: https://doi.org/10.25130/tjfps.v1i38.484

TJFPS

38

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

" الامن السيبراني وتأثيره في مستقبل الهيمنة الامريكية "

" Cybersecurity and its Impact on the Future of American Hegemony "

Ali Mohammed Amneef Al-Rufaie [a]
Nahrain University - College of Political Science [a]

م.د. علي محمد أمنيف الرفيعي * [a]
جامعة النهرين – كلية العلوم السياسية

Article info.

Article history:
- Received 08 Jan..2025
-Received in revised form 26. Jan .2025
- Final Proofreading 14 Feb. 2025
- Accepted 23. Feb 2025
- Available online: 31. March .2025

Keywords:
- Cybersecurity.
- American Hegemony.
- strategy.
- transformations& threats

Abstract: The qualifications possessed by the United States of America in the field of cybersecurity are an important foundation upon which the American decision-maker relies in achieving the goals of the National Security Strategy according to the strategic perception, in a way that made the United States of America work to manage this force within a purposeful framework that seeks to use the resources of some countries of the world to its advantage and to formulate partnerships with some other countries by adopting the approach of containment, dismantling, and reassembly in a way that suits and achieves American objectives, as artificial intelligence is one of the foundations of cybersecurity that has been employed. In electronic warfare, it made a big difference in curbing the capabilities of the opponent, and this is what the American administration seeks to achieve to achieve its ambition for global hegemony and control.

*Corresponding Author: Ali Mohammed Amneef Al-Rufaie ،EMail: ali.m.amnef@nahrainuniv.edu.iq ،Tel: +964 770 802 0989 ، Affiliation: Nahrain University / College of Political Science.

معلومات البحث :

تواريخ البحث:
- الاستلام: 08 كانون الثاني 2025
- بعد التنقيح 26 كانون الثاني 2025
- التدقيق اللغوي 14 شباط 2025
- القبول: 23 شباط 2025
- النشر المباشر: 31 أذار 2025

الكلمات المفتاحية :
- **الامن السيبراني .**
- **الهيمنة الامريكية.**
- **الاستراتيجية.**
- **تحولات و تهديدات.**

الخلاصـــة: تعد المؤهلات التي تمتلكها الولايات المتحدة الامريكية في حقل الامن الســيبراني هي مرتكز مهم يعول عليه صــانع القرار الامريكي في تحقيق الاهداف الاســتراتيجية للامن القومي وفق المدرك الاستراتيجي على النحو الذي جعل الولايات المتحدة الامريكية تعمل على ادارة هذه القوة في إطار اســتراتيجية هادفة تســعى لاســتخدام موارد بعض دول العالم لصــالحها وصــياغة شــراكات مع بعض الدول الاخرى باعتماد نهج الاحتواء والتفكيك وإعادة التركيب بما يتلائم وتحقيق الأهداف الأمريكية اذ يعد الذكاء الاصـــطناعي احد مرتكزات الامن الســـيبراني الذي تم توظيفه في الحرب الالكترونية وشـــكل فارقا كبيرا لكبح قدرات الخصـــم وهذا ما تســـعى الى تحقيقه الادارة الامريكية بضمان الهيمنة والسيطرة العالمية.

مقدمة:

اخذت تنظر الولايات المتحدة الامريكية الى الأمن الألكتروني من أكبر وأكثر التهديدات التي تواجه الأمن القومي الأمريكي في القرن الحادي والعشرين، وهذه التهديدات متأتية من القوى المنافسة لسياسات الولايات المتحدة الامريكية مثل الصين، وكوريا الشمالية، وايران، وهذا يثبت تنافسا دوليا على مستوى الذكاء الاصطناعي والقوة الألكترونية وبالتالي إستخدام هذه الإمكانيات في تنفيذ هيمنتها العالمية واذا ما نظرنا الى الى حجم التحديات التي تواجه الهيمنة الامريكية في هذا المسار فهي كثيرة ليس فقط من قبل الدول المناوئة للسياسات الامريكية انما حتى الدول الحليفة ومنها الاتحاد الاوربي ولكن يبقى التنافس تحت السيطرة بسبب التفوق الامريكي وهذا ما تسعى الى ترسيخه من خلال الامن السيبراني الذي اصبح عنصر مهم من عناصر القوة الامريكية التي تستثمرها لفرض هيمنها العالمية.

أهمية الدراسة:

تكمن اهمية وحيوية الموضوع أن الامن السيبراني يأخذ حيزا مهما على مستوى السياسة الدولية ولها موقع وحضور اكثر من أي وقت مضى لاهميتها في حسم التفوق الامريكي، وتعد الولايات المتحدة الامريكية على رأس الدول التي تتمتع بمقومات تكنولوجية وتقنية والتأثير والنفوذ كما وتكمن اهمية الدراسة في استمرار نهج توظيف الامن السيبراني اكثر فاكثر، لفرض الهيمنة والنفوذ الامريكي، مما يجعل الدراسة تدخل في باب التنظير والتطبيق والاهتمام بمواكبة الاحداث وافرازاتها، ومواكبة احدث النظريات المهمة في العلاقات الدولية ولاسيما نظرية الحرب الالكترونية وصراع الذكاء الاصطناعي.

اشكالية الدراسة

تنطلق اشكالية الدراسة من تساؤلات جوهرية ومهمة منها:

- هل الولايات المتحدة الامريكية نجحت في توظيف مقومات الامن السيبراني لصالح استراتيجيتها في الهيمنة العالمية ؟
- هل هذه المقومات هي ثابتة ام متغيرة حسب المعطيات والظروف التي تمر بها الاستراتيجية الامريكية تجاه الداخل والعالم اجمع؟

فرضية الدراسة:

ان استراتيجية الامن السيبراني للولايات المتحدة الامريكية ليست استراتيجية مؤقتة، فقد عمدت الى استخدام كافة الوسائل للحفاظ على امنها ومصالحها أكثر من أي دولة اخرى وبشكل مستمر خاصة بعد دخول عصر الذكاء الاصطناعي رأس حربة في تحقيق اهداف امنها القومي خدمتا لهيمنتها العالمية.

منهجية البحث:

عمدنا إلى استخدام المنهج التحليلي ومقترب الاستشراف المستقبلي لمستقبل الهيمنة الامريكية من خلال توظيف الامن السيبراني.

هيكلية الدراسة:

فقد تم توزيع الدراسة على مبحثين، فضلاً عن المقدمة والخاتمة.

وقد تضمن المبحث الاول الامن السيبراني (المفهوم والانواع والتأثير)، وقد تم تقسيمه على ثلاثة مطالب، تضمن المطلب الاول مفهوم الامن السيبراني، أما المطلب الثاني فقد تناول انواع الامن السيبراني بينما خصص المطلب الثالث الامن السيبراني والاستقرار (اشكالية التأثر والتأثير)

اما المبحث الثاني فقد تناول الامن السيبراني وسيلة لديمومة الهيمنة وقد تم تقسيمه الى مطلبين، إذ تضمن المطلب الأول الاتفاقيات الدَّولية للامن السيبراني ، أما المطلب الثاني فقد تناول الامن السيبراني مقترب للتفرد والسيطرة.

المبحثُ الأوَّل

الامن السيبراني (المفهوم والانواع والتأثير)

يعد الامن السيبراني من المفاهيم والمصطلحات التي اخذت مساحة مهمة في التأثير على الساحة الدولية ، يرجع تاريخه إلى الثورة التكنولوجية والرقمية ، حيث تم استخدامه بأشكال مختلفة وأدوات متعددة ولأهداف وغايات شتى. وتبعا لتطور الحياة وتوسع الحاجات الإنسانية والاجتماعية، نال استخدام وتوظيف الامن السيبراني تطورا هو الأخر حتى لاح أكثر المستويات وبطرق ومجالات متعددة، بل وأزدادت طرق استخدامه وتأثيره على الصعد والمستويات كافة. في حين تقر لدى الغالبية أن الامن السيبراني هو القدرة على التأثير في سلوك الافراد او الدول تجاه قضايا معينة إذ لم يعد هناك مجال ودور لسيطرة رقابة الأجهزة الحكومية عليها، فقد تجاوزت الحدود الوطنية، وتعدَّت إلى ما فوق القومية، ورُبَّما أخذت اوصافا متعددة سيتم توضيحها من خلال المطالب الثلاث:

المطلب الأوَّل: مفهوم الامن السيبراني

يعرف المختصون أن مصطلح الأمن السيبراني جاء من لفظ السيبر المنقول عن كلمة (Cyber)اللاتينية ومعناها (الفضاء المعلوماتي)، ويعني مصطلح الأمن السيبراني (أمن الفضاء المعلوماتي) من كل جوانبه، وهو عبارة عن تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستخدامات وآليات وتطبيقات وتجهيزات تقنية المعلومات والحاسب الآلي، والترابط فيما بينها من خلال شبكات الحاسب والاتصالات والانترنت[1].

ويعبر الأمن السيبراني عن مصفوفة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات من الاختراقات أو التلف أو التغيير أو تعطل الوصول للمعلومات أو الخدمات، ويعد توجها عالميا سواء على مستوى الدول أو حتى المنظمات الحكومية أو الشركات[2]..

والأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات

---

(1) حيدر علي حسين، **سياسة الولايات المتحدة الأمريكية ومستقبل النظام الدولي** (بغداد: دار الكتب العلمية للطباعه والنشر والتوزيع، 2017) ص279.

([2]) ريتشارد هاس و مارتن أنديك، **ما بعد العراق،إستراتيجية أمريكية جديدة للشرق الأوسط** (بغداد: مركز الدراسات الدولية جامعة بغداد، 2009) ص42.

وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول[1].

ويتضمن الأمن السيبراني أي أنشطة أو أشخاص أو تقنيات تستخدمها مؤسستك لتجنب الحوادث الأمنية أو خروقات البيانات أو فقدان الأنظمة المهمة. إنه الطريقة التي تحمي بها عملك من التهديدات وأنظمة الأمان الخاصة بك من التهديدات الرقمية. على الرغم من أن المصطلح يتم تداوله بشكل عرضي بما فيه الكفاية، إلا أن الأمن السيبراني يجب أن يكون جزءًا لا يتجزأ من عمليات ادارة الاشخاص ومؤسسات الدولة بشكل عام[2].

المطلب الثاني: انواع الامن السيبراني.

هناك العديد من أنواع ومجالات الأمن السيبراني، اذ تعد هذه العملية استراتيجية أساسية ونهجًا تتبعه الدولة ترغب في تأمين أنظمتها وبياناتها ضد الهجمات الإلكترونية التي ازدادت بشدة خلال السنوات الاخيرة وتختلف أنواع الأمن السيبراني وفقًا وللغرض المراد تحقيقه في ظل التطور التكنولوجي السريع والمذهل الذي نشهده الآن، حيث أصبح الأمن السيبراني ذو أهمية اكثر من أي وقت مضى حيث يمكن تقسيمه الى عدة انواع:

اولا: أمن الشبكة

يُعد أمن الشبكة من أبرز عناصر الأمن السيبراني، لأن معظم الهجمات تحدث عبر الشبكة، وهو عبارة عن عملية تتضمن مجموعة من تقنيات البرامج والأجهزة من أجل حماية البيانات من التهديدات ومن الدخول غير المصرح به, ويعمل أمن الشبكة كجدار بين شبكة المؤسسة والأنشطة الضارة، من أجل الاستمرار في تقديم الخدمات وتلبية متطلبات الدولة، وحماية سمعته[3].

ثانيا: أمن المعلومات

---

(1) اشرف محمد كشك، "حلف الناتو: من الشراكة الجديدة إلى التدخل في الازمات العربية"، **مجلة السياسة الدولية**، العدد 88(القاهرة: 2022)، ص ص 22-27.

(2) زياد خلف عبدالله ، "القرصنة التكنولوجية واثرها العلاقات الامريكية – الصينية" ، **مجلة جامعة تكريت للعلوم الانسانية**، العدد 9 (صلاح الدين: 2021)، ص 432.

(3) محمد محمود عمارة ، تاريخ القرصنة الالكترونية بين العبقرية وانتهاك الخصوصية ، شبكة صيد الفوائد ، على الرابط الالكتروني: http://www.Saaid.net/Minute

يُصنف أمن المعلومات بأنه واحدًا من أهم مجالات الأمن السيبراني، وهو عبارة عن عملية تصميم ونشر أدوات لحماية معلومات الأعمال الهامة من التدمير والتعطيل والتعديل.

ويُطبق أمن المعلومات بهدف التأكد من أن المستخدمين المعتمدين أو التطبيقات أو الأنظمة فقط، هم من يمكنهم الوصول إلى معلومات معينة. وهنالك نوعين من أمن المعلومات وهي: الأمن السحابي والذي يركز على نقاط الضعف القادمة من خدمات الإنترنت والبيئات المشتركة لحماية التطبيق وأمن البنية التحتية من المكونات المتصلة بالسحابة[1].

ثالثا: أمن المستخدم النهائي

يُعد المستخدم هو خط الدفاع الأول ضد الهجمات الإلكترونية على الدولة، إذ يمكنه معالجة العديد من المسائل الأمنية ومنعها.

وتُحمى المؤسسات من التعرض لأي نوع من التهديدات الإلكترونية، من خلال المعرفة والتعليم حول أفضل الممارسات الأمنية، في ظل التحول الرقمي الذي نعيشه الآن، والذي جعلن جميع الدول عُرضة للهجمات الإلكترونية بصورة مستمرة.

ويشمل أمن المستخدم النهائي تأمين الأجهزة الفردية مثل أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة والهواتف الذكية، باستخدام برنامج مكافحة الفيروسات، وأنظمة منع التسلل(IPS) ، وتشفير الجهاز، وتحديثات البرامج بشكل منتظم[2].

رابعا: أمن البنية التحتية

من مجالات تكنولوجيا المعلومات أمن البنية التحتية الخاصة بالدولة، إنه إجراء أمني يُتخذ لحماية البنية التحتية الحيوية مثل اتصالات الشبكة أو مركز البيانات أو الخادم أو مركز تكنولوجيا المعلومات، والهدف من تنفيذ هذا الإجراء هو الحد من نقاط ضعف هذه الأنظمة من الفساد أو التخريب أو الإرهاب.

وعلى الدول والمنظمات التي تعتمد على البنية التحتية الحيوية، إدراك جميع الالتزامات المتعلقة بهذا الإجراء، حتى لا يستطيع المهاجمون استهداف أنظمة المرافق الخاصة لمهاجمة مختلف الأعمال[3].

خامسا: أمن الهاتف المحمول

تتعرض الدول ومؤسساتها لتهديدات من التطبيقات الضارة المُحملة على الأجهزة المحمولة مثل الأجهزة اللوحية والهواتف الذكية. ولذلك، فإن أمن الهاتف المحمول من ضمن عناصر الأمن السيبراني، لأنه يتضمن

---

(1) هادي قبيس ، **السياسة الخارجية الامريكية بين مدرستين** (بيروت: الدار العربية للعلوم ، 2023)، ص78.

(2)محمود حجازي، **جرائم الحاسبات والانترنت والجرائم المعلوماتية** (القاهرة: المركز المصري للملكية الفكرية، 2020) ص 12.

(3) هادي قبيس ، **السياسة الخارجية الامريكية بين مدرستين** (بيروت: الدار العربية للعلوم ،2024)،ص 78.

تأمين البيانات التنظيمية والشخصية المُخزنة على الأجهزة المحمولة ضد التهديدات الضارة المختلفة، تلك التهديدات المتمثلة في الوصول غير المصرح به[1].

سادسا: أمن الإنترنيت

يعد أمن الإنترنت من القضايا الحساسة والمهمة التي تمس امن الدولة من خلال حماية تلك الأجهزة باكتشاف وتصنيف الأجهزة المتصلة، والتجزئة التلقائية للتحكم في أنشطة الشبكة التي من الممكن ان تكون معلوماتك متاحة من خلال الاختراق اثناء الارتباط بالشبكة العنكبوتية.

سابعا: أمن التطبيقات

يُعد أمن التطبيقات من أبرز أنواع الأمن السيبراني، لأن تطبيقات الويب المتصلة مباشرة بالإنترنت، تُعتبر دومًا من أهداف القائمون بالهجمات الإلكترونية التي توظف ضد الدول.

ويُستخدم أمان التطبيقات في إيقاف الهجمات، ومنع هجمات الروبوت، وإيقاف أي تفاعل ضار معها، وكل ذلك من خلال ممارسات ترميز آمنة وتحديثات وتصحيحات برنامجية منتظمة، وجدران حماية على مستوى التطبيق[2].

المطلب الثالث: الامن السيبراني والاستقرار (اشكالية التأثر والتأثير)

هنالك علاقة جدلية بين الامن السيبراني والاستقرار ويمكن تحليل هذه العلاقة من خلال الاولويات التي تسعى الدولة الى تحقيقها وهذا يتطلب الى توظيف كامل لعناصر ومقومات الامن السيبراني خدمتا لتحقيق الاستقرار الذي تصبوا اليه الدولة من سياستها العليا ولكافة القطاعات وهنا يمكن تسليط الضوء على اهم تلك القطاعات:

اولا: الاثر السياسي الامني

يبرز هذا الاثر من خلال القيام بعمليات التجسس على الشخصيات السياسية أو تهديدهم بالقتل أو اختراق مؤسسات رسمية وحيوية وايضا التأثير على توجهات الناخبين وتغير النتائج ، وفي هذا السياق هناك عدة حوادث تعرض بعض المراكز العسكرية لجرائم قرصنة معلوماتية بهدف الوصول والحصول على معلومات تكون مخزنة في ذاكرة الحاسبات التي يتم استخدامها في تلك المراكز، ويتمثل ذلك من خلال معلومات العسكرية التي تتعلق بالسفن الحربية للدول من خلال استغلال شبكة الانترنت في تسريب وثائق تحتوي معلومات ووثائق

---

(1) جياكومو بيروسي باولي وآخرون ، **خلف الستار: التجارة غير المشروعة بالأسلحة النارية المتفجرات والذخيرة على الانترنت المظلم**(سانتامونيكا: مؤسسة RAND ، 2022)، ص 9 .

(2) جمال سند السويدي، **آفاق العصر الأمريكي: السيادة والنفوذ في النظام العالمي الجديد** (أبو ظبي: مركز الدراسات الاستراتيجية، 2021) ، ص57.

سرية كشفها موقع " ويكليكس حيث كان لهذه الوثائق دور فاعل لكشف أمور سرية عديدة تخص البنية الاساسية للدولة الامريكية من الناحية السياسية والامنية[1].

ثانيا: الاثر الاقتصادي

يكمن تحديد الاثر الاقتصادي من خلال اختراق النظام المصرفي والحاق الضرر بأعمال البنوك وأسواق الاموال العالمية، والتعرض لعمليات تحويل الاموال. ومن اشهر جرائم سرقة الاموال ما حدث في امارة دبي في العام 2001 ما قام به مهندس حاسبات أسيوي، وقام بالعديد من السرقات المالية واختلاس الاموال من الحسابات الشخصية وتحويل تلك الاموال إلى حسابات وهمية قام هو بتخليقها بالاضافة الى ذلك القرصنة التي قامت بها حساسبات مجهولة للعديد من المشاريع الاقتصادية في الولايات المتحدة الامريكية وغيرها من الدول جعل من النشاط الاقتصادي غير مستقر وغير امن[2].

ثالثا: الاثر الاجتماعي:

تؤثر الاختراقات السيبرانية على حياة الافراد ورفاهيتهم، وتستهدفهم عبر الرسائل المُتعددة للجمهور والافراد وتقوم بترويعها وإرهابها، من خلال جرائم عدة تتمثل في الجرائم التي يتم الوصول إلى الهوية الالكترونية للافراد بطرق غير مشروعة؛ كحسابات البريد الالكتروني وكلمات السر الخاصة بهم وانتحالِ شخصياتهم والسطو على الملفات والصور المهمة في اجهزتهم وتهديهم بها، اضافة إلى النيل من منظومة العلاقات الاجتماعية وتفتيت النسيج الاخلاقي من خلال المساس بالعلاقات الاسرية وذلك بسبب النتائج التي تُخلفها بعض الجرائم السيبرانية ،كالتشهير ببعض أفراد الاسرة ونشر الاخبار الكاذبة والاشاعات، وظهور حالات الاختطاف والتهديد لدفع الفدية[3].

رابعا: اثر التجسس الالكتروني

نعني بالتجسس هو التسلل والاطلاع على معلومات الغير الخاصة والتي لا يتمكن ولا يسمح لاحد الاطلاع عليها .من منطلق انها مؤمنة من خلال ارقام وبصمات سرية ،الا أن الفضاء الالكتروني آثر عليها بشكل قوي من خلال الادوات الاستخبارية والتنصت والتجسس بشكل سري ، وذلك لما للامن والسيبرانية من علاقة قوية أصبحت اداة في خدمته، لتسهيل النشاطات السرية في العلاقات ما بين الدول كعملية الاغتيالات نتيجة

(1) جورج فريدمان، **الإمبراطورية والجمهورية في عالم متغير**، ترجمة: أحمد محمود(القاهرة : الدار المصـــرية اللبنانية، 2023)، ص100.

(2) عبادة محمد التامر، **سياسة الولايات المتحدة وإدارة الأزمات الدولية (إيران-العراق-سورية- لبنان أنموذجاً)** (بيروت: المركز العربي للأبحاث ودراسة السياسات، ، 2022) ص82.

(3) عبادة محمد التامر، **سـياسـة الولايات المتحدة وإدارة الأزمات الدولية (إيران-العراق-سـورية-لبنان أنموذجاً)**،مصـدر سبق ذكره، ص82.

تزايد العلاقة ما بين التكنولوجيا والامن .إذ تقوم مؤسسات استخباراتية خاصة باجتذاب القراصنة للاستفادة من خدماهتم في التعاقد مع شركات تسعى للحصول على معلومات مُهمة عن مُنافسيها، وتقوم شركات أخرى بتوظيفهم وتوجيههم لالحاق الضرر المادي والنفسي من خلال تدمير الثقة بينهم وبين عملائهم[1].

المبحثُ الثاني

الامن السيبراني وسيلة لديمومة الهيمنة

ان ما يؤديه الامن السـيبراني من دور وفاعلية على صـعيد النظام الدولي والمتمثلة بثورة المعلومات والاتصـالات، تؤكد اسـتمرار تزايد دورها في تعزيز الهيمنة الأمريكية مقارنة بوسـائل القوة الاخرى، ويرتبط نجاح الولايات المتحدة الأمريكية في الحفاظ على مكانتها ودورها عالميا عبر توظيف حقيقي لهذه القوة والعمل على مواجهة الاخفاقات والتحديات من أجل تعزيز الهيمنة الأمريكية في المسـتقبل، وجدنا مناسـبا ان يقسم هذا المبحث إلى ثلاثة مطالب كل واحده منها يمثل خيارا استراتيجيا ومستقبليا من خلال التفاهم مع وحدات النظام الدولي الأخرى.[2]

المطلب الاول: الاتفـاقيـات الدَّولـــية للامن السيبراني

تعمل هذه الاتفاقيات على الحدِّ من الأنشطة السيبرانية: كعمليات التجسس، والمراقبة وغيراها. وقد دخلت الولايات المتحدة طرفاً في هذا الاتفاقيات، إذ حدَّت من عملياتها السيبرانية، ويمكن ذكر أهم هذه الاتفاقيات التي اصبحت الولايات المتحدة رائدة فيها من خلال النقاط الآتية:

اولا. تحالف خمس عيون:

وهو عبارة عن مجموعة من وكالات استخباراتية لخمسٍ من الدول تعمل معاً تقودها الولايات المتحدة، وتتبادل المعلومات، وهي: (استراليا، نيوزلندا، المملكة المتحدة، كندا، الولايات المتحدة) ,وقد بدء هذا التحالف باتفاقية (Bursa)، إذ تم توقيعها في مارس (1946)، وانضمت إليها كلاً: (بريطانيا، وكندا، واستراليا، ونيوزلندا) في عام(1956) [3].

---

(1) حيدر علي حسين، **سياسة الولايات المتحدة الأمريكية ومستقبل النظام الدولي**، مصدر سبق ذكره،2020، ص279.

[2] Ali Mohammed Amneef Al-Rufaie, The components of global leadership of the United States of America after the events of September 11, 2001 , *Journal of International studies* , Issue 100 , Baghdad University, (2025) , :215-243

([3]) وليد عبد الحي، **مدخل إلى الدراسات المستقبلية في العلوم السياسية**(عمان: المركز العلمي للدراسات السياسية، 2022) ص 12.

تطورت الاتفاقية الأصلية إلى هذا التحالف، وتذكر مسودة (2005) بتوجيهات وكالة الأمن القومي (NSA): إن الشركاء يتحفظون بالحق في إجراء عمليات استخباراتية ضد مواطنين بعضهم البعض عندما يكون يصب ذلك في مصلحة الأمة[1].

وفي يوليو عام (2017)، رُفعت الخصوصية الدولية، إذ أُقيمت دعوى قضائية ضدَّ وكالة الأمن القومي الأمريكي ومكتب مدير الاستخبارات الوطنية، ووزارة الخارجية، والإدارة الوطنية للمحفوظات، والسجلات، من قبل الدول الأعضاء في التحالف، وذلك بسبب عدم الالتزام بتحالف الخمس عيون، وبموجب قانون حرية المعلومات وبموجب هذه الدعوى القضائية، أُتهمت الولايات المتحدة بانتهاك الخصوصية، ومخالفة بنود الاتفاقية التي تلزم بعدم تجسس الأطراف على مواطني بعضهم البعض وهذا ما حدث بالفعل[2].

ثانيا: اتفاقية مجلس أوروبا الخاصة بجرائم السيبرانية

وهي اتفاقية متعددة الاطراف، وملزمة قانوناً وقعت في نوفمبر (2001)، إذ دخلت حيز التنفيذ في يوليو(2004). وقد وقعت عليها (46) دولة، بما في ذلك: كندا، واليابان، وجنوب إفريقيا، والولايات المتحدة الأمريكية، وصدَّق عليها من قِبل (26) دولة فقط، ولم تصدَّق عليها روسيا.

وتقتضي اتفاقية المجلس الأوروبي أن تلتزم أطرافها بالتشريعات، لتلزم مقدمي خدمات الانترنت بحفظ بيانات معينة تُخزَّن على خوادمها لمدة تصل إلى تسعين يوم قابلة للتجديد، إذا طلب منهم ذلك مسؤول انقاذ القانون. ويُعدُّ هذا الأمر أمراً بالغ الأهمية، نظراً للصيغة المؤقتة للبيانات الإلكترونية. كما أن الإجراءات التقليدية للمساعدة القانونية المتبادلة غالباً ما تستغرق وقتاً طويلاً في القضايا العابرة للحدود الوطنية بالاضافة الى ذلك احتفضت الولايات المتحدة باعلوية في هذه المعاهدة لضمان الامن القومي للدولة واستمرار هيمنتها[3].

ثالثا. دلـــيل تالـــين:

تم إبرام صك قانوني عام 2013، وهو دليل تالين الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف الشمال الأطلسي (NATO)، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل الذي شنته روسيا على استونيا عام(2007) [4].

([1]) جيفري أي . إيسيناش، **الاستراتيجية الامريكية للفضاء السيراني : تعزيز الحرية والامن والازدهار**، ترجمة: باسم علي خريسان(ابو ظبي: مركز المستقبل للدراسات الستراتيجية ، 2001– 2017) ص265 .

([2]) ريتشارد هاس و مارتن أنديك، **ما بعد العراق،إستراتيجية أمريكية جديدة للشرق الأوسط**، مصدر سبق ذكره، ص26.

([3]) جيفري أي . إيسيناش، **الاستراتيجية الامريكية للفضاء السيراني : تعزيز الحرية والامن والازدهار**، مصدر سبق ذكره ،46.

([4]) ينظر: علي محمد امنيف الرفيعي، **القوة الناعمة وأثرها في مسقبل الهيمنة الامريكية**(بغداد: مكتبة السنهوري، 2023) ص87.

ويحتوي دليل تالين على (95) قاعدة، إذ تتمثل تحدياته الرئيسة في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين والبُنية التحتية الضرورية. وكُلُّ ذلك جاء نتيجةً لوجود فضاء سيبراني واحد، تتقاسمه القوات المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين ومن خلا هذه الاتفاقيات الدولية ضمنت الولايات المتحدة تفوقا واضحا على بقية وحدات النظام الدولي يوفر لها ضمانة في استمرار هيمنتها المطلقة بهذا الاختصاص. [1].

المطلب الثاني: الامن السيبراني مقترب للتفرد والسيطرة

وتأتي استراتيجية الامن السيبراني الجديدة للولايات المتحدة في إطار مساعي البيت الابيض لإنشاء فرع سادس للجيش الأمريكي يركز على الفضاء، ويُحقق هيمنة أمريكية عليه، بعد أن حققت بعض الدول منافسة لها في الفضاء الخارجي، ما يمثل تهديداً للتفوق العسكري الأمريكي, وقد أصدرت وزارة الدفاع والبيت الأبيض استراتيجيتهما لتعزيز الأمن السيبراني بعد تقرير صادم لمكتب المحاسبة الحكومي الأمريكي في سبتمبر من العام الجاري عن حالة الأمن السيبراني داخل الولايات المتحدة[2]، وانتقد غياب استراتيجية أمريكية شاملة للأمن السيبراني، ما قد يجعل الوكالات الفيدرالية، والبنية التحتية الحيوية للولايات المتحدة، بما في ذلك الطاقة، وأنظمة النقل والاتصالات، والخدمات المالية، معرضة للخطر [3]. وتزداد مخاطر الأمن السيبراني هذه مع تنامي التهديدات الأمنية وتعقّدها وهذا ما ترفضه الولايات المتحدة الامريكية حيث صاغت استراتيجية جديدة لتعزيز الأمن السيبراني بالاعتماد على أربع ركائز رئيسة، هي على النحو الآتي[4]:

أولا. تعزيز الأمن القومي الأمريكي: سعت الولايات المتحدة الامريكية الى تحصين امنها القومي من خلال تبادل المعلومات عبر الوكالات الفيدرالية؛ لحماية شبكات الكمبيوتر الاتحادية، وتأمين البنية التحتية الحيوية

([1]) زياد خلف عبد الله ، "الفاعل الدولي (الفرد) في العلاقات الدولية"، **مجلة تكريت للعلوم السياسية** ، المجلد 3 ، العدد 10(تكريت: 2022) ص 149 .

[2] Ali Mohammed Amneef Al-Rufaie, 2024. "The New Middle East in the Perspective of US Strategy (Constants and Variables)". *The International and Political Journal* 59 (59) 2024 2024:207-24.

[3] Muammar Muneim Sahi Al-Ammar. 2021. "'Strategic Doctrine and Cyber Threats Realization'". *Tikrit Journal For Political Science* 3 (25) 2021:196-249. https://doi.org/10.25130/tjfps.v3i25.360.

([4]) احمد فاروق عبد العظيم ، "سياسة القوة في المشروع الاميركي للنظام الدولي" , **مجلة السياسة الدولية** , العدد188(بغداد: 2022) ص19.

للبلاد، وذلك من خلال إعطاء وزارة الأمن الوطني مزيداً من الصلاحيات لرقابة جهود الأمن السيبراني المدنية، ومكافحة الجرائم السيبرانية من خلال التعاون مع الدول الأخرى لتعقب منفذيها[1].

ثانياً. تعزيز الاقتصاد الأمريكي الرقمي:

يتحقق هذا المرتكز من خلال تشجيع الابتكار في قطاع التكنولوجيا، وذلك من خلال العمل مع شركات التكنولوجيا لتعزيز اختبارات الأمن السيبراني في المنتجات الجديدة. بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن السيبراني من خلال توظيف المتخصصين من ذوي الكفاءات في مجال الأمن السيبراني في المؤسسات والوكالات الأمريكية[2].

ثالثاً. مكافحة التهديدات السيبرانية:

تكمن مكافحة التهديدات السيبرانية من خلال استخدام كافة أدوات القوة الأمريكية لردع أي هجمات سيبرانية، وتعزيز المعايير الدولية في الفضاء السيبراني وهذا يتطلب عمل تشاركي بين جميع مؤسسات الدولة الاتحادية بالاعتماد على الوسائل المتطورة للحرب الالكترونية[3].

رابعاً. الدعوة إلى حرية الإنترنت في جميع أنحاء العالم:

يتحقق هذا الهدف من خلال تزويد حلفاء الولايات المتحدة بقدرات سيبرانية؛ للتعامل مع التهديدات السيبرانية التي تستهدف المصالح المشتركة وهذا يضمن دعما مباشرا لجهود الولايات المتحدة الامريكية للتفوق السيبراني ومجابهة التهديدات بهذا القطاع[4]. وتعد جميع هذه المرتكزات عناصر دعم وقوة للولايات المتحدة باتباع نهج أكثر هجومية ضد الهجمات السيبرانية التي تتعرض لها، وبالتصدي العاجل والوقائي لأي هجوم وشيك. كما أنها تحقق التوازن الجيد بين الإجراءات الدفاعية وفرض عواقب مكلفة على منفذي الهجمات السيبرانية.

([1]) سليم كاطع علي، "مقومات القوة الأمريكية وأثرها في النظام الدولي"، **مجلة دراسات دولية**، العدد42 (بغداد:2023) ص160.

([2]) إيرل تيلفورد، **الحرب في القرن الحادي والعشرين**(أبو ظبي: مركز الامارات للدراسات والبحوث الإستراتيجية، 2022) ص174.

([3]) زبغنيو بريجنسكي، **رقعة الشطرنج الكبرى: الأولية الأمريكية ومتطلباتها الجيوستراتيجية**، ترجمة: امل الشرقي(عمان: الأهلية للنشر والتوزيع، 2009) ص42.

([4]) عادل كامل، "عالم أم عالمان"، **مجلة شؤون سياسية**"، العدد 5(دمشق: 20023) ص9.

الخاتمـــة

اخـذ الامـن السـيبراني بكـل تفاصـيله تـزداد أهميتـه باضـطراد نتيجـة التزايـد الـواقعي لحجـم التـأثير، والضغط المتبادل الذي تمارسه الولايات المتحدة الامريكية لديمومة الهيمنة على النظام الدولي.

وهنـاك الكثيـر مـن المتغيِّـرات التـي حكمـت وأثَّـرت فـي السياسـة الأمريكيـة الشـاملة، هـي جـزء مـن مصـادر السـبرانية التـي شـكَّلت الحـراك الأمريكـي فـي العـالم، لكـون السـبرانية غـدت مسـتقبلاً اسـتراتيجياً يتـداخل فـي كافـة القطاعـات، إذ لـم يكـن ذلـك المتغيَّـر، بـل كـان باسـتمرار فـي معـادلات القوى في المنطقة.

واصـبح الامـن السـيبراني يمثـل اهميـة بالغـة للعديـد مـن الأطـراف الإقليميـة والدوليـة، إذ باتـت تكشـف معضـلة مزمنـة لارتبـاط الوضـع الإقليمـي بالـدولي، والاهتمـام الأمريكـي بهـا لكـي تصـبح الحالـة المتحققـة فـي المنطقـة لـيس أمنـاً، بـل ترتيبـات إقليميـة أمنيـة جديـدة مـن الخـارج وهـذا مـا تسـعى الـى تحقيقـه الولايـات المتحـدة الامريكيـة وفـي ضـوء ذلـك، انـدفعت الولايـات المتحـدة لمعالجـة التحـديات الإلكترونيـة التـي تواجههـا لتـرك البـاب مفتوحـاً علـى مصـراعيه أمـام الـدول الراغبـة بـالانخراط فـي عضـوية (النـاتو)، وبلـورة التعـاون مـع تلـك التـي ليسـت لـديها الرغبـة فـي ذلـك ضـامنة تفوقهـا فـي الهيمنة العالمية.

وأصـبح الحلـف جـزءاً مـن المنظومـة السـبرانية الأمريكيـة لمواجهـة التحـديات الخارجيـة، إذ تُعـدُّ حمايـة البنيـة التحتيـة الحيويـة ضـد الهجمـات الإلكترونيـة، تحـدياً معقَّـداً، لأن لكـل قطـاع حـالات ومتطلبـات فريـدة للاسـتخدام. ومـع ذلـك، فأفضـل الممارسـات الأمنيـة التـي يمكـن وضـعها، تبقـى بحاجـةٍ إلـى تحـديثٍ مسـتمرٍ، لتكـون فاعلـة للغايـة فـي حمايـة هـذه الأنظمـة الحيويـة وهـذا مـا اكـد عليـه ترامب في خطابه اثناء حفل التنصيب كرئيس للولايات المتحدة الامريكية عام 2024.

النتائـــــج:

ومن خلال كُلِّ ما تقدَّم، نستنتج الأتي:

1- العمـل علـى صـياغة اسـتراتيجية متماسـكة بشـأن اسـتخدام الأمـن السـيبراني، وذلـك مـن أجـل مواجهـة التحـديات، والمنـع، والانتقـام مـن النشـاطات العدوانيـة التـي تقـوم بهـا دول ومنظمـات، وافراد.

2- توظيف امكانيات الدفاع السيبراني الأمريكية للدفاع استباقيا عن المؤسسات الحكومية المدنية، والبنية التحتية الحيوية، والتفكير في إنشاء خدمة الأمن السيبراني الاتحادية، للانخراط في الوقت المناسب بالعمليات الدفاعية والهجومية لتأمين تفوقا امريكيا سيبرانيا.

3- توجيه جهود وكالات الاستخبارات الأمريكية، لجمع العمليات: الاستخبارية التكتيكية، والاستراتيجية على الإنترنت، لمواجهة أي تهديدٍ للحكومة والبنية التحتية الحيوية للدولة بما يضمن اعلوية امريكية على بقية الدول.

4- إنشاء مؤسسات جديدة تمكَّن الحكومات الملتزمة بالقانون من التحرك ضدَّ التهديدات السيبرانية ومنها توظيف قدرات الذكاء الاصطناعي.

5- إعطاء الأولوية للحفاظ على مكانةٍ بارزةٍ للشركات الأمريكية في الإنترنت بحيث لايمكن منافستها على المستوى القريب والبعيد.

6- الاهتمام بمستقبل التكنولوجيا الرقمية لمواجهة الاختراقات السيبرانية وهذا يشكل التحدي لضمان أن الثورة الرقمية سوف تواصل تطورها بطريقةٍ تحترم وتعزز الهيمنة الامريكية.

7- الاستعداد الكلي لمواجهة التحدي الصيني والروسي والكوري الشمالي سيبرانيا ودول اخرى اخذت تقترب من المنافسة بهذا المجال مما يقوض الهيمنة الامريكية وهذا ما تخشاه الولايات المتحدة الامريكية وتعمل على مواجهته

Conclusion:

Cybersecurity, in all its details, is steadily gaining importance as a result of the actual increase in its influence and the reciprocal pressure exerted by the United States to maintain its dominance over the international system.

There are many variables that have governed and influenced comprehensive American policy, and they are part of the cybersecurity sources that have shaped American action in the world. Cybersecurity has become a strategic future intertwined with all sectors. This was not a single variable, but rather a constant in the power equations in the region. Cybersecurity has become of paramount importance to many regional and international parties. It has revealed a chronic dilemma due to the interconnectedness of the regional and international situation. American interest in cybersecurity has led to the region not being characterized by security, but rather by new regional security arrangements from abroad. This is what the United States seeks to achieve. In light of this, the United States has rushed to address the cyber challenges it faces, leaving the door wide open to countries willing to join NATO and developing cooperation with those unwilling to do so, ensuring its supremacy in global hegemony. The alliance has become part of the American cyber system to confront external challenges. Protecting critical infrastructure against cyberattacks is a complex challenge, as each sector has unique usage situations and requirements. However, the best security practices that can be put in place still need to be continuously updated to be highly effective in protecting these vital systems, as Trump emphasized in his inaugural address as President of the United States in 2024.

Results :

From all of the above, we conclude the following:

1. Work to formulate a coherent strategy for the use of cybersecurity to confront challenges, prevent, and retaliate against hostile activities carried out by countries, organizations, and individuals.
2. Employ American cyber defense capabilities to proactively defend civilian government institutions and critical infrastructure, and consider establishing a Federal Cybersecurity Service to engage in timely defensive and offensive operations to ensure American cyber superiority.
3. Direct the efforts of American intelligence agencies to combine tactical and strategic intelligence operations on the internet to confront any threat

to the government and the nation's critical infrastructure, ensuring American supremacy over other countries.
4. Establishing new institutions that enable law-abiding governments to act against cyber threats, including the use of artificial intelligence capabilities.
5. Prioritizing the preservation of a prominent position for American companies on the internet, ensuring they remain unrivaled in the near and long term.
6. Focusing on the future of digital technology to counter cyber intrusions. This poses the challenge of ensuring that the digital revolution continues to evolve in a manner that respects and enhances American hegemony.
7. Fully prepared to confront the cyber challenge posed by China, Russia, North Korea, and other countries, which are approaching competition in this field, undermining American hegemony. This is something the United States fears and is working to address.

قائمة المصادر

اولا: الكتب

1. الرفيعي، علي. **القوة الناعمة وأثرها في مسقبل الهيمنة الامريكية**(بغداد: مكتبة السنهوري، 2023).
2. إيسيناش، جيفري أي . **الاستراتيجية الامريكية للفضاء السيراني : تعزيز الحرية والامن والازدهار**، ترجمة: باسم علي خريسان(ابو ظبي: مركز المستقبل للدراسات الستراتيجية ، 2001– 2017).
3. بيروسي، جياكومو. **خلف الستار : التجارة غير المشروعة بالأسلحة النارية المتفجرات والذخيرة على الانترنت المظلم**(سانتامونيكا: مؤسسة RAND ، 2022).
4. بريجنسكي، زبغنيو. **رقعة الشطرنج الكبرى: الأولية الأمريكية ومتطلباتها الجيوستراتيجية**، ترجمة: امل الشرقي(عمان: الأهلية للنشر والتوزيع، 2009).
5. هاس، ريتشارد. **ما بعد العراق،إستراتيجية أمريكية جديدة للشرق الأوسط** (بغداد: مركز الدراسات الدولية جامعة بغداد، 2009).
6. فريدمان، جورج. **الإمبراطورية والجمهورية في عالم متغير**، ترجمة: أحمد محمود (القاهرة : الدار المصرية اللبنانية، 2023).
7. تيلفورد، إيرل. **الحرب في القرن الحادي والعشرين**(أبو ظبي: مركز الامارات للدراسات والبحوث الإستراتيجية، 2022).
8. علي، حيدر. **سياسة الولايات المتحدة الأمريكية ومستقبل النظام الدولي** (بغداد: دار الكتب العلمية للطباعه والنشر والتوزيع، 2017).
9. عبد الحي، وليد. **مدخل إلى الدراسات المستقبلية في العلوم السياسية**(عمان: المركز العلمي للدراسات السياسية، 2022).
10. قبيس، هادي. **السياسة الخارجية الامريكية بين مدرستين** (بيروت: الدار العربية للعلوم ، 2023).
11. سند، جمال. **آفاق العصر الأمريكي: السيادة والنفوذ في النظام العالمي الجديد**(أبو ظبي: مركز الدراسات الاستراتيجية، 2021).
12. حجازي، محمود. **جرائم الحاسبات والانترنت والجرائم المعلوماتية** (القاهرة: المركز المصري للملكية الفكرية، 2020).
13. محمد، عبادة. **سياسة الولايات المتحدة وإدارة الأزمات الدولية (إيران-العراق-سورية-لبنان أنموذجاً)** (بيروت: المركز العربي للأبحاث ودراسة السياسات، ، 2022).

ثانيا: الدوريات العلمية:

1. زياد، عبدالله . "القرصنة التكنولوجية واثرها العلاقات الامريكية – الصينية"، **مجلة جامعة تكريت للعلوم الانسانية**، العدد 9 (صلاح الدين: 2021).
2. فاروق، احمد. "سياسة القوة في المشروع الاميركي للنظام الدولي" , **مجلة السياسة الدولية** , العدد188(بغداد: 2022).
3. عبد الله ، زياد. "الفاعل الدولي (الفرد) في العلاقات الدولية"، **مجلة تكريت للعلوم السياسية** ، المجلد 3، العدد 10(تكريت: 2022).
4. كاطع، سليم. "مقومات القوة الأمريكية وأثرها في النظام الدولي"، **مجلة دراسات دولية**، العدد42 (بغداد:2023).
5. محمد، اشرف. "حلف الناتو: من الشراكة الجديدة إلى التدخل في الازمات العربية"، **مجلة السياسة الدولية**، العدد 88(القاهرة: 2022).

References :

First: Books

1. Al-Rafii, Ali. Soft Power and Its Impact on the Future of American Hegemony (Baghdad: Al-Sanhouri Library, 2023).
2. Eisenach, Jeffrey A. The American Cyberspace Strategy: Promoting Freedom, Security, and Prosperity (translated by Basem Ali Khreisan) (Abu Dhabi: Future Center for Strategic Studies, 2001-2017).
3. Perosi, Giacomo. Behind the Curtain: The Illicit Trade in Firearms, Explosives, and Ammunition on the Dark Web (Santamonica: RAND Corporation, 2022).
4. Brzezinski, Zbigniew. The Grand Chessboard: American Primacy and Its Geostrategic Imperatives (translated by Amal Al-Sharqi) (Amman: Al-Ahlia Publishing and Distribution, 2009).
5. Haas, Richard. Beyond Iraq: A New American Strategy for the Middle East (Baghdad: Center for International Studies, University of Baghdad, 2009).
6. Friedman, George. Empire and Republic in a Changing World, translated by Ahmed Mahmoud (Cairo: Dar Al-Masryia Al-Lubnaniyya, 2023).
7. Telford, Earl. War in the Twenty-First Century (Abu Dhabi: Emirates Center for Strategic Studies and Research, 2022).
8. Ali, Haider. US Policy and the Future of the International Order (Baghdad: Dar Al-Kotob Al-Ilmiyah for Printing, Publishing, and Distribution, 2017).
9. Abdul-Hay, Walid. Introduction to Future Studies in Political Science (Amman: Scientific Center for Political Studies, 2022).
10. Qubais, Hadi. US Foreign Policy Between Two Schools (Beirut: Arab Scientific House for Science, 2023).
11. Sanad, Jamal. Prospects for the American Era: Sovereignty and Influence in the New World Order (Abu Dhabi: Center for Strategic Studies, 2021).
12. Hijazi, Mahmoud. Computer and Internet Crimes and Cybercrimes (Cairo: Egyptian Center for Intellectual Property, 2020).
13. Muhammad, Obada. US Policy and International Crisis Management (Iran-Iraq-Syria-Lebanon as a Model) (Beirut: Arab Center for Research and Policy Studies, 2022).

Second: Journals:

1. Ziad, Abdullah. "Technological Piracy and Its Impact on US-China Relations," Tikrit University Journal for Humanities, Issue 9 (Salah al-Din: 2021).

2. Farouk, Ahmed. "Power Politics in the American Project for International Order," International Politics Journal, Issue 188 (Baghdad: 2022).
3. Abdullah, Ziad. " he International Actor (The Individual) in International Relations'". Tikrit Journal For Political Science 2 (10):133-52. https://doi.org/10.25130/tjfps.v2i10.129.
4. Ali Mohammed Amneef Al-Rufaie, 2024. "The New Middle East in the Perspective of US Strategy (Constants and Variables)". *The International and Political Journal* 59 (59) 2024:207-24.
5. Ali Mohammed Amneef Al-Rufaie, The components of global leadership of the United States of America after the events of September 11, 2001 , *Journal of International studies* , Issue 100 , Baghdad University, (2025) , :215-243
6.Katea, Salim. "The Elements of American Power and Its Impact on the International System," Journal of International Studies, Issue 42 (Baghdad: 2023).
7. Muhammad, Ashraf. "NATO: From the New Partnership to Intervention in Arab Crises," Journal of International Politics, Issue 88 (Cairo: 2022).
8. Muammar Muneim Sahi Al-Ammar. 2021. "'Strategic Doctrine and Cyber Threats Realization'". *Tikrit Journal For Political Science* 3 (25):196-249. https://doi.org/10.25130/tjfps.v3i25.360