رقم الترميز الدولي / ISSN (P): 2710-2653
ISSN (E): 2960-253X /
رقم الايداع الوطني / 2375 / 2019

تاريخ استلام البحث ١٢ / ١٠ / ٢٠٢٥
تاريخ قبول البحث ٢٤ / ١١/ ٢٠٢٥
تاريخ النشر ٣٠ / ١٢/ ٢٠٢٥

الأمن القومي الامريكي في بيئة التهديدات السيبرانية

US national security in the cyber threat environment

م .م .كرار محمد جواد
Karar Mohammad Jawad
جامعة الكوفة / كلية العلوم السياسية
University of Kufa / College of Political Science
kararm.albukhutar@uokufa.edu.iq

م .م. منى جبار خضر
Muna Jabbar Khudhair
جامعة الكوفة / كلية الاثار
University of Kufa / College of Archaeology
monaj.alukaili@uokufa.edu.iq

IRAQI Academic Scientific Journals
https://iasj.rdd.edu.iq/journals/journal/view/229

الملخص

يشكل الأمن السيبراني بمفهوم العام أحد العوامل المهمة للحفاظ على مكانة الولايات المتحدة الأمريكية كقوة دولية في عصر المعلومات والاتصالات، فمع التطور الهائل في التكنولوجيا الرقمية وانتشار الإنترنت والفضاء الواسع ، إذ لم يعد التهديد يقتصر على الهجمات العسكرية التقليدية، بل امتد ليشمل الفضاء الرقمي الذي يؤثر بشكل مباشر على الاقتصاد، والبنية التحتية الحيوية، والأمن المجتمعي، فالولايات المتحدة الامريكية تواجه تحديات متصاعة وعلى مستوى عالي من التهديدات الالكترونية التي تستهدف مؤسساتها الحكومية وغير الحكومية سواء على الأنظمة (المالية والطاقة والصحية والعسكرية وغيرها)، حيث تكون عرضة لتهديدات وهجمات سيبرانية متزايدة التعقيد، ومن هنا برز الأمن السيبراني كأولوية قصوى للأمن القومي الأمريكي، ليس فقط لحماية المؤسسات الحكومية والاقتصاد الوطني، بل أيضًا لضمان استقرار المجتمع وثقة الأفراد في الفضاء الرقمي، وقد دفعت هذه التحديات الولايات المتحدة الامريكية إلى تطوير استراتيجيات وطنية متقدمة، وتوظيف قدرات دفاعية وهجومية، وتعزيز التعاون الدولي لمواجهة المخاطر السيبرانية التي لا تعترف بالحدود الجغرافية، وبذلك يمكن القول ان الأمن السيبراني لم يعد مجرد قضية تقنية، بل أصبح ركيزة أساسية للأمن القومي الأمريكي وعنصرًا استراتيجيًا في بقاء الدولة والمحافظة على مكانتها العالمية، حيث يشكل خط الدفاع الأول ضد التهديدات الخارجية والداخلية، ويحافظ على استقرار الدولة سياسيًا واقتصاديًا وعسكريًا .

الكلمات المفتاحية : "الامن القومي"،"الامن السيبراني"،" التهديدات السيبرانية"،"الردع السيبراني"،" الامن القومي الامريكي"

Abstract

The Cyber Security Copeman is a important factor to maintain the status of the United States of America as an international force in the evaluation of information and communication. The threat is the limit of the traditional military attacks. The world is not limited to the digital space that affects direct economy on the economy, the vital infrastructure, community security, the United States of America faces a bad and challenging levels of electronic threats to the regulations of their website and the mainstream of the electronic threats to their regulations and their participation in the survival of the mainland and its political statistics. The United States of America. The United States of America The face of the United States of America and the United Nations, the mainland of the United States of America's national and national and economic cooperation. The United States of America has to be able to develop the cybersome and the defense of the defense and the attacks. The cross-by-cybersome is not just a technical issue. The "Cyber security is no longer a technical issue and the strategy of the State of the United States and the mainstream of the State and the intervention of the State and the intervention of the State and the conservation of the external and economic intervention

Keywords: "National security," "Cybersecurity," "Cyber threats," "Cyber deterrence," "US national security"

المقدمة

يشكل الأمن السيبراني بمفهوم العام أحد العوامل المهمة للحفاظ على مكانة الولايات المتحدة الأمريكية كقوة دولية في عصر المعلومات والاتصالات، فمع التطور الهائل في التكنولوجيا الرقمية وانتشار الإنترنت والفضاء الواسع ، إذ لم يعد التهديد يقتصر على الهجمات العسكرية التقليدية، بل امتد ليشمل الفضاء الرقمي الذي يؤثر بشكل مباشر على الاقتصاد، والبنية التحتية الحيوية، والأمن المجتمعي، فالولايات المتحدة الامريكية تواجه تحديات متصاعة وعلى مستوى عالي من التهديدات الالكترونية التي تستهدف مؤسساتها الحكومية وغير الحكومية سواء على الأنظمة (المالية والطاقة والصحية والعسكرية وغيرها)، حيث تكون عرضة لتهديدات وهجمات سيبرانية متزايدة التعقيد، ومن هنا برز الأمن السيبراني كأولوية قصوى للأمن القومي الأمريكي، ليس فقط لحماية المؤسسات الحكومية والاقتصاد الوطني، بل أيضًا لضمان استقرار المجتمع وثقة الأفراد في الفضاء الرقمي، وقد دفعت هذه التحديات الولايات المتحدة الامريكية إلى تطوير استراتيجيات وطنية متقدمة، وتوظيف قدرات دفاعية وهجومية، وتعزيز التعاون الدولي لمواجهة المخاطر السيبرانية التي لا تعترف بالحدود الجغرافية، وبذلك يمكن القول ان الأمن السيبراني لم يعد مجرد قضية تقنية، بل أصبح ركيزة أساسية للأمن القومي الأمريكي وعنصرًا استراتيجيًا في بقاء الدولة والمحافظة على مكانتها العالمية، حيث يشكل خط الدفاع الأول ضد التهديدات الخارجية والداخلية، ويحافظ على استقرار الدولة سياسيًا واقتصاديًا وعسكريًا .

اشكالية البحث : تكمن الإشكالية الرئيسة في أن التهديدات السيبرانية متنامية ومتنوعة، تتجاوز حدود الدولة، بدءًا من البنية التحتية الحيوية، مرورًا بالاقتصاد والسياسة، وصولًا إلى الأمن العسكري، مما يعقّد من قدرة الولايات المتحدة الامريكية على الردع والحماية، ويُضاف إلى ذلك صعوبة تحديد مصدر الهجمات بشكل قاطع، لذا جعل من الفضاء السيبراني ساحة مفتوحة للصراع، وبذلك تُطرح تساؤلات رئيسية : (كيف يمكن للولايات المتحدة أن تحافظ على أمنها القومي في بيئة تتغير فيها طبيعة التهديدات باستمرار؟)، (ماهي التحديات التي تواجهها في بناء استراتيجية سيبرانية شاملة وفعّالة؟) .

فرضية البحث : التهديدات السيبرانية تمثل خطراً موازياً أو يفوق التهديدات العسكرية التقليدية على الولايات المتحدة الأمريكية، وعاملًا استراتيجيًا مؤثرًا على الأمن القومي، وكلما ازدادت حدة وتعقيد التهديدات السيبرانية الموجهة ضد البنى التحتية الحيوية والمؤسسات العسكرية والاقتصادية الأمريكية، كلما ارتفعت مستويات المخاطر، إذ تؤدي الهجمات الإلكترونية إلى تقويض السيادة الوطنية، وزعزعة الاستقرار السياسي والاقتصادي، الأمر الذي يجعل من تطوير قدرات الأمن السيبراني ضرورة ملحّة لتعزيز منظومة الأمن القومي وحماية المصالح الوطنية، وكذلك الاعتماد على التعاون الدولي ووضع معايير ملزمة لإدارة الفضاء السيبراني يمثلان شرطاً أساسياً لتقليل المخاطر وتعزيز الأمن القومي الأمريكي .

هيكلية البحث : يتضمن البحث تحت عنوان (الامن القومي الامريكي في بيئة التهديدات السيبرانية) من ثلاثة مباحث، حيث يكون المبحث الاول بعنوان ماهيه الامن السيبراني وينشق منه (مفهوم الامن السيبراني ونظريات الامن السيبراني)، أما المبحث الثاني بعنوان الأمن السيبراني واثره على البعد القومي الامريكي ويتفرع منه

(الاثرعلى البعد الاقتصادي والسياسي والاستخباري والعسكري الامريكي)، وأخراً المبحث الثالث بعنوان تحليل مقومات الامن السيبراني الامريكي ويتكون من (البنية المؤسسية والاطار التشريعي والتنظيمي للامن السيبراني الامريكي) .

المبحث الاول : ماهيه الامن السيبراني

يعد الامن السيراني (Cyber security)، دوراً مهما ومحورياً في توفير المعلومات وايضا الحفاظ على سلامتها وسريتها، ويُعد عنصراً أساسياً في نجاح التحول الرقمي في اغلب المجالات منها السياسية والاقتصادية والامنية والاجتماعية والثقافية والاعلامية وغيرها

المطلب الاول : مفهوم الامن السيبراني : يعد مصطلح الامن السيبراني مصطلح حديث نسبيًا، ومشتقة من الكلمة الإنجليزية (Cyber)، وفي بعض الاحيان يستخدم مصطلح (سيبران) كاختصار لكلمة (سيبراني)[١]، والتي تعني كل ما يتصل بالتقنية الرقمية، عبر (أجهزة الالكترونية – البنية التحتية لتكنولوجيا المعلومات والاتصالات – شبكات الإنترنت – البيانات)، وغالبًا ما تُستخدم كلمة (السيبراني) في سياقات مثل، الفضاء السيبراني (Cyberspace) البيئة الافتراضية التي تحدث فيها التفاعلات الرقمية عبر الإنترنت، الحرب السيبرانية (Cyber warfare) استخدام الوسائل الرقمية لمهاجمة البنى التحتية أو المعلومات لأغراض سياسية أوعسكرية، الجرائم السيبرانية (Cybercrimes) الجرائم التي تُرتكب باستخدام التكنولوجيا الرقمية، مثل الاختراق الانظمة أو سرقة البيانات[٢]، لذا يكون المفهوم العام للأمن السيبراني (Cyber security) وهي مجموعة من الوسائل التقنية والممارسات التي تهدف إلى حماية الأنظمة الرقمية والشبكات والمعلومات من الهجمات وتخريب وتعطيل خدمات أو الوصول غير المصرّح به عبرعمليات واجراءات مصممة للدفاع ضد الهجمات السيبرانية وضمان سرية المعلومات وسلامتها وتوافرها، وعتمد مفهوم الامن السيبراني، نظرًا لاعتماد العالم المتزايد على التكنولوجيا والإنترنت، ومن ابرزها اولاً:(الافراد حماية معلومات الشخصية والبيانات الحساسة) مثل الهوية الشخصية، الحسابات البنكية، كلمات المرور، تأمين سجلات المرضى الرقمية، عدم التلاعب بالأجهزة الطبية المتصلة بالإنترنت، تأمين البيانات والصور الخاصة من السرقة أو الاستخدام غير المشروع، ثانياً:(أمان المعاملات المالية) مثل تأمين عمليات الدفع الإلكتروني والتجارة عبر الإنترنت، الحماية من الاحتيال المالي والقرصنة البنكية ،الحفاظ على استمرارية الأعمال والخدمات، تأمين بيانات المؤسسات والجهات الحكومية من التسريب أو السرقة، ثالثاً:(أمن البنية التحتية الحيوية المؤسسات والشركات) من خلال حماية البنية التحتية الرقمية للشركات من الهجمات السيبرانية، منع الاختراقات التي قد تؤدي إلى خسائر مالية أو تسريب معلومات سرية، حماية أنظمة الكهرباء، المياه، والاتصالات من الهجمات الإلكترونية، ضمان استمرار تشغيل الأنظمة الحيوية للدولة، رابعا:(الدفاع السيبراني للامن القومي) عبر حماية الأنظمة العسكرية والمعلومات الاستخباراتية، التصدي للهجمات السيبرانية التي تستهدف الأمن القومي، حماية منصات التعليم الإلكتروني، منع تسريب الامتحانات أو بيانات الطلاب والمعلمين، تتبع الجرائم مثل الابتزاز الإلكتروني، الاحتيال، وانتحال الهوية، دعم السلطات في التحقيقات الرقمية، لذا يكمن الامن السيبراني بالادارك والمعرفة من خلال (الأفراد بالسرية) لحماية حساباتهم الشخصية فقط

الأشخاص المناسبين يمكنهم رؤيتها والحفاظ على استمرارية الأعمال والخدمات،(الشركات اوالموسسات) لحماية البيانات والأنظمة لمنع الخسائر المالية والضرر بالسمعة، (الحكومات) لحماية الأمن الوطني والمعلومات الحساسة وتأمين البنية التحتية الرقمية مثل المصارف، والمستشفيات، والدوائر الحكومية، وتوسعت استخدامات مفهوم الامن السيبراني للإشارة إلى التهديدات الالكترونية التي تستهدف بنى تحتية للدول او المؤسسات بااستخدام الوسائل التكنولوجية والتطبيقات الرقمية للهجوم من خلال:(الفيروسات والبرمجيات الخبيثة)، (اختراق الحسابات والشبكات)، (التجسس الإلكتروني وسرقة البيانات)،(هجمات حجب الخدمة DDoS)،(هجمات الفدية Ransom ware)، (التصيّد الإلكتروني Phishing)، ومن الاساليب العملية لمواجهة تهديدات الأمن السيبراني تكمن في:(تطوير برامج مكافحة الفيروسات التي تحمي جهاز الكمبيوتر الخاص بك من البرامج الضارة)،(اضافة جدران الحماية تمنع حركة مرور الشبكة المشبوهة)،(انشاء كلمات المرور ذات مصادقية متعددة العوامل للحفاظ على الحسابات آمنة)، (تكوين من النسخ الاحتياطية تمنع فقدان البيانات في حالة وقوع هجمات مثل برامج الفدية) [٣] .

المطلب الثاني – نظريات الامن السيبراني (Cyber security Theories) : تمثل نظريات الأمن السيبراني الأطر الاساسية التي تساعد على فهم التهديدات ونقاط الضعف وكذلك الاستراتيجيات لحماية الأنظمة وآليات الدفاع عن البيانات الالكترونية، فيما يلي بعض النظريات والنماذج الرئيسية منها :

١- نظرية الثقة المعدومة (Zero Trust): تعبر هذه النظرية عن إطارحديث للامن السيبراني على خلاف نماذج الامن التقليدي،[٤] وهنالك توجد تسمية اخرى وهي (نموذج الثقة الصفرية Zero trust model)، حيث تفرض النظرية بعدم الثقة تلقائيًا بأي جهاز او كيان مستخدم، لان التهديدات السيبرانية، تحدث من (داخل الشبكة أو خارجها)، لذا يتم تقسيم الشبكة الى شرائح او اجزاء صغيرة لتقليل احتمالية انتشار التهديدات بحيث لايستطيع المهاجم التنقل بحرية داخل النظام، لانها تتطلب تحققٌ صارمًا من ادارة هوية الشبكة وتشفيرها ومراقبتها بشكل مستمر للأنشطة داخلها وكذلك يجب تحديد صلاحيتها قبل السماح بالوصول للشبكة اوالملفات الا المتسخدمين المصرح بهم [٥].

٢- نظرية القلعة والخندق (Castle & Moat Theory) : تعتمد هذه النظرية على فكرة قديمة عبر تأمين الشبكات والانظمة على شكل (القلاع او الحصن او الخندق)، وتتركز ببناء جدار حماية ناري قوي (Firewall)، ويكون فيه نقطة دخول واحدة (مثل البوابة في القلعة)، لتكون عملية المراقبة داخل النظام عمليا أقل واسهل واكثر صارمة على المستخدمين الشبكة، مما يجعل من الصعب على المهاجمين اختراقها، الا ان هذه النظرية واجهت بعض الانتقادات منها بعدم المرونة ولا تتماشى مع البنيه الشبكات الحديثة لل وصول لأماكن امنه ومتعددة ومتغيرة، وتفترض بالتهديدات تأتي من الخارج وتتجاهل من داخل النظام، لذا اصبحت غير مفيدة نسبياً باستخدام المؤسسات الحوسبة السحابية، ولاسيما مع تطور التهديدات السيبرانية والمشهد الرقمي .

٣ – نظرية الدفاع المتعدد الطبقات (Multilayer defense theory) : يكمن المنهج الامني لهذه نظرية بانشاء مجموعة من طبقات كحاجز للتهديد الخارجي يكون امن ومتعدد وقوي يفصل الشبكة الداخلية الآمنة عن

العالم الخارجي الغيرموثوق بها في جميع أنحاء نظام تكنولوجيا المعلومات، حيث توجد تسميه اخرى وهي الدفاع المتعمق (Defense in depth)، لذا تشمل تلك الطبقات المشتركة في استراتيجية الحماية من الاختراقات مثل (الجدران الحماية النارية Firewalls، أنظمة كشف التسلل IDS، التشفير، المصادقة متعددة العوامل MFA، التحكم بالوصول بالشبكة، إخفاء البيانات، توفير نسخ احتياط)،الأمان ولحماية الأنظمة واكتشاف الهجمات المتأخرة، وفي حال اختراق او فشل احد الطبقات تظل، هناك طبقات أخرى تمنع الهجمات والتهديدات من الدخول للشبكة، وأيضًا إبطاء المهاجمين واكتشاف عمليات الاختراق مبكر [٦].

٤ – نظرية السلوك والعوامل البشرية (Behavioral and Human Factors Theory) : تجمع هذه النظرية بين مجالات علم النفس والاجتماع والامن السيبراني، لفهم كيفيه تاثير سلوك الافراد من قرارات وقدرات ودوافع على أمن المعلومات والأنظمة[٧]، والذي غالبًا ما يُعد الفرد الحلقة الأضعف في نتائج الأمن، وذلك بسبب النية السيئة، الأخطاء البشرية، ونقص الوعي للمستخدمين، وكذلك تسمى بالهندسة الاجتماعية (Social Engineering Theory) [٨]، لاعتماد سلوب التهديد يكون بدلاً من استغلال ثغرات البرامج أو الأجهزة، ليكون اولا:الاحتيال: بإرسال رسائل بريد إلكتروني مزيفة لخداع المستخدمين، ثانيا:الاصطياد بالرمح: بهجوم مخصص لفرد أو مؤسسات معينة، ثالثا:التنكر: انتحال شخصية موظف رسمي او زميله للحصول على معلومات، رابعا:الإغراء: تقديم شيء مغرٍ مثل USB مجاني يحتوي على برمجيات خبيثة، خامسا:الاستجداء: وعد بتقديم خدمة مقابل معلومات، لذا يكمن الحماية من هذه التهديدات عبر توعيه المستمرة للمستخدمين، وضع سياسات صارمة للتحقق من الهوية المستخدمين وتقليل الصلاحيات الممنوحة للمستخدمين.

٥ – نظرية التهديدات المتماثلة وغير المتماثلة (Symmetric and Asymmetric Threat Theory) : تستخدم هذه النظرية لفهم طبيعة العلاقة للطرفان بين المهاجم والمدافع، وتقيم المزايا الاستراتيجية من الإمكانيات والأهداف وديناميكيات العمليات للبيئة التي تواجه الشبكات والانظمة الرقمة، فالتهديدات المتماثلة: تأتي من جهات فاعلة لها إقدرات متساوية نسبيًا، حيث تشن دولة هجوم على بنية تحتية لدولة أخرى أو مؤسسة منافسة تقوم بهجوم تجسسي ضد مؤسسة أخرى متقاربة في القوة والتقنية، وهي غالباً ما تكون هجمات ذات تكتيكات واضحة يمكن التنبؤ لها من الثغرات الامنية للأنظمة او معلومات، وهي تهديدات منظمة وتتمتع بدعم مالي وتقني فالهدف منه التجسس، التخريب، أو الردع، عادةً ما يختار المهاجمون وقت الهجوم، بينما يجب على المدافعين أن يكونوا دائمًا على أهبة الاستعداد، وهذا يمنح المهاجمين ميزة عدم التماثل الزمني، فتعد لعبة أكثرعدالة، ولكن هذا نادر في الواقع العملي، أما التهديدات غير المتماثلة: تأتي من جهات فاعلة صغيرة وغير حكومية عبر المتسللون اوالجماعات الإرهابية، فهي لا تملك نفس القدرات انما أضعف تقنياً ومالياً من الجهة المُستهدفة، ويتمتع أحد الطرفين بميزة واضحة على الآخر، بتوضيف وسائل غير تقليدية ومفاجئة وتقنيات غير متوقعة يصعبة تتبعها وبااستثمارات منخفضة التكلفة مثل برمجيات خبيثة أوالعبوات الناسفة، وباستغلال نقاط الضعف بالبنية التحتية والخوف النفسي، فالمهاجم غالبًا مايحتاج خاصية الذكاء واكتشاف فجوة أمنية واحدة فقط لإحداث تأثير كبيربالضحية، فيتعين على المدافعين حماية كل شيء، وتبني منهجيات استباقية ومرنة [٩].

٦ – **نظرية الفوضى (Chaos theory)** : هي حالة من الاضطراب بالبنية التحتية المعلوماتية، وفي سياق اخر بيئة رقمية غيرمنضبطة داخل مؤسسات الدولة والشركات، حيث تنشأ الفوضى السيبرانية من جهات تفتقد لرؤية شاملة وخطط لإدارة المخاطر السيبرانية، وايضا تضارب بالصلاحيات بين الفرق التقنية والإدارية وسوء تنسيق بينها، فالأنظمة السيبرانية تبدو منظمة لكنها تتصرف بشكل غير متوقع وبأنماط متغيرة ومتكررة وغير معلنة يصعب احتوائها والتعامل معها، مع توسع شبكات او أنظمة المراقبة دون ربطها معا، وتعدد الحسابات المجهولة وغير النشطة بالأنظمة يصعب متابعتها، كذلك الاعتماد المفرط على تقنيات امنية غير واضحة وتجاهل تصنيف البيانات وتحديثها وحمايتها، وجود نقص بالكفاءات المتخصصة وعدم الوعي للمستخدمين أنظمة الحوسبة السحابية وإنترنت الأشياء والذكاء الاصطناعي[١٠]، لان أجراء بسيط أو تهيئة غير صحيحة بنقطة واحدة، يسبب سلسلة من الاختراقات والنشاطات التخريبية، لذا يكمن أهمية الوعي بالأمن السيبراني من بناء أنظمة يمكنها التعامل مع السلوكيات غير المتوقعة، واستخدام تحليلات الذكاء الاصطناعي للتعرف على الأنماط المعقدة والفوضوية للهجمات، التركيز على إدارة التفاصيل الصغيرة لأنها قد تؤدي إلى تأثيرات ضخمة، لتقليل الفوضى وفرض الحوكمة والتنظيم داخل البيئة الرقمية

المبحث الثاني: الأمن السيبراني واثره على البعد القومي الامريكي .

يمثل الأمن السيبراني اليوم حجر الزاوية في معادلات القوة الوطنية الشاملة للدول، حيث لم تعد التهديدات في الفضاء الرقمي مقصورة على الهجمات العسكرية أو التجسسية، بل تجاوزت ذلك لتطال ركائز الدولة المعاصرة، من اقتصاد وثقافة ومجتمع وسياسة وإعلام. ومع تنامي الاعتماد على التكنولوجيا الرقمية والأنظمة المتصلة بالشبكات في إدارة مفاصل الحياة اليومية والمؤسسات العامة والخاصة، أصبح الأمن السيبراني عاملًا حاسمًا في حماية الاستقرار الداخلي والهوية السيادية للدول، من هذا المنطلق، يحاول هذا المحور العلمي تحليل التأثيرات متعددة الأبعاد للأمن السيبراني، باعتباره قضية استراتيجية تتجاوز البعد التقني، لتمتد إلى عمق البنى الاقتصادية والاجتماعية والثقافية والسياسية والإعلامية، مع تقديم رؤية شمولية لطبيعة التهديدات وتداعياتها المحتملة في ظل تصاعد التنافس الرقمي العالمي .

المطلب الاول : الامن السيبراني واثره على البعد الاقتصادي الامريكي .

يشكل الأمن السيبراني أحد الأعمدة الأساسية للأمن القومي الأمريكي إلا أن تأثيره لا يقتصر على الجوانب الاستخباراتية أو العسكرية فحسب، بل يمتد ليشمل القطاع الاقتصادي بكل مستوياته ، وبذلك أصبحت البنية التحتية الرقمية للاقتصاد الأمريكي عرضة لكثير من التهديدات السيبرانية التي تستهدف المؤسسات المالية، وسلاسل الإمداد، والشركات الكبرى، وحتى الشركات الناشئة، وهو ما شكل تأثير كبير على الأداء الاقتصادي والاستقرار المالي، قدر تقرير صادر عن مكتب المحاسبة الحكومي الأمريكي عام ٢٠٢١ أن الخسائر الناجمة عن الهجمات السيبرانية على البنية الاقتصادية الحيوية قد بلغت مليارات الدولارات سنويًا، نتيجة لانقطاع الخدمات،

والابتزاز الإلكتروني وسرقة الملكية الفكرية [١١]، كما أشار تقرير لشركة (اي بي ام) لسنة ٢٠٢٣ ان متوسط تكلفة اختراق البيانات في الولايات المتحدة الامريكية هو الأعلى عالميًا، ويبلغ حوالي ٩.٤٨ مليون دولار لكل اختراق الكتروني ، مما يجعل المؤسسات الاقتصادية الأمريكية الأكثر استهدافًا والأغلى تكلفة في حال التعرض لهجمات الكترونية ، اضافة لذلك، فإن ضعف الأمن السيبراني يمكن أن يؤدي إلى فقدان الثقة في السوق الأمريكي من قبل المستثمرين الدوليين، ومن ثم تأثيره على استقرار الدولار الأمريكي بوصفه عملة احتياط عالمية، اذ حذرت الاستراتيجية الوطنية للأمن السيبراني الأمريكية لعام ٢٠٢٣ من أن الهجمات على اي من القطاعات الاقتصادية الحيوية – مثل الطاقة، اوالخدمات المالية، والتكنولوجيا تُعد تهديدًا فعلياً يجب مواجهته بسياسات هجومية ودفاعية متقدمة [١٢]، ضمن هذا السياق، أشار المركز الإقليمي للأمن السيبراني في دراسة تحليلية لسنة (٢٠٢٣) إلى أن "الولايات المتحدة تعد السوق الأكثر نشاطًا في مجال الأمن السيبراني، لكنها كذلك الأكثر عرضة للخطر، وهو ما دفعها لزيادة استثماراتها في هذا المجال بمعدلات غير مسبوقة، حفاظًا على تفوقها الاقتصادي[١٣]، كما أوضح الباحث خالد عبد المجيد في مقال نُشر في المجلة العربية للأمن المعلوماتي أن "الهجمات السيبرانية باتت جزءًا من أدوات التأثير الاقتصادي الدولي، وأن الاقتصاد الأمريكي يظل هدفًا أول للهجمات الإلكترونية بالنظر إلى كثافة اعتماده على التكنولوجيا الرقمية المتقدمة [١٤]، يمكن القول ، ان الاستثمار في مجال الأمن السيبراني مثل فرصة اقتصادية واعدة إذ قُدّرت قيمة سوق الأمن السيبراني الأمريكي بأكثر من ٨٠ مليار دولار في عام ٢٠٢٤، وشهدت زيادة في الوظائف المتخصصة بنسبة تجاوزت ٣٥% خلال العقد الاخير وبالتالي يعدَ الامن السيبراني ليس فقط خط دفاع بل أصبح أيضًا محركًا للابتكارو للنمو الاقتصادي، نتيجة لما سبق بات الأمن السيبراني يشكل عاملًا حاسمًا في الحفاظ على استقرار الاقتصاد الأمريكي من جهة، ووسيلة لتعزيز التفوق التقني والاقتصادي للولايات المتحدة من جهة أخرى .

المطلب الثاني : الامن السيبرانية واثره على البعد السياسي – الاستخباراتي الامريكي .

شهد العالم في العقود الأخيرة تطوراً كبيرا في تكنولوجيا المعلومات والاتصالات مما انتج عن انشاء فضاء سيبراني يمثل بُعداً جديداً للسلطة والصراع بين الدول، اذ أصبح الأمن السيبراني أحد المفاصل الأساسية في منظومة الأمن القومي، لا سيما في الدول الكبرى مثل الولايات المتحدة نتيجة لتزايد الاعتماد على النظم الرقمية في إدارة الشؤون السياسية والعسكرية والاستخباراتية، وقد انعكس ذلك بشكل مباشر على البعدين السياسي والاستخباراتي من خلال التأثير على الرأي العام، والتدخل في السياسات الداخلية والخارجية للدول الاخرى وتطوير أدوات جديدة لجمع المعلومات،

تُعد الولايات المتحدة رائدة في هذا المجال اذ ضمت استراتيجيات سيبرانية متطورة عززت من قدراتها على الهجوم الإلكتروني والمواجهة والتجسس، حيث أكد تقرير وزارة الدفاع الأمريكية (٢٠٢٣) أن " التفوق والتطور السيبراني هو جزء أساسي من حماية المصالح القومية الأمريكية وهذا يتطلب تكاملًا بين القدرات الاستخباراتية والهجومية والدفاعية[١٥]، ويُشير هذا التكامل إلى تحول الأمن السيبراني من مجرد آلية حماية تقني إلى أداة استراتيجية تُستخدم لتحقيق أهداف عدة منها سياسية واستخباراتية على الصعيد العالمي، من الجانب الاستخباراتي، الأمن

السيبراني اسهم في توسيع قدرات وكالات مثل وكالة الأمن القومي (NSA) ووكالة الاستخبارات المركزية (CIA) في مجال جمع المعلومات عبر الفضاء الرقمي، ومراقبة الخصوم والحلفاء على حد سواء والتنصت على الاتصالات، في عام ٢٠١٣ كشف تسريب لإدوارد سنودن ، حجم البرامج السيبرانية التي تستخدمها الولايات المتحدة الأمريكية للتجسس على زعماء دول ومؤسسات وشركات، مما أثار جدلاً واسعاً حول شرعية هذه الممارسات وانعكاساتها على العلاقات الدولية [١٦]،

أما من الناحية السياسية، فقد أصبح للأمن السيبراني دورا كبيرا و مباشرا في صياغة السياسات الداخلية والخارجية، من خلال حماية البنية التحتية للمؤسسات الديمقراطية من التدخلات الخارجية، ومثال ذلك ما حصل في الانتخابات الرئاسية الأمريكية عام ٢٠١٦، حيث اشارت التحقيقات الى وجود عدة محاولات اختراق روسي عبر الفضاء السيبراني، ونتيجة لهذه التهديدات المتعددة ، تمت إعادة تعريف مفهوم الأمن السياسي ليشمل (الاستقلال السيبراني) و (السيادة الرقمية) كأبعاد ضرورية في أي سياسة وطنية [١٧]، ان الولايات المتحدة الامريكية باتت تستخدم الأمن السيبراني كوسيلة للهيمنة والتأثيرالاستراتيجي، سواء عبر عمليات هجومية رقمية أو عبر دعم الحركات السياسية المؤيدة لها في دول أخرى وهذا يؤكد ان الولايات المتحدة لم تعد تنظر إلى الأمن السيبراني من زاوية دفاعية فقط، وبذلك يمكن القول أن الفضاء السيبراني قد تحول إلى ساحة حرب غير تقليدية تُمارَس فيها سياسات الضغط الناعم والخشن على حد سواء دون أن تُطلق رصاصة واحدة [١٨]، ضمن هذا السياق يمكن القول ان الاستراتيجية السيبرانية الأمريكية تعكس منظومة فكرية الهدف منها ترسيخ النفوذ الأمريكي في العالم الرقمي، مع مراعاة وضرورة تقليص مساحة الخصوم الاستراتيجيين مثل الصين وروسيا ، وبالتالي هذا البعد الفكري فسر تبني واشنطن لعقيدة "الردع السيبراني" التي تعتمد على بناء تحالفات سيبرانية مع الحلفاء و توجيه ضربات إلكترونية استباقية[١٩].

المطلب الثالث : الامن السيبراني واثره على البعد العسكري الامريكي .

أدى التطور الكبير في تكنولوجيا المعلومات والاتصالات خلال العقود الأخيرة إلى إدخال بُعد جديد في ميدان الصراعات العسكرية، يتمثل في الفضاء السيبراني كبيئة عملياتية موازية للبر والبحر والجو والفضاء الخارجي، وفي الولايات المتحدة، بات الأمن السيبراني جزءاً محورياً من العقيدة العسكرية الحديثة، حيث يُنظر إليه كأداة دفاع وهجوم على حد سواء، تسهم في تحقيق التفوق الاستراتيجي وضمان الهيمنة العسكرية في مواجهة القوى المنافسة، تشير وزارة الدفاع الأمريكية إلى أن القدرات السيبرانية أصبحت مدمجة بشكل كامل في العمليات العسكرية، وتشمل مهام جمع المعلومات الاستخباراتية، وحماية البنية التحتية العسكرية الحيوية وشن الهجمات الرقمية [٢٠]، وهذا يعني أن الأمن السيبراني لم يعد مجرد وسيلة مساندة، بل أصبح سلاحاً استراتيجياً بحد ذاته دون استخدام القوة التقليدية و قادرًا على تعطيل قدرات الخصوم أو شل أنظمتهم الدفاعية والهجومية من الناحية العملياتية، الأمن السيبراني اسهم في إنشاء قيادة القوات السيبرانية الأمريكية التي تم تأسيسها عام ٢٠١٠ لتكون الجهة المسؤولة عن ضمان التنسيق بين الجيش والاستخبارات في الفضاء الرقمي وكذلك تنفيذ العمليات السيبرانية الهجومية والدفاعية، وقد برز دور هذه القيادة في تأمين شبكات القيادة والسيطرة، وحماية الأقمار الصناعية المستخدمة في الاتصالات

والملاحة العسكرية التصدي للهجمات[٢١]، كما عملت الولايات المتحدة على استخدام قدراتها السيبرانية في عمليات هجومية استباقية، مثل العملية التي استهدفت البرنامج النووي الإيراني عبر فيروس "ستاكس نت) في ٢٠١٠ والتي أظهرت قدرة الحرب السيبرانية على إحداث تأثيرات مادية على البنية التحتية الصناعية والعسكرية للخصم ، وتدل هذه العملية على انتقال الأمن السيبراني من كونه أداة دفاعية إلى سلاح هجومي دقيق وفعال.

المبحث الثالث : تحليل مقومات الامن السيبراني الامريكي .

ويشكل الأمن السيبراني أحد المرتكزات الأساسية في حماية الأمن القومي الأمريكي في القرن الحادي والعشرين، حيث لم تعد التهديدات مقتصرة على الأبعاد العسكرية أو الاستخباراتية التقليدية، بل امتدت لتشمل الفضاء السيبراني الذي بات مجالاً حيويًا للصراع بين الدول والجهات الفاعلة من غير الدول. وانطلاقاً من هذا التحول، تبنت الولايات المتحدة مقاربة استراتيجية شاملة للأمن السيبراني، تقوم على مجموعة من المقومات المؤسسية والتشريعية والتقنية، والتي تهدف إلى تعزيز القدرة على الردع، والكشف المبكر، والاستجابة السريعة للهجمات الرقمية،

ويهدف هذا المبحث إلى تحليل المقومات الرئيسية التي تقوم عليها البنية السيبرانية الأمريكية، من خلال استعراض الإطار المؤسسي الذي يشمل الجهات الفاعلة مثل وكالة الأمن القومي وقيادة العمليات، إضافة إلى استعراض السياسات والتشريعات السيبرانية ذات الصلة، مثل قانون الأمن السيبراني لعام ٢٠١٥ والاستراتيجية الوطنية للأمن السيبراني ٢٠١٨ –٢٠٢٣ ، كما يتناول المبحث الردع السيبراني والتحديات الراهنة، وإن تحليل هذه المقومات لا يهدف فقط إلى فهم عناصر القوة السيبرانية الأمريكية، بل يسعى أيضاً إلى إبراز التفاعل الديناميكي بين المؤسسات والتكنولوجيا والقانون ضمن سياق جيوسياسي معقد، حيث تشكل الحرب السيبرانية أحد أهم ملامحه المستقبلية. يركز هذا المبحث على تحليل مقومات الأمن السيبراني الأمريكي، عبر التطرق للأبعاد المؤسسية والسياساتية التي تشكّل المنظومة السيبرانية الأمريكية ، وكيف تُدارهذه التحديات .

المطلب الاول : البنية المؤسسية للأمن السيبراني الأمريكي : تدار المنظومة السيبرانية الأمريكية عبر تشابك مؤسسي معقد بين الوكالات المدنية والعسكرية والاستخباراتية وابرزها .

١- **القيادة السيبرانية الامريكية :** تعد القيادة السيبرانية إحدى الركائز الأساسية في هيكلية الأمن السيبراني للولايات المتحدة، وهي مسؤولة عن تنفيذ العمليات العسكرية في الفضاء السيبراني، سواء كانت دفاعية أو هجومية ، وعملها تحت إشراف وزارة الدفاع الأمريكية أنشأت عام ٢٠٠٩، ودخلت الخدمة الفعلية عام ٢٠١٠، نتيجة لتزايد التهديدات السيبرانية التي أستهدفت القوات المسلحة الأمريكية والبنية التحتية الحيوية للدولة [٢٢]،

اما عن مهامها الأساسية فتمثلت في الدفاع عن شبكات وزارة الدفاع إضافة لتنفيذ عمليات هجومية لتعطيل أو تقييد قدرات الخصوم وكذلك عملها كساند للوكالات الفيدرالية مثل (وكالة الامن القومي ، وكالة الأمن السيبراني، أمن البنية التحتية) فضلا على ذلك دورها في ما يعرف بالردع السيبراني الاستباقي لمنع اي تهديد محتمل قبل

وقوعه [٢٣]، هيكلياً فقد تم رفعها الى قيادة موحدة عام ٢٠١٨ وترأسها جنرال في القوات المسلحة الذي يتولى في الوقت ذاته قيادة وكالة الأمن القومي وبالتالي تظهر عملية الدمج بين القدرات العسكرية والاستخباراتية ، ونتيجة لتعطيل عدد من العمليات المهمة مثل تعطيل شبكات تنظيم داعش، والقيام بعمليات هجومية استباقية ضد البنية التحتية للقرصنة الروسية خلال الانتخابات الأمريكية ٢٠١٨ –٢٠٢٠ اتسمت القيادة السيبرانية بأهميتها،

وبذلك يمكن القول ان استراتيجية الردع السيبراني الأمريكي في حالة تطور مستمر[٢٤]، وهذا لا يعني ان القيادة الأمريكية آمنه بل تواجه تحديات متعددة، أبرزها الغموض القانوني المرتبط بالعمليات السيبرانية العابرة للحدود ومن الصعب تحديد مصادر الهجمات بدقة، اضافة لذلك النقص النسبي في الكفاءات البشرية مقارنة بالتطورالسريع للتهديدات الرقمية[٢٥]،

٢ – **وكالة الأمن السيبراني وأمن البنية التحتية** : بهدف حماية البنية التحتية الحيوية، وتعزيز الجاهزية الوطنية ضد الهجمات السيبرانية، وتنسيق الاستجابة على المستوى الوطني تم انشاء هذه الوكالة و وكالة امن البنية التحتية عام ٢٠١٨ بموجب قانون إعادة تنظيم الأمن الداخلي الأمريكي، لوكالة الأمن السيبراني دور حاسم في تقييم المخاطر السيبرانية عبر كافة القطاعات الحكومية والأقتصادية، كما تقدم الدعم الفني والاستشاري للمؤسسات العامة والخاصة لمواجهة التهديدات المختلفة والمتزايدة، كما تعمل على أصدار التحذيرات المبكرة حول الثغرات السيبرانية، وتنسيق سرعة الأستجابة للطوارئ الرقمية، ونشر التوصيات الأمنية، من ابرز مهامها هو إدارة نظام الإنذار الوطني للأمن السيبراني الذي يربط ما بين القطاع الخاص والوكالات الفيدرالية [٢٦]، تواجه هذه الوكالة عدة تحديات رغم قدراتها، ومن هذه التحديات هو نقص الكفاءات البشرية، والتنسيق الفعال مع الولايات ذات السياسات المستقلة وكذلك الحاجة الملحه لتطوير أدوات الذكاء الاصطناعي في تحليل التهديدات [٢٧] .

٣– **وكالة الأمن القومي والدور السيبراني** : تُعد من أبرز الأجهزة الاستخباراتية المتخصصة في مجال الأمن السيبراني، لها دور محوري منذ تأسيسها عام ١٩٥٢ في جمع المعلومات الاستخباراتية الأجنبية وحماية الاتصالات الأمريكية [٢٨]، عززت الوكالة من قدراتها السيبرانية تزامناً مع تصاعد التهديدات الرقمية، وخصوصًا بعد إنشاء مديرية الأمن السيبراني عام ٢٠١٩ ، التي تركز على حماية الشبكات الوطنية والبنية التحتية الحيوية ، اما الوظائف السيبرانية الأساسية للوكالة فهي تطوير أنظمة التشفير الوطنية وتأمين الاتصالات الحكومية الحساسة، مشاركة المعلومات التقنية والاستخباراتية مع القطاعين العام والخاص عبر برامج مثل (مشاركة التهديدات السيبرانية) فضلا عن رصد التهديدات السيبرانية الأجنبية والتصدي لها قبل وصولها إلى الشبكات الأمريكية [٢٩]، تعد وكالة الامن القومي الذراع الاستخباراتية التي تغذي العمليات العسكرية السيبرانية بالبيانات الدقيقة حول البنية التحتية الرقمية للخصوم من خلال شراكتها مع القيادة السيبرانية الأمريكية [٣٠]، الوكالة لعبت دورا رئيسيًا في منظومة الأمن السيبراني الأمريكي رغم اثارة الجدل بعد تسريبات إدوارد سنودن عام ٢٠١٣، التي كشفت وعلى نطاق عالمي حجم عمليات التجسس الإلكتروني ، مما أدى إلى مراجعة العديد من القوانين المتعلقة بحماية الخصوصية، الا ان هذه الوكالة تمثل نقطة التقاء بين القدرات التقنية العالية والتحليل الاستخباراتي المتقدم، وهو

ما يجعلها محورية في الاستجابة للهجمات السيبرانية المتقدمة، بما فيها هجمات الدول ذات القدرات السيبرانية العالية كروسيا والصين [٣١] .

المطلب الثاني : الإطار التشريعي والتنظيمي للأمن السيبراني الأمريكي .

شهد هذا الإطار تطورًا كبيرًا منذ بداية الألفية الجديد وخاصة بعد هجمات ١١ سبتمبر ٢٠٠١، وما تبعها من إدراك استراتيجي لأهمية البنية التحتية الرقمية في الأمن القومي[٣٢]، يمثل الإطار التشريعي والتنظيمي للأمن السيبراني الأمريكي أحد الأعمدة الرئيسية في حماية الفضاء الرقمي الوطني، حيث يضم مجموعة من القوانين والسياسات الفيدرالية وكان ابرزها قانون الامن السيبراني لسنة ٢٠١٥ الذي نظم عمل الوكالات الأمنية وكذلك حدد مسؤوليات القطاعين العام والخاص في مواجهة التهديدات السيبرانية، يمثل الإطار التشريعي والتنظيمي للأمن السيبراني الأمريكي أحد الأعمدة الرئيسية في حماية الفضاء الرقمي الوطني، حيث يضم مجموعة من القوانين والسياسات الفيدرالية وكان ابرزها قانون الامن السيبراني لسنة ٢٠١٥ الذي نظم عمل الوكالات الأمنية وكذلك حدد مسؤوليات القطاعين العام والخاص في مواجهة التهديدات السيبرانية [٣٣]، ومن أبرز التشريعات والسياسات: (قانون أمن الفضاء السيبراني الفيدرالي لعام ٢٠٠٢ والمعدل في ٢٠١٤، الذي ينظم إدارة المخاطر السيبرانية في الوكالات الفيدرالية وحدد مسؤولياتها CISA Act لعام ٢٠١٨، الذي أنشأ وكالة)، (قانون تعزيز الأمن السيبراني التنظيمية)، (الأوامر التنفيذية الرئاسية، مثل الأمر التنفيذي رقم ١٤٠٢٨ الصادر عام ٢٠٢١، الذي يشدد على أهمية تحديث الدفاعات السيبرانية وتطبيق نموذج الثقة المعدومة في شبكات الحكومة الفيدرالية)، (استراتيجية الأمن السيبراني الوطنية ٢٠٢٣التي تمثل الإطار السياسي الأشمل، وتدعو إلى تحمل القطاع الخاص مسؤولية أكبر في حماية البنية التحتية الرقمية، وتشجيع التعاون الدولي في مواجهة التهديدات العابرة للحدود) [٣٤]،

المحور الأول : التهديدات السيبرانية التي تواجه الأمن القومي الأمريكي .

واجهت الولايات المتحدة الأمريكية طيفًا واسعًا من التهديدات السيبرانية المتعددة التي تؤثر بشكل مباشر على أمنها القومي، بدايةً من الهجمات التي تستهدف البنية التحتية الحيوية، ومرورًا بالتجسس الإلكتروني، وانتهاءً بحروب المعلومات وحملات التضليل المعلوماتي، اظهرت التقارير السنوية الصادرة عن الاستخبارات الأمريكية أن التهديدات السيبرانية تمثل واحدة من أخطر التحديات الأمنية في القرن الحادي والعشرين ومن اهم مصادر التهديد كالآتي [٣٥]،

١- الدول المعادية للجانب الأمريكي كروسيا، الصين، إيران وكوريا الشمالية، والتي عملت على توظيف أدوات الحرب السيبرانية كجزء من استراتيجيتها السياسية والعسكرية ومثال ذلك ، سبق وان تم توجيه الأتهام لروسيا بتنفيذ هجمات سيبرانية على شبكات الانتخابات الأمريكية للعام ٢٠١٦ -٢٠٢٠ ، بينما يُشتبه في قيام الصين بهجمات متطورة لسرقة البيانات الحساسة وكذلك سرقة الملكية الفكرية من المؤسسات الأكاديمية والبحثية.

٢- الجهات غير الحكومية كجماعات القرصنة الإلكترونية (هكرز) وهم افراد او جماعات تستخدم عدة تقنيات مختلفة من اجل تحقيق أهداف سياسية او اجتماعية ، وكذلك منظمات الجريمة السيبرانية التي تستخدم هجمات

الفدية وقرصنة البيانات لتحقيق مكاسب مالية ومن الملاحظ ان هذه الهجمات باتت تمثل خطراً مباشراً على البنية التحتية الحيوية و قد تزايدت وتيرتها خلال جائحة كورونا [٣٦] .

٣- التهديدات الداخلية الصادرة من الموظفين السابقين أو العاملين الحاليين الذين يمتلكون صلاحيات دخول عالية ويقومون بتسريب أو استغلال البيانات لمصالحهم الخاصة ، وهو ما برز في حالة إدوارد سنودن عام ٢٠١٣ .

المحور الثاني : الردع السيبراني والسياسة الدفاعية الأمريكية في الفضاء الرقمي .

تعتبر الاستراتيجية الدفاعية السيبرانية للولايات المتحدة من الركائز الأساسية والمهمه في مواجهة التهديدات السيبرانية المتزايدة، ومن خلال القدرات السيبرانية العسكرية والاستخباراتية المتطورة يتم ردع تلك الهجمات السيبرانية، وقد تطورت هذه الاستراتيجية بشكل كبير في العقدين الماضيين خاصة مع تصاعد التهديدات من دول مثل روسيا والصين، التي تُستخدم فيها القدرات السيبرانية كأداة رئيسية في حروبها الحديثة [٣٧]،

الفرع الأول : مفاهيم الردع السيبراني :

يمكن القول ان الردع السيبراني هو إقناع الخصم بعدم اتخاذ أية خطوات هجومية في الفضاءالسيبراني من خلال تهديده بعواقب غير متكافئة ، يتمثل الردع في استراتيجيات متنوعة تتضمن

١- الردع الهجومي حيث قيام الولايات المتحدة الأمريكية بتنفيذ هجمات سيبرانية استباقية على الخصوم لإضعاف بنيتهم التحتية الرقمية قبل أن يتمكنوا من شن اي هجمات .

٢- الردع بالتكلفة تهدف الحكومة الأمريكية إلى جعل الهجمات السيبرانية ضدها مكلفة بما يكفي لردع العدو عن تنفيذها وخاصة اذا كان معلوم الطرف والجانب، من خلال تهديدات بعواقب مختلفة سياسية أو اقتصادية أو عسكرية .

٣- الاشتباك المستمراو الدفاع المستمر وهو احد الاستراتيجيات التي تطبقها القيادة السيبرانية الأمريكية لضمان أن تكون الولايات المتحدة في حالة استعداد دائم لمواجهة الهجمات السيبرانية (USCYBERCOM)*وإضعاف قدرة الخصم على تنفيذها او تقييدها [٣٨].

الفرع الثاني : السياسات الدفاعية الأمريكية :

نتيجة لتصعيد في الهجمات السيبرانية ادى إلى تعزيز السياسات الدفاعية الأمريكية، حيث تم تنفيذ مجموعة من المبادرات لتوجيه الردع السيبراني بشكل فعال ومنها :-

١- الأوامر التنفيذية الرئاسية مثل الأمر التنفيذي ١٣٨٠٠ الصادر في ٢٠١٧ والذي يحدد ملامح استراتيجية الأمن السيبراني الوطني .

٢- الاستراتيجية الوطنية للأمن السيبراني ٢٠٢٣ التي تدعو إلى اعتماد "الاستراتيجية السيبرانية الهجومية" والتي تتمثل في التصدي لأي من الهجمات الإلكترونية من خلال بناء قدرات هجومية للدفاع عن الأمن القومي .

٣- عدم القدرة في اتخاذ التصعيد المناسب لردع مناسب لحالة الهجوم السيبراني وقد يؤدي هذا التتصعيد الى نتائج غير مرضية او غير متوقعة [٣٩] .

ورغم هذه التحديات، تظل سياسة الردع السيبراني أحد الأدوات الفعالة في ردع الدول المعادية من استخدام الفضاء السيبراني كأداة لشن هجمات ضد الولايات المتحدة وحلفائها .

نتائج أثر الأمن السيبراني على الأمن القومي الأمريكي:

١- **حماية البنية التحتية الحيوية** : تعتمد الولايات المتحدة الامريكية بشكل واسع على شبكات رقمية معقدة لإدارة قطاعات الطاقة، النقل، الاتصالات، الصحة، والمال.، لذا أي اختراق سيبراني لهذه القطاعات قد يؤدي إلى تعطيل الخدمات الأساسية وشلّ الدولة، ما يجعله تهديدًا مباشرًا للأمن القومي.

٢- **التجسس والتهديدات الخارجية** : تستخدم دول منافسة (مثل الصين وروسيا وغيرها) التهديدات السيبرانية للتجسس على المؤسسات الأمريكية الدفاعية، الوكالات الحكومية وغير الحكومية، حي هذه التهديدات قد تكشف أسرارًا عسكرية وتقنية، مما يضعف القدرات الدفاعية للولايات المتحدة.

٣- **الإرهاب السيبراني** : قد تستغل الجماعات الإرهابية الفضاء الالكتروني للتخطيط، التجنيد، أو شنّ هجمات رقمية تستهدف شبكات حكومية أو اقتصادية، وهذا يشكل بعدًا جديدًا من التهديدات غير التقليدية.

٤- **التأثير الاقتصادي والأمني** : الهجمات السيبرانية على الأسواق المالية أو الشركات الكبرى قد تُلحق خسائر ضخمة وتؤثر على استقرار الاقتصاد الوطني، وهذا بدوره ينعكس على الأمن القومي باعتباره مرتبطًا بالقوة الاقتصادية.

٥- **الحروب السيبرانية** : أصبح الفضاء السيبراني ساحة مواجهة جديدة بين القوى الكبرى، يعد امتلاك قدرات سيبرانية هجومية ودفاعية يُعتبر عنصرًا أساسيًا في استراتيجية الأمن القومي الأمريكي.

٦- **التشريعات والسياسات** : دفعت التهديدات السيبرانية الولايات المتحدة إلى وضع استراتيجيات وطنية للأمن السيبراني، وإنشاء وحدات متخصصة داخل وزارة الدفاع ووكالات الاستخبارات، وكما أصبح التعاون مع الدول من الضروريا في مجال الفضاء السيبراني جزءًا مهمًا من السياسة الخارجية الأمريكية.

خاتمة :

يمكن القول وبشكل قطعي وواضح إن الفضاء الالكتروني ، يمثل اليوم أحد أهم المجالات الحيوية التي تؤثر بشكل مباشر على الأمن القومي الأمريكي، إذ لم يعد الصراع مقتصرًا على الميدان العسكري التقليدي، بل انتقل إلى الفضاء الرقمي مفتوح يتسم بالتعقيد والتشابك، فالتهديدات السيبرانية باتت تهدد البنى التحتية الحيوية، مثل شبكات الطاقة والاتصالات والأنظمة المالية، فضلًا عن دورها في التأثير على السياسة والاقتصاد والأمن الاجتماعي.،

ومن هنا، تسعى الولايات المتحدة إلى تعزيز قدراتها الدفاعية والهجومية في المجال السيبراني، وبلورة استراتيجيات متقدمة للتعامل مع المخاطر والتحديات، إن حماية الأمن القومي الأمريكي في العصر الرقمي تعتمد بشكل كبير على القدرة على الابتكار، والتعاون بين المؤسسات الحكومية والقطاع الخاص، إضافة إلى تعزيز الوعي المجتمعي بأهمية الأمن السيبراني وبالتالي، فإن مستقبل الأمن القومي الأمريكي سيظل مرتبطًا بمدى نجاحه في السيطرة على فضاء سيبراني دائم التطور والتغير الامن السيبراني .

الهوامش

[١] - ابراهيم محمد الحمامصة و فارس العمارات: الامن السيبراني (المفهوم وتحديات العصر)، دار الخليج للنشر والتوزيع، عمان، ص ١١.

[٢] - عبد الرحمن علي اللقاني : دور الامن السيبراني في تعزيز امن المعلومات المالية الالكترونية، دار اليازوري العلمية للنر والتوزيع، عمان، ٢٠٢١، ص ١٦١.

[٣] - إيهاب خليفة : الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، ٢٠٢١، ص ص ١٠٩ – ١١٦.

[٤] - مها شحادة : تأثيرأبعاد التحول الرقمي في النضج الرقمي للمصارف الإسلامية، مجلة الجامعة القاسمية للاقتصاد الاسلامي، المجلد ٢، العدد١، تصدر عن جامعة الشرق الأوسط، الأردن، يوليو ٢٠٢٢، ص ص ٧٣-٧٦.

[5] - Mark Dunkerley : Resilient Cyber security Reconstruct Your Defense Strategy in an Evolving Cyber World, Copyright, Packt Publishing, Birmingham, United Kingdom, 27 September 2024, p7.

[٦] - مريم عمر سعيد لطرش: دراسة درجة الوعي بالامن السيبراني لدى معلمي ومعلمات الحاسب الالي، المجلة الدولية للعلوم والتقنية، المجلد ٢، العدد ٣٣، تصدر عن الجمعية الليبية للبحوث والدراسات العلمية، ليبيا، يناير ٢٠٢٤، ص ٤.

[٧] - علي زياد العلي، وعلي حسين حميد: تكتيكات الحروب الحديثَة الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنر والتوزيع، مصر، ٢٠٢٢، ص ٤١.

[8] - John McAlaney ،Lara Anne Frumkin: Psychological and Behavioral Examinations in Cyber Security, IGI Global, Disseminator, Pennsylvania, United States, 2017, p 26.

[9] - Aaron Franklin Brantly: The Decision to Attack Military and Intelligence Cyber Decision-Making, University of Georgia Press – USA, 2016, P166.

[10] - Tobias Stærmose, Maria Papaioannou, Gaurav Choudhary and Nicola Dragoni: Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments, 2022, 123.

[11] - U.S. Government Accountability Office. Cybersecurity: Federal agencies need to implement recommendations to protect critical infrastructure (GAO-21-288). Washington, DC: U.S. Government Accountability Office. Retrieved from https://www.gao.gov/products/gao-21-288

[١٢] - المركز الاقليمي للأمن السيبراني، التحديات الاقتصادية للهجمات السيبرانية في الولايات المتحدة الامريكية ، تقرير تحليلي ، جامعة نايف للعلوم الامنية ، ٢٠٢٣.

[١٣] - عبد المجيد خالد . الأمن السيبراني وتأثيره على الاقتصاد العالمي ، المجلة العربية للأمن المعلوماتي ، العدد ١٠، ٢٠٢٢.

[١٤] - مركز الأهرام للدراسات السياسية والاستراتيجية ، التهديدات السيبرانية وتأثيرها على الاقتصاد العامي : الولايات المتحدة الأمريكية انموذجا ، سلسلة تقديرات استراتيجية ، العدد ٤٥, ٢٠٢٢.

[15]- U.S. Department of Defense. Cyber Strategy Summary,٢٠٢٣ , Retrieved from https://www.defense.gov.

[١٦] - علي محمود، الهجمات السيبرانية وتأثيرها على التوازن الدولي، المجلة الدولية للدراسات الأمنية ، العدد (١٩) ص١١٠-١٢٨،٢٠٢٣.

[١٧] - حسن السيد، السياسة الأمريكية للأمن السيبراني: تحليل استراتيجي، المجلة العربية للعلوم السياسية، العدد ٧٤، ص ٨٥-١٠٢، ٢٠٢٢.

[١٨] - علي محمود، مصدر سبق ذكره ، ص١١٢.

[١٩] - حسن السيد، المصدر اعلاه ، ص٨٨.

[20] - U.S. Department of Defense ,Cyber Strategy Summary,٢٠٢٣, Retrieved from https://www.defense.gov.

[21] - Lynn, W. J. Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs,2010, 89(5), 97–108.

[22]- Healey J (Ed),Afierce Domain :Conflict in Cyberspace 1986-،2012Cyber Conflict Studies Association ،U.S،2023.

[23] - Nye J. S. Cyber power ،Harvard Kennedy School ،2010.

[24] - Rid, T. Active measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux.2020،

[٢٥] - - مجلة السياسة الدولية , القيادة السيبرانية الأمريكية : بين الدفاع والردع ، السياسة الدولية ،مجلة الاهرام ، مصر ، العدد ٢٢٣، ٢٠٢١.

[26]- - Krekel, B. Infrastructure Cyber Defense and Sectoral Partnerships. RAND Corporation. Retrieved from https://www.rand.org.2020

[27] - Healey, J. (Ed.). (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012. Washington, DC: Cyber Conflict Studies Association.

[٢٨] - عبدالله حسين الشمري،الامن السيبراني في الاستراتيجية الامريكية:دراسة تحليلية، مجلة الأمن والدفاع، مركز الابحاث الاستراتيجية، العراق، العدد١٢، ٢٠٢١, ص ٨٥.

[٢٩] - خالد عبد الله السعيد، الهيمنة الامريكية في الفضاء السيبراني:الاجهزة والادوات، مجلة المستقبل العربي، مركز دراسات الوحدة العربية،العدد٥٠٢، ٢٠٢٢، ص٩١.

[30] - Nye, J. S. (2010). Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org.

[31] - - Libicki, M. C. Cyberspace in peace and war. Annapolis: Naval Institute Press ،U.S.A ,2017, P139.

[32] - Libicki, M. C. Cyberspace in peace and war. Annapolis: Naval Institute Press،2017, 422p.

[٣٣] - أحمد عبد الحميد الزبيدي، السياسات الامريكية في الفضاء السيبراني: قراءة تحليلية في التشريعات والممارسات، مجلة السياسة الدولية، مؤسسة الأهرام، العدد٢٢١، ص١١٢، ٢٠٢٠.

[34] - The White House ،National Cyber security Strategy (2023 Retrieved from https://www.whitehouse.gov.

[35] - ODNI Annual ،Threat Assessment of the U.S. Intelligence Community. Retrieved،٢٠٢٣، from https://www.dni.gov.

[٣٦] - علاء حسين محمود، التهديدات الجديدة للأمن القومي الأمريكي في ظل التحول نحو الفضاء السيبراني، مجلة العلوم السياسية، جامعة بغداد، العدد٦٦، ٢٠٢١، ص٨٨.

[37] - Thomas Rid. Active measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux, 2022, p 64.

* (USCYBERCOM) في ٢٠٢٣ اعلن الجنرال بول ناكاسوني قائد القيادة السيبرانية عن استراتيجية جديدة تحت شعار "امتلاك المجال" ضمت تحت طيتها ثلاث من المحاور الرئيسية وهي (تعزيز القوة العاملة ، تقوية ميزة الحرب السيبرانية وتفعيل عمل الشركاء جنبا لجنب) .

[38] - USCYBERCOM, Persistent Engagement and Strategic Cyber Defense, 2023, Retrieved from https://www.cybercom.mi.

[٣٩] - احمد عبد الحليم ,الاستراتيجية الأمريكية للأمن السيبراني ٢٠٢٣: قراءة في وثيقة الردع والهجوم الرقمي , مركز الأهرام للدراسات السياسية والاستراتيجية,٢٠٢٣، https://acpss.ahram.org.eg/News/17717.as

المصادر والمراجع:

- **باللغة العربية**

[١] – ابراهيم محمد الحمامصة وفارس العمارات: الامن السيبراني (المفهوم وتحديات العصر)، دار الخليج للنشر والتوزيع، عمان.

[٢] – عبد الرحمن علي اللقاني : دور الامن السيبراني في تعزيز امن المعلومات المالية الالكترونية، دار اليازوري العلمية للنر والتوزيع، عمان، ٢٠٢١.

[٣] – إيهاب خليفة : الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، العربي للنشر والتوزيع، القاهرة، ٢٠٢١، ص ص ١٠٩ – ١١٦.

[٤] – مها شحادة : تأثيرأبعاد التحول الرقمي في النضج الرقمي للمصارف الإسلامية، مجلة الجامعة القاسمية للاقتصاد الاسلامي، المجلد ٢، العدد١، تصدر عن جامعة الشرق الأوسط، الأردن، يوليو ٢٠٢٢.

[٥] – مريم عمر سعيد لطرش: دراسة درجة الوعي بالامن السيبراني لدى معلمي ومعلمات الحاسب الالي، المجلة الدولية للعلوم والتقنية، المجلد ٢، العدد ٣٣، تصدر عن الجمعية الليبية للبحوث والدراسات العلمية، ليبيا، يناير ٢٠٢٤.

[٦] – علي زياد العلي، وعلي حسين حميد: تكتيكات الحروب الحديثَة الأمن السيبراني والحروب المعززة والهجينة، دار العربي للنر والتوزيع، مصر، ٢٠٢٢.

[٧] – المركز الاقليمي للأمن السيبراني، التحديات الاقتصادية للهجمات السيبرانية في الولايات المتحدة الامريكية ، تقرير تحليلي ، جامعة نايف للعلوم الامنية ، ٢٠٢٣.

٨ – عبد المجيد خالد . الأمن السيبراني وتأثيره على الاقتصاد العالمي ، المجلة العربية للأمن المعلوماتي ، العدد ١٠، ٢٠٢٢.

٩ – مركز الأهرام للدراسات السياسية والاستراتيجية ، التهديدات السيبرانية وتأثيرها على الاقتصاد العامي : الولايات المتحدة الأمريكية انموذجا ، سلسلة تقديرات استراتيجية ، العدد ٤٥, ٢٠٢٢.

١٠ – علي محمود، الهجمات السيبرانية وتأثيرها على التوازن الدولي، المجلة الدولية للدراسات الأمنية ، العدد (١٩) ٢٠٢٣.

١١– حسن السيد، السياسة الأمريكية للأمن السيبراني: تحليل استراتيجي، المجلة العربية للعلوم السياسية، العدد ٧٤، ٢٠٢٢.

١٢ – مجلة السياسة الدولية , القيادة السيبرانية الأمريكية : بين الدفاع والردع ، السياسة الدولية ،مجلة الاهرام ، مصر ، العدد ٢٢٣، ٢٠٢١.

١٣ – عبدالله حسين الشمري،الامن السيبراني في الاستراتيجية الامريكية:دراسة تحليلية، مجلة الأمن والدفاع، مركز الابحاث الاستراتيجية، العراق، العدد١٢، ٢٠٢١.

١٥ – خالد عبد الله السعيد، الهيمنة الامريكية في الفضاء السيبراني:الاجهزة والادوات، مجلة المستقبل العربي، مركز دراسات الوحدة العربية،العدد٢، ٢٠٢٢.

١٦– أحمد عبد الحميد الزبيدي، السياسات الامريكية في الفضاء السيبراني: قراءة تحليلية في التشريعات والممارسات، مجلة السياسة الدولية، مؤسسة الأهرام، العدد٢٢١، ٢٠٢٠.

١٧– علاء حسين محمود، التهديدات الجديدة للأمن القومي الأمريكي في ظل التحول نحو الفضاء السيبراني، مجلة العلوم السياسية، جامعة بغداد، العدد٦٦، ٢٠٢١،.

- **مصادر باللغة الانكليزية .**

[39] - Mark Dunkerley : Resilient Cyber security Reconstruct Your Defense Strategy in an Evolving Cyber World, Copyright, Packt Publishing, Birmingham, United Kingdom, 27 September 2024.
[2] - John McAlaney ،Lara Anne Frumkin: Psychological and Behavioral Examinations in Cyber Security, IGI Global, Disseminator, Pennsylvania, United States, 2017.

3 - Aaron Franklin Brantly: The Decision to Attack Military and Intelligence Cyber Decision-Making, University of Georgia Press – USA, 2016.
4 - Tobias Stærmose, Maria Papaioannou, Gaurav Choudhary and Nicola Dragoni: Deepfake-Driven Social Engineering: Threats, Detection Techniques, and Defensive Strategies in Corporate Environments, 2022.
[5] - Lynn, W. J. Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Affairs,2010, 89(5), 97–108.
[6]- Healey J (Ed),Afierce Domain :Conflict in Cyberspace 1986-،2012Cyber Conflict Studies Association ،U.S،2023.
[7] - Nye J. S. Cyber power ،Harvard Kennedy School ،2010.
[8] - Rid, T. Active measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux.2020،
[9] - Healey, J. (Ed.). (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012. Washington, DC: Cyber Conflict Studies Association.

10 - Libicki, M. C. Cyberspace in peace and war. Annapolis: Naval Institute Press ،U.S.A , 2017.
11- Thomas Rid. Active measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux, 2022, p 64.

المواقع الالكترونية :

[39] - U.S. Government Accountability Office. Cybersecurity: Federal agencies need to implement recommendations to protect critical infrastructure (GAO-21-288). Washington, DC: U.S. Government Accountability Office. Retrieved from https://www.gao.gov/products/gao-21-288
2 - U.S. Department of Defense. Cyber Strategy Summary,٢٠٢٣ , Retrieved from https://www.defense.gov.
3 - U.S. Department of Defense ,Cyber Strategy Summary,٢٠٢٣, Retrieved from https://www.defense.gov.
4 -- Krekel, B. Infrastructure Cyber Defense and Sectoral Partnerships. RAND Corporation. Retrieved from https://www.rand.org.2020.
5 - Nye, J. S. (2010). Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs. Retrieved from https://www.belfercenter.org
6 - The White House ،National Cyber security Strategy (2023 Retrieved from https://www.whitehouse.gov.
7 - ODNI Annual ،Threat Assessment of the U.S. Intelligence Community. Retrieved، 2023، from https://www.dni.gov.
8 - The White House ،National Cyber security Strategy (2023 Retrieved from https://www.whitehouse.gov.
9 - ODNI Annual ،Threat Assessment of the U.S. Intelligence Community. Retrieved،٢٠٢٣، from https://www.dni.gov.
10 - USCYBERCOM, Persistent Engagement and Strategic Cyber Defense, 2023, Retrieved from https://www.cybercom.mi.
[11] - احمد عبد الحليم ,الاستراتيجية الأمريكية للأمن السيبراني ٢٠٢٣: قراءة في وثيقة الردع والهجوم الرقمي , مركز الأهرام للدراسات السياسية والاستراتيجية,٢٠٢٣، https://acpss.ahram.org.eg/News/17717.as