



مجلة العلوم السياسية

اسم المقال: التأثير السيراني في الأمن القومي للدول الفاعلة (الولايات المتحدة الاميركية) انموذجاً

اسم الكاتب: أ.د. اسراء شريف الكعوب

رابط ثابت: <https://political-encyclopedia.org/library/445>

تاريخ الاسترداد: 2025/04/20 10:45 +03

الموسوعة السياسية هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترن.

لمزيد من المعلومات حول الموسوعة السياسية – Encyclopedia Political – يرجى التواصل على

info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسية – Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام

<https://political-encyclopedia.org/terms-of-use>

تم الحصول على هذا المقال من موقع مجلة العلوم السياسية جامعة بغداد ورفده في مكتبة الموسوعة السياسية مستوفياً
شروط الملكية الفكرية ومتطلبات رخصة المشاع الإبداعي التي يتضمن المقال تحتها.



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/jcopol.vi64.628>



This work is licensed under a [Creative Commons](#)
[Attribution 4.0 International License](#)

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 الأمريكية) المودجا

أ.د. اسراء شريف الكعوب

جامعة بغداد/ كلية العلوم السياسية

drisraashareef68@gmail.com

تاریخ الاستلام: ٢٠٢٢/٦/١١ تاریخ قبول النشر: ٢٠٢٢/٨/١٤

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 بالوسيل 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 الأمريكية لاستغلال مكامن القوة التي وفرها الفضاء السiberاني وقد بُرِزَ
الحِيز السiberاني كحالة جديدة في أنماط الحروب والصراعات استحوذت على اهتمام
الولايات المتحدة الأمريكية واعتبرت من أهم التحديات التي تواجه الامن القومي الأمريكي
وعنصراً مؤثراً في العلاقات الدولية.

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

المقدمة:

ما لا شك فيه ان موضوع الامن السiberاني 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 السiberاني انما هو احد اهم الثوابت في استراتيجيات الدول، وقد ادلت الدول الفاعلة ومنها الولايات المتحدة الأمريكية اهتماماً كبيراً للجانب السiberاني مع تحول ادوات الصراع بين الدول الكبرى الى وسائل وسبل جديدة اكثر ابتكاراً من ذي قبل كأحد مخرجات التطورات التقنية والعلمية المتمثلة بشبكة الانترنت والوسیط الرقمي.

لقد ترك التأثير السiberاني 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 والاحاديث يكسب موضوع البحث أهمية قدر تعلق الأمر بحدثة الجانب السiberاني في العلاقات الدولية وتناول الولايات المتحدة الأمريكية وبعد مكاني وقوة مهيمنة على الساحة الدولية في ظل الأحادية القطبية (unipolar).

أهمية البحث:

تكمّن أهمية البحث في تحليل مفهوم السiberانية والاختراقات التي تستهدف الامن القومي الأمريكي 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 ترسيخ انمنها 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: ما هي ردود الأفعال والاستجابة الأمريكية بعد ظهور التهديدات الغير منظورة لا منها القومي ومحاولة الضرار بالمصالح القومية العليا والبني التحتية وتزايد العمليات الفضائية الإرهابية من قرصنة وتجسس؟.

فرضية البحث:

تنطلق فرضية الدراسة من أن الاستراتيجية السيبرانية قائمة على أسس رقمية - معلوماتية وإن التهديدات السيبرانية تؤثر بشكل مباشر وحيوي للأمن القومي الأمريكي وما تمثله من خطر على ارواح المواطنين الأمريكيين من حيث التهديدات بالقتل أو الخسائر المادية التي تتعرض لها الشركات الأمريكية او الانكشاف الاستراتيجي لها، لذلك تعمل على صياغة انمنها 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 الإقليمي والدولي في الفضاء السيبراني وتصارعها مع الاستراتيجية الدولية والإقليمية لهيمنتها سيبرانياً وحماية أنمنها 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 السiberانية الأمريكية.

المبحث الرابع: التهديدات الفضائية السiberانية للأمن القومي الأمريكي.

المبحث الأول: الإطار المفاهيمي والنظري للسiberانية

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

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

وهناك من يشير إلى أن مصطلح السiberانية ورد لأول مرة في حقل الرياضيات ويدع (نوربرتوينر) أول من استعمل هذا المصطلح ١٩٤٨ في اثناء معالجته مشكلة القيادة والسيطرة (الفتلاوي ٢٠١٦، ٦١٤).

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

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

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

لقد اصبح العلاقة بين مفهوم الامن القومي والتهديد علاقة تأثير متبادل وان أي محاولة لتفسيير الامن لابد ان تبدأ بتحديد مصاد التهديدات وادى تصاعد حجم الاخطار الالكترونية من تغير مضمون 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 لتعامل 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 مؤشرات 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 وال الحرب 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:

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

يبين هذا النمط في حالات منها حالات الحروب ذات الطابع السياسي ذات الأبعاد الدينية - الاجتماعية الممتدة، مثل الصراع الصهيوني-العربي، أو 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 إلى أن 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 والمترافق للقدرات التكنولوجية والاعتماد بين الدول و الفواعل غير الدولية على الفضاء الالكتروني بشكل واسع من خلال سيطرة العامل التكنولوجي على القيادة العسكرية للعمليات (عبد الصادق ٢٠١٣).

المبحث الثالث: الإستراتيجية السيبرانية الأمريكية

ان النجاح في الفضاء السيبراني أمر ضروري لتعزيز المصالح الحيوية الأمريكية، وتحدد التكنولوجيات الرقمية عدد العمليات التي تصنف عمل المجتمعات الحديثة والتي تمتد من الاتصال إلى التمويل ومن الكهرباء إلى النقل ومن التجسس إلى 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 الانترنت في تعزيز الحرية والامن والازدهار، وهناك اعتراف بأن أمريكا هي من اخترع الانترنت، وإن الفضاء الالكتروني أصبح اليوم عالم حقيقي أقل من ١ من اصل ١٠ في العالم من ثلاثة مليارات مستخدم للانترنت يعيشون في أمريكا بينما

تقريباً رباعهم يعيش في الصين، الطبيعة العالمية للفضاء السيبراني يعني أن أمريكا لا تستطيع عزل نفسها عن عالم الانترنت ولا يتوقع منها ان تتملي من جانب واحد السياسات والمارسات التي تحكم استخدامه وتطوره في المستقبل، حيث يجب عليها استخدام نفوذها وسلطتها لضمان بقاء الانترنت قوة للخير في العالم، ولكي تكون ناجحة فإنها تحتاج إلى 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 التكنولوجيا السيبرانية يدعم حرية الإنسان ويتبنى اجراءات قوية وفعالة لتعزيز قيم الليبرالية الديمقراطية في الفضاء السيبراني وفي هذا المجال قدم 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 تبني 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 الانترنت.
- ٣-اضفاء الطابع الرسمي وتوسيع وتعزيز تحالف حرية الانترنت.
- ٤-تشجيع زيادة الوصول الى الانترنت من خلال سياسات التسويق.
- ٥-تعزيز دور منظمات بالأخص منظمات المجتمع المدني في الدراسة ودعم حرية الانترنت.
- ٦-توسيع وتكييف ودعم القطاعين: العام والخاص، للمشاركة في المحافل الدولية حيث تم تعيين سياسات الانترنت.

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 الأساسية الوطنية الحرجية، والجريمة والشركات بين الولايات ، فأنشأت وزارة الدفاع الأمريكية البتاغون قوة دفاع شبكات الكمبيوتر المشتركة (JTF - CND) لتتولى مسؤولية الحماية بشقيها (الداعي الإلكتروني والهجومي الإلكتروني)، قبل ان يتم الفصل بينهما، لتهوّل مهمة الهجوم إلى وكالة الأمن القومي، ومهمة الدفاع إلى وكالة الدفاع عن أنظمة المعلومات، وللتين اجتمعتا لاحقاً تحت مظلة القيادة الإلكترونية الأمريكية في عام ٢٠٠٩، التي يقودها مدير وكالة الأمن القومي نظراً لتمتعها بإمكانات كبيرة في مجال تكنولوجيا المعلومات والاتصالات، كما تدل على ذلك التسريبات الأخيرة بخصوص تجسس الوكالة على عدد من الدول (نون بوست ٢٠١٥). في عام ٢٠٠٠ اخذت الولايات المتحدة بتطوير برنامج سمي (كارنيفول) أو (المتهم) وظيفته التجسس على جميع أنواع الاتصالات التي تتم عبر الانترنت لا سيما مع وجود شبكة تجسس عالمية أمريكية أوروبية اسمها ايشلون، أسستها وكالة الأمن القومي الأمريكي مع عدد من المؤسسات الاستخبارية العالمية هدفها التجسس على الاتصالات الرقمية عن طريق الأقمار الصناعية، وهذا البرنامج المتهם هو نظام الكتروني مصمم يسمح لوكالة المباحث الفيدرالية الأمريكية بالتعاون مع شركة المزودة بالانترنت بتطبيق حكم محكمة جمع المعلومات محددة حول رسائل البريد الإلكتروني لمستخدم يستهدفه التحقيق (الزنط ٢٠١٠).

وقد قامت أمريكا منذ عام ٢٠٠٥ بعمل مناورات تعرف بـ (Ceberstrom) (ال العاصفة الإلكترونية) لاختبار قدراتها على مواجهة الاخطار كان آخرها عام ٢٠١٠ مع تزايد عمليات الاختراق لشبكاتها الداعية لما تسببه من خسائر اقتصادية عالمية تقدر ١٠٠ مليون دولار سنوياً، واخذت هذه القضية منحى آخر بعد تزايد الاختراقات لوزارة الدفاع الأمريكي في إطار الحرب الباردة مع الصين لأنها المتهمة الأولى في هذه الاختراقات في ظل التجسسات الإلكترونية التي تتبعها الدول من أجل خرق الأمن القومي للولايات المتحدة الأمريكية.

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 والأسلحة ، ونظم استخراج وصناعة ونقل وتخزين الغاز والنفط، والزراعة وتوزيع الاطعمة والخدمات المصرفية والمالية ، ونظم المواصلات وامدادات المياه، وخدمات طبية وخدمات البريد والنقل وخدمات الطوارئ واخيراً 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 لدعيم الامن القومي الامريكي (خليفة ٢٠١٧، ٢٠١٨، ٢٠١٩-٢٠٢١). وقد اعلنت الولايات المتحدة الامريكية عام ٢٠٠٩ بتشكيل قيادة عسكرية للفضاء الالكتروني لحماية شبكات الجيش الامريكي ليرز اهمية الفضاء الالكتروني بما يتضمنه من عدة قضايا ذات صلة وثيقة بأمنها القومي في ظل الاعتماد الدولي عليه فيما يتعلق بتسخير عمل البنية التحتية الكونية للمعلومات امام المنشآت المدنية والعسكرية من خلال تعرضه للهجوم يستهدفه ك وسيط وحامل للخدمات او برشل عمل انظمتها المعلوماتية فأن التحكم في تنفيذ هكذا هجمات يعد ادارة السيطرة ونفوذ استراتيجية باللغة الأهمية في زمن السلم وال الحرب.

لاحظت وزارة الدفاع الامريكية في تقريرها حول الميزانية المالية ٢٠١٤ ، اعادة تنظيم على مستوى الموارد البشرية والكافاءات لديها لتعزيز قوتها السيبرانية في مواجهة تهديدات منها القومي ضمن فرق متخصصة في مجالات ثلاث هي حماية الشبكات ، وشل قوة العدو السيبرانية، وحماية الدفاع الوطني وانشاء قوة سيرانية لعام ٢٠٠٦ مؤلفة من (٤٠) فرقة موزعة على مهام 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 إليها العمليات الهجومية فضلاً عن وحدات من وكالة الاستخبارات المركزية، في المقابل يتولى الجهاز القيادي السيبراني التابع لقيادة

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

المبحث الرابع: التهديدات الفضائية السيبرانية للأمن 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 الحيوى قليل الجهد والتكلفة من ناحية تنفيذ الهدف و ذات نتيجة هائلة من حيث الاستخدام العملياتي ضد الولايات المتحدة الأمريكية (شلوش ٢٠١٨، ١٩٢).

ولعل منابرز التهديدات التي ممكن ان يواجهها الامن القومي الامريكي في المجال الفضائي السيبراني وله تداعيات على منها 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 لقوة 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 الانترنت) 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 او لأسباب سياسية إذا كان موجهاً دولة معينة (اللجنة الاقتصادية والاجتماعية لغربي آسيا الاسكوا ٢٠١٥، ٧٢)، حيث قررت واشنطن خسائرها نتيجة القرصنة عام ٢٠٠٢، و ٨,٤٥٥ مليون دولار وقدرت وزارة العدل الأمريكية بحدود ١٥٠ الف شخص تأثروا بخسائر تتجاوز ٢١٥ مليون دولار ، وفي عام

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

فخلال عام ٢٠١٤ بعد هجمات حجب الخدمة ٢٠١٣-٢٠١٢ 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 متقدمة للغاية مثل روسيا الاتحادية التي أنشأت قيادتها الإلكترونية 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 ٢٠١٣-٢٠١٢ ضد الولايات المتحدة ومؤسساتها المالية وفي هجوم عبر الانترنت في شباط ٢٠١٤ على شركة كازينو لاس فيغاس ساندز وكوريا الشمالية المسؤولة عن الهجوم الإلكتروني 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 لأن أجهزة الاستخبارات العسكرية الصينية يسعى إلى الحصول على التكنولوجيا الأمريكية العسكرية، بناءً على تقرير شركة لوكيد مارتن انه عام ٢٠١٣ تم إطلاق هجوم سايبيري يستهدف الانموذج الجديد الذي تصننه الشركة من طائرة الشبح المقاتلة ذات المهام المشتركة (بيرسول ٢٠١٤ ، ٢٠١٧).

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

لأفكار الإرهابية أو نشر مواد تدريبية كمصنع متجرات أو لجمع التمويل او لتجنيد اشخاص او للتواصل بين الشبكات الإرهابية وهو ما تخشى منه الولايات المتحدة الأمريكية منذ احداث ١١ سبتمبر (٢٠٠١، عبد الفتاح ٢٠١٧، ٢٥-٢٩)، فدور الانترنت 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 اتخذه فإنه 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" اعلامياً فإنه يعد مفهوماً قدماً يقتصر على رصد حالات التشويش على انظمة الاتصال والرادار واجهزه الانذار بينما يكشف الواقع الحالي في الفضاء الالكتروني السيبراني عن دخول شبكات الاتصال والمعلومات على بنية و المجال 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 الانترنت ولا سيما على الموقع الالكتروني ومواقع التواصل الاجتماعي من

اجل جعل سمعة الولايات المتحدة الأمريكية 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 الأجنبية وهو استهدف لأمن المعلومات الوطنية والسرية للشركات والمؤسسات الأمريكية 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 الأمريكية وخدماتها في العام ٢٠١٥ وما بعده وذلك مع تزايد الخصوم المحتملين واظهارهم قدرات الفضاء المضاد التخريبية، لدى الصين قدرات تشویش على الأقمار الصناعية فأجرت في تموز عام ٢٠١٤ تجربة صواريخ غير مدمرة مضادة للأقمار الصناعية ، فتزايـد المخاوف الدولية من سباق عالمي حاد حول التسلح في الفضاء الخارجي بعد قيام الصين عام ٢٠٠٧، بدمـير القمر الصناعي (فونغ يون اسي) المخصص للأحوال الجوية في الفضاء بصاروخ مضاد للأقمار الصناعية ، وهو ما اعتبرته واشنطن في وقتها نقلة نوعية وتطوراً تكنولوجياً غير مسبوق بالنسبة إلى بكين (شير ٢٠٢١). إن من ابرز الأهداف الالكترونية التي يتم استهدافها في الجغرافيا الأمريكية تتمثل في (الخليفة ٢٠١٧، ١١٤-١٢٠):

١. على المستوى الاتحادي البيت الابيض والكونغرس الأمريكي 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 الأمريكية المختلفة ، وهذه بني حرج للولايات المتحدة الأمريكية لأنها تتضمن النظم والأصول سواء كانت مادية أم افتراضية والتي يؤدي تدميرها أو التلاعب بها في تهديد للأمن القومي الأمريكي او الاقتصاد الأمريكي او الرعاية الصحية أو الأمن العام.

الخاتمة:

ما زال مصطلح الهجوم السiberاني من المفاهيم الحديثة التي لا يوجد اجماع دولي بشأن تعريفه مما ادى إلى صعوبة تكييف وتحديد المسؤولية الدولية عنه، وان ميزة الهجمات السiberانية في انخفاض التكلفة والسهولة في اللجوء لها، إذ لا تتطلب عدداً كبيراً من العسكريين المقاتلين والآلاف من الأسلحة كالنزعات التقليدية بل يكفي لتنفيذها شخص أو مجموعة صغيرة من لديهن الخبرة والمهارة التكنولوجيا السiberانية وثغرات برامج الأنظمة الكومبيوترات لاستخدامها ضد دولة أو دول أخرى، إلا أن هذه الميزة تحول إلى مصدر قلق كبير إذا ما نظرنا إلى آثار هذه الهجمات وتباعتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشأة نووية أو مصادر الطاقة كشبكة الكهرباء والمياه، ونظرًا لطبيعة التهديدات الفضائية السiberانية المتتجدة بصورة مستمرة فهناك عناصر تغيير واستمرار حيوية في الطرق والمعالجات التي تتضمنها الاستراتيجيات الأمريكية للأمن القومي فيما يخص الأمن الفضائي السiberاني وهي استراتيجيات استباقية وقائية لردع الهجمات الفضائية السiberانية شاملاً الأبعاد السياسية والعسكرية والاقتصادية والمدنية إذ إدخالها وحدات السiberانية داخل جيوشها وتعزيز الأطر التشريعية والقانونية لملائحة مصادر التهديد والتعاون مع الدول الأخرى لمكافحة هذه الظاهرة لأن الأمن القومي مهدد بصورة مستمرة من التهديدات السiberانية 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 مضمون الامن القومي للدول واصبحت تبحث عن اعادة تعريفه مع ظهور جهة الفضاء الالكتروني كمهدد لامنها وهو وما دفعها الى ادخاله الى استراتيجيات الامن القومي، والعمل على تطوير قدراتها في المجال الداعي وكذلك الحماية والهجوم والتحديث المستمر لجيوشها للتعامل مع هذا النوع من الحرب الالكترونية الجديدة، ما ترك اثره في العلاقات الدولية ولاسيما مع بروز خطر التهديدات من دول او جهات لا تكترث بالقانون الدولي.

قائمة المصادر:

- اركلا، 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 ٦١٠: ٦٨٧-٤.

- اللجنة الاقتصادية والاجتماعية لغربي آسيا الاسكندرية، 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 ساينرون. ٥ نوفمبر، ٢٠٢١
https://cyberone+com&sa=X&ved=2ahUKEwjOpaCzirT5AhXcW_EDHc2vq0QpBd6BAgBAAE&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. أكتوبر، ٢٠١٧ .
<https://annabaa.org/arabic/informatics/12978>
- خليفة، إيهاب. ٢٠١٧. القوة الالكترونية: كي يمكن ان تدير الدول شؤونها في عصر الانترنت. بيروت: دار العربي للنشر والتوزيع.
- شلوش، نورة. ٢٠١٨. "القرصنة الالكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الإنسانية، المجلد ٨. العدد ٢. ١٩٢-١٨٧: ٢ .
- شوقي، إيهاب. "الحرب السيبرانية حرب المستقبل المفزعه". شبكة الاخبار العربية. ٩. اشباط، ٢٠١٥ .
<https://www.anntv.tv>
- شير، هشام . "التناقض على عسکرة الفضاء" ، صحيفۃ الخلیج السعوڈیة. ٢٤ نیسان، 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. ١١ فبراير، 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: ٢٥٠-٢٩ .
- 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- mohaqqiq 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 terrorm". *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=2ahUEwjOpaCzirT5AhXcW_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 cyberspace: 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%25A
9-
%25D8%25A7%25D9%2584%25D9%2581%25D8%25B6%25D8%25A
7%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>