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

تاريخ استلام البحث ٢٣ / ٨ / ٢٠٢٤
تاريخ قبول البحث ٢٦/ ١٢ / ٢٠٢٤
تاريخ النشر ٣٠ / ٣ / ٢٠٢٥

الهجمات الإلكترونية وانعكاساتها على الأمن السيبراني في الولايات المتحدة الأمريكية

Cyber attacks and their implication for cyber security in the United State of America

م.د.اياد طارق عبد المجيد

D.Ayad Tariq Abdul majeed

جامعة تكنولوجيا المعلومات والاتصالات

University of Information Technology and Communications

dina.hatif@cis.uobaghdad.edu.iq

IRAQI Academic Scientific Journals

https://www.iasj.net/iasj/journal/393/issues

الملخص

اضحت الهجمات الإلكترونية تشكل خطر كبير على الأمن السيبراني في ساحة التفاعلات العالمية المعاصرة, ولما كانت الهجمات الإلكترونية ذات طابع عالمي فإن لضمان الأمن السيبراني أهمية كبيرة على المستوى الوطني والاقليمي والدولي, وقد اصبحت الإستراتيجيات الوطنية للأمن السيبراني أكثر أهمية بالنسبة لأي دولة, وفي هذا إلاطار نجد ان الولايات المتحدة الأمريكية تعمل على تعزيز وتطوير استراتيجيتها للأمن السيبراني في ظل تنامي الهجمات الإلكترونية المتزايدة على أمنها.

الكلمات المفتاحية : "الهجمات الإلكترونية", "الأمن السيبراني", "الولايات المتحدة الأمريكية"

Abstract

Cyber attacks have become a major threat to cyber security in the arena of contemporary global interactions. And since cyber attacks are global in nature, ensuring cyber security is of great importance at the national, regional and international levels. National cyber security strategies have become more important for any country. And in this The Framework, we find that the United States of America is working to enhance and develop its cyber security strategy in light of the increasing cyber attacks on its security.

Keywords: "cyber attacks", "cyber security", "United States of America"

المقدمة

يعالج هذا البحث مسالة التغير في مفهوم الهجمات الإلكترونية الحاصلة بسبب التقدم الواسع في الوسائل التكنولوجية وأنظمة الاتصالات والمعلومات, إذ اصبحت قضية الأمن السيبراني من التحديات الكبرى التي تواجهها الدول على الصعيدين الاقليمي والعالمي لاسيما مع تزايد حجم الهجمات الإلكترونية, التي باتت تشكل تهديد للأمن السيبراني كونها لاتحتاج الى كلفة عالية أو انها غالبا ما تكون مجهولة المصدر, التي فرضت على على الدول مواجهتها و لاسيما الدول الكبرى مما يؤدي الى اختراق أمنها الوطني. اذ سيتم التركيز في هذه الدراسة على التصورات الأمريكية في مجابهة مخاطر الهجمات الإلكترونية التي أصبحت احد التحديات الرئيسية للأمن السيبراني, والسعي لدرء هذه المخاطر وتداعياتها عبر تكييف المنظومة الأمنية مع تصاعد حدة الهجمات الإلكترونية التي أصبحت بشكل غير مسبوق من أكثر القضايا أهمية والحاحاً بالنسبة للأمن القومي, ولذلك وجب ضرورة تعزيز إستراتيجية الأمن والدفاع الأمريكية مع الاخذ بأن الأمر أصبح لا يتعلق بمواجهة طرف مماثل بل افراد وجماعات غير خاضعة لأي سلطة مما يتطلب اجراءات أكثر صرامة لمواجهة التهديدات الإلكترونية, حسب درجة خطورتها, والتركيز في بناء المنظومة الأمنية السيبرانية على احتمال ماسيقوم به الفاعلون لمجابهة الخطر القائم والتعاطي مع هذه التهديدات الإلكترونية وفق منطق التوقع والاحتمال.

أهمية البحث: تنبثق اهمية البحث في تسليط الضوء على الهجمات الإلكترونية التي اخذت تتزايد في الاونة الاخيرة, وأصبح من الصعب تحديد الجهة التي صدرت عنها هذه الهجمات اذ أن واقع تلك الهجمات بات أكثر

تعقيداً باتساع مطالب الأمن, وتكمن أهمية هذا البحث في كونه يعالج موضوع حديث ما يزال في طور التبلور ويسلط الضوء على مفهوم هذه الهجمات وطبيعتها الاستثنائية.

اهداف البحث: يهدف البحث الى وصف وتفصيل الهجمات الإلكترونية وتداعياتها على الأمن السيبراني الأمريكي ومدى قدرة الولايات المتحدة في مجابهة تنامي الهجمات الإلكترونية لمختلف القطاعات العامة والخاصة, والعمل على ايجاد برامج متطورة في الأمن السيبراني لحمايتها من الحروب والتجسس الإلكتروني والحفاظ على سريتها من القرصنة الإلكترونية, والمساومات, وعمليات المنافسة.

إشكالية البحث: إن الإشكالية التي سنسعى لمقاربتها من خلال هذا البحث تتحدد أساسا بمفهوم الهجمات الإلكترونية وحدود تلك الهجمات التي يمكن أن تحدثه على الأمن السيبراني في الولايات المتحدة الأمريكية من خلال الاجابة عن التساؤل الرئيس الاتي:

ما مدى تأثير الهجمات الإلكترونية على الأمن السيبراني في الولايات المتحدة الأمريكية؟

وينبثق من السؤال الرئيس الاسئلة الفرعية الاتية:

١. ماهي الهجمات الألكترونية؟
٢. ماهو الأمن السيبراني؟
٣. ماهي اهداف ومؤسسات الأمن السيبراني في الولايات المتحدة الأمريكية؟
٤. ماهي إستراتيجية الأمن السيبراني الولايات المتحدة الأمريكية؟
٥. ماهي تداعيات الهجمات الإلكترونية على إستراتيجية الأمن السيبراني في الولايات المتحدة الأمريكية؟

فرضية البحث: ينطلق البحث من فرضية مفادها "ان تزايد حدة الهجمات الإلكترونية واتساع نطاقها على البنية التحية الحيوية الحرجة في الولايات المتحدة الأمريكية دفعتها لمواجهة المخاطر وتداعياتها بتعزيز الأمن السيبراني وتطوير الاستراتيجية الأمريكية للأمن القومي".

منهجية البحث: يعتمد هذا البحث على المنهج الوصفي والتحليلي بما يتناسب مع طبيعة البحث ومتطلباته للوصول الى تحقيق الطموحات المنشودة في دراسة وبيان الهجمات الإلكترونية وانعكاساتها على الأمن السيبراني في الولايات المتحدة الأمريكية.

هيكلية البحث: تم تقسيم هيكلية البحث الى خمسة محاور فضلا عن المقدمة والخاتمة والاستنتاجات وكما يلي:

المحور الاول: مفهوم الهجمات الإلكترونية

أولاً: تعريف الهجمات الإلكترونية

لا يوجد ثمة اتفاق بين الباحثين على تعريف محدد حول مفهوم الهجمات الإلكترونية, وذلك لتشابك طبيعتها, وتعقيدها, ولهذا , فسيتم استعراض أهم تلك التعريفات فقد عرفت الهجمات الإلكترونية بأنها "وسيلة قتالية من خلال استخدامها بذاتها للتسلل الى أنظمة إلكترونية, معدة لحماية أو لتنظيم سير عمل منشات حيوية, كمحطات توليد الطاقة النووية, أو السدود, أو وسائل النقل كالمطارات, بهدف تطويعها والسيطرة عليها, لتدمير ذاتها بذاتها عبر

تغذيتها بمعلومات غير صحيحة لأجهزة التحكم والحماية الإلكترونية"(١). وعرفها بعض الباحثين بأنها "فعل يقوض من قدرات وظائف شبكة الكمبيوتر, لغرض قومي أو سياسي من خلال استغلال نقطة ما يمكن للمهاجم من التلاعب بالنظام"(٢). بينما هناك من عرف الهجمات الإلكترونية على أنها "هجوم عبر الانترنت يقوم على التسلل الى مواقع إلكترونية غير مرخص الدخول اليها من أجل تعطيل البيانات المتوفرة فيها, أو إتلافها, أو الاستحواذ عليها"(٣). وقد عرفت القيادة الاستراتيجية الأمريكية الهجمات الإلكترونية بأنها "تطويع نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها, فضلاً عن التسلل الى أنظمة المعلومات وشبكات الاتصال, بهدف جمع وحيازة وتحليل البيانات التي تحتويها"(٤).

ثانياً: نشأة الهجمات الإلكترونية

ترتبط الهجمات الإلكترونية مباشرة بحدثين مهمين: الحدث الأول: باستحداث أجهزة الكمبيوتر في منتصف الخمسينات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً, وقد تطورت بصورة جذرية في العقود اللاحقة, حتى أصبح جهاز الكمبيوتر, أساساً في عمل الكثير من المؤسسات الخاصة والعامة, فضلاً عن الحياة اليومية للأفراد. أما الحدث الثاني: يتمثل بظهور الشبكة العنكبوتية والذي أحدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل البيانات المرسلة عبر الاثير(٥).

هذا وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري وذلك في مطلع التسعينات من القرن المنصرم حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة أو سباق التسلح السيبراني. أما في مرحلة ما بعد التسعينات وبداية الالفية فقد تطورت هذه الهجمات بنحو أوسع, وتم استخدام المعلومات في الإرهاب المنظم ومن طرف الدول أيضاً, عبر ضرب البنى التحتية للدول الأخرى سواء أكانت مرافق عامة أم خدمات البنى العسكرية والاقتصادية وغيرها(٦). في عام ٢٠٠٣ أصدر دانون فرنون وهو أحد أعضاء جهاز المخابرات الأمريكية كتابا بعنوان (الثلج الاسود التهديد الخفي للارهاب المعلوماتي) عرض فيه نوع المخاطر التي يمكن أن تهدد العالم في المستقبل القريب, نتيجة اختراق أنظمة المعلومات المتوافرة لدى الحكومات والمؤسسات المالية والشركات الاقتصادية الكبرى, واستخدامها في تدمير البنية التحتية الإلكترونية التي تعتمد عليها الدول(٧). وتشير العديد من التقارير الى تزايد أعداد الهجمات الإلكترونية التي تقوم بها مجموعات أو حكومات تتدرج في الاستهداف من أبسط المستويات الى أكثرها تعقيداً وخطورة, وأن الواقع يثبت أن عدداً من الدول كانت ضحايا لهجمات إلكترونية وبدرجات متفاوتة من حيث الشدة والضرر(٨).

ويجمع الخبراء على أن الهجوم الإلكتروني الذي استهدف استونيا في عام ٢٠٠٧, يكاد يكون الهجوم الإلكتروني الاول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والأعلامية, وعلى الرغم من أن الشكوك كانت تحوم حول روسيا على اعتبار ان الهجوم جاء بعد فترة قصيرة من خلاف إستوني- روسي كبير, إلا أن أحداً لم يستطيع أن يحدد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم, وهي من المصاعب والمشاكل التي ترتبط بحروب الانترنت الى الان(٩).

وكذلك النزاع بين روسيا وجورجيا عام ٢٠٠٨, إذ لجأت روسيا الى الهجمات الإلكترونية بهدف تعطيل أنظمة الاتصالات للقوات الجورجية واسهمت في اضعاف وسائل الدفاع الجوية, فضلا عن تعرض مواقع حكومية رسمية في البنية التحتية الجورجية للتعطيل(١٠). وتبقى الضربة الإلكترونية الأمريكية للهجوم على البرنامج النووي الإيراني للتأثير على عمليات التخصيب وأجهزة الطرد المركزي في منشأت الطاقة النووية الإيرانية من خلال فيروس "ستكسنت" في عام ٢٠١٠, هي الاخطر على صعيد الهجمات الإلكترونية لمنشأت مدنية أو عسكرية(١١).

وأجرت كوريا الشمالية في عام ٢٠١٤ هجوماً إلكترونياً ضد خوادم تابعة لشركة سوني في الولايات المتحدة الأمريكية, وادى الهجوم عند حدوثه الى تعطيل شبكة الشركة, وتم اختراق المعلومات السرية للشركة, فضلا عن الطبيعة المدمرة للهجمات, سرقت كوريا الشمالية نسخاً رقمية لعدد من الافلام التي لم يتم اطلاقها من قبل الشركة, كما سرقت الاف المستندات التي تحتوي على بيانات شخصية لموظفي الشركة, وكانت تلك الهجمات الإلكترونية من أكثر الهجمات تهديدا للولايات المتحدة الأمريكية ودفعت الى مزيد من النقاشات حول طبيعة الهجمات والحاجة الى تحسين الأمن السيبراني(١٢).

وعلى نحو مماثل توالت الهجمات الإلكترونية من قبل الصين للولايات المتحدة ومن قبل روسيا للولايات المتحدة, اذ نفذت الصين في عام ٢٠١٥ اختراق الكتروني لشبكات تابعة لمكتب ادارة شؤون الموظفين الأمريكي وسرقت ملفات تعود الى نحو مليونين موظف اتحادي سابق أو متقاعد وموظف حالي, بما في ذلك معلومات تعود لتصاريح أمنية سرية, ولكن الابرز جاء في عام ٢٠١٦ في الاتهام الروسي بالتدخل في الانتخابات الرئاسية الأمريكية لتشكل أزمة ودعوة للاستيقاظ لمواجهة الهجمات الإلكترونية(١٣).

ثالثاً: وسائل الهجمات الإلكترونية

تأتي الهجمات الإلكترونية على عدة اشكال وسيتم توضيح أبرز الوسائل التي تعد أسلحة للهجمات الإلكترونية والتي تعد أكثر استخداماً على الساحة الدولية وهي كالاتي:

١-**القنابل المنطقية:** وتعد برنامج ينفذ في لحظة محددة, أو في فترة زمنية منتظمة, ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام, لغرض تسهيل تنفيذ العمل غير المشروع, كادراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محلاً للاعتداء, كان تسعى قنبلة منطقية للبحث عن الحرف (A), في أي سجل يتضمن أمراً بالدفع, وعندما تكتشفه, تتحرك متتالية منطقية تعمل على ازالة هذه الحرف من السجل(١٤).

٢-**هجمات حجب الخدمة:** وتتم بإغراق المواقع بسيل من البيانات غير اللازمة, التي يجري إرسالها ببرامج متخصصة تعمل على نشرها, فتؤدي الى بطء في الخدمات أو ازدحام في المرور على هذه المواقع, فيصعب بالتالي وصول المستخدمين إليها(١٥).

٣-**الفايروسات:** وهي مجموعة من التعليمات المرمزة, التي تنتج لنفسها نسخاً مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات, لتقوم في مرحلة محمية بالتحكم في اداء النظام الذي أصابته, وقد عرفها المركز القومي للحاسب الالي في الولايات المتحدة الأمريكية بأنه" برنامج مهاجم يصيب أنظمة الحاسبات, بأسلوب يماثل الى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان, حيث يقوم هذا البرنامج بالتجول في الحاسب الالي باحثاً عن برنامج غير

مصاب, وعندما يجد أحدهما ينتج نسخة من نفسه لتدخل فيه, حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس, ومن أهم خصائصه قدرته على الاختفاء, والانتشار, والاختراق, وقدرته على تدمير نظام الحاسب الالي بأكمله"(١٦).

٤-**التجسس الإلكتروني:** وتعني القيام بالتنصت على شبكات الخصم, لجمع معلومات سرية, بغض النظر عن الاهداف, فالتجسس قد يهدف الى تعطيل عمل الشبكات العنكبوتية وحواسيبها وانظمتها بغية سرقة معلومات اقتصادية, أو سياسية, أو عسكرية من دولة ونقلها الى دولة اخرى, فالتجسس السيبراني تعتبر من الاساليب التي تلجأ اليها التنظيمات الاجرامية والإرهابية لجمع معلومات حول المؤسسات والقطاعات الحكومية ليتم استخدامها من الاضرار بالمجتمع ومصالحه(١٧).

المحور الثاني: مفهوم الأمن السيبراني

اولاً: تعريف الأمن السيبراني

يعد مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للاهتمام والدراسة, حيث عرف تعدداً في التعريفات المقدمة والتي يمكن ابرازها فيما يلي:

يعرف الأمن السيبراني بأنه "مجموعة الاجراءات التقنية والأطر القانونية والتنظيمية التي يتم وضعها من قبل الأجهزة الأمنية للمحافظة على سرية المعلومات الإلكترونية, وتعد جهوداً مشتركة ما بين القطاع العام والخاص والجهود المحلية والدولية, بهدف حماية الفضاء السيبراني والعمل على توفير أنظمة معلومات رقمية , بخصوصية عالية, مقومة للاختراقات الفيروسية وتتمتع بسرية عالية"(١٨).

فقد عرفه ريتشارد كمرر على أنه " عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة "(١٩). بينما يعرفه ادوارد أمورسو على أنه " وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات, وتشمل تلك الوسائل الادوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة"(٢٠).

وقد جاء تعريف الأمن السيراني في تقرير الاتحاد الدولي للاتصالات بعنوان (اتجاهات الاصلاح في الاتصالات لعام ٢٠١٠-٢٠١١) هو "مجموعة من المهمات, مثل تجميع وسائل وسياسات, واجراءات أمنية, ومبادى توجيهية, ومقاربات لادارة المخاطر, وتدريبات, وممارسات فضلى, وتقنيات, يمكن استخدامها لحماية البيئة السيبرانية, وموجودات المؤسسات والمستخدمين". وتهدف الحماية الى جعل المعتدين يحجمون عن خططهم, أو منعهم من تحقيقها, والى ضمان حد مقبول من الأخطار, وذلك عبر وضع خطة تتلائم والمحيط التقني, البشري, التنظيمي, والقانوني(٢١). وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فعرفته على أنه "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها الإلكترونية, من مختلف الجرائم , الهجمات, التخريب, التجسس والحوادث"(٢٢).

ثانياً: ابعاد وفواعل الأمن السيبراني

يرتبط الأمن السيبراني بمجالات مختلفة ومتعددة تهدف الى تحقيق منظومة أمن متكاملة تعمل بالحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية, ومن أهم الابعاد الإستراتيجية التي تعمل الدولة على تحصينها من الهجمات الإلكترونية, وهي كالاتي.

١- البعد العسكري

لقد كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد الى الأوساط الاكاديمية، والعلمية, تمثلت من أبحاث تخدم القدرات العسكرية، التي تسهم في تفوق بلد على آخر، حيث كان التنافس على أشده، بين الاتحاد السوفياتي(السابق)، والولايات المتحدة الأميركية، في مجال الوصول الى الفضاء الخارجي، وتطوير الأسلحة النووية مهمين(٢٣).

ويتجسد هذا البعد في توظيف الأمن السيبراني في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية بالشكل الذي يؤمن تبادل المعلومات وتدفقها, وسرعة اتخاذ القرارات العسكرية, ومن ثم تحقيق الاهداف عن بعد, ومن دون شك فأنها تشكل كذلك نقطة ضعف, لاسيما إذا لم تكن مؤمنة من الاختراق, الذي قد يؤدي الى تدمير قواعد البيانات العسكرية, أو قطع الاتصال بين القيادة والوحدات العسكرية, فضلا عن إمكانية التحكم في بعض الاسلحة وخروجها عن السيطرة(٢٤).

٢- البعد الاجتماعي

تعتبر الشبكة الدولية للمعلومات مجالا مفتوحا لجميع الأفراد, حيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية, إذ تغطي التحديات والمخاطر, وتدابير الأمن والتدابير الرادعة, لاجل تثقيف جميع الافراد السيبرانيين للتعاطي مع عمليات الأمن السيبراني(٢٥).

٣- البعد السياسي

يتمثل البعد السياسي للأمن السيبراني، بشكل أساسي، في حق الدولة في حماية نظامها السياسي، وكيانها، ومصالحها الاقتصادية، التي تعني حقها وواجبها في السعي الى تحقيق رفاه شعبها، في وقت تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، إذ أصبح بامكان الفرد، ان يتحول الى لاعب أساسي في اللعبة السياسية, كما أصبح بامكانه الاطلاع على خلفيات ومبررات القرارات السياسية، التي تتخذها حكومته، عبر الكم الهائل من المعلومات(٢٦).

ويعد التدخل الروسي السيبراني في الانتخابات الرئاسية الأمريكية لعام ٢٠١٦ أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي, إضافة الى التسريبات المختلفة للوثائق الحساسة والاختراقات التي غالباً ما تؤدي الى أزمات دبلوماسية بين الدول(٢٧).

٤- البعد الاقتصادي

يرتبط الأمن السيبيراني، ارتباطاً وثيقاً بالاقتصاد فقد توسع استخدام تقنيات المعلومات والاتصالات، كماً بالقيمة التي تمثلها البيانات والمعلومات المتداولة، والمخزنة، والمستخدمة، على كل المستويات, كذلك، تتيح تقنيات المعلومات والاتصالات، تعزيز التنمية الاقتصادية لدول كثيرة، عبر إفادتها، من فرص الاستخدام، التي تقدمها

الشركات الدولية الكبرى، التي تبحث عن إدارة كلفة انتاجها بافضل الشروط, بالاضافة الى دخول العالم، عصر المال الإلكتروني، ضمن بيئة تقنية متحركة بعد اطلاق الخدمات الإلكترونية، فالأمن السيبراني، يضمن تقديم الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الاقبال عليها، بما يترجم عملياً، بتطوير أسس اقتصاد سليم(٢٨).

٥- البعد القانوني

ينطوي البعد القانوني على إن التطورات التكنولوجية المتسارعة, تفرض مواكبة التشريعات القانونية لها, من خلال وضع أطر وتشريعات للاعمال القانونية وغير القانونية في الفضاء السيبراني, فالملاحظ ان الفعل السيبراني يفتقد في معظم الحالات والبلدان أطراً قانونية صارمة للتعامل معها, فضلا عن ضرورة تفعيل التعاون الدولي المشترك لمكافحتها (٢٩).

أما الفواعل في الأمن السيبراني فان جوزيف.س.ناي يحدد أنواع من الفاعلين الذين يمتلكون القدرة على الفعل السيبراني أو شن الهجمات الإلكترونية وهي كالاتي(٣٠):

١-**الدولة:** تعد الدولة الفاعل المحوري والاكثر قوة على تنفيذ هجمات إلكترونية و تطوير البنية التحتية وممارسة السلطات داخل حدودها لما لها من مكانة على أساس التفوق التكنولوجي.

٢-**الفواعل من غير الدول:** ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس, ويشمل هذا النوع من الفاعلين:

أ-**الافراد القراصنة:** وهم الافراد الذين لديهم معرفة تكنولوجية ذات كفاءة عالية في القدرة على توظيفها, وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم, على اختلاف توجهاتهم, ومن الصعب ملاحقتهم.

ب-**الشركات متعددة الجنسية:** تمتلك هذه الشركات تكنولوجيا موارد للقوة تفوق قدرة بعض الدول، فخوادم الشركات مثل كوكل, وفيسبوك, ومايكروسوفت, وغيرها تسمح لها بامتلاك قواعد البيانات العملاقة التي تمكنها من التأثير المباشر في اقتصاديات الدول وفي ثقافة المجتمعات.

ج-**المنظمات الاجرامية:** تقوم هذه الجماعات الإجرامية المنظمة بعمليات القرصنة السيبرانية أو سرقة المعلومات والتجسس الإلكتروني واختراق الحسابات المصرفية والاحتيال المالي، كما توجد سوق سوداء على شبكة الانترنيت المظلم لتجارة المخدرات والأسلحة والإتجار بالبشر.

د- **المجموعات الارهابية:** تعد ضمن ابرز الفواعل خاصة بعد احداث ١١ ايلول لعام ٢٠٠١ , إذ بدأ التركيز على الفضاء السيبراني في عملياتها كتهديد أمني جديد, وبالرغم من ذلك فأنها لم تصل بعد الى مرحلة القيام بهجمات إلكترونية حقيقية على منشأت البنية التحتية الحيوية للدول.

ثالثاً: عناصر الأمن السيبراني

يتم التعبير عن النهج الناجح للأمن السيبراني في شكل حماية متعددة المستويات تغطي أجهزة الكمبيوتر والشبكات والبرامج والبيانات التي تحتاج الى تأمين, ويجب ان يكمل الموظفون وسير العمل والتقنيات بعضهم

البعض في المؤسسات لتوفير حماية فعالة ضد الهجمات الإلكترونية التي تتعرض لها الدول اذ ان هناك عناصر رئيسية يستند عليها الأمن السيراني(٣١):

١-**الاشخاص:** ينبغي على المستخدمين فهم المبادىء الأساسية للأمن السيبراني والالتزام بها, من اختيار كلمات مرور قوية, والاهتمام بمرفقات البريد الإلكتروني, والنسخ الاحتياطي للبيانات.

٢-**العمليات:** يجب على المؤسسات تطوير مجموعة من التدابير الأساسية لمواجهة الهجمات المستمرة, وبالامكان الاسترشاد بمجموعة من التدابير الموثوقة التي توضح كيفية تحديد الهجمات وحماية الأنظمة وتحديد التهديدات والتصدي للهجمات.

٣-**التكنولوجيا:** تتمثل في تزويد المؤسسات والافراد بالادوات التي يحتاجونها للدفاع ضد عمليات الاختراق السيبراني والتنصت الإلكتروني لاسيما وان ابرز الأجهزة المعرضة للهجمات السيبرانية تكون بحاجة ماسة الى الحماية, كأجهزة الكمبيوتر, والأجهزة الذكية, وأجهزة توجيه الشبكات, وتتضمن تقنيات أكثر شيوعاً في الاستخدام لحماية هذه الأجهزة, جدران الحماية من البرامج الضارة , وبرامج مكافحة الفيروسات, وحماية البريد الإلكتروني.

المحور الثالث : اهداف ومؤسسات الأمن السيبراني في الولايات المتحدة الأمريكية

أولاً: الاهداف(٣٢).

١-**ضمان الاتصال:** ويعني الحفاظ على الانترنت مفتوح وأمن, وذلك لتسهيل عملية النمو الاقتصادي, والقدرة على الابتكار والتقدم العلمي, وزيادة التفاعل الاجتماعي والثقافي, فضلا عن مكافحة الجريمة السيبرانية من إجل الحفاظ على موثوقية الانترنت لاسيما في التعاملات الاقتصادية والمالية بما يخدم استمرارية المصالح الوطنية للولايات المتحدة الأمريكية.

٢- **ضمان الأمن:** ويتم بردع الهجمات الإلكترونية, وزيادة مرونة النظم والشبكات من خلال الهندسة المناسبة, وإنشاء نظام الدفاع بالطبقات (الدفاع في العمق) إضافة الى بناء وتطبيق المعايير العالمية فيما يتعلق بالسلوك المقبول للجهات الفاعلة الحكومية وغير الحكومية, وحماية المدنيين لضمان الاستخدام السليم للقوة السيبرانية كوسيلة لخدمة المصالح القومية للولايات المتحدة الأمريكية.

٣-**ضمان الهيمنة (القوة):** الحفاظ على ميزة التفوق للجيش الأمريكي في الفضاء السيبراني من أجل تعزيز ردع الهجمات الإلكترونية خلال وقت السلم والحرب, وحماية المعلومات والاسرار التجارية والملكية الفكرية من التدمير, سواء عبر الجريمة السيبرانية أو التجسس السيبراني, اللذان يضعفان القدرة التنافسية للولايات المتحدة في الاقتصاد العالمي, فضلا عن السعي لبناء وتطوير رأس المال التكنولوجي والبشري من أجل تعزيز التنافس الأمريكي في الفضاء السيبراني.

ثانياً : مؤسسات الأمن السيبراني في الولايات المتحدة الأمريكية

وزارة الدفاع: تقوم بمراقبة الأنظمة المعلوماتية العسكرية, مع تعزيز أمن الشبكات التي تتداول البيانات السرية ونشر أنظمة وقائية للحيلولة دون تسريب البيانات.

وزارة الأمن الوطني: تتولى حماية الأنظمة المعلوماتية الخاصة بالوكالات المدنية الأمريكية, بما في ذلك تحصين نقاط الدخول الخارجية ونشر مستشعرات على الشبكات, فضلا عن عقد اتفاقات شراكة وتعاون مع الشركات الخاصة(٣٣).

وزارة الأمن الداخلي: تختص مسؤوليتها في حماية الاراض الأمريكية من أي هجمات وتبذل جهود لتأمين الهيئات الحكومية المدنية والشبكات غير السرية وهي تعد الأمن السيبراني واحد من خمس مجالات اساسية في الوزارة. هذا فضلا عن وكالة الاستخبارات الامريكية ومكتب التحقيقات الفدرالي والكونغرس والبيت الابيض الذي اقر انشاء وكالة جديدة لمساعدة الولايات المتحدة في مجال الأمن السيبراني, اطلق عليها مركز تكامل استخبارات التهديد السيبراني مهمتها توفير الدعم والاسناد لعمل الوكالات الاخرى(٣٤).

المحور الرابع: إستراتيجية الأمن السيبراني في الولايات المتحدة الأمريكية

بعد احداث ١١ ايلول ٢٠٠١ تم التأكيد على الفضاء الإلكتروني كتهديد أمني جديد, في فبراير عام ٢٠٠٣ اطلق الرئيس (جورج دبليو بوش) "الإستراتيجية القومية لتامين الفضاء الإلكتروني", واشرت هذه الإستراتيجية على ان البنية التحتية الأمريكية تتكون من مؤسسات عامة في مجالات الاتصالات والمعلومات والطاقة والمعاملات المالية... الخ ويعتبر الفضاء الإلكتروني عصب هذه المجالات, إذ انه يمثل نظام التحكم الخاص بالدولة. ومن ثم عملية تأمينه والقدرة على التحكم فيه وادارته من العوامل الرئيسية للمحافظة على الاقتصاد والأمن القومي الأمريكي, وتسعى الإستراتيجية الى تحقيق الاتي(٣٥):

١- منع الهجمات الإلكترونية.
٢- تقليل نقاط الضعف التي يمكن اختراقها.
٣- سرعة التعامل مع الهجمات الإلكترونية.

واعلنت الولايات المتحدة الأمريكية عام ٢٠٠٩ تشكيل قيادة عسكرية للفضاء الالكتروني لحماية الجيش الأمريكي لتبرز أهمية الفضاء الإلكتروني بما يتضمنه من قضايا عدة ذات صلة وثيقة بالأمن القومي الأمريكي في ظل الاعتماد الدولي عليه فيما يتعلق بتسيير عمل البيئة التحتية الكونية للمعلومات امام المنشات المدنية والعسكرية عن طريق تعرضه لهجوم يستهدف كوسيط وحامل للخدمات أو بشل عمل أنظمتها المعلوماتية فإن التحكم في تنفيذ هكذا هجمات يعد إدارة سيطرة ونفوذ إستراتيجي بالغ الأهمية في زمن السلم والحرب(٣٦).

بذلك جاءت إستراتيجية الأمن القومي الأمريكي للعام ٢٠١٠ لتؤكد " التهديدات الإلكترونية تمثل واحدة من أخطر التهديدات التي تواجه الأمن القومي والسلامة العامة للمواطنين, فضلا عن أنها أحد أهم التحديات التي تواجه الاقتصاد القومي, ومن ثم يجب تأمينها, كما يجب أن تكون جديرة بثقة مستخدميها, ويتم ذلك عبر الاستثمار في الافراد والتكنولوجيا, وعبر تدعيم قدرات الشركات مع القطاعات المختلفة"(٣٧).

وفي عام ٢٠١٤, اكدت وزارة الدفاع الأمريكية في تقريرها الإستراتيجي, بأنها تعمل على اعادة تنظيم مواردها لتعزيز قدرات الأمن السيبراني لها لمواجهة التهديدات التي تؤثر على الأمن القومي في ثلاث مجالات هي حماية الشبكات وشل قوة العدو السيبرانية وحماية الدفاع الوطني(٣٨). وبحلول عام ٢٠١٦ تم انشاء قوة سيبرانية تتالف من ٤٠ فرقة موزعة على مهمات هجومية ودفاعية وتتوزع مسؤولية الأمن السيبراني بين وزارة الداخلية ومكتب

التحقيقات الفدرالية ووزارة الدفاع التي تضم قيادة الأمن السيبراني, ووكالة الأمن القومي التي تسند اليها العمليات الهجومية وقد وصل عدد قوات القيادة العسكرية للفضاء الإلكتروني في عام ٢٠١٦ الى ٦٠٠٠ مقاتل(٣٩).

وفي عام ٢٠١٧ حددت إدارة الرئيس (دونالد ترامب) إستراتيجية تتضمن توجيهات يمكن اتخاذها للمساعدة في الحفاظ على الأمن الأمريكي من التهديدات السيبرانية ومنها تحديد اولويات المخاطر, بناء شبكة حكومية يمكن الدفاع عنها, ردع وتعطيل الفواعل السيبرانية, تحسين تبادل المعلومات والاستشعار(٤٠).

ونتيجة لذلك اقرت الولايات المتحدة الأمريكية في العام ٢٠١٨ إستراتيجية جديدة للأمن السيبراني اتخذت فيها موقف أكثر صرامة في مقابل تهديدات كل من روسيا والصين, ودخلت حيز التفيذ بعد قرار الرئيس (دونالد ترامب) بإلغاء قواعد حددها سلفه الرئيس (بارك اوباما) للعمليات السيبرانية, والاتجاه لاستعدادات الحرب السيبرانية من خلال بناء قوة أكثر فتكاً, وتوسيع التحالفات والشراكات, وهي ترى ان الفضاء السيبراني يجب ان يعزز بالتفوق العسكري وممارسة الأنشطة الاستخباراتية, وحماية الأمن القومي, والعمل على ردع القوى الدولية المنافسة, وسرقة الاسرار الصناعية, وتهديد البنية التحتية المعلوماتية وذلك بالعمل على ما يأتي(٤١):

١- ضمان قدرة الجيش الأمريكي على القتال وكسب الحروب في أي مجال, بما في ذلك الفضاء السيبراني, وحماية الأمن القومي وردع العدوان الذي قد يشنه الاعداء, والاستجابة السريعة للهجمات الإلكترونية التي تمثل استخداماً للقوة ضد مصالح الولايات المتحدة وحلفائها وشركائها الإستراتيجين.

٢- السعي لشن هجمات استباقية وردع الأنشطة السيئة عبر الانترنت, التي تستهدف البنية التحتية, والتي قد تؤثر في قدرة وزارة الدفاع على حماية المصالح الوطنية, واعتماد أسلوب الدفاع الى الأمام عن طريق ضرب مصادر الخطر خارج حدود الولايات المتحدة الأمريكية قبل ان تصل الى الداخل.

٣- تعزيز التعاون مع الهيئات المعنية بالدفاع مع القطاعين العام والخاص لتنسيق أنماط الاستجابة, ونقل الخبرات والتعاون في تنفيذ الإستراتيجية القومية للأمن السيبراني.

٤- التعاون مع الحلفاء والشركاء من أجل تعزيز القدرة على مواجهة الهجمات الإلكترونية, وتعزيز جاهزيتها في مجال الدفاع السيبراني والردع ومواجهة الهجمات, ومشاركة المعلومات للعمل على فاعلية مواجهة الهجمات الإلكترونية وتعزيز وضع الأمن السيبراني.

٥- تعزيز قواعد السلوك الرسمي للدولة في الفضاء السيبراني, وتأييد عمل لجنة فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالتطورات في مجال الاتصالات والمعلومات ضمن سياق الأمن الدولي.

وعلى الرغم من الإستراتيجيات العسكرية التي سعت لوضعها الولايات المتحدة الأمريكية في مجال الأمن السيبراني, إلا أن هذا لا يمنع من حدوث هجمات إلكترونية واختراقات وتسريبات للمعلومات في بعض الاحيان, لان مجال التهديدات والحروب السيبرانية مجال حيوي متجدد, كلما تتوصل الى طرق وبرامج لمعالجة والحماية من الاختراق, وحماية البيانات والشبكات, كلما ظهر نمط جديد من الاختراقات والتحديدات, فلابد للدول ان تكون حيوية وسريعة دائما لاكتشاف ومعالجة الثغرات الرقمية التي يستغلها العدو للوصول الى اهدافه المطلوبة(٤٢).

المحور الخامس: تداعيات الهجمات الإلكترونية على إستراتيجية الأمن السيبراني في الولايات المتحدة الأمريكية.

يؤكد جوزيف.س.ناي أن هناك أربع فئات رئيسية من الهجمات الإلكترونية على الأمن القومي الأمريكي, تختلف في المدى الزمني ومن حيث المبدأ فالحرب السيبرانية والتجسس السيبراني يرتبط بالدول, والجريمة السيبرانية والإرهاب السيبراني ترتبط بفاعلين من غير الدول, وبالنسبة للولايات المتحدة الأمريكية في الوقت الحاضر تأتي أعلى الخسائر من التجسس السيبراني والجريمة السيبرانية, ولكن على مدى العقد المقبل, قد تصبح الحرب السيبرانية والإرهاب السيبراني على رأس التهديدات(٤٣).

وقد تعرضت الولايات المتحدة الأمريكية لهجمات إلكترونية في ديسمبر لعام ٢٠٢٠, شملت عمليات قرصنة إلكترونية واسعة النطاق, استهدفت وكالات حكومية أمريكية, من بينها إدارة الأمن النووي, ووزارات الدفاع والخارجية والخزانة وشبكات نقل الكهرباء ومحطات الطاقة, وشركات خاصة مرتبطة بالحكومة الفدرالية, إثر الهجوم نقلت صحيفة "وول ستريت جورنال" عن مسؤول أمريكي استخباري قوله "إن التوصل الى معرفة ابعاد عملية الهجمة الإلكترونية الاخيرة وتجاوز تداعياتها يحتاج الى اشهر ان لم يكن سنوات" وإن أبعاد العملية مذهلة وكبيرة بالنظر الى طبيعتها الحذرة والمتخفية وأن أكثر مايزعج فيها هو عدم القدرة حتى الان على تحديد أنظمة الكمبيوتر المتأثرة"(٤٤). وأكد الرئيس الحالي (جو بايدن) قبل تنصيبه رئيساً للولايات المتحدة الأمريكية في ٢٠ يناير لعام ٢٠٢١, اذ ورد في تأكيده في ديسمبر لعام ٢٠٢٠ على أن الأمن السيبراني هو أولوية قصوى لإدارته القادمة وضمن خطته على إثر تعرض الولايات المتحدة الأمريكية للهجمات الإلكترونية الواسعة, وانتقد (جو بايدن), (دونالد ترامب) باعتباره رئيساً للولايات المتحدة الأمريكية لغاية قبل التنصيب أنه مقصراً في تعزيز الأمن السيبراني وأنه كان غير يقظ في ذلك وأنه سيأخذ الأمر بجدية خلال إدارته القادمة وتعزيز وحماية الأمن القومي الأمريكي من خلال الرد على الهجمات الإلكترونية ضد منطلقيها(٤٥).

وفي هذا الاطار ينبغي القول أن الولايات المتحدة الأمريكية تبقى عرضة للحوادث الأمنية والهجمات الإلكترونية وهو ما يمثل تهديد للمؤسسات الحيوية والوكالات الأمريكية في الحفاظ على الأمن السيبراني, لاسيما اذا ماتم الاخذ بالحسبان التوظيف المتزايد لمنافسيها وخصومها بالقدرة على الوصول الى معلومات أمريكية حساسة أو الافصاح عنها, أو تعديلها, أو اتلافها, والاضرار بمصالحها الاقتصادية الأمر الذي يمثل تهديد حقيقي لامنها القومي (٤٦).

وكان الرئيس الأمريكي (جو بايدن) قد اشار في كلمته في ٢٨ ديسمبر ٢٠٢٠ بالقول " ان الهجمات الإلكترونية التي واجهتها المؤسسات الأمريكية في المرحلة الماضية شكلت تحدي للأمن القومي الأمريكي, وأن الولايات المتحدة ستتجاوز الصعاب التي مرت بها خلال المرحلة الماضية وستستعيد مصداقيتها أمام العالم" (٤٧).

وقام الرئيس الأمريكي (جو بايدن)، إثر ذلك بتوقيع أمراً تنفيذياً ينص على تدعيم القدرات في مجال الأمن السيبراني للولايات المتحدة. وأعلن مجلس الأمن القومي الأمريكي في بيان له بهذا الشأن، إلى أن الأمر التنفيذي يسعى الى حماية شبكات الوكالات الفدرالية من "أنشطة سيبرانية خبيثة" من قبل أطراف مرتبطة بالدول وغير الدول .ويقضي الأمر التنفيذي بالعمل على إزالة المعوقات التي تواجه تبادل المعلومات بين الحكومة الأمريكية والقطاع الخاص بشأن تهديدات الأمن السيبراني، والعمل على تحديث معايير الأمن للحكومة، وتأمين وتدعيم أمن توريدات

البرمجيات، ووضع التوصيات المناسبة للتعامل مع حوادث الأمن السيبراني والقيام بتوسيع القدرات في الكشف عن الانشطة السيبرانية التي تستهدف الأنظمة المعلوماتية والشبكات الحكومية, ودعا الأمر التفيذي الى انشاء مجلس لتحليل القضايا المرتبطة في الأمن السيبراني، يضم ممثلين عن الحكومة والقطاع الخاص(٤٨).

واعلن مسؤولون في الإدارة الأمريكية أن الرئيس(جو بايدن) يبحث عدة خيارات للرد على الهجمات الإلكترونية الروسية الأخيرة، ووفقاً للمدير السابق لوكالة الأمن السيبراني وأمن البنية التحتية الأميركية (كريستوفر كريبس) حدد بالقول "بأن هناك ما يشبه الحرب الباردة برؤية جديدة أمريكية روسية تتخذ طابعاً الكترونياً في الوقت الحالي", ويرى عضو مجلس الشيوخ للأمن الداخلي السيناتور الجمهوري (ميت رومني)" إن المتسللين الإلكترونيين من روسيا قد تصرفوا بوهم على ان لديهم القدرة على تجنب الرد ولم يخشوا ما يمكننا القيام به ولم يعتقدوا أن المنظومة الدفاعية لدينا كافية، كما انهم على ما يبدو لم يفكروا في أننا سنرد بحزم، وهذا يتطلب منا رد الفعل، والرد المتوقع حصوله سيكون إلكترونياً"(٤٩).

واتساقاً لما سبق, قدمت إلادارة الأمريكية خيارات عدة أمام الرئيس (جو بايدن) للتعامل مع ملف الأمن السيبراني مع روسيا، أولها: إعلان الولايات المتحدة رسمياً بأن روسيا تقف خلف الهجمات الإلكترونية لمصالحها الحكومية والأمنية، ويرجع ذلك بعد تنفيذ عملية تقييم مشترك بين الوكالات الحكومية ومجتمع الأمن السيبراني, أما ثاني خيارات الادارة الأمريكية يتمثل في فرض العقوبات الاقتصادية على روسيا، ولعل ذلك قد يكون أكثر أساليب الرد تأثيراً, وجاء الخيار الاخير بالقيام بعمل انتقامي إلكتروني أمريكي مماثل، وهو خيار معقد يصعب اللجوء إليه, لانه يعد بمثابة إعلان حرب, من خلال رد صارم وفعال على الهجوم الإلكتروني الذي لحق بوزارات الأمن القومي والدفاع والخزانة والطاقة والتجارة، ووكالة الأمن النووي القومي التي تشرف على ضمان وأمن موجودات الولايات المتحدة الأمريكية من الأسلحة النووية(٥٠).

وفي مارس لعام ٢٠٢١ بدأت إستراتيجية (جو بايدن) في الفضاء السيبراني لمواجهة التهديدات الإلكترونية, اذ تعكس الإستراتيجية السيبرانية لإدارة (جو بايدن) الركائز الايدلوجية والجيوسياسية والتكنولوجية والدبلوماسية لرؤية الرئيس (جو بايدن) الشاملة للسياسة الخارجية والأمن القومي للولايات المتحدة الأمريكية, وتاكيداً لإستراتيجة (جو بايدن) لتعزيز الأمن السيبراني ومواجهة الهجمات الإلكترونية كانت قمة (جو بايدن) مع الرئيس الروسي (فلاديمير بوتين) في ١٦ يوليو لعام ٢٠٢١ حاضرة فيه الهجمات الإلكترونية في اعلى قمة المحادثات بين الطرفين, ويجب ابعاد شبح الخطر النووي السيبراني ومواجهة الدول التي تنطلق منها الهجمات الإلكترونية أو أنها تشكل مصدر تهديد سيبراني وشيك, وفي يوليو ٢٠٢١ أكد الرئيس الأمريكي (جو بايدن) أنه من المنطقي أن تشن الولايات المتحدة الأمريكية هجمات إلكترونية على الخوادم المستخدمة في الهجمات الإلكترونية ضدها, وفي السياق نفسه أكد مسؤول في الادارة الأمريكية ان الولايات المتحدة ستتخذ الخطوات الضرورية لحماية بنيتها التحتية وأمنها القومي من الهجمات الإلكترونية(٥١).

وجاءت دراسة حديثة لمجلس الأطلسي وهو "مؤسسة بحثية أمريكية مستقلة" بعنوان" الفرص المستقبلية للإدارة الأمريكية الجديدة خلال عام ٢٠٢١ "، مؤكدة أن الاتجاه نحو المزيد من السياسات التعددية في القرن الحادي والعشرين هو الذي سيُحدث نقلة نوعية مميزة في بعض القضايا ذات الأولوية مثل معالجة أوجه القصور في

حوكمة الفضاء، والأسلحة المستقلة الفتاكة ذاتية التشغيل، والنماذج الجديدة من التكنولوجيا الحيوية والهندسة الجيولوجية ذات الاستخدام المزدوج، ويمكن لإدارة الرئيس الأمريكي (جو بايدن) أن تأخذ خطوة للأمام في مواجهة الأزمات القادمة من خلال العمل على ايجاد ظروف تسهم في توظف التقنيات الناشئة من أجل تحقيق الصالح العام(٥٢).

سعت الادارة الأمريكية، لإصدار إستراتيجية لجعل الوكالات الفيدرالية تلتزم بتشديد الضوابط في مجال الأمن السيبراني، بعد سلسلة من الهجمات الإلكترونية ضد البنية التحتية الحيوية في القطاعين العام والخاص، في واحدة من أكبر الجهود المبذولة للولايات المتحدة من اجل تأمين شبكات الحواسيب التي تعتمد عليها الحكومة, وتتطلع الإستراتيجية إلى تطبيق مفهوم الأمن السيبراني المسمى "الثقة الصفرية"، وهو مفهوم سائد في الشركات الكبرى، على الحكومة الفيدرالية، فضلا عن كونها مسعى في سبيل وضع سياسة للأمن السيبراني حول الأهداف والنتائج، بدلاً من قوائم المراجعة. ويشير كريس إنجليس، مدير الإنترنت الوطني في هذا الصدد: "هذه الإستراتيجية هي خطوة اساسية في جهودنا لبناء نظام محكم وقابل للدفاع عنه في دفاعاتنا الإلكترونية الفيدرالية"(٥٣).

واتجهت الولايات المتحدة الأمريكية في اطار سعيها إلى تعزيز الأمن السيبراني في أصدار الإستراتيجية الوطنية للأمن السيبراني في مارس ٢٠٢٣، وفي يونيو ٢٠٢٣، أصدرت خطة تنفيذية أعقبتها وثيقة إستراتيجية سيبرانية صادرة عن وزارة الدفاع في سبتمبر٢٠٢٣. وقد كانت هناك مجموعة من الدوافع والمحفزات التي شجَّعت الولايات المتحدة على إصدار هذه الإستراتيجية و فيما يلي، يمكن تسليط الضوء على أبرز هذه الدوافع والمحفزات(٥٤):

١- **تأمين الفضاء السيبراني الأمريكي:** بالرغم من انشغال الولايات المتحدة بالحروب التي تخوضها حلفاؤها في مختلف أنحاء العالم، وتحديداً أوكرانيا وإسرائيل وتايوان، فإنها تولي المخاطر السيبرانية المحيطة بها اهتماماً كبيراً، في ظل تكرار الهجمات الإلكترونية على بنيتها الحيوية السيبرانية من حين إلى آخر، من جانب خصومها، وعلى رأسهم روسيا والصين وإيران وكوريا الشمالية؛ ولذلك تم إصدار هذه الاستراتيجية التي ترمي إلى تعزيز أمن الفضاء السيبراني الأمريكي.

٢- **تحقيق مكاسب انتخابية:** مع اقتراب موعد الانتخابات الأمريكية في نوفمبر ٢٠٢٤، تسعى الإدارة الأمريكية إلى أمرين, يتمثل أولهما في تأمين الانتخابات المقبلة، وحمايتها من أي محاولة للتأثيرات الخارجية، في ظل زيادة الشكوك المتعلقة باحتمالية تدخل روسيا والصين وإيران للتأثير على توجهات الناخبين الأمريكيين، بينما يتمثل الأمر الآخَر في تحقيق مكسب جديد يمكن الترويج له لإظهار مدى اهتمام الإدارة بحماية الأمن السيبراني، وتعزيز الشراكات العالمية.

٣- **مجابهة خصوم الولايات المتحدة:** سعت الولايات المتحدة الأمريكية إلى مواجهة النفوذ المتنامي للأنظمة التي تصفها بـ"الاستبدادية"، وتحديداً روسيا والصين حيث ترى الولايات المتحدة أن هذه الأنظمة تسعى إلى إعادة رسم ملامح النظام الدولي، وانتهاك خصوصية الأفراد عبر الفضاء الرقمي؛ لذلك فإنها تسعى إلى حوكمة الفضاء الرقمي، ووضع أسس يمكن من خلالها محاسَبة الأطراف المخطئة، وتقويم السلوك الرقمي، وهو أمر يصبُّ في

النهاية في الصالح العالمي من جهة، كما أنه يحمي أمنها القومي، ومصالحها السياسية والاقتصادية في مختلف مناطق العالم من جهة أخرى.

٤- استكمال الخطوات الأمريكية السابقة في مجال الأمن السيبراني: لا تعد هذه الإستراتيجية هي الجهد الأول من نوعه للولايات المتحدة الأمريكية, إذ سبق أن دشَّنت مبادرة مكافحة برامج الفدية في عام ٢٠٢١ التي انضم إليها ما يزيد عن ٦٠ دولة، كما وقَّعت عدد من الدول على معاهدة تهدف إلى "الحد من إساءة استخدام برامج التجسس التجارية".

ويبقى القول بأن الغموض لايزال يحيط بحجم تداعيات هذه الهجمات الإلكترونية التخريبية في الولايات المتحدة الأمريكية على صعيد الهيئات الفيدرالية والمحلية والشركات الكبرى, وطبيعة البيانات والمعلومات التي تسنى للمخترقين الحصول عليها, ودوافع العمليات السيبرانية سواء كانت عملية تجسس إلكتروني أو جهود لتدمير نظم البرمجيات والمعلومات في الولايات المتحدة, ويؤكد مجموعة من خبراء الأمن السيبراني ان الهيئات التي تعرضت لهذه الهجمات الإلكترونية ستكون بحاجة الى مدة أطول لتحديد عمق الاثار التي ترتبت على البيانات والمعلومات الموجودة في مستودعاتها الرقمية, ومن ثم فإن حجم التداعيات المحتملة على نظم البرمجيات والمعلومات في الهيئات الفيدرالية والمحلية والشركات الكبرى لم تتضح بعد أذ ذهب البعض من خبراء الأمن السيبراني الى عدم وجود ادلة حاسمة على انتهاء العملية وامكانية وجود اهداف بعيدة المدى لا يمكن التكهن بها في الوقت الراهن, لذلك من الصعب التنبوء بطبيعة حجم الرد المرتقب من الولايات المتحدة الأمريكية على الهجمات الإلكترونية بعد الانكار الحاسم لروسيا والصين بممارسة أي دور في هذه العمليات السيبرانية غير المسبوقة(٥٥).

الخاتمة

مع تطور التكنولوجيا في وسائل القتال وأساليبه، وبخاصةٍ المستعملة في النموذج الجديد من التهديدات الإلكترونية، مقارنة مع القضايا الدولية الأخرى المهددة للسلم والأمن الدوليين، برزت تحديات كبيرة على صعيد مواجهة الهجمات الإلكترونية الراهنة, باتت أمر ضروري, لكن الخطر الحقيقي يكمن في التهديدات المستقبلية, لذلك فإن تجاهلها, سيعرض الأمن السيبراني الأمريكي الى خطر دائم واكيد. إلا أن التحدي في هذا الشأن يعني الاستعداد لدى الولايات المتحدة للتهديدات القادمة بتطوير إستراتيجية المواجهة والعمل مع بقية دول العالم من أجل المشاركة في قيم الأمن والاستقرار واحترام قواعد السلوك الجيد من أجل فضاء سيبراني أمن, والمشاركة بين الحكومة والقطاع الخاص في انشاء معايير مشتركة للحماية الإلكترونية, على الرغم من أن الفضاء السيبراني يتميز بالغموض وشدة تنوع التهديدات مما يجعل الأمن السيبراني على رأس الاولويات في الإستراتيجية العسكرية والأمنية للولايات المتحدة الأمريكية في ظل صعوبة تحديد الجهات المسؤولة من دول أو مجموعات ما عن الهجمات الإلكترونية, ومنافسة شديدة في الفضاء السيبراني من روسيا والصين بما قد يهدد أمنها القومي ودورها في الأمن العالمي.

توصلت الدراسة الى مجموعة من الاستنتاجات الاتية:

١- ان الهجمات الإلكترونية بتنوع اساليبها ووسائلها المتبعة ما زالت من المفاهيم الحديثة التي لا يوجد لها اتفاق دولي بشان تعريفها.

٢- ان الهجمات الإلكترونية معقدة في طريقة تنفيذها من قبل الدول والجهات الفاعلة من غير الدول وقد تكون ذات مصادر مجهولة يصعب تعقبها أو معرفة مصيرها.

٣- ان الأمن السيبراني مفهوم متعدد الابعاد والمستويات, ومفهوم مركب متسع النطاق فالتطورات المعاصرة التكنولوجية ادت الى اتساع نطاق مفهوم الأمن السيبراني في حماية البنية التحتية للمعلومات.

٤- ان الولايات المتحدة الأمريكية رغم ما تمتلك من قدرات عسكرية هائلة تعرضت الى هجمات إلكترونية متكررة شكلت هاجساً استراتيجياً, ومثلت تهديد الى أمنها القومي, لذلك اتخذت خطوات عاجلة عن طريق تبني إستراتيجية الأمن السيبراني وتقوية المعايير التي تخفف التهديدات السيبرانية, وتعزيز الاستقرار في الفضاء السيبراني.

٥- ان الأمن السيبراني في الولايات المتحدة الأمريكية بات يشكل أولوية في استراتيجية الأمن القومي لمواجهة تصاعد الهجمات الإلكترونية ضد المصالح الحيوية الأمريكية.

الهوامش

(١) طلال ياسين العيسى, عدي محمد عناب, المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر, مجلة الزرقاء للبحوث والدراسات الانسانية, الاردن , المجلد ١٩, العدد١, ٢٠١٩, ص٨٤.

(٢) نورة شلوش, القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول", مجلة مركز بابل للدراسات الانسانية, جامعة بابل,المجلد٨, العدد٢, ٢٠١٨, ص١٩١.

(٣) فارس محمد العمارات, إبراهيم الحمامصة, الأمن السيبراني: المفهوم وتحديات العصر, دار الخليج للنشر والتوزيع, عمان, الاردن, ٢٠٢٢, ص١٠٤.

(٤) بن صابر بلقاسم, حيدر محمد, الهجمات السيبرانية ومواجهتها في ظل القانون الدولي المعاصر, مجلة حقوق الإنسان والحريات العامة, الجزائر, العدد٤, ٢٠١٧, ص ١٨٨.

(٥) احمد عبيس نعمة الفتلاوي, الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر, مجلة المحقق الحلي للعلوم القانونية والسياسية, كلية القانون, جامعة بابل, العدد٤, ٢٠١٩, ص٦١٢.

(٦) عمر محمود أعمر, الحرب الإلكترونية في القانون الدولي الإنساني, مجلة دراسات, الاردن, المجلد ٤٦, العدد٣, ٢٠١٩, ص١٣٥.

(٧) علاء الدين فرحات, الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين, مجلة العلوم القانونية والسياسية, الجزائر, المجلد ١٠, العدد ٣, ٢٠١٩, ص٩١.

(٨) عمر محمود أعمر, مصدر سبق ذكره, ص١٣٥.

(٩) علاء الدين فرحات, مصدر سبق ذكره, ص٩٣.

(١٠) اماني عصام محمود, استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية, مجلة كلية الاقتصاد والعلوم السياسية, جامعة القاهرة, المجلد٢٢, العدد٤, ٢٠٢١, ص١٧٧.

(١١) بن صابر بلقاسم, حيدر محمد, مصدر سبق ذكره, ص١٩٣.

(١٢) ماجد محمد الحنيطي, تكنولوجيا الصراعات الدولية المعاصرة, الان ناشرون وموزعون, عمان, الاردن, ٢٠٢١, ص٢٦٢.

(١٣) سو غوردن, ايريك روزنباخ, أمريكا تصفي حساباتها السيبرانية وتعيد النظر فيها, اندبندنت عربية, ٢٠٢١/١٢/١٨.

https://www.independentarabia.com/node/286926

(١٤) طلال ياسين العيسى, عدي محمد عناب, مصدر سبق ذكره, ص٨٦.

(١٥) خالد وليد محمود, الهجمات عبر الإنترنت: ساحة الصراع الإلكتروني الجديدة, المركز العربي للأبحاث ودراسة السياسات, الدوحة, ٢٠١٣, ص٨.

(١٦) طلال ياسين العيسى, عدي محمد عناب, مصدر سبق ذكره, ص٨٦.

(١٧) أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, مجلة البحوث الفقهية والقانونية, كلية الشريعة والقانون, مصر, العدد٣٥, ٢٠٢٠, ص ص٤١٥-٤١٦.

(١٨) زياد علي العلي, الصراع والأمن الجيوسيبراني في السياسة الدولية: دراسة في استراتيجيات الاشتباك الرقمي, دار امجد للنشر والتوزيع, عمان, الاردن, ٢٠١٩, ص٥٧.

(19)Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department Computer Science, 2003, p3.

(20) Edward Amoroso, Cyber Security, Silicon Press, 2007, p10.

(٢١) دليل الأمن السيبراني للبلدان النامية, الاتحاد الدولي للاتصالات, جنيف, ٢٠١٠, ص٤٢١.

(٢٢) منى عبد الله السحمان, متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات. مجلة كلية التربية, جامعة المنصورة, مصر,العدد١١١, ٢٠٢٠, ص١٠.

(٢٣) لامية طالة, التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول وأستراتيجيات مكافحتها, مجلة معالم للدراسات القانونية والسياسية, الجزائر,المجلد٤,العدد٢ ,٢٠٢٠, ص٦٢.

(٢٤) شيماء معروف فرحان, التحول في مفهوم القوة والصراع : دراسة في الحروب السيبرانية, مجلة قضايا سياسية, كلية العلوم السياسية, جامعة النهرين, العدد٧٥, ٢٠٢٣, ص٥٠٣.

(٢٥) يوسف بو غرارة, الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع السيراني, مجلة الدراسات الافريقية وحوض النيل, المركز الديمقراطي العربي, برلين, المجلد١, العدد٣, ٢٠١٨, ص١٠٨.

(٢٦) ادريس عطية, مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري, مجلة مصداقية, الجزائر, المجلد١, العدد ٢, ٢٠٢٠, ص١٠٥.

(٢٧) احمد حامد علي, سعاد عبد الله محمد, احمد حامد علي, سعاد عبد الله محمد, الأمن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر, مجلة جامعة الانبار للعلوم الانسانية, المجلد١,العدد٣, ٢٠٢٠, ص٣٧٥.

(٢٨) لامية طالة, مصدر سبق ذكره, ص٦٣.

(٢٩) احمد حامد علي, سعاد عبدالله محمد, مصدر سبق ذكره, ص٣٧٥.

(٣٠) اسماعيل زروقة, الفضاء السيبراني والتحول في مفاهيم القوة والصراع, مجلة العلوم القانونية والسياسية, الجزائر, المجلد ١٠, العدد١, ٢٠١٩, ص ١٠١٩.

(٣١) ضحى لعيبي كاظم السدخان, البعد الجيوسياسي للأمن السيبراني, مجلة العلوم الانسانية, المركز الجامعي علي كافي تندوروف, الجزائر, المجلد ٥, العدد١, ٢٠٢١, ص ص٢٠٠-٢٠١.

(٣٢) سليم دحماني, أثر التهديدات السيبرانية على الأمن القومي :الولايات المتحدة الأمريكية-أنموذجا-(٢٠٠١-٢٠١٧), مذكرة مقدمة لنيل شهادة الماستر, جامعة محمد بوضياف, كلية الحقوق والعلوم السياسية, المسيلة ,الجزائر, ٢٠١٧- ٢٠١٨, ص٦٥.

(٣٣) إيهاب خليفة, القوة الالكترونية : كيف يمكن أن تدير الدول شؤونها في عصر الانترنت, دار العربي للنشر والتوزيع,
القاهرة, ط١ ,٢٠١٧, ص١٤٣.

(٣٤) مركز استخبارات أمريكي جديد للتنسيق حول التهديدات الإلكترونية, موقع الخليج اونلاين,٢٠١٥/٢/١٧.
https://alkhaleejonline.net

(٣٥) ايهاب خليفة, مصدر سبق ذكره, ص١٣٥.

(٣٦) يونس مؤيد يونس مصطفى, استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني, مجلة قضايا سياسية, كلية العلوم السياسية, جامعة النهرين, العدد٥٥, ٢٠١٨, ص١٤٢.

(٣٧) دنيا جواد مطلك, احمد عبد الجبار عبد الله, انعكاسات تطور القوة المعلوماتية الأمريكية في البيئة الداخلية, مجلة حمورابي للدراسات, مركز حمورابي للبحوث والدراسات الإستراتيجية, بغداد, العدد٣٥, ٢٠٢٠, ص١٦٣.

(٣٨) محمد منذر جلال الربيعي, سرى غضبان غيدان, الأمن السيبراني وسياسات المواجهة الدولية, مجلة الدراسات الاستراتيجية والعسكرية, المركز الديمقراطي العربي, برلين, المجلد٢, العدد٩, ٢٠٢٠, ص٢٠٦.

(٣٩) نفس المصدر السابق, نفس الصفحة.

(٤٠) سليم دحماني, مصدر سبق ذكره, ص٧٥.

(٤١) دنيا جواد مطلك, احمد عبد الجبار عبد الله, مصدر سبق ذكره, ص- ص١٦٧-١٦٨.

(٤٢) محمد منذر جلال الربيعي, سرى غضبان غيدان, مصدر سبق ذكره, ص ٢٠٨.

(٤٣) سليم دحماني, مصدر سبق ذكره, ص٦٢.

(٤٤) صلاح حيدر عبد الواحد, حروب الفضاء الالكتروني: دراسة في مفهومها وخصائها وسبل مواجهتها, رسالة ماجستير في العلوم السياسية, جامعة الشرق الاوسط , كلية الاداب والعلوم, عمان, الاردن, ٢٠٢١, ص٣٦.

(٤٥) كرار عباس متعب فرج, الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران, مجلة حمورابي للدراسات, مركز حمورابي للبحوث والدراسات الإستراتيجية, بغداد, العدد٤٠, ٢٠٢١, ص٢٠٧.

(٤٦) علي محمد امنيف الربيعي, تحديات الأمن في الفضاء السيبراني الأمريكي, مجلة دراسات دولية, جامعة بغداد, العدد ٨٥, ٢٠٢١, ص٣٠٦.

(٤٧) جو بايدن, الهجمات الالكترونية ضدنا "تحدي للأمن القومي", اخبار اليوم, ٢٠٢٠/١٢/٢٨
https://m.akhbarelyom.com/news/newdetails/3209314

(٤٨) بايدن يوقع أمراً تنفيذياً حول تعزيز الأمن السيبراني للولايات المتحدة, موازين نيوز, ٢٠٢١/٥/١٣.
https://www.mawazin.net/Details.aspx?jimare=153106

(٤٩) احمد تركي, بعد الاختراق الاخير..إدارة بايدن تدرس التحول من الدفاع الى الهجوم في حروبها السيبرانية, وكالة انباء الشرق الاوسط , ٢٠٢٠/١٢/٢٣.
https://www.mena.org.eg/news/dbcall/table/webnews/id/8723777

(٥٠) إدارة بايدن تدرس التحول من الدفاع الى الهجوم في حروبها السيبرانية, الدستور, ٢٠٢٠/١٢/٢٣.
https://www.dostor.org/3303854

(٥١) كرار عباس متعب فرج, مصدر سبق ذكره, ص ص٢٠٧-٢٠٨.

(٥٢) سارة عبد العزيز, الفرص والمخاطر الأكثر بروزاً امام إدارة "بايدن" في ٢٠٢١, مركز المستقبل للابحاث والدراسات المتقدمة, أبو ظبي, ٢٠٢٠/١٢/٢١.
https://futureuae.com/ar-AE/Mainpage/Item/5972

(٥٣) نهال ابو السعود, بايدن يطلق إستراتيجية لتعزيز الأمن السيبراني بعد تكرار عمليات اختراق للسلطات الفيدرالية, اليوم السابع, ٢٠٢٢/١/٢٦.
https://www.youm7.com/story/2022/1/26

(٥٤) مجابهة الخصوم: ما ملامح الاستراتيجية الأمريكية الجديدة للأمن السيبراني؟, انترريجونال للتحليلات الاستراتيجية, أبوظبي, العدد٣٦٣, ٢٠٢٤, ص٤.

(٥٥) حسن مظفر الرزو, اعصار سيبراني: انكشاف أمني غير مسبوق, ورقات تحليلية, مركز الجزيرة للدراسات, الدوحة, ٢٠٢٠, ص٨.

المصادر

أولاً:الكتب العربية والمترجمة

(١) إيهاب خليفة, القوة الإلكترونية : كيف يمكن أن تدير الدول شؤونها في عصر الانترنت, دار العربي للنشر والتوزيع, القاهرة, ط١ ,٢٠١٧,

(٢) زياد علي العلي, الصراع والأمن الجيوسيبراني في السياسة الدولية: دراسة في استراتيجيات الاشتباك الرقمي, دار امجد للنشر والتوزيع, عمان, الاردن, ٢٠١٩.

(٣) فارس محمد العمارات, إبراهيم الحمامصة, الأمن السيبراني: المفهوم وتحديات العصر, دار الخليج للنشر والتوزيع, عمان, الاردن, ٢٠٢٢.

(٤) ماجد محمد الحنيطي, تكنولوجيا الصراعات الدولية المعاصرة, الان ناشرون وموزعون, عمان, الاردن, ٢٠٢١.

ثانياً: الرسائل والاطاريح الجامعية

(١) سليم دحماني, أثر التهديدات السيبرانية على الأمن القومي :الولايات المتحدة الأمريكية- أنموذجا-(٢٠٠١-٢٠١٧), مذكرة مقدمة لنيل شهادة الماستر, جامعة محمد بوضياف, كلية الحقوق والعلوم السياسية, المسيلة, الجزائر, ٢٠١٧-٢٠١٨.

(٢) صلاح حيدر عبد الواحد, حروب الفضاء الالكتروني: دراسة في مفهومها وخصائها وسبل مواجهتها, رسالة ماجستير في العلوم السياسية, جامعة الشرق الاوسط , كلية الاداب والعلوم, عمان, الاردن, ٢٠٢١.

ثالثاً: البحوث والدراسات

(١) احمد حامد علي, سعاد عبد الله محمد, الامن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر, مجلة جامعة الانبار للعلوم الانسانية , المجلد١,العدد٣, ٢٠٢٠.

(٢) احمد عبيس نعمة الفتلاوي, الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر, مجلة المحقق الحلي للعلوم القانونية والسياسية, كلية القانون, جامعة بابل, العدد٤, ٢٠١٩.

(٣) ادريس عطية, مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري, مجلة مصداقية, الجزائر, المجلد١, العدد ٢, ٢٠٢٠.

(٤) اسماعيل زروقة, الفضاء السيبراني والتحول في مفاهيم القوة والصراع, مجلة العلوم القانونية والسياسية, الجزائر, المجلد ١٠, العدد١, ٢٠١٩.

(٥) اماني عصام محمود, استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية, مجلة كلية الاقتصاد والعلوم السياسية, جامعة القاهرة, المجلد٢٢, العدد٤, ٢٠٢١.

(٦) أميرة عبد العظيم محمد عبد الجواد, المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام, مجلة البحوث الفقهية والقانونية, كلية الشريعة والقانون, مصر, العدد٣٥, ٢٠٢٠.

(٧) بن صابر بلقاسم, حيدر محمد, مصدر سبق ذكره, الهجمات السيبرانية ومواجهتها في ظل القانون الدولي المعاصر, مجلة حقوق الانسان والحريات العامة, الجزائر, العدد٤, ٢٠١٧.

(٨) حسن مظفر الرزو, اعصار سيبراني: انكشاف أمني غير مسبوق, ورقات تحليلية, مركز الجزيرة للدراسات, الدوحة, ٢٠٢٠.

(٩) خالد وليد محمود, الهجمات عبر الإنترنت: ساحة الصراع الإلكتروني الجديدة, المركز العربي للأبحاث ودراسة السياسات, الدوحة, ٢٠١٣.

(١٠) دنيا جواد مطلك, احمد عبد الجبار عبد الله, انعكاسات تطور القوة المعلوماتية الامريكية في البيئة الداخلية, مجلة حمورابي للدراسات, مركز حمورابي للبحوث والدراسات الإستراتيجية, بغداد, العدد٣٥, ٢٠٢٠.

(١١) شيماء معروف فرحان, التحول في مفهوم القوة والصراع : دراسة في الحروب السيبرانية, مجلة قضايا سياسية, كلية العلوم السياسية, جامعة النهرين, العدد٧٥, ٢٠٢٣.

(١٢) طلال ياسين العيسى, عدي محمد عناب, المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر, مجلة الزرقاء للبحوث والدراسات الانسانية, الاردن, المجلد ١٩, العدد١, ٢٠١٩.

(١٣) ضحى لعيبي كاظم السدخان, البعد الجيوسياسي للأمن السيبراني, مجلة العلوم الانسانية, المركز الجامعي علي كافي تندوروف, الجزائر, المجلد ٥, العدد١, ٢٠٢١.

(١٤) علاء الدين فرحات,الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين, مجلة العلوم القانونية والسياسية, الجزائر, المجلد ١٠, العدد ٣, ٢٠١٩.

(١٥) علي محمد امنيف الربيعي, تحديات الأمن في الفضاء السيبراني الأمريكي, مجلة دراسات دولية, جامعة بغداد, العدد٨٥, ٢٠٢١.

(١٦) عمر محمود أعمر, الحرب الإلكترونية في القانون الدولي الإنساني, مجلة دراسات, الاردن, المجلد ٤٦, العدد٣, ٢٠١٩.

(١٧) كرار عباس متعب فرج, الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران, مجلة حمورابي للدراسات, مركز حمورابي للبحوث والدراسات الإستراتيجية, بغداد, العدد٤٠, ٢٠٢١.

(١٨) لامية طالة, التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول وأستراتيجيات مكافحتها, مجلة معالم للدراسات القانونية والسياسية, الجزائر, المجلد٤,العدد٢ ,٢٠٢٠.

(١٩) مجابهة الخصوم: ما ملامح الاستراتيجية الأمريكية الجديدة للأمن السيبراني؟, انتريجونال للتحليلات الاستراتيجية, أبوظبي, العدد٣٦٣, ٢٠٢٤.

(٢٠) محمد منذر جلال الربيعي, سرى غضبان غيدان, الامن السيبراني وسياسات المواجهة الدولية, مجلة الدراسات الاستراتيجية والعسكرية, المركز الديمقراطي العربي, برلين, المجلد٢, العدد٩, ٢٠٢٠.

(٢١) منى عبد الله السحمان, متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات, مجلة كلية التربية, جامعة المنصورة, مصر, العدد١١١, ٢٠٢٠.

(٢٢) نورة شلوش, القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول", مجلة مركز بابل للدراسات الانسانية, جامعة بابل,المجلد٨, العدد٢, ٢٠١٨.

(٢٣) يوسف بو غرارة, الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع السيراني, مجلة الدراسات الافريقية وحوض النيل, المركز الديمقراطي العربي, برلين, المجلد١, العدد٣, ٢٠١٨.

(٢٤) يونس مؤيد يونس مصطفى, استراتيجية الولايات المتحدة الأمريكية للأمن السيبراني, مجلة قضايا سياسية, جامعة النهرين, العدد٥٥, ٢٠١٨.

رابعاً: الانترنت

(١) احمد تركي, بعد الاختراق الاخير..إدارة بايدن تدرس التحول من الدفاع الى الهجوم في حروبها السيبرانية, وكالة انباء الشرق الاوسط , ٢٠٢٠/١٢/٢٣.

https://www.mena.org.eg/news/dbcall/table/webnews/id/8723777

(٢) إدارة بايدن تدرس التحول من الدفاع الى الهجوم في حروبها السيبرانية, الدستور, ٢٠٢٠/١٢/٢٣.

https://www.dostor.org/3303854

(٣) بايدن يوقع أمرا تنفيذيا لتعزيز الأمن السيبراني في الولايات المتحدة, وكالة الانباء العراقية, ٢٠٢١/٥/١٣.

https://www.ina.iq/125764

(٤) جو بايدن, الهجمات الالكترونية ضدنا "تحدي للأمن القومي", اخبار اليوم, ٢٠٢٠/١٢/٢٨.

https://m.akhbarelyom.com/news/newdetails/3209314

(٥) سارة عبد العزيز, الفرص والمخاطر الأكثر بروزاً امام إدارة " بايدن " في ٢٠٢١ : المجلس الاطلسي, مركز المستقبل للابحاث والدراسات المتقدمة, ٢٠٢١/١٢/٢١.

https://futureuae.com/ar/Mainpage/Item/5972

(٦) سو غوردن, ايريك روزنباخ, أمريكا تصفي حساباتها السيبرانية وتعيد النظر فيها, اندبندنت عربية, ٢٠٢١/١٢/١٨.

https://www.independentarabia.com/node/286926

(٧) مركز استخبارات أمريكي جديد للتنسيق حول التهديدات الإلكترونية, موقع الخليج اونلاين,٢٠١٥/٢/١٧.
https://alkhaleejonline.net

(٨) نهال ابو السعود, بايدن يطلق استراتيجية لتعزيز "الامن السيبراني" بعد تكرار عمليات اختراق للسلطات الفيدرالية, اليوم السابع, ٢٠٢٢/١/٢٦.
https://www.youm7.com/story/2022/1/26

خامساً: المصادر الاجنبية

Richard A.Kemmererm, Cyber security, University of California Santa Barbara,Depatment)1 (. Computer Science, 2003
Edward Amoroso, Cyber Security, Silicon Press, 2007.)2(