وزارة التعليم العالي والبحث العلمي
جامعة كربلاء
مركز الدراسات الاستراتيجية

مجلة
المستقبل العراقي
للدراسات السياسية والاستراتيجية

المستقبل العراقي

للدراسات السياسية والاستراتيجية

ISSN print : 2790-8240

ISSN online : 3006-7227

مجلة علمية محكمة متخصصة نصف سنوية تصدر عن مركز الدراسات الاستراتيجية في جامعة كربلاء
تُعنى بالشؤون السياسية والاستراتيجية

في هذا العـــدد ..

العدد (6)

حزيران 2026

وزارة التعليم العالي والبحث العلمي
جامعة كربلاء
مركز الدراسات الاستراتيجية

المستقبل العراقي

للدراسات السياسية والاستراتيجية

العـدد (6) حزيران/ 2026

الترميز الدولي: 2790-8240

رقم الإيداع في دار الكتب والوثائق ببغداد (2570) لسنة 2022

المستقبل العراقي

للدراسات السياسية والاستراتيجية

مجلة علمية متخصصة نصف سنوية يصدرها مركز الدراسات الاستر اتيجية في جامعة كربلاء
تُعنى بالشؤون السياسية والاستر اتيجية

المستقبل العراقي

للدراسات السياسية والاستراتيجية

مجلة يصدرها مركز الدراسات الاستراتيجية / جامعة كربلاء

- مركز بحثي علمي أكاديمي مستقل، من مؤسسات جامعة كربلاء.
- يُعنى بإنجاز البحوث والدراسات العلمية في ضوء خطط وزارة التعليم العالي والبحث العلمي ورئاسة جامعة كربلاء.
- يلتزم بالموضوعية والحيادية في طرح القضايا المحلية والدولية، ولا يُعنى ولا يُسهم في النشاطات السياسية والحزبية.

البريد الالكتروني للمجلة
ifpss-kcss@uokerbala.edu.iq

دليل المؤلف:

تعتمد مجلة (المستقبل العراقي للدراسات السياسية والاستراتيجية) في انتقاء محتويات أعدادها المواصفات الشكلية والموضوعية للمجلات الدولية المحكمة وفقاً لما يلي:

أولاً: أن يكون البحث أصيلاً معدَّاً خصيصاً للمجلَّة، وألا يكون قد نُشر جزئياً أو كلياً أو نُشر ما يشبهه في أيِّ وسيلة نشرٍ إلكترونية أو ورقية.

ثانياً: أن يُرفق البحث بالسيرة العلمية (C.V) للباحث باللغتين العربية والإنكليزية.

ثالثاً: يجب أن يشتمل البحث على العناصر التالية:

- الصفحة الأولى تتضمن عنوان البحث باللغتين العربية والإنكليزية، وتعريف موجز بالباحث والمؤسَّسة العلمية التي ينتمي إليها في صفحةٍ مستقلة ووسائل الاتصال الخاصة بالباحث.
- الملخَّص التنفيذي باللغتين العربية والإنكليزية على نحو 250_300 كلمة والكلمات المفتاحية (Key Words) بعد الملخَّص، ويقدَّم الملخص بجمل قصيرة ودقيقة وواضحة إشكالية البحث الرئيسة، والطرق المستخدمة في بحثها، والنتائج التي توصَّل إليها البحث.
- تحديد مشكلة البحث، وأهداف الدراسة، وأهميتها، والمراجعة النقدية لما سبق وكُتب عن الموضوع، بما في ذلك أحدث ما صدر في مجال البحث، وتحديد مواصفات فرضية البحث أو أطروحته، ووضع التصور المفاهيمي وتحديد مؤشراته الرئيسة، ووصف منهجية البحث، والتحليل والنتائج، والاستنتاجات. على أن يكون البحث مذيلاً بقائمة المصادر والمراجع التي أحال إليها الباحث، أو التي يُشير إليها في المتن.
- أن يتقيد البحث بمواصفات التوثيق في (تنسيق وتدوين المراجع والهوامش) وفقاً للصيغة العالمية المعروفة وأسلوب فانكوفر (Vancouver)
- لا تنشر المجلَّة مستّلاً أو فصول من رسائل جامعية أُقرَّت إلا بشكلٍ استثنائي، وبعد أن يعدَّها الباحث من جديد للنشر في المجلَّة، وبما يتناسب مع تعليماتها، وفي هذهِ الحالة على الباحث أن يُشير إلى ذلك، ويقدم بيانات وافية عن عنوان الأطروحة وتاريخ مناقشتها والجامعة التي جرت فيها المناقشة.
- أن يقع البحث في مجال أهداف المجلَّة واهتماماتها البحثية.
- تهتم المجلَّة بنشر مراجعاتٍ نقدية للكتب المهمة التي صدرت حديثاً في مجالات اختصاصها بأيِّ لغةٍ من اللغات، شرط ألا يكون قد مضى على صدورها أكثر من ثلاث سنوات، وألا يتجاوز عدد كلماتها 2500- 3000 كلمة، ويجب أن يقع هذا الكتاب في مجال اختصاص الباحث أو في مجال اهتماماتهِ البحثية الأساسية، وتخضع المراجعات الى ما تخضع له البحوث من قواعد التحكيم.
- يتراوح عدد كلمات البحث، بما في ذلك المراجع في الإحالات المرجعية والهوامش الإيضاحية، وقائمة المراجع وكلمات الجداول في حال وجودها، والملحقات في حال وجودها، (8000 -10000) كلمة وللمجلة أن تنشر بحسب تقديراتها وبصورةٍ استثنائية، بعض البحوث والدراسات التي تتجاوز هذا العدد من الكلمات. ويكون نوع وحجم الخط كالاتي:
  - أ- العنوان الرئيس حجم الخط (16) غامق ونوع الخط: (Sakkal Majalla)
  - ب- العناوين الفرعية: حجم الخط (16) غامق ونوع الخط: (Sakkal Majalla)
  - ت- المتن: حجم الخط (14) عادي ونوع الخط : (Sakkal Majalla)
  - ث- الهوامش: حجم الخط (12) عادي ونوع الخط: (Sakkal Majalla)
  - ج- تدون المصادر والمراجع نهاية البحث بحجم ونوع الخط كما في المتن.

- تُنشر البحوث والدراسات في المجلَّة باللغتين العربية والإنكليزية.

رابعاً: الاستلال الإلكتروني والتحكيم العلمي:

- تُعرض البحوث والدراسات المقدَّمة للنشر في المجلَّة على برنامج الاستلال الإلكتروني(Turnitin)، ويتحمل المؤلف تكاليف الاستلال.

- يخضع كلّ بحث إلى تحكيم سري تام، يقوم بهِ قارئان (محكِّمان) من القُرَّاء المختصين اختصاصاً دقيقاً في موضوع البحث، ومن ذوي الخبرة العلمية بما أُنجز في مجالهِ، وفي حال تباين تقارير القراء، يُحال البحث إلى قارئ مرجِّح ثالث. وتلتزم المجلَّة موافاة الباحث بقرارها الأخير؛ النشر/ عدم النشر بعد إجراء تعديلات محددة/ وذلك في غضون ثلاثة أشهر من استلام البحث.

خامساً: تلتزم المجلَّة ميثاقاً أخلاقياً يشتمل على احترام الخصوصية والسرية والموضوعية والأمانة العلمية وعدم إفصاح المحرِّرين والمراجعين وأعضاء هيأة التحرير عن أيِّ معلوماتٍ بخصوص البحث المحال إليهم إلى أيِّ شخصٍ آخر غير المؤلِّف والقُرَّاء وفريق التحرير.

سادساً: يخضع ترتيب نشر البحوث إلى مقتضياتٍ فنية لا علاقة لها بمكانة الباحث.

سابعاً: يتّحمل المؤلف أجور النشر التي تفرضها المجلة وفقا لسياساتها المعلن عنها، ولا يحق للمؤلف استرجاع هذه الأجور في حال رفض بحثه.

دليل المُقيَّم:

إنَّ المهمة الرئيسة للمُقيِّم العلمي للبحوث المُرسلة للنشر هي أنْ يقرأ المُقيِّم البحث الذي يقع ضمن تخصصهِ العلمي بعنايةٍ فائقةٍ وتقييمهِ وفق رؤىً ومنظورٍ علمي أكاديمي لا يخضع لأيِّ آراءٍ شخصية، ومن ثمَّ يقوم بتثبيت ملاحظاتهِ البنَّاءة والصادقة بخصوص البحث المُرسل إليه.

قبل البدء بعملية التقييم، يُرجى من المُقيِّم التأكد من استعدادهِ الكامل لتقييم البحث المُرسل إليه، وفيما إذا كان يقع ضمن تخصصهِ العلمي أم لا، وهل يمتلك المُقيِّم الوقت الكافي لإتمام عملية التقييم، وإلا فيمكن للمُقيِّم أنْ يعتذر ويقترح مُقيِّم آخر.

بعد موافقة المُقيِّم على إجراء عملية التقييم والتأكد من إتمامها خلال الفترة المحددة، يُرجى إجراء عملية التقييم وفق المحددات التالية:

- يجب أنْ لا تتجاوز عملية التقييم مدَّة أسبوعين، كي لا يؤثر ذلك بشكلٍ سلبي على المؤلِّف.
- عدم الإفصاح عن معلومات البحث ولأيِّ سببٍ كان خلال وبعد إتمام عملية التقييم، إلا بعد أخذ الإذن الخطِّي من المؤلِّف ورئيس هيأة التحرير للمجلَّة، أو عند نشر البحث.
- عدم استخدام معلومات البحث لأيِّ منافع شخصية، أو لغرض إلحاق الأذى بالمؤلِّف أو المؤسَّسات الراعية له.
- الإفصاح عن أيِّ تضاربٍ محتمل في المصالح.
- يجب أنْ لا يتأثر المُقيِّم بقومية أو ديانة أو جنس المؤلِّف، أو أيَّةِ اعتباراتٍ شخصية أخرى.
- هل أنَّ البحث أصيلاً ومهم لدرجة يجب نشره في المجلَّة.
- بيان فيما إذا كان البحث يتفق مع السياسة العامة للمجلَّة وضوابط النشر فيها.
- هل أنَّ فكرة البحث متناولة في دراساتٍ سابقة؟ إذا كانت نعم، يُرجى الإشارة إلى تلك الدراسات.
- بيان مدى تعبير عنوان البحث عن البحث نفسهِ ومحتواه.
- بيان فيما إذا كان ملخص البحث يصف بشكلٍ واضح مضمون البحث وفكرته.
- هل تصف المقدمة في البحث ما يريد المؤلِّف الوصول إليه وتوضيحه بشكلٍ دقيق؟ وهل وضَّح فيها المؤلِّف ما هي المشكلة التي قام بدراستها؟
- مناقشة المؤلِّف للنتائج التي توصل إليها خلال بحثهِ بشكلٍ علمي ومُقنع.
- يجب أنْ تُجرى عملية التقييم بشكلٍ سري وعدم اطلاع المؤلِّف على أيِّ جانبٍ فيها.
- إذا أراد المُقيِّم مناقشة البحث مع مُقيِّمٍ آخر، فيجب إبلاغ رئيس التحرير بذلك.
- يجب أنْ لا تكون هنالك مخاطبات ومناقشات مباشرة بين المُقيِّم والمؤلِّف فيما يتعلَّق ببحثهِ المُرسل للنشر، ويجب أنْ تُرسل ملاحظات المُقيِّم إلى المؤلِّف من خلال مدير تحرير المجلَّة.
- إذا رأى المُقيِّم بأنَّ البحث مست من دراساتٍ سابقة، توجَّب على المُقيِّم بيان تلك الدراسات لرئيس تحرير المجلَّة.
- إنَّ ملاحظات المُقيِّم العلمية وتوصياته سيُعتمد عليها وبشكلٍ رئيس في قرار قبول البحث للنشر من عدمهِ، كما يُرجى من المُقيِّم الإشارة وبشكلٍ دقيق إلى الفقرات التي تحتاج إلى تعديلٍ بسيط ممكن أنْ تقوم بها هيأة تحرير المجلَّة، وإلى تلك التي تحتاج إلى تعديلٍ جوهري يجب أنْ يقوم بها المؤلِّف نفسه.

اخلاقيات النشر:

- تعتمد مجلَّة المستقبل العراقي للدراسات السياسية والاستراتيجية قواعد السرية والموضوعية في عملية التحكيم، بالنسبة للباحث والقراء (المحكِّمين) على حدٍّ سواء، و يُحتل كل بحث قابل للتحكيم على قارئين معتمديْن لديها من ذوي الخبرة والاختصاص الدقيق بموضوع البحث، لتقييمه وفق نقاطٍ محددة. وفي حال تعارض التقييم بين القراء، يُحتل المجلَّة البحث على قارئ مرجِّح آخر.
- تعتمد المجلَّة تنظيماً داخلياً دقيقاً واضح الواجبات والمسؤوليات في عمل جهاز التحرير ومراتبه الوظيفية.
- تلتزم المجلَّة بإعلام الباحث بالموافقة على نشر البحث من دون تعديل أو وفق تعديلاتٍ معينة، بناءً على ما يرد في تقارير القراءة، أو الاعتذار عن عدم النشر، مع بيان أسباب الاعتذار.
- تلتزم مجلَّة المستقبل العراقي للدراسات السياسية والاستراتيجية بجودة الخدمات التدقيقية والتحريرية والطباعية والإلكترونية التي تقدمها للبحث.
- احترام قاعدة عدم التمييز: يقيِّم المحرِّرون والمراجعون المادَّة البحثية بحسب محتواها الفكري، مع مراعاة مبدأ عدم التمييز على أساس العِرق أو الجنس الاجتماعي أو المعتقد الديني أو الفلسفة السياسية للكاتب، أو أي شكل من أشكال التمييز الأخرى، عدا الالتزام بقواعد ومناهج ولغة التفكير العلمي في عرض وتقديم الأفكار والاتجاهات والموضوعات ومناقشتها أو تحليلها.
- حقوق الملكية الفكرية: تكون حقوق الملكية الفكرية للباحثين (المؤلفين) وتكون حقوق النشر الورقي والإلكتروني محفوظة لمركز الدراسات الاستراتيجية بالنسبة للمقالات والابحاث والدراسات المنشورة في المجلة، ولا يجوز إعادة نشرها جزئيًّا أو كلّيًا، سواءٌ باللغة العربية أو مترجمة إلى لغات أجنبية، من دون إذنٍ خطي صريح من المجلة.

المحتويات

افتتاحية العدد

في عالم يشهد تحولات متسارعة في بنية النظام الدولي، وتبدلًا متواصلًا في موازين القوة والنفوذ، تبرز الحاجة إلى قراءة علمية رصينة تستوعب تعقيد المشهد السياسي والاستراتيجي، وتربط بين الظواهر وتحولاتها في سياقاتها المحلية والإقليمية والدولية. فالمتغيرات الراهنة لم تعد منفصلة عن بعضها، بل باتت تتداخل ضمن مشهد عالمي تتقاطع فيه اعتبارات الأمن والطاقة والتنمية والتكنولوجيا والاقتصاد والجغرافيا السياسية في إطار أكثر سيولة وتشابكًا.

ويأتي هذا العدد السادس استمرارًا للمسار العلمي الذي انتهجته المجلة في تقديم دراسات وبحوث رصينة تُعنى بالقضايا السياسية والاستراتيجية المعاصرة، وتسعى إلى بناء معرفة أكاديمية معمقة تستند إلى التحليل المنهجي والاستشراف العلمي، بما يواكب طبيعة التحولات المتسارعة التي يشهدها العالم والمنطقة.

وقد تضمّن هذا العدد باقةً متنوعة من الدراسات والبحوث التي تناولت قضايا محورية تتصل بالشأن العراقي وامتداداته الإقليمية والدولية، من بينها الأمن المائي، والأمن الوطني، والتنمية المستدامة، والهجرة، والأمن السيبراني، إلى جانب موضوعات التنافس الدولي بين القوى الكبرى، وتحولات السياسات الخارجية، وصعود الفاعلين الجدد، ومستقبل الدولة القومية في البيئة الدولية المعاصرة.

ويحضر العراق في هذا العدد بوصفه محورًا أساسيًا في العديد من المقاربات البحثية، بالنظر إلى مكانته الجيوسياسية ودوره المتنامي في معادلات التفاعل الإقليمي والدولي، وما يواجهه من تحديات وفرص في ظل التحولات الراهنة. وقد سعت الدراسات المنشورة إلى مقاربة هذه الموضوعات من زوايا تحليلية متعددة، جمعت بين البعد النظري والتطبيقي، وبين قراءة الواقع واستشراف آفاقه المستقبلية.

إن ما يميّز هذا العدد لا يكمن في تنوع موضوعاته فحسب، بل في تعدد مقارباته المنهجية وتكامل رؤاه البحثية، بما يعكس حيوية الحقل المعرفي في الدراسات السياسية والاستراتيجية، ويؤكد أهمية البحث العلمي بوصفه أداةً للفهم والتحليل والمساهمة في إنتاج المعرفة الرصينة.

وإذ نقدّم هذا العدد السادس إلى الباحثين والمهتمين، فإننا نأمل أن يمثّل إضافة علمية نوعية ترفد المكتبة الأكاديمية، وتسهم في إثراء النقاش العلمي حول القضايا السياسية والاستراتيجية المعاصرة، وأن يواصل دوره في ترسيخ المعرفة العلمية، وتعزيز الوعي بطبيعة التحولات التي يشهدها العالم، وبموقع العراق ضمن معادلاته المتغيّرة.

أ. د. نصر محمد علي

رئيس التحرير

استراتيجية الولايات المتحدة الأمريكية في مواجهة التهديدات السيبرانية

The Strategies of the United States of America in Confronting Cyber Threats

الباحث/ م.م زينب ضياء محمد أمين
جامعة بغداد / مركز الدراسات الاستراتيجية والدولية

The Researcher : Zainab Diaa Mohammed Amin
University of Baghdad / Center for Strategic and International Studies
zainab.d@cis.uobaghdad.edu.iq

الملخّص

يتناول البحث واحد من أهم الموضوعات المهمة، التي طرأت على الساحة الدولية، بوصفها أحد التحديات الأمنية غير التقليدية، التي تمكنت من إعادة تشكيل مفهوم الأمن القومي للنظام الدولي. إذ إنَّ التطور والتقدم التكنولوجي الذي شهدته العديد من القوى الدولية، بما فيها الولايات المتحدة الأمريكية، الأمر الذي أدى إلى بروز أنماط جديدة من التهديدات غير التقليدية (التهديدات السيبرانية)، مما دفع بالولايات المتحدة الأمريكية إلى تبني العديد من الاستراتيجيات الوقائية، وأخرى هجومية تستهدف حماية أمنها القومي. كما يهدف البحث إلى تحليل الاستراتيجيات السيبرانية الأمريكية، وتقييمها، ومدى فاعليتها في الحد من الهجمات السيبرانية، فضلاً عن دراسة انعكاس مدى نجاحها في حماية الأمن القومي الأمريكي، وتحقيق ما يسمى بالردع السيبراني.

الكلمات المفتاحية: الأمن القومي، الفضاء السيبراني، الاستراتيجيات السيبرانية، التهديدات السيبرانية.

Abstract

This research addresses one of the most significant issues that has emerged on the international scene as one of the non-traditional security challenges that has succeeded in reshaping the concept of national security within the international system. The technological development and advancement witnessed by many international powers, including the United States of America, have led to the emergence of new patterns of non-traditional threats, namely cyber threats. This has prompted the United States to adopt numerous preventive as well as offensive strategies aimed at protecting its national security.

The research also aims to analyze and evaluate American cyber strategies, as well as to assess their effectiveness in reducing cyberattacks. Furthermore, it examines the extent of their success in safeguarding American national security and achieving what is known as cyber deterrence.

Keywords: National security, cyberspace, cyber strategies, cyber threats.

المقدمة

أحدث الفضاء السيبراني، وتكنولوجيا المعلومات، ثورة شاملة أثّرت في العديد من المجالات (السياسية، الاقتصادية، الاجتماعية، الأمنية، الثقافية)، إذ يُعدّ الفضاء السيبراني أحد أهم المفاهيم المؤثرة في النظام الدولي، وكذلك التفاعلات الدولية، إذ يشكّل أحد أهم المتغيرات الجوهرية في بنية النظام السياسي، وتفاعلاته، كما يشكّل أحد المرتكزات لإدارة التعاون، والصراع، نتيجة لتأثر العلاقات الدولية بهذا الفضاء، وكذلك تكنولوجيا المعلومات، إذ تُعدّ التهديدات السيبرانية أحد مظاهر الفضاء السيبراني، والتي أثرت في العديد من المجالات، وأهمها السياسية، والأمنية، والتي تعتمد على توظيف القوة في تحقيق المصالح، والأهداف المنشودة. ونتيجة للتطور التكنولوجي الذي أسهم في خلق بيئة جديدة للصراعات، حول العديد من المفاهيم، وأهمها: (التهديدات السيبرانية، والأمن السيبراني، والإرهاب السيبراني، والقوة السيبرانية، والحروب السيبرانية)، والتي أسهمت في التأثير في العلاقات الدولية بأشكالها كافة (التعاون أو التنافس)، إذ أصبحت قضايا التهديدات السيبرانية، والأمنية، أحد أهم التحديات أمام استراتيجة الدول، ومنها الولايات المتحدة الأمريكية، والتي تُعدُّ من أبرز الفاعلين الدوليين في مجال الفضاء السيبراني، نتيجة للتطور التكنولوجي التي تشهده، الأمر الذي دفعها لتبني العديد من الاستراتيجيات، لمواجهة التهديدات السيبرانية، فضلاً عن تطوير قدراتها الدفاعية، والهجومية، لهدف حماية البنى التحتية، وضمان تفوقها في هذا المجال. وانطلاقاً من ذلك، يهدف البحث إلى دراسة طبيعة الاستراتيجية الأمريكية، وفهمها، وذلك عن طريق بيان أهدافها، ودوافعها، ومدى نجاحها في حماية الأمن القومي الأمريكي، وكذلك الحفاظ على مستوى متقدم من التطور في مجال الفضاء السيبراني، في ظلّ بيئة دولية تتسم بالتنافس، والهيمنة، على هذا المجال.

أولاً- أهمية البحث

تنطلق أهمية البحث كونه يهتم بدراسة أحد أبرز الموضوعات الاستراتيجية، والأمنية، للولايات المتحدة الأمريكية، إذ تأتي هذه الأهمية نتيجة تزايد التهديدات، والمخاطر السيبرانية، وهذا ما دفع الولايات المتحدة إلى تطوير فضائها السيبراني، وتوظيفه في مجالاتها الاستراتيجية كافة (الدفاعية، والأمنية، والاقتصادية، والسياسية)، لذا فإنَّ أي تهديد يمسّ أحد هذه المجالات، يُعدّ خرقًا، وتهديدًا مباشرًا لأمنها القومي.

ثانيًا- أهداف البحث

يسعى البحث إلى تحقيق العديد من الأهداف، والمتمثلة بما يأتي:

1. فهم طبيعة التهديدات السيبرانية، وتحليلها، وبيان مدى تأثيرها في الأمن القومي الأمريكي.
2. توضيح أهم الأبعاد السياسية، والأمنية، الاستراتيجية السيبرانية الأمريكية.
3. دراسة أهم الاستراتيجيات الوطنية السيبرانية الأمريكية، التي تبنتها الولايات المتحدة في مواجهة التهديدات، والمخاطر السيبرانية.

ثالثًا- إشكالية البحث

تتمحور إشكالية البحث حول تساؤل رئيس، هو: (إلى أي مدى نجحت الاستراتيجية الأمريكية في مواجهة المخاطر، والتهديدات السيبرانية؟ وما مدى فاعليتها في تحقيق الأمن القومي الأمريكي، وحمايته؟) ومن هنا يمكن طرح مجموعة من التساؤلات الفرعية، وبحسب الأتي:

1. ما أهداف الاستراتيجية السيبرانية الأمريكية؟
2. ما مدى فاعلية الاسترتيجية السيبرانية في تحقيق الأمن السيبراني؟

رابعًا- فرضية البحث

تقوم فرضية البحث على فكرة، مفادها: (إنَّ الاستراتيجية الأمريكية في مواجهة التهديدات السيبرانية، تشكّل الأداة الأكثر فاعلية في تعزيز الأمن القومي، وحماية البنى التحتية، إلا أنَّ فاعليتها مرتبطة بحجم التهديدات، والمخاطر، التي تتعرض لها، مما قد يؤثر في قدرتها على تحقيق الردع السيبراني، تجاه التهديدات الموجهة لها).

خامسًا- منهجية البحث

يعتمد البحث على منهجين مهمين، هما:

1. **المنهج الوصفي (التحليلي)**: وذلك عن طريق دراسة التهديدات السيبرانية، وأثرها في الأمن القومي الأمريكي، فضلاً عن دراسة أهم استراتيجيات مواجهة المخاطر، عبر الرئاسات الأمريكية المتعاقبة.
2. **المنهج المقارن:** والذي يتم عن طريقه تحديد أوجه التباين بين هذه الاستراتيجيات.

سادسًا- هيكلية البحث

تقوم هيكلية البحث على ثلاثة محاور، هي:

المحور الأول: الإطار النظري والمفاهيمي للأمن.

المحور الثاني: دور القدرات السيبرانية في تعزيز الأمن القومي الأمريكي.

المحور الثالث: آليات توظيف الاستراتيجية الأمريكية في مواجهة التهديدات السيبرانية.

المحور الأول

الإطار النظري والمفاهيمي للأمن

أولاً- مفهوم التهديدات السيبرانية

لقد برز مفهوم الفضاء السيبراني في الساحة الدولية، بوصفه أحد الأدوات الجديدة التي تحكم شكل الصراعات بين الفاعلين الدوليين، لاسيَّما بعد تحوّل ظاهرة الصراع الدولي التقليدي، إلى صراع سيبراني أثّر في بنية النظام الدولي، وكذلك العلاقات الدولية، والذي عبّر عن حالة من التباين، والتناقض، في الأهداف والمصالح بين الفاعلين، سواء أكانوا من الدول أم من غير الدول (شركات متعددة الجنسيات، والمنظمات، والتنظيمات الإرهابية). نتيجة التطور التكنولوجي والسيبراني، اتسعت دائرة الحروب السيبرانية، وكذلك التهديدات السيبرانية التي أثّرت بشكل مباشر في الأمن القومي للدول. كما يتضمن الصراع السيبراني سمات عدة، منها[1]:

1. ساحة صراع مفتوحة: بمعنى أنَّها لا تقتصر على ساحة جغرافية محددة، بل تمتد لتصل إلى ساحات مفتوحة تضم أطراف عدة.

2. إنَّ أدوات الصراع السيبراني أدوات إلكترونية، تضم العديد من المعلومات، والبيانات، التي يمكن اختراقها عن طريق الأجهزة الإلكترونية، ومنها أجهزة الحواسيب.

3. إنَّ الصراع السيبراني عزز من فرض الحروب غير التقليدية، كونه أقل كلفة في شنّ الهجمات، والتهديدات السيبرانية، على الدول الأخرى.

4. إنَّ استراتيجية الردع في الصراعات التقليدية، تختلف عن استراتيجية الردع في الصراعات السيبرانية، فهي لم تقتصر على الردع النووي، بل امتدت لتشمل البنية التحتية بأشكالها كافة، وكذلك أهم المؤسسات الأمنية، والاستخباراتية، للدول[2].

كما يُعرَّف الفضاء السيبراني، على أنَّه: "الساحة الافتراضية التي تعتمد على نظام الحواسيب، وشبكات الإنترنت، وما توفره من بيانات، ومعلومات، يمكن الاستفادة منها في شنّ الهجمات، والتهديدات السيبرانية". ويُعرف أيضًا، على أنَّه: "البعد الخامس في شنّ الحروب السيبرانية بين الأطراف المتنازعة". لذا فقد فرض الواقع السيبراني بيئة افتراضية

---

(1) شيماء معروف فرحان، التحول في مفهوم القوة والصراع: دراسة في الحروب السيبرانية، مجلة قضايا سياسية، جامعة النهرين، العدد 75، 2023، ص201.

(2) صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، جامعة الشرق الأوسط، كلية الآداب والعلوم، قسم العلوم السياسية، 2021، ص8.

جديدة تحكم العلاقات الدولية، لم تقتصر على البيئة التقليدية لتشمل ادخال التكنولوجيا الرقمية في المجالات كافة، التي تحكم شكل العلاقات الدولية، وعلى المستويات الاستراتيجية والجيوسياسية كافة[3].

لذلك فإنَّ الفضاء السيبراني يشكّل الأداةً في توجه سلوك الدول من جهة، وأحد الوسائل الاحتوائية من جهة أخرى، ومن هنا تنبع خطورة التهديدات السيبرانية، ومدى تأثيرها في العقيدة الاستراتيجية، والعسكرية للدول، نتيجة لما تمتلكه من أدوات من شأنها تدمير أهم المنشآت العسكرية، والأمنية، إذ يمكن القول: إنَّ مفهوم السيبرانية، والقدرة على توظيف الفضاء السيبراني، من شأنه التأثير في الأحداث، والمتغيرات، عن طريق توظيف جميع أدوات القوة السيبرانية، المرتبطة بالبيانات، والمعلومات الإلكترونية[4].

إذ نجد مصالح الدول ارتبطت ارتباطًا مباشرًا بمفهوم الفضاء السيبراني، عن طريق توظيف البنية السيبرانية، التي تُعرف بـ (البنية التحتية للمعلومات)، والمتمثلة في العديد من القطاعات، ومنها: (النفط، والغاز، والنقل، والاتصالات)، فضلاً عن القطاعات الحكومية، والتجارية، والمالية، إذ إنَّ أي تهديد أو هجوم سيبراني على أي قطاع من هذه القطاعات، يمكن أن يؤدي إلى الإخلال بالتوازن الاستراتيجي (الإقليمي، والدولي)، الأمر الذي وضعنا أمام تهديدات جديدة، وأهمها التهديدات السيبرانية، التي تشكّل تحديًا أمام تحقيق الأمن القومي للدول، بما فيها الولايات المتحدة الامريكية، إذ إنَّ تنامي التهديدات السيبرانية، وبروز الحروب السيبرانية، ما هو إلا لقلة تكلفتها مقارنةً بالحروب التقليدية، ومستويات الردع التقليدي[5].

وتُعرَّف التهديدات السيبرانية، بأنَّها: "التلويح بإلحاق الضرر بالأطراف الأخرى، أو القيام بأعمال عدائية ضدهم. كما تعرَّف بأنَّها: "التعبير عن نية التدخل أو ممارسة العداء، وإلحاق الأذى تجاه الطرف الآخر، وهذا ما يُعدُّ أحد التهديدات الأمنية التي تمسّ الأمن القومي للدول". وتعرَّف ايضًا بأنَّها: "مجموعة من المخاطر والتهديدات التي تواجه المستخدمين، سواء كانوا أفرادًا أم دولًا أم منظمات من غير الدول، هدفهم إلحاق الضرر، والتدمير، بالبنى التحتية للدول"[6].

---

(3) نوره شلوش، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، المجلد الثامن ، المجلد 8، العدد 2، 2018، ص189.

(4) معمر منعم العمار، *العقيدة الاستراتيجية وإدراك التهديدات السيبرانية* ، مجلة جامعة تكريت للعلوم السياسية، المجلد3، العدد 25، 2021، ص208.

(5) جاسم محمد طه، *التهديدات السيبرانية وتأثيرها على الأمن القومي الأمريكي*، مجلة جامعة تكريت للعلوم السياسية،المجلد22، 2023، ص184.

(6) *مخاطر الأمن السيبراني*، شركة سايبر للأمن السيبراني، متاح على الرابط الآتي:

https://share.google/WhVy1yd4wNPFLzNzk

ويُعرَّف التهديد السيبراني أيضًا، بأنَّه: "ممارسة عدوانية تُوظَّف فيها الحواسيب، والبرمجيات، والفيروسات، بهدف إلحاق الضرر بالبنى التحتية للدول"، إذ أصبحت التهديدات السيبرانية، وكذلك الهجمات السيبرانية، جزءًا لا يتجزأ من الاستراتيجية الأمنية الخاصة بالدول، فضلاً عن كونها إحدى الأدوات المهمة في تحقيق المصالح والأهداف العليا للدولة[7].

ويُعدُّ مفهوم الأمن، والتهديد، من أهم المفاهيم التي طرأت على النظام الدولي، إذ إنَّ العلاقة بين الأمن والتهديد علاقة متبادلة، ذات تأثير مباشر في مختلف المجالات. ففي السابق اقتصر مفهوم التهديد على الجانب العسكري، المتضمن الهجمات العسكرية، والحروب بأشكالها كافة الصلبة والناعمة (الذكية)، أمَّا اليوم فقد أصبح مفهوم التهديد أخطر واعقد عمَّا كان عليه، والذي ضمَّ أشكالًا عدة، منها: (التهديدات السياسية، والتهديدات الاقتصادية، والتهديدات التكنولوجية، والتهديدات الأمنية) ببعدها الداخلي، والخارجي، إذ يمكن تفسير التهديد على أنَّه: "تعارض المصالح، والأهداف القومية، للدول، وعدم ايجاد حلٍّ سلمي يمنع الدول الحد الأدنى من تحقيق أهدافها السياسية، والعسكرية، والأمنية، وهذا ما يدفع الأطراف المتنازعة إلى اللجوء لاستعمال القوة العسكرية، وهذا ما يؤدي إلى تهديد أمنها القومي". ويُعرِّف باري بوزان التهديد على أنَّه: "تعرض مؤسسات الدولة لتهديد عن طريق استعمال الأيدولوجية، واستخدام جميع مقومات الدولة ضد دولة أخرى، مما قد يعرّض الدولة للخطر الخارجي أو الداخلي (الاحتلال، أو استعمال القوة المسلحة)[8]. ويمكن تحديد عدة معايير لتصنيف التهديدات الأمنية، وعلى النحو الآتي:

1. **المجال**: والذي يتضمن عدة أنواع من التهديدات، منها: (الاقتصادية، والسياسية، والأمنية، والثقافية).
2. **نسبة الخطورة**: والذي تضمن التهديدات المحتملة، والتهديدات الفعلية.
3. **التأثير**: وينقسم على (التهديدات المؤثرة، والتهديدات غير المؤثرة)[9].

إذ تشكّل الدراسات الأمنية أهمية قصوى لدى الباحثين، والمتخصصين، في مجال العلاقات الدولية، ولاسيَّما بعد التطور التكنولوجي، والرقمي الحاصل، مما أدى إلى ظهور فواعل دولية جديدة مؤثرة في السياسة الدولية، والمتمثلة بالفضاء السيبراني، إذ إنَّ المصالح القومية للدول مرتبطة ارتباطاً وثيقًا بالبنية التحتية السيبرانية، وهو ما جعلها أمام مخاطر، وتهديدات سيبرانية دائمة، وهذا ما دفع الولايات المتحدة الأمريكية للتوجه نحو تطوير فضائها السيبراني، بما يحقق أهدافها، ومصالحها المنشودة، إذ يمكن القول: إنَّ الفضاء السيبراني تمكن من خلق بيئة أمنية جديدة في مواجهة التهديدات، حيث عرف قاموس اكسفورد التهديدات السيبرانية بأنَّها: "محاولة طرف ما اتلاف نظام

---

(7) جاسم محمد طه، *مصدر سبق ذكره*، ص185.

(8) سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي للولايات المتحدة الأمريكية أنموذجًا (2001–2017)، رسالة ماجستير، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، (2018)، ص19–20.

(9) عباس بدران، الحروب الإلكترونية: الاشتباك في عالم متغير، مركز دراسات الحوكمة الإلكترونية، بيروت، (2010)، ص4.

الكومبيوتر، أو تدميره، أو تخريبه، أو اختراق المعلومات، والبيانات، الموجود عليه، وتغييرها". كما يمكن تفسيره على أنَّه: "مجموعة من الفايروسات الخبيثة، والتي بإمكانها أن تحدث في مجال الفضاء السيبراني". أمَّا وكالة الأمن السيبراني، وأمن البنية التحتية السيبرانية، فقد عرَّفت التهديدات السيبرانية بأنَّها: "نظام التحكم لأفراد يحاولون اختراق الأجهزة الإلكترونية، عن طريق انعدام مسار اتصال البيانات، والذي يتم بواسطة مستخدمين مجهولين". وتُعرَّف أيضًا بأنَّها: "نظام تحكم أفراد مجهولين، يحاولون العبث، أو اختراق، أو تدمير، جهاز ما، أو شبكة بيانات إلكترونية"[10].

ثانيًا- أنماط التهديدات السيبرانية

يمكن تحديد أهم أنماط التهديدات السيبرانية، بما يأتي:

1- **انقطاع الخدمة:** وذلك عن طريق اطلاق مجموعة من الطلبات على خوادم الحاسوب، وبصورة متسارعة، وبقدرة تفوق الخادم، أو الجهاز، مما يؤدي إلى توقفه بصورة مفاجئة، أو جزئية، ويمكن استخدامها ضد العديد من المواقع الإلكترونية، وكذلك مؤسسات الدولة، أو البنوك، بهدف المساومة المالية.
2- **مسح البيانات أو تعديلها:** إذ يمكن الوصول إلى بيانات دولة ما، ومعلوماتها، ومحاولة العبث في البيانات، أو تضليلها، لاسيَّما البيانات، والمعلومات، الحساسة الخاصة بالمؤسسات الأمنية، والعسكرية، ذات السرية العالية.
3- **عملية التجسس:** وتتم عن طريق التجسس على شبكات الخصم، من دون القيام بعملية التدمير، أو تغيير المعلومات، بهدف الحصول على المعلومات[11].

وعليه يمكن تحديد مفهوم التهديدات السيبرانية، على أنَّها: "مجموعة أفعال تستهدف الامكانات، والقدرات التكنولوجية، بما فيها أجهزة الكومبيوتر، لأغراض قومية أو سياسية، وذلك عن طريق استغلال نقاط الضعف من قبل الخصم، وهذا ما يُمكِّن المهاجم من التلاعب بأنظمة الشبكات". ويمكن وصفها ايضاً على أنَّها: "مجموعة من الهجمات التي تتم عن طريق استعمال مجموعة شبكات، وآليات اختراق، تهدف إلحاق الضرر بالبيانات، والمعلومات، الموجودة على أجهزة الكمبيوتر". لذا فإنَّ التهديدات السيبرانية تهدف إلى تسريب المعلومات، والبيانات، وانتهاك الخصوصية، بهدف سرقتها أو تعديلها[12].

ويمكن تصنيف التهديدات السيبرانية، على النحو الآتي:

---

(10) فاتح حراك ، الفضاء السيبراني والتحول في مفهوم الامن في الولايات المتحدة الامريكية ، اطروحة دكتوراه، جامعة قسطنطينية – صالح بوبندر، كلية العلوم السياسية، 2024، ص75-76.

(11) منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي لبحوث القانونية والفضائية، ط1، بيروت ، 2017، ص25.

(12) رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، المركز المصري للفكر والدراسات الاستراتيجية، (2017)، ص3.

- **التهديدات التقليدية:** تهدف القيام بعدة هجمات سرية، بغرض القيام بعملية التجسس على المعلومات المتعلقة بالمؤسسات الخاصة بالدولة، وبأشكالها كافة (السياسية، والاقتصادية، والعسكرية، والأمنية)، والتي تقوم بها دولة تجاه دولة أخرى، بهدف تحقيق مكانة مهمة، ومتقدمة، في نظرية التنافس الإقليمي، والدولي.
- **التهديدات الرقمية غير التقليدية:** والتي تستهدف نظم معلومات الخصم، بهدف نشر معلومات وهمية داخل نظام المعلومات، والشبكات، كخطوة تكتيكية، واستباقية، ضد الخصم[13].

وبناءً على ما سبق، فإنَّ الفضاء السيبراني يمثل أحد أهم الساحات المفتوحة، التي تضم الفاعلين الدوليين، والفاعلين من غير الدول (التنظيمات الإرهابية، والشركات متعددة الجنسية، والافراد)، فضلاً عن امتلاكه ثلاثة أركان أساسية، وكما يأتي:

1- **الركن المادي:** والذي يصف الفضاء السيبراني على أنَّه: بُعد مادي غير محدد بنطاق معين، إنَّما يشكّل مساحة مفتوحة ذات تأثير كبير، في شكل العلاقات الدولية، وكذلك بنية النظام الدولي.
2- **الركن المنطقي:** هو عبارة عن جهاز عصبي يربط ما بين الاجهزة التكنولوجية، بما فيها أجهزة الكمبيوتر، وشبكة التوجيه.
3- **الركن المعرفي:** ويتضمن العديد من البيانات، والمعلومات، التي يسهل اختراقها، وحذفها، ونقلها، الأمر الذي كشف عن وجود فواعل من غير الدول، ذات تأثير كبير في هذا المجال، فضلاً عن رقمنة جميع قطاعات أمن الدولة (العسكرية، والسياسية، والأمنية)[14].

---

(13) عبد الغاني شرقي، التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة واستفاليا، مجلة السياسة العالمية، المجلد (7)، العدد (2)، (2023)، ص275.

(14) مروة زين العابدين سعد، تأثير تغير مفهوم السيادة على الاقتصاص القضائي في الجرائم السيبرانية، المجلة الدولية للفقه والقضاء والتشريع، المجلد (3)، العدد (3)، (2022)، ص700.

المحور الثاني

دور القدرات السيبرانية في تعزيز الأمن القومي الأمريكي

أولاً- القدرات السيبرانية وتطوير أدوات الردع

تعدُّ الولايات المتحدة الأمريكية الفضاء السيبراني، أحد محركات الاقتصاد العالمي، وأحد العوامل المؤثرة في التجارة العالمية، فضلاً عن كونه أحد الأهداف الرئيسة، التي تسعى الولايات المتحدة الأمريكية إلى تحقيقها، ومحاولة فرض هيمنتها على هذا المجال، وبمستوياته كافة (الأمنية، والاقتصادية، والعسكرية)، إذ نجد الولايات المتحدة الأمريكية تحاول وضع المعايير، والقواعد، التي يجب أن تتبناها المؤسسات الدولية الخاصة في إدارة مجال الأمن السيبراني، وذلك عن طريق تعزيز التعاون المشترك مع حلفائها، ومعادلة فرض الهيمنة على هذا المجال، لما يحمله من مميزات بإمكانها تحقيق أهدافها، ومصالحها الاستراتيجية. إذ يعدُّ البنتاغون أول من أسس شبكة حاسوب في العالم، والتي عرفت باسم (اربانت) (Arpanet)، والتي تشكل النواة الأساسية لإدارة شبكات الإنترنيت الدولية. ويضم البنتاغون ما يقارب (15) ألف شبكة حاسوب، موزعة في (88) دولة، وتخضع الكثير منها لما يعرف بـ (الجدران النارية) (Firewalls)، كما يحتفظ البنتاغون على نسخته السرية من الأمن السيبراني، والتي تعرف باسم (سيبرينت) (Slprnent). وعلى الرغم من أنَّ الولايات المتحدة الأمريكية، تمتلك مقومات القوة السيبرانية، إلا أنَّ أغلبها تخضع خارج الحكومة الأمريكية وسيطرتها، باستثناء وكالة الأمن القومي الأمريكي، والتي تمتلك الامكانات، والوسائل التكنولوجية المتطورة، في مجال الفضاء السيبراني، وكذلك امتلاكها القدرة على المراقبة، وتنفيذ مهمات استباقية، وهجومية، لتحقيق الأهداف المنشودة[15].

كما تهيمن الولايات المتحدة الأمريكية، على أهم الشبكات والمواقع التكنولوجية، ومنها محركات البحث على الإنترنيت (جوجل)، والتي تمتلكه شركة جوجل الأمريكية، بالإضافة إلى شركة مايكروسوفت (أبل)، اللتان تشكلان أهمية كبيرة في قطاع أنظمة الشبكات (operating systems)، وكذلك سيسكو سيستمز (cisco systems) الأمريكية، التي تُعدُّ الأولى في العالم في مجال المعدات الشبكية، فضلاً عن سيطرتها على شبكات التواصل الاجتماعي (تويتر، وفيسبوك، وجوجل)[16].

ففي الآونة الاخيرة أصبح الفضاء السيبراني الفاعل، المهيمن، والمؤثر، في محركات العلاقات الدولية، إذ يشهد العالم تزايدًا في عدد الهجمات السيبرانية، والتهديدات السيبرانية بأشكالها كافة (التجسس السيبراني، والردع السيبراني، والإرهاب السيبراني، والحرب السيبرانية)، إذ يمكن تحديد حجم تلك الهجمات، لاسيَّما أنَّ أغلبها يتم التبليغ عنها. فعلى الرغم من تباين أغراض الهجمات، إلا أنَّ الغاية واحدة وهي الحاق الضرر في الأمن السيبراني للدولة، ومحاولة

---

(15) عمر عبد الله عفتان، الاستراتيجيات والسياسات المتبعة في مواجهة التهديدات السيبرانية، مجلة الفارابي للعلوم الانسانية، العدد (3)، الجزء (1)، (2024)، ص248.

(16) عبد الله مسعود، دراسات في الأمن القومي، رسالة ماجستير، كلية الادارة والاقتصاد، جامعة بنغازي، (2002)، ص42.

إضعاف الخصم، واستغلال نقاط الضعف، عن طريق اختراق أجهزة الشبكات (الإنترنيت)، وتدميرها. وعليه يمكن القول: إنَّ الفضاء السيبراني يشكّل مجالاً لإدارة الحرب، والصراع، فضلاً عن كونه أحد الفواعل المؤثرة في بناء الاستراتيجيات، وهذا ما أكده صناع القرار، والمختصين في هذا المجال[17].

تُعدُّ الولايات المتحدة الأمريكية من أوائل الدول التي قامت بإنشاء جيوش سيبرانية، وظيفتها تحقيق الأهداف الاستراتيجية العليا للدولة، عن طريق السيطرة على البيانات، والمعلومات الخاصة بالمؤسسات العسكرية، والأمنية، الأمر الذي دفع بالدول الأخرى ومنها الصين، وروسيا، إلى إنشاء وحدات سيبرانية، أو ما يسمى بالمجالس السيبرانية، بهدف حماية أنظمتها، ومعلوماتها من أي خرق سيبراني محتمل، إذ خصصت الولايات المتحدة ما يقارب (7) مليار دولار سنوياً، لخدمة المجال السيبراني، والأمن السيبراني، والعمل على تطويره، كما بلغ عدد الموظفين العاملين في مجال القرصنة السيبرانية، أكثر من (9) آلاف عامل، وهي بذلك تحتل المرتبة الأولى عالميًا، من ناحية الاتفاق السنوي على مجال الفضاء السيبراني. وتعتمد الولايات المتحدة الأمريكية في مواجهة التهديدات السيبرانية، على خمسة عناصر أساسية، تتمثل في:

1- **القيادة:** والتي تختص بالتنظيم، والتنسيق المسبق، وإدارة الهجمات السيبرانية بالتعاون مع الوحدات الأخرى، ومنها وحدة الجيش السيبراني الأمريكي.
2- **السايبر:** وضيفتها حماية منشأة المارينز، وتأمينها، من أي خروقات، وهجمات سيبرانية مؤكدة، أو محتملة.
3- **وحدة الجيش السيبراني البحرية:** وضيفتها جمع البيانات، والمعلومات، وعملها عمل الوحدات السابقة.
4- **وحدة القوة الجوية (24):** والمسؤولة عن حماية القوات الجوية الأمريكية، وتضم (3) أجنحة.
5- **الاسطول العاشر الأمريكي:** ومهامه جمع المعلومات الاستخباراتية لصالح القوات الأمريكية[18].

لذلك فإنَّ القدرات السيبرانية جزءًا لا يتجزأ من استراتيجية الأمن القومي للدول، بما فيها الولايات المتحدة الأمريكية، كما أنَّها تشكّل إحدى الأدوات الأساسية في تعزيز النفوذ الاستراتيجي، وتحقيق التوازن، إذ إنَّ الولايات المتحدة الأمريكية قد حققت تطورًا شاملاً وسريعًا في مجال فضائها السيبراني، والعمليات السيبرانية الهجومية ذات السرية العالية، والتي استخدمتها لأغراض أمنية، وعسكرية، مع ضمان استمرار عمل الوكالات الاستخباراتية التابعة لها، عن طريق جمع المعلومات، والبيانات الخاصة، للسيطرة على شبكات الإنترنيت. ولأنَّ مجال الفضاء السيبراني مسيطر عليه من قبل الولايات المتحدة الأمريكية، الأمر الذي دفعها إلى تطوير هذا المجال، والذي يشكّل أحد أهدافها

---

(17) حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة الأمريكية وروسيا أنموذجًا)، الطبعة الأولى، دار انكي للنشر والتوزيع، (2022)، ص128.

(18) ما هي أفضل خمسة جيوش إلكترونية في العالم؟ وما ترتيب الجيش السيبراني الروسي، 2017/1/3، مركز أبحاث كاتيغون، متاح على الرابط الآتي: https://2u.pw/d7mGez

الاستراتيجية[19]. إذ يرى المختصون في هذا المجال، ومنهم ديفيد كلارك، أنَّ الولايات المتحدة هي الدولة الأقوى، والأعظم، من حيث قدراتها السيبرانية، كما أكد مركز أبحاث بريطاني في تقرير نُشر عام (2021)، على أنَّ الولايات المتحدة هي الدولة الأولى عالميًا، في امتلاك القدرات، والإمكانات السيبرانية، ولا توجد دولة أخرى منافسة لها في هذا المجال. أمَّا المعهد الدولي للدراسات الاستراتيجية فيرى أنَّ الولايات المتحدة الأمريكية، هي الدولة الأولى المهيمنة على القوة السيبرانية، ومجال الفضاء السيبراني، فضلًا عن امتلاكها القدرة على المنافسة في هذا المجال (روسيا، والصين، وكوريا الشمالية)[20]. ويمكن القول: إنَّ الولايات المتحدة هي الدولة الأكثر تفوقًا، وتطورًا، في مجال الفضاء السيبراني، والأمن السيبراني، بجميع أشكاله، كذلك امتلاكها ما يُعرف بـ "القيادة السيبرانية الأمريكية" (USCYBERCOM)، التابعة للقيادة المركزية في وزارة الدفاع الأمريكية، والتي أُنشئت عام (2009) في مقر الأمن القومي الأمريكي في ولاية ميريلاند، والتي تمتلك سلطة توجيهه لإدارة القدرات السيبرانية، والفضاء السيبراني، فضلاً عن قدرتها على الحد من الهجمات، والتهديدات السيبرانية، عن طريق سيطرتها على الأنظمة الحيوية، وحمايتها من أي خرق، أو تهديد سيبراني[21].

وتمتلك الولايات المتحدة العديد من العوامل، التي منحتها لأن تكون قوة بارزة، ومؤثرة، في هذا المجال، سواء كان على صعيد التنافس أم التعاون مع القطاع الخاص، ومجال الاستثمار، إذ إنَّها تسيطر على أهم شركات التكنولوجيا العملاقة في العالم، والتي يُطلق عليها تسمية "الشركات الخمس العظمى" (big tech)، والمتمثلة بـ (أمازون، وآبل، وغوغل، وميتا، ومايكروسوفت)، ومقرها في الولايات المتحدة الأمريكية، والتي تشكّل إحدى أهم الأدوات الرئيسة في التوجهات الاستراتيجية الأمريكية، وأحد مرتكزات قوتها الناعمة[22]. وبحسب الاحصاءات، والمعطيات، فقد بلغ عدد المستخدمين لوسائل التواصل الاجتماعي في الداخل الأمريكي، ما يقارب (245.5) مليون مستخدم، أي ما يعادل نحو (72.5%) من إجمالي السكان حتى عام (2023). لذلك فإنَّ التفوق، والتطور، في المجال السيبراني، وتعزيز القدرات السيبرانية، بات أمرًا ضروريًا لتعزيز المصالح الاستراتيجية الأمريكية، إذ أصبحت التكنولوجيا الرقمية أحد أهم المحددات في بناء الاستراتيجيات الأمريكية، وتطويرها، إذ ترى الحكومة الأمريكية أنَّ مجال الفضاء السيبراني، يجب أن يعزز القدرات العسكرية، فضلاً عن ممارسة الأنشطة الاستخباراتية، والأمنية، بهدف حماية أمنها القومي من أي خرق، أو تهديد سيبراني محتمل، والعمل على ردع القوى الدولية المنافسة لها (الصين، وروسيا، وكوريا الشمالية)، وحماية بنيتها التحتية من أي خرق سيبراني، وبالتعاون مع

---

(19) فرد كايلان، *المنطقة المعتمة: التاريخ السري للحرب السيبرانية*، ترجمة: لؤي عبد المجيد، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، (2019)، ص12.

(20) خالد وليد محمود، الفضاء *السيبراني وتحولات القوة في العلاقات الدولية*، الطبعة الأولى، المركز العربي للأبحاث ودراسة السياسات، بيروت، (2025)، ص232.

(21) Defense, 3/5/2018, accessed & to combatant command) us Departmant) zisa Ferdinando, (cyber com to Elevate on https://bit.ly/3 at: 21/9/20231 .

(22) خالد وليد، مصدر سبق ذكره، ص240.

حلفائها الدوليين. وعليه فيمكن القول: إنَّ الولايات المتحدة تمتلك قوة سيبرانية متطورة، وهذا ما دفعها إلى الهيمنة على مجال الفضاء السيبراني، وتحقيق السيادة السيبرانية، عن طريق مجموعة من الاستراتيجيات، والآليات، التي تتبعها الولايات المتحدة، ومنها السيطرة على منظمة "آيكان" (ICANN)، وهي إحدى المنظمات المسيطرة على إدارة النطاقات على شبكات الإنترنيت، وهذا ما يعزز من دور الولايات المتحدة في تحقيق أهدافها، ومصالحها، وضمان استمرارية الهيمنة على مجال الفضاء السيبراني، فضلاً عن تطوير مجالها التكنولوجي، ومكافحة التهديدات السيبرانية، وزيادة قدراتها الدفاعية، والهجومية، في هذا المجال[23].

ثانيًا- أثر التهديدات السيبرانية في الأمن القومي الأمريكي

نتيجةً للمتغيرات، والتحديات، التي يشهدها العالم، وأهمها ثورة المعلومات، والتكنولوجيا، التي أحدثت نقلة نوعية في مسار العلاقات الدولية، برزت ظاهرة ما يُعرف بالتهديدات السيبرانية، وكذلك الحروب السيبرانية، والتي صُنّفَت من قِبل البعض على أنَّها مجموعة من الأعمال التي تقوم بها الدول، بهدف اختراق المعلومات، والبيانات، التي تمتلكها دول أخرى، هدفها إلحاق الضرر، وسرقة المعلومات التابعة لها. إذ أصبحت التهديدات السيبرانية إحدى أدوات إدارة الصراع، والتنافس، والتي تستعملها الدول المتقدمة بما فيها الولايات المتحدة، لتحقيق أهدافها، ومصالحها الاستراتيجية، وهذا ما أكَّده "ديفيد جوميرت" قائلاً: "إنَّ من أهم الآثار المترتبة لثورة المعلومات، والتكنولوجيا، هو قيام الحرب السيبرانية، أي الحرب التي تقتصر في خوضها على المعلومات، والبيانات، مؤكدًا أنَّها سلاح، وهدف تسعى الدول إلى تحقيقه". ومما لا شكَّ فيه إنَّ من يمتلك قدرات، وإمكانات سيبرانية، والقدرة على توظيف الفضاء السيبراني بأشكاله كافة، في عالمنا اليوم فهو الأكثر قدرة في التأثير في سلوك الفاعلين، والمستخدمين لهذا المجال، إذ تشير التطورات التكنولوجية، بما فيها مجال الذكاء الاصطناعي، وتعدد الإمكانات، والقدرات، فضلاً عن تعدد الوسائل، والأهداف، في هذا المجال، إلا أنَّها تشكّل أكثر المجالات خطرًا، وتهديدًا في القرن الحادي والعشرين، نتيجة لتوظيفه في مجال الفضاء السيبراني، وإسهامه في تهيئة بيئة إقليمية، ودولية جديدة، تستند إلى معايير، وفواعل، مؤثرة في هذه البيئة (الأفراد، والدول، والشركات المتعددة الجنسيات، والمنظمات الإرهابية)[24].

لذلك يمكن القول: إنَّ المصالح القومية الأمريكية مرتبطة ارتباطًا وثيقًا، في بنية الفضاء السيبراني والتي تُعرف باسم (البنية التحتية القومية للمعلومات)(N11)، والمتمثلة بمجالات عدة، منها (الطاقة، والاتصالات، والمؤسسات المالية والتجارية)، ومن ثَمَّ فإنَّ أي تهديد سيبراني يمس هذه المجالات، قد يؤدي إلى الإخلال في التوازن الاستراتيجي الإقليمي، والدولي، وهذا ما سيؤدي إلى ظهور أنماط جديدة من التهديدات، التي تمس الأمن القومي للدول، فضلاً عن بروز

(23) خالد وليد، المغالبة والتنافس في القدرات السيبرانية الأمريكية الصينية، مجلة شؤون استراتيجية، العدد (18)، (2024)، ص184.

(24) فراس جمال شاكر الحربي، المعلوماتية في المجال الأمني والعسكري: أمريكا والصين أنموذجًا، الطبعة الأولى، الدار العربية للنشر والتوزيع، بيروت، (2023)، ص195.

أنماط جديدة من الحروب، ومنها الحروب السيبرانية غير التقليدية. وهنالك عدة محفزات لظهور مثل هذه الأنماط من الحروب، والمتمثلة في ما يأتي[25]:

1. **تزايد التهديدات السيبرانية**: والمتمثلة في قدرة المؤسسات سواء العسكرية أم المدنية، على شن هجمات سيبرانية تجاه الدول الأخرى، ومحاولة خرق أنظمتها الإلكترونية، وسرقة معلوماتها. ومن ثَمَّ فإنَّ التهديد السيبراني أصبح أحد الأدوات المهمة، التي يمكن للدول توظيفها في زمن السلم، والحرب.

2. **تعزيز القدرات السيبرانية**: إذ أثّر مجال الفضاء السيبراني، في إعادة تشكيل الفواعل المؤثرة في هذا المجال، وفي مقدمتها الولايات المتحدة الأمريكية، التي تُعدُّ إحدى القوى المهيمنة، والمسيطرة على هذا المجال، ولكن سرعان ما أصبح هذا المجال متاحًا لجميع القوى الأخرى، مما أثَّر في العديد من المجالات، كمجالي التنافس والتعاون، وعلى الصعيدين الإقليمي، والدولي.

3. **درج الأمن السيبراني ضمن الأمن القومي للدول**: عن طريق إنشاء وحدات تمتلك مهام عدة، أهمها القيام بالمناورات العسكرية لتعزيز قدراتها السيبرانية، وإنشاء مشاريع وطنية تعزز من القوة، والقدرة، السيبرانية للدولة.

4. **عسكرة الأمن السيبراني**: عن طريق بناء استراتيجيات عدة في مواجهة التهديدات، والمخاطر، السيبرانية (دفاعية، وهجومية، ووقائية)، فضلاً عن تعزيز القدرات في مجال سباق التسلح السيبراني[26].

---

(25) عادل عبد الصادق، *أنماط الحرب السيبرانية وتداعياتها على الامن العالمي*، مجلة السياسة الدولية، مؤسسة الأهرام، مصر، (2017)، ص53.

(26) جاسم محمد طه، *مصدر سبق ذكره*، ص 205.

المحور الثالث

آليات توظيف الاستراتيجية الأمريكية في مواجهة التهديدات السيبرانية

نتيجة تزايد التهديدات السيبرانية، والهجمات السيبرانية، اتجهت العديد من القوى الدولية بما فيها الولايات المتحدة الأمريكية، إلى تعزيز قدراتها الدفاعية، والهجومية، في المجال السيبراني، فضلاً عن توظيف مجال فضائها السيبراني لأغراض عسكرية، وأمنية، بهدف حماية أمنها القومي. فقد دفع التطور المعلوماتي، والتكنولوجي، الذي يشهده عالمنا اليوم، القوى الدولية إلى إعداد استراتيجيات سيبرانية، لمواجهة المخاطر، والحروب الجديدة، والتي أثرت في العديد من المجالات، وأهمها الأمنية، والعسكرية. كما تُعدُّ الولايات المتحدة من أوائل الدول، التي انتهجت العديد من الاستراتيجيات السيبرانية، هدفها حماية مصالحها القومية من أي مخاطر، وتهديدات سيبرانية محتملة[27]. ويمكن تحديد أهم الاستراتيجيات الأمريكية المرتبطة بالفضاء السيبراني الأمريكي، وخلال الرئاسات المتعاقبة، وعلى النحو الآتي:

أولاً- استراتيجية الأمن السيبراني في عهد الرئيس الأمريكي (باراك أوباما)

اتخذت الإدارة الأمريكية في عهد الرئيس الأمريكي السابق باراك اوباما، مجموعة من الاجراءات، والتدابير الوقائية، لمواجهة التهديدات، والحروب السيبرانية. ففي عام (2009)، أعلنت وزارة الدفاع الأمريكية عن تشكيل خلية عسكرية للأمن السيبراني، مهمتها حماية الشبكات، والأنظمة التابعة للجيش الأمريكي، والتصدي للهجمات، والتهديدات السيبرانية، من أي خرق، أو تدمير، من قبل الخصم، إذ ارتبط مجال الفضاء السيبراني بالأمن القومي الأمريكي بأشكاله كافة، نتيجة لما يحمله هذا الفضاء من مخاطر، وتهديدات، تمس الأمن القومي الأمريكي. وفي عام (2010)، أصدرت حكومة اوباما استراتيجية وطنية، تستهدف مواجهة التهديدات (الحرب السيبرانية، والإرهاب السيبراني، والتهديدات السيبرانية)[28]. أمَّا في عام (2011)، فقد أصدرت الحكومة الأمريكية أول وثيقة للأمن السيبراني، والتي تُعدُّ بمنزلة استراتيجية وطنية، تضمن العديد من الأهداف الثابتة، وأهمها الحفاظ على المزايا المستمدة من الفضاء المعلوماتي، والسيبراني، وتطوير البنى التحتية[29].

كما اعتمدت الاستراتيجية الوطنية الأمريكية، على توظيف الإمكانات، وتطوير مجالات التعاون في قضايا الأمن السيبراني، على المستويين الإقليمي، والدولي، فضلاً عن إنشاء منصّة موحّدة تُدير التفاعلات الدولية داخل الفضاء السيبراني، بهدف تعزيز الأمن السيبراني للاستراتيجية السيبرانية الدولية، وكذلك تعزيز القدرات عن طريق إرساء مبدأ التعاون مع الدول النامية، والتي تفتقر إلى التطور التكنولوجي، والمعلوماتي، وفتح المجال أمام الدول لإعداد

---

(27) عبد الغفار عفيفي ، استراتيجية الردع السيبراني: التجربة الامريكية، مجلة السياسة الدولية، مركز الاهرام للدراسات الاستراتيجية ، العدد 213، 2018، ص196.

(28) عادل عبد الصادق، الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، المركز العربي للأبحاث الفضاء الالكتروني، متاح على الرابط: https://2u.pw/XJ06Z9

(29) جاسم محمد طه، *مصدر سبق ذكره*، ص207.

الاستراتيجية الوطنية السيبرانية، عن طريق توفير عنصري الدعم، والمساندة، للدول، عن طريق توفير الخبرات، والمتخصصين، في المجال السيبراني، وتحسين البنية التحتية، وهذا ما جعل الولايات المتحدة في الدول الأولى عالميًا، في إعداد الاستراتيجيات السيبرانية لمواجهة المخاطر، والتهديدات، والتي ركزت في ضمان السلام بالقوة، وإدارة المخاطر التي تمس الأمن القومي الأمريكي، فضلاً عن تفعيل الأدوار، وتعزيز الامكانات، والقدرات المحفزة للتعاون الدولي، وتبادل المعلومات[30]، لاسيَّما أنَّ الفضاء السيبراني، أصبح يُشكّل أخطر التحديات الأمنية، والاقتصادية، وأهمها، للولايات المتحدة الأمريكية[31]. إذ أكدت الإدارة الأمريكية على تعزيز الأهداف الوطنية للاستراتيجية السيبرانية الأمريكية، وأهمها تعزيز الأمن القومي الأمريكي في الداخل، إذ أعلن وزير الدفاع الأمريكي السابق "ويليام جم"، التعامل مع الأمن السيبراني كعقيدة عسكرية، بوصفها أحد المجالات المؤثرة في الفضاء الخارجي، فضلًا عن الأهداف الأخرى، والمتضمنة دعم المعايير الدولية، وتعزيزها، عن طريق التطور التكنولوجي لاسيَّما في مجالي التجارة الحرة، والاستثمار، فضلاً عن حماية الملكية الفكرية، كذلك دعم الأسس، والمبادئ الديمقراطية، وحرية التعبير عن الرأي، وهذا ما جاءت به حكومة أوباما، التي اتّصفت بأنَّها إدارة تفاعلية في دعم الأسس الديمقراطية العالمية، وحقوق الإنسان، والتي نادت بها الاستراتيجية الأمريكية في عهد الرئيس اوباما[32]. وعليه يمكن تحديد أهم الأهداف التي جاءت بها الاستراتيجية الوطنية للأمن السيبراني، في عهد الرئيس الأمريكي السابق باراك أوباما، وكالآتي:

- تعزيز القدرات والإمكانات التكنولوجية، والمعلوماتية، في مواجهة التهديدات، والمخاطر، السيبرانية، في المستقبل.
- إنشاء مبادرة وطنية شاملة للفضاء السيبراني (cncl)، تحت إشراف وحدات الأمن القومي الأمريكي.
- حماية البنى التحتية من أي خرق، أو هجوم سيبراني محتمل، أو مؤكد (الطاقة، والنقل، والتجارة، والأمن)[33].

وقد جاءت هذه الأهداف بعد تعرض الولايات المتحدة الأمريكية، للعديد من الهجمات، والتهديدات السيبرانية، من قبل كلٍّ من الصين، وروسيا، والتي كانت لها تداعيات خطيرة على الأمن القومي الأمريكي، وكذلك المؤسسات الأمريكية[34].

---

(30) حازم جري، مصدر سبق ذكره ، ص194.

(31) سليم الدحماني، مصدر سبق ذكره، ص72.

(32) ثامر سعيد عبد اللطيف، الاستمرارية والتغيير في استراتيجية الأمن السيبراني للولايات المتحدة الأمريكية خلال المدة 2009–2024، مجلة تكريت للعلوم السياسية، العدد 69، 2020، ص 270–271.

(33) The Comprehensive White Hou Se & National Cybersecurity initiative / (2008 /https://www.witehouse.gov issues / foreign – Policy.

(34) ثامر سعيد عبد اللطيف، مصدر سبق ذكره ، ص272.

نستنتج ممَّا تقدم أنَّ الاستراتيجية الوطنية السيبرانية، في عهد الرئيس السابق أوباما في ولايته الأولى، كانت أكثر مرونة، وأكثر دبلوماسية، في التعامل مع مجال الفضاء السيبراني، عن طريق تعزيز القيم التعاونية بين القوى الدولية، فضلاً عن تعزيز مبدأ الحريات، وترسيخه، وإحلال أسس الديمقراطية، ومبادئها التي نادت بها الحكومة الأمريكية، منذ تولي الرئيس باراك أوباما السلطة في عام (2009). أمَّا في ولايته الثانية، وبعد عام (2015)، وبعد تعرض الولايات المتحدة الأمريكية للعديد من الهجمات السيبرانية الخطيرة، اتخذت الاستراتيجية الوطنية السيبرانية، نحو استعمال القوة، وإعادة هيكلة أولوياتها تجاه الدول المهددة للأمن القومي الأمريكي (الصين، وروسيا، وكوريا الجنوبية)، وهذا ما جعلها تعيد رؤيتها في صياغة استراتيجيتها السيبرانية، وكذلك أهداف أمنها السيبراني.

ثانيًا- استراتيجية الأمن السيبراني في عهد الرئيس الأمريكي (دونالد ترامب)

أطلق الرئيس الأمريكي دونالد ترامب بعد توليه الرئاسة في أمريكا، الاستراتيجية السيبرانية الوطنية عام (2018)، والتي استهدفت مواجهة التهديدات، والمخاطر السيبرانية، الموجهة ضد الولايات المتحدة الأمريكية، وتُعدُّ أول استراتيجية قدمت هيكلية مفصلة لحماية الفضاء السيبراني الأمريكية. وتقوم الاستراتيجية السيبرانية في عهد الرئيس ترامب، على قناعة ثابتة بأنَّ الولايات المتحدة الأمريكية، هي التي أنشأت شبكات الإنترنت، لذا فهي المسيطرة على مجال الفضاء السيبراني، وكذلك المسؤولة عن حمايته، إذ تعمل الاستراتيجية الأمريكية على الحد من القيود، التي فرضتها الإدارات السابقة للحكومة الأمريكية، والتي تقيّد القيام بهجمات سيبرانية على الخصوم، كونها قائمة على مبدأ التعاون أكثر من التنافس، إذ أكَّد ترامب على ضرورة السماح للمؤسسات، والوكالات الأمنية، والعسكرية، بالقيام بهجمات سيبرانية تستهدف حماية الأنشطة، والشبكات المعلوماتية. وتتصف هذه الاستراتيجية بكونها استراتيجية هجومية، مقارنة بالاستراتيجيات السابقة المرتبطة بالإدارة الأمريكية، فهي تهدف إلى ردع الخصم، وتقييده، واستنزاف مصادر قوته السيبرانية، إذ تأتي هذه الاستراتيجية في إطار مساعي إدارة ترامب، لإنشاء جيش سادس للولايات المتحدة الأمريكية، تكون مهمته إدارة الفضاء السيبراني، وحمايته، وتحقيق السيطرة، والهيمنة عليه، لاسيَّما في ظل وجود قوى منافسة في مجال الفضاء السيبراني (الصين، وروسيا، وكوريا الجنوبية)[35]. وتقوم الاستراتيجية السيبرانية في عهد الرئيس ترامب، على أربعة مرتكزات رئيسة، تتضمن ما يأتي:

1-**تعزيز الأمن القومي الأمريكي:** ويجري ذلك عن طريق تبادل المعلومات، والبيانات، بين المؤسسات والوكالات الفيدرالية الأمريكية، بهدف حماية الشبكات، والأنظمة المعلوماتية، وحماية البنى التحتية، وتأمينها، من أي خرق، أو هجوم سيبراني محتمل، فضلاً عن إعطاء، ومنح صلاحيات شاملة لوزارة الأمن الوطني الأمريكية، لأخذ دورها الرقابي، ومكافحة التهديدات السيبرانية، ومخاطرها، وذلك عن طريق تعزيز التعاون المشترك مع الدول الأخرى[36]. إذ تسعى إدارة الرئيس الأمريكي ترامب، إلى التصدي للمخاطر، والتهديدات، التي تشكّل خطرًا أمام تحقيق أمنها القومي. وركَّزت

---

(35) عمرو عبد العاطي، استراتيجية أمريكية هجومية ضد التهديدات السيبرانية، المركز المصري للفكر والدراسات الاستراتيجية، متاح على الرابط الآتي: https://ecss.com.eg/2077/

(36) علي محمد الرفاعي، تحديات الامن في الفضاء السيبراني الامريكي ، مجلة دراسات دولية، العدد 85، 2021،ص 308.

الاستراتيجية الأمريكية للأمن السيبراني، في عنصرين الهجومية، والاستباقية في مواجهة المخاطر السيبرانية وبأشكالها كافة (النقل، والصحة، والاتصالات، وتكنولوجيا المعلومات)، فضلاً عن حماية البنى التحتية من أي خرق سيبراني.

2- **انتعاش الاقتصاد الأمريكي:** تسعى الإدارة الأمريكية إلى تعزيز الفضاء السيبراني، وتطويره، بما فيها المجال التكنولوجي، والمعلوماتي، فضلاً عن تحقيق النمو الاقتصادي، وذلك عن طريق دعم الاقتصاد الرقمي، وتقديم الدعم اللازم للقوى الأمريكية العاملة، وتوظيف المجال السيبراني بما يخدم الاقتصاد الأمريكي، في تحقيق مستويات عالية من التقدم، والازدهار الاقتصادي[37].

3- **إحلال السلام باستعمال القوة:** تعمل الإدارة الأمريكية على تحقيق قيم الأمن والسلام، وترسيخها، وذلك عن طريق تعزيز قدراتها، وإمكاناتها، واستعمال القوة في فرض الأمن، والاستقرار، وحماية أمنها القومي، بالتعاون مع حلفائها الاستراتيجيين، والتي تتيح استعمال القوة لأغراض الدفاع من أي تهديد، أو خطر سيبراني، وتحقيق مستوى عالٍ من الاستقرار في مجال الفضاء السيبراني الدولي.

4-**تعزيز الهيمنة والنفوذ الأمريكي في المحيط الخارجي:** ذلك بغرض توسيع نطاقها في مجال الفضاء السيبراني.

5-**مكافحة التهديدات السيبرانية:** ذلك عن طريق توظيف جميع مقومات القوة الأمريكية، بما فيها التكنولوجيا لمنع أي هجوم سيبراني، فضلاً عن تعزيز المعايير الدولية في مجال الأمن السيبراني، بما يخدم المصالح، والأهداف الأمريكية[38].

6- **عسكرة الفضاء السيبراني:** ذلك عن طريق إنشاء وكالات فضائية، وقيادة فضائية، مهمتها التصدي للحروب السيبرانية، والحفاظ على الهيمنة الدولية على القوى المنافسة للولايات المتحدة الأمريكية (الصين، وروسيا)، وتبنى استراتيجيات دفاعية، وهجومية سيبرانية، مرتبطة بالأجهزة الأمنية، والدفاعية، مهمتها تطوير أدوات الردع السيبراني تجاه التهديدات السيبرانية[39]، إذ يمكن القول: إنَّ الاستراتيجية السيبرانية الأمريكية هي الأقوى في مجال الفضاء السيبراني، فضلًا عن أنَّ هدفها الهيمنة على مجال الأمن السيبراني الدولي، ومن ثمَّ فإنَّ الاستراتيجية السيبرانية في عهد الرئيس ترامب، كانت تعمل على رسم مستقبل قريب فريد من نوعه، يتجه نحو قيام نظام سيبراني متعدد الأقطاب، وفق مفهوم توازن القوى السيبراني[40]. إذ دعا الرئيس الأمريكي ترامب عام (2019)، إلى تأسيس ذراع عسكري جديد تحت مسمى (القيادة الفضائية)، والتي تخضع للمقوّمات العسكرية

---

(37) ثامر سعيد عبد اللطيف، مصدر سبق ذكره، ص273-274.

(38) حازم جري، مصدر سبق ذكره ، ص201.

(39) سوزي رشاد، التهديدات الأمنية: الهجين في العلاقات الدولية السيبرانية والذكاء الاصطناعي نموذجًا، مجلة وادي النيل للدراسات والبحوث الإنسانية والاجتماعية والتربوية، المجلد (33)، العدد (33)، (2022)، صفحة81.

(40) حازم حمد موسى، مطارحات هيمنة الاستراتيجية الأمريكية السيبرانية، مجلة جامعة تكريت، المجلد (3)، العدد (37)، (2021)، صفحة32.

الأمريكية، ممّا أثار طموحات القوى، والأحزاب المنافسة لها، بما فيها الصين، والتي عدَّت الهيمنة الأمريكية على مجال الفضاء السيبراني، ما هي إلا انتهاك لمعايير الأمن، والسلام الدولي، كما دعا المجتمع الدولي إلى تقييد مجال الفضاء السيبراني، كي لا يتحول إلى ساحة معركة جديدة، وسيخل بميزان القوى الدولي، إذ أعلنت القيادة الروسية بأنَّ الولايات المتحدة الأمريكية، توظف المجال السيبراني لتحقيق أهدافها العسكرية، عن طريق عسكرة الفضاء السيبراني، وهذا ما سيهدد مصالح روسيا، وأهدافها الاستراتيجية[41].

كما تبنت الولايات المتحدة الأمريكية استراتيجية الهجوم السيبراني، التي تُعدُّ أحد أهم الاستراتيجيات الأمنية في مواجهة التهديدات السيبرانية، والتي تعمل بخطوات استباقية بهدف حماية الأمن القومي الأمريكي، والمصالح الحيوية، وتضمن هذه الاستراتيجية عدة أهداف، أهمها:

1- تعزيز التعاون المشترك بين الولايات المتحدة الأمريكية، وحلفائها الاستراتيجيين (أستراليا، وبريطانيا، وكندا، ونيوزيلندا)، في مواجهة المخاطر السيبرانية.
2- استثمار الفرص والتجارب الدولية في مجال الحرب السيبرانية، بما فيها الحروب السيبرانية بين روسيا، وأوكرانيا، والتي وضَّفت الأدوات السيبرانية إلى جانب التقليدية، في حربها ضد أوكرانيا.
3- الاستباقية: التي تتضمن توظيف ما يسمى بسياسة "الانخراط المستمر"، والذي يدعو إلى الكشف المبكر عن التهديدات السيبرانية كخطوة استباقية، وتدمير البنى التحتية التي تستخدمها الجهة المهددة (الدول، والأفراد، والمنظمات)، وتعطيلها.
4- القيام بهجمات سيبرانية عدة بهدف تحديد التهديدات، والمخاطر، ومحاولة القضاء عليها، كما هو الحال مع الهجمات السيبرانية التي تعرضت لها، كل من دول البلطيق، وأوروبا الشرقية[42].

ويمكن القول: إنَّ الاستراتيجية السيبرانية في عهد الرئيس الأمريكي ترامب، تقوم على خمسة مرتكزات أساسية، والمتمثلة بما يأتي:

أ- توظيف جميع مقومات الأمن السيبراني، بهدف تحويل القيادة السيبرانية إلى قيادة دفاعية، وقتالية موحدة، وهذا ما يعزز التعاون بين الوحدات العسكرية الأمريكية، المعنية في مجال الأمن السيبراني.

---

(41) مروة الأسدي، الفضاء: أحدث ساحة قتال في العالم، المقال متاح على الرابط الآتي: https://annabaa.org/arabic/sciences/21860

(42) تقى اياد خليل القيسي، حروب الجيل السادس واستراتيجية المواجهة السيبرانية أنموذجًا، مجلة كلية القانون والعلوم السياسية، السنة السابعة، العدد (227)، (2025)، ص414-415.

ب_ القيام بعمليات، وهجمات سيبرانية، تعزز المزايا العسكرية، والأمنية الأمريكية[43].

ج_ تأمين أمن المعلومات، وشبكات التعاون، وحمايتها، من أي هجوم سيبراني، وذلك عن طريق عدة تشريعات تمنح سلطة وزارة الدفاع، حق الرد على أي خروقات سيبرانية بطرق قانونية.

د_ تعزيز التعاون المشترك في مجال الأمن السيبراني، مع الشركات التي تعمل في القطاع الخاص، أو على المستوى العالمي.

هـ- حماية البنى التحتية من أي هجمات سيبرانية، وذلك عن طريق رفع مستوى جاهزية الدفاع السيبراني الأمريكي[44].

ممَّا تقدم، يمكن أن نستنتج أنَّ الاستراتيجية السيبرانية الأمريكية في عهد الرئيس الأمريكي ترامب، تهدف إلى وضع الأسس والمعايير العالمية، لكيفية استعمال الفاعلين (الدول، والأفراد، والشركات) للفضاء السيبراني من جهة، واستمرار الهيمنة الأمريكية على مجال الفضاء السيبراني، وحماية المصالح القومية من أي هجوم سيبراني من جهة أخرى، لاسيَّما بعدما شنت القوى الفاعلة (روسيا، والصين)، هجمات عدة بهدف زعزعة أمن الولايات المتحدة الأمريكية، واستقرارها، وكذلك ضرب مصالحها الاستراتيجية. كما يمكن وصف الاستراتيجية السيبرانية، على أنَّها استراتيجية دفاعية، وهجومية، تتيح للدولة القيام بمزيد من الهجمات السيبرانية، ووفقاً لمذكرة التفاهم التي أبرمتها الإدارة الأمريكية مع الأمن القومي الأمريكي، وعلى العكس من الاستراتيجية السيبرانية المتبعة في عهد الرئيس الأمريكي السابق باراك أوباما.

ثالثاً- استراتيجية الأمن السيبراني في عهد الرئيس الأمريكي جو بايدن

يشكّل الفضاء السيبراني في عهد الرئيس الأمريكي جو بايدن، أحد أهم أولويات السياسة الخارجية الأمريكية، إذ أكَّد الرئيس الأمريكي جو بايدن، وقبل توليه السلطة في أمريكا عام (2020)، أنَّ الأمن السيبراني هو أولوية قصوى في إدارته القادمة، لاسيَّما بعد تعرض الولايات المتحدة الأمريكية للعديد من الهجمات السيبرانية. ووفقاً لما تناولته الصحيفة الأمريكية (وول ستريت جورنال)، أنَّ الاختراقات السيبرانية مست العديد من المؤسسات الأمريكية، وإلى ما يقارب (20) مؤسسة في عهد الرئيس الأمريكي الحالي ترامب، إذ اتهم الرئيس الأمريكي جو بايدن الحكومة السابقة بالتقصير، والاهمال، في مجال الأمن السيبراني، كما أكَّد أنَّه سوف يتخذ العديد من الاجراءات الصارمة، لتعزيز الأمن السيبراني الأمريكي، وحمايته، وذلك عن طريق الرد المباشر على الهجمات السيبرانية. ففي عام (2021) وبعد توليه السلطة في أمريكا، بدأ يوضع استراتيجية سيبرانية واضحة المعالم، تهدف إلى توظيف الفضاء السيبراني في

---

(43) محمد المنشاوي، كيف فشلت استراتيجية (الدفاع للأمام) في حماية أمريكا من الهجمات السيبرانية، شبكة الجزيرة الإعلامية، (2020)، متاح على الرابط الآتي: https://n9.cl/0dz9n

(44) نورا رياض الدباغ، تطور استراتيجية الأمن السيبراني الامريكية: الدور الحاسم لإدارة جو بايدن: دراسة مقارنة، مجلة حمورابي، السنة الرابعة عشر، العدد (55)، (2025)، ص201.

مواجهة المخاطر، والحروب السيبرانية. وتعكس الاستراتيجية السيبرانية لعام (2021)، رؤية شاملة للسياسة الخارجية الأمريكية، وكذلك الأمن القومي الأمريكي، والتي تقوم على العديد من المرتكزات الايدولوجية[45].

وقد أكَّد الرئيس الأمريكي بايدن، بأنَّ الهيمنة على الفضاء السيبراني أمرًا ضروريًا، لتعزيز المصالح الاستراتيجية القومية، وفي الوقت نفسه أشار إلى أنَّ مهمة وضع استراتيجية سيبرانية، وبنائها، أمرًا معقدًا نتيجة الطبيعة الشاملة للفضاء السيبراني، والذي يشتمل على تحقيق العديد من الأهداف، أهمها حرية التصفح على الإنترنيت، وكذلك تعزيز التجارة الدولية، وحماية البنى التحتية. إلى جانب ترسيخ مبادئ عدة، منها الديمقراطية وحقوق الإنسان، وتحقيق الأمن السيبراني الشامل[46].

وفي عام (2023)، ونظرًا لتهديدات الهجمات السيبرانية المتزايدة، أطلقت حكومة جو بايدن الاستراتيجية الوطنية للأمن السيبراني، والتي تُعدُّ بمنزلة وثيقة استراتيجية تستهدف تأمين الفضاء السيبراني الأمريكي، وحماية البنى التحتية الحيوية، والقيام بعمليات سيبرانية دفاعية، وهجومية، في مواجهة المخاطر، والتهديدات السيبرانية، والتي تشكِّل أحد أهم التحديات أمام المصالح، والأهداف العليا للدولة، إذ أشارت التصريحات التي أدلى بها مستشار الأمن القومي الأمريكي السابق (جون بولتون)، إلى أنَّ الهجمات السيبرانية الدفاعية، والتي تشنها القيادة السيبرانية الأمريكية، قد أزالتها الإدارة الأمريكية في عهد الرئيس الأمريكي ترامب، واستبدلتها بما يعرف بـ (هياكل الردع)، وهذا ما جعل الاستراتيجية السيبرانية في عهد الرئيس ترامب، أكثر عدوانية وهجومية في مواجهة المخاطر السيبرانية. أمَّا بالنسبة لإدارة بايدن فتعدُّ أكثر حذرًا في إدارة الفضاء السيبراني، بوصفه أحد أهم عناصر القوة الوطنية الأمريكية، التي تقوم على مبدأ التعاون الأمني، والدفاعي، والاقتصادي، وذلك عن طريق تعزيز التعاون مع الشركات العالمية في مجال الأمن السيبراني، ولم تقتصر على التعاون مع الشركاء، كما كان في إدارة ترامب، وهذا ما جعل الاستراتيجية السيبرانية للعام (2023)، هي الأبرز بين الاستراتيجيات السابقة، كونها لم تقتصر على سياسة الردع فحسب، بل على تعزيز مبدأ الحوار، والتعاون، وعلى المستويات كافة (العسكرية، والأمنية، والاقتصادية، والتكنولوجية)[47].

ففي هذا السياق، عملت الولايات المتحدة الأمريكية على تعزيز قدراتها الدفاعية، والهجومية، في مجال الأمن السيبراني، إذ خصصت إدارة جو بايدن ما يقارب (1.3) مليار دولار، لتطوير برامج القيادة السيبرانية، ووكالة الفضاء السيبراني، إلى جانب تطوير التكنولوجية الرقمية، والتي تخضع تحت إشراف القيادة السيبرانية والفضائية، إذ أكَّد مستشار الفضاء السيبراني السابق (بيتر هاريسون)، أنَّ التهديدات السيبرانية تدفع الولايات المتحدة الأمريكية، إلى زيادة الانفاق في تطوير مجال فضائها السيبراني. وبحسب التقرير الذي نشرته مؤسسة (secourc world

---

(45) كرار عباس متعب، مصدر سبق ذكره، ص207.

(46) جفري أي. إيسيناس، الاستراتيجية الامريكية للفضاء السيبراني (تعزيز الحرية والأمن والازدهار)، ترجمة باسم علي خريسان، مركز المستقبل للدراسات الاستراتيجية، (2017)، متاح على الرابط الآتي: https://n9.cl/11ez8

(47) كين تشن شيان آن، الفضاء السيبراني والقوة الأمريكية _استراتيجية الأمن السيبراني الأمريكية لعام 2023، ترجمة باسم علي خريسان، (2023)، متاح على الرابط الآتي: https://url-shortener.me/9ST4

foundation)، والتي حملت عنوان (القدرة العالمية المادة للفضاء السيبراني)، تمتلك الولايات المتحدة الأمريكية القوة التكنولوجية اللازمة، لتطوير القدرة المدارية الخاصة بالأقمار الصناعية، فضلاً عن امتلاكها صواريخ اعتراضية للدفاع الجوي، يمكن استعمالها في العديد من البرامج أهمها برنامج حرب الملاحة، وبرنامج تطوير القدرات المضادة للاتصالات (mead wlands)[48].

كما صادق مجلس الشيوخ الأمريكي عام (2022)، على الميزانية الدفاعية لعام (2023)، والتي تضمنت تخصيص ما يقارب (11.2) مليار دولار، لحماية الأمن السيبراني الأمريكي الذي أصبح ساحة لنشوب الصراعات الدولية، فضلاً عن تخصيص (2.9) مليار دولار، لتطوير وكالة الأمن السيبراني الأمريكي، وحماية البنى التحتية الرقمية، في المقابل طالبت إدارة بايدن الكونغرس الأمريكي، بزيادة الانفاق على مجال الفضاء السيبراني، ليصل إلى (26.6) مليار دولار للسنة المالية لعام (2024)[49].

أمَّا في عام (2024)، فقد أطلقت الإدارة الأمريكية، استراتيجية سيبرانية بعنوان (الاستراتيجية الأمريكية الخاصة بالفضاء الإلكتروني والمجال الرقمي)، وتضم خمسة أهداف، هي:

أولًا- تعزيز المجال الرقمي والتكنولوجي، وذلك عن طريق توظيف الدبلوماسية الرقمية، وتعزيز التعاون المشترك مع الدول المعنية بالمجال الرقمي، وبناء تكتلات جديد تقوم على أساس التعاون، وتحقيق الأهداف المنشودة.

ثانيًا- هيمنة الولايات المتحدة الأمريكية على الفضاء السيبراني، إذ تسعى الولايات المتحدة الأمريكية إلى تعزيز قدراتها السيبرانية، بهدف السيطرة على مجال الفضاء السيبراني، لاسيَّما في ظل وجود تنافس دولي، وتفوق تكنولوجي (روسي، وصيني).

ثالثًا- وضع أسس ومرتكزات تنظم عمل مجال الفضاء الرقمي، وذلك عن طريق إقرار التشريعات، والقوانين، التي تدعو إلى احترام حقوق الأفراد، وتوفير فضاء سيبراني آمن[50].

وممَّا تقدم يمكن أن نستنتج أنَّ الاستراتيجية الأمريكية تتباين فيما بينها، في مواجهة التهديدات السيبرانية ووفقًا لتبدل الإدارة الأمريكية، إذ يمكن وصف الاستراتيجية الأمريكية في عهد الرئيس السابق أوباما، بأنَّها استراتيجية وقائية شاملة نجحت في تعزيز الأمن السيبراني، لكنَّها أخفقت في مسألة الردع السيبراني، على عكس الاستراتيجية الأمريكية المتبعة في عهد الرئيس الأمريكي ترامب، والتي اتسمت بطابع هجومي، ووقائي، فضلًا عن تطوير قدراتها السيبرانية، لكنَّها تراجعت في مسألة تعزيز التعاون الدولي المشترك، أمَّا بالنسبة للاستراتيجية السيبرانية في عهد الرئيس الأمريكي بايدن، فقد اتصفت بكونها استراتيجية متوازنة، تدعو إلى تعزيز التعاون المشترك من جهة، ومواجهة

---

(48) رغدة البهي، عسكرة الفضاء الخارجية، رؤية تحليلية.مجلة السياسة والاقتصاد، العدد (16)، (2022)، ص463.

(49) (Mark Stone, "How much is the us. investing in cyber Landis it enough? " 2011/2023 Secuity in accessed telligence) on 21/9/2023, at: https

(50) نورا رياض الدباغ، مصدر سبق ذكره، ص209.

المخاطر والتهديدات السيبرانية، التي تمس الأمن القومي الأمريكي من جهة أخرى، فهي تعدُّ الأبرز، والأكثر نجاحًا، من بين الاستراتيجيات المتبعة في مواجهة التهديدات السيبرانية، في ظلّ بيئة دولية تتسم بالتشابك، والتعقيد.

الخاتمة

أحدث التطور التكنولوجي، والمعلوماتي، نقلة نوعية في شكل العلاقات الدولية، وتأثيرها في العديد من المجالات الاستراتيجية (السياسية، والاقتصادية، والأمنية، والعسكرية)، ممَّا أسهم في ظهور ما يسمى بالفضاء السيبراني، والذي أحدث تغييرات واضحة في مفاهيم العلاقات الدولية، بما فيها مفهوم التعاون والصراع، الأمر الذي دفع بتطوير مفهوم الأمن في مواجهة التهديدات السيبرانية، إذ إنَّ مفهوم الأمن لم يعد مقتصرًا على تعزيز الإمكانات، والمقومات التقليدية فحسب، بل إلى توظيف التكنولوجيا والمجال الرقمي في مواجهة التهديدات، والمخاطر، والتي تمس الأمن القومي للدول، وهذا ما دفع القوى الدولية، ومنها الولايات المتحدة الأمريكية، إلى استحداث، وإنشاء قواعد البيانات، وتطوير شبكات الإنترنت والاتصالات، فضلاً عن وضع رؤية استراتيجية لمواجهة المخاطر السيبرانية، وهذا ما جعل الفضاء السيبراني يشكل ساحة مهمة لإدارة التفاعلات الدولية، نتيجة زيادة الهجمات السيبرانية بين الدول، إذ نجد الولايات المتحدة الأمريكية حريصة على تطوير قدراتها، وإمكاناتها السيبرانية، وتوظيفها في استراتيجياتها الدفاعية، والوقائية، على مدار الحكومات والإدارات المتعاقبة، بهدف حماية أمنها القومي، والبنية التحتية، من أي هجوم محتمل. وبما أنَّ الأمن السيبراني لا يقتصر على رقعة جغرافية معينة، لذلك فإنَّ مساعي الدول واضحة في التزامها في وضع الأطر القانونية، الخاصة بالتعامل مع مجال الفضاء السيبراني، وجعله بيئة آمنة لمستخدميه، كما أنَّ التفوق في مجال الفضاء السيبراني، سيؤدي إلى الاستمرارية في النمو، والتقدم التكنولوجي، والمعلوماتي في العالم، وهذا ما عملت به الولايات المتحدة الأمريكية، وعلى تعاقب الإدارات فيها، عن طريق توظيف جميع مقومات القوة السيبرانية والمعلوماتية في مواجهة المخاطر، والتهديدات السيبرانية، التي تقودها القوى الدولية المنافسة.

الاستنتاجات

أولًا- تشكّل التهديدات السيبرانية أحد أهم التحديات التي تمس الأمن القومي الأمريكي، في ظلّ التحول الرقمي، والاعتماد على توظيف مجال الفضاء السيبراني، في المجالات الاستراتيجية كافة وأهمها السياسية، والأمنية.

ثانيًا- لم تقتصر الاستراتيجية الأمريكية على كونها استراتيجية وقائية فحسب، بل امتدت لتكون أكثر شمولية في مواجهة التهديدات غير التقليدية (الدفاع، والهجوم، والردع).

ثالثًا- إنَّ تحقيق أمن سيبراني مستدام، يتطلب من الولايات المتحدة الأمريكية العمل على توظيف قدرتها ومقوماتها السيبرانية كافة، وتطوير استراتيجيتها، لتصبح أكثر مرونة، وقدرة على التكيف المستمر مع التهديدات غير التقليدية، وكيفية مواجهتها.

رابعًا- إنَّ فاعلية الاستراتيجية الأمريكية في مواجهة التهديدات السيبرانية، تبقى مرهونة بالعديد من العوامل، وأهمها مواكبة التطور التكنولوجي، وتحقيق مستوى عالٍ من التنسيق المؤسسي الداخلي، وكذلك التعاون الدولي المشترك في استخدام هذا المجال.

المصادر

أولاً- الكتب

1. حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى (الولايات المتحدة الأمريكية وروسيا أنموذجاً)، دار أنكي للنشر والتوزيع، (2022).
2. خالد وليد محمود، *الفضاء السيبراني وتحولات القوة في العلاقات الدولية*، المركز العربي للأبحاث ودراسة السياسات، بيروت، (2025).
3. عباس بدران، *الحروب الإلكترونية: الاشتباك في عالم متغير*، مركز دراسات الحوكمة الإلكترونية، بيروت، (2010).
4. فراس جمال شاكر الحربي، *المعلوماتية في المجال الأمني والعسكري: أمريكا والصين أنموذجًا*، الدار العربية للنشر والتوزيع، بيروت، (2023).
5. فرد كايلان، *المنطقة المعتمة: التاريخ السري للحرب السيبرانية*، ترجمة لؤي عبد المجيد، المجلس الوطني للثقافة والفنون والآداب، الكويت، (2019).
6. منى الأشقر جبور، *السيبرانية هاجس العصر*، المركز العربي لبحوث القانونية والفضائية، بيروت، (2017).

ثانيًا- الرسائل والأطاريح

1. سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي للولايات المتحدة الأمريكية نموذجًا (2001–2017)، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، (2018).
2. صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، جامعة الشرق الأوسط، كلية الآداب والعلوم، (2021).
3. عبد الله مسعود، دراسات في الأمن القومي، جامعة بنغازي، كلية الإدارة والاقتصاد، (2002).
4. فاتح حراك، الفضاء السيبراني والتحول في مفهوم الأمن في الولايات المتحدة الأمريكية، جامعة قسطنطينّة – صالح بونيدر، كلية العلوم السياسية، (2024).

ثالثًا- المجلات والدوريات

1. تامر سعيد عبد اللطيف، *الاستمرارية والتغيير في استراتيجية الأمن السيبراني للولايات المتحدة الأمريكية خلال المدة 2009–2024*، مجلة تكريت للعلوم السياسية، (2020).
2. جاسم محمد طه، *التهديدات السيبرانية وتأثيرها على الأمن القومي الأمريكي*، مجلة جامعة تكريت للعلوم السياسية، (2023).
3. خالد وليد، *المغالبة والتنافس في القدرات السيبرانية الأمريكية الصينية*، مجلة شؤون استراتيجية، (2024).
4. رغدة البهي، *الردع السيبراني: المفهوم والإشكاليات والمتطلبات*، المركز المصري للفكر والدراسات الاستراتيجية، (2017).
5. سوزي رشاد، *التهديدات الأمنية الهجينة في العلاقات الدولية: السيبرانية والذكاء الاصطناعي نموذجاً*، مجلة وادي النيل، (2022).
6. شيماء معروف فرحان، *التحول في مفهوم القوة والصراع: دراسة في الحروب السيبرانية*، مجلة قضايا السياسة، جامعة النهرين، (2023).
7. عادل عبد الصادق، *أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي*، مجلة السياسة الدولية، (2017).
8. عبد الغني شرقي، *التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة وستفاليا*، مجلة السياسة العالمية، (2023).
9. علي محمد الرفاعي، *تحديات الأمن في الفضاء السيبراني الأمريكي*، مجلة دراسات دولية، (2021).
10. عمر عبد الله عفتان، *الاستراتيجيات والسياسات المتبعة في مواجهة التهديدات السيبرانية*، مجلة الفارابي للعلوم الإنسانية، (2024).
11. مروة زين العابدين سعد، *تأثير تغير مفهوم السيادة على الاقتصاص القضائي في الجرائم السيبرانية*، المجلة الدولية للفقه والقضاء والتشريع، (2022).
12. نورا رياض الدباغ، *تطور استراتيجية الأمن السيبراني الأمريكية: الدور الحاسم لإدارة جو بايدن – دراسة مقارنة*، مجلة حمورابي، (2025).

13. نوره شلوش، *القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول*، مجلة مركز بابل للدراسات الإنسانية، (2018).

رابعاً: المصادر الإلكترونية

1. مخاطر الأمن السيبراني، شركة سايبر للأمن السيبراني، متاح على الرابط:`

https://share.google/WhVy1yd4wNPFLzNzk

2. مركز أبحاث كاتيغون، *ما هي أفضل خمسة جيوش الكترونية في العالم؟ وما ترتيب الجيش السيبراني الروسي؟* (2017)، متاح على الرابط: https://share.google/5fGTzSaZ1BA08tZQ3

3. عادل عبد الصادق، *الفضاء الإلكتروني وتهديدات جديدة للأمن القومي*، المركز العربي للأبحاث، متاح على الرابط: https://2u.pw/XJ06Z9

4. مروة الأسدي، *الفضاء: أحدث ساحة قتال في العالم*، متاح على الرابط: https://annabaa.org/arabic/sciences/21860

5. عمرو عبد العاطي، *استراتيجية أمريكية هجومية ضد التهديدات السيبرانية*، المركز المصري للفكر والدراسات الاستراتيجية، متاح على الرابط: https://ecss.com.eg/2077/

6. محمد المنشاوي، *كيف فشلت استراتيجية الدفاع للأمام في حماية أمريكا من الهجمات السيبرانية*، الجزيرة، 2020، متاح على الرابط: https://n9.cl/0dz9n

7. جفري أي. إيسيناس، *الاستراتيجية الأمريكية للفضاء السيبراني (تعزيز الحرية والأمن والازدهار)*، ترجمة باسم علي خريسان، (2017)، متاح على الرابط: https://n9.cl/11ez8

8. كين تشن شيان آن، *الفضاء السيبراني والقوة الأمريكية – استراتيجية الأمن السيبراني الأمريكية لعام 2023*، ترجمة باسم علي خريسان، (2023)، متاح على الرابط:

https://url-shortener.me/9ST4

خامسًا- المصادر الأجنبية

1. Mark Stone, "How much is the U.S. investing in cyber...?" Security Intelligence, accessed 2023.

2. Zisa Ferdinando, *Cybercom to Elevate to Combatant Command*, U.S. Department of Defense, accessed 2018.

3. White House, *National Cybersecurity Initiative: The Comprehensive*, 2008.