تطور إستراتيجية الأمن السيبراني الأمريكية
الدور الحاسم لإدارة جوزيف بايدن: دراسة مقارنة

م.م. نورا رياض الدباغ
مركز الدراسات الإستراتيجية والدولية / جامعة بغداد
noura.r@cis.uobaghdad.edu.iq

https://doi.org/10.61884/hjs.v1i55.624

ملخص :

تركز هذه الدراسة على مفهوم (الأمن السيبراني) وتأثير التطور التكنولوجي على الأمن القومي الأمريكي. وتبحث في تأثير التقنية على أنواع القوى المختلفة وما للقوة الذكية من أهمية بوصفها أداة لتطوير الأمن السيبراني وتعزيز قوة الدولة. كما تسلط الضوء على أهمية التفكير الإستراتيجي والتكتيكي في تنفيذ تلك الاستراتيجية لحماية البنى التحتية الحيوية، عبر التصدي للتهديدات والمخاطر السيبرانية بانواعها. مما يقتضي ضرورة التعاون الدولي في مجال الأمن السيبراني، وتعزيز الأمن الجماعي لمواجهة التحديات المشتركة. وتُعد مسألة الأمن السيبراني من المسائل الأساسية التي تواليها الولايات المتحدة الأمريكية أهمية كبيرة في العصر الرقمي الحالي. إذ سعت الإدارة السابقة بقيادة الرئيس الأمريكي جوزيف بايدن إلى تطوير إستراتيجية شاملة للأمن السيبراني تهدف إلى تعزيز الحماية السيبرانية للبنية التحتية الحيوية عبر دعم القوى العاملة في المجال السيبراني، وتنمية الوعي بأمن المعلومات والإبلاغ عن الحوادث السيبرانية، وترسيخ التعاون والشراكات مع القطاع الخاص من جهة، والشركاء الدوليين من جهة ثانية، لمكافحة التهديدات السيبرانية وتحسين الأمن السيبراني الأمريكي الشامل.

الكلمات المفتاحية: الأمن السيبراني، القوة الذكية، الإستراتيجية، الأمن القومي، إدارة بايدن

The Evolution of U.S. Cybersecurity Strategy: The Critical Role of the Biden Administration – A Comparative Study

M.M. Noura Riyadh Al-Dabbagh
Center for Strategic and International Studies / University of Baghdad
noura.r@cis.uobaghdad.edu.iq

ABSTRACT:

This study focuses on the concept of cybersecurity and the impact of technological advancement on U.S. national security. It examines the influence of technology on various forms of power and underscores the significance of smart power as a tool for developing cybersecurity and enhancing state power. The research also highlights the importance of strategic and tactical thinking in implementing cybersecurity strategies aimed at protecting critical infrastructure by countering the various types of cyber threats and risks. This necessitates international cooperation in the field of cybersecurity and the strengthening of collective security to confront shared challenges.

Cybersecurity has become a central issue that the United States prioritizes in the current digital era. The previous administration, led by President Joseph Biden, has sought to develop a comprehensive cybersecurity strategy designed to bolster the protection of critical infrastructure by supporting the cyber workforce, enhancing information security awareness, reporting cyber incidents, and consolidating cooperation and partnerships with both the private sector and international partners to combat cyber threats and improve overall U.S. cybersecurity.

KEYWORDS: Cybersecurity, Smart Power, Strategy, National Security, Biden Administration.

المقدمة:

شهد القرن الواحد والعشرين تطور مفهوم الأمن السيبراني بوصفه مفهوماً إستراتيجياً مهماً، إذ لم يعد يقتصر على كونه إجراءً تقنياً لحماية البيانات والأنظمة الرقمية فحسب، بل أصبح عنصراً أساسياً في موازين القوى الدولية يساهم في تحديد مكانة الدول في المشهد العالمي. ومع تسارع التطور التكنولوجي وإزدياد الإعتماد على الفضاء السيبراني، برز الأمن السيبراني بوصفه أحد أهم التحديات التي تواجه الدول، نظراً لتنامي التهديدات الإلكترونية التي تستهدف البنى التحتية الحيوية، والقطاعات الحكومية والإقتصادية، مما يفرض عليها تطوير إستراتيجيات شاملة تتجاوز الدفاع التقليدي إلى مفاهيم الردع والإستجابة الإستباقية. فكيف يمكن للدول تحقيق التوازن بين تعزيز الأمن السيبراني وحماية الخصوصية والحريات الرقمية؟ وإلى أي مدى يمكن إعتبار الفضاء السيبراني ساحة جديدة للصراع الجيوسياسي؟

أهمية البحث

١- تعزيز الوعي والألمام بالتكنولوجيا وتوظيف القوة الذكية لتبني إستراتيجيات إستباقية، لمواجهة التهديدات السيبرانية المستمرة.

٢- تحليل وتقييم أثر إستراتيجيات الأمن السيبراني للولايات المتحدة الأمريكية، في حماية الأمن القومي للدولة.

٣- دراسة إستراتيجية الرئيس الأمريكي جوزيف بايدن للأمن السيبراني والتركيز على الإستراتيجية الوطنية الأمريكية للأمن السيبراني.

٤- تحليل الإجراءات والتدابير التي إتخذتها كل إدارة، وتقييم فعالية تلك الإجراءات في تعزيز الأمن السيبراني للولايات المتحدة الأمريكية.

مشكلة البحث:

١- كيف يؤثر التطور التكنولوجي على الأمن القومي الأمريكي في مجال الأمن السيبراني؟

٢- ما هي أهمية التفكير الإستراتيجي في تنفيذ إستراتيجيات الأمن السيبراني لحماية البنى التحتية الحيوية للولايات المتحدة الإمريكية من جهة، ومدى ضرورة التعاون الدولي في مجال الأمن السيبراني وتعزيزه لمواجهة التحديات المشتركة من جهة أخرى؟

فرضية البحث:

إن تطور إستراتيجية الأمن السيبراني الأمريكية يعكس تباين سياسات الإدارات المتعاقبة في مواجهة التهديدات السيبرانية، إذ تؤثر طبيعة هذه السياسات ما بين التركيز على الدفاع، الهجوم، أو التوازن بينهما على قدرة الولايات المتحدة في حماية أمنها القومي وتعزيز مكانتها في الفضاء السيبراني.

منهجية البحث:

تعتمد هذه الدراسة على المنهج الإستقرائي، والمنهج المقارن.

هيكلية البحث:

يتبع البحث هيكلية تقسمه إلى مبحثين رئيسيين، يتفرع كل منهما إلى ثلاثة مطالب رئيسة بهدف توفير تحليل شامل ومتعمق لمختلف جوانب الموضوع. ففي المبحث الأول درسنا مفهوم الأمن السيبراني في الإستراتيجية الأمريكية عبر تحليل الإطار النظري والمفاهيمي.

وفي المبحث الثاني حللنا إستراتيجية الرئيس الأمريكي جوزيف بايدن للأمن السيبراني.

المبحث الأول

مفهوم الأمن السيبراني في الإستراتيجية الإمريكية

- **المطلب الأول: الأمن السيبراني، مقاربة معرفية**

لكي نفهم معنى (الأمن السيبراني) لابد من التطرق إلى التطور التكنولوجي وتأثيره على أنواع القوى: الصلبة والناعمة والذكية، بوصفه مدخلاً لمعرفة تأثيره في الأمن القومي الأمريكي، ففي ضوء التطورات التكنولوجية السريعة. كان من الضروري المحافظة على قيم الأمة وحماية الدولة والإقتصاد والسكان والثقافة إذ لا يمكن إنكار أهمية التكنولوجيا في تعزيز الأمن القومي وذلك يتطلب إتخاذ إجراءات قانونية وإدارية وعسكرية وأمنية للحماية من التهديدات والمخاطر القائمة والمحتملة. فضلاً عن، حماية البنية التحتية للإتصالات والمعلومات. وعليه تسهم القوة الذكية في جعل (الأمن السيبراني) مفهوماً إستراتيجياً، يهدف إلى حماية كيان الدولة وتعزيز قوتها. ومن جهة ثانية فقد ركزت أبحاث العلاقات الدولية في مجالي الدراسات الأمنية والإستراتيجية على تقييم تأثير التكنولوجيا على الأمن الدولي عموماً، والقومي خصوصاً، لما لها من دور أساس في تعزيز القوة والسيادة الوطنية [١]. لقد وصف فيه (جوزيف ناي) [*] الأمن القومي «بأنه الحفاظ على القيم العليا للأمة متمثلةً بأمن وسيادة الدولة وإقتصاديها وسكانها وثقافتها من الخطر والدمار [٢]، والذي يُعبر عنه بكل التصرفات التي يسعى المجتمع عن طريقها

---

(١) إبراهيم محمد الحمامصة، فارس العمارات، الامن السيبراني: المفهوم و تحديات العصر، (دار الخليج للتوزيع و النشر، الأردن، الطبعة الأولى:)٢٠٢٢، ص ٢٠.

(*) جوزيف ناي: مساعد وزير الدفاع الأمريكي للشؤون الأمنية الدولية في حكومة بل كلينتون، ورئيس مجلس الاستخبارات الوطني الأمريكي.

(٢) فرح يحيى زعاترة، التهديدات السيبرانية على الامن القومي الأمريكي، القاهرة، (العربي للنشر والتوزيع:)٢٠٢٣، ص٣٠

إلى حفظ حقه في البقاء، عبر صوّن الوجود أمام إي تهديد بالفناء حسب رؤية وزير الخارجية الأسبق (هنري كيسنجر) [١]. إن التطور التكنولوجي يعزز من صياغة الأمن القومي بشكل كبير في سياق الإجراءات القانونية والإدارية والعسكرية والأمنية التي تهدف إلى حماية البلاد من التهديدات والمخاطر المحتملة، بما في ذلك حماية البنية التحتية للإتصالات والمعلومات [٢]. مما يعني تنامي الإلمام بشبكة المعلومات الدولية (الإنترنت) وعَدّها عاملاً ومُحركاً مهماً في إحداث التغييرات في قواعد القوة الدولية [٣].

فمع الإنتقال إلى ما يُعرف بـ (مجتمع المعرفة) أو (عصر التقنية)، يشهد العالم اليوم تحولاً كبيراً، أصبحت فيه المعرفة العلمية وتطبيقات التكنولوجيا هي العامل الأساسي في إنتاج القيمة المضافة على المستوى العالمي. و عليه، بات من الصعب على أي بلد أن يكون قوياً عسكرياً وإقتصادياً بدون الإعتماد على إنتاج وتوظيف المعرفة و التكنولوجيا في مجالات الحياة المختلفة [٤]. وعليه فأنّ مصادر قوة الدولة وأشكالها تتغير باستمرار فمفهوم (القوة الصلبة) التي تستدعي إستخدام الوسائل العسكرية لتحقيق الأهداف السياسية كان يُنظر إليها على أنها أحد العناصر الأساسية للتفوق، ومع تزايد الإهتمام بالأبعاد غير المادية للقوة حلت حيازة (القوة الناعمة) التي تعتمد على مدى تأثير الدولة على الدول الأخرى في المجتمع الدولي بالجذب والاقناع محلها [٥] فهي تعتمد على نشر الثقافة والقيم السياسية الى الدول الاخرى لتحقيق التفاعل المثمر بين الثقافات المختلفة [٦].

فغالباً ما يُقاس التقدم في التكنولوجيا العسكرية اليوم بعدة عوامل، هي:

١- مدى إبعاد أفراد الخدمة العسكرية عن منطقة الصراع.

٢- القدرة على تعزيز القوة وفرض هيمنها، بدون الإصطدام المباشر.

٣- إمكانية تقليل التكاليف خلال مدة الحرب [٧].

---

(١) المصدر نفسه، ص ٢٩.

(٢) حسام محمد نبيل عبد الرؤوف مرسي، الامن السيبراني (ضرورته - متطلبات تحقيقه)، مجلة كلية الدراسات العليا، مصر، العدد ٣٤، ٢٠١٦، ص ٣٤٧.

(٣) إبراهيم محمد الحمامصة، د. فارس العمارات، الامن السيبراني، مصدر سبق ذِكره، ص ٢٠.

(٤) صفاء حسين علي، استراتيجية القوة الذكية وأثرها في السياسة الخارجية الصينية، (مجلة الجامعة العراقية، بغداد، العدد :٤٧)٢٠٢٠، ص ٣٦٤

(٥) المصدر نفسه، ص ٣٦١.

(٦) المصدر نفسه، ص ٣٦٧.

(٧) مصطفى شلش، سباق الجيل السادس بين الولايات المتحدة و الصين: إستخدامات الذكاء الإصطناعي العسكري، (مركز الدراسات العربية الأوراسية، القاهرة: ٢٠٢٣)، ص ٥.

لقد قللت (القوة الناعمة) الولايات المتحدة الأمريكية من التكاليف الباهظة التي عند استخدام (القوة الصلبة) بشكل مباشر وظهرت (القوة الناعمة) كبديل جوهري يُمكّن من حصول الدولة على ما تريده عبر توظيف ثورة التكنولوجيا و المعلوماتية، ووسائل التواصل الإجتماعي على شبكة الإنترنت لكسب عقول الكثير من الشباب في مجتمعات الرفض و الممانعة[1]. لقد أختلفت الأولويات السياسية فاصبحت معظم الدول تخشى من تعرض أمنها القومي إلى الخطر جَرّاء الإعتداءآت إلالكترونية، لاسيما أن تقنية المعلومات والإتصالات باتت متطورة بظهور وسائل التواصل الاجتماعي (فيسبوك، أنستغرام، منصة أكس) و غيرها الأمر الذي أدى إلى ظهور تحديات ومخاطر جديدة مثل : نشر الأخبار المزيفة، و الدعاية في الإتصالات الرقمية، و الإستخدامات الناشئة لمنصات التواصل الاجتماعي بوصفها أسلحة، بدلاً من كونها جسور تطرح أسئلةجدية بغية إيجاد الحلول، و التي شكلت بدورها تحدياً للتركيز على الأساليب الناعمة [٢].

ظهرت (القوة الذكية) بوصفها مصطلحاً يجمع بين (القوة الصلبة) و (القوة الناعمة)، وهي أكثر فاعلية منهما بشكل منفصل وجاءت بوصفها ردة فعل داخلية من المؤسسات السياسية الأمريكية، تهدف إلى تغيير المسار الإستراتيجي، عبر التأثير على الآخرين للحفاظ على الأمن القومي الأمريكي [٣]. أن كثافة المعلومات وتشابكها خلقت مناخاً مختلفاً وأعطت معنى أوسع وأشمل للإستراتيجية الأمنية عن طريق المزاوجة بين القوتين: الصلبة والناعمة في معالجة الأحداث والتطورات الدولية، مما أدى إلى تراجع إستخدام الجانب العسكري (القوة الصلبة) لصالح استخدام (القوة الذكية)، لفرض السيطرة في حروب الشبكات، والحروب الإلكترونية [٤]. إن إعادة الهيكلة تستلزم تعديلات عملياتية وتكتيكية في إدارة الصراعات، عن طريق إدارة شؤون الدفاع بواسطة مقاربة جديدة و مغايرة لا تستلزم الأسلحة و لا الجنود المدربين على إطلاق النار، بقدر ما تتطلب توظيف التكنولوجيا، والأدوات الرقمية، ومعالجة

(1) Luigi Di Martino , Fear and empathy in international relations: Diplomacy, cyber engagement and Australian foreign policy ,)Place Branding and Public Diplomacy , Volume 20, Issue 1: 2024(. p p 14-.

(٢) حسام محمد نبيل عبد الرؤوف مرسي، الامن السيبراني (ضرورته - متطلبات تحقيقه)، (مجلة كلية الدراسات العليا، العدد ٣٤، مصر: ٢٠١٦)، ص ٣٤٥.

(٣) سيف الهرمزي، مقتربات الذكية الأمريكية كآلية من آليات التغيير الدولي : الولايات المتحدة الأمريكية أنموذجاً، (المركز العربي للأبحاث ودراسة السياسات، الدوحة: ٢٠١٦)، ص ٥٨.

(٤) صفاء حسين علي، استراتيجية القوة الذكية وأثرها في السياسة الخارجية الصينية، مصدر سبق ذِكره، ص ٣٦٨.

و تسويق المعلومات [١]، و لما كانت (القوة الذكية) لها الدور الفعّال في مواجهة تلك التحديات الأمنية التي لا يمكن تجاهلها وفي ظل إمتلاك الولايات المتحدة الأمريكية تفوقاً عالمياً فضلاً عن الخبرة التراكمية المتعلقة بالتقنيات المتطورة في المجالات كافة وفي مقدمتها لتقنيات المُتطورة في مجال المعلومات و الاتصالات لذا أصبحت تضع الاستراتيجيات للرد على محاولات تهديد وإختراق للأمن القومي الأمريكي فظهر ما يُعرف بمفهوم(الأمن السيبراني) [٢]. بدأ إهتمام الولايات المتحدة الأمريكية بمجال الفضاء الإلكتروني منذ عام (١٩٩٣) إذ إفتتحت «مركز الحروب المعلوماتية التابع للقوات الجوية» وكانت عمليات الدفاع والهجوم أنذاك تتم تحت قيادة «وحدة الحرب المعلوماتية رقم ٦٠٩ "، إلا إن دورها ظل مقتصراً على التنسيق مع وزارة الدفاع الأميريكية (البنتاجون)، وتقديم الإقتراحات له دون القدرة على شن هجمات أو حملات دفاع في المجال الإلكتروني[٤].

- **المطلب الثاني: الأمن السيبراني في المدرك الإستراتيجي الأمريكي**

بدأت الإدارة الأمريكية في تطوير مفهوم السيبرانية في عهد الرئيس الأمريكي الأسبق بيل كلينتون عام (١٩٩٨) وتم الإشارة له في وثائق الأمن القومي للعامين (٢٠٠٠) و (٢٠٠١) بوصفه تهديدات إلكترونية للبنى التحتية الأمريكية الحيوية. الأمر الذي يفرض حماية الهياكل الأساسية الوطنية الحساسة. وعليه، أنشأت وزارة الدفاع الأمريكية (البنتاجون) قوة للدفاع عن شبكات الحاسوب المشتركة (JTF-CND)، وأعطت مسؤولية الهجوم إلى "وكالة الأمن القومي" ومهمة الدفاع إلى "وكالة الدفاع عن أنظمة المعلومات" اللتان إجتمعتا تحت مظلة "القيادة الإلكترونية الأمريكية" في العام (٢٠٠٩) التي قادها مدير وكالة الأمن القومي آنذاك؛ نظرا لتمتعها بإمكانات كبيرة في مجال تكنولوجيا المعلومات، والإتصالات التي تميزت بإمكانية تجسسها على دول مختلفة حول العالم [٣]. إن الولايات المتحدة الأمريكية بوصفها القوة المهيمنة عالمياً لا تستطيع الإحتفاظ بتلك المكانة إلا عبر إستراتيجية شاملة مرتكزة على أدوات ووسائل هدفها التوسع والسيطرة عبر الإهتمام بتجميع المعلومات و تحليلها وإمتلاك العقلية الشمولية للنظر إلى الأمور من الزوايا كافة وكذلك الرؤية المستقبلية و التنبؤ بأحداث

(١) عامر مصباح، الفضاء السيبراني نموذج لتوسيع عقيدة الدفاع الإستراتيجي، كلية العلوم السياسية والعلاقات الدولية، مجلة دراسات الدفاع و الإستشراف : دراسة ستراتيجيا، (الجزائر العدد ١٦ السداسي الثاني: ٢٠٢١)، ص. ٣٨.

(٢) منعم صاحي العامر، من يدين لمن ؟ مكانة الاستخبارات في الاستراتيجية الأمريكية الشاملة، (بغداد، مكتبة الغفران للخدمات الطباعية: ٢٠١٢)، ص ٧٠

(٣) المصدر نفسه، ص ١٣٩.

المستقبل و الإرتكاز على المبادئ و القيم في العمل لإتخاذ المواقف الملائمة والحصول على رؤية عميقة ذات بُعد إستراتيجي طويل الأمد [١] وهو ما بلور الإهتمام بمفهوم (الأمن السيبراني) و تعريفه ضمن الجانب الإستراتيجي. فقد رأى (جوزيف ناي) أن تلك القوة (الذكية) ترتبط بإمتلاك المعرفة التامة بالتكنولوجيا والقدرة على إستخدامها فأضحى (الأمن السيبراني)[*] مجالاً حيوياً تهتم به الحكومات والشركات و حتى الأفراد ؛ لحماية بياناتهم ومعلوماتهم الحساسة من التهديدات الإلكترونية [٢].

إن الولايات المتحدة الأمريكية بوصفها القوة المهيمنة عالمياً لا تستطيع الإحتفاظ بتلك المكانة إلا عبر إستراتيجية شاملة مرتكزة على أدوات ووسائل هدفها التوسع والسيطرة

إن الأمن السيبراني هو سلاح إستراتيجي لا يمكن الإستغناء عنه في التكتيكات و الهجمات ما بين الدول[٣].فمفهوم (الأمن السيبراني) كما يذهب (ناي) يرتكز في قوته على مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسوب ومعلومات والشبكات إلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه المسائل. الأمر الذي يفرض وجود بُنية تحتيه سيبرانية تشمل: أجهزة الحاسوب لمختلف الأنظمة و القطاعات تعمل ضمن إستراتيجية واضحة الأهداف،

---

(١) فرح يحيى زعاترة، التهديدات السيبرانية على الامن القومي الأمريكي، (القاهرة، العربي للنشر و التوزيع: ٢٠٢٣)، ص٢٤.

(*) إن الأمن السيبراني: لغوياً: يتكون من مفردتين إثنتين (الأمن) و (السيبراني)، فالأمن نقيض الخوف، و بمعنى السلامة. و الأمن هو مصدر الفعل (أمِنَ)، (أمْناً)، (أماناً). ويُقال (أمَنَةً) أي بمعنى الإطمئنان وسكون القلب والراحة وذهاب الخوف. أما مفردة (السيبراني) فهي مفردة غير عربية مشتقة من كلمة (cyber) اليونانية الأصل، والتي أُشتقت في الأصل من كلمة (kybernetes) التي تعني الشخص المُتحكم بالأمور، والقائد المسؤول عن دفة السفينة، يُرجع أصلها آخرون إلى عالم الرياضيات الأمريكي (نوربرت وينرز) الذي عَبر عنها بالتحكم الآلي. **(يُنظر: منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، (مجلة كلية التربية، جامعة المنصورة، القاهرة: ٢٠٢٠)، العدد ١١١، ص ٩).** في حين عرّف قاموس (أوكسفورد) الأمن السيبراني لغوياً: حالة الأمان من الجريمة الإلكترونية، والإجراءات المتخذة لتنفيذ ذلك. أما موسوعة (إنفستوبيديا) عرّفت الأمن السيبراني لغوياً: كل التدابير المتخذة لحماية المعلومات الإلكترونية من التلف والسرقة، كما ويُشار إلى الأمن السيبراني يعدم إساءة إستخدام الأجهزة والبيانات، من حماية المعلومات الشخصية إلى الأنظمة الحكومية المعقدة. (يُنظر: فاطمة علي إبراهيم، رحاب يوسف، وليد محمود السيد، الأمن السيبراني والنظافة الرقمية، (المجلة المصرية لعلوم المعلومات، جامعة بني سويف، القاهرة، مجلد ٩، العدد ٤: ٢٠٢٢)، ص ص ٣٩٦ -٣٩٧).

(٢) محمد قاسم هادي، مكانة القوة في الفكر الاستراتيجي الأمريكي، جامعة بغداد، (كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٥٤: ٢٠١٨)، ص ص ٣٧٦ – ٣٧٨

(٣) علي محمد أمنيف، تحديات الأمن في الفضاء السيبراني الأمريكي، مجلة دراسات دولية، (مركز الدراسات الاستراتيجية والدولية، جامعة بغداد ، العدد ٨٥: ٢٠٢١)،ص ٢٩٥.

تحدد طرق العمل و الأهداف المرجوة[١].ترى الولايات المتحدة الامريكية أن شبكة المعلومات الدولية (الإنترنت) قد رفعت مستوى الأخطار في النظام الدولي بشكل غير مسبوق مما يُعرّض أمنها القومي إلى تهديدات جدية تطال مجالات أساسية وحيوية، ما جعل الأمن السيبراني في مقدمة إهتماماتها الأمنية، إذ تم تعريفه في عهد الرئيس الأمريكي الأسبق (باراك أوباما) « بأنه قدرة النظام المعلوماتي على مقاومة محاولات الإختراق التي تستهدف البيانات» [٢]. أما وزارة الدفاع الأميريكية فقد عرّفت (الأمن السيبراني) بأنه «جميع الإجراءات التنظيمية اللازمة، لضمان حماية المعلومات بجميع أشكالها الإلكترونية، و المادية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث»[٣]، وعرّفت الفضاء السيبراني بأنه: «مجال يتسم بإستخدام الإلكترونيات (أي تكنولوجيا المعلومات) والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الإتصال و البنية التحتية المادية المرتبطة بها « [٤]. أما تأثير الفضاء السيبراني على الجيوبوليتيك، فيمكن رصد تناقص أهمية العوامل المادية مثل: الأرض و رأس المال والسلع قياساً بأهمية المال والمعرفة و أهمية التوسع في السوق، بدلاً من التركيز على الإحتلال الأرضي[٥]. لقد أصبحت البيئة السيبرانية عالماً يشمل: جميع أنظمة المعلومات ومستخدميها[٦]. وعلى الرغم من إن (الأمن السيبراني) وفضاءه خاص بالولايات المتحدة الأمريكية، التي تحتفظ بالمِلكية الحصرية للقاعدة المعلوماتية والأنظمة المعقدة في التخزين والتشغيل والتوزيع لكل الخدمات المتوفرة بواسطة شركاتها السيبرانية العملاقة، لكن قرارها بفتح هذا الفضاء للمساهمة العالمية وتحويله إلى فضاء مشترك بين الدول للإستخدام والتطوير حوّله إلى ميدان حيوي للمنافسة الإستراتيجية وليس مجرد فضاء لإنتاج الخدمات السريعة

(١) مهوب وسام، نموذج الولايات المتحدة الأمريكية في مجال الأمن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع، مجلة البيبان للدراسات القانونية والسياسية، جامعة برج بوعريريج، (الجزائر، المجلد ٨٠ العدد ٢: ٢٠٢٣)، ص ص ١٢٢-١٢٣.

(٢) إبراهيم محمد الحمامصة، فارس العمارات، الامن السيبراني: المفهوم وتحديات العصر، مصدر سبق ذِكره، ص ٢٠.

(٣) صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، (كلية العلوم السياسية، جامعة النهرين: ٢٠٢٠، العدد ٦٢)، ص ٢٧٦.

(٤) شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، (مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر، المجلد ١٥، العدد: ١: ٢٠٢٢)، ص ٢٩٤.

(٥) نور علي صكب، الأمن الوطني العراقي في ظل الإختراق السيبراني (أمن المعلومات)، (مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، بغداد، العدد ١١: ٢٠٢١)، ص ١٠.

(6) Albalas, T., Modjtahedi, A., Abdi, R. (Cyber security governance: a scoping review, International journal of professional business review ,) Miami , v. 7 , n. 4 : 2022 (, p. 4.

وتدفق الأرباح التجارية [١]. وهذا ما يُشكل تهديداً لأمن الولايات المتحدة الإمريكية السيبراني؛ جَراء إمكانية الكيانات المدنية أو العسكرية أو الإرهابية من إستخدام تكنولوجيا المعلومات في الفضاء السيبراني لضرب أهداف إستراتيجية وحيوية[٢]. لقد إعتبرت جامعة هارفرد الفضاء السيبراني (الذراع الرابعة للجيوش الحديثة) فظهور الإنترنت وإقبال الدول على إستخدامه في المجال الأمني والعسكري لتحقيق قفزات نوعية في المجالات الأمنية والسياسية جعلت العلماء عموماً يهتمون بدراسة التطور التكنولوجي وآثاره على السياسة، ومع هذا التطور جاء الحديث عن (الأمن السيبراني) الذي يهتم بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية، التي تستهدف عادة الوصول للمعلومات الحساسة أو تغييرها أو إتلافها [٣]. و عليه فإن أكبر قاعدة للعالم السيبراني مشيدة في مواقع التخزين و التوزيع العملاقة للمعلومات تقع في الولايات المتحدة الأمريكية، و عليه تبقى الأصول المطوّرة في هذا الصدد تحت السيطرة الأمريكية بطريقة ما، لكن على الرغم من ذلك يبقى التهديد قائماً، خصوصاً إن هناك الكثير من الدول تسعى لتطوير قوة سيبرانية مستقلة خاصة بها للتحرر من الهيمنة السيبرانية الأمريكية إلا في حدود قواعد الاتصال الدولي، والإتجاه نحو ما يُعرف بـ (بالسيادة السيبرانية الوطنية) أو (الإستقلال السيبراني الوطني) و الذي يُعرَف حالياً بشكل أدق بـ (السيادة الرقمية للدولة)[*]. تمثل السيادة السيبرانية الوطنية الحق المطلق في إستخدام البنية التحتية والكيانات والإجراءات والبيانات والمعلومات ذات الصلة داخل أراضي الدولة. وبالتالي التحرر من الهيمنة والسيطرة والإنكشاف الإستخباري أمام الدول الاخرى التي تسعى بدورها إلى تطوير تطبيقاتها الدفاعية لإحباط أي محاولات للوصول إلى المعلومات الحساسة الخاصة بأمنها القومي أو التي تستهدف

(١) عامر مصباح، الفضاء السيبراني نموذج لتوسيع عقيدة الدفاع الإستراتيجي، مصدر سبق ذِكره، ص ص. ٤١ - ٤٢

(٢) شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مصدر سبق ذِكره، ص ٢٩٤.

(٣) هبة جمال الدين: الأمن السيبراني والتحول في النظام الدولي، جامعة القاهرة، مصر، مجلة كلية الإقتصاد والعلوم السياسية، (المجلد ٢٤، العدد الأول: ٢٠٢٣)، ص ص - ١٩١-١٩٠

(*) إن السيادة بالمفهوم الحالي من الناحية القانونية يشير إلى قدرة الدولة على إتخاذ قراراتها من جهة، والسماح لمواطنيها بممارسة حقوقهم الأساسية من جهة ثانية. و مع التطور الحاصل في المجال السيبراني أصبح مصطلح السيادة الرقمية الأكثر شيوعاً والذي يُعرف « قدرة الدولة في إدارة بنيتها التحتية، و معلوماتها و بياناتها، بهدف تطوير رؤية وطنية متميزة للإنترنيت «. يُنظر:

Maleh Yassine, Youness Yassine, Cyber Sovereignty in Morocco, Springer Briefs in Cyber security,) Switzerland: 2022(, p 78

بنيتها التحتية منعاً لتهديد مصالحها من جهة أخرى [١].

إن أبرز الأهداف الإلكترونية التي يتم إستهدافها في الجغرافية الأمريكية هي:

أولاً: على المستوى الاتحادي: البيت الأبيض والكونغرس الأمريكي ووزارة الداخلية، كونها من رموز الأمن القومي الأميركي.

ثانياً: على المستوى العسكري: يتم إستهداف وزارة الدفاع والوحدات القتالية القيادية، لعرقلة العمليات العسكرية.

ثالثاً: على المستوى المدني: إستهداف البنى التحتية، فضلاً عن المؤسسات المالية ومحطات الطاقة والكهرباء، الأمر الذي يضع الشعب الأمريكي تحت طائلة أخطر الأهداف، لأنها لا تقتصر على الإستخدامات المدنية فحسب بل العسكرية كذلك، وتهدد المصالح الحيوية المختلفة. بالتالي تُعد بُنى حرجة للولايات المتحدة الأمريكية، لأنها تتضمن النظم والأصول سواء كانت المادية أو الإفتراضية التي يؤدي تدميرها أو التلاعب بها إلى تهديد الأمن والاقتصاد الأمريكي والرعاية الصحية[٢].

إن الجانب الإستراتيجي لمفهوم (الأمن السيبراني) صُنِفَ من ضمن الأولويات في السياسات الدفاعية للولايات المتحدة الإمريكية إذ تستطيع أي دولة أو أي محترف أن يستغل أي ثغرة في أي منظومة إلكترونية في دولة ما، بتوجيه هجمات إلى أي مكان في العالم وهو ما قد يتسبب بفقدان المعلومات الحيوية أو خسائر فادحة وتعطل للحياة اليومية [٣]. وعليه، صَنفت المؤسسة العسكرية الأمريكية (الأمن السيبراني) إلى قسمين رئيسين هما: الدفاع الإلكتروني ويشمل:

التعرف على أي نشاط سيبراني عدواني، والكشف عن هوية الأطراف التي تقوم بهذا النشاط، والتدخل لمنعه وإعاقته بنجاح. أما القسم الثاني فهو الهجوم الإلكتروني الذي يشمل: جميع العمليات التي تهدف إلى تدمير أو تعطيل الإمكانيات السيبرانية لأي دولة معادية للولايات المتحدة الأمريكية أو أي من حلفائها، فضلاً عن جمع المعلومات من أجهزة الحاسوب

---

(1) Lidia Tri Chris Nia Wati, Mahmud Syaltout Syahidullhaq Qudratullah , Bimantoro Kushari Parmono ,Comparative Analysis of Cyber Sovereignty: Case from Indonesia and Iran , JuSS: Jurnal Sosial Soedirman , Universitas Paramadina ,) Indonesia ,Vol.6, No. 1: 2023 , p. 30.

(٢) هبة جمال ا(لدين : الأمن السيبراني والتحول في النظام الدولي، مصدر سبق ذِكره، ص ص. ١٩٠ -١٩١.

(٣) علي ادهم، الامن السيبراني Cyber Security الجزء الاول ، مركز النهرين للدراسات الاستراتيجية، مستشارية الامن القومي، بغداد، ٢٠١٩ https://alnahrain.iq/post/٣٨٢ .

والأنظمة والشبكات المعلوماتية، وإجراء تعديلات أو تعطيلها أو تدميرها [١].

- **المطلب الثالث: مرتكزات الأمن السيبراني في الإستراتيجية الأمريكية**

ترتكز الإستراتيجية الأمريكية للأمن السيبراني على ثلاثة عناصر أساسية تشكل الإطار العام لحماية الفضاء السيبراني الأمريكي وتعزيز الردع ضد التهديدات الإلكترونية، وهي:

١- **القوة السيبرانية:** وهي القدرة على إستخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، للحصول على النتائج المرجوة حسب نظرة (جوزيف ناي) [٢].

٢- **الدفاع السيبراني:** مجموعة الإجراءات الأمنية الدفاعية التي تهدف إلى حماية الأنظمة والشبكات الحاسوبية من الهجمات السيبرانية [٣]، ويتم التركيز في هذا السياق على توفير إستجابة فورية للتهديدات السيبرانية بهدف منع إختراق البنية التحتية وسرقة المعلومات [٤]. مما يعني إن الركائز التي تستند عليها إستراتيجية الدفاع السيبراني هي: مصداقية الدفاع أولاً، والقدرة على الردع ثانياً، والرغبة في الردع ثالثاً [٥].

٣- **الردع السيبراني:** يُعرف الردع السيبراني " بمنع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني، والأصول التي تدعم العمليات الفضائية " [٦]. ويتم تحقيق ذلك من خلال التحليل التكتيكي والإستراتيجي للسيناريوهات السيبرانية المحتملة وتجارب المحاكاة. علاوة على ذلك، يتعين تطوير تصور رقمي ضخم يعكس الهيمنة الأمريكية في الفضاء السيبراني [٧].

وبذلك فإن الرؤية الإستراتيجية الحديثة القائمة على مواجهة عمليات الإختراق الإلكتروني تعكس الإدراك لدى أعلى المستويات في السلطة الأمريكية بضرورة التصدي للهجمات إلكترونية

(١) يونس مؤيد يونس مصطفى، إستراتيجية الولايات المتحدة الأمريكية للأمن السيبراني، (جامعة النهرين، كلية العلوم السياسية، بغداد، العدد ٥٥: ٢٠١٨)، ص ص ١٣٨ - ١٣٩.

(٢) نهي علي أمير، الأمن السيبراني في إستراتيجية الامن القومي الروسي، آفاق آسيوية، الهيئة العامة للإستعلامات، (جمهورية مصر العربية، العدد ١١: ٢٠٢٣)، ص ص. ١٧٣- ١٧٤ .

(٣) المصدر نفسه، ص ١٧٤.

(٤) كرار عباس متعب فرج، الحرب السيبرانية: دراسة في إستراتيجية الهجمات السيبرانية بين الولايات المتحدة الإمريكية وإيران، (مجلة حمورابي للدراسات، بغداد: العدد ٤٠، ٢٠٢١)، ص ٢٠٢.

(٥) علاء الدين فرحات، من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، (مجلة المفكر، جامعة الجيلالي بونعامة خميس مليانة، الجزائر، المجلد ١٦، العدد: ١: ٢٠٢١)، ص ٢٧٢.

(٦) المصدر نفسه، ص ٢٧٢.

(٧) المصدر نفسه، ص ص ٢٠٢ – ٢٠٣.

المتزايدة، ويقتضي عدم الإقتصار على الدفاع فحسب، بل وتجاوزه بالتصدي والهجوم يكون ضرورياً كذلك، حسب رؤية وزارة الدفاع الإمريكية (البنتاجون) [١]. وبالتالي، يُعد (الأمن السيبراني) جزءاً أساسياً من الإستراتيجية الدفاعية للولايات المتحدة الأمريكية. التي تلعب دوراً قوياً على الصعيد الدولي مما يتعين علها أن تتبنى إستراتيجيات شاملة تهدف إلى التصدي لهذه التحديات وضمان الأمن القومي الامريكي.

المبحث الثاني

إستر اتيجية الرئيس الإمريكي جوزيف بايدن للأمن السيبر اني

- **المطلب الأول:الأمن السيبر اني من منظور إدارة الرئيس بايدن**

حرصت إدارة الرئيس الأمريكي جو بايدن بجدية على التركيز على مسألة الأمن السيبراني من خلال إعتماد "الإستراتيجية الوطنية للأمن السيبراني". الذي جعلتها الإدارة الأولى من نوعها في الولايات المتحدة الأمريكية بعد إدارتي أوباما وترامب التي تدرك بشكل كبير مدى أهمية الأمن السيبراني، وتعمل على توحيد سياساته مع إستراتيجية الأمن القومي المتمثلة بـ: تعزيز الدفاعات السيبرانية للبنية التحتية الحيوية من جانب، وتعزيز اللوائح التنظيمية لضمان الحد الأدنى من معايير الأمن السيبراني من جانب ثاني، ومكافحة الهجمات الإلكترونية التي ترعاها دول أجنبية من جانب ثالث [٢].

ولدراسة التطورات التي أحدثتها إدارة بايدن في مقاربتها للوضع الحالي، يتعين علينا أن نسلط الضوء على الإستراتيجية الأمريكية للأمن السيبراني التي تبنتها إدارتي أوباما وترامب أولاً.

إذ سعت إدارة الرئيس الأميركي الأسبق براك أوباما إلى إتخاذ إستراتيجية وقائية مبنية على مجموعة من الإجراءات الإحترازية؛ جراء الزيادة في الهجمات السيبرانية والتي تمثلت بـ:

١. تعزيز الإطار التشريعي والقانوني بإصدار قانون خاص لمكافحة الإرهاب على الإنترنت عُرف بإسم «قانون حماية الشبكات السيبرانية».
٢. تفعيل دور مركز الإتصالات الإستراتيجي لمكافحة الإرهاب التابع لوزارة الخارجية، الذي يعمل فيه متخصصون لنشر مواد معادية للإرهاب.
٣. إطلاق مشروع مخصص لمكافحة الهجمات الإرهابية السيبرانية، ومحاولات التجنيد

(١) بلموهوب رياض، قدوج نور الدين، الردع الإلكتروني كآلية لمواجهة الحروب السيبرانية، كلية الحقوق والعلوم السياسية، (جامعة محمد بشير الإبراهيمي، الجزائر، رسالة ماجستير منشورة: ٢٠٢٣)، ص ٥٤.

(2) Vivek Mishra and Sameer Pati , Decoding the Biden Administration's Cyber Security Policy , Observer Research Foundation ,) New Delhi , 2024 : ISSUE NO. 686(, p 15.

عبر الإنترنت عبر بث منشورات مضادة للإرهاب، وإستهداف حسابات الإرهابيين عبر الوسائط الإلكترونية.

٤. إنشاء قواعد التعاون المشتركة دولياً، بإطلاق مبادرات مثل: مبادرة محاربة الإرهاب الإعلامي مع الدول الحليفة، أو عن طريق تفعيل تبادل المعلومات بين أجهزة طوارئ الإنترنت، فضلاً عن إنشاء خلايا مشتركة لرصد التهديدات السيبرانية.

٥. إنشاء جهاز للتجسس يقوم بمراقبة مواقع التواصل الاجتماعي، وتتبع الأنشطة المنشورة من الجهات المعادية [١].

- **المطلب الثاني: الأمن السيبراني من منظور إدارة الرئيس دونالد ترامب (الولاية الأولى)**

لقد تولى الرئيس الأمريكي السابق دونالد ترامب منصبه بعد إجراء إنتخابات تأثرت بتدخل سيبراني من جهات أجنبية، وذلك في إطار عالمي يتسم بتراجع حرية الإنترنت [٢]. ومع تعرض النظام الأمريكي للتهديد السيبراني فقد واجهت إدارة ترامب تحدياً لم يسبق له مثيل[٣].

ففي العام (٢٠١٨) أصدرت وزارة الدفاع الأمريكية (البنتاجون) إستراتيجية عُرفت بإسم "الدفاع للأمام" التي أعلن عنها و نفذها الجنرال (بول ناكاسوني) قائد القيادة السيبرانية الأمريكية وهي إستراتيجية إستباقية هجومية أشارت إلى أن القيادة السيبرانية الأميركية التابعة لوزارة الدفاع ستحافظ على تفوقها العالمي، من خلال وجود مستمر في الشبكات الخارجية المعادية حتى تتمكن من مواجهة خصومها سيبرانياً، إذ إستهدفت الإستراتيجية خمسة نقاط أساسية في مجال الأمن السيبراني[٤] :

١- تمكين قوات الأمن السيبراني الأميركية من تحقيق مهامها في بيئة الفضاء الإلكتروني، بتحويل القيادة السيبرانية إلى قيادة قتالية موحدة، لتنظيم الجهود وتعزيز التفاعل والتعاون بين الوحدات العسكرية في مجال السيبراني[٥].

---

(١) يونس مؤيد يونس مصطفى، إستراتيجية الولايات المتحدة الأمريكية للأمن السيبراني، مصدر سبق ذكره، ص ١٤٥.

(2) David P. Fidler , President Trump's Legacy on Cyberspace Policy , Council on Foreign Relations , 2020 ,
https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy

(3) Op cit.

(٤) محمد المنشاوي، كيف فشلت إستراتيجية «الدفاع للأمام» في حماية أميركا من الهجمات السيبرانية؟، شبكة الجزيرة الإعلامية، ٢٠٢٠، https://aja.me/umsfa .

(٥) المصدر نفسه ، ص ٢٠٧.

٢- دفع قدرات قوات الأمن السيبراني للقيام بعمليات تعزز من خلالها المزايا العسكرية الأميركية، إذ نفذت عمليات سيبرانية هجومية، إستهدفت خلالها قدرات روسيا على التدخل السيبراني خلال الإنتخابات الأمريكية لعام (٢٠١٨)، وقدرات إيران في عام (٢٠١٩) بالرد على إسقاطها طائرة أمريكية بدون طيار، ومهاجمتها لناقلات النفط أمريكية [١].

٣- الدفاع عن البنية التحتية الحيوية للولايات المتحدة من أي هجمات إلكترونية، عبر رفع قدرات الدفاع السيبراني القوية مثل: تعزيز قوة الحماية والإستجابة العاجلة في حالة وقوع هجمات سيبرانية محتملة [٢].

٤- تأمين معلومات وأنظمة وشبكات (البنتاجون) ضد أي هجمات سيبرانية. إذ قامت الإستراتيجة بدعم التشريعات التي توضح سلطة وزارة الدفاع فيما يتعلق بالعمليات السيبرانية العسكرية، بهدف توفير الإرشادات والضوابط اللازمة لتنفيذ هذه العمليات بطريقة قانونية وفعالة [٣].

٥- توسيع نطاق التعاون في مجال الأمن السيبراني مع الشركاء سواء في القطاع الخاص أو على المستوى الدولي[٤].

وعليه تلقت القيادة السيبرانية الأمريكية توجيهات إرساء عقيدة تتمحور حول العمليات الهجومية والردع، مع الإستمرار إلى حد كبير في التعاون بين القطاعين العام والخاص الذي كان محورياً للدفاع السيبراني.

وفي الفترة التي سبقت الإنتخابات الأمريكية لعامي (٢٠١٨) و(٢٠٢٠) وأثناءها، نفذت القيادة السيبرانية الأمريكية عشرات الهجمات لتهديد المصادر الروسية أو تعطيلها. ووصف المسؤولون الأمريكيون عمليات التسلل المتزايدة إلى الشبكة الكهربائية والبنية التحتية الروسية، بأنها جزء من مجموعة واسعة من العمليات السيبرانية السرية ضد إيران وأهداف أخرى. ووقع الرئيس الأمريكي ترامب مذكرة للأمن القومي تسمح بمزيد من الحرية في الهجمات السيبرانية [٥].

على الرغم من التطورات الحاصلة، **وُصف نهج الرئيس السابق ترامب، باللامركزي ذي الأولوية المنخفضة في التعامل مع قضايا الأمن السيبر اني الوطني**، خصوصاً مع تخوف كبار

(١) المصدر نفسه ، ص ٢٠٧.

(2) David P. Fidler, President Trump's Legacy on Cyberspace Policy, ibid.

(3) Op cit.

(4) Op cit.

(5) Jacob Shively, Cybersecurity Policy, Punctuated Equilibrium Theory, and the Biden Administration, ibid, p 5.

المسؤولين في الإدارة الأمريكية آنذاك من الإعلان الصادر في نهاية العام (٢٠٢٠) من شركة الأمن السيبراني (Fire eye) عن تمكن مجموعة قراصنة روس من إدخال تعليمات برمجية ضارة على تحديث برنامج (Orion) التابع لشركة (Solar winds) مما أدى إلى إختراق موقعي : وزارة الأمن الداخلي، و وزارة الدفاع على عكس إدارة الرئيس جوزيف بايدن، التي تحركت بسرعة فور توليه السلطة في كانون الثاني للعام (٢٠٢١) من خلال تكليف السلطة التنفيذية الداخلية بمراجعة التهديدات السيبرانية، و إعداد إستراتيجية تعزز الأولوية السيبرانية وتضعها في مقدمة الأولويات، بالمقارنة مع ما كانت عليه في إدارة ترامب [١].

- **المطلب الثالث: التحديات والتحولات الإستراتيجية السيبرانية لإدارة الرئيس جوزيف بايدن**

ورثت إدارة الرئيس الأمريكي بايدن تحديات كبيرة في مجال الأمن السيبراني، وفقاً لتقرير مكتب محاسبة الحكومة الأمريكية (GAO) لعام (٢٠٢١)، فشلت الحكومات السابقة في تنفيذ العديد من توصيات مكتب محاسبة الحكومة الأمريكية لعام (٢٠١٨)، بالإستجابة للتحديات الرئيسية للأمن السيبراني الأمر الذي جعل الأمن السيبراني أولوية قصوى لإدارة الرئيس الأمريكي بايدن، وذلك بالإستعداد للتصدي للهجمات السيبرانية التي تهدد الأمن القومي مباشرةً، عبر تحسين عمليات الدفاع والردع السيبرانية للجهات المعادية لها [٢]. وبالتالي شكلت هذه الإستراتيجية تحولاً في نهج الإدارة الأمريكية في تعاملاتها مع التهديدات السيبرانية، إذ إعترفت بالقصور في السياسات السابقة، وتصاعد خطورة التهديدات، والحاجة إلى نهج إستباقي وشامل وتعاوني للأمن السيبراني. خصوصاً مع غياب معايير ولوائح موحدة للأمن السيبراني في القطاعات ما يشكل تحدياً كبيراً في صياغة إستراتيجية شاملة. نظراً لأن التكنولوجيا تتغلغل في كل جانب من جوانب المجتمع الحديث، مما يعني أن معايير الصناعة المختلفة يمكن أن تجعل الأنظمة الحيوية والبيانات عرضة للخطر بشكل دائم. وتسعى إدارة الرئيس الأمريكي بايدن إلى معالجة هذه المشكلة من خلال تعزيز تطوير معايير الأمن السيبراني بتعزيز التعاون بين الوكالات الحكومية، وكيانات القطاع الخاص [٣]. ففي الوقت الذي جمدت

(1) Op cit, p.p 56-.

(٢) كرار عباس متعب فرج، الحرب السيبرانية: دراسة في إستراتيجية الهجمات السيبرانية بين الولايات المتحدة الإمريكية وإيران، مصدر سبق ذِكره، ص ٢٠٧.

(3) President Joseph Biden Jr., Interim National Security Strategic Guidance. ibid. P. 18,

فيه إدارة ترامب التوظيف الفيدرالي، والغت المناصب السيبرانية الرئيسة ما أدى إلى إضعاف الوضع العام للأمن السيبراني للحكومة الفيدرالية من جهة، وإحداث نُقط ضعف خطيرة في قدرة الحكومة الشاملة على إجراء عمليات أمن سيبراني فعالة من جهة أخرى [١]. إعادت إدارة الرئيس الأمريكي بايدن المركزية الإستراتيجية، وأعطت سياسة الأمن السيبراني أولوية ضمن الأمن القومي بشكل واضح. [٢]. لقد أنشأت إدارة الرئيس الأمريكي بايدن أيضاً منصب «كبير مسؤولي الذكاء الرقمي والإصطناعي» في وزارة الدفاع ورئيساً للتكنولوجيا في وكالة المخابرات المركزية. بوصفه مسؤولاً عن جميع البيانات والأعمال المتعلقة بالذكاء الإصطناعي التي يقودها مركز الذكاء الإصطناعي المشترك التابع لوزارة الدفاع، ومكتب كبير موظفي البيانات، والخدمة الرقمية للدفاع. وكذلك منصب «كبير مسؤولي التكنولوجيا الجديد» في وكالة المخابرات المركزية نتيجة لسلسلة من المراجعات الإستراتيجية بهدف إعادة هيكلة الوكالة لتضعها في أفضل وضع يمكنها من مواجهة تحديات الأمن القومي الحالية والمستقبلية [٣]. في آذار (٢٠٢١) أصدرت إدارة الرئيس الأمريكي بايدن الإستراتيجية المؤقتة الخاصة بالأمن السيبراني بعنوان «التوجيه الإستراتيجي المؤقت للأمن القومي» التي ركز فيها على الثورة الصناعية الرابعة في مجال الذكاء الإصطناعي [٤].

وبذلك يمكن ملاحظة الإختلافات في نهج الرئيس الأمريكي بايدن مقارنة مع إستراتيجية الرئيس الأمريكي السابق ترامب، ضمن عدة أصعدة رئيسة وكما في الجدول الآتي:

(1) Op cit.

(2) Vivek Mishra and Sameer Patil , Decoding the Biden Administration's Cyber Security Policy , ibid , p. 6.

(3) Aaron Clarke , Tom Klein , 2021 Year in Review: The Biden Administration's Efforts on Cyber security , ibid.

(٤) محسن محمد صالح، التقرير الاستراتيجي الفلسطيني ٢٠٢٠-٢٠٢١، (مركز الزيتونة للدراسات والاستشارات، بيروت: ٢٠٢٢)، ص ص ٤٢٠-٤٢١

إستراتيجية ترامب الوطنية السيبرانية للعام 2018	إرشادات بايدن المؤقتة للعام 2021
على صعيد الأولوية: إن حماية الأمن القومي الأميركي وتعزيز رخاء الشعب الأميركي هما على رأس أولويات الإدارة. و يُعد ضمان أمن الفضاء الإلكتروني أمرا أساسيا لكلاهما.	على صعيد الأولوية : سنجعل الأمن السيبراني أولوية قصوى، ونعزز قدرتنا و إستعدادنا ومرونتنا في الفضاء السيبراني باعتباره ضرورة حتمية في جميع الولايات الأمريكية.
على صعيد التعاون و الشراكات : سوف نتعاون مع القطاع الخاص و المجتمع المدني لفهم التقدم التكنولوجي وتزيز التفوق الامريكي في التقنيات الحديثة و ضمان إعتماد الممارسات الآمنة.	على صعيد التعاون و الشراكات : سنعمل معا لإدارة المخاطر و تقاسمها، وتشجع التعاون بين القطاع الخاص و الحكومة من أجل بناء بيئة آمنة على الإنترنت للشعب الأمريكي.
على صعيد الإستثمارات : ستقوم الحكومة الفيدرالية بتحديث الخطة الوطنية لأبحاث و تطوير أمن البنية التحتية الحيوية لمعالجة مخاطر الأمن السيبراني على البنية التحتية الحيوية. ستقوم الإدارات والوكالات بالتركيز على بناء نهج جديد للأمن السيبراني باستخدام التقنيات الناشئة، و تحسين تبادل المعلومات و إدارة المخاطر و بناء القدرة على التكيف مع الإضطرابات واسعة النطاق أو طويلة الأمد.	على صعيد الإستثمارات : سوف نقوم بتوسيع إستثماراتنا في البنية التحتية و الأشخاص الذين نحتاجهم للدفاع بشكل فعال عن الأمة ضد النشاط السيبراني المُضاد، وتوفير الفرص للأميركيين من خلفيات متنوعة بينما نقوم ببناء قاعدة كفاءات لا مثيل لها.
على صعيد الدولي : ستسعى الولايات المتحدة جاهدة لتحسين التعاون الدولي في التحقيق في الأنشطة السيبرانية عبر تطوير حلول للحواجز المحتملة أمام جمع الأدلة و مشاركتها، و النظر في تدابير بناء الثقة العملية للحد من مخاطر الصراع الناجم عن النشاط السيبراني.	على صعيد الدولي : سوف نجدد إلتزامنا بالمشاركة الدولية في القضايا السيبرانية، والعمل جنبا إلى جنب مع حلفائنا و شركائنا لدعم المعايير العالمية الحالية وصياغة معايير جديدة في الفضاء السيبراني.
على صعيد الردع : سنعمل على ردع الجهات السيبرانية المعادية من خلال فرض تكاليف عليها و على رُعاتها بالإستفادة من مجموعة من الأدوات، بما فيها الملاحقات القضائية، و العقوبات الاقتصادية، بوصفها جزء من إستراتيجية ردع أوسع [1].	على صعيد الردع: سنُحمّل الجهات الفاعلة المعادية المسؤولية عن الأنشطة السيبرانية أو التخريبية وسنرد بسرعة و بشكل متناسب على الهجمات السيبرانية، بفرض تكاليف باهظة من خلال الوسائل السيبرانية و غير السيبرانية [2].

(1) Herb Lin , How Biden's Cyber Strategy Echoes Trump's : Comparing the Biden administration's Interim National Security Strategic Guidance with Trump's National Cyber Strategy , The Lawfare Institute , 2021 ,
https://www.lawfaremedia.org/article/how-bidens-cyber-strategy-echoes-trumps

(2) president joseph R. Biden, Interim National Security Strategic Guidance, the white house, Washington, D.C. , march 2021 , www.whitehouse.gov.

لاحقاً، وبسبب هجوم الفدية [*]. الذي وقع يوم الخميس الموافق السادس من آيار للعام (٢٠٢١) على شركة خطوط الأنابيب الأمريكية كولونيال، أعلن الرئيس الأمريكي بايدن على أثرها حالة الطوارئ، و أصدر الأمر التنفيذي في ١٣ آيار بشأن تطوير الأمن السيبراني في الحكومة الفيدرالية، و الذي تضمن تنفيذ التركيز على العديد من الخطوات مثل تشفير البيانات أثناء عبورها وتحسين الجهود لتحديد و ردع و حماية و الرد على الحملات السيبرانية كما وشدد على أهمية القطاع الخاص الذي يجب أن يتكيف مع بيئة التهديدات المتغيرة بإستمرار وأيضاً تعزيز عمل الوكالات الفيدرالية عبر الإنتقال إلى الخدمات السحابية الآمنة، و مشاركة مقدمي الخدمات و المعلومات الحوادث و التهديدات السيبرانية المحتملة [١]. في تشرين الأول من العام (٢٠٢١)، أعلنت وكالة المخابرات المركزية الأمريكية (CIA) أيضاً عن إنشاء مركز المهام الصيني الجديد لأنه المجال الرئيسي للمنافسة بين الولايات المتحدة الأمريكية والصين [٢]. كما و أعلن وزير الخارجية (أنتوني بلينكن) عن إنشاء «مكتب الفضاء الإلكتروني والسياسة الرقمية» الذي سيعمل مع الحلفاء لمكافحة الهجمات السيبرانية الأجنبية، لدول مثل : الصين و روسيا [٣]. وقّع الرئيس بايدن «قانون إعادة تفويض الدفاع الوطني» للسنة المالية (٢٠٢٢)، والذي سمح بإنفاق (٧٧٠) مليار دولار على إستراتيجيتها السيبرانية الجديدة، وعَمِل «قانون إعادة تفويض الدفاع الوطني» على توسيع التعاون مع القطاع الخاص كذلك [**] وقامت سلطة تفويض الدفاع الوطني بتدوين وتوسيع برنامج الأمن السيبراني بمراقبة حركة المرور عبر الإنترنت بشكل إستباقي كما أنشأ مشروع القانون برامج للتعاون الطوعي بين القطاع

(*) هجوم الفدية على شركة خطوط الأنابيب كولونيال: تأسست في عام (١٩٦١)، وهي اليوم مالكة لأكبر نظام خطوط أنابيب للمنتجات النفطية المكررة في الولايات المتحدة، تعرضت لهجوم الفدية الذي يمكن تعريفه أنه «مجموعة برامج ضارة تستخدم لأغراض الإبتزاز الفيروسي الإلكتروني المشفر، ثم المطالبة بفدية مالية لفك التشفير «، تسبب ذلك بوقف إمدادات الوقود في الشرق الأمريكي لمدة ستة آيام متتالية، و دفع فدية قدرها (٤,٤ مليون دولار) للقراصنة للحصول على مفتاح فك التشفير. تعكس حادثة هجوم الفدية على شركة خطوط الأنابيب كولونيال أهمية تعزيز الأمن السيبراني، وتوفير الحماية للبنى التحتية الحيوية في الولايات المتحدة. يُنظر: مات أولوني، خطوط الأنابيب كولونيال: تجاوز دعوات و أفكار برامج الفدية الضارة، من: الدفاع ضد التهديدات الخطيرة: تحليل توجهات الحوادث الرئيسية، شركة ساسكو،(كاليفورنيا: ٢٠٢٢)، ص ص ٤ -٧.

(1) Gisela Grieger , The US cybersecurity posture under Biden , EPRS | European Parliamentary Research Service , European Union, 2023 , https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)753929.

(2) Aaron Clarke , Tom Klein , 2021 Year in Review: The Biden Administration's Efforts on Cyber security , ibid.

(3) Op cit.

الخاص والقيادة السيبرانية الأمريكية في مكافحة الهجمات السيبرانية [١].

كما وقّع الرئيس بايدن اعام ٢٠٢٢ على «قانون الإبلاغ عن الحوادث السيبرانية للبنية التحتية الحيوية» (CIRCIA) الذي كان إصداره بمثابة علامة فارقة مهمة في تحسين الأمن السيبراني في الولايات المتحدة الأمريكية؛ لما توفره من حماية كبيرة للشركات التي تُبلغّ عن الحوادث السيبرانية [٢]. لقد حظي القانون بإهتمام كبير بين العاملين في قطاعات البنية التحتية الحيوية، لكنه قد لا تدخل حيز التنفيذ لعدة سنوات. إذ يتطلب هذا القانون من مدير وكالة الأمن السيبراني و أمن البنية التحتية (CISA) نشر القواعد المقترحة لتنفيذ متطلبات الإبلاغ، إذ يجب نشر القواعد النهائية في موعد أقصاه أيلول من العام (٢٠٢٥) [٣] كما أصدرت إدارة الرئيس بايدن عام (٢٠٢٣) «إستراتيجية الأمن السيبراني الوطنية الأمريكية». لتأمين الفوائد الكاملة لنظام بيئي رقمي آمن [٤]، و فتحت هذه الإستراتيجية آفاقاً جديدة في السعي إلى تحويل مسؤوليات الأمن السيبراني من مستخدمي الخطوط الأمامية (بما في ذلك الأفراد و الشركات الصغيرة و الحكومات المحلية) إلى مؤسسات أكبر حجماً و ذات موارد أفضل،

(**) إن أكثر من (٨٠٪) من البنية التحتية العسكرية والمدنية الأمريكية مملوكة ومدارة من قبل القطاع الخاص، إذ أصبحت الشركات الخاصة، ولا سيما موردي تكنولوجيا المعلومات والاتصالات، والوكالات الحكومية، أهدافاً رئيسية للهجمات السيبرانية التي تستغل نقاط ضعف البرمجيات في الشبكات. مما يؤدي إلى تزايد الضرر الإقتصادي الناجم عن هجمات برامج الفدية المتكررة والمحتملة بإستخدام الذكاء الاصطناعي على الشركات ومع ذلك، فإن العديد من الشركات الأمريكية الخاصة تبقي الهجمات طي الكتمان، وأكثر من (٨٠٪) منها تدفع فدية للجهات الفاعلة موضع التهديد (كما تفعل ٦٠٪ من الشركات الأوروبية) لإسترداد الأصول المهمة وتجنب الإضرار بالسمعة. يُنظر:

United States Government Accountability Office (GAO), HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cyber security Challenges, 2021, https://www.gao.gov/products/gao-21288-.

(1) Op cit.

(2) Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) , www.cisa.gov.

(3) Michael T. Borgia , The Cyber Incident Reporting for Critical Infrastructure Act of 2022: An Overview , Davis Wright Tremaine LLP , 2022 , https://www.dwt.com/blogs/privacy--security-law-blog/202205//cyber-incident-reporting-act-2022

(4) The White House, "FACT SHEET: Biden-Harris Administration Announces National Cyber security Strategy" (Mar. 2, 2003) ,https://www.whitehouse.gov/briefing-room/statements-releases/202302/03//fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

مثل : مطوري البرامج و شركات تصنيع الأجهزة [١]. **وأستندت بذلك إلى تحولين إثنين في نهج الحكومة الفيدرالية تجاه الأمن السيبراني:**

- التحول الأول: تسعى الإستراتيجية إلى إعادة التوازن إلى المسؤولية عن الدفاع عن الفضاء السيبراني، مع الإعتراف بأن المسؤولية الأعظم عن حماية البنية الأساسية الحيوية تقع حالياً على عاتق المستخدمين الذين قد لا يكونون مجهزين للتعامل معها[٢].
- التحول الثاني: تُحدد الإستراتيجية أولويات الإدارة لإعادة تنظيم الحوافز للقطاع الخاص للإستثمار في الأمن السيبراني. وتهدف الإستراتيجية إلى تعزيز التعاون بين القطاعين العام والخاص؛ لتحقيق مكاسب في مجال الأمن السيبراني، وبناء قوة عمل سيبرانية قوية ومتنوعة [٣].

دعماً لهذين التحولين ركزت الإستر اتيجية على خمسة محاور أساسية هي:

١- الدفاع عن البنية التحتية الحيوية: وذلك بتفعيل نموذج دائم وفعال للدفاع التعاوني الذي يوزع المخاطر ويوفر مستوى أمن أساسي ومرن للنظام وقد فعّلت الحكومة الفيدرالية ذلك في بعض القطاعات مثل: النقل، وتواصل العمل لتطوير توجهات إلزامية للأمن السيبراني في قطاعات أخرى [٤].

٢- تعطيل وتفكيك الجهات التهديدية: تواصل الحكومة الفيدرالية تنسيق دفاعاتها بما في ذلك الدفاعات الدبلوماسية والعسكرية والإستخباراتية لمتابعة تعطيل الجهات الفاعلة التي تركز على التهديد السيبراني. وتعطي وزارة العدل الأمريكية الأولوية للتحقيق في الجرائم الإلكترونية ومحاكمتها، بما في ذلك برامج الفدية [٥].

٣- تشكيل قوى السوق لتعزيز الأمن والقدرة على الصمود: تدعم الإستراتيجية جهود

(1) The White House, National Cyber security Strategy (March 1, 2023), https://www.whitehouse.gov/wp-content/uploads/202303//National-Cybersecurity-Strategy-2023.pdf

(2) Op cit.

(3) Op cit.

(4) Shoba Pillay, David Bitkower, Sara Crook Hickey, Client Alert: Biden-Harris Administration Cybersecurity Strategy, Jenner & Block Publications,)Washington, DC: 2023(, p. 2.

(5) Op cit, p.2.

الكونغرس لسن تشريعات شاملة بشأن حماية البيانات الشخصية وتحديد الموقع الجغرافي والبيانات الصحيحة على وجه الخصوص عبروضع تشريعات لأسواق التأمين ضد المخاطر الواقعة لخروقات للأمن السيبراني وتحميل المؤسسات مسؤولية حماية بيانات للعملاء [١].

٤- الاستثمار الفيدرالي للأمن السيبراني: تعمل الحكومة الفيدرالية على استثمار المزيد من الموارد في تأمين الإنترنت، والبحث في التطورات في مجال الأمن السيبراني، وتطوير ممارسات التشفير القوية بعدة طرق. وتخطط الحكومة الفيدرالية أيضاً لتخصيص الموارد لتطوير نظام آمن للطاقة النظيفة لضمان مصادر طاقة مرنة للهوية الرقمية وتعزيز الأمن والحد من الإحتيال [٢].

٥- إقامة شراكات دولية لتحقيق الأهداف المشتركة، في بعدها الدولي : تؤكد الإستراتيجية ضرورة الاستفادة من الشراكات الدولية القائمة، وهو التزام سياسي لتعزيز الأهداف المشتركة المتعلقة بالإنترنت وتم التوقيع عليه من قبل أكثر من ستين دولة، لوضع إستراتيجيات لمكافحة التهديدات المشتركة، و وضع معايير الأمن السيبراني، ومحاسبة الدول غير الملتزمة [٣].

تؤمن وزارة الخارجية الإمريكية بأن ثورات التكنولوجيا اليوم تمثل قلب التنافس الجيوسياسي مما يدعوها لإكمال الخطوات السابقة لإداراتها في مجال الأمن السيبراني لذا فقد أعلن وزير الخارجية الأمريكية (أنطوني بلينكن) في آيار من عام ٢٠٢٤ عن إستراتيجية بعنوان «إستراتيجية الولايات المتحدة الأمريكية الخاصة بمجال الفضاء الإلكتروني والسياسة الرقمية: نحو مستقبل رقمي مبتكر وآمن ويحترم الحقوق «. **ركزت على مجموعة من المبادئ والأهداف هي [٤]:**

- **تعزيز الدبلوماسية الرقمية والتضامن الرقمي:** تهتم الاستراتيجية بمبدأ التضامن الرقمي من خلال تعزيز دور الدبلوماسية الرقمية، وتعاون الدول في المجال الرقمي، لتشكيل تحالفات جديدة تعتمد المبادئ الأمريكية، وتُسهم في توفير شبكة إنترنت

(1) Op cit, p.2.
(2) Op cit, p.3.
(3) Op cit, p.4.

(٤) تقديرات إنتر ريجونال، مجابهة الخصوم: ما ملامح إستراتيجية الإدارة الأمريكية الجديدة للأمن السيبراني ؟، إنتر ريجونال للتحليلات الإستراتيجية،(ابو ظبي، العدد : ٣٩٣: ٢٠٢٤)، ص ١

مفتوحة و شاملة و آمنة و مرنة [١].

- **إبقاء الولايات المتحدة الأمريكية في صدارة المشهد التكنولوجي:** إذ تعكس الإستراتيجية الرغبة في الحفاظ على التفوق التقني للولايات المتحدة الأمريكية، وقيادتها في مجال التكنولوجيا العالمية، خصوصاً مع مساعي بكين وموسكو للتفوق عليها في المجال الرقمي [٢].

تؤمن وزارة الخارجية الإمريكية بأن ثورات التكنولوجيا اليوم تمثل قلب التنافس الجيوسياسي مما يدعوها لإكمال الخطوات السابقة لإداراتها في مجال الأمن السيبراني

- **طرح مبادئ تنظيم عمل الفضاء الرقمي:** تضمنت مبادئ رئيسة تسعى الإستراتيجية لتحقيقها، هي [٣] :

١- خلق فضاء إلكتروني يحترم قواعد القانون الدولي ويحترم حقوق الأفراد ويوفر فضاء إلكتروني آمن [٤].

٢- بلورة سياسة شاملة تستخدم مختلف الوسائل الدبلوماسية في فضاء رقمي عالمي مرن قادر على مواجهة مختلف الأزمات و التعافي منها بسرعة [٥].

٣- القدرة على معاقبة المتسللين والمخترقين الذين يسعون إلى الإضرار بأمن الولايات المتحدة السيبراني، مما يستدعي تعزيز القدرات السيبرانية الخاصة بها وبحلفائها [٦].

---

(١) بيان صحفي لمكتب المتحدث باسم وزارة الخارجية، إطلاق استراتيجية الولايات المتحدة الدولية الخاصة بمجال الفضاء الإلكتروني والسياسة الرقمية: ترجمات باللغة العربية، موقع وزارة الخارجية الأمريكية، ٦ آيار/ ٢٠٢٤، https://www.state.gov

(٢) أنتوني بلينكن، التكنولوجيا وتحول السياسة الخارجية للولايات المتحدة: ترجمات باللغة العربية، موقع وزارة الخارجية الأمريكية ، ٦ آيار/مايو ٢٠٢٤، https://www.state.gov/

(٣) تقديرات إنتر ريجونال، مجابهة الخصوم : ما ملامح إستراتيجية الإدارة الأمريكية الجديدة للأمن السيبراني ؟، مصدر سبق ذِكره، ص ٣.

(٤) المصدر نفسه، ص ٣.

(٥) المصدر نفسه، ص ٣.

(٦) المصدر نفسه، ص ٣.

الخاتمة:

يمثل الأمن السيبراني تحدياً وجودياً للعالم بأسره فهو لم يعد مجرد قضية تقنية، بل هو قضية أمن قومي وإقتصادي وإجتماعي، فضلاً عن تهديد الحريات المدنية وحقوق الإنسان. وقد أدركت الولايات المتحدة الامريكية هذه المخاطر، وإتخذت خطوات جادة لتعزيز قدراتها الدفاعية والهجومية في الفضاء السيبراني، من خلال إصدار الإستراتيجيات الوطنية للأمن السيبراني، وإنشاء الوكالات المتخصصة، وتخصيص الموارد المالية والبشرية، وتعزيز التعاون الدولي والشراكة مع القطاع الخاص. وقد أظهر البحث أنها قد حققت تقدماً في تطوير إستراتيجياتها للأمن السيبراني خاصة في عهد إدارة بايدن، التي تبنت نهجاً شاملاً ومتوازناً، يجمع بين الدفاع النشط والتعاون الدولي والشراكة مع القطاع الخاص. رغم وجود تحديات عديدة تعترض طريق الولايات المتحدة الامريكية مثل: نقص الكوادر المؤهلة، وتطور أساليب الهجوم السيبراني، وصعوبة تحقيق التوازن بين الأمن والخصوصية، وتزايد التهديدات السيبرانية من الدول المعادية والجماعات الإرهابية. ولمواجهة هذه التحديات، يتعين عليها مواصلة الإستثمار في البحث والتطوير، وتعزيز التعاون الدولي، وتطوير آليات فعالة للردع والهجوم السيبراني، مع الإلتزام بالقوانين الدولية والقيم الأخلاقية. فضلاً عن تعزيز الوعي بأهمية الأمن السيبراني وتوفير التدريب والتأهيل اللازمين للكوادر المتخصصة، ونشر الوعي بين الجمهور. وعليه يمكن القول إن الأمن السيبراني هو سباق تسلح مستمر، يتطلب إستمرار تطوير الاستراتيجيات المتطورة لمواجهة التهديدات المتغيرة. وإن النجاح في هذا المجال الحيوي يتطلب رؤية إستراتيجية شاملة، وتعاوناً وثيقاً بين جميع الجهات المعنية، والتزاماً راسخاً بالقيم الديمقراطية وحقوق الإنسان، ومسؤولية مشتركة بين الحكومات والقطاع الخاص والمجتمع المدني.

الإستنتاجات:

١- الأمن السيبراني هو مفهوم إستراتيجي يهدف إلى حماية الدولة، وتعزيز قوتها من خلال الحفاظ على أمن البنى التحتية الحاسوبية والمعلوماتية.

٢- الدول جميعها لا سيما الولايات المتحدة الأمريكية، تعتمد على الأمن السيبراني لحماية مصالحها الوطنية وسيادتها ومنظومتها السياسية والاقتصادية والاجتماعية.

٣- إن الإستثمار في تكنولوجيا المعلومات والإتصالات يساهم في تعزيز القوة الذكية والقدرة على التصدي للتهديدات السيبرانية المتطورة بوصفها إستراتيجية إستباقية؛ لمواجهة التحديات الرقمية المستمرة، وحماية البنية التحتية الحاسوبية.

٤- إن إستراتيجية إدارة الرئيس الأميركي الأسبق باراك أوباما في مجال الأمن السيبراني تمحورت حول توطيد الإطار التشريعي والقانوني وإتخاذ إجراءات إحترازية لتعزيز الأمن السيبراني.

٥- أما إستراتيجية الرئيس الأمريكي السابق دونالد ترامب، فقد أعتمدت على تعزيز الردع السيبراني والقدرة على الهجوم السيبراني الدفاعي ضد أي دولة تهدد الأمن القومي الأمريكي. وقد تم تكثيف العمليات السيبرانية الهجومية بشكل إستباقي لمواجهة الخصوم السيبرانيين وتقويض قدراتهم.

٦- قدمت إدارة الرئيس الأمريكي بايدن توجهاً مختلفاً عن سابقتها، ركزت على زيادة الأولوية للأمن السيبراني وتعزيز التعاون مع القطاع الخاص والشركاء الدوليين، وتطوير البنية التحتية الحيوية وتعزيز قدرات الدفاع والردع السيبراني.

٧- تدعو إستراتيجية الأمن السيبراني للرئيس الأمريكي بايدن إلى تعزيز الإطار التشريعي والقانوني، وتفعيل دور المركز الإستراتيجي لمكافحة الإرهاب، وإطلاق مشروع مخصص لمكافحة الهجمات السيبرانية، وإنشاء قواعد التعاون المشتركة دولياً.

٨- تستهدف الإستراتيجية الامريكية تعزيز الدفاع السيبراني للبنية التحتية الحيوية وتشكيل مبادئ تنظيم عمل الفضاء الرقمي، بتعزيز الردع السيبراني وتطوير قدرات الدفاع والرد السيبراني للتخفيف من التهديدات السيبرانية.

قائمة المصادر

اولاً: المصادر العربية:

أ- الكتب العربية والمترجمة:

١- إبراهيم محمد الحمامصة وفارس العمارات، الامن السيبراني: المفهوم وتحديات العصر، دار الخليج للتوزيع والنشر، الأردن، الطبعة الأولى، ٢٠٢٢.

٢- فرح يحيى زعاترة، التهديدات السيبرانية على الامن القومي الأمريكي، القاهرة، العربي للنشر والتوزيع، ٢٠٢٣.

٣- مصطفى شلش، سباق الجيل السادس بين الولايات المتحدة والصين: إستخدامات الذكاء الإصطناعي العسكري، مركز الدراسات العربية الأوراسية، القاهرة، ٢٠٢٣.

٤- سيف الهرمزي، مقتربات الذكية الأمريكية كآلية من آليات التغيير الدولي: الولايات المتحدة الأمريكية أنموذجاً، المركز العربي للأبحاث ودراسة السياسات، الدوحة، ٢٠١٦.

٥- الهرمزي، سيف (٢٠١٦). مقتربات الذكية الأمريكية كآلية من آليات التغيير الدولي: الولايات المتحدة الأمريكية أنموذجاً. الدوحة: المركز العربي للأبحاث ودراسة السياسات.

٦- منعم صاحي العمّار، من يدين لمن؟ مكانة الاستخبارات في الاستراتيجية الأمريكية الشاملة، بغداد، مكتبة الغفران للخدمات الطباعية، ٢٠١٢.

٧- محسن محمد صالح، التقرير الاستراتيجي الفلسطيني ٢٠٢٠-٢٠٢١، مركز الزيتونة للدراسات والاستشارات، بيروت، ٢٠٢٢

ب- الاطاريح والرسائل الجامعية:

١- بلموهوب رياض وقدوج نور الدين، الردع الإلكتروني كآلية لمواجهة الحروب السيبرانية، كلية الحقوق والعلوم السياسية، جامعة محمد بشير الإبراهيمي، الجزائر، رسالة ماجستير غير منشورة، ٢٠٢٣.

ج- المجلات والصحف:

١- حسام محمد نبيل عبد الرؤوف مرسي، الامن السيبراني (ضرورته - متطلبات تحقيقه)، مجلة كلية الدراسات العليا، مصر، العدد ٣٤، ٢٠١٦.

٢- صفاء حسين علي، استراتيجية القوة الذكية وأثرها في السياسة الخارجية الصينية، مجلة الجامعة العراقية، بغداد، العدد ٤٧،.٢٠٢٠.

٣- عامر مصباح، الفضاء السيبراني نموذج لتوسيع عقيدة الدفاع الإستراتيجي، كلية العلوم السياسية والعلاقات الدولية، مجلة دراسات الدفاع والإستشراف: دراسة ستراتيجيا، الجزائر العدد ١٦ السداسي الثاني، ٢٠٢١.

٤- يونس مؤيد يونس مصطفى، إستراتيجية الولايات المتحدة الأمريكية للأمن السيبراني، جامعة النهرين، كلية العلوم السياسية، بغداد، العدد ٥٥، ٢٠١٨.

٥- محمد قاسم هادي، مكانة القوة في الفكر الاستراتيجي الأمريكي، جامعة بغداد، كلية العلوم السياسية، مجلة العلوم السياسية، العدد ٥٤، ٢٠١٨.

٦- علي محمد أمنيف، تحديات الأمن في الفضاء السيبراني الأمريكي، مجلة دراسات دولية، مركز الدراسات الاستراتيجية والدولية، جامعة بغداد، العدد ٨٥، ٢٠٢١.

٧- مهوب وسام، نموذج الولايات المتحدة الأمريكية في مجال الأمن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع، مجلة البيبان للدراسات القانونية والسياسية، جامعة برج بوعريريج، الجزائر، المجلد ٨٠ العدد ٢، ٢٠٢٣.

٨- شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر، المجلد ١٥، العدد: ١، ٢٠٢٢.

٩- صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، ٢٠٢٠، العدد ٦٢.

١٠- نور علي صكب، الأمن الوطني العراقي في ظل الإختراق السيبراني (أمن المعلومات)، مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، بغداد، العدد ١١، ٢٠٢١.

١١- هبة جمال الدين: الأمن السيبراني والتحول في النظام الدولي، جامعة القاهرة، مصر، مجلة كلية الإقتصاد والعلوم السياسية، المجلد ٢٤، العدد الأول، ٢٠٢٣.

١٢- جمال الدين، هبة. (٢٠٢٣). الأمن السيبراني والتحول في النظام الدولي. مصر:

جامعة القاهرة، مجلة كلية الإقتصاد والعلوم السياسية، المجلد (٢٤)، العدد (١).

١٣- إسراء شريف الكعود، التأثير السيبراني في الامن القومي للدول الفاعلة (الولايات المتحدة الأمريكية) انموذجا، مجلة العلوم السياسية، جامعة بغداد، العدد ٦٣، ٢٠٢٢.

١٤- نهي علي أمير، الأمن السيبراني في إستراتيجية الامن القومي الروسي، آفاق آسيوية، الهيئة العامة للإستعلامات، جمهورية مصر العربية، العدد ١١، ٢٠٢٣.

١٥- كرار عباس متعب فرج، الحرب السيبرانية: دراسة في إستراتيجية الهجمات السيبرانية بين الولايات المتحدة الإمريكية وإيران، مجلة حمورابي للدراسات، بغداد، العدد ٤٠، ٢٠٢١.

١٦- علاء الدين فرحات، من الردع النووي إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، مجلة المفكر، جامعة الجيلالي بونعامة خميس مليانة، الجزائر، المجلد ١٦، العدد: ١، ٢٠٢١.

١٧- إنتر ريجونال. (٢٠٢٤). مجابهة الخصوم: ما ملامح إستراتيجية الإدارة الأمريكية الجديدة للأمن السيبراني؟ إنتر ريجونال للتحليلات الإستراتيجية، العدد (٣٩٣).

د- شبكة الانترنت:

١- علي ادهم، الامن السيبراني Cyber Security الجزء الاول ، مركز النهرين للدراسات الاستراتيجية، مستشارية الامن القومي، بغداد، ٢٠١٩ https://alnahrain.iq/post/382.

٢- محمد المنشاوي، كيف فشلت إستراتيجية «الدفاع للأمام» في حماية أميركا من الهجمات السيبرانية؟، شبكة الجزيرة الإعلامية، ٢٠٢٠، https://aja.me/umsfa .

٣- أنتوني بلينكن، التكنولوجيا وتحول السياسة الخارجية للولايات المتحدة : ترجمات باللغة العربية،موقع وزارة الخارجية الأمريكية ، ٦ آيار/مايو ٢٠٢٤،
https://www.state.gov/%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7-%D9%88%D8%AA%D8%AD%D9%88%D9%84-%D8%A7%D9%84%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9-%D8%A7%D9%84%D8%AE%D8%A7%D8%B1%D8%AC%D9%8A%D8%A9-%D9%84/

ثانياً:المصادر الأجنبية:

1- Luigi Di Martino, Fear and empathy in international relations: Diplomacy, cyber engagement and Australian foreign policy, Place Branding and Public Diplomacy, Volume 20, Issue 1, 2024.

2- Albalas, T., Modjtahedi, A., Abdi, R. (Cyber security governance: a scoping review, International journal of professional business review, Miami, v. 7 , n. 4 , 2022.

3- Maleh Yassine, Youness Yassine, Cyber Sovereignty in Morocco, Springer Briefs in Cyber security, Switzerland, 2022.

4- Vivek Mishra and Sameer Pati, Decoding the Biden Administration's Cyber Security Policy, Observer Research Foundation, New Delhi, 2024, ISSUE NO. 686.

5- Jacob Shively, Cyber security Policy, Punctuated Equilibrium Theory, and the Biden Administration, American Political Science Association (APSA), Washington, D.C, 2022.

6- David P. Fidler, President Trump's Legacy on Cyberspace Policy , Council on Foreign Relations , 2020 ,

https://www.cfr.org/blog/president-trumps-legacy-cyberspace-policy

7- Niranjan Shankar, The Biden Administration's National Cybersecurity Strategy: Opportunitys & Challenges, Middle East institute, Washington, D.C., 2024.

8- President Joseph Biden Jr., Interim National Security Strategic Guidance, White House, Washington, March 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-security-strategic-guidance/

9- United States Government Accountability Office (GAO), HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cyber security Challenges, 2021, https://www.gao.gov/products/gao-21-288

10- Aaron Clarke, Tom Klein, 2021 Year in Review: The Biden Administration's Efforts on Cybersecurity, Third Way report, Published January 25, 2022, https://www.thirdway.org/report/2021-year-in-review-the-biden-administrations-efforts-on-cybersecurity.

11- Herb Lin , How Biden's Cyber Strategy Echoes Trump's : Comparing the Biden administration's Interim National Security Strategic Guidance with Trump's National Cyber Strategy , The Lawfare Institute , 2021 , https://www.lawfaremedia.org/article/how-bidens-cyber-strategy-echoes-trumps.

12- Gloria McDonald , Defining National Security: A comparison of the Trump and Biden Administration's National Security Strategies , Center for American Security , RESEARCH REPORT , WASHINGTON, D.C. , 2023.

13- Gisela Grieger, The US cybersecurity posture under Biden , EPRS | European Parliamentary Research Service , European Union, 2023 , https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2023)753929.

14- Michael T. Borgia , The Cyber Incident Reporting for Critical Infrastructure Act of 2022: An Overview , Davis Wright Tremaine LLP , 2022 , https://www.dwt.com/blogs/privacy--security-law-blog/2022/05/cyber-incident-reporting-act-2022

15- The White House, "FACT SHEET: Biden-Harris Administration Announces National Cyber security Strategy " (Mar. 2, 2003) ,https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

16- Shoba Pillay, David Bitkower, Sara Crook Hickey, Client Alert: Biden-Harris Administration Cybersecurity Strategy, Jenner & Block Publications, Washington, DC, 2023.