
مجلة علمية محكمة

**دورية فصلية**

تصدر عن كلية التربية للبنات

Iraqi University

COLLEGE OF EDUCATION FOR WOMEN JOURNAL

**جهة الإصدار: كلية التربية للبنات / الجامعة العراقية اختصاص المجلة:**

**العلوم الإنسانية والتربوية**

ISSN 2708-1354 (Print)

**ISSN 2708-1362 (Electronic)**

**رقم الاعتماد في دار الكتب والوثائق العراقية 2138 لسنة 2016م نوع الإصدار:**

**(فصلي) كل ثلاثة أشهر.**

**نطاق التوزيع: داخل العراق البريد الإلكتروني:-**

***wom.mag.uni@aliraqia.edu.iq***

**هاتف سكرتارية التحرير: 07747936814 (الهاتف الأرضي) داخلي: (2028)**

**مجلة كلية التربية للبنات – الجامعة العراقية ، المجلات الأكاديمية المحكمة:**

**https://www.iasj.net/iasj/journal/349/issues**

وزارة التعليم العالي والبحث العلمي
الجامـــــعة العراقية
كلية التربية للبنات

# مـــــجَـــلَـــة


مَجلة عِلمية محكمة

تصدر عن كلية التربية للبنات

فـصلية دوريـــة

العدد الحادي والثلاثـــــون (31) الجزء الأول (1)
الصادر بتاريخ: 15/كانون الأول/2025

بسم الله الرحمن الرحيم

﴿ الرَّحْمَٰنُ ۝١ عَلَّمَ الْقُرْآنَ ۝٢ خَلَقَ
الْإِنسَانَ ۝٣ عَلَّمَهُ الْبَيَانَ ﴾

**سورة الرحمن: الآيات ١ - ٤**

١٥. أ.م.د سماح ثائر خيري / تخصص: رياض اطفال .....عضواً
١٦. أ.د يونس يحيى عبدالله / تخصص: اللغة العربية / اللسانيات النصية.....عضواً ومدققاً لغوياً.
١٧. أ.م سيناء احمد جار الله / تخصص: دراسات مالية / ادارة مالية .....عضواً ومحاسباً مالياً.

## خامساً : موظفو المجلة

١. م.م. مروة مرزا حمزة / تخصص : تاريخ / مسؤولة وحدة المجلة .

٢. براء إبراهيم سالم / سكرتيرة المجلة .

## قائمة المحتويات – العدد (٣١) الجزء الأول 15/كانون الأول/2025– البحوث المحكمة

**التعريف:**

**مجلة علمية دورية محكمة فصلية تصدر عن كلية التربية للبنات الجامعة العراقية**

**تحمل الرقم الدولي:**

**ISSN (print): 2708 – 1354 ISSN (online): 2708 – 1362**

**مجلة معتمدة في دار الكتب والوثائق العراقية بالرقم: (2138) لسنة 2016م**

**وتقوم بنشر البحوث العلمية القيمة والأصيلة**

**في مجالات العلوم الإنسانية المختلفة باللغتين العربية والإنجليزية.**

## دعـــوة:

ترحب هيئة تحرير المجلة بإسـهامات الباحثين، وأصـحاب الأقلام من الكتاب والمثقفين في أقسـام الفكر الإسـلامي، والعلوم الإنسـانية، والاجتماعية، والتعليمية والتربوية، وكل ما له صـلة بشـؤون المرأة والمجتمع، وقضـايا الإنماء التربوي والتعليمي، والبرامج التطويرية المعاصـرة على وجه العموم ، على وفق قواعد النشـر المعتمدة من هيئة تحرير المجلة ، على وفق تعليمات وضـوابط النشـر في الـمجلات العلمية الصادرة من دائرة البحث والتطوير في وزارة التعليم والبحث العلمي الموقرة.

## ضوابط النشر في المجلة

١. تتخصص المجلة بنشر الحوث العلمية القيمة والأصيلة في المجالات الإنسانية، والتي لم يسبق نشرها أو تقديمها إلى أي جهة أخرى (بتعهد خطي من صاحب البحث) ضمن المحاور المشار إليها في التعريف أعلاه ،شرط الالتزام بمنهجية البحث العلمي وخطوات المتعارف عليها محلياً وعالمياً، وتقبل البحوث بإحدى اللغتين العربية أو الانجليزية بنسبة محددة.

٢. تخضع البحوث المرسلة إلى المجلة جميعها لفحص أولي من هيئة التحرير لتقرير مناسبتها لتخصص المجلة، ثم لبيان أهليتها للتحكيم، ويحق لهيئة التحرير أن تعتذر عن قبول البحث بالكامل، أو تشترط على الباحث تعديله بما يتناسب وسياسة المجلة قبل إرسال إلى المحكمين.

٣. ضرورة تحقق السلامة اللغوية مع مراعاة علامات الترقيم، ومتانة الأسلوب ووضوح الفكرة علل أن يكون الباحث مسؤولًا عن السلامة اللغوية للبحث المقدم باللغتين العربية والإنجليزية.

٤. ترسل البحوث المقبولة للتحكيم العلمي السري إلى خبراء من ذوي الاختصاص قبل نشرها، للتأكد من الرصانة العلمية والموضوعية والجدة والتوثيق على وفق استمارة معتمدة ولا تلتزم هيئة التحرير بالكشف عن أسماء محكميها، وترفض البحوث المتضمنة في خلالها إشارات تكشف عن هوية الباحث.

٥. لضمان السرية الكاملة لعملية التحكيم تكون المعلومات الخاصة بهوية الباحث أو الباحثين في الصفحة الأولى من البحث فحسب.

٦. يلتزم الباحث بإجراء التعديلات الجوهرية المقترحة من المحكمين للبحث.

٧. يحق لهيئة تحرير المجلة رفض البحث واتخاذ القرار وعدم التعامل مع الباحث مستقبلاً عند اكتشافها ما يتنافى والأمانة العلمية المطلوبة بعد التثبت من ذلك.

٨. تنتقل حقوق طبع البحث ونشره الى المجلة عند إخطار صاحب البحث بقبول للنشر، ولا يجوز النقل أي عن البحث إلا بالإشارة إلى مجلتنا، ولا يجوز لصاحب البحث أو لأي جهة أخرى إعادة نشره في كتاب أو صحيفة أو دورية إلا بعد أن يحصل على موافقة خطية من رئيس التحرير.

٩. لا تدفع مكافأة للباحثين عن البحوث المحكمة التي تقبل للنشر في المجلة وتقدم رئاسة هيئة التحرير مكافأة خاصة للمحكمين.

١٠. تعتمد المجلة آلية التوثيق المتنوعة فتقبل البحوث بآلية التوثيق بالهوامش سواء أكان في نفس الصحيفة ، أم في نهاية البحث، كما تقبل البحوث بآلية التوثيق في المتن بالطريقة

المتعارف عليها عالمياً بـ APA.

١١. تقبل المجلة كذلك البحوث الميدانية أو المعملية ،شرط أن يورد الباحث مقدمة يبين فيها طبيعة البحث ومدى الحاجة اليه ، ومن ثم يحدد مشكلة البحث في هيئة مساءلات أو فرضيات، ويعرف المفاهيم والمصطلحات، ويقدم ،عندها قسماً خاصاً بالإجراءات يتناول فيه خطة البحث ومجتمع والعينات والادوات ، فضلا عن قسم خاص بالنتائج ومناقشتها، ويورد أخيراً قائمة المراجع.

١٢. لا يجوز نشر أكثر من بحث للباحث في العدد الواحد من المجلة سواء أكان بحث منفرداً أم مشتركاً مع باحث آخر.

١٣. يزود صاحب البحث– عند نشره– بنسخة واحدة مستلة مختومة من البحث المنشور في العدد.

١٤. تحتفظ هيئة التحرير بحقها في أولوية النشر في كل ما يرد إليها من مطبوعات، تأخذ بنظر الاعتبار توازن المجلة، والأسبقية في تسليم البحث معدلاً بعد التقويم، واعتبارات أخرى، ويخضع ترتيب البحوث في العدد الواحد للمعايير الفنية المعتمدة في خطة التحرير.

١٥. البحوث المنشورة في المجلة تعبر عن آراء أصحابها، ولا تعبر بالضرورة عن رأي هيئة التحرير أو رأي الكلية.

١٦. جميع المراسلات المتعلقة بالمجلة كافة تكون باسم رئيس التحرير، أو مدير التحرير عبر العنوان البريدي :wom.Mag.uni@aliraqia.edu.iq ، أو رقم هاتف المجلة.

١٧. أخيرا تؤكد هيئة التحرير على ضرورة الالتزام بالبحث الموضوعي الحر والهادئ والبعيد عن كل أشكال التهجم أو المساس بالرموز والشخصيات، وتنأى عن نشر الموضوعات التي تمس المقدسات، أو تلك التي تدعو إلى العصبيات الفئوية والطائفية، وكل ما يوجب الفرقة ويهدد السلم المجتمعي.

# دليل المؤلف Author Guidelines

١. يقدم الباحث طلب خطي (استمارة رقم 1 المرفقة) مختوم بالختم الرسمي لجهة الانتساب .

٢. يقدم الباحث ثلاث نسخ ورقية مطبوعة مكبوسة على ورق( A4) وعلى وجه واحد، وتكون إعدادات حواشي الصفحة 5.2سم من كل جانب بخط( Simplified Arabic)بحجم 14 للمتن و 12 للهامش، و16 غامق للعنوان الرئيسي و 15 غامق للعنوان الفرعي. واذا كان البحث باللغة الانجليزية فيكون بخط( Times New Roman) .

٣. لا يزيد البحث عن خمس وعشرين صفحة ، ويكون من ضمنها المراجع والحواشي والجداول والأشكال والملاحق. ويتحمل الباحث ما قيمته ثلاثة آلاف دينار عن كل صحيفة زائدة.

٤. يوقع الباحث التعهد الخاص بكون البحث لم يسبق نشره، ولم يقدم للنشر الى جهات أخرى، ولن يقدم للنشر في الوقت نفسه حتى انتهاء إجراءات التحكيم (استمارة رقم 2).

٥. يلتزم الباحث بتقديم نسخة من كتاب الاستلال الإلكتروني للبحث وبخلافه يتعذر النشر.

٦. يتعهد الباحث بجلب نسخة إلكترونية من البحث على قرص حاسوب (CD) بعد إجراء جميع التعديلات المطلوبة وقبول البحث للنشر في المجلة.

٧. يرفق مع البحث خلاصة دقيقة باللغتين العربية والانجليزية على ألا تزيد على صحيفتين مع السيرة الذاتية.

٨. يسدد الباحث أجور النشر والخبراء بحسب مقدارها بكل لقب علمي على وفق المنصوص عليه في الكتب الرسمية ، ويتم تسليم الاجور الى الجهة الرسمية في القسم المالي للكلية بوصولات رسمية تحفظ حق الباحث وادارة المجلة ، ولا تسترد الاجور في حالة رفض رئيس التحرير او المقيمين للبحث المقدم لأسباب علمية او لسلامة الفكرية او غيرها.

٩. يستلم الباحث إيصالا خطيا بتاريخ تسليم البحث. ثم يُعلم بالإجراءات التي تمت.

١٠. إذا استخدم الباحث واحدة من أدوات البحث في الاختبارات أو جمع البيانات فعليه أن يقدم نسخة كاملة من تلك الأداة اذا لم تنشر في صلب البحث أو ملاحق .

١١. تلتزم المجلة بإرسال البحث الى مقومين بخطاب تأليف، استمارة رقم 3 المرفقة ، على أن يتم تقويم البحث في مدة أقصاها ١٠ أيام، وبخلافهِ يقدم الخبير اعتذاره في أسبوع، وعندما يكون التقويم العلمي ايجابياً باتفاق اثنين من المقومين يحال البحث إلى المقوم اللغوي لتدقيقه لغوياً.

# دليل المقوم Reviewer Guidelines

أدناه الشروط والمتطلبات الواجب مراعاتها من قبل المقوم للبحوث المرسلة:

١. يقوم البحث على وفق استمارة معتمدة للتقويم (استمارة رقم 4) تتضمن الآتي:

أ- فقرة تتعلق بموضوع البحث هل سبقت دراسته من قبل بحسب علمكم؟ وهل يوجد اقتباس حرفي؟ (الإشارة إلى الاقتباس إن وجد) أو استلال مع تحديد مكان الاستلال.

ب - جدول تقويمي فني تفصيلي يعبر عنه بـ (24) فقرة محددة صيغت على وفق مقياس ليكرت الثلاثي: جيد (3)، مقبول :(2)، ضعيف:( 1) ويقوم الخبير بالتأشير على اختيار واحد منها تبعاً لقناعته بمحتوى الفقرة وعدم ترك أي فقرة بدون إجابة.

ت - مكان محدد لملاحظات الخبير الخاصة بتفاصيل البحث، أو بأساسيات العامة (علمية أو منهجية) كي يستفيد منها الباحث.

ث - خلاصة التقويم المتعلقة بصلاحية النشر على وفق ثلاث خيارات (صالح للنشر أو صالح بعد إجراء التعديلات، أو غير صالح للنشر) على وفق المعايير المحددة في الاستمارة.

ج - مكان محدد لتثبيت مسوغات عدم الصلاحية للنشر إذا حكم بذلك.

٢. على المقوم التأكد من تطابق وتوافق عنوان الخلاصتين العربية والإنجليزية لغوياً.

٣. أن يبين المقوم هل أن الجداول والأشكال التخطيطية الموجودة واضحة ومعبرة.

٤. أن يبين المقوم هل أن الباحث اتبع الأسلوب الإحصائي الصحيح.

٥. أن يوضح المقوم هل أن مناقشة النتائج كانت كافية ومنطقية.

٦. على المقوم تحديد مدى استخدام الباحث المراجع العلمية.

٧. يمكن للمقوم أن يوضح بورقة منفصلة التعديلات الأساسية لغرض قبول البحث.

٨. توقيع الخبير على الاستمارة تمثل تعهداً خطياً بأنه قام بتقويم البحث علميا على وفق المعايير الموضوعية، وان البحث يستحق التقويم الحاصل عليه ومطلوب تسجيل اسمه على وفق ما مثبت في الاستمارة.

بسم الله الرحمن الرحيم

## افتتاحيةُ العدد...

الحمدُ للهِ ربِّ العالمين ، والصلاةُ والسلامُ على نبيِّنا محمدٍ ، وعلى آلهِ وصحبهِ تسليماً كثيراً...

أما بعدُ...

يولدُ عدد جديد من مجلة ( كلية التربية للبنات / الجامعة العراقية ) يحمل الرقم31 ، الواحد والثلاثين ، بتأريخ 2025/12/15 ، يحوي بحوثاً متنوعة بين لغوية وأدبية وتربوية ونفسية وتاريخية واجتماعية ، وبحوث اللغة الإنكليزية ، ليكون العدد منهلاً للباحثين والدارسين والقراء عموماً ، يروي عطش المعرفة وحب العلم والتميز.

وفي هذا الإطار تؤكد إدارة المجلة حرصها على أن تكون البحوث المنتخبة في المجلة مثمرة للمجتمع والإنسان العراقيين ، وأن تلتزم بمبادئ وزارة التعليم العالي والبحث العلمي وتعليماتها ، في نوعية الموضوعات التي تعالجها ، واسهامها المباشر في تنمية المجتمع العراقي والارتقاء به في سلم العلم والمعرفة .

نسأل الله السداد والتوفيق للباحثين والقراء ، ونسأله تعالى السداد لنا في عمل تحرير المجلة ، وأن يكون العمل خالصاً لوجهه الكريم ، ويكون لبنة في البناء المعرفي والعلمي لكليتنا الرصينة ، وخطوة نحو التقدم والازدهار العلمي لعراقنا الحبيب ، ومن الله التوفيق ، وصلى الله على سيدنا محمد وآله وصحبه وسلم تسليماً كثيراً.

**مدير تحرير المجلة**

**أ.د.أحمد عبد الجبار فاضل**

**شتاء 2025/12/15**

# الحروب السيبرانية وانعكاساتها على العلاقات الدولية :

# دراسة تحليلية للعلاقات بين واشنطن وطهران

# Cyber wars and their repercussions on international relations: an analytical study of relations between Washington and Tehran

المدرس المساعد/عبد الرحمن محمد داود

كلية الهندسة/الجامعة العراقية

**المستخلص**

تعد الحرب السيبرانية من أبرز مظاهر التهديدات الحديثة التي فرضها التطور التكنولوجي على الأمن الدولي، حيث لم تعد النزاعات بين الدول تقتصر على المواجهات العسكرية التقليدية، بل امتدت لتشمل الفضاء الرقمي كساحة صراع جديدة. يتناول هذا البحث الحرب السيبرانية بوصفها أداة استراتيجية تستخدمها الدول للتأثير على الخصوم وتحقيق أهداف سياسية وأمنية دون اللجوء إلى القوة العسكرية المباشرة.

تسعى الدراسة إلى تحليل تأثير الهجمات السيبرانية المتبادلة بين الولايات المتحدة وإيران على العلاقات الثنائية بين البلدين، مع التركيز على أبرز الحوادث السيبرانية التي شكلت نقاط تحول في مسار العلاقات، مثل الهجمات على البنى التحتية الحيوية. كما تستعرض الدراسة كيف ساهمت هذه المواجهات الرقمية في تصعيد التوتر، وإعادة تشكيل مفاهيم الردع والتهديد في النظام الدولي المعاصر.

وعليه فأن الحرب السيبرانية أصبحت جزءًا لا يتجزأ من العلاقات الدولية، وأن تزايد استخدامها يعيد صياغة قواعد التفاعل بين الدول، ويفرض تحديات جديدة أمام أدوات الدبلوماسية التقليدية. كما أكدت أن الصراع السيبراني بين الولايات المتحدة وإيران يمثل نموذجًا معقدًا يعكس التداخل بين التكنولوجيا والسياسة والأمن في البيئة الدولية الحديثة.

Cyber warfare is one of the most prominent manifestations of modern threats imposed by technological development on international security, as conflicts between countries are no longer limited to traditional military confrontations. It has even extended to include cyberspace as a new arena of conflict. This research examines cyber warfare as a strategic tool used by states to influence adversaries and achieve political and security objectives without resorting to direct military force. The study seeks to analyze the impact of mutual cyber attacks between the United States and Iran on bilateral relations between the two countries, focusing on the most prominent cyber incidents that constituted turning points in the course of relations, such as attacks on critical infrastructure. The study also examines how these digital confrontations have contributed to escalating tensions and reshaping the concepts of deterrence and threat in the contemporary international system.

Reshaping the concepts of deterrence and threat in the contemporary international system.

Therefore, cyber warfare has become an integral part of

international relations, and its increasing use is reshaping the rules of interaction between states, posing new challenges to traditional diplomatic tools. It also emphasized that the cyber conflict between the United States and Iran represents a complex model reflecting the interplay

between technology, politics, and security in the modern international environment .

## المقدمة

تعُد ظاهرة الحرب بشكل عام من الظواهر الأساسية في النظام الدولي والعلاقات الدولية ، لأنها ظاهرة قديمة والمحرك الأساسي للتاريخ والعلاقات الدولية ، ومع تطور أجيال الحروب برزت أشكال جديدة من الحروب ومنها الحروب السيبرانية ، تمثلت الحروب السيبرانية شكل جديد من أشكال الحروب ألحديثة ولجأت الدول في شنها لما تنطوي من مزايا وخصائص تختلف عن الحروب التقليدية ، أذ أضحى التطور ألتكنولوجي والثورة في ميدان ألتكنولوجيا يمثل ركيزة أساسيه في بنية النظام الدولي ، اذ عمل هذا التطور على توسيع مجال الفضاء السيبراني وسهوله الدخول الية الى امتلاك الدول للقدرة وألقوه السيبرانية واستطاعت من خلالها هذه الدول من شن هجمات سيبرانية فيما بينها لتحقيق أهدافها وغاياتها بوسائل غير تقليديه وبشكل حروب غير عسكرية لما تنطوي عليه تلك الحروب من خسائر مادية وبشرية ، وبفعل تحولات القوة بكامل خصائصها تضمنت تلك التحولات الى أنتشار القوة السيبرانية الى مراكز وأطراف غير فاعلة في النظام الدولي ، مثل الجماعات الإرهابية ، والشركات ألمتعددة ألجنسيات بالإضافة الى الدول ألرئيسية في هذا النظام .

ولجأت الدول الي شن هجمات سيبرانية متفاوتة الشده وبأنماط مختلفة لتحقيق غاياتها ، مثل القرصنة والتجسس ، وسرقه المعلومات ، وتدمير البنية ألتحتية للدول والمؤسسات الحكومية المدنية والعسكرية ، مما أدى الى التأثير على شكل العلاقات بين الدول في بيئة السياسة الدولية ، وتضمن هذا التأثير تغيير في بعض مفاهم وظواهر العلاقات الدولية منها (التحالفات ، توازن القوى ، سباق التسلح) ، اذ لجأت الدول الى العمل وفق استراتيجيات أمنية سيبرانية وركزت على التعاون الدولي وتعزيز مفهوم الشراكة في مجال الفضاء السيبراني ،تصاعدت حدة الهجمات بين الدول بشكل كبير في ألحقيه الأخير عما كانت علية ، من هذه الدول هي ( الولايات المتحدة وإيران) ، واستطاعت هذه الدول بفضل امتلاكها للقوة السيبرانية الى تطوير قدراتها السيبرانية وأنشاء مؤسسات أمنية حكومية وأخرى غير حكومية ، وتخصيص ميزانيات ضخمة في هذا الجانب ، أذ تعتبر الولايات المتحدة الأمريكية الأولى في مجال الفضاء السيبراني لما تملكه من قدرات ومؤسسات وبنية تحتية

في هذا المجال ، وبرزت أيران كدولة ثانية وعملت على تطوير قدراتها بشكل لافت مما أدى الى نشوب صراع آخر في بيئة الفضاء السيبراني بين الدولتين ،وأخذت الهجمات تتوالى فيما بينهم واستطاعت هذه الدول بفعل الهجمات السيبرانية من تدمير البنية ألتحتية وتحقيق أهدافها من خلال هذه الهجمات وبشكل غير تقليدي ويختلف عما كانت عليه طبيعة الهجمات في ألسابق ، كل هذه الأحداث دفعت بالدول الى تحقيق ألتفوق في الفضاء السيبراني وتحصين نفسها من الهجمات السيبرانية في ألمستقبل من خلال أتخاذ التدابير الأمنية في هذا الجانب

أهمية البحث : تكمن أهمية البحث في مكانة الحرب السيبرانية في العلاقات الدولية ، أذ أن البحث في مفهوم الحرب السيبرانية تعد بحد ذاتها عملية نوعية وهادفة طالما أنها تشكل ظاهرة مهمه في حياة ألمجتمعات والدول والافراد في ألوقت ألحالي ، ومعرفه طرق تأثيرها على العلاقات الدولية من خلال تناول مفهوما وخصائصها ومكوناتها ، ومحاولة تبيان طريقة تأثيرها على بنية النظام الدولي ومعرفه الأطراف والفواعل غير ألرئيسيين في النظام الدولي وكيف تمكنوا من امتلاك القوه السيبرانية وشن هجمات سيبرانية فيما بينهم ، ومدى تأثير الدول فيما بينهم وقدرتهم على شن هجمات سيبرانية متبادلة مما عزز ذلك التأثير عل شكل العلاقات بين الدول .

أهداف البحث : أن هدف البحث هوة تبيان ألطريقة التي أثرت بها الحرب السيبرانية على العلاقات الدولية ، من خلال ألتطرق الى مفهوم هذه الحروب وأنماطها ونشأتها ، ومعرفة واقع الهجمات السيبرانية بين الدول الأطراف في النظام الدولي ، والتعرف على خصائص القوة السيبرانية والأسلحة ألخاصة بهذه الحروب ، ومدى تأثيرها على البنية ألتحتية للدول ، وانعكاس تلك الهجمات على بنية النظام الدولي ، والآثار التي تتركها تلك الحروب على العلاقات ألمتبادلة بين الدول .

أشكالية البحث : تكمن أشكالية ألدراسة في جملة من الأسئلة ألفرعية تتكامل لتكون السؤال ألرئيسي والذي مفاده : ما هو أثر الحرب السيبرانية على العلاقات الدولية ، وما هو الدول في هذا التأثير وكيف استطاعت تلك الدول من توظيف الحرب السيبرانية لتحقيق أهدافها ؟ وتنطلق ألعديد من الأسئلة ألفرعية من هذا التساؤل بالشكل ألآتي :

١- ما مفهوم الحرب السيبرانية وماهي هي خصائصها ومكوناتها ؟

٢ – ما تأثيرها على العلاقات الدولية وهل وضعت الدول استراتيجيات أمنية سيبرانية في مجال الفضاء السيبراني؟

٣- ما طبيعة الهجمات السيبرانية بين الولايات المتحدة إيران ومدى تأثيرها ؟

٤- ما هي الرؤية ألمستقبلية لتلك الهجمات ؟

فرضية البحث : للإجابة على التساؤلات ألمطروحة ينطلق البحث من فرضية مفادها : أن هنالك تأثير للحرب السيبرانية على العلاقات الدولية ، واستطاعت الدول بفعل الهجمات السيبرانية من التأثير على شكل وطبيعة العلاقات بين الدول في البيئة ألسياسية ، وأن هذه الحروب تحتوي على خصائص وأنماط ومكونات ، أذ هنالك هجمات بين الولايات المتحدة إيران دفعت بالدولتين الى تبني استراتيجيات أمنية سيبرانية في مجال الفضاء السيبراني ، والتعرف على الرؤية المستقبلية وفق مشاهد محددة .

منهجية البحث : تم الاعتماد على المنهج ألوصفي ألتحليلي ألذي يهدف الى دراسة الحرب السيبرانية من خلال تحديد الهجمات السيبرانية وتحليلها وكيفية تأثيرها على العلاقات الدولية ، وتم الاعتماد على المنهج الاستشرافي ألمستقبلي وذلك لإعطاء رؤية مستقبلية عن الهجمات السيبرانية في ألمستقبل .

الدراسات السابقة : تتميز المعرفة العلمية بخاصية متميزة هي الصفة التراكمية وهذا ما يجعل كل دراسة تستند إلى دراسات سابقة، ولهذا استعانت هذه الدراسة بمجموعة لدراسات التي تفيد في معالجة الموضوع وهي :

١- صلاح حيدر عبد الواحد ، ( حرب الفضاء الإلكتروني : دراسة في مفهومها وخصائصها وسبل مواجهتها ) : تناولت هذه الدراسة الحروب الإلكترونية ومنها السيبرانية كمظهر جديد للحروب ، والسمات والخصائص التي تتميز بها هذه الحروب عن غيرها من الحروب التقليدية ، وسبل معالجتها والامكانيات ألمتاحة لمنع شن هجمات سيبرانية في ألمستقبل

٢- سليم دحماني ، أثر التهديدات " السيبرانية " على الأمن القومي – الولايات المتحدة انوذجاً : تتناول هذه ألدراسة أثر الهجمات السيبرانية على الأمن ألقومي للدول وعلى العلاقات بين الدول في بيئة السياسة الدولية ، وتقدم رؤيا مستقبلية لتلك الهجمات ، وتستعرض ألاستراتيجيات الأمنية السيبرانية للولايات المتحدة ، وتبين التعاون ألمشترك في مجال الفضاء السيبراني وسبل تعزيز الأمن العالمي .

**حدود البحث :**

١- الحدود ألمكانية : مع تصاعد الهجمات السيبرانية وسبل الدول في مواجهتها ووضع استراتيجيات أمنية للحد من الهجمات ، أخترنا حالة الهجمات السيبرانية بين الولايات المتحدة

وإيران.

٢- الحدود ألزمانية : الفترة ألزمانية للدراسة تنطلق منذ بداية الهجمات السيبرانية بين الولايات المتحدة و إيران من ٢٠١٠ الى الآن .

هيكلية البحث : تم تقسيم البحث ألي مقدمة وثلاث مباحث والخاتمة والاستنتاجات وكالآتي: كل مبحث تضمن ثلاث مطالب، اذ المبحث الأول أطار نظري للحرب السيبرانية وتم تقسيمة الى ثلاث مطالب : المطلب الأول ( مفهوم الحرب السيبرانية وأنماطها ومكوناتها ) ، والمطلب ألثاني ( خصائص الحرب السيبرانية ومراحلها ) ، والمطلب الثالث ( تأثير الحرب السيبرانية على العلاقات الدولية ) ، أما المبحث ألثاني بعنوان ( الحرب السيبرانية بين الولايات المتحدة أيران ) وتم تقسيمة الى مطلبين : المطلب الأول ( ألاستراتيجية الأمنية السيبرانية للولايات المتحدة وإيران ) ،أما المطلب ألثاني ( الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران) ، اما المبحث الثالث بعنوان ( رؤية مستقبلية حول الهجمات السيبرانية) وتم تقسيمة الى ثلاث مطالب : المطلب الأول ( تصاعد الهجمات السيبرانية )، والمطلب ألثاني ( تراجع الهجمات السيبراني بفعل التعاون الدولي ) ، والمطلب الثالث ( تقدم وتوقف الهجمات الدولية )

## المبحث الأول :الحرب السيبرانية وأثرها على العلاقات الدولية ( أطار نظري – مفاهيمي)

أصبحت الحرب السيبرانية حقيقة لا يمكن أن يجادل فيها أولئك الذين يعتقدون أن خطر الحرب السيبرانية مبالغاً ، فضلاً عن ذلك قيام العديد من الدول بتطوير إمكانياتها في الفضاء السيبراني وتخصيص جيوش الإلكترونية لهذا الغرض ويدل هذا على حدوث تحول في الحرب وتراجع النمط التقليدي المقتصر على الجيوش في مواجهة بعضها لصالح الحرب السيبرانية.

### المطلب الأول : مفهوم الحرب وانماطها ومكوناتها

#### أولا : تعريف الحرب السيبرانية

السيبرانية في اللغة مصطلح مشتق من الكلمة اليونانية (kybermetes) بمعنى القيادة والسيطرة والتحكم عن بعد، ويتضمن الاشتقاق الحديث لهذه الكلمة (السيبرانية) مجموعة من آليات التعقيب تتيح وظائف التحكم والقيادة في الأنظمة المغلقة، أما التعريف الاصطلاحي للحرب السيبرانية، حيث عرفها الباحث الأمريكي "مايكل ان شميت" الحرب السيبرانية على أنّها " تلك الإجراءات التي تتخذها دولة من أجل الهجوم على نظم وشبكات المعلومات" للعدو بهدف التأثير والاضرار فيها والدفاع عن شبكة المعلومات الخاصة بالدولة المهاجمة) [١] ، وتم تعريفها من قبل وزارة الدفاع الأمريكي بانها : مجال يتميز باستخدام أجهزة الحاسوب والأجهزة الإلكترونية الأخرى لتخزين وتعديل وتبادل البيانات بوساطة الأنظمة الشبكية وبنية تحتية المادية مرتبطة بها ، والحرب السيبرانية عرفها (ديفيد رونفيلود ) في مقالة المنشور بعنوان (الحرب السيبرانية القادمة ) "بأنها تنفيذ العمليات العسكرية والاستعداد لتنفيذها وفقاً للمبادئ المعلوماتية، عن طريق تعطيل شبكة

المعلومات والاتصالات على أوسع نطاق" [٢] ، وتعرف أيضاً بأنها : "الحروب التي تستهدف تعطيل أو تدمير نظم المعلومات ألخاصة بالشبكات والاتصالات في الدولة المستهدفة"، وهي تشن اساساً داخل بيئة المعلومات بحيث تستهدف تعطيل كفاءة السيطرة والقدرة على التحكم في منظومة اجهزة أو شبكات الحاسوب، وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين أو تقليلها أو حتى تدميرها سواء كان ذلك على مستوى البنى التحتية الوطنية للدولة أو على مستوى مصادر قوتها ألعسكرية، وهناك تنوع في الأدوات والوسائل واشكال الهجمات والحروب السيبرانية بما في ذلك أرسال فيروسات والبرامج التخريبية والمدمرة للأنظمة والشبكات الحاسوبية أو اختراق حسابات والوصول الى معلومات سرية ومشفرة من أجل تسريبها أو الاستفادة منها لأغراض عسكرية وامنية عدائية [٣] .

من ناحية أخرى يرتبط مفهوم الحرب السيبرانية بهجمات إلكترونية بقيادة عسكرية تقوم باختراق الأنظمة الإلكترونية العالمية وتقوم بأعمال تضر بالأجهزة التي تستخدم الإنترنت مثل سرقة البيانات الخاصة وغيرها إلى الحد الذي قد يسبب وقوع حروب نووية، ومع انتشار شبكة الإنترنت أصبحت أجهزة المخابرات الدولية لكل دولة تسعى الاستغلال هذه الشبكات في حروبها الدولية بواسطة التغلغل فيها والسيطرة عليها أو تعطيلها أو نفي البيانات أو إتلافها أو التحكم فيها لإخضاع دولة العدو، ويمكن تعريف "مصطلح" حروب الفضاء الإلكتروني على أنه " الإجراءات والخطوات التي تتخذها أي دولة أو منظمة أو مجموعة معينة لاختراق أجهزة الحاسوب أو الشبكات الخاصة بدولة أخرى لغرض السيطرة عليها أو التحكم بها أو إتلافها أو تعطيلها عن العمل من خلال إرسال رسائل مشفرة مكتوبة بلغة رقمية ثنائية مشفرة مكونة من رقمين"، ويجدر القول إلى أن الحروب السيبرانية لا تلغي الحروب التقليدية البرية والبحرية والجوية، فمع نهايات القرن العشرين بدأ استخدام الإنترنت من طرف الأشخاص والدول سواء النامية أو المتقدمة و أصبح الفضاء السيبراني الذي تصنعه المعلومات وتكنولوجيا الاتصالات أداة من أدوات التنمية الاقتصادية والاجتماعية، ودخلت دول العالم في علاقة تأثر و تأثير بالنسبة لهذا الفضاء خصوصا بالنسبة لنقل المعلومات والبيانات وتحولت الحروب من الرغبة في تدمير العدو إلى الرغبة في التحكم فيه والسيطرة على تصرفاته وسلوكه ، وعليه انبثق مفهوم حرب المعلومات أو الحروب الإلكترونية وهي تحمل في مضمونها هذا التوجه الحديث، ولأن الصراع بين الفاعلين في "الفضاء السيبراني" ما هو إلا انعكاس للمصالح ألمادية بين الدول والجماعات، فقد أصبح الفضاء الإلكتروني مجالا مركبا مادي وغير مادي يشمل مجموعة من العناصر وهي أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات ، حوسبة المعلومات، نقل وتخزين البيانات [٤] .

، وقد عرف الرئيس بوش (٢٠٠٣-٢٠٠١) الحرب السيبرانية على النحو التالي: "أفعال تقوم بها

دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى يعرض التسبب في الضرر أو التعطيل" [٥]. ان الحروب الالكترونية باتت احد أوجه الحروب التي تهدد الأمن العالمي، وذلك من خلال قيام احد اطرافها بإيقاع خسائر ويتسبب في شل قدرة الخصم والبنية المعلوماتية له، عن طريق استخدام الأسلحة التكنلوجية والعسكرية كبرامج التجسس ونشر الفيروسات وخلق بيئة دولية جديدة تمثلت في الفضاء الالكتروني، التي باتت تتألف من الارض والبحر والجو الفضاء الحر، واضحى يؤثر بشكل كبير في تفاعلات البيئة العالمية، اخذت أشكالا متعددة وانتشرت بين اكبر عدد من الفاعلين على المستويين المحلي والعالمي، مما جعلها مجالا للحروب بين الدول من جهة والفاعلين غير الدوليين من جهة ثانية [٦]، ومن هذا المنطلق يتم استخدام القوة الالكترونية من خلال نمطين وكالاتي [٧] :

**النمط الأول** : ممارسة نمط القوة الصلبة – التقليدية عبر الفضاء الالكتروني، اذ يتم استخدامه في اعمال تدميرية وتخريبية من خلال أتلاف كابلات الاتصال والاقمار الصناعية بين الوحدات والمؤسسات العسكرية، أو في سرقة المعلومات والبيانات وتدمير الانظمة المعلوماتية بما يهدد أمن الدولة والافراد مثل ما تعرضت له استونيا من هجمات الكترونية عام ٢٠٠٧ ، والتي كانت بداية لظهور التهديدات الالكترونية

**النمط الثاني:** استخدام نمط القوة الناعمة عبر الفضاء الالكتروني وذلك من خلال دعم دوره في التأثير في الرأي العام وفي العمليات النفسية وتكوين التحالفات الدولية وعمل اجهزة التجسس.

**ثانياً :انماط الحرب السيبرانية :** ووفقاً للأنماط السابقة المتعلقة باستخدام ألقوه الإلكترونية يمكن طرح عده أنماط للحرب السيبرانية من حيث مدى وشده الصراع ومن أبرز هذه الأنماط هي :

**النمط الأول – الحرب السيبرانية (منخفضة الشدة)** : حيث يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويعبر هذا ألنمط عن صراع مستمر بين الفاعلين المتنازعين، وقد يكون ذا طبيعة متواصلة، ودائمة ألنشاط العدائي أو غير السلمي، بخلاف أنه عميق الجذور ومتداخل، وله جوانب متعددة ثقافية، أو اقتصادية، أو اجتماعية، وتأخذ شكل التجسس والاختراع والقرصنة وسرقة المعلومات بواسطة جماعات مثل (أنونيموس) وتستخدم القوة الناعمة في مثل هكذا حروب ، وإن كانت لا تصل إلى استخدام القوة المسلحة بشكلها ألتقليدي، أو شن حروب إلكترونية واسعة النطاق ([٨]) .

**ألنمط ألثاني – الحرب السيبرانية (متوسطة الشدة):** في هذه الحالة، تدور الحرب السيبرانية من خلال اختراق المواقع الإلكترونية وتخريبها، وشن هجمات معلوماتية وتجسسية ضد الخصوم، يتزامن هذا النوع من الصراع في الفضاء الإلكتروني مع حرب تقليدية قائمة على الأرض، مما يعكس حدة المواجهة بين الأطراف، أو قد يكون تمهيدًا لعمل عسكري، مثل الحرب بين لبنان وإسرائيل في عام ٢٠٠٨ [٩].

**ألنمط الثالث – الحرب السيرانيه (عالية الشدة)** : تبرز هذه الحروب بتميزها في الاعتماد الكبير على التكنولوجيا لإدارة الصراعات، حيث يتم استخدام الأسلحة الإلكترونية لاستهداف منشآت العدو، فضلاً عن توظيف الروبوتات والطائرات بدون طيار، تزداد أهمية الامكانيات والقدرات في الدفاع والهجوم الإلكتروني والسيطرة على القوة الإلكترونية لتكون أساسية في هذه الصراعات المتطور، وتجري الاستعدادات للحرب باستخدام الفضاء الإلكتروني، حيث تجري الدول تدريبات لتوجيه الضربات الأولى ضد أجهزة كمبيوتر العدو واختراق العمليات العسكرية ذات التقنية العالية [١٠].

**ثالثاً: مكونات الحرب السيبرانية :**

لكي يكتمل مفهوم الحرب السيبرانية لابد من التعرف على مكونات هذه الحرب [١١] :

١. **الفضاء السيبراني (Cyber Space)**:عرفت وزارة الدفاع الأمريكية معلومات النشر المشترك (DoD)في (١٣) فبراير (٢٠٠٦) الفضاء السيبراني على أنه (البيئة النظرية التي يتم فيها توصيل المعلومات الرقمية عبر شبكات الكمبيوتر)، وقدمت الاستراتيجية العسكرية الوطنية لعمليات الفضاء السيبراني تعريفاً على أنّه (المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لتخزين البيانات وتعديلها وتبادلها عبر الأنظمة المتصلة بالشبكات والبنى التحتية المادية المرتبطة بها).

٢. **القوة السيبرانية (Cyber power)** :هي ( القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير
الاستراتيجي على الأحداث في البيئات العملياتية الأخرى وعبر أدوات القوة المختلفة). بعبارة أخرى هي
(مجموعة من الموارد التي تتعلق بالتحكم والاتصال بالمعلومات الإلكترونية والمعلومات المستندة إلى
الكومبيوتر والبنية التحتية والشبكات والبرمجيات والمهارات البشرية).

٣. **ألاستراتيجية السيبرانية (Cyber Strategy)**:هي عملية تطوير وتوظيف القدرات أللازمة للعمل في الفضاء السيبراني وتكون متكاملة مع المجالات العملياتية الأخرى لتحقيق الأهداف عبر عناصر القوة الوطنية .

٤.**أمن المعلومات (security information)**: إن المعلومات هي الهدف والسلاح في الحرب السيبرانية التي أخذت مفهوم أمن المعلومات إلى بعد جديد إنها معركة لخاص في مجال افتراضي من الفضاء المعلوماتي مما يجعلها مميزة عن المجالات المادية للأرض والبحر والجو والقضاء أحد أوائل الكتاب البارزين في هذا الموضوع هو إدوارد والتز المدير السابق البرامج فهم المعلومات في معهد أبحاث البيئة في ميشيغان في كتابه الرائد الذي نشر عام ١٩٩٨ ذكر أن حرب المعلومات

تغطي ثلاثة جوانب أساسية للصراع على المستوى الوطني هي (هيمنة المعلومات وحماية المعلومات والهجوم على المعلومات) [١٢] .

## المطلب ألثاني : خصائص الحرب السيبرانية ومراحلها

**أولاً : خصائص الحرب السيبرانية :** الحرب السيبرانية هي استخدام الأسلحة الإلكترونية لتدمير أو شل مكونات الاتصالات وأنظمة الطاقة التي يعتمد عليها الفضاء الإلكتروني. وتتضمن بعض خصائص مجال الحرب الجديد ما يلي[١٣] :

١. القدرة على العمل بسرعة الضوء تقريبا، دون قيود جغرافية تقليدية. تتيح هذه الميزة للمهاجمين فرصة تنفيذ هجمات بعيدة المدى في أجزاء من الثانية دون الحاجة إلى مواجهة العدو في ساحة مادية. في الوقت نفسه، يعتمد الفضاء الإلكتروني على المجال المادي والبنى التحتية للشبكة المنتشرة في الفضاء المادي على الجانب الدفاعي، تتطلب إمكانية الهجوم السريع أساسا من أنظمة دفاعية ديناميكية تتفاعل تلقائيا مع الهجمات في الوقت الفعلي وبصرف النظر عن الحسابات البشرية.

٢. القدرة على العمل في الخفاء، تشير الهجمات السيبرانية التي وقعت بالفعل والمعلومات حول استراتيجيات العمل في الفضاء الإلكتروني إلى أن المهاجم لديه القدرة على العمل في الفضاء الإلكتروني بشكل مجهول دون ترك توقيع علامات تعريف والاختباء وراء آخرين مثل القراصنة الخاصين أو العناصر الإجرامية أو الوكالات والدول الأجنبية.

٣. يمكن استخدام الأسلحة السيبرانية أيضًا كأسلحة غير قاتلة لغد القدرة على إحداث أضرار جسيمة في أداء الدولة دون تدمير بنيتها التحتية المادية أو قتل الناس، ميزة للأسلحة السيبرانية مقارنة بالهجمات الحركية الاستراتيجية (القوة النارية)، في الوقت نفسه، يمكن للهجمات السيبرانية أيضا أن تسبب قدرا كبيرا من الدمار وخسائر في الأرواح البشرية من خلال إتلاف الأنظمة الموجودة في المجالات المادية ولكنها متصلة بالقضاء الإلكتروني.

٤. القدرة على إصابة أهداف استراتيجية يصعب استهدافها في الهجمات التقليدية، مثل قواعد بينات الدولة، لا تنحصر الحرب السيبرانية في استهداف المواقع العسكرية إنما تستهدف أيضاً البنى التحتية المهمة والحساسة في دولة الخصم مثل شبكات الكهرباء والنقل والطاقة وكذلك الانظمة المالية والمنشأة المائية والنفطية والصناعية ،عن طريق استخدام فايروس قادر على أحداث أضرار مادية كبيرة[١٤] .

٥. يتصل بذلك إحدى أهم خصائص حرب الفضاء الإلكتروني، وهي فشل إمكانية القيام بتطبيق

فكرة ومبدأ (الردع) في حروب الفضاء السيبراني ، والتي عادة ما تستخدم من قبل دولة ضد دولة أخرى في إطار استراتيجية الحروب التقليدية أو النووية، أما في الحروب الإلكترونية فهذا الجانب يكون صعب تحقيقه [١٥].

**ثانياً : مراحل الحرب السيبرانية :**

إن فهم تطور الهجوم السيبراني يشكل أساسًا سليماً للتعرف على التهديدات قبل حدوثها ومتى تحدث،

تظل المراحل ألمتسلسلة للهجوم الإلكتروني أساسية لفهم كيفية وصول المتسللين إلى البنية التحتية الحيوية واستغلالها، والمراحل هي [١٦] :

**المرحلة الأولى:** استطلاع هدف الاختراق: في مرحلة الاستطلاع، يحدد المتسللون هدفًا ضعيفًا ويستكشفون كيفية استغلاله، يحتاج المهاجمون إلى نقطة دخول واحدة فقط للبدء، تعد رسائل التصيد المستهدفة شائعة كطريقة فعالة لتوزيع البرامج الضارة في هذه المرحلة، إن الهدف الأساسي من هذه العملية هو التعرف على الهدف وفي هذه المرحلة، يسأل المتسللون أنفسهم عن الأشخاص المهمين في الشركة، ومن يتعاملون معهم، وما هي البيانات العامة المتاحة عن المنظمة المستهدفة.

**ألمرحلة ألثانية** : تسليح المعلومات : في مرحلة التسليح، يستخدم المخترق المعلومات التي تم جمعها مسبقًا لإنشاء طرق للدخول إلى شبكة الهدف، قد يتضمن هذا إنشاء رسائل بريد إلكتروني احتيالية مقنعة تبدو مثل رسائل البريد الإلكتروني التي من المحتمل أن يتلقاها الهدف من بائع معروف أو جهة اتصال تجارية أخرى.

**المرحلة الثالثة:** "تنفيذ" الهجوم يبدأ الهجوم في مرحلة التسليم حيث يتم إرسال رسائل البريد الإلكتروني الاحتيالية، ويتم نشر صفحات الويب الخاصة بـ "البرك المائية" على الإنترنت، وينتظر المهاجم وصول جميع البيانات التي يحتاجها.

**المرحلة الرابعة:** استغلال الاختراق الأمني: في مرحلة الاستغلال، يبدأ المخترق في جني ثمار التحضير وتنفيذ الهجوم بمجرد وصول أسماء المستخدمين وكلمات المرور، يحاول المهاجم استخدامها عبر أنظمة البريد الإلكتروني المستندة إلى الويب أو اتصالات الشبكة الخاصة الافتراضية (VPN)بشبكة الشركة، وإذا تم إرسال مرفقات مصابة بالبرامج الضارة، فإن المهاجم يتمكن من الوصول عن بُعد إلى أجهزة الكمبيوتر المصابة.

**المرحلة الخامسة** : التعطيل والغزو الإلكتروني : قد تتضمن المرحلة النهائية سرقة بيانات حساسة، أو تعطيل العمليات، أو المطالبة بدفع فدية، أو استغلال الأنظمة المتصلة وغزو أنظمة البيانات، لا تتشابه أهداف جميع المتسللين، ولا يندفعون بدوافع مالية حصرية، ولكن هذا النوع من الجرائم الإلكترونية هو الأكثر شيوعًا[١٧] .

**المرحلة السادسة: ممارسة القيادة والسيطرة** : أصبح لديهم الآن إمكانية الوصول غير المقيد إلى الشبكة بأكملها وحسابات المسؤول، وكل الأدوات المطلوبة موجودة في مكانها لمرحلة القيادة والتحكم، يمكن للمهاجم أن ينظر إلى أي شيء، وانتحال شخصية أي مستخدم على الشبكة، وحتى إرسال رسائل بريد إلكتروني من الرئيس التنفيذي إلى جميع الموظفين، والآن بعد أن أصبح المخترق تحت السيطرة، فإنه يستطيع منع مستخدمي تكنولوجيا المعلومات في الشركة من الوصول إلى شبكة المنظمة بأكملها إذا أرادوا ذلك، وربما يطلبون فدية لاستعادة الوصول[١٨] .

**المرحلة السابعة: تحقيق أهداف الهاكر** : تبدأ الآن مرحلة العمل على الأهداف وقد يتضمن ذلك سرقة معلومات عن الموظفين والعملاء وتصميمات المنتجات وما إلى ذلك، أو قد يبدأ المهاجم في تعطيل عمليات المؤسسة المستهدفة، لا يسعى كل المتسللين إلى الحصول على بيانات يمكن تحقيق أرباح منها أو رسائل إلكترونية تدينهم وينشرونها، بل إن بعضهم يريد ببساطة إحداث الفوضى أو إلحاق الأذى بالمؤسسة فإذا تلقت شركة طلبات عبر الإنترنت، فقد يوقف المتسلل نظام الطلبات أو يحذف الطلبات، على سبيل المثال، بل وقد ينشئ طلبات ويرسلها إلى عملاء الشركة إذا تمكن أحد المتسللين من الوصول إلى نظام التحكم الصناعي، فيمكنه إيقاف تشغيل المعدات، وإدخال نقاط ضبط جديدة، وتعطيل أجهزة الإنذار[١٩] .

لقد أدى التحول التكنولوجي وتكامل القدرات إلى زيادة سرعة نقل المعلومات وسهولة الوصول إلى كميات هائلة من البيانات بشكل كبير عبر مجموعة واسعة من الأنشطة والعمليات، تم تقليص الوقت المطلوب من الأفراد للوصول إلى المعلومات ذات الصلة بقرار أو إجراء أو جمعها بأوامر من حيث الحجم وهذا يجعل حرب المعلومات أكثر احتمالا، لأن التوافر المتزايد والقدرة على تحمل تكاليف المعلومات وتكنولوجيا المعلومات وأسلحة عصر المعلومات يزيد من إمكانية خلق أعداء هائلين من خصوم عاجزين وهذا واضح في الطبيعة الشاملة للترابط بين الأنظمة العسكرية والمدنية، واعتماد الجيش على البنية التحتية المدنية أنظمة الأمن القومي والسلامة العامة الحيوية متصلة، بما في ذلك مراقبة الحركة الجوية، وخطوط أنابيب .

النفط والغاز، وأنظمة توليد ونقل الكهرباء وأنظمة المستشفيات، وخدمات الطوارئ، وأنظمة النقل، وأقمار نظام تحديد المواقع العالمي، والأنظمة المالية، والأنظمة الزراعية، والبنية التحتية الحيوية الأخرى[٢٠].

**ثالثاً : وسائل الحرب السيبرانية** : إن أي مناقشة للوسائل السيبرانية المستخدمة في الحرب ينبغي أن تنطلق من المفهوم الأكثر عمومية لأسلوب الحرب، وتتكون وسائل الحرب من كل الأسلحة ومنصات الأسلحة والمعدات المرتبطة بها والتي تستخدم بشكل مباشر لإيصال القوة أثناء الأعمال

العدائية، ومن هذه الوسائل[٢١]:

-**الأسلحة السيبرانية** : يوجد تعريف واحد للأسلحة السيبرانية ففي عام ٢٠١١ أصدرت الولايات المتحدة تعريفا جديدًا للأسلحة السيبرانية، وقد عرف قاموس المصطلحات العسكرية والمصطلحات المرتبطة بها التابع لوزارة الدفاع الأميركية الأسلحة السيبرانية، بأنها سلاح مصمم يُستخدم في المقام الأول بهدف شل قدرة الأفراد أو المعدات مع تقليل الوفيات والإصابات الدائمة للأفراد والأضرار غير المرغوب فيها للممتلكات والبيئة" ويصف دليل تالين الأسلحة السيبرانية من خلال تأثيراتها، وليس من خلال كيفية بنائها أو وسائل تشغيلها، ويُعرف على النحو التالي: الأسلحة السيبرانية هي وسائل حرب سيبرانية تستخدم أو تصمم أو يُقصد استخدامها لإحداث إصابة أو وفاة للأشخاص أو إتلاف أو تدمير الأشياء، أي أنها تؤدي إلى العواقب المطلوبة لتصنيف العملية السيبرانية على أنها هجوم، السلاح السيبراني هو أداة لتكنولوجيا المعلومات تعتمد على البرمجيات ويمكنها أن تؤثر بشكل ضار أو مدمر أو محطم على نظام الشبكة الذي يتم توجيهها ضده[٢٢] . السلاح السيبراني هو مزيج من عدة عوامل هي[٢٣] :

– نقاط الضعف: نقاط الضعف في خصائص متأصلة في الأنظمة الأجهزة أو البرامج التي يسعى المرء إلى اختراقها، نقاط الضعف أو الخلل في الأجهزة أو البرامج التي يمكن للمهاجم الاستفادة منها.

– الاستغلال: تتم كتابة البرامج للاستفادة من ثغرة أمنية والتسبب في تأثير معين، مثل الوصول إلى نظام أو إيقاف تشغيل قطعة من الأجهزة.

– الانتشار: في هذه الطريقة يتم تسليم الشقرة إلى الهدف مثل البريد الإلكتروني الاحتيالي .

إن الأسلحة السيبرانية مكتوبة في أكواد الكمبيوتر. ويمكنها التسلل إلى شبكات كاملة أو إصابة أجهزة كمبيوتر فردية، وهي تعتمد على نقاط ضعف في البرامج، وضعف النظافة السيبرانية، والأشخاص الذين يفتحون عن غير قصد المرفقات المصابة بالبرامج الضارة، ويمكنها إرباك العدو، وإيقاف الهجمات العسكرية قبل وقوعها وإرباك أنظمة الاتصالات، ووفقاً لإريك روزنباخ قيصر الإنترنت في البنتاغون أثناء إدارة أوباما، فإن النشاط السيبراني الهجومي هو "عمل شاق" يتضمن تحديد منصة في بلد آخر والحصول على إمكانية الوصول إليها.

تكمن خطورة الحرب السيبرانية في كون العالم اصبح يعتمد اكثر على الفضاء السيبراني لاسيما في البنى التحتية المعلوماتية العسكرية والحكومية والمؤسسات ألرسمية والاعتماد على شبكات الكومبيوتر والأنترنيت في البنى التحتية الأساسية للدول مما أدى إلى زيادة الهجمات السيبرانية التي نشهدها اليوم حيث تطورت لتصبح سلاحاً مهماً في الصراعات الدولية وتأتي هذه الهجمات دون مقدمات ثم تعم الفوضى والخراب وتؤدي الى انهيار جميع الخدمات سواء أكانت عسكرية أم صحية

أم حيوية أم مالية وتجارية نتيجة لهذه الهجمات الخطيرة[٢٤] .

وبعد أن كانت القوة السيبرانية مقصورة على الدول، شاركها في ذلك فواعل آخرين مثل الأفراد العاديون الجماعات الإرهابية عبر استخدام أسلحة سيبرانية عبارة عن فيروسات وبرامج بسيطة متطورة ورخيصة التكلفة ولها قدرات تخريبية تقارب تأثير الأسلحة التقليدية، في حال استهدافها البنية التحتية للدول من محطات الطاقة، والسدود، وخطوط ألنقل، بكاملها، والمستشفيات وغيرها من الشبكات الذكية، وبعد أن كانت ألعمليات العسكرية بين جيوش نظاميه يمكن من خلالها تحديد من المنتصر فيها ومن الخاسر بناء على الأراضي التي تم اكتسابها أو الخسائر التي تحققت، أصبحت الحروب سيبرانية داخل بيئة إلكترونية وليست بيئة طبيعية تحكمها قوانين الطبيعية كالأرض أو البحر أو الجو، ولا يستطيع النظام الدولي ان يحكم التفاعلات بينهما، لصعوبة الوصول للفاعل الحقيقي الذي قام بشنّ هذه الحرب أو الهجمات السيبرانية على الطرف الآخر أيضًا، والخسائر فيها يمكن ان تكون مباشرة مثل تدمير البيانات والبنى التحتية والقدرات العسكرية، وقد تكون غير مباشرة تتمثل في تراجع ألتنافس ألاقتصادي للدولة وفقدان الثقة في الاقتصاد القومي للدول وذلك بسبب الهجمات السيبرانية التي تعمل على استهداف المؤسسات المالية والتجارية والصناعية، كل هذه التطورات التكنولوجية لها ألعديد من التداعيات والآثار على بيئة العلاقات الدولية والسياة الدولية بصورة عامة، وعلى الأمن ألوطني للدول بصورة خاصة[٢٥].

## المطلب الثالث / تأثير الحرب السيبرانية على العلاقات الدولية

تعمل الحرب السيبرانية على أعادة تشكل العلاقات الدولية وذلك بسبب دورها المتعاظم والمتسارع في بلورة شكل العلاقات في النظام الدولي مما جعلها أن تكتسب مكانة مهمة في صياغة نمط العلاقات الدولية حيث أدت الهجمات السيبرانية على تراجع مكانة بعض الدول وخاصة في مرتبة القوة حيث كشفت هذه الحرب على الإمكانيات والقدرات التكنولوجية و الالكترونية التي تمتلكها بعض الدول على حساب الدول الاخرى وسيتم من خلال هذا المبحث بيان دور الحرب السيبرانية في تشكل العلاقات الدولية .

**أولاً : التأثير على شكل القواعد التي تحكم النظام الدولي** : ادى اهتمام الدول المتزايد في الفضاء الالكتروني وما خلفة هذا الاهتمام من هجمات الكترونية وسيبرانية أدت الى تزايد المخاطر والتداعيات على العلاقات الدولية يمكن طرح أبرزها :

١- عدم مقدرة الدول في النظام الدولي في اللجوء الى تطبيق قواعد القانون الدولي على الاطراف والدول التي تستخدم الفضاء السيبراني لشن الهجمات السيبرانية وذلك بسبب عدم مقدرتها في تحديد مصدر الهجمات وحتى عندما يتم تحديد مصدر الهجوم فتجد المؤسسات الدولية صعوبة في تطبيق

القواعد القانونية باعتبار أن آثار الهجوم السيبراني لا تصل أثارة الى درجة الهجوم العسكري التقليدي وامكانية خضوع تلك الحروب والهجمات وأطرافها الى الاختصاص الجنائي الوطني الداخلي للدول حيث أدى ذلك الى التأثير على قواعد القانون الدولي وتتطلب وضع قواعد جديدة تساير التطور الحاصل في مجال الفضاء الالكتروني [٢٦].

٢- أصبح الفضاء الالكتروني أحد العناصر الرئيسية التي تؤثر على العلاقات الدولية وشكلها في النظام الدولي، وذلك بما يمتلكه من ادوات تكنولوجية تلعب دوراً مهماً في عملية التعبئة الأمنية الدولية ، كما تعد الحروب السيبرانية أحد أوجه الصراع الدولي اذ يستطيع أحداً طراق الصراع ان يوقع خسائر عسكرية واقتصادية فادحة من خلال قطع أنظمه الاتصال بين الوحدات العسكرية أو من خلال التلاعب بالبيانات الاقتصادية والمالية، كل هذه العوامل ادت الى أن تلجأ الدول الى شن الحروب السيبرانية وتستخدمها كأداة بديلة عن الحروب التقليدية والنووية في تحقيق أهدافها حيث، عملت على دفع شبح الحرب النووية التي كانت تشكل رعب نووي مخيف يسيطر على الدول في النظام الدولي، وعملت على تطوير وسائل أخرى مثل العمل على زيادة مستوى سباق التسلح الالكتروني و توسيع مجال الفضاء الالكتروني من خلال أنشاء مؤسسات رسمية وشبة رسمية داخلية وخارجية وبشكل تعاوني بين الدول [٢٧] .

٣- أن الصراع السيبراني والحروب السيبرانية تمثل أداة فعاله في التأثير على الوحدات الرسمية والغير رسمية في السياسة الدولية حيث أدى التطور التكنولوجي والثورة في ميدان الفضاء الإلكتروني الى إلى توجيه الدول والفواعل الاخرى في النظام الدولي الى زيادة الاهتمام في مجال الفضاء الالكتروني وهذا الاهتمام ادى الى السماح لأطراف من غير الدول في امتلاك القوة السيبرانية وتوظيفها لخدمة مصالحها وأهدافها من خلال شن هجمات على دولة رئيسية في النظام الدولي مما أنتج ذلك إلى عدم مقدرة الدولة التي تم شن هجوم عليها من تحديد مصدر هذا الهجوم وبالتالي ادى ذلك الى زيادة حدة التوتر في العلاقات بين الدول على المستوى الدولي [٢٨] .

**ثانياً : التأثير على الأمن الدولي والأمن ألقومي للدول : سيتم تفصيل هذا التغيير من حلال عده نقاط وكالآتي** [٢٩] :

١- عملت الحرب السيبرانية على انتشار القوة السيبرانية من خلالها الى مراكز وأطراف غير رئيسية في السياسة الدولية مثل الجماعات الارهابية والمنظمات الغير حكومية مما ادى ذلك الانتشار إلى ازدياد التوتر في العلاقات بين الدول الرئيسة في النظام الدولي وتلك الاطراف .

٢- تشكيل هيئات ومؤسسات سيبرانية رسمية في أطار التعاون الدولي بين الدول وهذه الهيئات تعمل على رفع مستوى الوعي الأمني السيبراني لدى أطراف السياسة الدولية واعداد استراتيجية وطنية ودولية للأمن السيبراني ووضع السياسات والمعايير الوطنية للتشفير وهذا النوع من التعاون

يمكن ملاحظة بين الولايات المتحدة وإسرائيل في أطار التعاون الاستراتيجي المشترك.

٣- من التأثيرات الايجابية سعي الدول الى تطوير قدراتها في ميدان القوة الالكترونية حيث ادى ذلك إلى بلورة استراتيجية أمنية سيبرانية للدول على المستوى الداخلي ورفع قدراتها الدفاعية السيبرانية والعمل على زيادة تشفير معلوماتها وعدم قدرة الاطراف الأخرى في السياسة الدولية التجسس على برامجها وخططها وما تملكه من معلومات على مستوى مؤسسات الدولة الكاملة .

٤- مؤثرة في السياسة والاقتصاد على الصعيد الدولي، وذلك بسبب انتقال الصراع بين الدول العظمى الى ميدان الفضاء الالكتروني الشامل والوسط الرقمي وخاصة مع تزايد ارتباطات الدول في ميدان الفضاء السيبراني وفي الوقت ذات تصاعد أطراف أخرى من غير الدول مثل الشركات المتعددة الجنسيات في ميدان التكنولوجيا وامتلاك القوة الالكترونية.

٥- تعمل الحرب السيبرانية على التأثير النفسي حيث تسبب حالة من الهلع والخوف لدى الدول من خلال اختراق المواقع الالكترونية وإعلان حالة الطوارئ مما يثير القلق لدن مواطنين تلك الدول.

**ثالثاً : التأثير من خلال امتلاك القوة السيبرانية** : فرض الواقع الدولي بعد انتهاء الحرب الباردة وتفكك الاتحاد السوفيتي الى ضرورة مراجعة مفهوم القوة في العلاقات الدولية، حيث تراجع النمط التقليدي للقوة من خلال استخدام الادوات العسكرية واستخدام مصادر القوة الصلبة ووسائلها لما تنطوي عليها من تكلفة مادية وبشرية عالية، بالإضافة الى القدرة التدميرية للأسلحة التقليدية، وبرزت ادوات أخرى للقوة مثل القوة السيبرانية او الالكترونية أدت هذه القوة الى تغييرات في الساحة الدولية حيث أن مفهوم العلاقات الدولية هو مفهوم تطوري يتأثر بالتغيرات البيئية ومن أمثلتها ظهور الفضاء السيبراني كساحة جديدة للمنافسة على الصعيد الدولي ، وهنا تأتي أهمية القوة السيبرانية في التأثير على العلاقات الدولية، حيث أضحت مجال للتنافس بين الدول وغير الدول من الفاعلين واذ برزت كيانات أخرى زاحمت الدول القومية للحصول على مقدرات القوة السيبرانية مما جعل عدم قدرة الدول من السيطرة الكاملة على القدرات السيبرانية، واذ أضحى العلم والتطور التكنولوجي المحرك الاساسي للتحكم في العلاقات بين الدول [٣٠].

**وتعرف القوة السيبرانية بأنها** " قدرة الدولة القومية على السيطرة والتأثير داخل وعبر الفضاء السيبراني لدعم عناصر ومقومات القوة الأخرى " ويعتمد امتلاك القوة السيبرانية لاي دوله من خلال قدرتها على تطوير مؤسسات سيبرانية وتطوير الموارد الخاصة في مجال الفضاء السيبراني[٣١] ، قد حدد جوزيف ناي ثلاث انواع من الفاعلين يمتلكون القوة السيبرانية هم[٣٢] :

١- الدول :: تعد الدول اللاعب الرئيسي في حقل العلاقات الدولية ، وتلجأ الدول الى شن الحروب السيبرانية بدلا من الحروب العسكرية التقليدية المباشرة، فالدول التي تمتلك بنى تحتية سيبرانية وإمكانيات سيبرانية قوية قادرة على أن تشن هجمات سيبرانية تسبب خسائر فادحة للخصم.

٢- الشركات المتعددة الجنسيات : تمثل هذه الشركات القدرة على اختراق المعلومات للأفراد

والجماعات والمؤسسات كما هو الحال على المستوى ألداخلي للدولة وخاصة المستوى الاجتماعي من خلال مواقع التواصل الاجتماعي، وتعمل على سرقة البيانات والمعلومات الى الجهات ألمرتبطة بها وتابعة لها سواء كانت هذه الجهات حكومية رسمية او غير حكومية .

٣- الافراد : للأفراد قدرة على تهديد أمن الدولة من خلال شن هجمات سيبرانية حيث يمتلك الأفراد القدرة التي تؤهلهم للقيام بهذا التهديد مثل " المال – الاعلام – الأفكار – المعلومات " وتوظيف هذه القدرات ضمن الأهداف الخاصة بهدف التأثير في سلوك وحدات النظام الدولي والفواعل على المستوى الدولي.

بعد أحداث ١١ سبتمبر التي شهدتها الولايات المتحدة برزت بعدها تحولات عالميه للقوة وكان أبرز تلك التحولات هي امتلاك الجماعات الإرهابية للقدرات والقوة الإلكترونية وحصلت عليها من خلال العوامل التي عملت على انتشار القوة في النظام الدولي بعد ان كانت مقتصره على الدول ألقومية من هذه الجماعات هي[٣٣] :

- الجماعات الارهابية : تعد من ابرز الفواعل في النظام الدولي خاصة بعد احداث برجي التجارة العالمي في الولايات المتحدة والتي عرفت بما يسمى أحداث (١١ سبتمبر )، حيث عملت هذه الجماعات على امتلاك القوة السيبرانية لشن هجمات على الدول حيث أن تحولات القوة مكنت هذه الجماعات من الحصول على مصادر القوة الالكترونية والسيبرانية.

أصبحت الحروب السيبرانية لها تأثير كبير على النظام الدولي وذلك لما تملكه من قوة تدميرية تسبب ضرر واسع على مستوى المؤسسات الداخلية للدول أو الخارجية التي تحكم العلاقات الدولية في النظام الدولي حيث أن من يمتلك القدرة لشن الحروب السيبرانية من خلال الهجمات السيبرانية يستطيع أن يأثر في سلوك الفاعلين في السياسة الدولية، ويعمل على أعادة وترتيب شكل العلاقات بين الفواعل والوحدات من خلال قيام اتفاقات جديدة قائمة على مفهوم القوة السيبرانية والعمل على زيادة سباق التسلح على المستوى التكنولوجي وفي ميدات الفضاء الالكتروني وكل هذه العوامل عملت على تغيير مفهوم العلاقات الدولية التقليدي والتحول الى ميدان جديد قائم على العلاقات الأمنية السيبرانية. من خلال ما تقدم وبيان ألطريقة التي تؤثر بها الحرب السيبرانية على الوحدات الدولية في بيئة السياسة الدولية سواء على العلاقات بين هذه الدول او على المستوى ألداخلي للدولة نفسها ، سنتناول نماذج تطبيقه للدول أثرت من خلالها الحرب السيبرانية عليها وبالتالي أنعكس هذا التأثير على ألمحيط ألخارجي والمسرح التي تتفاعل فيه هذه الدول ، من هذه الدول هي الولايات المتحدة كما سيتم توضيح التفاصيل في ألمطالب القادمة.

## المبحث الثاني / الحروب السيبرانية بين (الولايات المتحدة وإيران )

مع ظهور وتطور العولمة تصاعدت حدة الخلافات والصراع بين الدول ، ظهرت وترافقت معها أشكال جديده من الصراع وأحداث مختلفة وبوسائل غير تقليديه ، من بين هذه الاشكال هي الحروب السيبرانية، وأخذت هذه الحروب تأخذ صدى وبعد دولي، ففي ألوقت ألحالي تشكل هذه الحروب تهديد مباشر ومستمر على السلم والأمن الدوليين ، لذلك فأن بيئة السياسة الدولية تحتاج الى استراتيجيات ورسم سياسات أمنيه قوية وصلبة وجدية تتخذها الدول لمواجه مثل هذه الأشكال من الحروب ، سواء كانت هذه الخطوات الأمنية دفاعية أو هجومية ، وهذه الحرب أدت الى تغير جذري في العلاقات بين الدول وخاصة في العلاقة بين الولايات المتحدة وإيران كمثال على هذا ألتغير، وتلجأ كلا الدولتين الى شن هجمات سيبرانية ضد بعضها ألبعض من أجل تطبيق استراتيجيهما الأمنية واستخدام الأسلحة السيبرانية لتكون أسلحة دفاعية لضمان وبقاء أمنها ألقومي والوطني .

وقد شنت الولايات المتحدة ألعديد من الهجمات السيبرانية ضد أيران بحجه امتلاكها لأسلحة وقدرات سيبرانية والتي من الممكن أن تكون خطر على الأمن ألقومي للولايات المتحدة الأمريكية ، وفي السياق نفسة هاجمت الولايات المتحدة المنشآت والبنى ألتحتية ألنووية بهدف تعطيل البرنامج ألنووي الإيراني لكون هذا البرنامج يشكل تهديد مباشر عليها .

لذلك سنتناول في هذا المبحث الحروب السيبرانية بين الولايات المتحدة وإيران من خلال مطلبين، نتناول في المطلب الأول الاستراتيجية الأمنية السيبرانية للولايات المتحدة الأمريكية وإيران ، وفي المطلب ألثاني الحرب السيبرانية بين الولايات المتحدة وإيران .

### المطلب الأول : ألاستراتيجية الأمنية السيبرانية للولايات المتحدة وإيران

**أولاً : القدرات السيبرانية للولايات المتحدة الأمريكية :** بدأت الولايات المتحدة في تطوير قدراتها السيبرانية ألهجومية والدفاعية وبشكل خاص بعد احداث ١١ أيلول من خلال أنشاء مؤسسات أمنية سيبرانية منها :

١- مركز القيادة ألمشتركة السيبرانية : بعد أحداث ١١ أيلول ، عملت الولايات المتحدة على زياده الإنفاق لتطوير القدرات السيبرانية ، أذ أنشأت في عام ٢٠٠٩ مركز القيادة ألمقاتلة المركزية في مجال الفضاء السيبراني ، يتألف هذا المركز من الإمكانيات ألاستخباراتية وتكنولوجيا المعلومات ألمتقدمة ، وتتولى مهام السيطرة والتوجيه والدفاع عن نظم المعلومات ألتابعة لوزارة الدفاع ، ويدعم القوات السيبرانية ألمشتركة في مجال الفضاء السيبراني [٣٤] .

٢- قيادة الإنترنت ( سايبر كوم cybercom) : وهي القيادة التي أنشأها ألرئيس باراك أوباما في عام ٢٠١٠ وعين مدير الجنرال ( كيث ألكساندر keith alexander) قائداً عليها، تعمل هذه القيادة على حماية الشبكات الأمنية ألعسكرية الأمريكية وتضم هذه القيادة مجموعه من القراصنة

وألف فرد من نخبة الجواسيس الإلكترونيين ألمحترفين[٣٥] .

٣- وكاله الأمن ألقومي السيبرانية (CNSA) : وهي وكالة مخابراتية تابعة لحكومة الولايات المتحدة الأمريكية ، تعمل على جمع وتحليل البيانات والمعلومات لغرض التجسس ولأغراض المخابرات ، لديها أمكانية سيبرانية عالية وتم تفويضها لقياده جهود الأمن السيبراني[٣٦].

٤- وزارة الأمن ألداخلي (DHS): تعتبر الأمن السيبراني واحدة من أهم المجالات الأمنية في الوزارة ، اذ تعمل على حماية البنى ألتحتية الأمريكية من الهجمات السيبرانية وتبذل جهود في تأمين الهيئات ألحكومية ألمدنية ، وذلك بالتنسيق مع وكاله الاستخبارات الأمريكية (CIA) [٣٧] .

وأثناء فتره ألرئيس باراك أوباما ، تزايد الاعتماد على شبكة المعلومات لذلك عمل على زياده الإنفاق المالي ومضاعفة الميزانية المخصصة لهذا الجانب من مئتين وسبعة مليار دولاً الى سبع مليارات دولار، مما ادى ذلك ألي زياده في عدد ألعاملين في ذلك المجال وبالأخص في الجيش الأمريكي من تسعة آلاف الى أربعة آلاف شخص ، وعمل على وضع سياسية أمنية سيبرانية من خلال أنشاء فريق عمل لوضع الإستراتيجيات السيبرانية الخاصة في هذا المجال ، وأعتبر بأن قضية الأمن السيبراني تمثل أهمية كبيره للأمن ألوطني للولايات المتحدة الأمريكية ، وعمل على تطوير أنظمة محاكاة وافتراضية من خلال وضع نماذج افتراضية في أطار ( معارك الحرب السيبرانية ) تحاكي الهجمات السيبرانية التي تشن من الخارج ومن القراصنة في ألداخل ، جاءت هذه الاستراتيجية لتطوير القدرات الدفاعية للولايات المتحدة الأمريكية، أما في عهد الرئيس دونالد ترامب ، حيث ازدادت أهمية تطوير القدرات السيبرانية وذلك بفعل تزايد وتيره الهجمات السيبرانية والجرائم ألمتعلقة بها ، اذ وضعت أداره ترامب في عام ٢٠١٧ استراتيجية أمنية سيبرانية محكمة لمواجهة التهديدات السيبرانية ، كما ذكر ترامب أن قرار أنشاء قياده مركزيه سيبرانية موحدة ظهر مدى اهتمام الإدارة ألحالية في عزمها ألمتزايد على مواجهة الهجمات السيبرانية . مجال الفضاء السيبراني[٣٨].

**ثانياً : القدرات السيبرانية لإيران :** في عام ٢٠١٠ عندما أنتشر الفيروس السري ( ستاكس نت) في جميع أجهزة المفاعل لتخصيب اليورانيوم النووي في "نطنز" ادركت إيران أنها تلقت درس صعب في مجال الحرب الالكترونية، اذ ادى الفيروس الى أضرار كبيرة في أنظمة التحكم وأجهزة الطرد المركزي سريعة الدوران ، لذلك ادركت إيران أنها بحاجة الى تطوير قدراتها في مجال الفضاء الالكتروني، وكان من الصعب أتخاذ إجراءات آنية وسريعة لمواجهة هذا الخطر لذلك عملت على أتخاذ خطوات سريعة المعالجة هذه المشكلة ، لذا اتجهت إلى إفراد من القطاع الخاص لمعالجة القدر الذي تسبب به هذا الفيروس، لذلك عملت على تطوير مؤسسات حكومية تعمل تحت سيطرة الحرس الثوري الايراني [٣٩] ، ومن هذه المؤسسات هي [٤٠] :

١- **المجلس الاعلى للقضاء السيبراني(Scc):** تم تأسيس هذا المجلس في عام ٢٠١٢ برئاسة

رئيس الجمهورية اذ يعمل هذا المجلس على تنسيق العمليات الدفاعية والهجومية السيبرانية ، ويعمل على تطوير استراتيجيات الأمن السيبراني من خلال وضع خطط شاملة لحماية الفضاء السيبراني وصد الهجمات السيبرانية.

٢- **كتائب الباسيج السيبراني** : وهي كتائب تابعة للحرس الثوري الايراني وتعمل على دعم النظام الايراني من خلال شبكات التواصل ونظم المعلومات، وتعمل على بث ونشر المنشورات التي تدعم النظام واختراق مواقع التواصل أو المحطات الاخبارية في الدول الاخرى وبث وترويج الافكار التي تدعم نظام الحكم في إيران.

٣- **الجيش السيبراني الإيراني** : يضم الجيش مجموعة من المتخصصين ذوي مهارات وإمكانيات عالية في مجال التكنولوجيا ونظم المعلومات غير معروفة هويتهم ، و اذ يمتلك الحيث السيبراني الايراني قدرات عالية في اختراق المواقع الحكومية للدول الأخرى واختراق وسائل الاعلام المشفرة والسرية لدى الدول الأخرى الأخرى وتعمل على النحس والحصول على المعلومات

٤- **منظمة الحرب الالكترونية والدفاع السيبراني:** هذه المنظمة تابعة للحرس الثوري الايراني تعمل بالتنسيق مع الجيش السيبراني الايراني في الفضاء السيبراني .

٥- **هيليكس كيت ( HELIX KITTEN):** وهي عبارة عن مجموعة من القراصنة، وتكون غير حكومية، تتعاون مع الحكومة الايرانية وخاصة مع وزارة المخابرات الايرانية وبدأت عملها في عام ٢٠١٥ .

أن الاستراتيجية السيبرانية، تتمحور حول هدفين اذ تمثل الاول يمنع الهجمات التي تستهدف البنى التحتية لاسيما المؤسسات الأمنية والعسكرية (الحيوية ) ووضع آلية تشفير تعمل على حماية المؤسسات من الفيروسات مثل فايروس (ستاكسنت) ، وثانياً تعمل على حجب ومنع دخول المعلومات وبالأخص تلك التي تضلا النظام الايراني ويعتبرها خطر يهدد وجودة، أن ايران تضع عدة أهداف أساسية تعمل على تحقيقها في مجال الحرب السيبرانية، وهي : الدفاع عن المؤسسات والبنية التحتية للدولة ، والعمل على شن هجمات الكترونية للحصول على المعلومات وتحليل البيانات والتجسس، والعمل على تعزيز القدرات السيبرانية من خلال وضع عقيدة سيبرانية أمنية لحماية الأمن الوطني الايراني ووضع استراتيجيات أمنية في هذا المجال على المستوى الدفاعي والهجومي، وأنشاء جيوش الكترونية وتعزيز القدرات الاستخباراتية في مجال الشبكات ونظم المعلومات ت ودخلت إيران في عام و ٢٠٠ من قبل شركة " American" security من بين أقوى الدول التي تمتلك قدرات أنترنت في العالم [٤١] .

تطورت استراتيجية إيران السيبرانية على ثلاث مراحل أساسية، كانت المرحلة الأولى من عام ٢٠٠٩ إلى عام ٢٠١١ بمثابة جرس إنذار واستجابة أولية للمظاهرات التي أعقبت انتخابات عام ٢٠٠٩ وهجوم ستوكسنت في العام التالي، وشهدت المرحلة الثانية من عام ٢٠١٢ إلى عام ٢٠١٨

إنشاء المؤسسات السيبرانية المذكورة أعلاه، وبداية التعاون السيبراني مع روسيا والصين والانتقال من العمليات السيبرانية الدفاعية إلى حد كبير إلى العمليات الهجومية في المقام الأول لأغراض الاستخبارات، في المرحلة الثالثة، من عام ٢٠١٩ إلى الوقت الحاضر، لقد عملت إيران على استهداف البنية التحتية والدفاع وغيرها من الأهداف في جميع أنحاء العالم، ووسعت نطاق عملياتها الهجومية، وكان هذا صحيحًا بشكل خاص في مجالات العمليات المعلوماتية وفي العديد من حالات الهجمات المشتركة CNA و CNE و CNI وبرامج الفدية ، ٣٣ وكما سيتضح، فإن الكثير من الأنشطة السيبرانية الإيرانية على مر السنين كانت ذات طبيعة تفاعلية، ردًا على الهجمات التي نسبتها إلى إسرائيل أو الولايات المتحدة، لقد أدى هذا الشعور العميق إلى العزم ليس فقط على ردع إيران والدفاع عنها ضد أعدائها، بل وأيضاً على تطوير قدرات هجومية فعّالة لتعزيز مصالحها وتوسيع نفوذها في الخارج، لقد شكلت الحرب غير المتكافئة منذ فترة طويلة عنصراً حاسماً في استراتيجية الأمن القومي الإيرانية، المصممة للتعويض عن مزايا خصومها الأكثر قوة، وقد اكتسبت الحرب الإلكترونية دوراً مهماً في ذلك، إن الحرب الإلكترونية مناسبة بشكل خاص للثقافة الاستراتيجية الإيرانية، التي تؤكد على الغموض[٤٢] .

## المطلب ألثاني \ الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران

تمثلت الحرب السيبرانية بين الولايات المتحدة إيران أداة فاعلة لدى الطرفين في تدمير أكبر قدر ممكن من البنى ألتحتية والمؤسسات ألعسكرية والمدنية وأنهاك أكبر قدر من المواقع ألحيوية من خلال شن هجمات سيبرانية وبشدة متفاوتة لتحقيق الأهداف ألمهمة وبوسائل تختلف عن وسائل الحروب التقليدية ، أذ أستطاع الطرفين في وضع ألاستراتيجيات السيبرانية ألمهمة في سبيل تحقيق تلك الغايات ، سنتناول الهجمات السيبرانية بين الولايات المتحدة و إيران كالآتي :

**اولاً : الهجمات السيبرانية للولايات المتحدة تجاه إيران :** انطلقت بداية الهجمات السيبرانية، من قبل الولايات المتحدة تجاه إيران في عام ٢٠٠٦ أثناء فترة حكم الرئيس (جورج دبليو بوش ) من خلال استهداف أجهزة التحكيم الالكترونية، للحكومة الايرانية، وبعد مجيء الرئيس الامريكي باراك أوباما في عام ٢٠١٠ عمل على توسيع هذه الحملة لتشمل المفاعل ( النووية) ( الحيوية) ، اذ صرح مسؤولون حكوميون إيرانيون أن أجهزة الطرد المركزي لتخصيب اليورانيوم في محطة (نطنز) و (بوشهر) قد تعرضت لهجوم سيبراني مما ادى الى توقف تلك الاجهزة عن العمل جراء الفيروس المعروف باسم (ستوكينت ) ، مما دفع بالحكومة الايرانية الى فصل ١٦٠ جهاز طرد مركزي عن شبكة التحكم واخراجها عن الخدمة [٤٣] .

وهنالك العديد من الهجمات السيبرانية شنتها الولايات المتحدة تجاه إيران وعلى فترات زمنية متفاوتة سنذكرها كآلاتي[٤٤]:

- **مايو / ٢٠١٢ :** صرح مسؤولون أمريكيون لصحيفة واشنطن بوست أن (اسرائيل) و (الولايات

المتحدة) قد نشرنا فيروس يدعى ( فليم ) لجمع المعلومات والتجسس وسرقه البيانات من نظم الشبكات والمعلومات للحكومة الايرانية

– **سبتمبر ٢٠١٨** : أثناء حكم الرئيس ترامب في فترة الرئاسة الاولى سمحت ادارته في شن هجمات سيبرانية واسعة ضد البنى التحتية الايرانية بشكل واسع .

– إبريل ٢٠١٩ : تعرضت مراكز البيانات الايرانية إلى اختراق سيبراني مما ادى الى ظهور العلم الامريكي على شاشات الكمبيوتر الايرانية، وظهرت رساله تطالب بعدم التدخل في الانتخابات الأمريكية.

– **في عام ٢٠٢٠** : تعرضت إيران الى عدة صعبات سيبرانية وذلك رداً على الهجمات الايرانية في تلك الفترة حيث استهدفت العصبات السيبرانية هيئة الموانئ الايرانية في أكتوبر، وبعد شهر أغلقت الولايات المتحدة و٢٩ موقعاً على مواقع التواصل وشبكة الانترنت تستخدمها إيران للتأثير على سياسة الولايات المتحدة والرأي العام، ومن الهجمات المؤثرة لجأت الولايات المتحدة الى شن هجوم سيبراني على موزع خدمة الانترنت (DDos) أدى إلى انخفاض كفاءة بالإنترنت الى نسبة ٧٥% بعدها اتخذت إيران إجراءات مضادة لهذا الهجوم.

**ثانياً : الهجمات السيبرانية لإيران تجاه الولايات المتحدة الأمريكية :** لجأت إيران إلى تعزيز قدراتها السيبرانية الدفاعية والهجومية بعد الهجمات التي تعرضت لها مفاعلها النووية ومؤسساتها الحيوية وقد طورت من قدراتها السيبرانية لتتمكن من شن الهجمات، وقد انعكست تلك التطورات في سلسلة من الهجمات التي وقعت في عام ٢٠١٣، اذ بدأت بشن الهجمات على المؤسسات المالية والبنوك الرئيسة في الولايات المتحدة الامريكية من خلال فك تشفير نظم الشبكات والمعلومات تلك البنوك مثل (جية بي مورجان ) و ( بنك اوف أمريكا Bank of America) اذ أدت الى تعطيل الخدمة في تلك البنوك، وفي عام ٢٠١٤ نشرت الحكومة الايرانية برمجيات خبيثة ( (wipermalver) ضد الشبكات الموجودة في (لاس فيغاس) ووصلت الخسائر إلى حوالي ١٤ مليار دولار[٤٥].

وفي عام ٢٠١٩ ذكرت شركة مايكروسوفت أن أيران اخترقت شبكة الحسابات المتعلقة بحملة أعادة انتخاب الرئيس الامريكي دونالد ترامب، وفي عام ٢٠٢٠ وتحديداً في الشهر العاشر استهدفت جماعات ايرانية مواقع الانتخابات الامريكية وحصلت على بيانات ومعلومات تسجيل الناخبين وفقاً لمكتب التحقيقات الفيدرالي (FBI)، وفي يوليوان ) قال مكتب المخابرات الوطنية أن أيران سمحت بحملة تأثير سيبراني خلال فترة انتخابات الرئاسة الامريكية – العام ٢٠٢٠ وكان الهدف منها التأثير على نتائج انتخابات الرئيس دونالد ترامب [٤٦].

وفي عام ٢٠٢٤ تمكنت جماعة قرصنة سيبرانية نابعة للحرس الثوري الايراني من اختراق شبكة اتصالات الرئيس السابق دونالد ترامب واختراق البريد الالكتروني لمستشار الرئيس (روجر ستون) وأحد المساعدين المهمين في حملة ترامب الانتخابية ووفقاً لشركة (مايكروسوفت ) فأن قراصنة

معروفون باسم (مينت ساندستورم) تقف وراء هذا الهجوم السيبراني والعمل على حذف قواعد البيانات لحملة ترامب الانتخابية [٤٧].

مما تقدم تبين أن طبيعة الصراع في الفضاء السيبراني هي طبيعة غامضة ومعقدة ، اذ تتوسع وتختلف الاهداف التي تعمل الدول على استهدافها ولا تقتصر على جانب واحد محدد، وتبين هذا من خلال هجمات الحكومة الايرانية على الولايات المتحدة ومستخدمة وسائل واهداف متنوعة مما ادى الى زيادة المنافسة الأمنية السنوات القادمة وتصاعد حدة الصراع السيبراني بين الدولتين في.

## المبحث الثالث \ رؤية مستقبلية حول الهجمات السيبرانية

### المطلب الأول : تقدم وتصاعد الهجمات السيبرانية

أن حجم الهجمات السيبرانية أخذ يتسبأكملها،زايد في مجال الفضاء السيبراني واخذ ينمو بشكل مطرد مما، يؤدي الى احتمالية وقوع هجمات سيبرانية بشكل كارثي وبشده عالية في ألمستقبل ، أن توسع مجال الفضاء السيبراني وسهوله الدخول أليه أدى الى أن تتوسع دوائر الاستهداف والبنى ألتحتية للدول ، أذ في ألسابق كانت مقتصره على الهجمات التي تشن في الفضاء الإلكتروني ألمحدد بشبكة ونظم المعلومات الخاصة بكل مؤسسه لدى الدول سواء كانت مدنية أو عسكرية ، لكن التطور الحاصل في ميدان الفضاء السيبراني والثورة ألتكنولوجية أدت الى تطور وظهور الأسلحة السيبرانية وأخذت القوه السيبرانية تتطور بشكل هائل مما دفع الدول في وضع خطوات سياسية وأمنيه للحصول على تلك ألقوه ، وفي ظل معطيات التطور الحاصلة في الفترة السابقة وظهور فواعل من غير الدول والتي عملت على امتلاك ألقوه السيبرانية، فلن تقتصر الهجمات بشكل محدد داخل دول معينه بل ستشمل في ألمستقبل مؤسسات دوليه سواء كانت اقتصادية أو أمنيه وبشكل واسع في ميدان الفضاء السيبراني ، أذ سيزداد تهديد الصراع السيبراني ألمدمر على مدار العقد ألمقبل ، ولن يقتصر على الدول القومية فقط بل ستشمل مؤسسات أمنيه واقتصادات دول بأكملها ، وستكون الدول معرضه للقرصنة وسرقه البيانات مما يعرض أمن تلك الدول الى ألخطر ألمستقبلي [٤٨] .

كما أن التوقعات العسكرية المستقبلية تتجاوز ما سبق إلى درجة أعلى من الحرب الإلكترونية تتمثل في تجهيز وإعداد روبوتات آلية فتاكة تقوم بالهجوم مباشرة على منشآت العدو ورغم عدم الوصول لمثل هذه الدرجة والشكل من الهجمات بعد، إلا أن احتمالات وجودها مستقبلا تتزايد مع تطور القدرات التكنولوجية واتساع الاعتماد على القطع ذاتية القيادة أو التي يتم التحكم بها عن بعد، كما هو الحال في الطائرات المسيرة عن بعد، والمعروفة بـ "الطائرات بدون طيار أو "الدرونات"، دولة التغاضي عنه أو اغفاله وأياً كان الشكل أو المستوى فإن حروب الفضاء الإلكتروني قد أصبحت واقعا ليس بإمكان أي حيث لا تكاد تسلم دولة اليوم من التعرض لإحدى أشكالها، بما في ذلك حروب المعلومات والشائعات أو التجسس والاختراقات، وكل ذلك يستدعى المبادرة الأخذ الإجراءات

الوقائية، بداية من تطوير منظومات الدفاع الإلكتروني وتعزيز الأمن السيبراني، وحتى المشاركة والدفع باتجاه تطوير منظومات تشريعية دولية تسهم في تحديد تقييد هذه الحروب بشكل حاسم وفعال [٤٩] .

وستتعرض البنيه التحتية للدول بما فيها من البنيه التحتية ألحساسة مثل الطاقة والنقل لهجمات سيبرانية عالية الشده، ولن تقتصر على سرقه البيانات والمعلومات والقرصنة بل ستتخذ شكل أخر من أشكال التدمير وتصل الى حد حدوث الانفجارات الشديدة وتوقف أجهزه رئيسيه للتحكم بتلك البنى ألتحتية ، اذ ستزاد الهجمات تعقيداً بشكل واسع بسبب ظهور ألاصطناعي ألذي يعطي نتائج سريعة في تحليل المعلومات والعمل على شن هجمات سريعة على مصادر شبكات نظم المعلومات، مما أتاح للمهاجمين القدرة على الوصول الى الهدف ألمراد تدميره بسرعه فائقة والتسبب بأضرار لا تقتصر على الجانب ألمادي والمعنوي فقط ،بل تطورت الى حدوث أضرار جسدية جسيمة مما تسبب خسائر وسقوط جرحى وضحايا جراء تلك الهجمات ، هذا الشكل من الدمار التي تسببه تلك الهجمات يعطي مؤشرات على أن مجال الهجمات بدأ يتخذ مجال مغاير عما كانت عليه سابقاً وستزداد تلك الهجمات بشكل متزايد و متواصل وبشده عالية بفعل التطور الحاصل .

## المطلب ألثاني : تراجع الهجمات السيبرانية بفعل استراتيجيات الدفاع والتعاون ألمشترك

استجابت ألعديد من الدول للتهديدات ألجديدة للحرب السيبرانية ووضعت سياسات أمنيه واستراتيجيات سيبرانية مشتركه لمواجهه مثل هذه التهديدات، وأدى ألتوسع في مجال الفضاء السيبراني الى أنشاء مؤسسات ومنشآت حيوية أكانت عسكرية أو مدنيه تعمل على حماية البنية ألتحتية للدول ووضع التشفير ألللازم وحماية شبكه ونظم المعلومات الخاصة بالدولة، اذ على المستوى ألداخلي وضعت الدول عدة سياسات سيبرانية أمنية تمثلت في أنشاء فرق حربية سيبرانية ووكالات استخباراتية في هذا المجال، وأنشاء قطاعات جديدة تكون مكرسة للنشاط السيبراني ، كانت هذا الخطوات بمثابة أنشاء هيكل أمني سيبراني متكامل يكون مكرس لتحقيق الأمن السيبراني للدول، فهذه التهديدات تتطلب جهود دولية مشتركة وتعاون دولي لمعالجتها على نحو ملائم ، اذ يمثل التعاون الدولي أحد العناصر ألرئيسية في تحقيق وضمان الأمن السيبراني على الصعيد الدولي، ويمكن الاستفادة من هذا التعاون من خلال وضع اتفاقيات مثل اتفاقية مكافحة الجريمة الإلكترونية ألعابرة للقومية ، فالهجمات السيبرانية تمتد عبر الحدود وتشكل شبكات وأنظمة معقده تعمل بشكل غير سلمي ، وهنالك ألعديد من الإجراءات التي على الدول أن تبتغيها للوصول أليها لمواجهه الهجمات السيبرانية ومنها [٥٠] :

١- تأمين الشبكات المعلوماتية؛ لعل محاولة الدول والمؤسسات ألحكومية تأمين شبكاتها ضد الاختراق لتكون بمثابة وسيلة تمنع وتقلل الهجمات السيبرانية وبالتالي تؤدي الى منع اختراق شبكاتها ووضع التشفير ، ويقصد بالتشفير تحويل المعلومات والبيانات الى ارقام ورمز سرية لا أحد

يستطيع حلها فقط من يملك أمكانية الوصول لتلك الرموز.

٢- جدار النار أو حائط المنع، fire walls : نظام معلوماتي متكامل متكون من أنظمة فرعية ( برامج) توفر عوازل أمنية ما بين الشبكات الخارجية للأنترنت وشبكات المؤسسات ألحكومية الداخلية للدول والحكومات ، وتعمل على صد الهجمات السيبرانية ومحاولات سرقة البيانات واختراقها ، ويوجد ألعديد من هذه البرامج مثل برنامج جدران النار firewalls ، ومزودات الخدمة proxy servers .

ومن ثم يجب أن تكون هنالك استراتيجيات أمنية سيبرانية فعالة تتكيف مع ألتقدم ألتكنولوجي بشكل كافٍ وتستجيب للتحديات الأمنية السيبرانية في الفضاء السيبراني ، وتنوعت الجهود الدولية المبذولة في مكافحة الهجمات السيبرانية ألا أن التطور ألتكنولوجي ألمتزايد على مستوى المجال السيبراني والاستعمال اللامتناهي لشبكات ونظم المعلومات والإنترنت وظهور فواعل آخرين يمتلكون القدرة والقوة السيبرانية وتوظيفها للحصول على أهدافها ، كل هذه تشكل تحديات تفرض على الدول أن تكثف من الجهود الأمنية المشتركة في ميدان الفضاء السيبراني للحد من الهجمات السيبرانية [٥١] .

تعمل الولايات المتحدة الأمريكية الى تعزيز الشراكات وتوسيع مبادئ الأمن والسلام في الفضاء السيبراني ، لذلك سعت الولايات المتحدة الى وضع قواعد ومبادئ وبناء توافق دولي حول قواعد السلوك في الفضاء السيبراني وخاصه في مجال الشراكة ، وتسعى الى أشراك وأقناع عدد كبير من ألفاعلين برؤيتها للفضاء السيبراني من أجل حماية مؤسساتها والبنية التحتية المهمة والحيوية ألسياسية والأمنية والاجتماعية ، وعززت قدراتها في مجال الدفاع السيبراني من خلال حماية الشبكات والردع ، سواء كانت تلك الهجمات تشكل تهديد من الإرهابيين أو الدول أو الوكلاء ، والعمل على ردع أولئك الذين يهددون الأمن القومي من خلال الهجمات السيبرانية [٥٢].

كل هذه التطورات الإيجابية والتعاون الدولي ألمشترك في مجال الفضاء السيبراني ووضع ألاستراتيجيات الأمنية السيبرانية ، تكون كفيله بتراجع الهجمات السيبرانية ، ومن ألمرجح في العقد ألقادم ستتراجع الهجمات السيبرانية وتنخفض بشكل كبير بعد أن وقعت الدول على اتفاقيات " الأمن السيبراني العالمي " أذ تنص هذه الاتفاقية تبادل الدول المعلومات فيما بينها حول التهديدات السيبرانية وتحديد ألمتورط في هذه الهجمات ومعاقبته وفرض عقوبات صارمة وبشكل قانوني ، وأصبحت شبكات الإنترنت ونظم المعلومات محمية بشكل آمن بسبب التنمية الإلكترونية وتعزيز قدرات الأفراد في هذا المجال وبالتالي أنعكس إيجابيا على ثقة الأفراد في ألعالم ألرقمي، مما يؤدي الى تراجع الهجمات السيبرانية وتأثيرها على الاستقرار العالمي .

## المطلب الثالث : تقدم الهجمات السيبرانية وتوقفها لحقبة زمنية

أن الحرب السيبرانية تشهد أنماط متقلبة بين ألتقدم والتوقف وفق عوامل تؤثر عليها ، وهذه العوامل ذات طبيعة جيوسياسية وتقنية وتنظيمية ، أذا هنالك استراتيجيات وإجراءات تلجأ اليها الدول تؤدي الى توقف الهجمات السيبرانية فتره زمنيه معينه ومن هذه الإجراءات هي [٥٣] :

- **عمليات دولية تركز على التعاون الدولي** : العمل على ألتصدي ألمشترك للتحديات الأمنية ، مما يفرض على الدول التركيز على وضع استراتيجيات أمنيه سيبرانية وبذل الجهود الدولية ألمشتركة للتصدي لهذه الهجمات ، هذا الامر من شأنه أن يؤدي الى توقف الهجمات السيبرانية لفتره معينة

- **حوكمة الأمن السيبراني وتطوير الوسائل ألدفاعية** : تعمل الدول على تطوير البنية ألتحتية ألخاصة بها في مجال الدفاع السيبراني ووضع تشفير متلائم مع التطورات الحاصلة في ميدان الفضاء السيبراني ، هذا ألعامل من شأنه أن يوقف الهجمات السيبرانية والعمل على وضع أساليب جديدة يستطيع من خلالها المهاجمون شن هجمات قادره على اختراق نظم الحمايات المتطورة ، وهذا الأمر يتطلب فتره زمنية معينه للوصول ألية، بالإضافة الى تغيير استراتيجيات ألمهاجمين بعد أن أصبحت الهجمات التقليدية غير فعاله بسبب هذا التطور الحاصل في أنظمة الدفاع الحديثة ، وفرض عقوبات صارمه على ألمهاجمين من الدول من جانب آخر .

هذه الرؤية ألمستقبلية هي الأرجح في استشرافها للواقع ألمستقبلي للحرب السيبرانية وتصورها لما ستكون علية الهجمات السيبرانية في الحقبة القادمة ، أذ ستتوقف الهجمات السيبرانية لفترات معينة بفعل انشغال الدول في تطوير البنية ألتحتية ألخاصة بها والعمل على وضع استراتيجيات دفاعية وهجومية للسيطرة أكثر على مجال الفضاء السيبراني ، وستشن هجمات بعد هذا ألتوقف بشكل يلائم التطور الحاصل داخل بيئة الفضاء السيبراني .

**ألخاتمة :**

لقد أدى التطور التكنولوجي وخاصة في ميدان الفضاء الالكتروني والثورة التكنولوجية في ميدان أسلحة الجيل الخامس، والتقدم المذهل الذي حصل في العشرين سنة السابقة أدى إلى ظهور نوع جديد من الحروب أطلق عليه الحروب السيبرانية ، حيث عملت الدول على زيادة الانفاق الاقتصادي في سبيل الحصول على الأسلحة والقدرات السيبرانية لتتمكن من خلالها تحقيق أهدافها بوسائل بديلة عن الوسائل العسكرية التقليدية ،ومن دون الحاجة إلى الدخول في معارك ميدانية، لما تنطوي عليه هذه الحروب وهذا النوع من المعارك من استنزاف مادي وبشري، وقد عملت الحرب السيبرانية على التأثير المباشر على بنية النظام السياسي من خلال التأثير على حركة التفاعل بين وحدات النظام وبالتالي أنعكس على طبيعة العلاقات الدولية التي تفاعل في اطارها الدول، حيث أدى استخدام الأسلحة السيبرانية وشن هجمات سيبرانية الى الضرر في المؤسسات الأمنية

والعسكرية والاقتصادية على المستوى ألداخلي للدول وحتى على مؤسسات النظام الدولي ، وكان ذلك بسبب الخصائص التي تتميز بها الحرب السيبرانية في كونها غير مرئية ولا يمكن تحديد مصدر الهجمات من قبل الدولة المستهدفة ، مما ادى بتلك الدول الى تبادل الاتهامات او الشك بمصدر الهجمات وبالتالي توترت العلاقات الدولية بشكل كبير ، وفي الفترة الأخيرة شهدت بعض الدول من زياده حدة الهجمات السيبرانية عليها بشكل كبير عما كانت علية سابقاً ، وتنوعت شده الهجمات من التجسس والاختراق الى حتى التفجيرات ألقاتلة وبوسائل وأجهزه اتصالات مختلفة ، من هذه الدول هي (الولايات المتحدة إيران )، حيث تعرضت هذا الدول الى هجمات عديدة سواء في فترة السلم أو الحرب ، وتنوعت امكان الاستهداف والبنى التحتية من مدنية الى عسكرية واقتصادية ، وتعتبر الولايات المتحدة الدولة ألرائدة من بين دول ألعالم في مجال الفضاء السيبراني لما تمتلكه من قدرات ومقومات القوة السيبرانية ، اذ عملت على وضع استراتيجيات أمنية سيبرانية دفاعية وهجومية بالإضافة الى التمويل المالي ألعالي في هذا المجال ، وفي الحقبة السابقة شهدت الولايات المتحدة تحدياً امنياً ي بيئة الفضاء السيبراني وتمثل هذا التحديد في بروز إيران كدولة معادية للولايات المتحدة في الفضاء السيبراني ، وتمكنت بفضل ما تملكه من قدرات سيبرانية على شن هجمات سيبرانية متفاوتة الشدة على البنية ألتحتية للولايات المتحدة ، مما دفع الدولتين في الدخول الى صراع سيبراني مستمر الى الآن ، وأنعكس شكل هذا الصراع على المستوى الدولي، اذ عملت ألعديد من الدول على تطوير قدراتها في مجال الفضاء السيبراني وتغير شكل الصراع من عسكري تقليدي الى إلكتروني غير مرئي ، أذ تشير التوقعات الى استمرار الهجمات السيبرانية لفترات متباعدة وشده متفاوتة ، وستتنوع مجالات الاستهداف من البنية ألعسكرية الى المؤسسات ألمدنية والاقتصادية والاجتماعية .

**ألاستنتاجات**

**هنالك عدة استنتاجات توصلت أليها هذه ألدراسة سيتم إيضاحها على شكل نقاط :**

١- عدم الصول الى أتفاق بين ألباحثين والمهتمين والاكاديميين لوضع تعريف عام وشامل للحرب السيبرانية على ألرغم من الجهود المبذولة من قبلهم ، لذلك يتميز مفهوم الحرب السيبرانية بالغموض والصعوبة في تحديد تعريف عام شامل لها .

٢- علمت الحرب السيبرانية الى تغيير ألعديد من الظواهر الموجودة في العلاقات الدولية منها ( سباق (ألتسلح ) ( توازن القوى ) ( التحالفات ) من خلال تغيير القواعد التي تحكم العلاقات بين الدول ، مما دفع تلك الدول الى العمل على الدخول بسباق تسلح إلكتروني وسيبراني بعيد عن سباق ألتسلح ألعسكري ألتقليدي والنووي ، ودفت الحرب السيبرانية بالدول الى إقامة تحالفات واتفاقات جديدة قائمة على مفهوم الأمن السيبراني والالكتروني وغيرت مرتبة القوة التي كان قائم عليها نظام توازن القوى وبرزت دول تمتلك مؤسسات سيبرانية عالمية متقدمة مثل إسرائيل في

الشرق الأوسط.

٣- تصاعدت شدة الحرب السيبرانية بشكل كبير واستطاعت أن تنتقل من مرحلة التجسس وسرقة المعلومات الى القدرة على قتل الأنسان من خلال تفجير أجهزة الاتصالات وحتى جميع الأجهزة الإلكترونية مخلفة عدد كبير من الضحايا والجرحى وبوقت قياسي قصير جداً .

٤- أن التطور في ميدان الفضاء السيبراني أنعكس على الحرب ألميدانية بشكل كبير حيث تستطيع الدول التي تقوم بهجمات سيبرانية الى أحداث قدرة تدميريه بشرية وبسرعه فائقة وبمدة زمنية لا تتجاوز دقائق معدودة بحيث الدول ألمستهدفة لا تعطي هكذا خسائر بشرية أن دخلت حرب عسكرية ميدانية مباشرة ،

٥- بفعل التطور الحاصل في ميدان الفضاء السيبراني سوف تتجه الدول الى زيادة قدراتها السيبرانية والعمل على زيادة الإنفاق ألعسكري في هذا الجانب ووضع خطط واستراتيجيات دفاعية وأمنية من أجل تحصين حدودها والعمل على حماية أمنها ألقومي وبالتالي سينعكس هذا الأمن على المستوى الخارجي في البيئة ألسياسية .

٦- أدى أنتشار القوة بمختلف أنماطها وبالإحص القوة السيبرانية الى تمكن فواعل من غير الدول في النظام الدولي من الحصول على هذه القوة ، مثل الجماعات الإرهابية والشركات ألمتعددة ألجنسيات وحتى الأفراد ، عملت هذه الجماعات لا تحقيق مطامعها وشن هجمات على الدول ذات السيادة ألقومية ألكاملة مما أنعكس سلباً على الأمن العالمي حيث أن تحولات القوة أفرز جماعات استطاعت ان تمتلك مصادر القوة ألمادية والعمل على شن هجمات سيبرانية واختراق نظم وشبكات الاتصالات والمعلومات الموجودة داخل وحدات النظام الدولي .

٧- كلما أهملت الدولة تطوير مؤسسات سيبرانية وأمنية داخلية كلما كانت عرضه للاختراق والتجسس وبالتالي ينعكس سلباً على أمنها ألقومي وتكون مهددة بشكل كامل .

٨- ما تزال الولايات المتحدة تمثل الدولة الأولى في مجال الفضاء السيبراني لما تملكه من قدرات سيبرانية ومؤسسات أمنية متطورة في هذا المجال ، لاسيما علمت الرئاسات ألمتعاقبة على زيادة الإنفاق المالي بدرجة كبيرة ووضع سياسيات أمنية سيبرانية للسيطرة المستقبلية على الفضاء السيبراني بشكل محكم .

**الهوامش**

[١] - بسمة يونس محمد ،ألحروب ألسيرانية واثرها في ألتنظيم الدولي ، مجلة العلوم والدراسات ألانسانية ،جامعة بنغازي ، ليبيا كلية ألآداب والعلوم بالمرج، العدد (٤٩) ، ألمجلد(٥) ، (فبراير ٢٠٢٣) ،ص ٦.

[٢] – صدام مرير حمد ألجميلي ،الحرب الهجينة وأثرها في مستقبل الصراع العالمي،مجله العلوم السياسية ،، كلية العلوم ألسياسية ، جامعه تكريت، ألعراق ، ألعدد (١) ، المجلد (٣٤) ، (٣١ أذار ٢٠٢٤) ، ص١١١.

[٣] – أنعام عبد الرضا سلطان ، توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى ، مجلة قضايا سياسية ، كلية الاعلام ، جامعة بغداد ، المجلد (١) ، العدد (٧٣) ، (أكتوبر ٢٠٢٤) ، ص٤٢٩.

[٤] – شويرب جيلالي ، مفهوم ألحروب السيبرانية الأمن السيبراني ، مجلة ألحقوق والحريات ، كلية ألحقوق وألسياسة ، جامعة ألاغواط ، ألجزائر ،ألمجلد (١١) ، ألعدد (١) ، ( أبريل ٢٠٢٣) ، ص ١٦٢.

[5] –Michael Robinson and other , cyber warfare : issues and challenges , Elsevier journal , faculty of Technology,de Monntfort university , Leicester ,United Kingdom ,e9,no4 , 2015 ,p73 .

[٦]– رشا سهيل محمد زيدان ، التحولات المعاصرة للقوة وتاثيرها في مستقبل سيادة الدولة القومية بعد عام ٢٠١٠: نماذج مختارة ، أطروحة دكتوراه منشورة مقدمة ألى ، كلية ألعلوم ألسياسية ، جامعة ألنهرين ، بغداد ، ٢٠٢٤، ص ٢٢٨ .

[٧]– ايمان قديح ، تحول مفهوم القوة في العلاقات الدولية بعد نهاية الحرب الباردة ، رسالة ماجستير غيرمنشورة ، كلية الحقوق والعلوم السياسية ،جامعة محمد بوضياف_المسيلة ، ألجزائر ، ٢٠١٧/٢٠١٨، ص ٥٩.

٨ – عادل عبد الصادق ، ألحرب السيبرانية وتداعياتها على الأمن العالمي ، مؤسسه ألاهرام . https://www.siyassa.org.eg/Print/12072.aspx ٢٠٢٤\١١\٢٢

[٩]– نبيلة عبد ألفتاح قشطة ، ألحرب السيبرانية وسبل مواجهتها ، مجلة شؤون أستراتيجيه ، كلية ألحقوق ، جامعة ألمنوفيه ،القاهره ، عدد (١٧)، (آذار ٢٠٢٤)، ص٤٩٢ .

[١٠]– نبيلة عبد ألفتاح قشطة ، ألحرب السيبرانية وسبل مواجهتها ، ألمصدر سبق ذكرة ، ص٤٩٣.

[١١] – مريم عماد شاكر ، ألانماط ألمستجده للحرب وأثرها على الأمن الدولي ، رسالة ماجستير غير منشوره ، كليه القانون والعلوم ألسياسية ، ألجامعة ألعراقية ، ألعراق ، ٢٠٢٢ ، ص ٨٥.

1 ـ Major General Bipin Bakshi , information warfar : concept and components , Journal of Defence Studies ,Chaudhary Charan University , Meerut , volume 5 , issue 4 , DEC 2018 .

–13 Shmuel Even and david siman ,cyber warfare concept and strategic trends , institute for national security studies , tel aviv ,No.117 , May 2012 , p16

[١٤]– مريم عماد شاكر ، مصدر سبق ذكره ، ص ٨٩.

[١٥] – صلاح حيدر عبد ألواحد ، حروب ألفضاء ألالكتروني ، رسالة ماجستير غير منشورة ، كلية ألآداب وألعلوم ، جامعة ألشرق ألاوسط ، ألاردن ، عمان ، تموز ٢٠٢١ ، ص٤٣.

–16 Recognizing the seven stages of a cyber-attack , https://www.dnv.com/ ,2024\11\15 .

-17 stages of the cyber attack lifecycle , op , https://www.maddyness.com/uk/ .

-18 – Recognizing the seven stages of a cyber-attack , op , https://www.dnv.com/ .

-19 stages of the cyber attack lifecycle , op , https://www.maddyness.com/uk/

-20 Peter Pascucci , Distinction and Proportionality Cyber war : Virtual Problems With a Real Solution , Minnesota Journal of International Law , College of Law , University of Minnesota , Vol 26 , iss 2 , DEC 2017 ,P 424

-21 William H.Bootgby , methods and Means of Cyber WarFare , Journal of Iternational Studies , U.S.NAVAL WAR COLLEGE , Vol 89 , iss 37 , NOV 2013 , p387.

-22 PK Mike , Cyber weapon – Weapon Of War , Vivekanda International Foundation , published in 2021 , New Delhi , p7-8 .

-23 PK Mike , Cyber weapon – Weapon Of War , same source ,p9 .

٢٤- مريم عماد شاكر، تأثير ألانماط ألمستجده في ألحرب ، مصدر سبق ذكره ، ص ٩٠ .

٢٥- أيهاب خليفة ، ألحالة السيبرانية في نظريات ألعلاقات الدولية ، صحيفه مركز المعلومات ودعم أتخاذ ألقرار، العدد (٢٣) ، مصر ،٢٠٢١، ص٧.

٢٦ – عمر أحمد أعمر ، ألحرب ألالكترونية في ألقانون الدولي ألانساني ، مجلة دراسات علوم الشريعه والقانون ، كلية البلقاء ، جامعة ألبلقاء ألتطبيقيه ، ألاردن ، المجلد (٤٦) ، عدد (٣) ، (مارس ٢٠١٩) ، ص ١٤٠ .

٢٧ – قاسم خضير عباس ألعرداوي ، ديناميكيات ألحروب ألالكترونيه واثرها في ألصراع الدولي ، المركز ألديمقراطي ألعربي ، ٢٢ فبراير ٢٠٢١ ، تاريخ ألزياره ٢٠٢٤\١١\٢٧ ، متاح على الرابط : https://democraticac.de/?p=73151 .

٢٨ – رشا سهيل محمد زيدان ، التحولات المعاصرة للقوة وتاثيرها في مستقبل سيادة الدولة القومية ، مصدر سبق ذكره ، ص ١٥٧ .

٢٩ – أحمد عثمان محمد ، ألحروب السيبرانية وأثرها في ألعلاقات الدولية : روسيا والولايات ألمتحده أنموذجاً ، مجلة ألجامعة ألعراقية ، جامعة ألتقنية ألوسطى ، معهد ألادارة ، بغداد ، مجلد (٢) ، عدد (٥٩)، (أكتوبر ٢٠٢٣) ، ص ٤٦٥-٤٦٦

٣٠- سماح عبد الصبور، القوة السيبرانية في العلاقات الدولية : دراسة في الحروب السيبرانية بالتطبيق عام ٢٠٢٠ مركز الحضارة للدراسات والبحوث، تاريخ المقال ٢٧-١٢٠٢١ ابريل، تاريخ الزيارة ٢٨/١١/٢٠٢٤ متاح على الرابط https://hadaracenter.com/

٣١- شيماء معروف فرحان، التحول في مفهوم القوة والصراع : دراسة في الحروب السيبرانية ، مجلة قضايا سياسية ، كلية ألعلوم ألسياسية ، ألجامعه ألمستنصرية ، بغداد ، ألمجلد (١٥) ، عدد(٧٥ ) ، (ديسمبر ٢٠٢٣) ، ص ٥٠٠ .

٣٢- شيماء معروف فرحان ، ألمصدر نفسة ، ص ٥٠١ .

[٣٣]– محمود علي عبد ألرحمن ، ألفضاء ألالكتروني وأثرة على مفاهيم ألقوة والأمن وألصراع في ألعلاقات الدولية ، مجلة ألسياسة وألاقتصاد ، كلية ألسياسية والاقتصاد ، جامعة بني سويف ، مصر ، ألمجلد (١٦) ، عدد (١٥) ، (يوليو ٢٠٢٢) ، ص ٤٣٢ .

[٣٤] – باخان ناكو نجم ألدين ، تأثير ألحرب السيبرانية على رفع مستوى ألصراع بين ألولايات المتحدة إيران ، مجلة جامعة رابرين ، كلية ألعلوم ألسياسية ، جامعة ألسليمانية ، ألسلمانية ، ألعراق ، ألمجلة (٨) ،العدد (٤) ، ٤ ديسمبر (٢٠٢٤) ، ص ٣١٤ .

[٣٥] – باخان ناكو نجم ألدين ، مصدر سبق ذكرة ، ص ٣١٧.

[٣٦] – سليم دحماني ، أثر ألتهديدات " السيبرانية " على الأمن ألقومي : ألولايات ألتحدة انموذجاً ، رسالة ماجستير غير منشورة ، كلية ألحقوق والعلوم السياسية ، جامعة محمد بوضياف ، ألمسيلة ، ألجزائر ، ٢٠١٨ ، ص ٧٥ .

[٣٧]– سليم دحماني ، ألمصدر نفسة ، ص ٧٦

[٣٨] – باخان ناكو نجم ألدين ، مصدر سبق ذكرة ، ص ٣١٧.

[٣٩] – قدرات ألقرصنة السيبرانية الإيرانية ، مركز ألملك فيصل للبحوث والدراسات ألاسلامية ، تقرير خاص، ألرياض ، ألسعودية ، يناير ٢٠٢٠، ص ١٠.

[٤٠] – هبة عبد ألسلام خطاب ، مؤسسات ألفضاء السيبراني في منطقة ألشرق الاوسط : ايران وإسرائيل نموذجاً ، مجلة جامعة تكريت ، كلية ألعلوم ألسياسية ، ألعراق ، ألمجلد (٣٠) ، ألعدد (٤) ، ديسمبر ٢٠٢٢ ، ص ٣٨٥– ٣٨٦ .

[٤١] – هبة عبد ألسلام خطاب ، مصدر سبق ذكرة ، ص ٣٦١.

[٤٢]– CHUCK FREILICH , THE IRANIAN CYBER THREAT , part 2 , 2024\11\25 : https://www.inss.org.il/wp-content/uploads/2024/02/Part-2.pdf .

[٤٣]– كرار عباس متعب فرج ، ألحرب السيبرانية : دراسة في إستراتيجية ألهجمات السيبرانية بين ألولايات المتحدة ألامريكية إيران ، مجلة حمورابي للدراسات ، مركز حمورابي للدراسات وألبحوث ألاستراتيجية ، ألعراق ، ألعدد (٤٠) ، ألسنة ألعاشرة ، شتاء ٢٠٢١ ، ص٢٠٦.

[٤٤]– كرار عباس متعب فرج ، ألمصدر نفسة ، ص٢٠٩–٢١٠ .

[٤٥] – باخان ناكو نجم ألدين ، مصدر سبق ذكرة ، ص ٢٢٤.

[٤٦]– كرار عباس متعب فرج ، مصدر سبق ذكرة ، ص ٢١٦ .

[٤٧] – أتجاهات تزايد ألتهديدات السيبرانية للأنتخابات ألرئاسية ألامريكية ، مركز ألمستقبل للأبحاث والدراسات ألمتقدمة ، تاريخ ألزيارة ٢٨\١١\٢٠٢٤ ، متاح على ألرابط : https://futureuae.com/ar/Home/Index/2/%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9 .

[٤٨] – علاء ألدين فرحات ، ألحرب السيبرانية ومستقبل الأمن العالمي ، مجلة ألناقد للدراسات ألسياسية ، ألمدرسة ألوطنية ألعليا للعلوم ألسياسية ، ألجزائر ، ألمجلد (٦) ، ألعدد (٢) ، أكتوبر ٢٠٢٢ ، ص ٦٨٩.

[٤٩] – صلاح حيدر عبد ألواحد ، حروب ألفضاء ألالكتروني : دراسة في مفهومها وخصائص سبل مواجهتها ، رسالة ماجستير غير منشورة ، جامعة ألشرق ألاوسط ، عمان ، ألاردن ، تموز ٢٠٢١، ص ٧٤ .

[٥٠]– أميرة عبد ألعظيم محمد ، ألمصدر نفسة ، ص ٥٢٢ ..

[٥١]– أميرة عبد ألعظيم محمد ، ألمصدر نفسة ، ص ٥٢٣ .

[٥٢]– سليم دحماني ، مصدر سبق ذكرة ، ص ٨١

[٥٣] – محمد ألكويتي ، الأمن السيبراني في عام ٢٠٢٣ : تحولات وتحديات عصر ألذكاء ألاصطناعي ، ترينذز للبحوث والاستشارات ، تاريخ ألزيارة ٢١\١٢\٢٠٢٤ ، متاح على ألرابط : https://trendsresearch.org/ar/