسلام في الفضاء السيبراني ، ودعا المجتمع الدولي الى تبني نهج مسؤول لمنع تحول الفضاء الى ساحة معركة جديدة[2]، كما اعلنت روسيا وفق ما تناقلته وسائل الاعلام الروسية الرسمية ان الولايات المتحدة تقوم من خلال انشاء القيادة العسكرية الجديدة بتشكيل المقدمات اللازمة لعسكرة الفضاء السيبراني لاستخدامه في تحقيق مأربها العسكرية[3].

لعل من اخطر ما تشير اليه هذه التطورات ان ادارة ترامب كانت تنظر الى الفضاء كساحة حرب ، والاخطر من ذلك ان هذه الرؤية لا ترتبط فقط بشخص الرئيس ترامب وتوجهاته ، بل ترتبط بالمدرك الاستراتيجي العسكري الامريكي وله مؤيدوه داخل القوات العسكرية الامريكية ذاتها، وخلال كشفه في 17 يناير 2019 عن تقرير المراجعة الذي اعده البنتاجون بشأن التطوير الضروري لنظام الدفاع الصاروخي الامريكي ، قال ترامب ان الولايات المتحدة الامريكية بحاجة لنشر نظام لأجهزة الاستشعار المدارية بما يتيح اعتراض الصواريخ وايقافها وهي في مساراتها، وشدد ترامب على ان العالم يتغير ونحن سنتغير بشكل اسرع بكثير، يشير هذا الاعلان الى اقتراب العالم بشكل سريع من عصر تسليح الفضاء ، وعلى غرار سابقه حرب النجوم فان هذا المقترح الامريكي يهدد بتغيير بنية وهيكلية التوازن الاستراتيجي العالمي بشكل كامل وليس في الفضاء فقط، اذ يعني نجاح الولايات المتحدة الامريكية في نشر هذا النظام تحييد القدرات والامكانيات الصاروخية لكل الاطراف الدولية ، ومن ثم تقويض الركن الاهم الذي يتأسس عليه هيكل الردع العالمي الحالي[4].

---

[1] – مروة الاسدي، الفضاء افضل ساحة للقتال، على الرابط: https://annabaa.org/arabic/sciences

[2] – المصدر نفسه .

[3] – صراع الكبار، مصدر سبق ذكره.

[4] – مالك عوني، مصدر سبق ذكره، ص 3.

وخلال انعقاد المجلس القومي للفضاء في البيت الابيض عام 2018 صرح ترامب بانه "لا يكفي ان يكون هناك وجود امريكي في الفضاء، بل يجب ان تكون لدينا هيمنة امريكية في الفضاء، ومضى قائلاً لا اريد ان تتسيدنا الصين وروسيا ودول اخرى في الفضاء وان الولايات المتحدة ستكون قائدة الفضاء على المدى البعيد[1] "

المطلب الثالث: ملامح استراتيجية الفضاء الوطنية الامريكية في عهد (جون بايدن):

اكد الرئيس الحالي للولايات المتحدة (جون بايدن) قبل تنصيبه رئيساً للولايات المتحدة في 20/يناير/ 2021 في برنامجه الانتخابي، ان الأمن السيبراني يحتل اولوية قصوى في ادارته القادمة ضمن خطته الاستراتيجية للفضاء السيبراني ، وانتقد (جون بايدن) (دونالد ترامب) بانه مقصرا في تعزيز الامن السيبراني، واكد (جون بايدن) انه سيأخذ الامر بجدية خلال ادارته القادمة لحماية الأمن القومي الامريكي من خلال الرد بقوة على الهجمات السيبرانية ضد مطلقيها[2]، وفي 28/يوليو/ 2021 تحدث (جون بايدن) عن احتمالات دخول الولايات المتحدة حرباً جديدة بسبب التكنلوجيا ، وانه اذا انتهى المطاف بحرب حقيقية مع قوة عظمى فسيكون ذلك نتيجة خرق سيبراني[3].

في اذار/ 2021 اطلقت ادارة الرئيس(جون بايدن)استراتيجية وطنية للأمن السيبراني، في اطار مساعيها لوضع لوائح اكثر شمولاً واماناً في الفضاء السيبراني ضد المتسللين في العالم الرقمي بما في ذلك معالجة هجمات برامج الفدية باعتبارها تشكل تهديداً للأمن القومي، وضعت الاستراتيجية اهدافاً طويلة المدى لكيفية عمل الافراد والشركات والحكومة بأمان في البيئة السيبرانية، استناداً الى خمسة ركائز وهي: الدفاع عن البنى التحتية الحيوية وتشويش الجهات الفاعلة ، وتشكيل قوى السوق لدفع الأمن السيبراني، وتعزيز القدرة على الصمود، والاستثمار في مستقبل مرن، واقامة شراكات دولية من اجل تحقيق الاهداف المشتركة بقطاع الأمن السيبراني[4].

---

[1] – مسلم عباس ، حرب القوة الفضائية، على الرابط: https://annabaa.org/arabic/strategicissues

[2] – كرار عباس متعب، الحرب السيبرانية، مجلة حمو رابي للدراسات، العدد 40، السنة العاشرة، بغداد، 2021، ص 207.

[3] –نورهان الشيخ، الارهاب السيبراني، على الرابط: https://idsc.gov.eg/DocumentLibrary/View/6239

[4] –الولايات المتحدة الامريكية تطلق استراتيجية وطنية للأمن السيبراني، على الرابط: https://www.ecssr.ae/global_news/271412/

صيغت الاستراتيجية في أعقاب سلسلة هجمات سيبرانية كبرى، بما في ذلك هجوم فدية استهدف خط أنابيب كولونيل الأكبر لنقل المنتجات النفطية في الولايات المتحدة، باستغلال ثغرات أمنية سمحت بالوصول إلى اكبر عدد من العملاء، وبموجب هذه الاستراتيجية، سيجري التعامل مع تهديدات برامج الفِدية على أنها مشكلات تهدد الأمن القومي الأمريكي، وتنص الاستراتيجية على أنها تعمل على مواجهة الصين وكوريا الشمالية والدول الاستبدادية التي تُضمر نوايا معادية ، مُتهمة إياها بالاستخدام العدواني للقدرات المتطورة للفضاء السيبراني، من اجل تحقيق مآرب تتقاطع مع المصالح الأمريكية والقوانين الدولية[1].

اكدت الاستراتيجية السيبرانية لإدارة (جون بايدن) على الركائز الايديولوجية والتكنلوجية والجيوسياسية والدبلوماسية لرؤية الرئيس(جون بايدن) الشاملة للسياسة الخارجية، والأمن القومي للولايات المتحدة الامريكية، وتركز ادارة (جون بايدن) على تحسين الدفاعات السيبرانية، وردع الهجمات السيبرانية المعادية ومواجهتها[2] .

ولعل من ابرز الملامح في استراتيجية الفضاء الوطنية الامريكية في عهد (جون بايدن) هو تطوير نظام سيبراني تشغيلي للحرب السيبرانية ، والاسلحة المضادة للأقمار الصناعية في الفضاء السيبراني فضلاً عن برامج الدفاع الصاروخي على نحو يتيح لها بتطوير القدرة المدارية للأقمار الصناعية[3]، وعلى الرغم من ان الولايات المتحدة الامريكية لم تعلن عن نشر اي اسلحة وصواريخ ذات سرعة فرط صوتية عملياتياً (يطلق مصطلح الاسلحة والصواريخ فائقة السرعة او ذات السرعة الفرط صوتية على الصواريخ التي تفوق سرعة طيرانها سرعة الصوت بنحو خمسة مرات اي نحو 3800 ميل في الساعة) فان وزارة الدفاع الامريكية تتبنى تسعة برامج مختلفة لتطوير انظمة اسلحة ذات سرعة فرط صوتية لتكون جزءاً من انظمة تسلح قواتها الفضائية، اذ كشفت شركة (ايروجيت روكيتداين) الامريكية المصنعة لأنظمة دفع الصواريخ عن انها تعمل على تطوير محرك قوي جديد لصاروخ ذي سرعة فرط صوتية لا تقل عن خمسة اضعاف سرعة الصوت لمصلحة القوات الجوية الامريكية ، وتخطط وزارة الدفاع الامريكية في حقبة الرئيس (جون بايدن)

[1] – الولايات المتحدة تطلق استراتيجية، المصدر السابق.

[2] – كرار عباس متعب، الحرب السيبرانية، مصدر سبق ذكره، ص 207.

[3] - Stephen M . McCall, Space as a War fighting Domain: lssues for Congress , Congressional Research Service, Washington , August 10, 2021, p. 2.

بان يكون صاروخها جاهزاً للاستخدام بحلول عام 2022، والذي يعرف باسم صاروخ الهجوم ذي السرعة الفرط صوتية .Hypersonic[1]

وفي ظل تسليح وعسكرة الفضاء السيبراني، يمكن تحديد النهج الامريكي لمواكبة التطور الهائل في الاسلحة ذات السرعة الفرطصوتية لدى القوى الدولية الاخرى ومنها روسيا والصين، في الاستراتيجية التي قدمتها الشركة المسؤولة عن تطوير الاعمال لحلول الدفاع الصاروخي ومضادات الاسلحة الفرط صوتية ، والتي تتكون من اربعة مستويات، هي مستوى طبقة الاستشعار القائمة في الفضاء السيبراني، ومستوى الحرب السيبرانية ومستوى الطاقة الموجهة، ومستوى انظمة القيادة والسيطرة، ومن ثم يرى كثير من الخبراء الامريكيين ان امتلاك قوى اخرى سيما الصين وروسيا للأسلحة الفرطصوتية وتوظيفها في الصراع السيبراني سيؤثر سلبياً في كل من الاستقرار الاستراتيجي والميزة التنافسية للجيش الامريكي ويفضي الى الاختلال في التوازن الاستراتيجي القائم بين الولايات المتحدة والقوى الدولية، وينتقص من القدرة الامريكية على الردع تجاه هذه القوى[2].

وفي هذا الاطار عملت الولايات المتحدة على تعزيز قدراتها الدفاعية والهجومية في الفضاء السيبراني لمواجهة القوى المنافسة لها، سيما في عام 2022 اذ خصصت ادارة الرئيس الامريكي(جون بايدن) ما يقرب من 1.3 مليار دولار لحزمة من برامج القوات الفضائية الامريكية ووكالة تطوير الفضاء من اجل تطوير التكنلوجيا التي تديرها القوة الفضائية لتمويل الفضاء السيبراني، وتخصيص مقابل مادي لقمر صناعي اضافي لنظام تحديد المواقع العالمي ومواجهة التهديدات السيبرانية للقوى المنافسة سيما الصين وروسيا[3].

و اياً ما كانت درجة مصداقية المخاوف الامريكية المعلنة من التهديد الذي تطرحه برامج التطوير العسكري الروسية الصينية للأمن في الفضاء السيبراني، فقد بات جلياً ان المشروع الامريكي لتشكيل القوة الفضائية يتضمن توجهاً عملياً وجدياً لعسكرة وتسليح الفضاء.

---

[1] – مالك عوني ، سباق الاسلحة فائقة السرعة ،ملحق مجلة السياسة الدولية، العدد 218، اكتوبر 2019، ص 3.

[2] – دلال محمود السيد، هاجس التفوق ، ملحق مجلة السياسة الدولية، العدد 218، اكتوبر 2019، ص 8.

[3] – رغدة محمود البهي، عسكرة الفضاء الخارجي، مجلة كلية السياسة والاقتصاد، جامعة بني سويف، ، العدد 16، اكتوبر، 2022، مصر، ص 463.

تضع عودة مشهد سباق التسلح في الفضاء السيبراني الى الساحة الدولية العالم في مواجهة معضلة اساسية حاكمة هي: هل تنتصر معطيات الصراع الاستراتيجي، ام ديناميات العولمة والياتها ؟ ومن ثم يقف الفضاء السيبراني على مفترق طرق تاريخي، يضعه امام ثلاثة سيناريوهات أو مشاهد مستقبلية[1]:

1- اما ان ينتهي الى قبول بهيمنة امريكية استراتيجية على العالم وهو المشهد المستبعد، على الرغم انه الاكثر بروزاً في اللحظة الراهنة، على مجمل انشطة استخدام الفضاء لأغراض سلمية ومدنية .

2- المشهد الثاني هو ان ينفتح المجال امام سباق تسلح مرتفع الخطورة وغير محدود ربما يفضي الى نشوب حرب في الفضاء السيبراني.

3- المشهد الثالث هو رضوخ القوى الكبرى لديناميات العولمة وتوجهها لصياغة نظام توافقي لإدارة الفضاء السيبراني بمعزل عن الصراعات الاستراتيجية على الارض، بحسب ما تحاول الامم المتحدة التي استضافت اجتماعاً ضم خمسة وعشرين دولة من اجل التباحث في شأن تأسيس هذا النظام.

والباحث يرى ان المشهد الثاني(مشهد نشوب الحرب السيبرانية) اقرب للتحقق استنادا الى زيادة تسابق التسلح بين القوى الدولية الكبرى سيما الولايات المتحدة والصين وروسيا، وهو سباق لم يعد تسارعه وتطور تقنياته يسمحان بكبح جماعة في حدود الجغرافيا السياسية للكرة الارضية ، اذ يقف العالم الان على اعتاب لحظة مصيرية لكسر الحد التاريخي الفاصل بين صراعات الجيو استراتيجية، وسلام الفضاء الخارجي، ومن ثم تحول الفضاء السيبراني الى ساحة جديدة للصراع الدولي بين القوى الكبرى من اجل فرض الهيمنة والنفوذ على الفضاء السيبراني، سيما أن هذا الطابع المتواصل لحرب الفضاء السيبراني يلغي الحدود الفاصلة بين السلم والحرب ويخلق بعداً خطيراً من حالة عدم الاستقرار.

[1] – مالك عوني، حرب نجوم جديدة، ملحق مجلة السياسة الدولية ، تحولات استراتيجية، التنافس على الفضاء، العدد 216، ابريل 2019، ص 4.

الخاتمة

استهدفت الدراسة بالرصد والتحليل مسألة التهديدات السيبرانية وتداعياتها على المصالح الحيوية الاستراتيجية للولايات المتحدة الامريكية في الفضاء السيبراني، ومن ثم تحليل الاستراتيجيات الوطنية السيبرانية التي صاغتها الولايات المتحدة الامريكية في عهد الادارات المتعاقبة على الحكم لمواجهة هذه التهديدات وحماية الامن القومي الامريكي.

وفيما يتعلق بالإجابة على التساؤل البحثي الرئيس والتساؤلات الفرعية ،فضلاً عن التحقق من صحية الفرضيات التي تبنتها الدراسة، اجابت الدراسة بان الفضاء السيبراني احتل أهمية كبيرة في المدرك الاستراتيجي الأمريكي بسبب ارتباط معظم البنى التحتية المدنية والعسكرية بالفضاء السيبراني، بما أفرز مصالح استراتيجية ترتبط بأمنها القومي، و بسبب هذ الارتباط والتشابك مع الفضاء السيبراني تواجه الولايات المتحدة الامريكية تهديدات ومخاطر جمة مصدرها الفضاء السيبراني، سيما ان هناك تغير في طبيعة التهديدات السيبرانية التي واجهتها الولايات المتحدة من اختراق مواقع الكترونية الى سرقة معلومات اقتصادية وعسكرية فضلاً عن تسريب وثائق سياسية، وسرقة انظمة حربية.

وكشفت الدراسة بان اخطر ما تعانيه الولايات المتحدة الامريكية في مجال التهديدات السيبرانية ذات البعد العسكري هو تعرضها المستمر لسرقة البيانات والمعلومات العسكرية أو التلاعب بها، والسيطرة على نظم الدفاع الجوي والطيران، لا سيما ان المؤسسات العسكرية الامريكية وادارة الاقمار الصناعية والصناعات الحربية والغواصات النووية ونظم الدفاع الجوي والطيران كلها مرتبطة بأنظمة الكترونية حديثة.

كما اكدت الدراسة بان الفضاء السيبراني اصبح مجال اخر لاستعراض القوى، وممارسة النفوذ وتحقيق التفوق والتنافس الدولي، فلم تعد ترسانات الاسلحة التقليدية وأسلحة الدمار الشامل هي المعيار الاساس لقياس القوة بعد الثورة المعلوماتية، اذ وفرت تكنلوجيا المعلومات والاتصالات اسلحة من نوع جديد تفضي الى احراز النصر وكسب المعركة، متجاوزة الفواعل بذلك الحدود الجغرافية ، والتقليل من الخسائر البشرية والمادية، سيما أن هذا الطابع المتواصل لحرب الفضاء السيبراني يلغي الحدود الفاصلة بين السلم والحرب ويخلق بعداً خطيراً من حالة عدم الاستقرار.

كما جادلت الدارسة بان العالم شهد تحولات واضحة في مسارات الاستراتيجية الامريكية تجاه الفضاء السيبراني نتيجة التفوق عالمياً، فالانفراد بكفة التوازن الاستراتيجي والقدرة على الاستقطاب الاقليمي والعالمي حفزها لاستكمال الهيمنة السيبرانية ، لذلك تنوعت الاستراتيجيات الامريكية السيبرانية ما بين الهجوم والدفاع من خلال الادارات المتعاقبة على حكم البيت الابيض ، وقد مثل اعلان الرئيس الامريكي (دونالد جون ترامب) انشاء فرع عسكري جديد في الفضاء نقطة تحول فارقة بهذا الشأن.

وفي هذا الاطار عملت الولايات المتحدة الأميركية على تعزيز قدراتها الدفاعية والهجومية في الفضاء السيبراني لمواجهة القوى المنافسة لها، سيما في عام 2022، اذ خصصت إدارة الرئيس الامريكي(جون بايدن) ما يقرب من 1.3 مليار دولار لحزمة من برامج القوات الفضائية الامريكية ووكالة تطوير الفضاء من اجل تطوير التكنلوجيا التي تديرها القوة الفضائية لتمويل الفضاء السيبراني، وتخصيص مقابل مادي لقمر صناعي اضافي لنظام تحديد المواقع العالمي ومواجهة التهديدات السيبرانية للقوى المنافسة سيما الصين وروسيا .

توصلت الدراسة الى مجموعة من النتائج لعل اهمها الاتي:

1- تحتل الهيمنة الامريكية على الفضاء السيبراني واستخدامه كوسيلة لكبح جماح الاستراتيجيات الصاعدة للقوى المنافسة لها، مكانة متقدمة جداً في اجندة الاستراتيجية الامريكية وسيما في حقب الرؤساء (باراك اوباما، دونالد جون ترامب، جون بايدن).

2- اصبحت القدرة على تنفيذ الهجمات السيبرانية اداة سيطرة ونفوذ استراتيجية في زمن السلم أو الحرب.

3- ان المشروع الامريكي لتشكيل القوة الفضائية يتضمن توجهاً عمليا وجدياً لعسكرة وتسليح الفضاء.

4- ادت عسكرة الفضاء الى تصاعد القدرات في سباق التسلح السيبراني، مما افضى الى تبني حزمة من الاستراتيجيات الدفاعية والهجومية السيبرانية لدى المؤسسات المعنية بالأمن السيبراني في الولايات المتحدة الامريكية.

5- التهديدات والمخاطر السيبرانية ستكون بمثابة المشهد الصراعي المستقبلي في البيئات الاستراتيجية الاقليمية والدولية على مستوى التنافس والصراع من قبل القوى المهيمنة على النظام الدولي والقوى الاقليمية الطامحة الى ايجاد مكان لها في البيئة الاستراتيجية السيبرانية.

6- تتنافس وتتطارح الاستراتيجية الامريكية في الفضاء السيبراني مع الاستراتيجيات الدولية والإقليمية التي تسعى للخروج من نطاق الهيمنة الأمريكية مثل (الصين، روسيا، المانيا، كوريا الشمالية) وغيرها من الاستراتيجيات والتي تنذر بحرب سيبرانية مستقبلية.

7- ان امتلاك قوى اخرى سيما الصين وروسيا للأسلحة الفرط صوتية وتوظيفها في الصراع السيبراني سيؤثر سلبياً في كل من الاستقرار الاستراتيجي والميزة التنافسية للجيش الامريكي ويفضي الى الاختلال في التوازن الاستراتيجي القائم بين الولايات المتحدة والقوى الدولية، وينتقص من القدرة الامريكية على الردع تجاه هذه القوى.

8- افضى تراجع سيادة الدولة مع تصاعد دور الفاعلين من غير الدول في العلاقات الدولية الى فرض تحديات عديدة في الحفاظ على الامن السيبراني العالمي، ودفع ذلك الى تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني.

Conclusion:

The study aimed to monitor and analyze the issue of cyber threats and their implications on the strategic interests of the United States of America in cyberspace. It then analyzed the U.S. national cyber strategies formulated by successive administrations to confront these threats and protect U.S. national security.

Regarding the main research question and sub-questions, as well as the verification of the study's hypotheses, the research revealed that cyberspace has gained significant importance in the U.S. strategic mindset due to the heavy reliance of both civil and military infrastructures on cyberspace. This has led to strategic interests closely tied to national security. As a result of this interconnectedness, the United States faces numerous threats and risks originating from cyberspace. The nature of cyber threats has evolved from website breaches to the theft of economic and military information, as well as the leakage of political documents and the infiltration of military systems.

The study identified that one of the most significant cyber threats to U.S. national security is the continuous exposure to data and military information theft or manipulation, as well as the

hijacking of air defense and aviation systems. This is particularly critical as U.S. military institutions, satellite management, defense industries, nuclear submarines, air defense, and aviation systems are all interconnected with modern electronic systems.

Furthermore, the study emphasized that cyberspace has become another arena for projecting power, exercising influence, achieving superiority, and engaging in international competition. Traditional weapons and weapons of mass destruction are no longer the sole measure of power after the information revolution. Information and communication technology has introduced new types of weapons that can lead to victory and success in battles, transcending geographical boundaries and reducing human and material losses. This continuous nature of cyber warfare blurs the lines between peace and war and creates a dangerous state of instability.

The study also highlighted clear shifts in the U.S. strategic approach towards cyberspace due to global dominance. The pursuit of maintaining strategic balance and regional and global influence motivated the U.S. to continue its cyber hegemony. Consequently, U.S. cyber strategies have diversified between offensive and defensive postures under successive administrations, with President Donald Trump's announcement of establishing a new military branch in space marking a significant turning point in this regard.

In this context, the United States has been working to enhance its defensive and offensive capabilities in cyberspace to counter competitive powers, particularly in 2022. President Joe Biden's administration allocated nearly $\$1.3$ billion to programs of the U.S. Space Force and the Space Development Agency to develop technology managed by the Space Force and to finance the cyberspace domain, in addition to dedicating funds to an extra satellite for the Global Positioning System to confront cyber threats from competing powers, especially China and Russia.

The study resulted in several findings, including the following:

1. The U.S. dominance over cyberspace and its utilization as a means to restrain the emerging strategies of competing powers occupies a very prominent position in the U.S. strategic

agenda, especially during the terms of Presidents Barack Obama, Donald Trump, and Joe Biden.

2. The ability to carry out cyber attacks has become a strategic tool of control and influence during peacetime and wartime.

3. The U.S. project of forming a Space Force involves a practical and serious trend towards militarizing and arming space.

4. The militarization of space has contributed to an escalation in the cyber arms race, leading to the adoption of various defensive and offensive cyber strategies by U.S. cybersecurity entities.

5. Cyber threats and risks will be the future conflict scene in regional and international strategic environments in terms of competition and conflict by dominant powers in the international system and aspiring regional powers seeking to establish themselves in the cyberspace strategic environment.

6. The U.S. cyber strategy competes and clashes with international and regional strategies that seek to break free from U.S. dominance, such as China, Russia, Germany, North Korea, and others, hinting at a future cyberwar.

7. The possession and utilization of hypersonic weapons by other powers, especially China and Russia, in cyber conflict will negatively impact both strategic stability and the competitive advantage of the U.S. military, leading to an imbalance in the strategic equilibrium between the United States and other international powers and diminishing U.S. deterrence capabilities towards these forces.

8.The decline of state sovereignty and the increasing role of non-state actors in international relations have led to numerous challenges in maintaining global cybersecurity. This has prompted the need for enhancing international cooperation in securing cyberspace.

المصادر

المصادر العربية

أَولاً : الكتُب العربية والمُترجمة

1. إبراهيم نصر الدين، **حال الأُمة العربية2014–2015: الإعصار مِن تغيير النظُم إلى تفكُك الدول**، (بيروت: مركز دِراسات الوحدة العربية،2015).

2. أَحمد الخولي، **الدور الاجتماعي وأَثرهُ في تاريخ إيران الحديث1900–2000**، (القاهِرة: دار النهضة العربية،2011).

3. أحمد حسين، **قراءة في استراتيجيات حزب الله صراع الأيديولوجيات والتحالُفات الإقليمية**، (إسطنبول: مركز الفكر الاستراتيجي للدِراسات،2018).

4. أَحمد سعيد نوفل(وآخرون)، **التداعيات الجيوستراتيجية للثورات العربية**، (الدوحة: المركز العربي للأَبحاث ودِراسة السياسات، 2014).

5. براجا خانا، **العالم الثاني: السلطة والسطوة في النِظام العالمي الجديد**، ترجمة: دار الترجمة، (بيروت: الدار العربية للعلوم ناشرون،2009).

6. بشير نصر الله(وآخرون)،**أَهم مراكز النفوذ الإيراني غير العسكري في سوريا**، (إسطنبول: مؤَسسة جسور للدِراسات،2021).

7. بهاء أَبو كروم، **المُمانعة وتحدي الربيع: عوائق الديمقراطية والصِراع على الدور الاقليمي**،ط1، (بيروت: دار الساقي،2013).

8. بهاء عدنان السعبري، **الاستراتيجية الأَمريكية تجاه ايران بعد احداث 11 أَيلول عام2001**، ط1، (بغداد: مركز حمورابي للبحوث والدِراسات الاستراتيجية،2012).

9. توماس ليونديمان، **الخطاب الداخلي في إيران والتحديات الأَمنية الحقيقية**، سلسِلة مُحاضرات الإمارات(179)، (أَبو ظبي: مركز الإمارات للدِراسات والبحوث الاستراتيجية،2014).

10. جوزيف س. ناي، **القوة الناعِمة: وسيلة النجاح في السياسة الدولية**، ط2، ترجمة محمد توفيق البجيرمي، (الرياض: العبيكان للنشر،2012).

11. حميد بارسا نيا، **الخريطة الفكرية الإيرانية عشية الثورة: دِراسة اجتماعية معرفية**، تعريب: خليل زامل العصامي، (بيروت: مركز الحضارة لتنمية الفكر الإسلامي،2012).

12. خالد المعيني، **كي لا تُسرق الثورات: دِراسة موضوعية في ثورات الربيع العربي**،(بيروت: منشورات ضِفاف،2014).

13. راشد أَحمد الحنيطي، **حركة أَنصار الله الحوثية والتمدُد الإيراني في منطقة الخليج العربي**، (عمان: دار زهران للنشر والتوزيع،2017).

14. راي تقيه، **إيران الخفية**، ترجمة: ايهم الصباغ، (الرياض: مكتبة العبيكان للنشر،2010).

15. رمضان علي فاضل، **المُخابرات الإيرانية: إيران بين الحرس الثوري والسافاك**، (القاهِرة: مكتبة النافِذة،2014).

16. روبرت كابلان، **انتِقام الجُغرافية**، ترجمة: إيهاب عبد الرحيم علي، سلسِلة عالم المعرفة(420)، (الكويت: المجلس الوطني للثقافة والفنون والآداب،2015).

17. روجر هاورد، **نفط إيران ودورهُ في تحدي نفوذ الولايات المُتحدة**، (بيروت: الدار العربية للعلوم ناشرون،2007).

18.زينة عبد الأَمير الشمري، **اتجاهات بِناء استراتيجية القوة الإيرانية وديناميكيتاها الإقليمية**،(بغداد: دار انكي،2020).
19.ستيفان لاربي وعلي رضا نادر، **العلاقات التُركية الإيرانية في شرق أَوسط بات مُتغيراً**، (نيويورك: مؤَسسة راند الأَمريكية، 2013).
20.سماح عبد الصبور عبد الحي، **القوة الذكية في السياسة الخارجية: دِراسة في أَدوات السياسة الخارجية الأَمريكية تجاه إِيران2005–2013**، (مصر: دار البشير للثقافة والعلوم،2014).
21.طلال عتريسي، الأَهداف والمصالح الإِيرانية في النِظام العربي بعد الثورات، في: مجموعة باحثين، **التداعيات الجيواستراتيجية للثورات العربية**، (الدوحة: المركز العربي للأَبحاث ودِراسة السياسات،2014).
22.طلال عتريسي، **الجمهورية الصعبة: إِيران في تحوّلاتها الداخلية وسياساتها الاقليمية**،(بيروت: دار الساقي للنشر،2018).
23.عاتق جار الله، **النفوذ الإِيراني في اليمن والفرص الموهوبة**،(اسطنبول: مركز الفكر الاستراتيجي،2018).
24.عرفات علي جرغون، **قطر وتغيُر السياسة الخارجية (حُلفاء.. أَعداء)**، (القاهِرة: العربي للنشر والتوزيع،2016).
25.عزمي بشارة ومحجوب الزويري(مُحرِران)، **العرب وإِيران: مُراجعة في التاريخ والسياسة**، ط1، (قطر: المركز العربي للأَبحاث ودِراسة السياسات،2012).
26.علي زياد العلي، **أَمن الخليج في ظل التضارُبات الاستراتيجية للقوى العالمية والاقليمية**،(عمان: دار أَمجد،2016).
27.عمار مرعي الحسن، **التنافُس التُركي الإِيراني للسيطرة على العِراق بعد عام2003 : من يرث الرجل المريض تُركيا العثمانية أَم إِيران الفارسية؟**، (بغداد: دار الكتُب العلمية،2014).
28.عمر كامل حسن،**المجالات الحيوية الشرق أَوسطية في الاستراتيجية الإِيرانية**،(بيروت:الدار العربية للعلوم ناشرون،2015).
29.غوين داير، **فوبيا داعش وأَخواتها**، ترجمة: رامي طوقان، (بيروت: الدار العربية للعلوم ناشِرون،2015).
30.فِراس عباس هاشم وعلي حسين حميد، **ارتدادات الجيوبولتيكا: الدلالات النظرية الموجهة لمسارات التأَثير الإِيراني في الشرق الأَوسط**، (القاهِرة: المكتب العربي للمعارف،2020).
31.فراس عباس هاشم، **النفوذ المُتعاظم: إِيران وأَعباء التفكير الاستراتيجي حيال الصعود الاقليمي**، (بغداد: دار سطور للنشر والتوزيع،2015).
32.كارين أ. منغست وايفان م.اريغون، **مبادئ العلاقات الدولية**، ترجمة: حُسام الدين خضور،(دِمشق: دار الفرقد،2013).
33.كتيلين تالماج، **وقت الإِغلاق والتهديد الإِيراني لِمُضيق هرمز**، دِراسات عالمية، العدد83، (أَبو ظبي: مركز الإِمارات للدراسات والبحوث الاستراتيجية،2009).
34.مايكل هورويتس، **انتِشار القوة العسكرية**، (أَبو ظبي: مركز الإِمارات للدِراسات والبحوث الاستراتيجية،2013).
35.مجموعة مِن المؤَلفين، **تقرير القوى الداخلية في المُجتمع الإِيراني**، (إِسطنبول: المعهد المصري للدِراسات، تشرين الأَول 2015).
36.مجموعة مؤلفين، **القوة الناعِمة في المنطقة العربية (السعودية، تُركيا، إِيران): دِراسة في الاستراتيجيات والتأَثير**، (إِسطنبول: مركز الفكر الاستراتيجي للدِراسات،2018).
37.محمد الأَحمري، **العلاقات العربية الإِيرانية في منطقة الخليج العربي**،(قطر: مُنتدى العلاقات العربية والدولية،2015).

38 .محمد السعيد عبد المؤمن، **الجمهورية الثالِثة في إيران**، (القاهِرة: الهيئة المصرية العامة للكِتاب،2012).

39 .مدحت أَحمد حماد، **الرؤَية الإيرانية لِمحاور الصِراع العربي–الإسرائيلي**،(القاهِرة: مركز البحوث والدِراسات السياسية،2001).

40 .منصور أَبو كريم، **الموقف الدولي والاقليمي مِن الأَزمة القطرية**، (فلسطين: مركز رؤَية للدِراسات الاستراتيجية،2017).

41 .منهل الهام عبدال عقراوي (واخرون)، **العلاقات التُركية–الإيرانية: دِراسة في العلاقات السياسية والاقتصادية**، (عمان: دار غيداء للنشر والتوزيع،2014).

42 .مهدي نور الدين، **الحِصار المُتبادل: العلاقات الإيرانية–الأَمريكية بعد احتلال العِراق**، (بيروت: مركز الحضارة لتنمية الفكر الإسلامي، 2012).

43 .ناصر التميمي، **الأَزمة الخليجية وتداعياتها على مُستقبل مجلس التعاون**،(الدوحة: مركز الجزيرة للدِراسات،2017).

44 .نجلاء مكاوي(وآخرون)، **الاستراتيجية الإيرانية في الخليج العربي**،(بيروت: مركز صِناعة الفكر للدِراسات،2015).

45 .نعيم قاسم، حزب الله : **المِنهاج والتجرِبُة والمُستقبل**، (بيروت: دار الهادي للنشر،2002).

46 .وضاح شرارة، **طوق العمامة: الدولة الإيرانية الخُمينية في مُعترك المذاهب والطوائف**، (لندن: رياض الريس للكتُب والنشر، 2013).

47 .وليد خالد المبيض وجورج شكري كتن، **خيارات إيران المُعاصِرة (تغريب...اسلمة...ديمقراطية)**، ط1، (دمشق: منشورات دار علاء الدين،2002).

48 .ياسر عبد الحسين، **السياسة الخارجية الإيرانية: مُستقبل السياسة في عهد الرئيس حسن روحاني**، ط1، (بيروت: شرِكة المطبوعات للنشر،2015).

ثانياً: البحوث والدِراسات

1. أَحمد أَمين الشجاع، "بعد الثورة الشعبية اليمنية: إيران والحوثيين: مراجع ومواجع"، **مجلة البيان**، العدد175، (الرياض: مركز البحوث والدِراسات،2012).

2. انتوني كوردسمان، "دروس أَولية بين إسرائيل وحزب الله"، **مجلة المُستقبل العربي**، العدد331، (بيروت: مركز دِراسات الوحدة العربية، أَيلول/سبتمبر 2006).

3. حُسام سويلم، "التقييم الأَمريكي للقوة العسكرية الإيرانية"، **مُختارات إيرانية**، العدد127، (القاهِرة: مركز الأَهرام للدراسات السياسية والاستراتيجية، شباط/ فبراير 2011).

4. حُسام عيتاني، "إيران مِن تصدير الثورة إلى حماية الدولة"، **مجلة آفاق المُستقبل**، العدد6، (أَبو ظبي: مركز الإمارات للدِراسات والبحوث الاستراتيجية،2020).

5. رانيا مكرم، "الاستراتيجية الإيرانية في اليمن: حِسابات المكسب والخسارة"، **مجلة السياسة الدولية**، العدد201، (القاهِرة: مركز الأَهرام للدِراسات السياسية والاستراتيجية، تموز/يوليو2015).

6. زهرة الثابت، "القوة الإيرانية الثقافية وتأَثيراتها على الهوية العِراقية"، **مجلة مدارات إيرانية**، العدد7، (برلين: المركز الديمقراطي العربي، اذار/ مارس2020).

7. صافيناز محمد أَحمد، "تقاطُعات سوريا والسعودية في لُبنان والعِراق"، **مجلة السياسة الدولية**، العدد183، (القاهِرة: مركز الأَهرام للدِراسات السياسية والاستراتيجية، كانون الثاني/يناير 2011).

8. عبد الوهاب بدرخان، "كيف أَصبحت حلب مركزاً للصِراعات الاقليمية ونقطة للمواجهة بين الدول الكُبرى؟"، **مجلة شؤون عربية**، العدد168، (القاهِرة: الأَمانة العامة لجامِعة الدول العربية،2016).

9. علاء عبد الوهاب، "توظيف العامل الديني في سياسة إيران الإقليمية بعد عام2003"، **مجلة قضايا سياسية**، العدد53، (بغداد: كُلية العلوم السياسية، جامِعة النهرين،2018).

10. علي محمد حسين، "التنافُس الاقليمي والدولي في منطقة آسيا الوسطى والإسلامية (إيران وتُركيا نموذجاً)"، **مجلة دِراسات دولية**، العدد34، (بغداد: مركز الدِراسات الدولية، جامِعة بغداد،2007).

11. فكرت نامق عبد الفتاح وكرار نوري ناصر، "العِراق وتنظيم داعش: دِراسة في الأَسباب المُنشئة للإِرهاب"، **مجلة قضايا سياسية**، العدد41 (بغداد: كُلية العلوم السياسية، جامِعة النهرين،2015).

12. مُثنى العُبيدي، "نمط التأَثير: التوافق والتناقض بين التحالُف الرُباعي والعِراق"، **مجلة شؤَون تُركية**، العدد3، (القاهِرة: مركز الأَهرام للدِراسات السياسية والاستراتيجية،2016).

13. مُثنى فائق مرعي، "العلاقات الروسية– التُركية والتحالُفات الدولية الراهِنة في الشرق الأَوسط: دِراسة في التأَثير والتأَثر"، **مجلة تكريت للعلوم السياسية**، العدد11، (تكريت: كُلية العلوم السياسية، جامِعة تكريت،2017).

14. محمد السعيد عبد المؤمن، "إيران ومحاولات استِعادة الحلم الإمبراطوري"، **مجلة السياسة الدولية**، العدد201، (القاهِرة: مركز الأَهرام للدِراسات السياسية والاستراتيجية، تموز/ يوليو2015).

ثالثاً : الرسائل والاطاريح العلمية

1. حمدان عبد الله عمران، **السياسة الخارجية الإيرانية تجاه حركة المقاومة الإسلامية حماس2006–2013**، رِسالة ماجستير غير منشورة، (غزة: أَكاديمية الدِراسات العُليا، جامِعة الأَقصى،2014).

2. سلام جِهاد حسين علي، **الفكر الاستراتيجي للقوى الاقليمية اتجاه منطقة الشرق الأَوسط: إِيران وتُركيا أَنموذجاً**، رِسالة ماجستير غير منشورة، (الموصل: كُلية العلوم السياسية، جامِعة الموصل،2022).

رابعاً : التقارير

1. التقرير الاستراتيجي السنوي، **إِيران في2017**، (الرياض: مركز الخليج العربي للدِراسات الإِيرانية،2017).

2. التقرير الاستراتيجي السوري، **تعاون إِيراني– كُردي ضد تُركيا**، المرصد الاستراتيجي، العدد34، (لندن:2017).

3. تقرير الحالة الإِيرانية،**تقليص الدور الإِيراني في الأَزمة السورية**،(الرياض: مركز الخليج العربي للدِراسات الإِيرانية، 2017).

4. حسنين توفيق إِبراهيم، **تقرير الخليج في عام2016/2015: خرائط التحديات والمُبادرات والتحالفُات**، (جدة: مركز الخليج للأَبحاث المعرفة للجميع،2016).

5. سقراط العلو، **تقرير** "الصِراع على الثروة السورية بين إِيران وروسيا: الفوسفات أَنموذجاً"، (الدوحة: مركز الجزيرة للدِراسات، تموز/ يوليو2018).

خامِساً: شبكة المعلومات العالمية (الانترنت)

1.Seyed Ali Alavi, Irans connections with Syria, current status and future perspective, Nawa, 20 June2014. https://www.opendemocracy.net.

2. رصيف22، الجالية الإِيرانية في دبي: روابط تاريخية وثقل اقتصادي لا يستهان بِه(مقال)، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاح على الرابط: https://raseef22.net/article/24-11-2020

3. عبد الله المدني، التدخُل الإيراني في اليمن ومألات الأَزمة اليمنية (مقالة)، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاحة على الرابط: https://www.alarabiya.net/ar/mol

4. عدنان هاشم، التدخل الإيراني في اليمن: حقائقه وأَهدافهُ ووسائلهُ (بحث)، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاح على الرابط: https://www.marsadpress.net

5. العربي، ارتفاع حجم التبادُل التجاري بين إيران والإمارات إلى20 مليار دولار رغم الخِلافات(مقالة)، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاحة على الرابط: https://www.alaraby.co.uk/economy/16-06-2021.

6. علي حسين باكير، إيران ومُرتكزات القوة: اكتِشاف القوة الناعِمة الإيرانية (مقالة)، مركز الجزيرة للدِراسات، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاحة على الرابط: https://www.studies.aljazeera.net.17-04-2013

7. وكالة DW الإخبارية، إيران والعِراق: تبادُل تجاري بالمليارات(مقالة)، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاحة على الرابط: https://www.dw.com./ar.2017

8. اليوم السابع، حلال على حزب الله حرام على الإيرانيين(بحث)، نقلاً عن شبكة المعلومات العالمية (الانترنت)، مُتاح على الرابط: https://www.youm7.com/story/2018/1/4

Arabic sources:

First: Arabic and translated books:

1. Ibrahim Nasreddin, The State of the Arab Nation 2014-2015: The Hurricane From Changing Regimes to Disintegrating States, (Beirut: Center for Arab Unity Studies, 2015).
2. Ahmed Al-Khouli, The Social Role and Its Impact on the Modern History of Iran 1900-2000, (Cairo: Arab Renaissance House, 2011).
3. Ahmed Hussein, A Reading of Hezbollah's Strategies, the Conflict of Ideologies and Regional Alliances, (Istanbul: Center for Strategic Thought for Studies, 2018).
4. Ahmed Saeed Nofal (and others), The Geostrategic Implications of the Arab Revolutions, (Doha: Arab Center for Research and Policy Studies, 2014).
5. Praga Khanna, The Second World: Power and Power in the New World Order, translation: Dar Al-Tarjamah, (Beirut: Arab House for Science Publishers, 2009).
6. Bashir Nasrallah (and others), the most important centers of Iranian non-military influence in Syria (Istanbul: Bridges Institute for Studies, 2021).
7. Baha Abu Kroum, Rejection and the Challenge of Spring: Obstacles to Democracy and the Conflict Over the Regional Role, 1st edition, (Beirut: Dar Al-Saqi, 2013).
8. Bahaa Adnan Al-Sabri, The American Strategy towards Iran after the events of September 11, 2001, 1st edition, (Baghdad: Hammurabi Center for Research and Strategic Studies, 2012).
9. Thomas Lindemann, Internal Discourse in Iran and Real Security Challenges, Emirates Lecture Series (179), (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2014).
10. Joseph S. Nay, Soft Power: The Means of Success in International Politics, 2nd Edition, translated by Muhammad Tawfiq Al-Bujerami, (Riyadh: Obeikan Publishing, 2012).

11. Hamid Parsa Nia, The Iranian Intellectual Map on the Eve of the Revolution: A Social Cognitive Study, Arabization: Khalil Zamil Al-Assami, (Beirut: Civilization Center for the Development of Islamic Thought, 2012).
12. Khaled Al-Muaini, In order not to steal revolutions: an objective study in the Arab Spring revolutions, (Beirut: Difaf Publications, 2014).
13. Rashid Ahmed Al-Hunaiti, Ansar Allah Houthi Movement and Iranian Expansion in the Arabian Gulf Region, (Amman: Dar Zahran for Publishing and Distribution, 2017).
14. Ray Taqih, Hidden Iran, translated by: Ayham Al-Sabbagh, (Riyadh: Obeikan Bookshop for Publishing, 2010).
15. Ramadan Ali Fadel, Iranian Intelligence: Iran between the Revolutionary Guards and the SAVAK, (Cairo: Al-Nafizah Library, 2014).
16. Robert Kaplan, The Revenge of Geography, translated by: Ihab Abdel Rahim Ali, The World of Knowledge Series (420), (Kuwait: National Council for Culture, Arts and Literature, 2015).
17. Roger Howard, Iran's oil and its role in challenging the influence of the United States, (Beirut: Arab House of Science Publishers, 2007).
18. Zina Abdul-Amir Al-Shammari, Directions for Building the Iranian Power Strategy and Its Regional Dynamics, (Baghdad: Anki House, 2020).
19. Stephane Larbe and Ali Reza Nader, Turkish-Iranian Relations in a Changing Middle East (New York: RAND Corporation, 2013).
20. Samah Abdel-Sabour Abdel-Hay, Smart Power in Foreign Policy: A Study in the Tools of US Foreign Policy towards Iran 2005-2013, (Egypt: Dar Al-Bashir for Culture and Science, 2014).
21. Talal Atrisi, Iranian goals and interests in the Arab system after the revolutions, in: A group of researchers, the geostrategic repercussions of the Arab revolutions, (Doha: Arab Center for Research and Policy Studies, 2014).
22. Talal Atrissi, The Difficult Republic: Iran in Its Internal Transformations and Regional Policies, (Beirut: Dar Al Saqi Publishing, 2018).
23. Itiq Jarallah, Iranian influence in Yemen and the gifted opportunities, (Istanbul: Center for Strategic Thought, 2018).
24. Arafat Ali Jargon, Qatar and the Change of Foreign Policy (Allies... Enemies), (Cairo: Al Arabi for Publishing and Distribution, 2016).
25. Azmi Bishara and Mahjoub Al-Zweiri (Editors), The Arabs and Iran: A Review of History and Politics, 1st Edition, (Qatar: The Arab Center for Research and Policy Studies, 2012).
26. Ali Ziyad Al-Ali, Gulf Security in Light of the Strategic Conflicts of Global and Regional Powers, (Amman: Dar Amjad, 2016).
27. Ammar Mari al-Hassan, Turkish-Iranian competition for control of Iraq after 2003: Who will inherit the sick man, Ottoman Turkey or Persian Iran?, (Baghdad: Dar al-Kutub al-Ilmiya, 2014).
28. Omar Kamel Hassan, Middle Eastern Vital Areas in Iranian Strategy, (Beirut: Arab House for Science Publishers, 2015).

29. Gwen Dyer, ISIS phobia and its sisters, translated by: Rami Touqan, (Beirut: Arab House for Science Publishers, 2015).
30. Firas Abbas Hashim and Ali Hussein Hamid, Geopolitics Repercussions: Theoretical Indications Directing the Paths of Iranian Influence in the Middle East, (Cairo: The Arab Bureau of Knowledge, 2020).
31. Firas Abbas Hashim, The Growing Influence: Iran and the Burdens of Strategic Thinking Regarding the Regional Rise, (Baghdad: Dar Sotoor for Publishing and Distribution, 2015).
32. Karen A. Mengust and Evan M. Erigon, Principles of International Relations, translated by: Hossam El-Din Khaddour, (Damascus: Dar Al-Farqad, 2013).
33. Katilin Talmag, The Time of the Iranian Closure and Threat to the Strait of Hormuz, International Studies, No. 83, (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2009).
34. Michael Horowitz, The Spread of Military Power, (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2013).
35. A group of authors, Report on Internal Forces in Iranian Society (Istanbul: Egyptian Institute for Studies, October 2015).
36. A group of authors, Soft Power in the Arab Region (Saudi Arabia, Turkey, Iran): A Study in Strategies and Influence, (Istanbul: Strategic Thought Center for Studies, 2018).
37. Muhammad Al-Ahmari, Arab-Iranian Relations in the Persian Gulf Region, (Qatar: Forum on Arab and International Relations, 2015).
38. Muhammad Al-Saeed Abdel-Moamen, The Third Republic in Iran, (Cairo: The Egyptian General Book Organization, 20 12).
39. Medhat Ahmed Hammad, The Iranian Vision of the Arab-Israeli Conflict Axes, (Cairo: Center for Research and Political Studies, 2001).
40. Mansour Abu Karim, The International and Regional Position on the Qatar Crisis, (Palestine: Vision Center for Strategic Studies, 2017).
41. Manhal Elham Abdul Aqrawi (and others), Turkish-Iranian Relations: A Study in Political and Economic Relations, (Amman: Dar Ghaida for Publishing and Distribution, 2014).
42. Mahdi Noureddine, Mutual Siege: Iranian-American Relations After the Occupation of Iraq, (Beirut: Civilization Center for the Development of Islamic Thought, 2012).
43. Nasser Al-Tamimi, The Gulf Crisis and its Repercussions on the Future of the Cooperation Council, (Doha: Al Jazeera Center for Studies, 2017).
44. Naglaa Makkawi (and others), The Iranian Strategy in the Arabian Gulf, (Beirut: Thought Industry Center for Studies, 2015).
45. Naim Qassem, Hezbollah: The Platform, the Experience and the Future, (Beirut: Dar Al-Hadi for Publishing, 2002).
46. Waddah Sharara, The Turban Collar: The Khomeinist Iranian State in the Battle of Doctrines and Sects, (London: Riyad Al-Rayes for Books and Publishing, 2013).

47. Walid Khaled Al-Mubayed and George Shukri Kitten, Options for Contemporary Iran (Westernization... Islamization... Democracy), 1st edition, (Damascus: Aladdin House Publications, 2002).
48. Yasser Abdel-Hussein, Iranian Foreign Policy: The Future of Politics under President Hassan Rouhani, 1st Edition, (Beirut: Publications Publishing Company, 2015).

Second: Research and studies

1.Ahmed Amin Al-Shuja', "After the Right-wing Popular Revolution: Iran and the Houthis: References and References," Al-Bayan Magazine, Issue 175, (Riyadh: Center for Research and Studies, 2012).
2.Anthony Cordesman, "Initial Lessons Between Israel and Hezbollah," Al-Mustaqbal Al-Arabi, Issue 331 (Beirut: Center for Arab Unity Studies, September 2006).
3.Hossam Sweilem, "The American Assessment of Iranian Military Power," Iranian Anthology, No. 127 (Cairo: Al-Ahram Center for Political and Strategic Studies, February 2011).
4.Hossam Itani, "Iran from Exporting the Revolution to Protecting the State," Future Horizons Magazine, Issue 6, (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2020).
5.Rania Makram, "The Iranian Strategy in Yemen: Calculations of Gain and Loss," International Policy Journal, Issue 201, (Cairo: Al-Ahram Center for Political and Strategic Studies, July 2015).
6.Zahra Al Thabit, "Iranian Cultural Power and Its Effects on Iraqi Identity," Iranian Orbits Magazine, Issue 7, (Berlin: Arab Democratic Center, March 2020).
7.Safinaz Mohamed Ahmed, "The Intersections of Syria and Saudi Arabia in Lebanon and Iraq," International Policy Journal, Issue 183, (Cairo: Al-Ahram Center for Political and Strategic Studies, January 2011).
8.Abd al-Wahhab Badrakhan, "How did Aleppo become a center of regional conflicts and a point of confrontation between the major powers?", Arab Affairs Magazine, No. 168, (Cairo: General Secretariat of the League of Arab States, 2016).
9.Alaa Abdel Wahhab, "Employment of the Religious Factor in Iran's Regional Policy after 2003," Journal of Political Issues, Issue 53, (Baghdad: College of Political Science, Al-Nahrain University, 2018).
10. Ali Muhammad Hussein, "Regional and International Competition in Central and Islamic Asia (Iran and Turkey as a Model)", Journal of International Studies, No. 34, (Baghdad: Center for International Studies, University of Baghdad, 2007).
11. Fikret Namik Abdel-Fattah and Karrar Nuri Nasser, "Iraq and ISIS: A Study of the Roots of Terrorism," Journal of Political Issues, No. 41 (Baghdad: College of Political Science, Al-Nahrain University, 2015).
9.Merei, Proof Muthanna Faeq. "Cyberspace Institutions in the Middle East: Iran and Israel as a model." *Tikrit Journal for Political Science* 4.30 (2022).
12. Muthanna Al-Obaidi, "Pattern of Influence: Compatibility and Contradictory Between the Quadruple Alliance and Iraq," Turkish Affairs Magazine, Issue 3, (Cairo: Al-Ahram Center for Political and Strategic Studies, 2016).

13. Muthanna Faiq Merhi, “Russian-Turkish Relations and Current International Alliances in the Middle East: A Study of Influence and Being Impacted,” Tikrit Journal of Political Science, Issue 11, (Tikrit: College of Political Science, University of Tikrit, 2017).
14. Muhammad Al-Saeed Abdel-Moamen, “Iran and Attempts to Restore the Imperial Dream,” International Politics Journal, Issue 201, (Cairo: Al-Ahram Center for Political and Strategic Studies, July 2015).

Third: Theses and scientific treatises:

1. Hamdan Abdullah Omran, Iranian Foreign Policy towards the Islamic Resistance Movement Hamas 2006-2013, an unpublished master's thesis, (Gaza: Graduate Studies Academy, Al-Aqsa University, 2014).
2. Salam Jihad Hussein Ali, The Strategic Thought of Regional Powers Towards the Middle East Region: Iran and Turkey as a Model, Unpublished Master's Thesis, (Mosul: College of Political Science, University of Mosul, 2022).

Fourth: Reports

1. Annual Strategic Report, Iran in 2017, (Riyadh: Arabian Gulf Center for Iranian Studies, 2017).
2. The Syrian Strategic Report, Iranian-Kurdish cooperation against Turkey, Strategic Observatory, Issue 34, (London: 2017).
3. Report of the Iranian case, reducing the Iranian role in the Syrian crisis, (Riyadh: Arab Gulf Center for Iranian Studies, 2017).
4. Hassanein Tawfiq Ibrahim, The Gulf Report in 2015/2016: Maps of Challenges, Initiatives and Alliances, (Jeddah: Gulf Center for Research Knowledge for All, 2016).
5. Socrates Al-Alou, “The Conflict Over Syrian Wealth Between Iran and Russia: Phosphate as a Case” report (Doha: Al-Jazeera Center for Studies, July 2018).

Fifth: the global information network (the Internet)

1. Seyed Ali Alavi, Iran’s connections with Syria, current status and future perspective, Nawa, 20 June 2014. https://www.opendemocracy.net.
2. Raseef22, The Iranian Community in Dubai: Historical Ties and Economic Weight.

The foreign sources

First: Books

1. Anthony H. Cordesman, Iran's Support of the Hezbollah in Lebanon, (Washington: Center for Strategic and international Studies, 2006).

Second: Research and studies

1. Chuck Freilich, "Speaking About the Unspeakable: Us-Israeli Dialogue on Iran's Nuclear Programme", Policy Focus, No.77, (U.S.A: the Washington Institute for Near East Policy, 2007).
2. Duane Chapman and Neha Khanna, "The Fourth Gulf War: Persian Gulf Oil Global Security", Working Paper, No.501, (New York: Binghamton University, December 2004).
3. Joseph S. Nye, Smart Power and the War on Terror: Asia-Pacific Review, Vol.15, 2008.
4. Nader Ibrahim M. Bin Nasur, "Syria-Iran Relations (2002-2014)", International Journal of Humanities and Social Science, Vol.4, (2014).

Third: Reports

1. Bijan Khajehpour, Anatomy of the Iranian Economy (Report), No 6, (Stockholm: The Swedish Institute of International Affairs (SIIA), April/2020).

Fourth: Internet

1. Mahdi Darius Nazemroaya, Are Syria and Pakistan Pieces of the puzzle for Assembling a mega Gas Pipeline to China? April 2013. http://www.globalresearch.ca.