حـروب الـجيل الـسادس واستراتيجية المواجهة : السيبرانية إنموذجا

الاستلام 7/25 القبول 8/20 النشر 2025/1/25

Sixth generation wars and confrontation strategy: cyber as a model

م .د تقى اياد خليل القيسي
دكتوراه علوم سياسية – جامعة النهرين – قسم الاستراتيجية
مكان العمل المجامعة العراقية – كلية الادارة والاقتصاد– قسم العلوم المالية والمصرفية
Tuka.a.khalil@aliraqia.edu.iq
رقم التلفون 07905673622

الملخص

شهد العالم اهتمام كبير بالحروب السيبرانية في السنوات الأخيرة ، ويأتي هذا الاهتمام نتيجة التطور التكنلوجي في عملية الاتصال وتبادل المعلومات، مما أدى إلى زيادة الاعتماد على بنُية تحتيه رقمية والإنترنت في العديد من جوانب الحياة .وقد تناول البحث الحرب السيبرانية ومفهومها وخصائصها وتطورها وامتدادها إلى مجالات تتجاوز الجوانب العسكرية، حيث يمكن أن تشمل استهداف البنى التَحتيه (المياه ، الكهرباء، الاتصالات) وتتجه الحروب السيبرانية أحيانا نحو الجوانب المجتمعية والسياسية، بهدف زعزعة استقرار المجتمع من الداخل، وتبرز اهميه البحث نتيجة التقدم الحاصل في الفضاء السيبراني والارتباط العالمي بالفضاء الإلكتروني، حيث تتعارض القيم والمصالح بين الأطراف. ومن خلال التعرف على الحروب السيبرانية وخصائصها وتأثيرها على العلاقات الدولية، يمكننا تحديد مدى انعكاسها على الاستراتيجيات الدولية المتبعة في البيئة الدولية وكيف تدافع هذه الدول عن هذه الهجمات وتردعها. وخلصت الدراسة بالتركيز على مدى تاثير الحروب السيبرانية على العلاقات الدولية في البعد الاستراتيجي الهجومي الدفاعي ، فالسيطرة على الفضاء السيبراني لا تحقق النصر بمفردها، ولكن في نفس الوقت لا يمكنك الفوز بدونها.

الَكلمات المفَتاحية:الحروب السيبرانية ، الهجمات السيبرانية، الاستراتيجية

Abstract

ln recent years, the world has witnessed interest in cyber war. This inters comes from the rapid technologic progress in the field of communications and Information exchange, which led to an more reliance about digital structures in various aspects of life. The research addressed the development of the characteristics of the concept cyber warfare and its extension to areas military aspect, as it contain target structures such as electricit, water and connection . Cyber wars tend towards political aspects that the aim to destabilize society from within. The importance of the research stems from the interest in space and global communication in space, where values and interests conflict between the parties, and by defining cyber wars and their objective characteristics and their impact on international relations, we can determine the extent of their reflection on international strategies followed in the international environment and how these countries defend and deter these attacks The study concluded that cyber wars have a significant impact on international relations with offensive and defensive strategic dimensions Control of cyberspace does not achieve victory alone but at the same time you cannot win without it

Keywords: cyber warfare, cyber attacks, strategy

المقدمة

لكل ظاهرة جذور تغزو أصلها وتطورها، ومنذ ظهور الإنترنت كشبكة عالمية تغيرت المفاهيم وطبيعة العلاقات الدولية وأصبح الفضاء السيبرانيي انعكاسا للتفاعلات بين الشعوب والدول ، فبالاضافة الى الدور الايجابي للتطور الفني المعلوماتي الذي سببته ثورة التكنولوجيا، هناك دور سلبي تمثل في تحول الدول للرقمية وظهورسياقات جديدة في الصراعات والحروب في كافة اتجاهات الحياة إلى درجة بروز الحرب السيبرانيه المدمرة التي توصف بالحرب اللاتلمسية عبر الشبكات باستعمال اسلحة رقمية، فالعالم الافتراضي هو الحيز الذي تحدث فيه الحروب، وبدأت الدول تتخذها حجة للتدخل الدولي وادارة النظام الدولي والسيطرة عليه وانتقلت من المواجهات

التقليدية إلى أشكال غير تقليدية تضم عناصر تقنية متقدمة تتسم بالتعقيد الشديد وتستند على الذكاء الاصطناعي والهجمات السيبرانية وإضعاف منشئات وانظمة الدول المستهدفة وتعطيل أنظمة القيادة والسيطرة.

اهمية الدراسة

تكمن اهميه البحث في توضيح المخاطر الناتجة عن التطور التكنولوجي للحرب السيبرانية التي يعيشها العالم اذ تجاوزت التحديات الداخلية والخارجية التي تؤثر على العالم الحقيقي، وارتبط العالم بالفضاء السيبراني الذي أصبح ساحة جديدة للتنافس والصراع، هذا الفضاء الذي تتضارب فيه القيم والمصالح بين الفاعلين فيه، الأمر الذي لفت انتباه الساسة وصناع القرار والأكاديميين بغرض توخي الحذر واعتماد استراتيجيات لمواجهته

اهداف الدراسة

استند البحث في التعرف على مفهوم الحرب السيبرانية واهم خصائصها وانماطها ووسائلها، وكذلك معرفة اثر الحرب السيبرانية علَى البيِئة الدولية والاستراتيجيات الفاعلة المتبعة للحد منها.

اشكالية الدراسة

مشكلة البحث تكمن في وجود تحديات استراتيجية غير مرئية أصبحت تشكل تهديدا للأمن العالمي ومجالها هو الفضاء الإلكتروني وعليه يمكن صياغتها بـ (**الى اي مدى تؤثر الحرب السيبرانية على استراتيجية المواجهة الدولية خاصة وأن الفضاء الإلكتروني يعد أحد عناصر القوة البارزة والمؤثرة في الدول؟)**

ويتفرع من رحم هذه المشكلة مجموعة من الأسئلة:-

1- ما هي الحروب السيبرانية وما هي خصائصها؟
2- ما هي مضامين الحروب السيبرانية انماطها وسائلها ؟
3- ما هي أهم استراتيجيات الفاعلة المواجهة المتبعة للحد من مخاطر هذه الحروب؟

فرضية الدراسة

يركز البحث على فرضية مفادها أن الاستراتيجية العالمية تواجه العديد من التهديدات والحروب، وأخطرها تلك التي تحدث في الفضاء الالكتروني، والتي لا يمكن المساس بها بشكل مباشر ولا يمكن مواجهتها إلا باستراتيجية سيبرانية هجومية او دفاعية متقدمة .

منهجية الدراسة

لاشك في أن تحديد المنهج هو من اولى متطلبات البحث، كونه الأسلوب او الالية التي يتم بموجبها معالجة المشكلة ، اذ اعتمد البحث على (المَنهج الوَصفي) في وصف وتحديد الهجمات

والحروب السيبرانية على الدول وما هي ابرز التهديدات والفرص التي من شانها تحد من خطرها وكذلك المنهج الوصفي لوصف الظاهرة وتوضيحها.

حدود الدراسة

تحدد على النحو الاتي :

1. **موضوعية** : الحروب والصراعات السيبرنية .
2. **زمانية** :ما بعد 2010 وانتشار استخدام الفضاء السيبراني في الحروب والصراعات الدولية.
3. **مكانية** : اتسعت لتشمل الساحة الدولية الواقعية والسيبرانية .

هيكلية الدراسة

تتوزع الهيكلية بالإضافة إلى المقدمة على ثلاثة مطالب وخاتمة، يتضمن المطلب الاول مفهوم الحرب السيبرانية وخصائصها ، اما المطلب الثاني تناول العناصر الفاعلة في الحرب السيبرانية وأنماطها بالإضافة إلى المفاهيم التي تقترب من مفهوم الحرب السيبرانية، ويسعى المطلب الثالث الى توضيح الاستراتيجية الدفاعية الهجومية للحرب السيبرانية، واختتم البحث بأهم الاستنتاجات و التوصيات .

المطلب الاول: الحرب السيبرانية (المفهوم – الخصائص)

لقد أصبح عالمنا عالم المعلومات فمن يملك المعلومات، يملك القوة ويسعى إلى حمايتها، وأصبحت الحروب السيبرانية والفضاء الإلكتروني سمة من سمات الاستراتيجيات والسياسات في كل أنحاء العالم.

أولاً : مفهوم الحرب السيبرانية(لغة – اصطلاحا)

الحرب هي ظاهرة إنسانية موغلة في القدم ارتبطت بالوجود الإنساني على الارض، وهي ظاهرة متغيرة ومتطورة من ناحية الميدان الخطط والادوات والاثار بفعل التطور الإنساني فالحرب(*)، عملية صدام وحشي يقاتل فيها البشر، أو يمكن ان توصف بأنها عملية قتل جماعي[1]

(*) هناك تداخل لعدة اجيال واستراتيجيات في الحروب الحالية سواء كانت حروب معنية بأفشال الدولة وتدمير قوتها ومؤسساتها فحروب الجيل الخامس تعنى بالتعامل مع كيانات صغيرة متعددة وتشكيلات (عصابات وتنظيمات) إرهابية اذ تستخدم الشعوب كلاعب اساسي وليس عن طريق الجيوش مع تفعيل المجال السايبري في كلاهما وحتى في حروب **الجيل السادس** التي تعنى بكل ما يتم التحكم والسيطرة عليه ، أي ادارة الحرب عن بعد الا ان حروب الجيل السادس لا تستخدم الاسلحة والجنود وانما تهدف الى خلق تناقضات بين الدولة والمجتمع باستغلال وسائل نشر المعلومات الزائفة التي تقوم على استراتيجية احتلال

اما السيبرانية في **اللغة** هي مصطلح اخذ من اليونانية (kybernetes) ، وتعني القيادة والتحكم عن بعد[2] وورد اللفظ في قاموس المورد حيث عرفها بأنها(علم الضَبط– cyberrnetics) اي ضبط الاشياء عن بعد والسيطرة عليها [3]، وانتشر مصطلح الحرب السيبرانية بسبب الجرائم السيبرانية والهجمات والخطيرة التي اعتمدت على تقنيات متقدمة كالذكاء الاصطناعي واجهزة مراقبة على الشبكات السلكية واللاسلكية وبرمجيات لفك واختراق أنظمة الشبكات والحاسبات وتستخدمها الدول لاغراض استراتيجية وحربية[4] ويعرفها مجلس الامن الدولي" استعمال الوسائل الرقمية او اجهزة الحاسوب من قبل الحكومة او بمعرفة او موافقة من تلك الحكومة ضد دولة اخرى او ملكية خاصة داخل الدول الاخرى، والوصول المتعمد او اعتراض الاجهزة التي يمكن استخدامها في تخريب النشاطات المحلية ".

وهي الحروب التي يتم ادارتها في مجال الفضاء الالكتروني وتكون الفواعل الرئيسية فيهما هي الدول والجماعات والمنظمات والافراد ويتم فيها استخدام الآليات والأسلحة الالكترونية في الهجوم وهذا الهجوم موجه بالاساس الى الشبكة الالكترونية او جهاز الحاسوب الآلي الخاص بالعدو او الانظمة – الالكترونية التي تدير الدولة وما تحتوي عليه من معلومات بهدف عرقلة الخصم[5] وعرفت كذلك بالحروب القائمة بين الدول وتتمثل في شبكات الانترنيت واجهزة الحاسوب [6] ، وهي الاعمال التي تفعلها الدول وتحاول من خلالها اختراق اجهزة الحاسوب والشبكات التابعة لدولة اخرى بهدف تعطيلها او تحقيق أضرار بالغة بها . [7]

العقول أولاً ثم الارض ، عمرو حسن فتوح، الحروب المتقدمة، الحروب التكنلوجية الباردة بين الدول العظمى نموذجاً (القاهرة ، مجلة السياسة الدولية، 2022) ، www.siyassa.org.eg .

(1) منير شفيق،الاستراتيجية والتكتيك في فن علم الحرب،(بيروت، الدار العربية للعلوم ناشرون، ط 1 ، 2008) ،ص 244.

(2) أحمد عبيس نعمه،الهجرات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنهما في ضوء التنظيم الدولي المعاصر، (بابل، مجلة المحقق المحلي العلوم القانونية والسياسية ، العدد (4) ، 2016) ، ص 614 .

(3) منُير البَعلبكي ،قاموس المَورد عربي أنكليزي ، (بيروت ،دار الملايين ، 2004)، ص 244.

(4) علاء عبد الرزاق السالمي، المدخل الى الامن السيبراني ، (بغداد، دار الذاكرة للنشر والتوزيع ، ط1 ، 2021) ، ص123.

(5) فراس شاكر،السيبرانية وتحولات القوة في النظام الدولي، (عمان ،دار امجد للنشر والتوزيع ، 2022) ، ص250 .

(6) علي العلي،الصراع والأمن الجيوسيبراني في السياسة الدوليه دراسة في استراتيجية الاشتباك الرقمي ، (عمان ، دار امجد للنشر والتوزيع ، ط1 ، 2019) ، ص 84 .

(7) فارس محمد العمارات ، الأمن السيبراني المفهوم وتحديدات العصر، (عمان،دار الخليج للنشر والتوزيع، ط 1 ، 2024) ، ص 123.

ثانيا : خصائص الحرب السيبرانية

اصبحت الحرب السيبرانية نموذجا تطمح إليه العديد من الدول نظراً للخصائص العديدة التي تنطوي عليها ومنها مايلي :

1) **حروب اللاتناظرية** : اي لا تحتاج الدولة قدرات ضخمة لتشكيل تهديد خطير، فالتكاليف قليلة نسبيا، اذ ان نشوئها في الفضاء يرتبط بالحاسبات وشيكات الاتصال وان هذا الهجوم يخلق الاضطراب ويعطل الانظمة ويعطل الانظمة والاجهزة اي لا يتطلب شراء الاسلحة والمعدات ، اذ يقتصر على اجهزة الكومبيوتر والمهارات الفنية ولا يحتاج إلى عناصر بشرية. [1]
2) **عدم التواجد بالمكان** لا يحتاج المهاجمون التواجد في المكان الذي يحدث فيه الهجوم او حتى في المكان الذي يظهر فيه ويستطيع المهاجمون اثناء القيام بالهجوم استخدام تكنولوجيا الأتصال مجهول الهوية وتشفير واخفاء الهوية مثل الضرر بنظم المعلومات والمواد الحيوية للاجهزة الهامة مثل تعطيل الانظمة (السياسية والاقتصادية والاجتماعية). [2]
3) **سرعة وسهولة الاتصال** يمكنها ان تصل الى اي مكان في العالم بسرعة خيالية عن طريق سرعة تبادل المعلومة وسرعة تنفيذ الهجمات التي قد لا تتجاوز الدقائق[3] فمن الممكن اطلاق برامج ضارة (فيروسات للكومبيوتر) ، فضلا عن سهولة شن الهجرات السيبرانية لاعتمادها على الحواسيب وتدريب المحترفين التي تكون اثارها سريعة. [4]
4) **تجاوز الحدود الوطنية (إنعدام السيادة)** اذ تؤثر هذه الحروب على عمليات نقل البيانات على اكثر من بلد في نفس الوقت وقد تسبب للجهات المعرضة للهجوم أضرارا مالية ضخمة ولا يوجد حدود واضحة للدول حيث تتداخل الدول في نفس الشبكات سواء كانت دولة صغيرة ام كبيرة .

---

(1) فارس محمد العمارات ، مصدر سبق ذكره ، ص124.

(2)عادل عبد الجواد، دور مركز المعلومات في التعامل مع الازمات (الرياض، مجلة الامن والحياة ، العدد 358 ، 2016) ، ص 70 .

(3) أيهاب خليفة ، الحرب السيبرانية:مواجهة العقيدة العسكرية استعدادا للمعركة القادمة ، (القاهرة ، مجلة السياسة الدولية ، العدد 11 ، المجلد 53 ، 2018) ، ص 64 .

(4) فرد كابلان، ترجمة لؤي عبد المجيد، المنطقة المعتمة : التاريخ السري للحروب السيبرانية ، (الكويت، المجلس الوطني للثقافة والفنون ، 2019) ، ص 200

5) **اخلاء المسؤولية** تستخدم الأسلحة السيبرانية للهجوم على عكس الاسلحة التقليدية تستخدم للهجوم والدفاع فالاسلحة السيبرانية هي غير مرئية وغير ملموسة[1] . اذ تتميز يفعل الردع كونها لا تترك اثر او دليل على حصولها ، وامكانية التلاعب والتمويه العالية فيما يتعلق بمصدر ومكان توجيه وشن الهجوم الالكتروني. [2]

6) **غامضة وغير محدودة** اذ تتميز الحروب السيبرانية عن الحروب التقليدية في ان الاخيرة تنطوي على تجنيد جيوش نظامية مع وجود ميدان محدد للقتال، اما الحروب السيبرانية فهي غير محددة المجال ميدانها الفضاء ،يتم تنفيذ اهدافها بواسطة الشَبكة الَفضائية .

المطلب الثاني: الحرب السيبرانية (الفواعل – الوسائل – الانماط)

أولاً : فواعل الحرب السيبرانية

امتازت الحرب السيبرانية باعتمادها على العديد من الفواعل سواء كانوا دول ما دونها وهناك ثلاث فواعل في الحرب السيبرانية وهي :-

1) **الدول:** التي لديها قدرة كبيرة على تنفيذ الهجمات والحروب السيبرانية فالدولة هي فاعل محوري في العالم الافتراضي نظراً لمكانتها التي تتحدد بالتفوق التكنلوجي. [3]

2) **الفواعل غير الدول:** ويستخدمون هؤلاء القوة الإلكترونيه للهجوم لان الَحروب السيبرانية تتطلب مساعدة من قبل اجهزة استخبارات متقدمة للدخول والتسلل الى المواقع الالكترونية لاستهداف انظمة الدفاع وتتمثل هذه الفواعل بما يأتي :-

أ) **شركات المتعددة الجنسيات: اذ** تمتاز بالتوجه نحو البعد الاقتصادي الذي يعد المفتاح الأول للعولمة الظاهرة في العالم، وتحتوي بعض الشركات الكبرى التكنلوجية والقدرة التي تتخطى قوة العديد من الدول ، اذ لا ينقصها سوى مشروعية استخدام القوة التي لا زالت الى هذه اللحظة حكرا للدول : (مثل خوادم شركات جوجل ، ومايكروسوفت).

ب) **المنظمات الإجرامية:** وهي المنظمات الاجرامية عابرة للحدود الوطنية يقوم بها مجموعة صغيرة من المتسللين ذوي الخبرة في تقنيات الحاسوب وقادرون على تحقيق تأثيرات سيبرانية ،وتندمج هذه المنظمات مع مصالح الدول المضيفة لها مثل استهداف القراصنة الشركات الامريكية التي تنتج تكنلوجيا تعنى بأولويات الصين العسكرية، وكذلك تسلل

---

(1) محمد كاظم المعيني، أيكلوجيا الارتقاء الصين وتجليات المستقبل دراسة في الامكانيات والتحديات (بيروت، دار السنهوري، 2018) ، ص 312.

(2) علي عبد الرحيم العبودي، الحروب السيبرانيه وتداعياتها على الامن والسلم الدوليين،(بغداد، المجلة الأكاديمية العلمية ، المجلد 57 ، 2019) ، ص96 .

(3) نوران شفيق،اثر التهديدات الالكترونيه على العلاقات الدولية:دراسة في أبعاد الأمن الإلكتروني، (القاهرة، المكتب العربي للمعارف ، 2019) ، ص 40 .

الاجهزة والحاسبات البنكية ، والقيام بنقل الاموال لخدمة تجارة الاسلحة والبشر، اذ تكلف هذه الجرائم مليارات الدولارات كل عام .

ج) **الجماعات الارهابية** : وهي من اهم الفواعل الغير دولية وذلك لانها تستغل الفضاء السيبراني لجمع البيانات على الاهداف وتجنيد المتطوعين والاعلان ، على الرغم أنها لم تصل الى مرحلة تنفيذ هجوم الكتروني _ سيبراني على البنى التحتية للدول، ولكن تحدث اضرار اقتصادية واضطرابات جيوسياسية ذات تاثير معنوي – مادي واسع . [1]

3) **الافراد** : وهم احد الفواعل المؤثرة في العلاقات الدولية خصوصاً من لديهم مهارات عالية اذ ساعدتهم التطورات التكنلوجية لتكوين شركات عالمية بعيدة عن سيطرة الدول ، وذلك بحكم الفضاء والتقدم التكنلوجي. [2]

ثانيا: وسائل تحقيق اهداف الحرب السيبرانية

من أجل تحقيق اهداف الحروب السبيرانية لابد من استخدام العديد من الوسائل.

1) **الحرمان:** قطع خدمة الموزع عن طريق جعل مورد الحاسوب غير متوفر للمستخدم من خلال برمجيات ترسل لأجهزة الحاسوب او الاجهزة الاخرى الهدف منها هو تعطيل مؤقت للخدمة، وتقوم به بعض الطائرات المتخصصة.

2) **التسلل والاختراق:** وتشمل اختراق الحاسبات والشبكات عن طريق البرامج الضارة بأساليب متعددة منها (الفيروسات) وشل فعاليات انظمة الحاسوب للعدو وارساله الى خوادم اخرى فضلا عن سرقة المعلومات الحساسة في المواقع الامنية وتكون اثارها مدمرة لانها تهدد المصالح القومية للدولة المستهدفة.

3) **العمليات الفسلجية:** وتنفذ هذه بواسطة الوسائل الاعلامية المطبوعة والمرئية والمسموعة او توزيع المنشورات والتي تعمل على زعزعة الثقة لدى الخصم وبث الفرقة بين صفوفه. [3]

4) **تشويه الصفحات والمواقع:** عن طريق حقن المواقع من اجل تشويه الصفحات او اتلافها اذ يستخدم هذا الشكل الفيروسات حيال المواقع لبضع ساعات او ايام .

---

(1) رغدة البهي،التجربة المصرية في مكافحة الأرهاب السيبراني: رؤية تحليلية ، (القاهرة،مركز الأهرام للدراسات السياسية والاستراتيجية، 2013) acpss.ahram.org.eg .

(2) سالم عبود محمد ، نظم المعلومات الاستراتيجية الامنية (بغداد، دار الدكتور للعلوم ، ط1 ، 2022) ، ص239.

(3) نصر سفاح ، الحروب الالكترونية واثرها على الامن القومي، (بغداد ، مركز النهرين للدراسات الاستراتيجية ، 2023) https://www.alnahrain.iq .

ثالثاً : انماط الحرب السيبرانية

يمكن وضع العديد من الانماط للحروب من ناحية تأثيرها وشدتها ابرزها :

1) **الحرب السيبرانية المنخفضة الشدة (الباردة)** : وتكون ساحة الحرب فيها هي الفضاء الالكتروني ، وتتميز هذه الحرب بالاستمرارية بين الفاعلين المتنازعين على كافة الاصعدة (الاقتصاديه،الثقافيه،الاجتماعيه) ووسيلة هذه الحرب تتمثل في التأثير النفسي والفكري والاختراقات المتعددة عن طريق سرقة المعلومات والتجسس مثل الحروب بين الكوريا الشمالية وكوريا الجنوبية .
2) **الحرب السيبرانية المتوسطة الشدة** : تكون ساحة الحروب في هذا النمط التوازي بين القضاء الالكتروني والحروب التقليدية ومثل ذلك الحرب بين روسيا وجورجيا.
3) **الحرب السيبرانية المرتفعة الشدة (الساخنة)** :ويوضح هذا النمط عن ظهور حرب في الفضاء الالكتروني غير متوازنة مع الاعمال التقليدية العسكرية ولم يشهد العالم هذا النوع من الحروب ومن الممكن حدوثها مستقبلا مع التطور التكنلوجي واعتماد الدول على مجموع فاعلين من غير الدول(الفضاء الالكتروني) [1]حيث يتم استعمال اسلحه الكترونيه اتجاه مرافق العدو والروبوتات آلالية في الحروب والطائرات بدون طيار وكذلك ضرب حواسيب العدو والهدف من وراء ذلك تحقيق السيطرة والتغلب الالكترونية بطرق اسرع. [2]

رابعا:المفاهيم المُقاربـة للحرب السيبرانية

1- **الابتزاز السيبراني** : هو كل سلوك غير قانوني يتم باستعمال التقنيات والاجهزة الإلكترونية ، ينتج عنها حصول المجرم على فوائد مادية ومعنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدفها سرقة او اتلاف للمعلومات غالبا ما تكون البيانات شخصية .
2- **الجريمة السيبرانية** : وهي نشاط اجرامي يتم بتوظيف الشبكات الإلكترونية للحصول على المعلومات او تدميرها او ايذاء الافراد او المؤسسات او الاضرار بالنظام السيبراني وهذا يجعله من الصعب التحقيق فيه ومحاسبة المسببين له .وهو كل فعل او امتناع عن فعل باستعمال نظام معلوماتي معين للأضرار بمصلحة او حق يحميه القانون من خلال جزاء

---

(1) سماح عبد الصبور، الصراع السيبراني طبيعة المفهوم وملامح الفاعلين ، (القاهرة ، مجلة السياسة الدولية ، مجلد 52 ، 2017) ، ص 6 .

(2) فارس محمد العمارات، مصدر سبق ذكره، ص191.

3- **الامن السيبراني** : هو وسيلة لحفظ البرامج وأجهزة الكومبيوتر والشبكات، وهو سلسلة الإجراءات المتخذة لمواجهة الهجمات والاختراقات السيبرانية وما ينتج عنها من أخطار. ظهر مع بداية الحرب الباردة وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وصار وسيلة أمنية وحربية دولية أساسية.

4- **الارهاب السيبراني** : هي التهديدات على أنظمة المعلومات بدوافع سياسية او دينية [1]، بعد ان اصبح الانترنيت اكثر الاسلحة تدميرا وفتكا نتيجة تدخل وتغلغل الِكتروني الذي يكون جزء من عمل الارهابين السيبرانيين والاستخبارات الاجنبية [2]

5- **الحرب الإلكترونية** :هي استعمال الطيف الكُهرومغناطيسي لتشويش وتعطيل الاتصالات وأنظمة التحكم والتوجيه الخاصة بالعدو، ويعد هذا النوع من الحروب أداة مهمة في العملية العسكرية الحديثة، حيث يستخدم لتعطيل اتصالات العدو، وإرباك أنظمة الرادار، وحتى حماية القوات العسكرية من الهجمات . وتختلف الحرب السيبرانية في جوهرها عن الحرب الإلكترونية. إذ تركز على الهجمات التي تستهدف الشبكات الحاسوبية والأنظمة الرقمية . هذه الهجمات يمكن أن تتراوح بين سرقة البيانات الحساسة وتعطيل البُنية الرقمية مثل محطة الطاقة او شبكة الاتصال.

6- **الفضاء السيبِراني**: وهو البيئة التفاعلية الالكترونية يحتوي عناصر مادية وغير مادية مكون من العديد من الاجهزة الرقمية والانظمة والبرمجيات ، الشبكة المتصلة في البنى الاساسية لتقنية المعلومات، والتي تشمل شبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها.

المطلب الثالث : الحروب السيبرانية واستراتيجية المواجهة

لقد ادى التقدم التكنلوجي الى ارتفاع التهديدات التي تواجه الدول فباتت التحديات والمخاطر عابرة للحدود مخترقة السيادة الوطنية بطريق لم يشهدها العالم من قبل ، فقصدت الدول إلى وضع استراتيجية لمواجهة هذه الهجمات او الحد منها فالعالم يتداخل بشبكة رقمية معقدة بديلة عن البيئة التقليدية اي مجال حيوي جديد، واصبح القضاء السيبراني ميدان للحرب اضافة الى الارض والبحر والجو ، وهذه القوة السيبرانية تعطي القوى النشطة قدرة عالية على المناورة الاستراتيجية كونها تحمل التهرب وعدم الانضباط.

وهناك نوعين من الاستراتيجيات لمواجهة الحروب السيبرانية :-

---

(1) منى الاشقر جبور، السيبرانية هاجس العصر،(القاهرة ، المركز العربي للبحوث القانونية والقضائية ، ط1 ،2018) ، ص85.

(2) فاطمة الزهراء عبد الفتاح، تطور توظيف جماعات العنف " الارهاب السيبراني " (القاهرة ،مجلة السياسة الدولية ، العدد 208، 2017) ص27.

1- **الحرب السيبرانية الدفاعية** :هي استراتيجية تستخدمها الدول والمؤسسات في الحفاظ على الانظمه والبيانات من أي تهديد سيبراني، وتشمل مجموعة من الاساليب والطرق التي تسعى لتعزيز الأمن السيبراني والتصدي للتهديدات الإلكترونية وتتمثل في استخدام أدوات أمان سيبراني (برامج أمان سيبراني مثل أنظمة اكتشاف التهديدات وجدران الحماية وبرمجيات الوقايه الفيروسات)، **كالتحديث والتصحيح** (ضمان تحديث البرامج وأنظمة التشغيل بانتظام لسد الثغرات الأمنية المعروفة) ، **وتدريب الموظفين**(تدريب الموظفين على أمور الأمان السيبراني وكيفية التعامل مع التهديدات المحتملة) **التشفير والحماية البيانية** (استخدام تقنيات التشفير للحفاظ على النظم والبيانات الحساسة)

2- **الحرب السيبرانية الهجومية** : وتشمل وضع الخطط واتخاذ الاجراءات للسيطرة او تزييف المعلومات المسجلة على انظمة الحاسوب والاتصالات المستخدمة في نظم الانترنيت في كافة الميادين العسكرية والمدنيه مثل الهجوم الالكتروني (التشويش والخداع الالكتروني والصواريخ) العمليات الفسلجية (وتنفذ هذه العمليات بواسطة وسائل الاعلام المرئية والمسموعة والمقروءة او توزيع منشورات تودي الى زعزعة الثقة لدى الخصم) الهجمات على شبكات الحاسوب (اختراق الشبكات والحاسبات المركزية لحقن الحاسبات ببيانات ومعلومات مزيفة ونشر الفايروسات) .

أولاً : استراتيجية المواجهة للولايات المتحدة الامريكية (بين الدفاع والهجوم)

تعزز الولايات المتحدة فاعليتها الالكترونية نتيجة ارتفاع التهديدات العسكرية لأمنها الاستراتيجي ورفاهية المواطن فوضعت استراتيجية تهدف الى توجيه السياسة على نظام أكثر صرامه لممارسة الأمن السيبراني واعتمادها على التكنولوجيا السيبرانيه في البنى الاساسية وانظمه مصادر الطاقة لِتجنب (حرب افتراضية) مدمرة لان الحرب السيبرانية مدمرة كأسلحة الدمار الشامل. [1] وتحولت سريعاً معالم التهديدات السيبرانية من التنافس إلى الصراع وبدأت تنمو بدرجة سريعة وكبيرة وصعبة لما تتضمنه من خاصية اخفاء المهاجم وصعوبة اثبات الهوية المنفذ وجهة التنفيذ فمن غير الممكن تحديد جهة التنفيذ هل هي دولة او مجموعة افراد.[2]وفي ظل التنافس والحروب بين الصين والولايات المتحدة الأمريكية وروسيا في المجال السيبراني حرصت واشنطن

(1) وزارة الخارجية الامريكية : httpss://www.stste.gov/release.ofunite

(2) محمد منُذر ،وسرى غضبان،تكنولوجيا الحروب السيبرانية وإستراتيجيات المواجهة الدوليه(بغداد ، دار ومكتبة عدنان ، ط1 ، 2021) ، ص181.

على اعلان استراتيجية دولية للفضاء السيبراني والرقمي عام 2024 في سان فرانسيسكو والتي ترمي الى العديد من الأهداف ، ومن اهم مبادئ هذه الاستراتيجية :

1) **التضامن الرقمي:** الذي يقوم على تعزيز الدبلوماسية الرقمية من خلال التعاون في مجال الفضاء الرقمي وتشكيل تحالفات دولية.
2) **التفوق التقني:** اذ تسعى الولايات المتحدة الامريكية ان تبقى القائدة لدفة القيادة الاستراتيجية التكنلوجية العالمية اي في صدارة المشهد التكنلوجي .
3) **تنظيم عمل الفضاء الالكتروني :** وذلك عن طريق احترام قواعد القانون الدولي وخصوصية الافراد ، ودمج المساعي لتحقيق أهداف التنمية المستدامة وبلورة (سياسة شاملة) ، تطوع مختلف الوسائل الدبلوماسية لمواجهة الازمات ومعاقبة المتسللين الذين يرغبون في الاضرار بأمن الدول وعلى غرار ذلك نجد ان الولايات المتحدة الأمريكية قد بادرت بنشر قدرات دفاعية بشكل استباقي عن الولايات الحكومية والمدينة وانشاء إطار للشراكة في القطاع العام والخاص خصوصاً واننا في عصر الحروب الذكية والتي تعتمد بالدرجة الاولى على الاسلحة الالكترونية لمواجهة العدو دون قدرته تحديد مصدر الهجوم أو حتى اكتشافه . [1]

فضلا عن الحد من سهولة الاختراق وسرعة التعامل مع الاختراقات السيبرانية عن طريق سرعة تبادل المعلومات من دون التلاعب بها والقدرة على اختراق البيانات مع سرعة الحركة داخل الفضاء السيبراني ومعرفة ما اذا كانت هذه التحركات دفاعيه او هجوميه[2]عن طريق معرفة نية الخصم وهدفه وقدرته ،وسعت الولايات المتحدة الأمريكية لحماية العديد من العناصر منها الاتصالات ومحطات الكهرباء والماء والبنى التحتية ونظم المواصلات عن طريق عدة استراتيجيات قد يكون دفاعية أو هجومية :-

1) استراتيجية الدفاع السيبراني للولايات المتحدة الامريكية:

تتسم بتعزيز امن الشبكات الوطنية والبنى الحيوية لمواجهة التهديدات السيبرانيه الحديثة وهنا بدأت الولايات المتحدة الأمريكية في عام 2008 مراقبة ومتابعة بيانات المواطنين من غير الولايات المتحدة الامريكية وذلك بتحليل وتجميع ومراقبة المواقع ومحاولة تعطيل انشطة المتسللين عن طريق تحميل برامج صانعي البرمجيات وتعد وكالة الاستخبارات المركزية ووكالة الامن القومي احد اهم الاجهزة المتخصصة في الأمور اللوجستية حيث تستخدم اجهزة متطورة

---

(1) وسام مهيوب، نموذج الولايات المتحدة الامريكية في مجال الامن السيبراني : بين الهجوم وإمكانيات الدفاع ، (الجزائر ، مجلة البيان ، العدد 2 ، 2023) ، ص131.

(2) ايهاب خليفة ، مصدر سيق ذكره، ص 135 – 136.

(طائرات بدون طيار وسفن حربية) للحصول على المعلومات[1] . ولا يقصر على ذلك بل تطوير وزيادة انتاج الاسلحة والذخائر للتخزين لتحقيق التوازن العالمي فضلاً عن امتلاكها شبكة في القواعد العسكرية العالمية التي سمحت لها تعزيز قدراتها الدفاعية. [2] وتقوم الاستراتيجية على تعزيز السيبرانية الأمريكية على اربع ركائز على النحو الأتي:

1- **تعزيز الأمن القومي الأمريكي** عن طريق تبادل المعلومات عبر الوكالات الفيدراليه لحماية الشبكات،وتأمين الثروات ، وذلك من خلال إعطاء وزارة الأمن الوطني المزيد من الصلاحيات لرقابة جهود الأمن السيبراني المدنية، والتقليل الجرائم السيبرانيه والتعاون مع الدول الأخرى لتعقب منفذيها.

2- **تعزيز الاقتصاد الأمريكي الرقمي** بتشجيع الابتكار والتطور وذلك العمل مع شركات التكنولوجيا لتعزيز اختبارات الأمن السيبراني في المنتجات الجديدة. وبناء قوة عاملة في مجال الأمن السيبراني وتعيين المتخصصين ذوي الكفاءات في المؤسسات والوكالات الأمريكية.

3- **الوقاية من التهديدات السيبرانية** استعمال أدوات القوة الأمريكية لردع أي هجمات سيبرانية، وتعزيز المعايير الدولية في المجال السيبرَانَي.

4- **الدعوة إلى حرية الإنترنت** تزويد حلفاء الولايات المتحدة بقدرات سيبرانيه للتعامل مع أي تهديد سيبراني يستهدف المصالح المشتركة.

واستخدمت امريكا استراتيجات عدة لزيادة عسكرة الفضاء الالكتروني للمحافظة على أمنها القومي ، لان الفضاء الالكتروني تجاوز حدود الدولة ومن الصعب وضع حدود للفضاء على التهديدات والحروب السيبرانية خصوصاً على التهديدات التي تؤثر على الامن القومي . اذ توجد العديد من الاختراقات للمعلومات لان مجال الحرب السيبرانية في حالة تجدد مستمر ، فكلما يتم التوصل والاكتشاف لطرق حماية ومعالجة ظهر تهديد جديد وهذا فرض على الدول ان تكون سريعة ومتجددة في معالجة التهديدات والمشاكل الرقمية للحد من اختراقات وتهديدات الاعداء[3] ووضع خطط للدفاع في وقت الهجوم بأساليب سيبرانية ، وستعمل الولايات المتحدة الامريكية مع

---

(1) علي زياد العلي، الخصخصة الأمريكية للحروب الجيل الخامس من وسائل التدخل والاستخبارات، (مركز دراسات كاتبغون، 2017/7/27) http://katehon.com

(2) توماس ج . ما تكين ترجمة نهى مصطفى ، استراتيجيات الدفاع الامريكي (جريدة عمان ، 2024) .http://www.omandaily.com

(3) محمد مندر و سرى غضبان ، مصدر سبق ذكره ، ص 191 .

مجموعة كبيرة من الشركاء في مختلف انحاء العالم من اجل تطوير الفضاء الرقمي ومعالجة تحديات العابرة للحدود اذ تعمل على وضع معايير عالمية لكيفية استخدام الدول والفاعلين ما دون الدول الفضاء السيبراني[1] ، اذ تعرضت الولايات المتحدة الأمريكية وكوريا الشمالية للعديد من الهجمات منها هجمات الحرمان من الخدمة بشكل واسع في عام 2009 واتسمت بالتعقيد لأنها استهدفت مواقع الحكومة العسكرية والمالية في كلا الدولتين. [2]

وكذلك الهجوم على شركة (eBay) الأمريكية في ايار 2014 الذي ادى الى سرقة 140 مليون حساب مصرفي لعملائها من أسماء وعناوين ومواقع الكترونية[3] ولحقتها هجوم 17 / تموز / 2020 اذ شنت مجموعة (APT29) هجمات الكترونية على مؤسسة تشارك في تطوير لقاح مضاد لكوفيد 19 في كندا والولايات المتحدة الأمريكية والمملكة المتحدة واكد مركز الامن الوطني البريطاني انها لصالح جهاز المخابرات الروسي فتحولت الحرب من شكلها التقليدي الى حروب سيبرانية وأصبحت بالفضاء ساحتها ، والشبكة العنكبوتية (الأنترنيت) اهم المرتكزات بها لمهاجمة الدول الكبرى ، لتنفيذ هجماتها بأقل تكلفة مادية وبشرية. [4]

2) إستراتيجية الهجوم السيبراني للولايات المُتحدة الأمريكية :

تعد جزء أساسي من توجهها الامني لمواجهة التهديدات المتزايدة في الفضاء الرقمي، و تعزيز قدرة الولايات المتحدة الامريكية على مواجهة الخصوم باستخدام العمليات السيبرانية بشكل استباقي لحماية امنها القومي ومصالحها الحيوية وتشمل هذه الاستراتيجية:

1- **الدفاع الامامي** اذ تقوم هذه الإستراتيجية على الإدراك المبكر للاعمال السيبرانية وردها في بداياتهاعن طريق تعطيل البنى المستخدمة من قبل الجهات المهددة وتسمى بسياسة (الانخراط المستمر).

2- **الشراكة** تسعى الولايات المتحدة الامريكية لتوسيع التعاون مع الحلفاء وشركاء مثل(أستراليا ، نيوزيلندا، المملكة المتحدة، كندا) الاعضاء في العديد من العمليات السيبرانية المشتركة .

---

(1) فراس جمال،السيبرانيه وتحولات القوة في النظام الدولي، (عمان ، دَار امجد للنشروالتوزيع ، ط1 ، 2022) ، ص 365.

(2) فراس جمال، نفس المصدر السابق، ص 338.

(3) cyber resilience, the cyber challenge and the role of insurance, December 2014, p.213.

(4) وسام الامير حميدي ، سلام بلا نهاية ، (القاهرة، دار الكتاب للطباعة والنشر، ط 1 ، 2014) ، ص214.

3- **الاستفادة من الصراعات** بنيت الاستراتيجية لاغتنام الفرصة في الحروب الحديثة مثل الحرب الروسية – الاوكرانية اذ برزت التداخل بين الادوات السِيبرانية وأدوات الحرب الَتقليدية.

4- **التركيز على الخصوم** تعتبر الاستراتيجية أن التهديدات السيبرانية القادمة من الصين وروسيا هي الأكثر حدة على وجه الخصوص، اذ تتهم الصين بالاستعداد لاستخدام الهجمات السيبرانية لتعطيل البنية التحتية الأمريكية وإثارة الرعب المجتمعي في حالات الحروب والصراعات

5- **العمليات السيبرانية** تتضمن تنفيذ حملات هجومية في دول حليفة لتحديد التهديدات السيبرانية والقضاء عليها، مثل العمليات في دول البلطيق وأوروبا الشرقية.

و تستخدم الولايات المتحدة الاسلحة الإلكترونية لمهاجمة الدول فنفذت عام 2010 مع اسرائيل هجوماً الكترونيا مشتركاً استهدف المنشات النووية الإيرانية والحق شبه شكل كامل بالبرنامج النووي الايراني وفي عام 2016 نفذت هجمات الكترونية ضد تنظيم داعش في سوريا وفي هذه المرة أعلنت أول مرة استخدام الحروب السيبرانية. والولايات المتحدة الامريكية تؤكد في استراتيجيتها على ضرورة تجنب التصعيد غير المقصود أثناء تنفيذ العمليات السيبرانية، مع الاستمرار في تعزيز قدرتها على مواجهة الخصوم بفاعلية .

ثانيا-إستراتيجية المواجهة الروسية للحرب السيبرانية (بين الدفاع والهجوم)

ان دراسة الحرب في روسيا تعد امرا جوهري لتعزيز فهمنا لظاهرة الحرب في السيبرانية وكيفية مواجهتها فلا بد من توضيح لاستراتيجية روسيا الهجومية والدفاعية اذ دخل المجال السيبراني مجريات الحرب الروسية –الأوكرانية التي اندلعت في 24 فبراير 2022، على الرغم من تفاوت القوة السيبرانية بين روسيا وأوكرانيا الا ان الأخيرة لقيت دعما غير مسبوق من قبل الغرب لتعزيز قدراتها ، وشهدت الحرب تصاعد أنماط جديدة مثل استخدام الطائرات بدون طيار والعملات المشفرة والأقمار الصناعية الى جانب بروز نمط الحرب السيبرانية "الناعمة" مقابل نمط الحرب "الصلبة" ، وهو الأمر الذي أثر في وتيرة العمليات الميدانية ، وتنامي تطبيقات الحرب النفسية ، ودخول فاعلين من غير الدول في النشاط غير العسكري ، وهو ما يعكس تنامي القوة السيبرانية في هيكل النظام الدولي وفي صعود قوى جديدة تحاول مواجهة الولايات المتحدة كقطب أوحد في النظام الدولي.

1- استراتيجية الهجوم السيبراني لروسيا

تبرز هذه الاستراتيجية ملامحها في الكشف عن أي محاولة اختراق غريبة قد تتعرض لها أنظمة الدولة الحيوية، وتبني استراتيجية للردع والدفاع في حال تعرضت لذلك، وهو الأمر الذي ظهر في الرد السريع لموسكو على محاولات اختراق مجموعات هاكرز أوكرانية لمواقع إلكترونية تابعة لمصالح حيوية في روسيا بعد بدء الحرب مباشرة. وقد برز استخدام موسكو لاستراتيجية الاختراق أو القرصنة الإلكترونية في بداية الحرب على أوكرانيا بعد قيامها بتعطيل الاتصالات وقطع التواصل بين جنود الجيش الأوكراني عبر استهداف الاتصالات، وكذلك اختراق هيئات ووزارات أوكرانية حيوية بهدف الاختراق والحصول على معلومات قد تساعدها في الحرب. وفور إعلان البرلمان الأوروبي موسكو كدولة راعية للإرهاب في اواخر نوفمبر 2022 تعرض البرلمان لهجوم إلكتروني خطير، وبرزت اوكرانيا كواحدة من اكثر الجهات التي استهدفتها روسيا بعملياتها السيبرانية التي شملت اختراق شبكات الاتصال الإلكترونية الحيوية وتوقفها عن الخدمة، ومحاولة التلاعب في الانتخابات الأوكرانية عن طريق عمليات التضليل. والتي ادت الى انطلاق العمليات العسكرية في 24 فبراير/شباط 2022 حتى منتصف شهر نيسان/إبريل 2022، ووقوع أوكرانيا تحت الهجوم السيبراني المتواصل من قبل روسيا إلى تطوير اليات الردع السيبرانية، وقد ساهمت بتقديم بيئة أكثر مرونة للعمل مع الاعتداءات السيبرانية والتخفيف من أضرارها، وقد برزت الحرب بينهما بوصفها مثالا واضحا على توظيف كل من روسيا وأوكرانيا للعمليات السيبرانية في تحقيق أهدافهما الاستراتيجية. وقد تنوعت هذه العمليات بين عمليات هجومية وأخرى دفاعية. كما برز مفهوم الردع الشامل بوصفه واحدا من أهم الاستراتيجيات في التصدي للبرمجيات وعمليات التلاعب والتأثير. ونظرا لان روسيا كانت الطرف الذي بدأ الحرب، فقد كانت أكثر توظيفا للعمليات السيبرانية الهجومية. وقد أشتملت هذه العمليات ضرب البنايات المدنية والعسكرية ، والتواصل الالكتروني للعديد من القطاعات في أوكرانيا، هذا فضلا

عن عمليات التلاعب والتأثير وبث الأخبار الكاذبة، التي حاولت الإتيان على الروح المعنويَّة للأوكرانيين من خلال تصويرهم ضعفاء وينشدون الاستسلام [1]

2- استراتيجية الدفاع السيبراني لروسيا

تعتمد الاستراتيجية الروسية على اسس تاريخه وجغرافية وامنية شاملة تركز على مواجهة التحدي الداخلي والخارجي عن طريق استعمال القوة العسكرية والدبلوماسية(الذكية)، سواء بالدفاع عن وحدة الارض وسيادتها من أي تهديد وكذلك استعمال الردع النووي كوسيلة ردع اساسية ضد أي عدوان محتمل خصوصا من الدول الكبرى والتوازن مع حلف الناتو اذ تعده تهديد رئيسي اذ تعمل على تطوير استراتيجيتها العسكرية لتحقيق التفوق والتوازن والمواجهة مع الحلف، والحفاظ على البنى التحتية وذلك بتطوير القدرات السيبرانية وشن هجمات رقمية سيبرانية ضد أي تهديد، وتعزيز التحالفات مع العديد من الدول مثل الصين ايران الهند لتحقيق تحالف يوازن النفوذ الغربي وكذلك التوسع وبسط النفوذ في افريقا والشرق الاوسط كالوجود العسكري في شبه جزيرة القرم وروسيا، والسعي الى الدفاع الاقليمي وحماية مناطق مهمة استراتيجيا كالقطب الشمالي الذي يشهد تنافس عالمي متزايد واستخدام الحروب السيبرانية الالكترونية لتحقيق اهدافها دون الدخول في مواجهة تقليدية .

الا انها في نفس الوقت واجهت تحديات في تطبيق استراتيجيتها الدفاعية:

1- **العقوبات الاقتصادية/** اثرت العقوبات الغربية على قدرة روسيا على توظيف وتطوير الانظمة العسكرية .

2- **التوتر الداخلي/** تواجه روسيا تحديات داخلية مثل المشكلات الاقتصادية وعدم الاستقرار السياسي في عدة المناطق.

3- **التنافس الجيوسياسي/**الامتداد الغربي في مناطق تعدها روسيا مجال نفوذ تقليدي لها، مثل اوكرانيا وجورجيا.

وان استراتيجية روسيا السيبرانية الدفاعية تعتمد بشكل رئيسي على المزج بين التقنية والتكتيكات المستمدة من عقيدتها في حرب المعلومات التي تنسب الفضاء

(1) محمود جمل ، كيف استخدمت روسيا الهجمات الإلكترونية في حربها مع أوكرانيا؟ ، 2023 : https://alqaheranews.net/new

السيبراني كونه جزء من الفضاء المعلوماتي الواسع حيث تتقاطع التكنولوجيا مع التأثيرات الاجتماعيه. ويمكن ان نحدد الاستراتيجية الدفاعية السيبرانية الروسية في الاتي

1- **حماية البنى التحتية** تعزز روسيا امن أنظمة الاتصالات والشبكات المستخدمة في العديد من القطاعات مثل الطاقة والنقل والدفاع، حيث ترى هذه البنى كجزء من سيادتها الرقمية التي يجب حمايتها من الهجمات.
2- **الردع السيبراني** تمزج روسيا بين الهجوم السيبراني الوقائي والدفاعي بهدف ردع أي محاولة اختراق أو هجوم محتمل، وتطوير القدرة على الهجوم والدفاع مما يمكنها من مواجهة التهديدات السيبرانية .
3- **الحرب المعلوماتية** وفق العقيدة الروسية لا يوجد خط واضح بين السلم والحرب في السيبرانية اذ تعمل روسيا على مراقبة الأنظمة والتدخل في الاعِتداءات المعلوماتيه للتفوق في مواجهة التهديدات السيبرانية .
4- **تطوير القدرات** تعتمد روسيا بشكل كبير على التعلم من الحوادث السابقة لتحسين دفاعاتها، وتمثل الهجمات التي تعرضت لها مصدر لتحليل نقاط الضعف وتقوية الدفاعات .

واتجهت روسيا الى هذه الاستراتيجية الدفاعية نتيجة لجوء أوكرانيا إلى بعض الاستراتيجيات السيبرانية الهجومية اذ قامت اوكرانيا بإنشاء الجيش الاوكرانيا السيبراني وغالبية عملياتها أخذت طابع الردع وتعزيز لقدرات الدفاع الذاتية، وبناء تحالفات بين القطاعات الخاصة والحكومية من جهة، وتحالفات مع حكومات ومنظمات دولية من جهة أخرى، قابل للتطبيق ومنح الأطراف مرونة في التعاطي مع الهجمات السيبرانية. واستعمالها تكتيكات حروب الدعاية والتأثير، حيث وظفت هذه التكتيكات في دعم الحرب من جهة، وبث روح العزيمة والصمود في الأوكرانية من جهة أخرى. وقد كان ذلك واضحا من خلال الدخول الكثيف للرئيس الأوكراني على خط هذه التكتيكات من خلال الفيديوهات التي كان يخرج بها على شعبه بشكل مباشر من شوارع العاصمة كييف عبر تطبيقات منصات التواصل الاجتماعي، مثل تيك توك. وكذلك عدد من

المتطوعين السيبرانيين الذي أبدوا استعدادهم للإسهام في تنفيذ هجماتٍ سيبرانية ضد روسيا نيابة عن الجانب الأوكراني. [1]

ومن خلال تحليل الإستراتيجية السيبرانيه للولايات المتحده الامريكية وروسيا، تبين أن كلا الدولتين قد طورتا سياسات واستراتيجيات معقدة لتواجه اي تهديد سيبراني، اذ ركزت الولايات المتحدة الامريكية على تعزيز الدفاعات السيبرانية وتطوير تقنيات متقدمة لرصد ومنع الهجمات، بينما ركزت روسيا على دعم القدرات الهجومية المتقدمة واستخدام الفضاء السيبراني كوسيلة لتحقيق أهدافها الجيوسياسية ، اي استعمال استراتيجية شاملة توظف القوة الصلبة والناعمة لتقوية أمنها القومي وضمان مكانتها في الهيمنة العالميه. ويظهر أن التهديدات السيبرانية لها تأثيرات بعيدة المدى على العلاقات الدولية. وتتطلب مواجهة هذه التحديات تعاونًا دوليًا فعالا وإطارا قانونيا لضمان أمن واستقرار الفضاء السيبراني. ومن الضروري أن يعمل المجتمع الدولي للتصدي لهذه التهديدات، وتعزيز الثقة المتبادلة بين الدول، والتاكيد على التفاهم والحوار المتبادل لتجنب النزاعات.

الخاتمة

إن حروب اليوم هي حروب تكنولوجية تسعى من خلالها الدول إلى الهيمنة والسيطرة، فسباق التسلح في الماضي الذي ميز العلاقات الدولية أصبح اليوم سباقاً نحو الرقمية، فيستخدم المهاجم أسلحة معلوماتية من أجل الحفاظ على المعلومات وحمايتها، فالفضاء الإلكتروني الذي تسيطر عليه شبكة الإنترنت والإجراءات الرقمية خلق مفهوماً جديداً للحرب تدخل فيه الاسلحة الالكترونية والنظم المعلوماتية، وهي الحرب السيبرانية كنظام جديد بين الدول التي اتبعت عدة استراتيجيات لمواجهتها، لأن الحرب السيبرانية هي اصعب واشد الحروب فتكاً في العصر الحديث على المستوى السياسي واقتصادي واجتماعي ، وهي نوع جديد من الاحتلال والسيطرة

الاستنتاجات

1- تزايد المخاطر الالكترونية السيبرانية وتعرض المرافق الحيوية للدول للهجمات مما يشل حركتها.

(1) نبيل عودة ، العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها وأنماطها، الشرق للأبحاث الاستراتيجية ، 2022 ، https://research.sharqforum.org

2- انتقلت الحروب السيبرانية من الرؤى المستقبلية إلى الواقع والتطبيق، وأصبح الفضاء الرقمي ساحة صراع بين الدول، وهو في اتجاه تصاعدي مستمر من حيث تطور أساليبه وتهديداته.

3- توحيد الجهود والاستراتيجيات الدولية لإبرام اتفاقيات وشراكات دولية تهدف إلى مواجهة واحتواء وتخفيف المخاطر والحروب السيبرانية.

4- لقد تآكلت سيادة الدول في الفضاء الإلكتروني بشكل كبير بسبب قدرة الأفراد على ممارسة السلطة في الفضاء بشكل غير مسبوق، وظهرت مجموعات وأفراد يمتلكون قدرة معلوماتية تساعدهم في الضغط على الدول.

التوصيات

1- استغلال التقدم التكنولوجي في اطار الثورة المعلوماتية بما يخدم مصلحة الدول بشكل عام والإنسانية بشكل خاص بدلا من خسارتها في الحروب السيبرانية.

2- تطوير استراتيجيات وسياسات قابلة للتطبيق في الجوانب المحليه والدولية والعالميه والتقليل من استعمال التطورات التكنلوجيا في الاتصال وحفظ البيانات .

3- إنشاء مراكز بحثية في مؤسسات الدولة وعمل نشاطات في مختلف الاختصاصات لنشر الوعي بخطورة هذه الحروب وأهدافها بما في ذلك تعريف المفاهيم المشابهة مثل الأمن السيبراني والإرهاب السيبراني.

4- تنفيذ آليات الدفاع والمواجهة والردع من الحرب السيبرانية، وأبرزها زيادة التعاون والشراكات بين الدول وكذلك بين القطاعين الخاص والعام للحد من الهجمات السيَبرانيه والحد منها .

5- تفعيل القوانين التي تنظم الفضاء خصوصا قوانين الحرب السيبرانية، وضرورة نشر الوعي والادراك للأفراد بخطورة هذه الحرب بطرق واضحة ومبسطة .

المصادر

المصادر العربية

1. احمد عبيس نعمة، الهجرات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنهما في ضوء التنظيم الدولي المعاصر، (بابل، مجلة المحقق المحلي العلوم القانونية والسياسية ، العدد (4) ، 2016) .
2. ايهاب خليفة ، الحرب السيبرانية : مواجهة العقيدة العسكرية استعداداً للمعركة القادمة ، (القاهرة ، مجلة السياسة الدولية ، العدد 11 ، المجلد 53 ، 2018) .
3. توماس ج . ما تكين ترجمة نهى مصطفى ، استراتيجيات الدفاع الامريكي (جريدة عمان، 2024) : http://www.omandaily.com .
4. رغدة البهي ، التجربة المصرية في مكافحة الارهاب السيبراني: رؤية تحليلية ، (القاهرة، مركز الأهرام للدراسات السياسية والاستراتيجية ، 2013) acpss.ahram.org.eg .
5. سالم عبود محمد ، نظم المعلومات الاستراتيجية الامنية (بغداد، دار الدكتور للعلوم ، ط1 ، 2022) .
6. سماح عبد الصبور، الصراع السيبراني طبيعة المفهوم وملامح الفاعلين ، (القاهرة ، مجلة السياسة الدولية ، مجلد 52 ، 2017) .
7. عادل عبد الجواد، دور مركز المعلومات في التعامل مع الازمات (الرياض، مجلة الامن والحياة ، العدد 358 ، 2016) .
8. علاء عبد الرزاق السالمي، المدخل الى الامن السيبراني، (بغداد، دار الذاكرة للنشر والتوزيع ، ط1 ، 2021) .
9. علي زياد العلي ، الصراع والامن الجيوسيبراني في السياسة الدولية دراسة في استراتيجية الاشتباك الرقمي، (عمان ، دار امجد للنشر والتوزيع ، ط1 ، 2019).
10. علي زياد العلي، الخصخصة الأمريكية للحروب الجيل الخامس من وسائل التدخل والاستخبارات، (مركز دراسات كاتبغون، 2017/7/27) http://katehon.com
11. علي عبد الرحيم العبودي ، الحروب السيبرانية وتداعياتها على الامن والسلم الدوليين، (بغداد، المجلة الأكاديمية العلمية ، المجلد 57 ، 2019) .
12. عمرو حسن فتوح، الحروب المتقدمة، الحروب التكنلوجية الباردة بين الدول العظمى نموذجاً (القاهرة ، مجلة السياسة الدولية، 2022) www.siyassa.org.eg

13. فارس محمد العمارات ، الامن السيبراني المفهوم وتحديدات العصر، (عمان، دار الخليج للنشر والتوزيع، ط 1 ، 2024) .
14. فاطمة الزهراء عبد الفتاح ، تطور توظيف جماعات العنف " الارهاب السيبراني " (القاهرة ، مجلة السياسة الدولية ، العدد 208، 2017) .
15. فراس جمال شاكر ، السيبرانية وتحولات القوة في النظام الدولي ، (عمان ، دار امجد للنشر والتوزيع ، 2022) .
16. فرد كابلان ، ترجمة لؤي عبد المجيد، المنطقة المعتمة : التاريخ السري للحروب السيبرانية ، (الكويت، المجلس الوطني للثقافة والفنون ، 2019) .
17. محمد كاظم المعيني، أيكلوجيا الارتقاء الصين وتجليات المستقبل دراسة في الامكانيات والتحديات (بيروت، دار السنهوري، 2018) .
18. محمد منذر ، وسرى غضبان ، تكنولوجيا الحروب السيبرانية واستراتيجيات المواجهة الدولية (بغداد ، دار ومكتبة عدنان ، ط1 ، 2021) .
19. محمود جمل ، كيف استخدمت روسيا الهجمات الإلكترونية في حربها مع أوكرانيا؟،2023، https://alqaheranews.net/new
20. منى الاشقر جبور، السيبرانية هاجس العصر،(القاهرة ، المركز العربي للبحوث القانونية والقضائية ، ط1 ،2018) .
21. منير البعلبكي، قاموس المورد عربي انكليزي ، (بيروت ، دار الملايين ، 2004).
22. منير شفيق ، الاستراتيجية والتكتيك في فن علم الحرب ، (بيروت، الدار العربية للعلوم ناشرون ، ط 1 ، 2008) .
23. نبيل عودة ، العمليات السيبرانية في الحرب الروسية الأوكرانية طبيعتها وأنماطها، 2022 الشرق للأبحاث الاستراتيجية https://research.sharqforum.org
24. نصر سفاح ، الحروب الالكترونية واثرها على الامن القومي، (بغداد ، مركز النهرين للدراسات الاستراتيجية ، 2023) https://www.alnahrain.iq .
25. نوران شفيق، اثر التهديدات الإلكترونية على العلاقات الدولية : دراسة في ابعاد الأمن الإلكتروني ، (القاهرة، المكتب العربي للمعارف ، 2019) .
26. وزارة الخارجية الامريكية : httpss://www.stste.gov/release.ofunite
27. وسام الامير حميدي ، سلام بلا نهاية ، (القاهرة، دار الكتاب للطباعة والنشر، ط 1 ، 2014) .
28. وسام مهيوب، نموذج الولايات المتحدة الامريكية في مجال الامن السيبراني : بين الهجوم وإمكانيات الدفاع ، (الجزائر ، مجلة البيان ، العدد 2 ، 2023) .

29.Cyber resilience, the cyber challenge and the role of insurance, December 2014

المصادر الاجنبية

1. Ahmed Abis Ne'meh, Cyber Migrations: Its Concept and the International Responsibility Arising from Them in Light of Contemporary International Organization, (Babylon, Local Investigator Journal of Legal and Political Sciences, Issue (4), 2016).
2. Ihab Khalifa, Cyber Warfare: Confronting Military Doctrine in Preparation for the Coming Battle, (Cairo, International Politics Journal, Issue 11, Volume 53, 2018).
3. Thomas J. Ma Tekin, translated by Noha Mustafa, American Defense Strategies (Oman Newspaper, 2024): http://www.omandaily.com.
4. Raghda Al-Bahi, The Egyptian Experience in Combating Cyber Terrorism: An Analytical Vision, (Cairo, Al-Ahram Center for Political and Strategic Studies, 2013) acpss.ahram.org.eg.
5. Salem Aboud Muhammad, Strategic Security Information Systems (Baghdad, Dar Al-Doctor for Sciences, 1st ed., 2022).
6. Samah Abdel-Sabour, Cyber Conflict, Nature of the Concept and Features of Actors, (Cairo, International Politics Magazine, Volume 52, 2017).
7. Adel Abdel-Gawad, The Role of the Information Center in Dealing with Crises (Riyadh, Security and Life Magazine, Issue 358, 2016).
8. Alaa Abdul Razzaq Al-Salmi, Introduction to Cyber Security, (Baghdad, Dar Al-Dhakira for Publishing and Distribution, 1st ed., 2021).
9. Ali Ziad Al-Ali, Conflict and Geo-Cyber Security in International Politics, A Study in the Strategy of Digital Engagement, (Amman, Dar Amjad for Publishing and Distribution, 1st ed., 2019).
10. Ali Ziad Al-Ali, American Privatization of Wars, the Fifth Generation of Intervention and Intelligence Means, (Katehon Studies Center, 7/27/2017) http://katehon.com

11. Ali Abdul Rahim Al-Aboudi, Cyber Wars and Their Implications for International Peace and Security, (Baghdad, Scientific Academic Journal, Volume 57, 2019).
12. Amr Hassan Fattouh, Advanced Wars, Cold Technological Wars between the Great Powers as a Model (Cairo, International Politics Magazine, 2022) www.siyassa.org.eg
13. Fares Muhammad Al-Amarat, Cybersecurity: The Concept and Determinations of the Era, (Amman, Dar Al-Khaleej for Publishing and Distribution, 1st ed., 2024).
14. Fatima Al-Zahraa Abdel Fattah, The Development of the Use of Violent Groups "Cyber Terrorism" (Cairo, International Politics Magazine, Issue 208, 2017).
15. Firas Jamal Shaker, Cyber and Power Transformations in the International System, (Amman, Dar Amjad for Publishing and Distribution, 2022).
16. Fred Kaplan, translated by Louay Abdul Majeed, The Dark Zone: The Secret History of Cyber Wars, (Kuwait, National Council for Culture and Arts, 2019).
17. Muhammad Kazim Al-Muaini, The Ecology of China's Ascension and Manifestations of the Future: A Study of Possibilities and Challenges (Beirut, Dar Al-Sanhouri, 2018).
18. Muhammad Munther and Sari Ghadhban, Cyber Warfare Technology and International Confrontation Strategies (Baghdad, Dar and Adnan Library, 1st ed., 2021).
19. Mahmoud Jamal, How Did Russia Use Cyber Attacks in Its War with Ukraine?, 2023, https://alqaheranews.net/new
20. Mona Al-Ashqar Jabour, Cyber Obsession of the Age, (Cairo, Arab Center for Legal and Judicial Research, 1st ed., 2018).
21. Munir Al-Baalbaki, Al-Mawrid Dictionary, Arabic-English, (Beirut, Dar Al-Malayin, 2004).
22. Munir Shafiq, Strategy and Tactics in the Art of War Science, (Beirut, Arab House for Science Publishers, 1st ed., 2008).
23. Nabil Awda, Cyber Operations in the Russian-Ukrainian War: Its Nature and Patterns, 2022, Al-Sharq for Strategic Research https://research.sharqforum.org

24. Nasr Safah, Electronic Wars and Their Impact on National Security, (Baghdad, Al-Nahrain Center for Strategic Studies, 2023) https://www.alnahrain.iq .
25. Nouran Shafiq, The Impact of Electronic Threats on International Relations: A Study in the Dimensions of Electronic Security, (Cairo, Arab Office for Knowledge, 2019).
26. US Department of State: httpsss www.stste.gov release.ofunite
27. Wissam Al-Amir Hamidi, Peace Without End, (Cairo, Dar Al-Kitab for Printing and Publishing, 1st ed., 2014).
28. Wissam Mahyoub, The US Model in Cybersecurity: Between Attack and Defense Capabilities, (Algeria, Al-Bayan Magazine, Issue 2, 2023).
29. Cyber resilience, the cyber challenge and the role of insurance, December 2014