Political Sciences Journal
Issue (69) June (2025) **ISSN**: 1815-5561 **E-ISSN**: 2521-912X

Continuity and Change in US Cyber Security Strategy from 2009 to 2024

Tamer Saeed Abdel Latif Mahmoud *

Receipt date: 2/1/2025 Accepted date:14/4/2025 Publication date:1/6/2025

https://doi.org/10.30907/jcopolicy.vi69.819

Abstract:

This study aims to analyze the continuity and change in U.S. cybersecurity strategy from 2009 to 2024, with a focus on evaluating why these strategies have been largely ineffective despite the United States' technological prominence. The study also seeks to understand the impact of cyber challenges on U.S. national security and to assess the extent to which adopted strategies have succeeded in achieving national objectives. The central problem addressed is that, despite the U.S. possessing advanced technological capabilities in cybersecurity, and despite successive administrations, particularly under Obama and Trump, recognizing the risks posed by cyber threats, the country continues to experience major breaches that threaten its national security.

The research employs an analytical approach to study the dimensions and determinants of U.S. cybersecurity strategy, alongside a case study method to use the U.S. model as a framework for understanding its successes and failures. A comparative approach is also used to analyze the evolution of cybersecurity strategies across different administrations, beginning with Obama, followed by Trump, and up to Biden.

The study concludes with several key findings, most notably that the lack of coordination among U.S. cybersecurity institutions has undermined the effectiveness of strategic responses. The study also highlights shifts in priorities across different administrations. It recommends strengthening interagency coordination to unify efforts and enhance emergency response capabilities. Moreover, it emphasizes the need to develop integrated strategies that link cybersecurity directly with national security.

Keywords: Cybersecurity, United States, Strategy, U.S. National Security.

*Ph.D. Candidate/ Egypt/ Cairo University/ Faculty of Economics and Political Science/ Department of International Relations.
tamermahboub@gmail.com

مجلة العلوم السياسية
العدد (69) حزيران (2025) E-ISSN: 2521-912X ISSN: 1815-5561

الاستمرارية والتغيُّر في استراتيجية الأمن السيبراني للولايات المتحدة الأمريكية في المدة من 2009 إلى 2024

تامر سعيد عبد اللطيف محمود*

الملخص:

ترمي الدراسة إلى تحليل استمرارية وتغير إستراتيجية الأمن السيبراني الأمريكي خلال المدة من عام 2009 حتى 2024، مع التركيز على تقييم أسباب عدم فعالية الإستراتيجيات السيبرانية بالرغم من ريادة الولايات المتحدة في المجال التكنولوجي. كما سعت الدراسة إلى فهم تأثير التحديات السيبرانية على الأمن القومي الأمريكي وتقييم مدى نجاح الإستراتيجيات المتبعة في تحقيق أهدافها الوطنية، تتمثل المشكلة البحثية في أنه على الرغم من امتلاك الولايات المتحدة قدرات تكنولوجية متقدمة في مجال الأمن السيبراني، وإدراك إداراتها المتعاقبة، خاصة في عهد أوباما وترامب، لمخاطر التهديدات السيبرانية، إلا أنها لا تزال تعاني من اختراقات كبرى تهدد أمنها القومي.

اعتمدت الدراسة على المنهج التحليلي لدراسة أبعاد ومحددات إستراتيجية الأمن السيبراني الأمريكي، ومنهج دراسة الحالة لاستعمال الأنموذج الأمريكي كإطار لفهم النجاحات والإخفاقات. كما استُعمل المنهج المقارن لتحليل تطور الإستراتيجيات عبر الإدارات المختلفة، بدءًا من إدارة أوباما ومرورًا بإدارة ترامب ووصولًا إلى إدارة بايدن.

توصلت الدراسة إلى عدة نتائج رئيسة، من أبرزها وجود فجوة في التنسيق بين المؤسسات السيبرانية الأمريكية، مما أثر في كفاية الإستراتيجيات. كما كشفت الدراسة عن تغير الأولويات بين الإدارات الأمريكية؛ أوصت الدراسة بضرورة تعزيز التنسيق الداخلي بين المؤسسات السيبرانية لتوحيد الجهود وزيادة فعالية استجابة الطوارئ. كما أكدت أهمية تطوير إستراتيجيات متكاملة تربط بين الأمن السيبراني والأمن القومي.

الكلمات المفتاحية: الأمن السيبراني، الولايات المتحدة، إستراتيجية، الأمن القومي الأمريكي.

* باحث في مرحلة الدكتوراة/ جمهورية مصر العربية/ جامعة القاهرة/ كلية الاقتصاد والعلوم السياسية/ قسم العلاقات الدولية.

المقدمة:

يعد "الأمن السيبراني" كمصطلح، جديد نسبيا مقارنة بالممارسات الفعلية التي إتخذتها الدول لتأمين شبكات الإنترنت، لم يتفق الفاعلون فى المجتمع الدولي فيما بينهم على تعريف محدد وواضح لمصطلح الأمن السيبراني فالمصطلح دائم التطور عبر الزمن كما أنه يختلف بإختلاف السياقات التي تتناوله، إلا أن هذه التعريفات فى عمومها قد اشتركت فى ربط الأمن السيبراني بحماية المؤسسات و الشركات من هجمات البرامج الضارة التي ترمي لإتلاف الملفات و البيانات و سرقة البيانات الشخصية. مع التطور التكنولوجي و إلتجاء معظم المؤسسات الحكومية في البلدان المختلفة لرقمنة أنشطتها و وثائقها، أصبح الأمن السيبراني مرتبطا بالأمن القومي بل و أصبح تحديا له، و أصبح التوسع في أمن الإنترنت يؤدي إلى التوسع في دائرة المخاطر السيبرانية مما يتطلب تبني بعض السياسات والإستراتيجيات التي قد تحد من تلك المخاطر.

تعد الولايات المتحدة الأمريكية هي الدولة الأكثر تقدما في هذا المجال إذ إنها من أوائل الدول التي ربطت بنيتها التحتية بشبكة الإنترنت، فضلاً عن بعض الدول العظمى الأخرى مثل الصين و روسيا و أسبانيا، وقد كانت البداية فى اعتماد الإدارة الأمريكية على وكالة المخابرات المركزية CIA ووكالة الأمن القومي الأمريكي NSA فى القيام بعملياتها فى الفضاء السيبراني إلى أن استحدث البنتاجون في يونيو 2009 قيادة عسكرية مهمتها الرد على الهجمات السيبرانية وتنفيذ عمليات فى الفضاء السيبراني إذ أسندت الإدارة الأمريكية للجنرال 'الكسندر كيث' قيادة حروب الفضاء السيبراني سواء فيما يتعلق بالتأمين أو الدفاع أو حتى تنفيذ عمليات خارجية سيبرانية. على الرغم من تمتع الولايات المتحدة الأمريكية بدور الريادة في مجال الأمن السيبراني، إلا أن هذا لم يمنعها من تبني إستراتيجية للأمن السيبراني كمحاولة للحد من تعرضها لتهديدات سيبرانية. وكانت البدية في عام ٢٠٠٣ عندما تبنى الرئيس الأسبق جورج بوش الابن الدعوة لإصدار أول إستراتيجية لحماية الإنترنت وتأمين نظم المعلومات موجها الدعوة للحكومة للعمل مع القطاع الخاص لإنشاء نظام استجابة للطوارئ كوسيلة لتقليل تعرض الدولة لهجمات سيبرانية. في عام 2010، أكدت إستراتيجية الأمن القومي الأمريكي الصادرة في عهد الرئيس الأسبق باراك أوباما على إن التهديدات الإلكترونية تمثل واحدة من أخطر التهديدات التي تواجه الأمن القومي فضلا عن أنها أحد أهم التحديات

التي تواجه الاقتصـاد القومي (National Security Strategy of the United States of America 2010). أشـارت تلك الإسـتراتيجية إلى ضـرورة تقييم المخاطر في سـت مجالات رئيسـة من ضـمنها الإتصـالات لحماية الولايات المتحدة من التهديدات الإلكترونية، داخلياً من طريق فرض الولايات المتحدة عقوبات سـريعة ومكلفة على الحكومات الأجنبية والجهات الفاعلة الأخرى التي تضطلع بأنشطة الكترونية خبيثة، وخارجياً من طريق العمل مع الحلفاء و الأصدقاء لتوسيع وعيها بالأنشطة الخبيثة. في عام 2011، أصدر البيت الأبيض "إسـتراتيجية دولية للفضـاء الإلكتروني" تعطي الحق للولايات المتحدة في الرد العسـكري على الهجمات السـيبرانية، وفي العام نفسـه أعلن نائب وزير الدفاع الأمريكي 'وليام لين' فى يونيو ٢٠١١ أنه سيتم التعامل مع الفضـاء السـيبراني كمجال جديد للحروب الأمريكية فضـلاً عن المجالات التقليدية وهى البر والبحر والجو، وتنفيذا لرؤية إدارة باراك أوباما والتي أعطت الولايات المتحدة الحق فى شـن أي هجمات اسـتباقية سـيبرانية ترى أن فيها مصـلحة لأمنها القومي، أتت الإسـتراتيجية السـيبرانية لوزارة الدفاع الأمريكية لعام ٢٠١٥ لتصـيغ تلك الرؤية فى إطار رسـمي يفتح الباب على مصـراعية أمام الولايات المتحدة لشـن هجمات سـيبرانية اسـتباقية، وعلى الرغم من تطوير الإدارة الأمريكية للعديد من الأسـلحة السـيبرانية إلا أنها فى الوقت نفسه تعرضت لقدر من الهجمات ربما يفوق أي دولة اخرى.

إتخذ البنتاجون مجموعة من الإجراءات ما بين عامي ٢٠١٧ – ٢٠١٨، أعلنت الإدارة الأمريكية في عام ٢٠١٨ عن أول إستراتيجية مفصلة لحماية الأمن السيبراني، أطلقت عليها الإستراتيجية السيبرانية القومية والتي من خلالها استعملت مصطلح "الأمن القومي السيبراني" لأول مرة فى تأريخها، كما أنها تعد الإسـتراتيجية الأكثر تفصـيلا فيما يتعلق بمجال الأمن السـيبراني الأمريكي، ومع ذلك تعرضـت الولايات المتحدة فى حقبة ترامب لهجمات أثارت أنتقادات واسعة لإدارته حتى أن الرئيس التالي لترامب وهو الرئيس بايدن كان قد وجه نداؤه فى بداية توليه الحكم للمحاربين القدامى للمسـاعدة فى الوصـول لحلول من شـأنها إصـلاح ما واجهته إدارة ترامب من مخاطر سيبرانية أثرت في الأمن القومي الأمريكي.

تهتم الدراسـة بدراسـة أسـباب عدم تمكن الولايات المتحدة الأمريكية من وضـع إسـتراتيجية تحد من تعرضـها لهجمات سـيبرانية، على الرغم من كونها الدولة صـاحبة الريادة في مجال الأمن السـيبراني، إذ أنه على الرغم من كونها الدولة الأكثر امتلاكا لآليات القوة السـيبرانية إلا أنها

تعرضت لهجوم سيبراني في عام 2020، وهو الأمر الذي بدوره وجه الأنظار إلى مدى فاعلية إستراتيجية الأمن السيبراني التي تتبناها الولايات المتحدة وأثار التساؤلات حول تلك الإستراتيجية وتأثيرها في الأمن القومي للولايات المتحدة. تغطي الدراسة المدة الزمنية الممتدة من عام 2009، بداية المدة الأولى للرئيس الأسبق باراك أوباما والتي شهدت تصنيف الأمن السيبراني كمصدر للخطورة عند إصدار إستراتيجية الأمن القومي الأمريكي في عام 2010 وحتى عام 2024 و هو موعد إنتهاء المدة الأولى للرئيس جو بايدن.

وتكمن المشكلة البحثية في أنه على الرغم من إن الولايات المتحدة الأمريكية تمتلك من قدرات تكنولوجية فائقة في مجال الأمن السيبراني وعلى الرغم من إدراك الإدارات الأمريكية فى العقود الأخيرة خاصة إدارتي أوباما وترامب لمخاطر التهديدات السيبرانية وتأثيراتها في قطاعات الدولة كافة وأمنها القومي، واعتمادها لإستراتيجيات منوط بها مواجهة هذه التهديدات السيبرانية من طريق هيئات ومؤسسات مخصصة لتولي هذه المهمة وتسخيرها للإمكانات التي تتيح لها القيام بمهمتها، إلا أنها مازالت تتلقى ضربة تلو الأخرى لأمنها السيبراني ولم تستطع الولايات المتحدة مواجهتها و الحد منها وذلك، على سبيل المثال، ما أعلنته الولايات المتحدة من تعرضها خلال مدة الرئيس ترامب لهجمات الكترونية غير مسبوقة ما يمثل ضررا بالغا واختراقا واضحا لمنظومة الأمن السيبراني الأمريكي، وتسببت فى أضرار كبيرة أبرزها حدوث شلل وتعطل فى الكثير من المنشآت الحيوية وأنظمة التشغيل الإلكتروني الخاصة بها، وقد وصل الأمر إلى حد وصف بعض بأن ما تعرضت له أمريكا بمثابة هجوم بيرل هاربر جديد ولكن سيبرانيا ، وهنا تتبلورت مشكلة الدراسة والتي ترتكز حول أسباب عدم قدرة الولايات المتحدة، وللإجابة على هذا التساؤل تتتبع الدراسة إستراتيجيات الأمن السيبراني للولايات المتحدة من مدة تولي الرئيس الأسبق باراك أوباما وحتى إنتهاء مدة الولاية الأولى للرئيس بايدن مرورا بولاية الرئيس ترامب، وذلك من خلال السؤال الرئيسي الآتي:

لماذا لم تستطع الولايات المتحدة الأمريكية مواجهة التهديدات والتحديات للأمن السيبراني على الرغم من امتلاكها قدرات تكنولوجية فائقة و إصدارها إستراتيجية للأمن السيبراني؟

الأسئلة الفرعية:

1. ماهي التهديدات السيبرانية التي واجهتها الولايات المتحدة خلال مدة محل الدراسة؟
2. ماهي محددات إستراتيجية الأمن السيبراني الأمريكي؟

3. ماهي أبعاد إستراتيجية الأمن السيبراني الأمريكي؟

4. ما مدى نجاح إستراتيجية الأمن السيبراني الأمريكي في تحديد أهدافها؟

وتنبع أهمية الدراسة من إنتمائها إلى مجال الدراسات الأمنية والإستراتيجية، الذي يُعد أحد أبرز مجالات العلاقات الدولية، خاصة في ظل التحولات المتسارعة التي شهدتها هذه الدراسات في الآونة الأخيرة. ويمثل الأمن السيبراني أحد أبعاد الأمن القومي الحديثة، ما يجعل دراسة إستراتيجياته أمرًا بالغ الأهمية، ليس فقط لفهم طبيعة التحديات التي تواجهها الولايات المتحدة، بل أيضًا لاستخلاص الدروس المستفادة للدول التي تسعى إلى التحول الرقمي، مثل مصر، من طريق الاستفادة من التجربة الأمريكية الرائدة في هذا المجال.

تحلل هذه الدراسة إستراتيجية الأمن السيبراني الأمريكي عبر الإدارات المختلفة، بدءًا من أوباما مرورًا بترامب وصولًا إلى بايدن، وهو ما يسهم في تسليط الضوء على مواطن القوة والضعف في هذه الإستراتيجيات. كما تقدم إطارًا تحليليًا لتطور الأمن السيبراني كعامل مؤثر في الأمن القومي الأمريكي، مما يساعد في بلورة فهم أعمق للتهديدات السيبرانية وسبل مواجهتها، خاصة إن الواقع أثبت خطورة الهجمات السيبرانية على أمن الدول واستقرارها.

وعلى المستوى العملي، تبرز أهمية الدراسة في تقديم تحليل شامل حول تأثير الأمن السيبراني في الأمن القومي، ما يسهم في صياغة رؤى وتوصيات تفيد صناع القرار، سواء في الولايات المتحدة أم في دول أخرى، في تبني سياسات أكثر فاعلية لمجابهة التهديدات السيبرانية. كما إن اعتماد الدراسة على الأنموذج الأمريكي كدراسة حالة يعزز من قيمتها التطبيقية، إذ يتيح فهماً دقيقاً لكيفية صياغة وتنفيذ إستراتيجيات الأمن السيبراني في دولة ذات نفوذ عالمي وتأثير واسع في المشهد السيبراني الدول، كما ترمي الدراسة إلى: -

- التعريف بأهم التهديدات السيبرانية التي واجهتها الولايات المتحدة خلال مدة الدراسة موضوع البحث ومدى تأثيرها في أمنها القومي.
- التعرف على محددات إستراتيجيات الأمن السيبراني.
- التعرف على أبعاد وأهداف وأدوات كل إدارة فى إستراتيجيتها للأمن السيبراني.

- التعرف على أوجه الاستمرارية والتغير فى الإستراتيجية الأمريكية للأمن السيبراني من حقبة ترامب وحتى حقبة بايدن.
- التعرف على أوجه الاتفاق والأختلاف بين إستراتيجيات الأمن السيبراني التي اعتمدتها إداراتها كلها.
- التعرف على أسباب نجاح أو فشل إستراتيجية الأمن السيبراني فى الحفاظ على الأمن القومي للولايات المتحدة.

المنهجية:

اعتمدت الدراسة على المنهج التحليلي لدراسة أبعاد ومحددات إستراتيجية الأمن السيبراني الأمريكي، ومنهج دراسة الحالة لاستعمال الأنموذج الأمريكي كإطار لفهم النجاحات والإخفاقات. كما استُعمل المنهج المقارن لتحليل تطور الإستراتيجيات عبر الإدارات المختلفة، بدءًا من إدارة أوباما ومرورًا بإدارة ترامب ووصولًا إلى إدارة بايدن كما تتبنى الدراسة منهج 'دراسة الحالة:' نظراً لكونها تعتمد على الأنموذج الأمريكي للتعرف من طريقه على مدى تأثير إستراتيجيات الأمن السيبراني على الأمن القومي للدول، ومن ثم الاستفادة من عوامل النجاح وعوامل الفشل للوصول لملائمة عامة مفيدة لنماذج ودول أخرى. أما حدود الدراسة:

– الإطار الزمني للدراسة: يتحدد الإطار الزمني للدراسة بدءًا من بداية ولاية الرئيس الأمريكي الأسبق "باراك أوباما"؛ تحديدًا عام (2009م)، وإنتهاء بعام (2024)، وهو تأريخ نهاية الولاية الأولى للرئيس الأمريكي 'جو بايدن.'

– الإطار المكاني للدراسة: يتحدد الإطار المكاني لهذه الدراسة حول الفضاء السيبراني بما فيه من تفاعلات وعلاقات سيبرانية، كما يشمل الإطار المكاني الولايات المتحدة الأمريكية كدولة مستقلة ذات سيادة تنتمي لقارة أميركا الشمالية بوصفها دراسة الحالة التي تقوم عليها الدراسة موضوع البحث.

– نطاق الدراسة: تقع الدراسة في النطاق المجالي للعلاقات الدولية، كحقل علمي من حقول العلوم السياسية.

الإطار النظري والمفاهيمي للدراسة:

تتبنى الدراسة مجموعة من المفاهيم الرئيسة وهى (الإستراتيجية، الإستراتيجية الوطنية للأمن السيبراني، الأمن السيبراني، الأمن القومي).

أولاً: الإستراتيجية:

تتعدد تعريفات الإســـتراتيجية وتختلف باختلاف الأزمنة و المجالات التي تتناول التعريف وبالرغم من عدم وجود تعريف واحد أو تعريف جامع لمفهوم الإســـتراتيجية إلا أن المفهوم قد شـــهد فى العقود الأخيرة العديد من التطورات والتوســـعات لتشـــمل مجالات أبعد من المجال العسـكري، وتتبنى الدراسـة مفهوم الإسـتراتيجية الذى قدمه مولتكه والذى يعرف الإسـتراتيجية على أنها "إجراء الملائمة العملية للوســـائل الموضـــوعة تحت تصـــرف القائد إلى الهدف المطلوب" (هارت2000).

ثانياً: الإستراتيجية الوطنية للأمن السيبراني :

يمكن تعريف إســتراتيجية الأمن الســيبراني القومي بأنها "خطة أو منهج دقيق لحماية كل من الإصـــول المعلومـاتيـة وغير المعلومـاتيـة للبنيـة التحتيـة من طريق تكنولوجيـا المعلومـات والإتصـــإلات وذلك لتحقيق أهداف وطنية معينة عادة ما تكون على المدى البعيد (Azmi et al. 2016).

ثالثاً: الأمن السيبراني:

يمكن تعريفه بأنه "النشاط أو العملية، أو القدرة، أو نظم المعلومات واتصالات الدولة إذ تكون المعلومات الواردة فيه محمية من التلف والاسـتعمال غير المصـرح بها للتعديل أو الاسـتغلال (أحمد 2020).

وكذلك يشـــير الأمن الســـيبراني إلى "مجموع الوســـائل التقنية والتنظيمية والإدارية التي يمكن اسـتعمالها لمنع الاسـتعمال غير المصـرح به وسـوء الاسـتغلال واسـتعادة المعلومات التي تحتويها؛ وذلك بهدف ضـــمان توافر واســـتمرار عمل نظم المعلومات وتعزيز ســـرية البيانات الشـخصـية وخصـوصـيتها واتخاذ التدابير جميعها واللازمة لحماية المواطنين والمسـتهلكين من المخاطر فى الفضاء السيبراني (لامية 2021، 61).

ومن الناحية الإجرائية يمكن تعريف الأمن السيبراني على أنه: يشمل حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق أو التدمير أو التوقف (علام 2014).

يعد مصـطلح الأمن القومي الأمريكي من المصـطلحات التي أطلقتها الولايات المتحدة نفسـها في إشارة للأخطار الداخلية والخارجية التي تمس الدولة، إذ ظهر هذا المصـطلح على الساحة الأمريكيـة عـام 1947 ومنهـا انطلق إلى بقيـة العـالم، إلا أن إســـتراتيجيـات الأمن القومي

الأمريكي دائمة التطور والتغير تحكمها التطورات الخارجية، فمع كل إدارة أمريكية تنطلق إستراتيجية للأمن القومي الأمريكي يضعها كل رئيس أمريكي أهدافها في الأساس الأمن الداخلي للولايات المتحدة والمحافظة على نفوذها وقوتها على الساحة الدولية وفقاً لما تشهده من تغيرات وتطورات، وهذه الإستراتيجية بطبيعة الحال لابد وأن تشمل الأبعاد الأمنية كافة سواء التقليدية أم غير التقليدية، إذ عرف 'هنري كيسنجر' الأمن القومي بأنه "تصرف المجتمع لتحقيق حقه في البقاء.

حاول الباحثون تفسير العلاقة بين الأمن السيبراني والأمن القومي من طريق الأطر التفسيرية التي تقدمها نظريات العلاقات الدولية، وتأتي أكثرها ملائمة لموضوع البحث – كما يرى الباحث – "مدرسة كوبنهاجن" والتي تنتمي للاتجاه التوسعي والذي ظهر في إطار الاتجاه المعارض للاتجاه التقليدي والذي ركز بالأساس على مركزية دور الدولة.

ومن أهم رواد مدرسة " كوبنهاجن 'باري بوزان وأولي ويفر'، والذي أكد في كتابه "People, states, and fear" الذي نُشر عام 1983 على ضرورة توسيع مجال البحث في دراسات الأمن إلى قطاعات أخرى غير العسكرية .

وقدمت هذه المدرسة ثلاث إسهامات أساسية وهما: مفهوم الأمن المجتمعي ويعني قدرة المجتمع للحفاظ على شخصيته الجوهرية في ظل الأوضاع المتغيرة والتهديدات المحتملة والحالية. أما الإسهام الثاني فهو نظرية الأمننة securitization وهي تعني إصباغ الصيغة الأمنية على قضايا معينة – قد تكون عادية – من أجل شرعنة اللجوء إلى ترتيبات معينة من قِبل القادة مما يأتي على حساب آليات الديمقراطية (كالنقاش والحوار والاستفتاء)، لذلك قدم ويفر مصطلح اللا أمننة Desecuritization والذي رأى فيه أن تحويل قضايا معينة إلى أمنية يتطلب إجراءات معنية ومن ثم التقليل من حدة الأمننة. وأخيراً مركب الأمن الإقليمي إذ تعد هذه المدرسة من أوائل من قدم مفهوم الأمن الإقليمي.

وفيما يتعلق بملائمة النظرية للدراسة موضوع البحث، فتتضح جليا في عد الرؤساء الأمريكيين وخاصة ترامب أن الهجمات السيبرانية هي سمة مميزة للصراع الحديث وأن الفواعل من غير الدول أصبح بإمكانهم استعمال الهجمات السيبرانية بغرض تهديد سلامة الأنظمة والمنظمات الديمقراطية والنظام الاقتصادي العالمي. ومن ثم رأت الإدارة الأمريكية ضرورة مواجهة وردع التهديدات السيبرانية ومستعمليها بقوة من طريق: تطوير القدرة على الاستجابة السريعة

للهجمات السيبرانية، تطوير الأدوات السيبرانية وامتلاك الخبراء في المجال السيبراني وتعزيز قدراتهم، تنمية وتطوير التكامل بين مؤسسات الحكومة- بالتعاون مع الكونغرس- حتى تكون العمليات السيبرانية الموجهة ضد أعداء الولايات المتحدة الأمريكية قوية وعلى أفضل مستوى (عبد الحميد 2020).

المحو الأول: الإستراتيجية السيبرانية للولايات المتحدة خلال المدة من 2009 وحتى 2016.

على مدار ولايتي الرئيس الأسبق باراك أوباما، وتعددت محاولات الإدارة الأمريكية لإنتاج إستراتيجية متكاملة يتحقق من طريقها الأمن السيبراني للولايات المتحدة. وفي إطار سعي الإدارة الأمريكية لإنتاج إستراتيجية للأمن السيبراني، وأعلن الرئيس أوباما في عام 2009:" نحن لسنا مستعدين كما يجب كحكومة وكدولة". إن الأمن السيبراني مسألة معقدة بحيث لا يمكن إدارته من طريق وكالة أو منظمة واحدة، مما يستدعي التنسيق بين كل الفاعلين خاصة وزارة الدفاع ووكالة الأمن القومي ووزارة الأمن الداخلي، فضلاً عن وكالة الاستخبارات الأمريكية (دحمانى 2018، 75-76). وفي هذا السياق استحدث البنتاجون القيادة السيبرانية الأمريكية في يونيو 2009 لتكون بمثابة قيادة عسكرية مسؤولة عن صد هجمات قراصنة المعلومات، وكذلك تنفيذ عمليات الفضاء السيبراني؛ نظرًا لتفاقم الأخطار السيبرانية التي تعد من أهم تحديات الاقتصاد العالمي والأمن القومي في القرن الحادي والعشرين، وتم تعيين الجنرال ألكسندر كيدز كأول جنرال عسكري مهمته إدارة حروب الفضاء السيبراني في الولايات المتحدة، وكان هدف وزارة الدفاع من إنشاء هذه القيادة والإشراف على الجهود المتعلقة كلها، وحروب الإنترنت في أفرع القوات المسلحة الأمريكية جميعها، والدفاع عن شبكات وزارة الدفاع والدولة الأمريكية ككل، والاستعداد لخوض الحروب، وضمان حماية حرية عمل الولايات المتحدة وعمل حلفائها في الفضاء السيبراني، وحرمان أعداء الولايات المتحدة من حرية العمل في هذا الفضاء إذا تطلب الأمر ذلك. وفي يونيو 2011 أعلن وزير الدفاع الأمريكي ويليام جيم لين أنه سيتم التعامل كعقيدة عسكرية جديدة مع الفضاء السيبراني كمجال تشغيل مماثل للأرض والجو والبحر والفضاء الخارجي (اسكندر 2020، 181-182).

مع إطلاق إدارة أوباما الإستراتيجية عام 2010، ظهر الحديث عن تأمين الفضاء الإلكتروني بوصفه الشق الآخر من الهدف الثاني للإستراتيجية (تعزيز الأمن القومي الأمريكى فى الداخل)

والذى يأتي مع التهديدات غير المتماثلة التي تهدد الأمن القومي الأمريكى، إذ حددت الإستراتيجية مستويين لمهاجمة وردع ومنع وكشف الاختراقات الإلكترونية. فعلى المستوى الداخلي: يتم ذلك من طريق التعاون مع القطاع الخاص فى انتاج تكنولوجيا أكثر أمنا تدعم القدرة على حماية و تحسين النظم والشبكات الحكومية والصناعية الحيوية، فضلاً عن الاستثمار في مجالات الأبحاث المتطورة اللازمة للإبتكار لمواجهه التحديات، و كذا للقيام بحملة موسعه لدعم التوعية الأمنية الإلكترونية. وفي إطار العمل المشترك بين الهيئات الأمريكية، شهد عام 2011 انطلاق أول إستراتيجية للأمن السيبراني، بعد أكثر من عام من إنشاء القيادة السيبرانية، وقد عكست تلك الإستراتيجية رؤية إدارة أوباما التي اتسمت بالتفاؤل بشأن دعم الديموقراطية العالمية في مجال الفضاء السيبراني، من طريق المشاركة في تغطية الفضاء السيبراني، وتعزيز حرية الحركة في الفضاء الإلكتروني بين فواعل النظام الدولي، وتوزيع الفرص الاقتصادية، ودعم حقوق الإنسان. وقد تبنَّت الإدارة الأدوات الدبلوماسية والإستراتيجية غير العسكرية لتحقيق هذه الغايات (Lonergan and Schneider 2023, 2).

وضعت الإستراتيجية الدولية للفضاء السيبرانى لعام 2011 للولايات المتحدة على رأس أولوياتها دعم وتعزيز المعايير الدولية والأسواق المنفتحة من طريق تشجيع الابتكار التكنولوجي فى إطار التجارة الحره المستدامة، كما دعمت حماية الملكية الفكرية والأسرار التجارية وكذلك إعطاء الأولوية للمعايير الفنية الآمنه فضلاً عن دعم القابلية للتشغيل البيئي.

علاوة على ذلك، فقد عدت إستراتيجية وزارة الدفاع الأمريكية للفضاء السيبرانى عام 2011 إن التهديدات السيبرانية للأمن القومي الأمريكي لاتقتصر فقط على الأهداف العسكرية وإنما تمتد لتشمل جوانب الحياة جميعها بما فيها البنية التحتية المدنية وشبكات الطاقة والنقل والأنظمة المالية (فودة 162،2023).

غير إن الهجوم السـيبراني الذي تعرضـت له الولايات المتحدة الأمريكية بين عامي 2014 و 2015، الذي كان قد اسـتهدف المكتب الأمريكي لإدارة شـؤون الموظفين، وهو قسـم الموارد البشـرية المسـؤول عن التصـاريح الأمنية للوكالات الفيدرالية، الذي عد الهجوم السـيبراني الأخطر، والأكثر إضـرارًا للولايات المتحدة آنذاك؛ ما دفع الإدارة الأمريكية لتطوير الجهود الرامية لتطوير اسـتراتيجياتها لمواجهة تحديات الأمن السـيبراني محليًّا وعالميًّا (علاءالدين

2021)؛ إذ دفعت المخاطر السـيبرانية الجسـيمة التي واجهتها الولايات المتحدة الإدارة الأمريكية لإعادة النظر في استراتيجيات الأمن السيبراني.

وقد شهد عام 2015 إطلاق إدارة أوباما إستراتيجية حملت الكثير من التدابير التي وُصِفت بأنها أكثر عدوانية، مما يعني اختلاف رؤية الإدارة للأمن السيبراني الأمريكي عن سابقتها في كونها أكثر وضوحًا في تحديد قدراتها وتسمية خصومها؛ خاصة الصين وروسيا وإيران) (National Security Strategy of the United States of America 2015). جاءت تلك الإستراتيجية بعد تعرض الولايات المتحدة لهجمات سيبرانية كان لها تداعياتها الخطيرة على أمن وسلامة العديد من المؤسسات والهيئات الأمريكية (Sanger 2015)، ولكن على الرغم من أن تحديد إستراتيجية عام 2015 خصوم الولايات المتحدة من غير الدول والفاعلين الدوليين غير الرسميين، عكس إستراتيجية عام 2011 التي – وفقًا لرأي المحللين – لم تميز بين أنواع الخصوم، فإن كليهما لم يحدد بشكل قاطع وواضح سبل معالجة تهديدات الخصوم كما اتفقت كل منهما في الاعتماد على مجموعة من الموضوعات المشتركة؛ منها التكنولوجيا، والموارد، والتعاون، فضلاً عن التركيز على سبل الوقاية والدفاع. وفيما يأتي عرض لمقارنة بين أهم موضوعات استراتيجيات الأمن السيبراني التي أطلقتها وزارة الدفاع في عامي 2011 و2015.

جدول (1) مقارنة بين اهم موضوعات استراتيجية الأمن السيبراني لوزارة الدفاع الأمريكية في عامي 2011 – 2015

إستراتيجية وزارة الدفاع للعمل في الفضاء السيبراني، أبريل 2015.	**إستراتيجية وزارة الدفاع للعمل في الفضاء السيبراني، يوليو 2011.**
البناء والصيانة التي تستهدف جاهزية قوات وقدرات للقيام بأي نوع من العمليات السيبرانية.	التعامل مع الفضاء الإلكتروني بوصفه مجالا تشغيليًا للتنظيم والتجهيز والتدريب بالشكل الذي يجعل وزارة الدفاع قادرة على الاستفادة الكاملة من إمكانيات الفضاء السيبراني.
الدفاع عن معلومات وزارة الدفاع؛ وذلك من طريق تأمين شبكة اتصال وزارة الدفاع وتخفيف المخاطر التي تتعرض لها.	توظيف مجموعة من المفاهيم التشغيلية الدفاعية الجديدة لحماية الأمن الشبكي لوزارة الدفاع.
الاستعداد الدائم للدفاع عن الولايات المتحدة ومصالحها الحيوية، ومواجهة الهجمات الإلكترونية التخريبية أو المدمّرة ذات العواقب الوخيمة.	دعم الشراكة بين الولايات المتحدة والدول الأخرى، وكذلك دعم التعاون بين الإدارات والهيئات الحكومية، وربط القطاع العام والخاص، لتمكين وزارة الدفاع من تنفيذ إستراتيجية الولايات المتحدة الشاملة للأمن السيبراني.

بناء وصيانة خيارات وخطط إلكترونية قابلة للتطبيق بهدف السيطرة على تصعيد الصراع وتشكيل بيئة الصراع في المراحل جميعاً.	بناء علاقة قوية لدعم سبل التعاون والمشاركة بين حلفاء الولايات المتحدة والشركاء الدوليين لتعزيز الأمن السيبراني الجماعي على المستوى الدولي.
بناء تحالفات وشراكات قوية للاستفادة من قوة عمل إلكترونية استثنائية لردع التهديدات المشتركة وزيادة الأمن والاستقرار السيبراني.	

Source: Caton, Jeffrey L. .2017. *Evaluation of the 2015 DOD Cyber Strategy:* Mild Progress in a Complex and Dynamic Military Domain. Strategic Studies Institute, US Army War College. https://apps.dtic.mil/sti/pdfs/AD1056843.pdf

نستخلص مما سبق إن رؤية إدارة أوباما للأمن السيبراني اختلفت باختلاف إستراتيجيتها للأمن السيبراني؛ إذ اتسمت الأولى بالمرونة والدبلوماسية، وإعلاء قيم التعاون والمشاركة الدولية والدفاع عن حقوق الإنسان؛ في حين أدت الهجمات الخطيرة التي واجهتها الإدارة في نهاية الولاية الأولى تقريبًا إلى إعادة مراجعة رؤيتها للأمن السيبراني، لتتخذ إستراتيجية أكثر شراسة وعدوانية تجاه خصوم الولايات المتحدة، الذين حددتهم بالفعل؛ وعلى رأسهم روسيا والصين.

المحور الثاني: الإستراتيجية السيبرانية للولايات المتحدة خلال المدة من 2017 وحتى 2024.

تشمل تلك المدة إستراتيجيتان للأمن السيبراني، إحداهما أطلقتها إدارة الرئيس الأمريكي السابق "دونالد ترامب "، والذي استمرت ولايته خلال المدة من 2017 وحتى 2021. أما الثانية فكانت لإدارة الرئيس "جوبايدن" والمستمرة ولايته من عام 2021 وحتى عام 2024.

أولاً: الإستراتيجية السيبرانية في مدة الرئيس الأمريكي ترامب

أطلقت إدارة ترامب إستراتيجيتها السيبرانية الوطنية عام 2018، في وسط أجواء مفعمة بالتهديدات السيبرانية الموجهة للولايات المتحدة من قبل خصومها الدوليين، التي أسفرت بدورها عن انتقادات موسَّعة موجَّهة لعدم قدرة الإدارة لمنع تلك التهديدات، أو حتى تحجيمها من طريق تبني إستراتيجية تعمل على تحقيق الأمن للولايات المتحدة في مجال الفضاء السيبراني (Aktinson 2020). هذا وقد أطلق مجلس الأمن القومي الأمريكي بيانًا وصف فيه الإستراتيجية بوصفها أول إستراتيجية مفصلة للأمن السيبراني للولايات المتحدة منذ عام 2003؛ إذ أطلقت إدارة بوش الابن – آنذاك– إستراتيجية مفصَّلة لحماية الفضاء الإلكتروني للولايات

المتحدة. وتنطلق إستراتيجية إدارة ترامب من قناعة إن "الولايات المتحدة هي التي أنشأت الإنترنت، وإن عليها أن تحافظ على دورها المهيمن في تحديد الفضاء السيبراني، وتشكيله وحمايته"، ومن هنا تنطلق إستراتيجية ترامب من مبدأ الحد من القيود التي وضعها سلفه أوباما على السياسات المتعلقة بالأمن السيبراني للولايات المتحدة؛ إذ وجه ترامب بالسماح للمؤسسة العسكرية الأمريكية والوكالات الأخرى بعمليات سيبرانية ترمي لحماية أنظمة وشبكات الولايات المتحدة الحرجة التي يؤثر استهدافها في قوة الولايات المتحدة ومكانتها الدولية (عبدالعاطى 2018)، وهو ما يوضِّح سعي ترامب الحثيث لجعل الفضاء الإلكتروني للولايات المتحدة بمثابة فرع سادس للجيش الأمريكي إذ يستوجب على الولايات المتحدة، وفقاً لإدارة ترامب، فرض الهيمنة عليه للحد من التهديدات التي تواجهها الولايات المتحدة نتيجة لتفوُّق منافسيها وخصومها في مجال الفضاء الإلكتروني. وبعد صدور التقرير الصادم من مكتب المحاسبة الحكومي الأمريكي؛ تحديدًا في سبتمبر من عام 2018 حول التهديدات والمخاطر السيبرانية التي تواجهها المؤسسات الأمريكية كافة، أطلقت وزارة الدفاع والبيت الأبيض إستراتيجية مفصَّلة للأمن السيبراني الأمريكي (الرفيعى 2021، 306-308). وتقوم الإستراتيجية الأمريكية للأمن السيبراني حقبة ولاية ترامب على أربع ركائز أساسية، وتشمل:

1- الحفاظ على الأمن الأمريكي في عصر الإنترنت:

في إطار هذه الركيزة ترى الإدارة ضرورة تأمين الشبكات والمعلومات الفيدرالية، مما يستوجب إعطاء قدر أكبر من السلطة لوزارة الأمن الداخلي للوصول إلى أنظمة معلومات الوكالة لأغراض الأمن السيبراني، كما تدعم الإدارة تأمين البنية التحتية كأولوية أخرى من طريق رفع مستوى وتحسين كفاءة الأمن السيبراني. من خلال مركزية الإدارة والإشراف على الأمن السيبراني المدني الفيدرالي، وتسعى إدارة ترامب من إطار إستراتيجيتها للأمن السيبراني إلى إدارة التهديدات وفقاً لحجم المخاطر التي تراها مستهدفة للأمن القومي للولايات المتحدة؛ إذ تركز بالأساس على تقليل المخاطر في سبعة مجالات رئيسة؛ ألا وهي: المالية والاتصالات والصحة والسلامة وتكنولوجيا المعلومات والنقل، كما ستواصل الحكومة الفيدرالية حماية معايير الأمن السيبراني للعمليات الانتخابية وما يرتبط بها من آليات كما تسعى الإدارة أيضًا للاستفادة من مقدمي تكنولوجيا المعلومات والاتصالات كعوامل تمكين للأمن السيبراني, وذلك في إطار دعمها لأمن البنية التحتية.

2- تعزيز الرخاء الأمريكي:

إذ تسعى الإدارة الأمريكية من طريق تلك الركيزة إلى الحفاظ على النفوذ الأمريكي في النظام البيئي التكنولوجي من خلال دعم وتطوير الفضاء الإلكتروني بوصفه محركًا مفتوحًا للنمو الاقتصادي والإبداع والمهارة. مما يتوجب على الإدارة دعم اقتصاد رقمي حيوي ومرن، فضلاً عن توفير سبل الحماية والدعم للبراعة الأمريكية من أجل تطوير قوة عاملة ماهرة في مجال الأمن السيبراني.

3- الحفاظ على السلام من خلال القوة:

تستهدف الإستراتيجية من طريق تلك الركيزة تحديد ومواجهة وتعطيل وتحطيم أي سلوك عدواني من شأنه المساس بالاستقرار الأمريكي والمصالح القومية للولايات المتحدة في مجال الفضاء السيبراني، جنبًا إلى جنب مع الحفاظ على التفوق الأمريكي في الفضاء الإلكتروني، ولتحقيق ذلك ترى الإدارة في إطار تلك الإستراتيجية ضرورة تعظيم دور الدولة في إرساء قواعد السلوك السيبراني المسؤول للدولة من أجل الحفاظ على الاستقرار السيبراني للولايات المتحدة، فقد أشارت الولايات المتحدة وبشكل واضح ومعلن إلى أنشطة روسيا في مجال الفضاء السيبراني، واستثماراتها في مجال القدرات العسكرية الجديدة، بما في ذلك "القدرات السيبرانية المزعزعة للاستقرار العالمي". كما أعلنت الإدارة الأمريكية تورط روسيا للتأثير في نتائج الانتخابات في الولايات المتحدة؛ فمن طريق الأشكال الحديثة من التكتيكات التخريبية تستطيع روسيا التدخل في السياسات الداخلية للدول؛ الأمر الذي يستلزم مواجهته وبقوة. من هنا ترى إدارة ترامب ضرورة دمج وتوظيف الخيارات السيبرانية عبر توظيف عناصر القوة الأمريكية المختلفة كافة باستعمال متكامل على المستوى الدبلوماسي والعسكري والاقتصادي. وهنا يجب، وفقاً للاستراتيجية الأمريكية للأمن السيبراني، ترسيخ الالتزام الدولي بالقوانين الدولية السيبرانية، والمعايير الدولية غير الملزمة لتحقيق الاستقرار في مجال الفضاء السيبراني العالمي. وأشارت الإدارة الأمريكية في سياق الركيزة الثالثة إلى استعمالها لمجتمع الاستخبارات الأمريكي والمبادرة الأمريكية الدولية للردع السيبراني لمواجهة النفوذ الخبيث من طريق التعاون والعمل المشترك بين الشركاء الحكوميين الأجانب والمجتمع المدني والقطاع الخاص والأوساط الأكاديمية.

4- الدعوة لحرية الإنترنت في أنحاء العالم جميعاً:

في إطار هذه الركيزة، تقدم الولايات المتحدة نفسها بكونها محط أنظار العالم لكونها المصدر الأول للتكنولوجيا، مما يستلزم عليها أن تضع نفسها في موقع قيادة الفضاء السيبراني العالمي؛ ومن هنا يجب على الإدارة التخطيط لبناء القدرة السيبرانية الدولية من طريق ضخ الاستثمارات في الشركات العالمية المكملة لجهود الحكومة في الفضاء السيبراني.

في هذا السياق، نصَّت الاستراتيجية على إن الإدارة ستعمل على تعزيز شبكة إنترنت مفتوحة وقابلة للتشغيل البيني وموثوقة وآمنة، مما يتطلب دعم مبدأ حرية الإنترنت كحق أساسي من حقوق الإنسان من طريق العمل جنبًا إلى جنب مع الدول الأخرى والصناعات العالمية والأوساط الأكاديمية والمدنيين الداعمين للآراء والمبادئ نفسها من أجل دعم التدفق الحر للاتصالات الدولية بالتكامل مع حرية التعبير والأمن القومي (NATIONAL CYBER STRATEGof the United States of America 2018).

في إطار العرض السابق، يمكن القول إن إستراتيجية الأمن السيبراني لعام 2018، التي بلورت رؤية الإدارة للأمن السيبراني، بوصف أن تحقيق أمن ورخاء الشعب الأمريكي أولوية قصوى لها لا يمكن أن تتحقق على أرض الواقع إلا من طريق تعزيز أمن الفضاء السيبراني، الذي لا بد وأن يحدث في ظل إطار حالة من التعاون بين الحكومة الفيدرالية والقطاع الخاص لتأمين البنى التحتية الأكثر تعرضًا للمخاطر كما ارتأت الإدارة ضرورة دعم الاستثمارات المتوائمة مع أولويات الولايات المتحدة، التي تركز على بناء نُهج جديدة للأمن السيبراني قائمة على التقنيات الناشئة، وداعمة لتحسين تبادل المعلومات وإدارة المخاطر الناجمة عن ربط البنى التحتية التكنولوجية للقطاعات المختلفة في إطار تسهيل التطوير المتسارع وإطلاق الجيل التالي من البنى التحتية للاتصالات والمعلومات. على صعيد المجال الدولي، قدمت إدارة ترامب رؤيتها في إطار الإستراتيجية التي دعمت الجهود الرامية لتحسين التعاون الدولي في المجال السيبراني، وتعزيز إطار سلوك الدولة المسؤولة في الفضاء الإلكتروني المبني على القانون الدولي على صعيد آخر؛ اتخذت إستراتيجيات الأمن السيبراني منحنى جديدًا أكثر عدوانية وشراسة في مواجهة من حددتهم الولايات المتحدة كخصوم لها في مجال الفضاء السيبراني؛ إذ اعتمدت إستراتيجية ترامب للأمن السيبراني الجانب الهجومي الاستباقي للدفاع عن أمن الولايات المتحدة

الإلكتروني، بوصفه أحد مجالات الأمن القومي للولايات المتحدة، من طريق قوة أكثر فتكًا تتحرك بها الولايات المتحدة إلى الأمام خارج الحدود، لاختراق شبكات الخصم، ودعم تعزيز القدرات لجمع المعلومات الاستخباراتية والاستعداد للصراعات المستقبلية (عبدالصادق 2022). على الرغم من وصف إستراتيجية ترامب للأمن السيبراني بكونها أول إستراتيجية مفصلة، فضلاً عن إنها كانت قد لاقت ترحيبًا من بعض السياسيين والمختصين في مجال الأمن السيبراني لكونها تعطي الولايات المتحدة نطاقًا أوسع مما كان للتصدي العاجل والوقائي لأي هجوم محتمل تراه الولايات المتحدة خطرًا على أمنها القومي؛ إذ تعطي الإستراتيجية الضوء الأخضر للمؤسسات والهيئات الأمريكية كافة المعنية لتوجيه هجمات سيبرانية استباقية، كما يرى الخبراء أن تلك الإستراتيجية تحقق حالة من التوازن بين الإجراءات الدفاعية الفعلية التي تقوم بها الولايات المتحدة وبين ما تفرضه من عقوبات وخيمة على كل من ينفذ هجمات سيبرانية ضدها (الرفيعى 2021، 309).

يرى الباحث؛ إن إستراتيجية ترامب للأمن السيبراني تبنَّت قدرًا كبيرًا من الاستمرارية مع سلفه أوباما بالرغم من انتقاد ترامب الدائم لأوباما وسياسته وإستراتيجيته، إلا أن الإستراتيجية التي أنتجها ترامب اتسمت – بما يخالف إستراتيجية أوباما – بكونها أكثر عدوانية من حيث تبنّيها لمبدأ إفساح المجال أمام الهجمات الدفاعية الاستباقية التي ترى فيها الولايات المتحدة داعمة لأمنها القومي ومصالحها العليا، فضلاً عن إن الإستراتيجية أوضحت ولأول مرة خصوم الولايات المتحدة في الفضاء السيبراني وعلى رأسهم الصين وروسيا، على عكس إستراتيجية أوباما.

ومع هذا فإن إستراتيجية ترامب للأمن السيبراني كانت قد تعرضت لهجوم حاد من قبل الرئيس الأمريكي بايدن قبيل تنصيبه؛ إذ تعرضت الولايات المتحدة الأمريكية إلى هجوم سيبراني واسع شمل حوالي 20 مؤسسة أمريكية، الأمر الذي جعل بايدن يحمل ترامب كامل المسؤولية عن تلك الهجمات الخطرة؛ نظرًا لكونه لا يزال رئيس البلاد قبل تولي بايدن السلطة بشكل رسمي، الأمر الذي جعل بايدن يطلق وبقوة خلال حملته الانتخابية وعوده بجعل الأمن السيبراني للولايات المتحدة أهمية قصوى بالنسبة لإدارته (فرج 2021، 207).

ثانياً: الإستراتيجية السيبرانية في مدة الرئيس الأمريكي بايدن

أطلقت إدارة بايدن في عام 2023 الإستراتيجية الوطنية الجديدة للأمن السيبراني التي تتصور من طريقها إدارة بايدن ما يُعرَف بـــ "تغيرات جوهرية في الديناميكيات الأساسية للنظام البيئي الرقمي"، التي تســعى الإدارة الأمريكية من طريقها للســيطرة على الغالبية العظمى من البنية التحتية الرقمية للبلاد من خلال توســيع دور الحكومة لاتخاذ إجراءات هجومية لاســتباق الهجمات الإلكترونية؛ وخاصة الهجمات الخارجية (Sanger 2023).

وقد حددت الإســتراتيجية خطة بعيدة المدى لتحقيق بيئة ســيبرانية أكثر أمنًا للولايات المتحدة استنادًا على تحولين أساسين؛ أولهما: إن "الكيانات الأكبر والأكثر قدرة والأفضل وضعًا" في كل من القطاعين العام والخاص "تتحمل فرصــة أكبر من عبء تخفيف المخاطر السيبرانية". وثانيهما: البحث في إعادة تنظيم "الحوافز لصــالح الاســتثمارات طويلة الأجل" التي ترمي إلى بناء "نظام بيئي رقمي مســتقبلي أكثر قابلية للدفاع عنه وأكثر مرونة بطبيعته " (Lostri and Pell 2023)

ركزت إستراتيجية الأمن السيبراني لإدارة بايدن على خمس أمور رئيسة، على النحو الآتي:

1- الدفاع عن البنية التحتية الحيوية:

تفيد بوجوب حرص مالكي ومشــغلي البنية التحتية الحيوية على أن ""يتمتعوا بوســائل حماية للأمن الســيبراني لجعل من الصــعب على الخصــوم تعطيلها"، وتنفيذ هذه الركيزة يتطلب مجموعة من المتطلبات الجديدة على المستوى التنفيذي والتشريعي؛ إذ تتطلب هذه الركيزة من الإســتراتيجية خمســة أهداف: 1- تحديد متطلبات الأمن الســيبراني لدعم الأمن القومي. 2- توســيع نطاق التعاون بين القطاع العام والخاص. 3- دمج مراكز الأمن الســيبراني الفيدرالية. 4 - تحديث خطط وعمليات الاستجابة للحوادث الفيدرالية. 5- تحديث الدفاعات الفيدرالية.

ولتحقيق هذه الأهداف، تسعى الإدارة لتشجيع الدول والجهات التنظيمية المستقلة على استعمال سلطتها لتحديد متطلبات الأمن السيبراني بطريقة منسقة، كما تحدد الاستراتيجية في ضوء هذه الركيزة الخدمات السحابية بالتحديد بوصفها محور التركيز؛ نظرًا لاعتماد العديد من القطاعات على البنية التحتية الســحابية. كما تدعم الإدارة التخطيط للعمل مع الصــناعة والكونجرس والجهات التنظيمية لسد أي فجوات في السلطات لدفع ممارسات أفضل للأمن السيبراني في صناعة الحوسبة السحابية.

2- تعطيل وتفكيك جهات التهديد:

تعد هذه الركيزة بمثابة نهج استباقي لمواجهة التهديدات السيبرانية، مما يتطلب – وفقاً للإستراتيجية – ضرورة إزالة الحواجز، ودعم التعاون المشترك بين القطاعين العام والخاص، في إطار تبادل المعلومات الاستخباراتية ومكافحة الأخطار الإلكترونية المستمرة؛ وعلى رأسها "برامج الفدية".

3- تشكيل قوى السوق لتعزيز الأمن والمرونة:

تنص الركيزة الثالثة على إن الإدارة "لن تحل محل، أو تقلل من دور السوق، ولكنها ستوجه قوى السوق بشكل منتج نحو الحفاظ على مرونة وأمان البلاد"، وفي هذا السياق تتبنَّى الركيزة الثالثة في إستراتيجية الأمن السيبراني للرئيس بايدن ستة أهداف إستراتيجية:

أ- مساءلة المشرفين على بياناتنا.

ب- دفع "IOT".

ت- تطوير أجهزة إنترنت الأشياء وتحويل المسؤولية عن المنتجات والخدمات غير الآمنة.

ث- استعمال المنح والحوافز الفيدرالية لبناء الأمن.

ج- الاستفادة بشكل أكبر من المشتريات الفيدرالية لتحسين نظم المساءلة

ح- استكشاف مساندة التأمين السيبراني الفيدرالي.

كما تؤكد الركيزة الثالثة على دعم الإدارة للتشريعات المتعلقة بالتعامل مع البيانات الشخصية؛ إذ تنص الإستراتيجية على إن "الإدارة تدعم الجهود التشريعية لفرض حدود قوية وواضحة للقدرة على جمع البيانات الشخصية وعلى الجانب الآخر فإن الإستراتيجية تتبنَّى أولوية جديدة تتمثل في تحويل مسؤولية الأمن السيبراني عن تلك الكيانات التي تفشل في اتخاذ الاحتياطات المعقولة لتأمين برامجها حتى وإن كانت تعترف أن برامج الأمان الأكثر تقدمًا لا يمكنها تفادي نقاط الضعف كافة. وفى سياق متصل تحدد الركيزة الثالثة تحفيز تطوير البرمجيات الآمنة من خلال أربع مجالات أخرى تعتزم الإدارة إتباعها لتعزيز برامج الأمن:

أ- تشجيع الكشف المنسق عن الثغرات الأمنية.

ب- تشجيع التطوير الإضافي.

ت- تطوير عملية SBOMs لقوائم مواد البرامج وتخفيف المخاطر الناجمة عن البرامج غير المدعومة.

ث- الشراكة مع القطاع الخاص ومجتمع البرمجيات بشكل مفتوح النطاق للاستثمار في تطوير البرامج الآمنة.

وأخيرًا تركز الركيزة الثالثة أيضًا على المبادرات الحالية بشأن الأمن السيبراني وإنترنت الأشياء، وكذلك التأمين ضد الحوادث السيبرانية، وبناءً على ذلك تعتزم الإدارة استكشاف الحاجة والهياكل المحتملة لاستجابة التأمين الفيدرالي للأحداث السيبرانية الكارثية.

4- الاستثمار في مستقبل مرن:

في إطار هذه الركيزة، تشير الإستراتيجية إلى ضرورة الحاجة لتطوير وتنفيذ الحلول التي من شأنها تأمين الأسس التقنية للإنترنت، التي وصفتها الإدارة بأنها "ضعيفة بطبيعتها"، كما تدعو الإستراتيجية في هذا الإطار إلى تجديد الاستثمار الفيدرالي في البحث والتطوير في المجال التقني مثل البيئات القائمة على التشفير الكمي وحلول الهوية الرقمية المحسنة، وأخيرًا تنص الركيزة على أن تتولى مسؤولية تنفيذ إستراتيجية توسيع القوى العاملة السيبرانية.

ولتحقيق هذه الأهداف، فإن الركيزة الرابعة للإستراتيجية التي تسعى من طريق الاستثمارات الإستراتيجية والعمل المنسق؛ تتبنى ستة أهداف:

أ- تأمين الأساس التقني للإنترنت.

ب- إعادة التطوير الفيدرالي في مجال الأمن السيبراني.

ت- الانطلاق للمستقبل التقني.

ث- تأمين مستقبل الطاقة النظيفة للولايات المتحدة.

ج- دعم تطوير النظام البيئي للهوية الرقمية.

ح- تطوير استراتيجية وطنية لتعزيز القوى العاملة السيبرانية.

5- إقامة شراكات دولية لتحقيق الأهداف المشتركة:

تستهدف هذه الركيزة بناء تحالف واسع من الدول التي تسعى للحفاظ على الإنترنت المفتوح والحر والآمن والعالمي، القابل للتشغيل البيني وموضع ثقة، وفي هذا الإطار تحدد الركيزة خمسة أهداف إستراتيجية:

أ- بناء تحالفات لمواجهة التهديدات التي يتعرض لها النظام البيئي الرقمي.

ب- تعزيز قدرات الشركاء الدوليين.

ت- توسيع قدرة الولايات المتحدة على مساعدة الحلفاء والشركاء الدوليين.

ث- بناء تحالفات لتعزيز المعايير الدولية لسلوك الدول المعنية.

ج- تأمين سلاسل التوريد العالمية للمعلومات والاتصالات ومنتجات وخدمات التكنولوجيا.

في إطار ما سبق؛ فإن هذه الركيزة تسلط الضوء على التزام الإدارة بتعزيز التعاون المشترك مع الشركاء الدوليين لمكافحة التهديدات المتمركزة في البلدان الأجنبية من خلال وضع سياسات لتوفير الدعم السيبراني للشركاء، وكذلك محاسبة الدول على انتهاك القانون الدولي في الفضاء السيبراني.

وأخيرًا تتبنَّى الإستراتيجية دعم جهود الحكومة الفيدرالية الحالية لتأمين سلاسل التوريد؛ مثل الصندوق الدولي لأمن التكنولوجيا والابتكار، الذي تم إنشاؤه عام 2022 لدعم سلاسل التوريد الآمنة للمواصلات والاتصالات (The White House 2023)

إيجازًا لما سبق، فإن إستراتيجية بايدن للأمن السيبراني، التي ركَّزت على وضع الأمن السيبراني للولايات المتحدة على قائمة الأولويات القصوى للإدارة من طريق رفع مستوى الأمن السيبراني كضرورة حتمية للهيئات الحكومية كافة؛ وذلك حتى تتعزز قدرات الولايات المتحدة واستعداداتها في الفضاء السيبراني، وفي سبيل تحقيق ذلك ترى إدارة بايدن إن التعاون بين القطاعين العام والخاص على الأصعدة جميعها لبناء بيئة آمنه للمواطنين الأمريكيين من طريق إدارة المخاطر وتقاسمها، ولذلك فعلى الدولة توسيع الاستثمارات ودعم المواهب القادرة على دعم المجال السيبراني، وهو ما اختلفت فيه إستراتيجية بايدن عن إستراتيجية ترامب التي لم تتناول بالأساس كيفية دعم الدولة للموهوبين في مجال الأمن السيبراني للاستعانة بهم.

وعلى الصعيد الدولي فإن إستراتيجية بايدن كانت قد أكدت على دعمها الالتزام بالمشاركة الدولية في القضايا السيبرانية، ودعم سبل التعاون والعمل المشترك مع الحلفاء في مجال الفضاء السيبراني لدعم المعايير العالمية الحالية وصياغة معايير جديدة أكثر ملاءمة لما يحدث في مجال الفضاء الإلكتروني من تطورات.

يرى الباحث. أنه بالنظر إلى الركائز الأساسية التي اعتمدت عليها كل إدارة في صياغة إستراتيجيتها للأمن السيبراني، فإن جوانب الاستمرارية أكثر بكثير من أوجه التغير.

المناقشات:

أدركت الإدارات الأمريكية المتعاقبة، وتحديدًا منذ عام 2009 وحتى عام 2024، أهمية تأمين المجال السيبراني بوصفه أحد أهم مجالات الأمن القومي للولايات المتحدة، غير أن كل إدارة

كانت قد قدمت إستراتيجيتها الخاصة للأمن السيبراني، التي تعكس من طريقها رؤيتها وأهدافها وأدواتها الخاصة.

هذا وقد شهدت هذه الإستراتيجيات منذ مدة الدراسة وحتى نهايتها مجموعة من التطورات التي حاولت من طريقها الإدارات الأمريكية مواجهة التهديدات والمخاطر سريعة التغيُّر والتطور أيضا؛ فخلال ولاية الرئيس الأمريكي أوباما، أصدرت الإدارة الأمريكية ما يُعرَف بـ "مرجعية سياسة الفضاء الإلكتروني"، التي أطلقتها تحديدًا عام 2009 لتؤكد من طريقها على أهمية تأمين البنية الحيوية التحتية في إطار من العمل المشترك بين القطاعين العام والخاص لتحسين قدرات الاستجابة للمخاطر، لتعود الإدارة مرة أخرى للتوجيه الرئاسي رقم 20 لتدعم من طريقه دمج القدرات العسكرية مع القدرات السيبرانية بهدف التحول في نهج العمليات السيبرانية إلى النمط الهجومي.

فمنذ بداية تولّيه الإدارة قاد أوباما العديد من الجهود لمواجهة التهديدات السيبرانية التي تواجه الأمن الأمريكي، ولهذا السبب أصدر في عام 2011 مقترحًا تشريعيًّا لدعم الأمن السيبراني، داعيًا الكونجرس لضرورة إصدار تشريعات عاجلة لمواجهة التهديدات السيبرانية في الداخل والخارج، ومع فشل الكونجرس في إقرار تشريع شامل للأمن السيبراني، استصدرت الإدارة أمرًا تنفيذيًّا لحماية البنية التحتية، استنادًا على وضع معايير أساسية للأمن السيبراني، وفي هذا الإطار قدَّمت إدارة أوباما استراتيجية دولية للفضاء السيبراني لتوجِّه بها أنظار العالم.

في عام 2015، أطلق الرئيس أوباما نسخة جديدة من الإستراتيجية التي تعلن فيها الولايات المتحدة الصين بشكل صريح كمصدر للخطر الذي يواجه الولايات المتحدة في مجال الفضاء الإلكتروني، مما يستلزم على الولايات المتحدة اتخاذ الإجراءات اللازمة لحماية المصالح الأمريكية والدفاع عن الشبكات الأمريكية ضد السرقة الإلكترونية، وخاصة تلك التهديدات الموجهة من الحكومة الصينية على وجه التحديد، مما عده الكثير من المحللين أمرًا ملفتًا.

أما ولاية ترامب، فقد شهدت العديد من التحولات في الإستراتيجية السيبرانية التي قدمتها الإدارة بوصفها "أول إستراتيجية واضحة المعالم للولايات المتحدة منذ عام 2003"، وقد عرفت إدارة

ترامب بوضـــوح أعداءها وأهدافها في الفضـــاء الســـيبراني، مؤكدة على إن الولايات المتحدة منخرطة في منافسة مستمرة ضد الخصوم الإستراتيجيين والدول المارقة والشبكات الإرهابية والإجرامية؛ خاصة خصومها التقليديين وعلى رأسهم روسيا والصين وإيران وكوريا الشمالية؛ إذ يستعمل هؤلاء الخصـــوم – وفقًا للإدارة الأمريكية – الأدوات الســـيبرانية لتقويض المصـــالح الأمريكية وتهديد الأمن القومي الأمريكي. ولذا تمت صياغة الإستراتيجية السيبرانية الأمريكية لتصـــبح أكثر تركيزًا على دعم القدرات الســـيبرانية الهجومية وإعادة تقييم الاتفاقات الدولية المرتبطة بالمجال السيبراني، والتركيز على العمل الأحادي الجانب في مجال الأمن السيبراني. وقد أعلنت الإدارة الأمريكية صراحة في إطار إستراتيجية عام 2017 ضرورة مواجهة الخصوم السيبرانيين بشكل أكثر عدوانية في إطار ما وصفته بالهجمات الاستباقية كأحد آليات الإدارة للحفاظ على أمن الولايات المتحدة وقوتها ومقدراتها في الفضاء السيبراني.

ومع الانتقال لولاية بايدن، تأتي إســـتراتيجية عام 2021 للأمن الســـيبراني لتعيد التركيز على أهمية الدبلوماسية السيبرانية، وضرورة إعادة بناء أواصر الصلة والتعاون بين أعضاء المجتمع الدولي لحماية البنية التحتية الحيوية من الهجمات الســـيبرانية، مع التأكيد على ضـــرورة دعم التعاون بين القطاعين العام والخاص لدعم آليات المرونة في المجال الســـيبراني، كما أعادت التركيز أيضًـــا على ضـــرورة إعادة حوافز السوق لصـــالح تصـــميم البرمجيات الآمنة، وتحويل المســؤولية عن المنتجات والخدمات المعرضـــة للخطر من المســـتعملين النهائيين إلى أفضـــل وضع وتنظيم حوافز السوق لصالح تصميم البرمجيات الآمنة. وعلى الرغم من إن الإستراتيجية تتشارك في معظم أهدافها على تلك التي تبنَّتها إستراتيجية سلفه ترامب فإن إستراتيجية بايدن اعترفت بشـــكل ضـــمني بان الولايات المتحدة لا يمكن لها مهما كانت قدراتها منع الهجمات السيبرانية الموجّهة للولايات المتحدة وحلفائها بشكل كامل.

كما تشـــير كل من الإســـتراتيجية الوطنية للأمن الســـيبراني (NSS) والإســـتراتيجية الوطنية السيبرانية(NCS) ، فإن عقد 2020 سيكون عقدًا حاسمًا، إذ ستشكل الإجراءات المتخذة الآن

معالم الفضـــاء الســـيبراني والتقنيات الرقمية والاقتصـــاد الرقمي في المســـتقبل. مع تنفيذ هذه الإسـتراتيجية، سـتعمل وزارة الخارجية بالتعاون مع الكونغرس والشـركاء من الوكالات المختلفة على تقييم السلطات السيبرانية الحالية وتعديلها أو إنشاء سلطات جديدة حسب الحاجة لتواكب الوزارة التطورات في التقنيات السيبرانية والرقمية.

كما شهد الفضاء السيبراني تطورات متسارعة في العقدين الأخيرين، إذ أصبح جزءًا أساسيًا من منتمية، وتعزيز التحالفات الدولية لمجابهة المخاطر الســـيبرانية والأمن القومي للدول الكبرى، وعلى رأســها الولايات المتحدة الأمريكية. وتبين من طريق التحليل الســابق أن الاســتراتيجيات الأمريكية المتعاقبة قد شـــهدت تحولات جوهرية للتكيف مع التهديدات المتزايدة التي تفرضـــها البيئة الرقمية.

أولاً: تعزيز القدرات الدفاعية والهجومية:

أظهرت نتائج البحث أن الولايات المتحدة قد انتقلت من مرحلة الدفاع الســلبي إلى اعتماد نهج هجومي أكثر فاعلية لمواجهة التهديدات الســيبرانية. فقد تبنت الإدارة الأمريكية في عهد باراك أوباما اســـتراتيجيات تعزز الدفاع الســـيبراني وحماية البنية التحتية الوطنية، إلا أن هذا النهج شــهد تحولات جذرية خلال إدارة دونالد ترامب، التي ركزت على اعتماد اسـتراتيجيات هجومية وسـياسـات أكثر مرونة في اسـتعمال الأسـلحة السـيبرانية. أما في عهد جو بايدن، فقد تم تبني اســـتراتيجية شـــاملة تدمج بين الدفاع والهجوم، مع التركيز على تقوية التعاون الدولي وتعزيز الدفاعات السيبرانية ضد الهجمات المعادية.

ثانياً: تأثير الهجمات السيبرانية في الأمن القومي الأمريكي:

تشـــير البيانات إلى أن الولايات المتحدة قد تعرضـــت لعدة هجمات ســـيبرانية كبرى أثرت في أمنها القومي، بما في ذلك هجمات اســـتهدفت البنية التحتية للطاقة مثل الهجوم على خط أنابيب كولونيال، فضـلاً عن الهجمات التي اسـتهدفت الانتخابات الأمريكية، مما دفع الحكومة الأمريكية إلى اتخاذ تدابير أكثر صـــرامة لحماية أنظمتها الرقمية. كما يتضـــح من التحليل أن

الجهات الفاعلة، سواء كانت دولًا مثل الصين وروسيا أو مجموعات قرصنة، قد طورت من تقنياتها السيبرانية، مما جعل المواجهة أكثر تعقيدًا.

ثالثاً: التعاون الدولي في الأمن السيبراني:

أحد النتائج المهمة التي أظهرتها المناقشة هو أن الولايات المتحدة لم تعتمد فقط على قدراتها الذاتية، بل عملت على تعزيز التعاون مع حلفائها في الناتو والاتحاد الأوربي، فضلاً عن التنسيق مع القطاع الخاص لمجابهة التهديدات السيبرانية. وقد أدت المنظمات الدولية مثل الأمم المتحدة دورًا في محاولة وضع معايير وضوابط للأمن السيبراني، إلا أن هناك تحديات كبيرة في تنفيذ هذه السياسات نظرًا لاختلاف الأجندات السياسية بين الدول الكبرى.

رابعاً: عسكرة الفضاء السيبراني ومستقبل التوازن الاستراتيجي:

تمثل عسكرة الفضاء السيبراني أحد التحديات الكبرى التي تواجه النظام الدولي، إذ تسعى الولايات المتحدة إلى الحفاظ على تفوقها في هذا المجال عبر تطوير أسلحة سيبرانية متقدمة، إلى جانب إنشاء القوة الفضائية الأمريكية. ومع ذلك، فإن تسارع سباق التسلح السيبراني قد يؤدي إلى تداعيات خطيرة على الأمن والاستقرار العالميين، خاصة مع دخول دول مثل الصين وروسيا في هذا المضمار، مما يزيد من احتمالية نشوب صراعات سيبرانية واسعة النطاق.

الخاتمة:

من خلال استقراء واقع الأمن السيبراني الأمريكي، يمكن استخلاص عدد من النتائج التي تعكس تحديات وفرص استمرارية الاستراتيجية السيبرانية. يتضح أن الأمن السيبراني لم يعد مجرد مسألة تقنية، بل أصبح مكونًا أساسيًا للأمن القومي، إذ تؤدي السياسات المتبعة اليوم دورًا محوريًا في تشكيل مستقبل الفضاء السيبراني، والتقنيات الرقمية، والاقتصاد الرقمي.

على الرغم من الجهود المبذولة عبر الاستراتيجية الوطنية للأمن السيبراني (NSS) والاستراتيجية الوطنية السيبرانية(NCS) ، فإن التهديدات السيبرانية لا تزال تشكل خطرًا متزايدًا، مما يستدعي تقييماً مستمرًا للسياسات القائمة، والعمل على تعديلها أو تطوير أطر

جديدة تستجيب للتطورات المتسارعة في المجال الرقمي. ومن هذا المنطلق، يظهر اتجاه واضح نحو تعزيز التعاون بين وزارة الخارجية الأمريكية والكونغرس والوكالات المختلفة لضمان تحديث القوانين والسلطات السيبرانية بما يواكب التهديدات الراهنة والمستقبلية.

تشير الاستنتاجات إلى أن تنفيذ الاستراتيجية السيبرانية الأمريكية سيشهد مراحل من التقدم والتحديات، ولكن هناك مؤشرات مبكرة تعكس تطورًا إيجابيًا في هذا المسار. فمن ناحية، تستند الولايات المتحدة وحلفاؤها إلى النجاحات السابقة مثل مدونة السلوك لمجموعة السبع في هيروشيما، والأمر التنفيذي لبايدن–هاريس بشأن الذكاء الاصطناعي، مما يعزز من نهج أكثر تنظيمًا لحماية الفضاء السيبراني. ومن ناحية أخرى، يظهر توجه واضح نحو تطوير تفاهمات مشتركة حول أمن وموثوقية البنية التحتية الرقمية، مثل كابلات الاتصالات البحرية، وخدمات السحابة، ومراكز البيانات، مع التركيز على دعم الاقتصادات الناشئة.

علاوة على ذلك، يتزايد اهتمام الولايات المتحدة وحلفائها بترسيخ نقاشات دولية فعالة في الأمم المتحدة حول الأمن السيبراني، وذلك من طريق التركيز على تنفيذ إطار سلوك الدول المسؤول، وبناء قدرات الدول في مواجهة التهديدات السيبرانية. كما إن الاستفادة من صندوق الفضاء السيبراني، والاتصال الرقمي، والتقنيات ذات الصلة، ستسهم في تحسين سرعة الاستجابة للحوادث السيبرانية، وتعزيز مرونة الدول المستهدفة، مما يرسخ مكانة الولايات المتحدة كشريك رئيسي في مجال الأمن الرقمي.

في النهاية، يؤكد هذا التحليل على أن استدامة الأمن السيبراني تتطلب نهجًا تكامليًا يجمع بين التطوير التقني، والتنسيق المؤسساتي، والشراكات الدولية، لضمان استجابة فعالة للتحديات المتغيرة في هذا المجال الحيوي.

قائمة المصادر:

احمد، سيد احمد. 2020. "في دلالات الهجوم الالكتروني على أمريكا". الاهرام، 2020.
https://gate.ahram.org.eg/News/2547973.aspx.

إسكندر، ماجد. 2020."تهديدات الفضاء السيبراني للأمن القومي: دراسة في أنماط التوظيف السياسي للهجمات السيبرانية." أطروحة دكتوراه.، جامعة القاهرة/ كلية الاقتصاد والعلوم السياسية.

الرفيعي، علي محمد إمنيف. 2018. "تحديات الأمن في الفضاء السيبراني الأمريكي." *مجلة دراسات دولية*، عدد 85. (ابريل): 291–314

https://www.iraqoaj.net/iasj/download/c2750450086aa82a

الكعود، إسراء شريف. 2022. "التأثير السيبراني في الامن القومي للدول الفاعلة (الولايات المتحدة الامريكية) نموذجاً." *مجلة العلوم السياسية*، عدد. 64 (ديسمبر): 1-18.
https://doi.org/10.30907/jcopolicy.vi64.628

لامية، طالة. 2021. "التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها." *معالم للدراسات القانونية والسياسية*، عدد .2 (ديسمبر): 69-56.
https://asjp.cerist.dz/en/downArticle/520/4/2/138496

دحماني، سليم. 2018. "أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة نموذجًا (2001-2017)." أطروحة دكتوراه.، جامعة محمد بوضياف/كلية الحقوق والعلوم السياسية.

عبد العاطي، عمرو. 2018. استراتيجية أمريكية هجومية ضد التهديدات السيبرانية. مصر: المركز المصري للفكر والدراسات الاستراتيجية.
https://ecss.com.eg/2077

عبد الصادق، عادل .2022. "صراع السيادة السيبرانية بين التوجهات الأمريكية والروسية". المركز العربي لأبحاث الفضاء الإلكتروني. 2022.
https://accronline.com/article_detail.aspx?id=32528&srsltid=AfmBOoq8jetVFawJ3_R0U_lHZxmQLjdQpj2YCSUKC5YVAsIL_AMo0MdV

عبد الحميد، محمود مدحت مختار. 2020. "الأبعاد الأمنية الحديثة والأمن القومي للدول: دراسة حالة إستراتيجية الأمن القومي للولايات المتحدة الأمريكية في عهد الرئيس دونالد ترامب 2017". المركز الديمقراطي العربي. 16أغسطس، 2020.
https://democraticac.de/?p=68983

علاء الدين، إيمان. 2021. "الأمن السيبراني: المفهوم والتداعيات في السياسة العالمية". مركز الحضارة للدراسات والبحوث. 1ابريل،2021.
https://hadaracenter.com/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D9%85%D9%81%D9%87%D9%88%D9%85-%D9%88%D8%A7%D9%84%D8%AA%D8%AF%D8%A7%D8%B9%D9%8A%D8%/A7%D8%AA-%D9%81

علام، مها محمد محمد. 2014."ثورة المعلومات والأمن القومي: دراسة حالة الولايات المتحدة الأمريكية." رسالة ماجستير.، جامعة القاهرة/ كلية الاقتصاد والعلوم السياسية.

فرج، كرار عباس متعب. 2021. "الحرب السيبرانية: دراسة في الهجمات السيبرانية بين الولايات المتحدة وإيران." *مجلة حمورابي للدراسات*، عدد. 40: 195-223.
https://hamm-journal.org/index.php/HJS/article/view/231/175

فودة، محمود سعودي علي. 2023. "الأمن السيبراني والعلاقات الأمريكية الصينية: بين التعاون والتنافس." أطروحة دكتوراه.، جامعة القاهرة/ كلية الاقتصاد والعلوم السياسية.

هارت، ليدل. 2000. *الإستراتيجية وتاريخها في العالم*. ترجمة الهيثم الأيوبي. بيروت: دار الطليعة للطباعة والنشر.

List of Reference:

Ahmed, Sayed Ahmed. 2020. "On the Implications of the Cyber Attack on America." Al-Ahram, 2020.https://gate.ahram.org.eg/News/2547973. (in Arabic)

Alaa El-Din, Iman. 2021. "Cybersecurity: Concept and Implications in Global Politics." Hadara Center for Studies and Research, April 1, 2021.https://hadaracenter.com/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A7%D9%84%D9%85%D9%81%D9%87%D9%88%D9%85-%D9%88%D8%A7%D9%84%D8%AA%D8%AF%D8%A7%D8%B9%D9%8A%D8%A7%D8%AA-%D9%81 (in Arabic)

Azmi, Riza, William Tibben, and khin Than Win. 2016. *Motives Behind Cyber Security Strategy Development.* Wollongong: Australasian Conference on Information Systems. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1051&context=acis2016

Atkinson, Wade H., Jr**.** 2020. "A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy." lnstitute World politics. October 22, 2020. https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/.

Al-Kaoud, Israa Sharif. 2022. "Cyber Impact on National Security of Active States (United States of America) as a Model." *Political Science Journal*, No. 64: (December): 1-18. https://doi.org/10.30907/jcopolicy.vi64.628. (in Arabic)

Allam, Maha Mohammed Mohammed. 2014. "The Information Revolution and National Security: A Case Study of the United States of America." Master's Thesis., Cairo University/ Faculty of Economics and Political Science.(in Arabic)

Al-Rafii, Ali Muhammad Imanif**.** 2018. "Security Challenges in American Cyberspace." *Journal of International Studies*, No. 85:(April): 291-314. https://www.iraqoaj.net/iasj/download/c2750450086aa82e. (in Arabic)

Abdel Hamid, Mahmoud Medhat Mokhtar. 2020. "Modern Security Dimensions and National Security of States: A Case Study of the National Security Strategy of the United States of America under President Donald Trump 2017." Arab Democratic Center. August 16, 2020.https://democraticac.de/?p=68983. (in Arabic)

Abdel Sadek, Adel. 2022. "The Struggle for Cyber Sovereignty between American and Russian Trends." Arab Center for Cyberspace Research.

2022.https://accronline.com/article_detail.aspx?id=32528&srsltid=AfmBOoq8jetVFawJ3_R0U_lHZxmQLjdQpj2YCSUKC5YVAsIL_AMo0MdV. (in Arabic)

Abdel-Ati, Amr. 2018. *America's Offensive Strategy Against Cyber Threats*. Egypt : Egyptian Center for Thought and Strategic Studies. https://ecss.com.eg/2077. (in Arabic)

Caton, Jeffrey L**.** 2017. Evaluation of the 2015 DOD Cyber Strategy: Mild Progress in a Complex and Dynamic Military Domain. Strategic Studies Institute, US Army War College. https://apps.dtic.mil/sti/pdfs/AD1056843.pdf.

Dahmani, Salim**.** 2018. "The Impact of Cyber Threats on National Security: The United States as a Model (2001-2017)." Master's Thesis., Mohamed Boudiaf University/ Faculty of Law and Political Science. (in Arabic)

Farag, Karar Abbas Mutab**.** 2021. "Cyberwar: A Study of Cyberattacks between the United States and Iran." *Hammurabi Journal of Studies*, No .40: 195-223. https://hamm-journal.org/index.php/HJS/article/view/231/175 (in Arabic)

Fouda, Mahmoud Saoudi Ali**.** 2023. "Cybersecurity and US-China Relations: Between Cooperation and Competition." Master's Thesis., Cairo University/ Faculty of Economics and Political Science. (in Arabic)

Hart, Liddell. 2000. S*trategy and its History in the World*. Translated by Al-Haitham Al-Ayyubi. Beirut: Al-Tali'ah Printing and Publishing House. (in Arabic)

Iskandar, Majed**.** 2020. "Cyberspace Threats to National Security: A Study of the Patterns of Political Employment of Cyber Attacks." Master's Thesis., Cairo University/ Faculty of Economics and Political Science. (in Arabic)

Lonergan, Erica D, and Jacquelyn Schneider**.** 2023. "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation." *Journal of Cybersecurity9,* No.1: (March 31): 1-10. https://doi.org/10.1093/cybsec/tyad006.

Lostri, Eugenia, and Stephanie Pell**.** 2023. "The Biden Administration's Implementation Plan for the National Security Strategy." September 19, 2023. https://www.lawfaremedia.org/article/the-biden-administration-s-implementation-plan-for-the-national-cybersecurity-strategy.

Lamia, Tala**.** 2021. "Cyber Threats and Crimes: Their Impact on National Security and Strategies to Combat Them." *Landmarks for Legal and Political Studies* 4, No. 2 (December): 56-69. https://asjp.cerist.dz/en/downArticle/520/4/2/138496 (in Arabic)

National Security Strategy of the United States of America. 2010. The White House. May, 2010. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

National Security Strategy of the United States of America. 2015. *The White House. February*, 2015. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

National Security Strategy of the United States of Americ. 2018. The White House. September, 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Sanger, David E**.** 2023. "New Biden Cyber Security Strategy Assigns Responsibility to Tech Firms." The New York Times. March 2, 2023. https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html

Sanger, David E. 2015. "Pentagon Announces New Strategy for Cyber Warfare." The New York Times. April 1, 2015. http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.

The White House. 2023. "Background Press Call by Senior Administration Officials Previewing the Biden-Harris Administration's National Cyber Strategy." MARCH 2, 2023. https://bidenwhitehouse.archives.gov/briefing-room/press-briefings/2023/03/02/background-press-call-by-senior-administration-officials-previewing-the-biden-harris-administrations-national-cyber-strategy/