The Cyber Influence of the National Security of the Active Countries (United States of America as a Model)

Prof. Dr. Israa shareef al-kaeud
University of Baghdad/ College of Political Science
drisraashareef68@gmail.com

Receipt date: 11/6/2022 accepted date:14/8/2022 Publication date:1/12/2022

https://doi.org/10.30907/jcopolicy.vi64.628

Abstract:

Briefly the term of cyber security is a bunch of operations and procedures working on insurance and protecting the network, computer devices, the programs and data from attack and from damaging penetration, also from breaking, abstraction and disturbing in spite of the fact that the concept of cyber conflict is got widening. So, the needs arise in the state to secure cyberspace and protect it by several methods to confront the electronic intrusions and threats which is known as cyber security. Countries seek to preserve its national security in particular the United States of America after the events of September 11 ,2001. In addition, the United States follow all ways to take over cyber threats.

Key words: cyber space, information security, terrorism, national security.

التأثير السيبراني في الأمن القومي للدول الفاعلة (الولايات المتحدة الأميركية) انموذجا

أ.د. اسراء شريف الكعود

جامعة بغداد/ كلية العلوم السياسية

drisraashareef68@gmail.com

تاريخ الاستلام:٢٠٢٢/٦/١١ تاريخ قبول النشر:٢٠٢٢/٨/١٤ تاريخ النشر:٢٠٢٢/١٢/١

الملخص:

شهدت العلاقات الدولية تطورات جلية من حيث الفواعل والمواضيع والأدوات المستخدمة في إدارة تلك التفاعلات وفي ظل هذا التطور النوعي الذي ظهر بشكل متزامن مع الثورة التكنولوجية بالوسيط الرقمي اقتحمت مختلف نواحي الحياة الإنسانية والتفاعلات الدولية لذا ظهرت تأثيرات جديدة من حيث النوع وتهديدات مبتكرة واجهت الحكومات والدول دون استثناء هذا الخطر المتمثل بالتهديدات السيبرانية لذا سعت الدول الكبرى وفي مقدمتها

الولايات المتحدة الامريكية لاستغلال مكامن القوة التي وفرها الفضاء السيبراني وقد برز الحيز السيبراني كحالة جديدة في أنماط الحروب والصراعات استحوذت على اهتمام الولايات المتحدة الامريكية واعتبرت من اهم التحديات التي تواجه الامن القومي الأمريكي وعنصراً مؤثراً في العلاقات الدولية.

الكلمات المفتاحية: الفضاء السيبراني، أمن المعلومات، الإرهاب، الأمن القومي.

المقدمة:

مما لا شك فيه ان موضوع الامن السيبراني يعد من المواضيع الحيوية الجديدة التي طرحت نفسها في ظل التطور الهائل في الثورة التكنولوجية ودخولنا في إطار العالم الرقمي والذي اقتحم. جميع نواحي الحياة على الصعيد الاجتماعي والسياسي والاقتصادي وقد ظهر ذلك التأثير جلياً على الامن القومي للدول وأثر على شكل التفاعلات الدولية حتى اننا لا يمكن لنا ان نطلق عليه متغير التأثير السيبراني انما هو احد اهم الثوابت في استراتيجيات الدول، وقد ادلت الدول الفاعلة ومنها الولايات المتحدة الأميركية اهتماماً كبيراً للجانب السيبراني مع تحول ادوات الصراع بين الدول الكبرى الى وسائل وسبل جديدة اكثر ابتكاراً من ذي قبل كأحد مخرجات التطورات التقنية والعلمية المتمثلة بشبكة الانترنت والوسيط الرقمي.

لقد ترك التأثير السيبراني اثراً بارزاً في أمنها القومي نتيجة التدخلات الخارجية منها احداث ١١ سبتمبر ٢٠٠١، وما حصل في الانتخابات الرئاسية في الولايات المتحدة عام ٢٠١٦ وانطلاقاً من هذه المعايير والاحداث يكسب موضوع البحث أهمية قدر تعلق الأمر بحداثة الجانب السيبراني في العلاقات الدولية وتناول الولايات المتحدة الأميركية كبعد مكاني وقوة مهيمنة على الساحة الدولية في ظل الأحادية القطبية (unipolar).

أهمية البحث:

تكمن أهمية البحث في تحليل مفهوم السيبرانية والاختراقات التي تستهدف الامن القومي الامريكي من فواعل من غير الدول متمثلة بالمنظمات الارهابية والتي تروم اختراق الامن القومي للدول الفاعلة ومنها القوة العظمى متمثلة بالولايات المتحدة، لذا جهدت الإدارات

الأمريكية المتعاقبة على ترصين امنها القومي لها من خلال وضع وبناء استراتيجيات فعالة لردع التهديدات السيبرانية.

إشكالية البحث:

نستهل الدراسة بطرح عدة تساؤلات متمثلة بالآتي:

اولاً: ما هو مفهوم السيبرانية؟

ثانياً: ما هي الاستراتيجية للأمن السيبراني؟

ثالثاً: ماهي ردود الأفعال والاستجابة الامريكية بعد ظهور التهديدات الغير منظورة لا منها القومي ومحاولة الاضرار بالمصالح القومية العليا والبنى التحتية وتزايد العمليات الفضائية الإرهابية من قرصنة وتجسس؟.

فرضية البحث:

تنطلق فرضية الدراسة من أن الاستراتيجية السيبرانية قائمة على أسس رقمية– معلوماتية وان التهديدات السيبرانية تؤثر بشكل مباشر وحيوي للأمن القومي الأمريكي وما تمثله من خطر على ارواح المواطنين الامريكيين من حيث التهديدات بالقتل أو الخسائر المادية التي تتعرض لها الشركات الامريكية او الانكشاف الاستراتيجي لها، لذلك تعمل على صياغة امنها القومي من خلال الخطط الكفيلة لمعالجة وتلافي تلك الاختراقات.

منهجية البحث:

اعتمد البحث على (عدة مناهج) منها: المنهج التاريخي والتحليلي والوصفي في التعرف على مفهوم السيبرانية، كما تناولت الدراسة تحليل مسارات الصراع الاستراتيجي الأمريكي الاقليمي والدولي في الفضاء السيبراني وتصارعها مع الاستراتيجية الدولية والإقليمية لهيمنتها سيبرانياً وحماية أمنها القومي.

هيكلية البحث: تناول البحث عدة مباحث اهمها:

المبحث الأول: الإطار النظري والمفاهيمي للسيبرانية.

المبحث الثاني: أنماط الحروب السيبرانية وأثرها في الامن الدولي.

المبحث الثالث: الاستراتيجية السيبرانية الأميركية.

المبحث الرابع: التهديدات الفضائية السيبرانية للأمن القومي الأميركي.

المبحث الأول: الإطار المفاهيمي والنظري للسيبرانية

مع ظهور الثورة التكنولوجية ولوجنا في العصر الرقمي في القرن الحادي والعشرون وما نتج عنه من تداعيات وتحديات للأمن الدولي ظهر ما يسمى بالأمن القومي السيبراني كبعد جديد ضمن حقول الدراسات الأمنية اكتسب أهمية كبيرة بين الدول.

ترتبط كلمة سايبر (Cyber) من القيادة والإدارة، وهي كلمة يونانية قديمة تعني إدارة دفة السفينة لكن لاحقاً أصبحت ترمي الى كل ما يخص الانترنيت وتتنوع التعريفات التي تتحدث عن الفضاء السيبراني وظهر لأول مرة في القرن التاسع عشر في رواية (نيورومانسر)Neuromancer، التي تتناول الخيال العلمي للكاتب وليام جبسون (بطو ٢٠٢١).

وهناك من يشير الى ان مصطلح السيبرانية ورد لأول مرة في حقل الرياضيات ويُعد (نوربرتوبينر) أول من استعمل هذا المصطلح ١٩٤٨ في اثناء معالجته مشكلة القيادة والسيطرة (الفتلاوي ٢٠١٦، ٦١٤).

أما مصطلح سيبيريه أو سايبورغ فهي كلمتان استخدمتا من قبل مانفريد كلاينس وناثان كلاين عام ١٩٦٠ الدلاله على المزج بين الالكترونيات والانسان (شوقي ٢٠٢١).

قدمت وزارة الدفاع الامريكية تعريفاً دقيقاً لمفهوم الأمن السيبراني، فاعتبرته انه (جميع الاجراءات التنظيمية اللازمة لضمان حماية البيانات بجميع اشكالها المادية والالكترونية، من مختلف الجرائم، الهجمات التخريبية التجسس، والحوادث).

ولمواجهة التهديدات السيبرانية تعمل الدول بوضع خطط وإستراتيجيات وتكشف قدرتها لمواجهة الهجمات السيبرانية كجزء لا يتجزأ من استراتيجيتها الشاملة، ومع ضعف وانهيار بعض الدول ظهرت أنماط جديدة من النزاعات والصراعات مما زاد من خطورة التهديدات السيبرانية وهذا ما دعا وتوجب على الأنظمة الدولية الى اخذ احتياطات ووضع رؤى إستراتيجية للحد وتقويض تلك الهجومات (شلوش ٢٠١٨، ١٨٧-١٩٢).

لقد اصبح العلاقة بين مفهوم الامن القومي والتهديد علاقة تأثير متبادل وان أي محاولة لتفسير الامن لابد ان تبدأ بتحديد مصاد التهديدات وادى تصاعد حجم الاخطار الالكترونية من تغيير مضامين الامن القومي للدول مع ظهور جبهة جديدة متمثلة بالفضاء الالكتروني كمهدد لا من الدول وهو ما دفعها لإدخاله ضمن استراتيجيات الامن القومي لها وكذلك تطوير وتعزيز مجال الدفاع والحماية وتحديث جيوشها ضمن أجيال متطورة لتتعامل مع الحروب السيبرانية الحديثة وهذا ما اثر بشكل عام على العلاقات الدولية مع ظهور التهديدات السيبرانية من قبل الدول و الفواعل من غير الدول والتي لا تأبه بالقانون الدولي.

ان اتساع مفهوم الامن تحت مؤثرات التقدم التقني في مجال ثورة المعلوماتية بعد نهاية الحرب الباردة قد أضاف هذا الامر ابعاداً جديدة ومفاهيم أخرى مقاربة مع بروز الفضاء الالكتروني كساحة للصراع ابرزت عدة مفاهيم أخرى مقاربة كالحرب الافتراضية والحرب المعلوماتية والأمم السحابي والقوة السيبرانية وامن الانترنت والردع السيبراني والفضاء السيبراني...الخ.

المبحث الثاني: أنماط الحرب السيبرانية وتداعياتها على الامن الدولي

هناك أنماط مختلفة من الحروب والهجمات السيبرانية تتراوح ما بين الحروب الباردة والساخنة نوجز أهمها:

أولاً: نمط الحروب السيبرانية الباردة المنخفضة الشدة:

يعد هذا النمط تعبيراً واضحاً عن الصراع المستمر بين فاعلين متصارعين وقد يكون ممتداً ودائم النشاط العدائي او غير السلمي. يتم ممارسة هذا النمط عبر القيام بعدة وسائل أهمها: شن الحروب النفسية والاختراقات المتنوعة والتجسس وسرقة المعلومات والأفكار والتنافس بين الشركات التكنولوجية وأجهزة الاستخبارات الدولية.

يبرز هذا النمط في حالات منها حالات الحروب ذات الطابع السياسي ذات الأبعاد الدينية – الاجتماعية الممتد، مثل الصراع الصهيوني–العربي، او الحروب الهندية – الباكستانية، الصراع بين الكوريتين (عبد الصادق ٢٠١٣).

ثانياً: نمط الحروب السيبرانية المتوسطة الشدة

يستمد هذا النمط من الحروب شدته من قوة أطرافه وكذلك الارتباط بالأعمال العسكرية التقليدية بالأخص في ظل بعض التقديرات التي تشير الى ان التكلفة لهذه الحروب (٤) اضعاف نظيراتها التقليدية كما يمكن من تمويل حملة حربية كاملة عبر الانترنت بتكلفة دبابة. من الأمثلة الواضحة لهذا النمط من الحروب متوسطة الشدة هجمات حلف الناتو على يوغسلافيا عام ١٩٩٩ كذلك في الحروب بين حزب الله (واسرائيل) عام ٢٠٠٦ والحروب الروسية الجورجية وغيرها من الحروب.

ثالثاً: نمط الحروب السيبرانية الساخنة العالية الشدة

لم يشهد العالم نشوب حرب في الفضاء الالكتروني بشكل منفرد ولكن احتمالية وقوعها غير مستبعد في المستقبل مع التطور المستمر والمتزايد للقدرات التكنولوجية والاعتماد بين الدول و الفواعل غير الدولية على الفضاء الالكتروني بشكل واسع من خلال سيطرة العامل التكنلوجي على القيادات العسكرية للعمليات (عبد الصادق ٢٠١٣).

المبحث الثالث: الإستراتيجية السيبرانية الأمريكية

ان النجاح في الفضاء السيبراني أمر ضروري لتعزيز المصالح الحيوية الامريكية، وتحدد التكنولوجيات الرقمية عدد العمليات التي تصف عمل المجتمعات الحديثة والتي تمتد من الاتصال الى التمويل ومن الكهرباء الى النقل ومن التجسس الى الامن القومي، القدرة على التحكم في كيفية استخدام هذه التقنيات في الحاضر، تؤثر على مسار تطورها في المستقبل – وهذا يعد عنصر حيوي للأمن القومي، هناك استراتيجية شاملة لضمان استمرار دور الانترنيت في تعزيز الحرية والامن والازدهار، وهناك اعتراف بأن امريكا هي من اخترع الانترنيت، وان الفضاء الالكتروني اصبح اليوم عالم حقيقي اقل من ١ من اصل ١٠ في العالم من ثلاثة مليارات مستخدم للانترنيت يعيشون في امريكا بينما

تقريباً ربعهم يعيش في الصين، الطبيعة العالمية للفضاء السيبراني يعني أن أمريكا لا تستطيع عزل نفسها عن عالم الانترنيت ولا يتوقع منها ان تملي من جانب واحد السياسات والممارسات التي تحكم استخدامه وتطوره في المستقبل، حيث يجب عليها استخدام نفوذها وسلطتها لضمان بقاء الانترنيت قوة للخير في العالم، ولكي تكون ناجحة فأنها تحتاج الى استراتيجية شاملة (خريسان ٢٠٢١).

ان مهمة وضع مثل هذه الاستراتيجية تكون معقدة بسبب الطبيعة الشاملة للفضاء السيبراني الذي يتخلل كل عنصر من العناصر للمجتمعات الحديثة، وان استخدام التكنولوجية السيبرانية يدعم حرية الإنسان ويتبنى اجراءات قوية وفعالة لتعزيز قيم الليبرالية الديمقراطية في الفضاء السيبراني وفي هذا المجال قدّم جيفري اي اسيناش من معهد المشروع الأميركي لأبحاث السياسة العامة توصيات إلى الإدارة الأميركية أهمها (خريسان ٢٠٢١):

١-استخدام جميع العناصر الدبلوماسية والاقتصادية الامريكية التي تثني الدول الاستبدادية عن ممارسة الرقابة والقمع.

٢-توسيع كبير في وسائل الاعلام الاجتماعية الامريكية وغيرها من جهود الاتصالات الرقمية للتأثير بالتواصل الفعال وتعزيز الحريات الاساسية على الانترنيت.

٣-اضفاء الطابع الرسمي وتوسيع وتعزيز تحالف حرية الانترنيت.

٤-تشجيع زيادة الوصول الى الانترنيت من خلال سياسات التسويق.

٥-تعزيز دور منظمات بالأخص منظمات المجتمع المدني في الدراسة ودعم حرية الانترنيت.

٦-توسيع وتكثيف ودعم القطاعين: العام والخاص، للمشاركة في المحافل الدولية حيث تم تعيين سياسات الانترنيت.

بدأت الادارة الامريكية في تصور مصطلح السيبرانية في عهد الرئيس الامريكي السابق بيل كلينتون عام ١٩٩٨، وجميع وثائقه المتعلقة بإستراتيجية الأمن القومي للأعوام

١٩٩٨ و ٢٠٠٠ و ٢٠٠١ وهي تهديدات الكترونية ذات صلة عامة بحماية الهياكل الاساسية الوطنية الحرجة، والجريمة والشراكات بين الولايات ، فأنشأت وزارة الدفاع الامريكية البنتاغون قوة دفاع شبكات الكومبيوتر المشتركة (JTF – CND) لتتولى مسؤولية الحماية بشقيها (الدفاعي الالكتروني والهجومي الالكتروني)، قبل ان يتم الفصل بينهما، لتؤول مهمة الهجوم الى وكالة الامن القومي، ومهمة الدفاع الى وكالة الدفاع عن انظمة المعلومات، واللتين اجتمعتا لاحقاً تحت مظلة القيادة الالكترونية الامريكية في عام ٢٠٠٩، التي يقودها مدير وكالة الامن القومي نظراً لتمتعها بإمكانات كبيرة في مجال تكنولوجيا المعلومات والاتصالات، كما تدل على ذلك التسريبات الاخيرة بخصوص تجسس الوكالة على عدد من الدول (نون بوست ٢٠١٥). في عام ٢٠٠٠ اخذت الولايات المتحدة بتطوير برنامج سمي (كارنييفور) أو (الملتهم) وظيفته التجسس على جميع انواع الاتصالات التي تتم عبر الانترنيت لا سيما مع وجود شبكة تجسس عالمية أمريكية أوربية اسمها ايشلون، أسستها وكالة الأمن القومي الامريكي مع عدد من المؤسسات الاستخبارية العالمية هدفها التجسس على الاتصالات الرقمية عن طريق الاقمار الصناعية، وهذا البرنامج الملتهم هو نظام الكتروني مصمم يسمح لوكالة المباحث الفيدرالية الامريكية بالتعاون مع شركة المزودة بالانترنت بتطبيق حكم محكمة جمع المعلومات محددة حول رسائل البريد الالكتروني لمستخدم يستهدفه التحقيق (الزنط ٢٠١٠، ٢٠).

وقد قامت امريكا منذ عام ٢٠٠٥ بعمل مناورات تعرف بـ (Ceberstrom) (العاصفة الالكترونية) لاختبار قدراتها على مواجهة الاخطار كان آخرها عام ٢٠١٠ مع تزايد عمليات الاختراق لشبكاتها الدفاعية لما تسببه من خسائر اقتصادية عالمية تقدر ١٠٠ بليون دولار سنوياً، واخذت هذه القضية منحى آخر بعد تزايد الاختراقات لوزارة الدفاع الامريكي في إطار الحرب الباردة مع الصين لأنها المتهمة الأولى في هذه الاختراقات في ظل التجسسات الالكترونية التي تتبعها الدول من اجل خرق الامن القومي للولايات المتحدة الامريكية.

وحددت استراتيجية واشنطن للأمن القومي (١٢) عنصراً من عناصر الامن القومي في عام ٢٠٠٦، هي الاتصالات السلكية واللاسلكية ومحطات الطاقة والبنية التحتية الخاصة بصناعة نظم الدفاع والاسلحة ، ونظم استخراج وصناعة ونقل وتخزين الغاز والنفط، والزراعة وتوزيع الاطعمة والخدمات المصرفية والمالية ، ونظم المواصلات وامدادات المياه، وخدمات طبية وخدمات البريد والنقل وخدمات الطوارئ واخيرا الحكومة نفسها، وهذه البنى تصبح مرمى الهجمات الالكترونية ، لدرجة ان لجنة المصالح القومية الامريكية اكدت على حماية هذه البنى من التهديد السيبراني في إستراتيجية الأمن القومي لعام ٢٠١٠، هذه البنية التحتية هي بمنزلة اصل قومي لتدعيم الامن القومي الامريكي (خليفة ٢٠١٧، ١٢٠-١٢١). وقد اعلنت الولايات المتحدة الامريكية عام ٢٠٠٩ بتشكيل قيادة عسكرية للفضاء الالكتروني لحماية شبكات الجيش الامريكي ليبرز اهمية الفضاء الالكتروني بما يتضمنه من عدة قضايا ذات صلة وثيقة بأمنها القومي في ظل الاعتماد الدولي عليه فيما يتعلق بتسيير عمل البنية التحتية الكونية للمعلومات امام المنشآت المدنية والعسكرية من خلال تعرضه للهجوم يستهدفه كوسيط وحامل للخدمات او بشل عمل انظمتها المعلوماتية فأن التحكم في تنفيذ هكذا هجمات يعد ادارة السيطرة ونفوذ استراتيجية بالغة الأهمية في زمن السلم والحرب.

لاحظت وزارة الدفاع الامريكية في تقريرها حول الموازنة المالية ٢٠١٤، اعادة تنظيم على مستوى الموارد البشرية والكفاءات لديها لتعزيز قوتها السيبرانية في مواجهة تهديدات امنها القومي ضمن فرق متخصصة في مجالات ثلاث هي حماية الشبكات ، وشل قوة العدو السيبرانية، وحماية الدفاع الوطني وانشاء قوة سيبرانية لعام ٢٠٠٦ مؤلفة من (٤٠) فرقة موزعة على مهمات هجومية ودفاعية، وتتوزع مسؤولية الأمن السيبراني فيها بين وزارة الداخلية ومكتب التحقيقات الفيدرالية ووزارة الدفاع بما فيها قيادة الأمن السيبراني التي تضم وكالة الأمن القومي التي تستند اليها العمليات الهجومية فضلاً عن وحدات من وكالة الاستخبارات المركزية، في المقابل يتولى الجهاز القيادي السيبراني التابع للقيادة

الفيدرالية مسؤولية حماية البنية التحتية السيبرانية العسكرية ويضم هذا الجهاز القيادة السيبرانية للجيش وقيادة القنوات الجوية والبحرية، وتتعاون الوزارتين على تنسيق جهودهما بموجب اتفاق عام ٢٠١٠ فاستخدمت الولايات المتحدة الأمريكية بعد هجمات الحادي عشر من ايلول عام ٢٠٠١، مكافحة الارهاب كذريعة لاستخدامها تقنيات حديثة للمراقبة والتجسس على مواقع شبكة المعلومات الدولية الانترنيت والاتصالات الهاتفية وبرامج الكترونية للتجسس(الاشقر ٢٠١٧، ٧٥-٧٧).

المبحث الرابع: التهديدات الفضائية السيبرانية للامن القومي الأمريكي

بعد احداث الحادي عشر من ايلول عام ٢٠٠١ بدأ التركيز على الفضاء الالكتروني كتهديد امني من حيث استخدام القوى الاقليمية والدولية والتنظيمات الارهابية لهذا المجال الحيوي قليل الجهد والتكلفة من ناحية تنفيذ الهدف و ذات نتيجة هائلة من حيث الاستخدام العملياتي ضد الولايات المتحدة الامريكية (شلوش ٢٠١٨، ١٩٢).

ولعل منابرز التهديدات التي ممكن ان يواجهها الامن القومي الامريكي في المجال الفضائي السيبراني وله تداعيات على امنها القومي وهي:

أولاً: التجسس الالكتروني السيبراني: وهذا يكون من خلال الدخول الى الانظمة الخاصة بالولايات المتحدة الأمريكية لإضعافها وضرب المصالح القومية لها، من قبل الدول التي تريد للقوة العظمى زوال مكانتها في النظام الدولي سواء كانت دول منافسة مثل روسيا وكوريا الشمالية والصين فيعترض المرتكبون خطوط الاتصالات السلكية واللاسلكية (البريد الالكتروني او اتصالات الصوت على الانترنيت) ويتم هذا الامر لضرب مصالحها القومية العليا واما لكشف امور سرية وفضحها امام الجمهور او لبيع المعلومات نظراً لقيمتها التجارية او لكشف اسرار مالية او صناعية عن الشركات المنافسة او لسرقة كلمة السر للحسابات المصرفية او البريد الالكتروني أو لأسباب سياسية إذا كان موجهاً دولة معينة (اللجنة الاقتصادية والاجتماعية لغربي آسيا الاسكوا ٢٠١٥، ٧٢)، حيث قدرت واشنطن خسائرها نتيجة القرصنة عام ٢٠٠٢، و٨,٤٥٥ بليون دولار وقدرت وزارة العدل الامريكية بحدود ١٥٠ الف شخص تأثروا بخسائر تتجاوز ٢١٥ مليون دولار ، وفي عام

٢٠٠٣ أصدرت لجنة التجارة الفيدرالية الامريكية تقريراً بأن هناك ٩,٩ مليون شخص تعرضوا لهجمات القرصنة والتجسس مع متوسط خسائر ١٢٠ مليار دولار امريكي ، والقضية المتهم فيها ٤٣ مصرياً عام ٢٠٠٩ بالسطو على بنك اوف امريكا بولاية كاليفورنيا والاستيلاء على مبلغ حوالي مليون دولار و ٧٠٠ الف دولار امريكي كل ذلك له اثر على الامن القومي.

فخلال عام ٢٠١٤ بعد هجمات حجب الخدمة ٢٠١٢-٢٠١٣ على القطاع المالي أعلن البنك جي بي مورغان عن إنفاقه ٢٥٠ مليون دولار للأمن السيبراني، وتم اختراق شركة هوم ديبوت لبطاقات الائتمان ومكتب إدارة شؤون الموظفين، هذه التهديدات للأمن القومي تأتي من دول قومية تمتلك برامج حاسوبية متطورة للغاية مثل روسيا الاتحادية التي أنشأت قيادتها الالكترونية والصين التي لا تزال تعمل على التجسس الاقتصادي ضد الشركات الأمريكية وهذا تهديد مستمر إما من دول ذات قدرات تقنية قليلة مثل إيران التي تورطت في هجمات DDOS بين عامي ٢٠١٢-٢٠١٣ ضد الولايات المتحدة ومؤسساتها المالية وفي هجوم عبر الانترنيت في شباط ٢٠١٤ على شركة كازينو لاس فيغاس ساندز وكوريا الشمالية المسؤولة عن الهجوم الالكتروني الذي نفذ في تشرين الثاني عام ٢٠١٤ ضد شركة سوني بيكتشرز انترتينمنت أو المجرمون الذين يقصدون الربح أو القراصنة ذو الدوافع الأيديولوجية أو المتطرفون (اركلابر ٢٠١٥)، وأوضحت الادارة الأمريكية إن تهديد الرئيس يأتي من الصين لان أجهزة الاستخبارات العسكرية الصينية يسعى إلى الحصول على التكنولوجيا الأمريكية العسكرية، بناءاً على تقرير شركة لوكيد مارتن انه عام ٢٠١٣ تم إطلاق هجوم سايبري يستهدف الانموذج الجديد الذي تصنعه الشركة من طائرة الشبح المقاتلة ذات المهام المشتركة (بيردسول٢٠١٤ ، ١٧).

ثانياً: الإرهاب السيبراني: ويتمثل بالاعتداء على شبكة الانترنيت بغية تعطيل خدماتها، والاهم من ذلك هو الهجمات على البنية الاساسية المعلوماتية التي تشغل كثيراً من القطاعات الحساسة كالنقل والطاقة والطيران . ويمكن ايضا استخدام الانترنيت للترويج

للأفكار الإرهابية أو لنشر مواد تدريبية كمصنع متفجرات او لجمع التمويل او لتجنيد اشخاص او للتواصل بين الشبكات الارهابية وهو ما تخشى منه الولايات المتحدة الامريكية منذ احداث ١١ أيلول ٢٠٠١ (عبد الفتاح ٢٠١٧، ٢٥–٢٩)، فدور الانترنيت ادى الى انتشار ظاهرة الارهاب ثم تناول الاستراتيجيات الاعلامية التي اعتمدها اسامة بن لادن قائد تنظيم القاعدة الارهابي حيث انشأ ادارة اعلام القاعدة عام ١٩٨٨ وذلك لتكريم المجاهدين ضد الاتحاد السوفيتي ثم تحولت هذه الاداة للهجوم على الولايات المتحدة وتكفيرها وكل الدول التي لا تطبق الشريعة (المعهد المصري للدراسات ٢٠٢١). مثلت حوادث القرصنة الالكترونية لأنظمة الطائرات والمخاوف من استهداف مجموعات ارهابية للنقل الجوي دافعاً للدول المواجهة لتلك المخاطر الالكترونية لأمن المطارات المتصل بالأمن القومي الامريكي، وبحسب قرار الحظر الذي اتخذته فأنه يسري على الرحلات القادمة مباشرة من ١٠ مطارات في ٨ دول وينطبق على ٩ شركات جميعها غير امريكية بسبب عدم امتلاكها خطوط طيران مباشرة من المطارات المذكورة للولايات المتحدة: شركات الخطوط الجوية التابعة للدول: مصر، الاردن، السعودية، الكويت، المغرب، قطر، الامارات، تركيا (هلال ٢٠٢١).

ثالثاً: الحروب الالكترونية السيبرانية: وتعني قيام دولة او فواعل من غير الدول بشن هجمات الكترونية في اطار متبادل او من قبل طرف واحد وبالرغم من ظهور مسمى "الحرب الالكترونية السيبرانية" إعلاميا فأنه يعد مفهوماً قديما يقتصر على رصد حالات التشويش على انظمة الاتصال والرادار واجهزة الانذار بينما يكشف الواقع الحالي في الفضاء الالكتروني السيبراني عن دخول شبكات الاتصال والمعلومات على بنية ومجال الاستخدامات العسكرية (عبد الصادق ٢٠١٤، ٣١).

رابعاً: الحث على الكراهية والعنف والعنصرية: تستخدم مجموعات متطرفة المواقع الالكترونية لنشر افكارها وهذه المواقع في ازدياد مستمر للذم والتشهير والتهديد والابتزاز عبر شبكة الانترنيت ولا سيما على الموقع الالكتروني ومواقع التواصل الاجتماعي من

اجل جعل سمعة الولايات المتحدة الامريكية سيئة الصيت امام الرأي العام الداخلي والعالمي (اللجنة الاقتصادية والاجتماعية لغربي آسيا الاسكوا ٢٠١٥، ٧٣).

خامساً: الاستخبارات المضادة وروسيا الاتحادية او الصيني: هي المصدر الرئيسي للتهديد لاختراق أجهزة صنع القرار الوطني ووكالة الاستخبارات السرية للولايات المتحدة من قبل استخبارات الدول الاجنبية وهو استهداف لأمن المعلومات الوطنية والسرية للشركات والمؤسسات الامريكية المتعاقدة مع الدفاع والمالية والطاقة وغيرها (اللجنة الاقتصادية والاجتماعية لغربي آسيا الاسكوا ٢٠١٥، ٣).

سادساً: الفضاء والفضاء المضاد: تزايدت التهديدات لأنظمة الفضاء التابعة للولايات المتحدة الامريكية وخدماتها في العام ٢٠١٥ وما بعده وذلك مع تزايد الخصوم المحتملين واظهارهم قدرات الفضاء المضاد التخريبية، لدى الصين قدرات تشويش على الاقمار الصناعية فأجرت في تموز عام ٢٠١٤ تجربة صواريخ غير مدمرة مضادة للأقمار الصناعية ، فتزايدت المخاوف الدولية من سباق عالمي حاد حول التسلح في الفضاء الخارجي بعد قيام الصين عام ٢٠٠٧، بتدمير القمر الصناعي (فنغ يون١سي) المخصص للأحوال الجوية في الفضاء بصاروخ مضاد للأقمار الصناعية ، وهو ما اعتبرته واشنطن في وقتها نقلة نوعية وتطورا تكنولوجيا غير مسبوق بالنسبة الى بكين (شير ٢٠٢١). إن من ابرز الأهداف الالكترونية التي يتم استهدافها في الجغرافيا الأمريكية تتمثل في (خليفة ٢٠١٧، ١١٤-١٢٠):

١. على المستوى الاتحادي البيت الابيض والكونغرس الامريكي ووزارة الداخلية كونها رموز للأمن القومي الأمريكي.

٢. على المستوى العسكري يتم استهداف وزارة الدفاع والوحدات القيادية القتالية لعرقلة عمليات عسكرية كما هو الحال في العراق وأفغانستان .

٣. على المستوى المدني استهداف البنى التحتية فضلاً عن المؤسسات المالية ومحطات الطاقة والاتصالات لأنها تصيد اكبر عدد من السكان الامريكيين وتعد من اخطر الأهداف

لأنها لا تقتصر على الاستخدامات المدنية بل والاستخدامات العسكرية وتشمل تهديد المصالح الحيوية القومية الامريكية المختلفة ، وهذه بنى حرجة للولايات المتحدة الأمريكية لأنها تتضمن النظم والأصول سواء كانت مادية ام افتراضية والتي يؤدي تدميرها او التلاعب بها في تهديد للأمن القومي الامريكي او الاقتصاد الامريكي او الرعاية الصحية أو الأمن العام.

الخاتمة:

ما زال مصطلح الهجوم السيبراني من المفاهيم الحديثة التي لا يوجد اجماع دولي بشأن تعريفه مما ادى إلى صعوبة تكييف وتحديد المسؤولية الدولية عنه، وان ميزة الهجمات السيبرانية في انخفاض التكلفة والسهوله في اللجوء لها، إذ لا تتطلب عدداً كبيراً من العسكريين المقاتلين والآلاف من الأسلحة كالنزاعات التقليدية بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهن الخبرة والمهارة التكنولوجيا السيبرانيه وثغرات برامج الأنظمة الكومبيوترات لاستخدامها ضد دولة أو دول أخرى، إلا أن هذه الميزة تتحول إلى مصدر قلق كبير إذا ما نظرنا إلى آثار هذه الهجمات وتبعاتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشأة نووية أو مصادر الطاقة كشبكة الكهرباء والمياه، ونظراً لطبيعة التهديدات الفضائية السيبرانية المتجددة بصورة مستمرة فهناك عناصر تغيير واستمرار حيوية في الطرق والمعالجات التي تتضمنها الاستراتيجيات الأمريكية للأمن القومي فيما يخص الأمن الفضائي السيبراني وهي استراتيجيات استباقية وقائية لردع الهجمات الفضائية السيبرانية شاملاً الأبعاد السياسية والعسكرية والاقتصادية والمدنية إذ إدخالها وحدات السيبرانية داخل جيوشها وتعزيز الأطر التشريعية والقانونية لملاحقة مصادر التهديد والتعاون مع الدول الأخرى لمكافحة هذه الظاهرة لان الأمن القومي مهدد بصورة مستمرة من التهديدات السيبرانية وليس هناك طريقة فعالة لمواجهة ذلك إلا بالتعاون مع الدول الأخرى ذلك إن الأمن القومي الأمريكي له انعكاس كبير على الأمن الدولي بأكمله.

لقد ادى تصاعد حجم الاخطار الالكترونية في تغيير مضامين الامن القومي للدول واصبحت تبحث عن اعادة تعريفه مع ظهور جبهة الفضاء الالكتروني كمهدد لامنها وهو وما دفعها الى ادخاله الى استراتيجيات الامن القومي، والعمل على تطوير قدراتها في المجال الدفاعي وكذلك الحماية والهجوم والتحديث المستمر لجيوشها للتعامل مع هذا النوع من الحرب الالكترونية الجديدة، ماترك اثره في العلاقات الدولية ولاسيما مع بروز خطر التهديدات من دول او جهات لاتكترث بالقانون الدولي.

قائمة المصادر:

- اركلاب، جيمس. ٢٠١٥. "تقييم التهديد العالمي للولايات المتحدة الامريكية. وكالة الاستخبارات الامريكية. ٥ تموز، ٢٠١٥.

https://newssyrian.net

- الاشقر، منى جبور. ٢٠١٧. *السيبرانية هاجس العصر*. بيروت: المركز العربي للبحوث القانونية والقضائية.

- الزنط، سعد عطوه، ٢٠١٠. "الارهاب الالكتروني واعادة صياغة استراتيجيات الامن القومي"، ورقة بحثية مقدمة الى مؤتمر الجرائم المستحدثة: كيفية إثباتها ومواجهتها. مصر: المركز القومي للبحوث الاجتماعية والجنائية، ١٥ –١٦ نوفمبر، ٢٠١٠.

- الفتلاوي، احمد عبيس نعمة. ٢٠١٦. "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد ٤:٦١٠-٦٨٧.

- اللجنة الاقتصادية والاجتماعية لغربي آسيا الاسكوا، ٢٠١٥. "الأمن في الفضاء السيبراني ومكافحة الإجرام السيبرانية في المنطقة العربية ": توصيات سياساتية، الأمم المتحدة .٧٣.

- المعهد المصري للدراسات. ٢٠١٦. "استخدام القوة الالكترونية في التفاعلات الدولية". المعهد المصري للدراسات.٢٩ اكتوبر، ٢٠١٦.https://eipss-eg.org

- الموسوعة السياسية. ٢٠١٦. "تعريف الأمن السيبراني". ٢٩ اكتوبر، ٢٠١٦.

https://www.political.encyclopedia.org

- بطو، احمد. ٢٠٢١. "ما هو الفضاء السيبراني؟". مقالات سايبروان. ٥ نوفمبر، ٢٠٢١.

https://cyberone+com&sa=X&ved=2ahUKEwjOpaCzirT5AhXcW_EDHc2vq0QpBd6BAgBEAE&biw=1366&bih=625&dpr=1

- بيردسول، مارك. ٢٠١٤. مستقبل الاستخبارات في القرن الحادي والعشرين. ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية.

- خريسان، باسم علي. "الإستراتيجية الأمريكية للفضاء السيبراني: تعزيز الحرية والأمن والازدهار". شبكة النبأ المعلوماتية .٢٤ اكتوبر، ٢٠١٧. https://annabaa.org/arabic/informatics/12978-

خليفة، ايهاب. ٢٠١٧. القوة الالكترونية: كي يمكن ان تدير الدول شؤونها في عصر الانترنيت. بيروت: دار العربي للنشر والتوزيع.

- شلوش، نورة .٢٠١٨. "القرصنة الالكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الانسانية، المجلد ٨. العدد ٢ :١٨٧-١٩٢.

- شوقي، إيهاب. "الحرب السيبرانية حرب المستقبل المفزعة". شبكة الاخبار العربية. ١٩شباط، ٢٠١٥.

https://www.anntv.tv

- شير،هشام ."التنافس على عسكرة الفضاء"، صحيفة الخليج السعودية.٢٤ نيسان،٢٠١٤.

https://www.alkhaleej.ae/%25D9%2585%25D9%2584%25D8%25AD%25D9%2582/%25D8%25A7%25D9%2584%25D8%25AA%25D9%2586%25D8%25A7%25D9%2581%25D8%25B3-%25D8%25B9%25D9%2584%25D9%2589-%25D8%25B9%25D8%25B3%25D9%2583%25D8%25B1%25D8%25A9-%25D8%25A7%25D9%2584%25D9%2581%25D8%25B6%25D8%25A7%25D8%25A1&cd=4&hl=en&ct=clnk&gl=iq

- عبد الصادق، عادل. ٢٠١٣. "الفضاء الالكتروني وتهديدات جديدة للأمن القومي"، قضايا استراتيجية. مصر: المركز العربي لأبحاث الفضاء الالكتروني. ١١فبراير، ٢٠١٣.

https://accronline.com/article_detail.aspx?id=8745

- عبد الفتاح، فاطمة الزهراء .٢٠١٧. "تطور توظيف جماعات العنف للإرهاب السيبراني". *ملحق مجلة السياسة الدولية*. العدد ٢٠٨. القاهرة: مركز الاهرام للدراسات الاستراتيجية والسياسية :٢٩-٢٥٠.

- نون بوست.٢٠١٥. "حروب الفضاء الالكتروني". نون بوست.٢٠ ايار، ٢٠١٥.

https://www.noonpost.com/content/5548&cd=1&hl=en&ct=clnk&gl=iq

- هلال، محمد عزت. "آليات المواجهة: تهديدات الأمن الالكتروني في قطاع الطيران المدني". مركز المستقبل للأبحاث والدراسات المتقدمة. الإمارات العربية المتحدة. ٢٥ ايار، ٢٠١٧.

https://futureuae.com/ar/Mainpage/Item/2827

List of references:

Al-Ashqar, Mona Jabbour. 2017. Cyber Obsession of the Age. Beirut: Arab center for Legal and Judicial Research.

Al-Fatlawi, Ahmed Obais Nehme. 2016. "Cyber-attacks: their concept and the international responsibility arising from them in the light of contemporary international organization*", al- mohaqiq al-hilli Journal for legal and political sciences*, No.610: 4-687.

Abdel fattah, Fatima al-zahra. 2017. " the evolution of the employment of violent groups for cyber terrorsm*". supplement of the international polities journal*, issue208.cairo:al-ahram center for strategic and political studies:29-250.

Abdel sadiq, adel. 2013. "cyberspace and new threats to national security", strategic issues. Egypt: the arab center for cyberspace reseaech. February 11,2013. https://accronline.com/article_detail.aspx?id=8745

Birdsall, mark. 2014. *the future of intelligence in the twenty-first century*. Abu Dhabi: emirates center for strategic studies and research.

Butto, Ahmed. 2021. "what is cyberspace? ". cyberspace articles. November5, 2021.https://cyberone+com&sa=X&ved=2ahUKEwjOpaCzirT5AhXcW_EDHc2vq0QpBd6BAgBEAE&biw=1366&bih=625&dpr=1

Economic and socal commission for western Asia Escwa, 2015, " security in cyberspace and combating cybercrime in the arab region". policy recommendations, united nations 73.

Egyptian institute for studies. 2016. "using electronic power in international interactions", Egyptian institute for studies. October 29, 2016. https://eipss-eg.org - Ehalifa, Ehab. 2017. electronic power: how states can manage their affairs in the age of the internet. Beirut: Dar al- Arabi for publishing and distribution.

El- Zant, Saad Atwa, 2010. "Cyber terrorism and reformulating national security strategies", a research paper presented to the new crimes conference: how to prove and confront it Egypt: national center for social and criminal research, November 15-16,2010.

Erclaber, James. 2015. "Global threat Assessment to the United States of America". CIA. July5, 2015. https://newssyrian.net

political. encyclopedia .2016. defining cyber security. October 29, 2016. https://www.political.encyclopedia.org.

Hilal, Mohamed Ezzat. Coping mechanisms: cyber security threats in the civil aviation sector. Future center for research and advanced studies, United Arab Emirates. may 25, 2017. https://futureuae.com/ar/Mainpage/Item/2827

Khreisan, Bassem Ali. "The American cyber strategy: promoting freedom, security, and prosperity". Al-naba information network. October 24, 2017. https://annabaa.org/arabic/informatics/12978

shaloush, noea. 2018. electronic piracy in cyberspeace: the escalating threat to the security of states. *Journal of Babylon center for human studies*,vol 8.issue 2:178-192.

Shawky, Ihab. "Cyber warfare, the frightening war of the future". Arab news network. February 19, 2015. https://www.anntv.tv

Sher, Hisham. "The competition for the militarization of space", the Saudi gulf newspaper, april 24,2014. https://www.alkhaleej.ae/%25D9%2585%25D9%2584%25D8%25AD%25D9%2582/%25D8%25A7%25D9%2584%25D8%25AA%25D9%2586%

25D8%25A7%25D9%2581%25D8%25B3-
%25D8%25B9%25D9%2584%25D9%2589-
%25D8%25B9%25D8%25B3%25D9%2583%25D8%25B1%25D8%25A9-
%25D8%25A7%25D9%2584%25D9%2581%25D8%25B6%25D8%25A7%25D8%25A1&cd=4&hl=en&ct=clnk&gl=iq

Noon post 2015. "Cyber wars". Noon post. may 20,2015. https://www.noonpost.com/content/5548&cd=1&hl=en&ct=clnk&gl=iq