الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وإيران

***أ.م.د. كرار عباس متعب فرج**
باحـث من العــراق

* جامعة كربلاء - كلية الإدارة والاقتصاد
karrarabbaskk@gmail.com

ملخص :

تعد الحرب السيبرانية احدى أدوات الجيل الخامس للحروب، إذ أخذت حيّزاً واسعاً ومؤثراً في الوقت الحاضر؛ بسبب كلفتها القليلة للجهة المهاجمة بخلاف الجهة المستهدفة التي تكون منشآتها ومواقعها الحيوية وبناها التحتية في مرمى التدمير والإنهاك والإبطاء، وهذا ما ترجم فعلياً بين طرفي الصراع بين الولايات المتحدة الامريكية وإيران (محلّ الدراسة) بعد عام 2006 وحتى وقتنا الحاضر، إذ كانت الهجمات السيبرانية بين الطرفين في الفضاء السيبراني الصفة الغالبة بينهما مستخدمين من البرامجيات والفايروسات المدمرة أسلحة استراتيجية سيبرانية ناتجة عن توجهاتهم الاستراتيجية عبر الإدارات الامريكية المتعاقبة من جهة، وعبر الرؤساء الإيرانيّون المتعاقبون من جهة أخرى، إذ أنشأت مؤسّسات مختصة بذلك، إذ تسعى الولايات المتحدة الأمريكية من جراء تلك الهجمات إلى تدمير المواقع الحيوية والبنى التحتية لإيران خاصة في مجالها النووي، مع هجمات سيبرانية إيرانية ضد المواقع الحيوية للولايات المتحدة الأمريكية في رسالة لها أن إيران لها القدرة الفاعلة في هذا المجال، مع طرح تلك الهجمات السيبرانية بين الطرفين وفق توقيتات وأحداث زمنية ووفق مسار بياني التي قد تمهد مستقبلاً لمرحلة تصعيد لحرب شاملة إلّا إذا تم التحكم الاستراتيجي بها، وفضلاً عن ما تقدّم وللضرورة العلمية تم طرح الحرب السيبرانية من حيث نشأتها ومفهومها مع المفاهيم المقاربة لها استكمالاً لموضع البحث.

كلمات مفتاحية : الحرب السيبرانية، الهجمات السيبرانية، الاستراتيجية السيبرانية، الولايات المتحدة الأمريكية، إيران .

Cyber war: a study in the strategy of cyber attacks between the United States of America and Iran

Assist Prof. Dr. Karrar Abbas Miteb Farag
researcher from Iraq
Karbala University/ College of Administration and Economics

ABSTRACT

The cyber war is one of the tools of the fifth generation wars, as it has taken a wide and influential space at the present time, as it not cost the attacker side a big fund unlike the targeted party, whose facilities, vital sites and infrastructure are in the crosshairs of destruction, exhaustion and slowness, and this is actually translated between the two sides of the conflict between the united states of America and Iran (the focus of the study is on the period after 2006 until the present time, as cyber attacks between the two parties in the cyberspace were the dominate feature between them using destructive software and viruses as cyber strategic weapons resulting from their strategic orientations through successive US administrations on the one hand and through successive Iranian presidents on the other hand, specialized institutions were established on the foregoing basis. The United States of America seeks, as a result of these attacks, to destroy the vital sites and infrastructure of Iran, especially in its nuclear field, with Iranian cyber attacks against the vital sites of the United States of America in a message to it that Iran has effective ability in this field, with the introduction of these cyber attacks NS between the two parties according to timings and temporal events and according to a graphic path that may pave the future for the comprehensive war unless it is strategically controlled, and in addition to the foregoing and for the scientific necessity, the cyber war was presented in terms of its origin and concept with comparative approaches to complete the topic of the research.

KEY WORDS: cyber warfare, cyber attacks, cyber strategy, the United States of America, Iran.

المقدمة

تنبع اهمية الموضوع من الحرب السيبرانية نفسها باعتبارها احدى أدوات الجيل الخامس للحروب التي مجال صراعها هو الفضاء السيبراني وأسلحتها هي البرامجيات والفايروسات ذات الصفة التدميرية الموجّهة ضدّ المواقع الحيوية والبنى التحتية للدول المستهدفة مع أقل كلفة للدول المهاجمة وهذا ما ترجم بين الطرفين الولايات المتحدة الأمريكية وإيران (محط الدراسة) الذي اصبح صراع الهجمات السيبرانية بينها هو السائد بدءاً من عام 2006 وحتى وقتنا الحاضر، من خلال تلك الهجمات الاستراتيجية السيبرانية لكل طرف والرد عليه بالمثل او بهجوم استباقي، وهذا ما دفعنا للبحث العلمي في هذا الموضوع لمعرفة مسار تلك الهجمات الاستراتيجية السيبرانية لكل طرف لأهميّة ذلك لأنّه قد يمهّد في المستقبل للمواجهة الشاملة بين الطرفين إلاّ إذا بقيت تحت التحكم الاستراتيجي لكل طرف.

- مشكلة البحث

تنبع مشكلة البحث من الآتي:

تطرح بين الحين والآخر جملة من الاتهامات المتبادلة بين طرفي الصراع، الولايات المتحدة الامريكية وإيران حول الاستهداف السيبراني ضد المواقع الحيوية والبنى التحتية لكل طرف مما يسبب دمار وإنهاك وإبطاء في تلك المؤسسات الحيوية، فارتأينا أن نبحث في ذلك الصراع وتلك الاتهامات لمعرفة وطرح حقيقة تلك الهجمات ووضعها في مسار واضح ووفق جداول ومخطط بياني لتلك الهجمات السيبرانية، وعليه ستكون الصفحات اللاحقة من البحث هي الإجابة على تلك التساؤلات التي ستطرح في ادناه لتصل بنا لمعرفة ذلك المسار الاستراتيجي لتلك الهجمات السيبرانية بين الطرفين، وهي كالآتي:

تعد الحرب السيبرانية أداة من أدوات الجيل الخامس للحروب التي تستهدف المواقع الحيوية والبنى التحتية للطرف المستهدف

1- ما هي الحرب السيبرانية من حيث نشأتها ومفهومها والمفاهيم المقاربة لها؟
2- ما هي وسائل وأهداف الحرب السيبرانية؟
3- ما هي التوجّهات الاستراتيجية للولايات المتحدة الأمريكية عبر ادارتها المتعاقبة في طرح استراتيجيتها السيبرانية الخارجية ؟ وما هي الهجمات السيبرانية للولايات المتحدة الامريكية التي استهدفت فيها ايران منذ انطلاقها حيالها في عام 2006 وحتى وقتنا الحاضر؟
4- ما هي التوجهات الاستراتيجية لإيران في طرح استراتيجيتها السيبرانية الخارجية، وما هي الهجمات السيبرانية الإيرانية التي استهدفت فيها الولايات المتحدة الامريكية منذ عام 2009 وحتى وقتنا الحاضر؟

- فرضية البحث

تنطلق فرضية البحث من الآتي:

تعد الحرب السيبرانية أداة من أدوات الجيل الخامس للحروب التي تستهدف المواقع الحيوية والبنى التحتية للطرف المستهدف من الجهة القائمة بتلك

الهجمات السيبرانية بواسطة أسلحتها من البرامجيات والفايروسات التدميرية وهذا ما نجده بين طرفي الصراع الولايات المتحدة الامريكية وإيران (محط الدراسة) من خلال طرح استراتيجية الهجمات السيبرانية ضمن التوجهات الاستراتيجية لكل طرف عبر الإدارات المتعاقبة داخل الولايات المتحدة الامريكية وكذلك في ايران، خاصة منذ انطلاقها منذ عام 2006 وحتى وقتنا الحاضر، وأخذت تلك الهجمات السيبرانية بين الطرفين عبر مسار استراتيجي سيبراني ووفق توقيتات واحداث زمنية ضد مواقع حيوية لطرفي الصراع حتى وقتنا الحاضر التي بدورها قد تمهد مستقبلا لحرب شاملة بين الطرفين الا اذا بقيت تحت التحكم الاستراتيجي لكل طرف ، وصفحات البحث اللاحقة هي الكفيلة بإثبات صحة فرضية البحث.

- منهج البحث

من أجل ان تكون دراستنا ضمن المنهج العلمي البحثي الصحيح وجب علينا ان نستخدم عدد من المناهج العلمية فكان المنهج التاريخي والمنهج الوصفي ومنهج التحليل النظمي مناهج الدراسة.

- هيكلية البحث

تضمّن البحث فضلاً عن المقدمة والخاتمة مبحثين: الأوّل: تناول الحرب السيبرانية بمطلبين: المطلب الأول: الحرب السيبرانية (النشأة والمفهوم، المفاهيم المقاربة لها), اما المطلب الثاني: تناول الحرب السيبرانية (الوسائل والأهداف) اما المبحث الثاني: تناول الحرب السيبرانية (الولايات المتحدة الامريكية وإيران) بمطلبين: المطلب الأول: استراتيجية الهجمات السيبرانية للولايات المتحدة الأمريكية حيال إيران, اما المطلب الثاني: استراتيجية الهجمات السيبرانية الإيرانية حيال الولايات المتحدة الأمريكية.

المبحث الأوّل: الحرب السيبرانية

اشتُقّت السيبرانية من الكلمة اللاتينية (cyber) ويقصد بها "افتراضي" أو "تخيُّلي" وتستخدم ضمن مجال الفضاء الذي يضم الشبكات العنكبوتية المحوسبة

تُعدّ الحرب السيبرانية أحدى أدوات الجيل الخامس من الحروب التي ساحة صراعها هو الفضاء السيبراني التي انطلقت خلال الحرب الباردة التي تستخدم فيها الأسلحة السيبرانية من براميجيات وفايروسات تأخذ طابع تدميري ضد الجهة المستهدفة بأقلّ كلفة للجهة المهاجمة التي تقوم بها دول بعينها او فاعلين من غير الدول، وعليه سنطرح في هذا المبحث بمطلبين:

المطلب الأوّل: الحرب السيبرانية (النشأة والمفهوم – المفاهيم المقاربة لها).

المطلب الثاني: الحرب السيبرانية (الوسائل والأهداف).

المطلب الأوّل: الحرب السيبرانية (النشأة والمفهوم – المفاهيم المقاربة لها)

اشتُقّت السيبرانية من الكلمة اللاتينية (cyber) ويقصد بها «افتراضي» أو «تخيُّلي» وتستخدم ضمن مجال الفضاء الذي يضم الشبكات العنكبوتية المحوسبة،

ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد وكل ما يتعلق بأنظمة الحواسيب وتكنلوجيا المعلومات والواقع الافتراضي, **والسيبرانية هي:** علم التحكم الأوتوماتيكي والقيادة والتوجيه عن بعد.[1]

وجاء معنى كلمة سايبر (cyber) في قاموس المورد بـ (الكمبيوتري) أو (عصري جدّاً)، وعند البحث عن مصطلح السايبر في القواميس نجد غالبية القواميس الإنجليزية بصورة عامّة والعربية بصورة خاصة تفتقر لهذا المصطلح لحداثته، وان قاموس مايكروسوفت للحاسوب قد تناول هذا المصطلح وبأنه مشتق البادئة (cy-ber) وهو علم التحكم الآلي.[2]

(1) أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، الجزء3، كلية القانون، جامعة الامـارات العربية المتحدة، 2020، ص378 .

(2)حيـدر ناظم عبد علي، رباب محمود عامر، التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة، مجلة الكوفة، العـدد47، جامعة الكوفة، 2019، ص109.

إذ تعود بداية نشأة الحروب السيبرانية الى مرحلة الحرب الباردة فإن أوّل حرب سيبرانية وقعت كانت بين الولايات المتحدة الأمريكية والاتحاد السوفييتي في عام 1982، إذ قام جهاز المخابرات السوفييتي (سابقاً) (KGB) بعملية تسمى (Line x) صممت لتساعد الاتحاد السوفياتي على سرقة تكنلوجيا المعلومات لكل أنشطة الغرب، إذ قامت المخابرات السوفييتية بتدريب جيش من العلماء على التسلل الى الشركات والوكالات لسرقة المعلومات مع تسرب المعلومات إلى وكالة المخابرات الامريكية (CIA) والتي قامت بدلاً من القاء القبض عليهم تركتهم يواصلون العمل ولكن مع امدادهم بمعلومات مغلوطة، وإذ حصل الجواسيس السوفييت على وثائق تتضمّن مخططات ولكن تتضمن خطأ بسيطاً في الشفرة مع استمرار السوفييت باستخدام المعلومات المغلوطة لبناء العمود الفقري لخطوط نقل الغاز الطبيعي والنفط القادم من سيبيريا، وبعد فترة قصيرة تسبب الخطأ المتعمّد في الشفرة في حدوث انفجار لخط الأنابيب وكان هذا الانفجار يعادل ثلث حجم انفجار القنبلة النووية في هيروشيما.[3]

الحرب السيبرانية كإطار عام للمفهوم فإنها تُشَنّ ضد كيانات محددة بهدف تعطيلها والحفاظ على مجال المعلومات من أي اعتداء سيبراني

أمّا الحرب السيبرانية كإطار عام للمفهوم فإنها تُشَنّ ضد كيانات محددة بهدف تعطيلها والحفاظ على مجال المعلومات من أي اعتداء سيبراني من طرف الخصم باستخدام الوسائل التكنلوجية والمعلوماتية المتطورة.[4]

(3)الـحـروب السـيبـرانيـة – نتائج ملموسة لمعارك غير مرئية، الجندي، بتاريخ 1/ابريل/2021، ص1، الشبكة الدولية للمعلومات:
https//www.aljundi.ae%d8%a7%84%d9

(4)Michael Robinson, Kevin jones, helge janicke, cyber war fare: issues and challenges, article in computer and security, Elsevier ,volume – 49 -, march, united kingdom, 2015, p – 24 -

وعرّفت وزارة الدفاع الامريكية الحرب السيبرانية بأنهّا: توظيف القدرات السيبرانية حيث يكون الهدف الأساسي هو تحقيق الأهـداف والآثـار العسكرية في الفضاء السيبراني أو من خلاله، وهي أيضاً نشاط مماثل أو غير متماثل دفاعي كان أم هجومي على الشبكة الرقمية من قبل فواعل دولية أو غير دولية الغرض منها هو إلحاق الضرر بالبنى التحتية الحيوية والأنظمة العسكرية.[5]

الحرب السيبرانية ميدانها الفضاء االسيبراني وهي غير محدودة المجال وتكون غامضة الأهداف لأنّها تتحرك عبر شبكة المعلومات والاتصالات

(5) زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد2، جويلية (يوليو)، الجزائر، 2020، ص91.

وإن الحرب السيبرانية ميدانها الفضاء االسيبراني وهي غير محدودة المجال وتكون غامضة الأهداف لأنّها تتحرك عبر شبكة المعلومات والاتصالات المتعدية للحدود الدولية فضلاً عن اعتمادها على أسلحة الكترونية ذكية ومتطورة تلائم طبيعة السباق

الإلكتروني لعصر المعلومات، أو يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات.[6]

وعليه فإن الفاعل الرئيسي في الحرب السيبرانية هي الدول، إذ بدأت بعض الدول الاستعداد لهذا النوع من الحروب إنشاء جيوش سيبرانية داخل صفوف القوات المسلحة للدول عن طريق إبرام الاتفاقات السياسية والعسكرية، إذ توصّلت الولايات المتحدة الأمريكية والصين في عام 2015 لاتفاق خاص بالحروب السيبرانية بعدم شن أي هجمة سيبرانية، وأعلن الاتحاد الأوروبي في عام 2017 من أن شن أي هجمة سيبرانية من دولة عدائية على الاتحاد الأوروبي يعد (تصرف حرب) يجب التصدي له، رغم الهجمات السيبرانية بين الحين والآخر وإنكار كل طرف ذلك.[7]

واستكمالاً لمفهوم الحرب السيبرانية فيعرفها كل من (ريتشارد كلارك) و (روبرت كناكي) بأنّها: أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تدميرها, ويعرّفها (بولو شاكريان) على أنّها: استمرار او امتداد للسياسة عن طريق الاجراءات المتخذة في الفضاء السيبراني من دول أو فاعلين غير دوليين، إذ تشكّل تهديداً خطيراً للأمن القومي.[8]

فالحروب السيبرانية تتميز بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتع بها المهاجم

وتتميّز الحرب السيبرانيّة بمجموعة من الخصائص وهي[9]:-

1- هي حرب رقمية ذات تقنية متطورة، وإن قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي شكلت بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيسي لها.
2- حرب لا تناظرية: فلا تحتاج الدول الى تخصيص ميزانيات ضخمة لإنتاج أسلحتها أسوة بالأسلحة المستخدمة في النزاعات التقليدية ذات الكلفة العالية وانها ذات تكلفة متدنية نسبةً للأدوات اللازمة لشنّها.
3- تمتع المهاجم بأفضلية واضحة في حروب الانترنت على المدافع؛ فالحروب السيبرانية تتميز بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتع بها المهاجم بأفضلية من الصعب جدّاً على عقلية التحصّن لوحدها أن تنجح.
4- حرب هلامية الشكل والملمح: فهي متعددة بميادينها، متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوّراً وتبدلاً في الحياة المعاصرة للدول وهي تطال بتدميرها أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال.
5- إن الحرب السيبرانية تمتاز : بقوة تدميرية لا تصاحبها دماء وأشلاء، إذ يتضمّن التجسس ثم النسف لكن لا دخان ولا غبار فيتم التدمير بوابل من الفيروسات، كما ان انتشار الفضاء الالكتروني وسع دائرة استهداف المواقع بمستوياتها كافة.

(6)يحيى ياسين سعود، الحرب السيبرانية في ضوء القانون الدول الإنساني، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية), العدد 4، جامعة القاهرة – كلية الحقوق – فرق الخرطوم، 2018، ص6.

(7) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، العربي للنشر والتوزيع، ط1، القاهرة، 2019، ص114.

(8) إسماعيل زروقـــة، الفضاء السيبراني والتحول في مفاهيم القوة والـصـراع، مجلة العلوم القانونية والسياسية، منشورات جامعة الشهيد حمة لخضر بالوادي، المجلد 10، العدد1، الجزائر، 2019، ص12.

(9) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد 57، جامعة النهرين – كلية العلوم السياسية، 2019، ص 99 – 101.

وسنطرح **المفاهيم المقاربة** للحرب السيبرانية للضرورة العملية البحثية، وهي كالآتي:

1- الفضاء السيبراني (cyber space).

أصبح الفضاء السيبراني في الوقت الحاضر يمس جميع الأرواح وأصبح ضرورياً ويطلق عليه العالم الافتراضي لأنه غير موجود في الواقع المادي والناس في العالم الافتراضي يعيشون حياة افتراضية جنباً إلى جنب مع حياتهم الواقعية.[10]

ويعرف الفضاء السيبراني بأنّه عالم افتراضي يتشارك مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد، إذ تقوم العلاقة بين العالمين على نظرة تكاملية ويوصف بأنه الذراع الرابع للجيوش الحديثة الى جوار القوات البرية والجوية والبحرية.[11]

ويعرف الفضاء السيبراني بأنّه عالم افتراضي يتشارك مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد،

ويعرف أيضاً بأنّه المستودع الكبير الذي تجري فيه جميع عمليات التواصل الالكتروني عبر شبكات الحواسب، وهو منظومة من العناصر المتفاعلة فيما بينها والمتكونة من أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات.[12]

كما عرَّفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي بأنّه فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، وأنه لا يقتصر على شبكة الانترنت فقط وإنّما شبكات عالمية وخاصة أخرى مثل (/Gps/ AcARs/ swift/ psth).[13]

1- الهجمات السيبرانية (cyber attacks).

أصبحت الهجمات السيبرانية أكثر فأكثر حقيقة يومية خاصة مع التطور التكنلوجي المتسارع والتي تسمح للمخترقين من الاختراق بسهولة سواء من الدول او من غيرها.[14]

الهجمات السيبرانية بأنهّا الجهود الرامية الى تغيير، تعطيل او تدمير أنظمة الحاسوب او الشبكات أو المعلومات او البرامج الموجودة عليها

وتعرف الهجمات السيبرانية وفق ما تبنته القيادة الاستراتيجية الامريكية عام 2007 بأنّه تطويع عمليات نظام الكمبيوتر بهدف منع الخصم من الاستخدام الفعال لها فضلاً عن التسلل الى أنظمة المعلومات وشبكات الاتصال بهدف جمع البيانات التي تحتويها وحيازتها وتحليلها، وعرَّفته شميت (Schmitt) المتخصص في القانون الدولي الإنساني بأنه الهجوم السيبراني هو أي تصرف الكتروني دفاعي كان أو هجومي يتوقع منه وعلى نحو معقول في التسبب بجرح او قتل شخص او الحاق اضرار مادية او دمار بالهدف المُهاجَم.[15]

ويعرف (Mattew C.Waxman) الهجمات السيبرانية بأنهّا الجهود الرامية الى تغيير، تعطيل او تدمير أنظمة الحاسوب او الشبكات أو المعلومات او البرامج الموجودة عليها، والأضرار التي تسببها هذه الهجمات يمكن انْ تصيب شبكة

(10) - tim Jordan, cyber power: the culture and politics of cyber space and the internet, routledge, London, 1999, p 12.

(11) نـــورة شـلـوش، القرصنة الالكترونية في الفضاء السيبراني «التهديد المتصاعد لأمن الدول» ، مجلة مركز بابل للدراسات الإنسانية، المجلد8، الـعـدد2، جامعة بابل، 2018، ص190.

(12) محمد وائل القيسي، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو – معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، مركز الدراسات الإقليمية، السنة14، العدد44، نيسان، جامعة الموصل، 2020، ص 153 – 154 .

(13) تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي للدراسات، مركز حمورابي للبحوث والـدراسـات الاستراتيجية، العدد 33 – 34، السنة 8، شتاء -ربيع، بغداد، 2020، ص149.

(14)Andreea bendovschi, cyber – attacks – trends, patterns and security counter measures, arti_cle in procedia economics and finance, Elsevier, volume 28, 2015, p 2 – 3.

(15) زهراء عماد مجيد كلنتر، احمد عبيس نعمة الـفـتـلاوي، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 1، العدد 44، آذار، جامعة الكوفة – كلية القانون، 2020، ص 51 - 52.

الحاسوب او المرافق المادية او الأشخاص و تتراوح اضرار الهجمات السيبرانية من القرصنة الخبيثة وتشويه مواقع الانترنت الى دمار واسع النطاق للبنية التحتية العسكرية والمدنية المرتبطة بتلك الشبكات.[16]

2- الأمن السيبراني (cyber security)

إنّ الأمن السيبراني هو عبارة عن التقنيات الالكترونية المستخدمة لحفظ سلامة الشبكات والبرامج والبيانات من الوصول غير المصرح به.[17]

وإن الأمن السيبراني يهدف الى ضمان تحسين الأمن الذي من شأنه الدفاع عن المنظمات من التعرض لهجوم من قبل المتسللين عبر الشبكة العنكبوتية.[18]

وهذا مرده إلى أن العالم أصبح أكثر ارتباطاً بواسطة الشبكات العنكبوتية لتنفيذ المعاملات العامة ويقوم الأمن السيبراني بالحفاظ عليها.[19] وعليه فإنّ الأمن السيبراني وفق ما يراه الكاتبان (Pekka Nettaanmaki) و (Martti Lento) في كتابهما:

(cyber security: Analytics, technology and Automation)

بأنه مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات السيبرانية (قراصنة الكمبيوتر) وعواقبها وتنفيذ التدابير المضادة المطلوبة.[20]

3- القوة السيبرانية (cyber power)

تعرف القوة السيبرانية بأنّها القدرة على القيام بنشاط سيبراني مؤثر في الفضاء السيبراني، أو القدرة على استخدام الفضاء السيبراني لتحقيق مجموعة من الأهداف والتاثير على الأحداث, وتعرف أيضاً على أنها الموارد البشرية والمادية المتاحة ضمن بيئة استراتيجية يمكن استخدامها لإحداث تأثير في الفضاء السيبراني او من خلاله.[21]

4- الصراع السيبراني (cyber conflict)

تواجه الحكومات والمؤسسات الى هجمات مضادة من نوع آخر وهي الهجمات السيبرانية بسبب الارتباط الكبير بين دول العالم افتراضياً وضمن الفضاء السيبراني خاصة بعد ثورة المعلومات التي حفزت ذلك تدريجياً[22]، وهذا يدخل في مفهوم الصراع السيبراني الذي هو تعارض بين دول ما ضمن نطاق القدرات السيبرانية في الفضاء السيبراني من اجل تحقيق اهداف يسعى إليها أطراف الصراع.[23]

5- الدفاع السيبراني (cyber defence)

يعرف الدفاع السيبراني بأنه آلية دفاع لشبكة الكمبيوتر وتشمل الاستجابة للإجراءات الفعالة من اجل حماية البنى التحتية الحيوية فتأمين المعلومات والحفاظ عليها للمنظمات والهيئات الحكومية والشبكات الأخرى, ويركز الدفاع السيبراني على المنع والكشف، وتوفير الاستجابة في الوقت المناسب ضد الهجمات السيبرانية من اجل منع العبث بالبنى التحتية او المعلومات.[24]

6- الردع السيبراني (cyber deterrence)

يعرف الردع السيبراني بأنّه التلصص الإعلامي والاستعراض التكنلوجي والمحاكاة

(16) حيدر أدهم الطائي، علي محمد كاظم، المشاركة المباشرة للهية الجماعية في الهجمات السيبرانية، مجلة كلية الحقوق، المجلد 21، العدد 2، جامعة النهرين، 2019، ص30.

(17) p.s. seemma, s.nandhini, m.sowmiya, over view of cyber security, international journal of advanced research in computer and communication engineering, article in ijarcce, volume 7, issue 11, November, 2018, p2.

(18) darko galince, darko moz_ink and boris guberina, cyber security and cyber defence: national level strategic approach, journal for control, measurement, electronics, computing and communications, article in automatika, volume 58, number 3, july, 2017, p3.

(19) g.n reddy, g.j.u.reddy, a study of cyber security challenges and its emerging trends on latest technologies, computer science, arxiv, 8 February, 2014, p 5.

(20) صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، السنة 12، العدد 62، جامعة النهرين، كلية العلوم السياسية، 2020، ص277.

(21) _Robert "Jake" bebber, cyber power and cyber effectiveness: an analytic framework, comparative strategy an international journal, routledge, taylor & francis group, volume 36, November 5, 2017, p 4.

(22) Athina karatzogianni, cyber conflict and global politics, Routledge ,London and new York, 2009, p 3.

(23) alexander kosenkov, cyber conflict a new global threat, future internet, mdpi, 8, 45, 2016, p1.

(24) darko galinec, darko moz_ink and boris, I bid, p 4.

الاستراتيجية لإنشاء صورة رقمية مفرطة لهيمنة دولة مّا سيبرانيّاً عبر نطاق الفضاء السيبراني لردع الخصم سيبرانيّاً.[25]

7- الاستراتيجية السيبرانيّة (cyber strategy)

هي تطوير وتوظيف القدرات اللازمة للعمل في الفضاء السيبراني متكاملة مع المجالات العملياتية الأخرى لتحقيق او دعم تحقيق الأهداف عبر عناصر القوة الوطنية وتعتمد الاستراتيجية السيبرانية على مزيج منظم من الغايات، والوسائل، والطرق لتحقيق اهداف الامن العسكري والسياسي والاقتصادي والمعلوماتي والوطني الأوسع من خلال الاعتماد على القدرات السيبرانية وتوفير الموارد والتكاليف الواجب اتخاذها لمواجهة المخاطر خاصة السيبرانية.[26]

المطلب الثاني: الحرب السيبرانية (الوسائل والأهداف)

تستخدم في الحرب السيبرانية وسائل محددة التي هي كيانات برمجية ضارة يتم نشرها لتحقيق اهداف منها الحاق الضرر بالخصوم والشبكات العنكبوتية وأنظمة الكمبيوتر التي تهدد سلامة والوظيفة الرقمية للأنظمة التي تمكن الدوائر العالمية من الاتصال والتبادل مع إمكانيات التأثير على النظام الاجتماعي والاقتصادي والسياسي.[27]

الهجمات السيبرانية بأنهّا الجهود الرامية الى تغيير، تعطيل او تدمير أنظمة الحاسوب او الشبكات أو المعلومات او البرامج الموجودة عليها

وانَّ وسائل الحرب السيبرانية والأسلحة المستخدمة فيها تتنوع مثل الفيروسات والديدان والبرمجيات الخبيثة التي يتم تصميمها عبر أكواد وبرامج كمبيوتر من أجل شن هجمات سيبرانية على أهداف عسكرية ومدنية تهدف الى تدمير النظم والأجهزة المادية والبرمجيات والتي تؤدي بالنهاية الى تدمير البنى التحتية للدول او الفواعل من غير الدول عبر التجسس وغيرها من الأعمال التخريبية التي تهدد الأمن والسلم الدوليين جراء تلك الأعمال.[28]

وطرح (توماس ريد) أربع وسائل أو أسلحة أساسية توظف من أجل تحقيق هدف الحرب السيبرانية وهي[29]:

1- **لغة الاستعلام الهيكلية:** وهي الحقن أو البرمجة النصية للمواقع من أجل تشويه صفحات الويب او اتلافها اذ يستخدم هذا الشكل من الفيروسات حيال المواقع لبضع ساعات او أيام ومثال على ذلك ما حدث في عام 2005 عندما قام القراصنة الروس بتشويه العديد من الواقع الحكومية.

تؤدي هجمات الحرمان الموزع دوراً رئيسياً في الحرب السيبرانية وهي محاولة لجعل مورد الحاسوب غير متوفر للمستخدمين المقصودين

2- **الحرمان من خدمة الموزع:** تؤدي هجمات الحرمان الموزع دوراً رئيسياً في الحرب السيبرانية وهي محاولة لجعل مورد الحاسوب غير متوفر للمستخدمين المقصودين به من خلال هجمات منسقة لأجهزة الحاسوب أو أجهزة أخرى و إنَّ الهدف الرئيسي لهذه الوسيلة او الأسلوب هو التعطيل المؤقت للخدمة.

3- **الاختراقات:** عنَّ هذا الأسلوب أو الوسيلة يكون أشد من التشوهات والتخريب

(25) Stefan soesanto and max smeets, cyber deterrence: the past, present and future, center for security studies (css), Swit_zerland, 2021, p 5.

(26) زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، مصدر سبق ذكره، ص 92.

(27) tim stevens, cyber weapons: power and the governance of the invisible ,article in international politics, springer, king's collage London, may, 2018, p 1.

(28) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، مصدر سبق ذكره، ص115.

(29) زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، مصدر سبق ذكره، ص 98 – 99.

فيما يتعلق بالضرر طويل الأجل، إذ يعتمد على برامج فعالة لسرقة المعلومات الحساسة من المواقع الأمنية وتكون لهذه الأساليب آثار مدمرة ومهددة للمصالح الوطنية والقومية للدولة المستهدفة.

4- **التسلل:** حيث يستخدم ضمن هذا الأسلوب في الحرب السيبرانية أكثر البرامج الضارة من أجل اختراق الشبكات المستهدفة، ومن أهم أساليب التسلل هي: (القنابل المنطقية، الديدان، الفايروسات) التي تختلف عن الاختراقات من حيث شدّة تأثيرها، ويسبب هذا التسلل الى الحاق الضرر في الجهاز المضيف وارساله الى الخوادم البعيدة.[30]

وعليه سنطرح أيضاً أهم أنواع الأسلحة السيبرانية التي تستخدم كوسائل في الحرب السيبرانية ساعية لتحقيق هدفها وهي[31]:

1- **فايروسات الحاسوب (viruses):** وهي برمجيات خبيثة صنعت قصداً من أجل تغيير خصائص الملفات التي تصيبها لتقوم بتنفيذ بعض الأوامر إمّا بالإزالة او التعديل او الحذف او التخريب هدفها الأساس هو الحاق الضرر.

2- **الديدان(worms):** وهي برامج صغيرة تتكاثر بنسخ نفسها عن طريق الشبكات هدفها هو العمل التخريبي، مثال على ذلك قطع الاتصال بالشبكة او سرقة البيانات الخاصة وتمتاز بسرعة الانتشار ومن الصعوبة التخلص منها بسبب قدرتها على التلون والتناسخ والمراوغة مكانها الأساس هي حرب المعلومات وتستهدف الشبكات المالية مثل شبكات البنوك.

3- **أحصنة طـروادة (Trojan horses):** وهي شفرة او برنامج صغير يختبئ في برنامج كبير من البرامج ذات الشعبية العالية، إذ يقوم على نشر دودة او فايروس، اذ يعمل دائماً مسح آثاره ويهدف على اضعاف قوى الدفاع ليسهل اختراق جهاز الحاسوب وسرقة بياناته.

4- **القنابل المنطقية (logic bombs):** وهي برمجيات يتم زرعها داخل النظام او البرنامج إذ أنَّ البرنامج او الجهاز مصاباً منذ البدء بالبرنامج الضار أي بالسلاح السيبراني اذ يبدأ عمل البرنامج الضار تحت ظروف معينة تكون في المحصّلة والهدف النهائي هو التحكم في الجهاز بصورة تامة او اتلافه.

5- **البرمجيات الخبيثة مثل «اريـد البكاء» (wanna cry):** وقد تميزت هذه البرمجيات بأنها تستهدف الكيانات الاقتصادية وليست الافراد وذلك لأنّ هذه المؤسسات هي الأقدر على دفع الفدية، أو نلاحظ في عام 2017 قام مجموعة من القراصنة المجهولين بشن هجوم ضار باسم (اريد البكاء / wanna cry) اذ تكمن الهجوم من إصابة اكثر من (200.000) مائتي ألف ضحية في أكثر من مائة وخمسين دولة خلال أول (48 ساعة) من الهجوم، والشيء المخيف والمقلق انَّ هذه الهجمة اعتمدت على أسلحة وثغرات تم تسريبها من وكالة الأمن القومي الأمريكي، اذ اشارت بعض التحليلات الى ضلوع الوكالة في تطوير هذه البرامج قبل انْ تتم سرقتها منها وتسريبها.

(30) jeetendra pande, introduction to cyber security (fcs), published by: uttarkhand open university, haldwani, 2017, p 19.

(31) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، مصدر سبق ذكره، ص 116 – 119.

6- **الفايروسات الالكترونية (electronic viruses):** تتنوع الأسلحة السيبرانية من نماذج من الفايروسات وهي فيروس (ستاكس نت / stuxnet) وهو اخطر أنواع الأسلحة السيبرانية التي تم اكتشافها في عام 2009 ومثّل نقلة نوعية في خطورة الحرب السيبرانية من خلال (ستاكس نت) انتقلت الحرب من تدمير البيانات وسرقتها الى تدمير المكونات المادية نفسها ونظم التشغيل وليس فقط البيانات,وأيضاً فيروس (دوكو/ duqo) وهو فيروس تم اكتشافه في عام 2011 بواسطة معامل التشفير والأمن الالكتروني (crysys lab) التابع لجامعة بودابست.

فيروس (ستاكس نت / stuxnet) وهو اخطر أنواع الأسلحة السيبرانية التي تم اكتشافها في عام 2009

وفيروس (فليم / flame) الذي تم اكتشافه في عام 2012 بواسطة فريق الاستجابة والطوارئ الإيراني فضلاً عن شركة كاسبر سكي ومعمل التشفير والأمن الالكتروني التابع لجامعة بودابست، إذ أصدرت الأمم المتحدة تحذيراً اعتبرته الأكثر خطورة وتعقيداً بسبب أهدافه التدميرية.

فضلاً عن ما تقدم فإن أهداف الحرب السيبرانية ليس لأضرارها حدود، فبإمكانها التسبب بانفجارات في مخازن الوقود والمحطات النووية وكافة المراكز الحيوية او تعطيل وسائل النقل برّاً وبحراً وجوّاً أو تغيير مسار الرحلات، فضلاً عن تعطيل أنظمة الطاقة وقطع الكهرباء عن مدن بأكملها.[32]

(32) غيث علاو، الهجمات السيبرانية أكبر من حروب نووية بوسائل الكترونية، موقع جادة ايران، بتاريخ 5/يوليو/2020، الشبكة الدولية للمعلومات: https://www.jadehiran.com/archives/16835

المبحث الثاني: الحرب السيبرانية (الولايات المتحدة الأمريكية وإيران)

تعد الحرب السيبرانية بين الولايات المتحدة الامريكية وايران احدى الأدوات الفاعلة والمؤثرة بين الطرفين الساعية لتدمير وانهاك اكبر قدر ممكن من المواقع الحيوية والبنى التحتية لكلا الطرفين عبر طرح كل طرف استراتيجية سيبرانية خاصة به نابعة من توجهاتهما الاستراتيجية عبر استخدام الهجمات السيبرانية الساعية لتحقيق اهداف كل طرف عبر الفضاء السيبراني ساحة الصراع، وعليه سنطرح في هذا المبحث مطلبين وهما:

المطلب الأوّل: استراتيجية الهجمات السيبرانية للولايات المتحدة الامريكية حيال ايران.

المطلب الثاني: استراتيجية الهجمات السيبرانية الإيرانية حيال الولايات المتحدة الامريكية.

تعد الولايات المتحدة الامريكية من القوى العظمى والمستوى الأول في المجال السيبراني إذ انَّها قادرة على تنفيذ مهام معقدة للغاية من الهجمات السيبرانية السرية

المطلب الأوّل: استراتيجية الهجمات السيبرانية للولايات المتحدة الامريكية حيال ايران.

تعد الولايات المتحدة الامريكية من القوى العظمى والمستوى الأول في المجال السيبراني إذ انَّها قادرة على تنفيذ مهام معقدة للغاية من الهجمات السيبرانية السرية باستخدام برامج ضارة ضمن الأهداف الموجهه لديها.[33] إذ تعود بداية الهجمات السيبرانية للولايات المتحدة الأمريكية حيال إيران الى حملة سرية تدعى (عملية

(33) mattias schulze, joseph kerscher, Paul bochtler, cyber escalation: the conflict dyad USA / Iran as a test case, working paper, swp, german institute for international and security affairs, December, 2020, p 8.

الألعاب الأولمبية) التي انطلقت في عام 2006 تحت إدارة الرئيس الأمريكي الأسبق (جورج دبليو بوش) من أجل استهداف أنظمة الكمبيوتر للحكومة الإيرانية وقدرات إيران النووية.[34] وقد وسع الرئيس الأمريكي الأسبق (باراك أوباما) هذه الحملة لتضم الأسلحة السيبرانية ضد منشآت التخصيب النووية الإيرانية.[35]

وفي عام 2010 اعترف المسؤولون الإيرانيون بأنّ أجهزة الكمبيوتر في محطة بوشهر النوويّة قد أصيبت بفايروس له تأثير بالغ أدى الى توقف تخصيب اليورانيوم في محطة (نطنز) النووية بالكامل جراء الفايروس الموجه لها المعروف باسم (ستوكسنت) التي اتهمت ايران الولايات المتحدة الامريكية بالوقوف وراءه.[36]

وقد أكد نائب مدير الوكالة الدولية للطاقة الذرية السابق (اولي هينونن) انَّ الفايروس الالكتروني المعروف باسم (ستوكسنت) قد ولّد مشاكل تقنية أثرت على البرنامج النووي الإيراني مما أدى الى إيقاف الآلاف من أجهزة الطرد المركزي الخاصة بتخصيب اليورانيوم، وأظهر بحث أجرته شركات الأمن المعلوماتي أنَّ (60%) من الأجهزة المصابة بفايروس (ستوكسنت) توجد في ايران، وعليه جاء تقرير للوكالة الدولية للطاقة الذرية نشر في أيلول عام 2010 أنَّ ايران فصلت (160) جهاز طرد مركزي عن شبكة التحكم.[37]

ورغم قدرته الفريدة على الانتشار ومعدل الإصابة على نطاق واسع إلّا أن برنامج (ستوكسنت) يلحق ضرراً ضئيلاً او معدوماً لأجهزة الحاسوب غير المستخدمة في تخصيب اليورانيوم، أمّا في حالة ايران فإنّ الفايروس (ستوكسنت) غيّر برمجة أجهزة التحكم المنطقي القابلة للبرمجة، ممّا أسفر عن دوران أجهزة الطرد المركزي سرعة كبيرة جدّاً لمدة طويلة مما أدى الى تلف وتدمير المعدات الحساسة في الهجوم، التي دخلها خلال مدة (13) يوماً في سجل بيانات أجهزة الطرد المركزي بتسجيل (سلوك طبيعي) وبعد تلك المدة الـ (13) يوماً بدأ التعرف على أجهزة الطرد المركزي مؤدّياً الى اهتزازها مسببة ارتفاع درجة الحرارة المؤدية في النهاية الى تعطل المعدات الحساسة كما اسلفنا.[38]

أمّا خلال فترة إدارة الرئيس الأمريكي السابق (دونالد ترامب) فقد طرح استراتيجية سمّيت بـ (الاستراتيجية القومية السيبرانية) في عام 2018 التي عدت الفضاء السيبراني أمراً أساسيّاً وأنه جزء لا يتجزّأ من جوانب الحياة الامريكية ومع أصدار هذه الاستراتيجية يكون لدى الولايات المتحدة الامريكية القوة في الدفاع عن أمنها السيبراني بشكل خاص وأمنها القومي بشكل عام التي ركزت على ما يلي[39]:

1- الدفاع عن الوطن من خلال حماية الشبكات و الأنظمة والبيانات.
2- تعزيز الدفاع الامريكي من خلال رعاية وتعزيز اقتصاد رقمي آمن ومزدهر مع ابتكار محلي قوي.
3- الحفاظ على السلام والأمن من خلال تعزيز قدرة الولايات المتحدة الأمريكية بالتنسيق مع الحلفاء والشركاء لردع ومعاقبة الذين يستخدمون الأدوات السيبرانية من أجل الإضرار بالأمن القومي الأمريكي.

(34) Andrew Hanna, the invisible U.S. – Iran cyber war, The iran primer, united states institute of peace , 29/july/2021,international information network :
https://www.iranprimer.usip.org/blog/2019/oct/25/invisible

(35) وقائع الحرب السيبرانية «الخفية» بين الولايات المتحدة وإيران، الحرة، ترجمات – واشنطن، بتاريخ 25/فبراير/2021، الشبكة الدولية للمعلومات:
https://www.alhurra.com/iran/2021/02/25

(36) marie baezner, Patrice robin, stuxnet, publisher(s) :center for security studies (css), issue 4, E t H Zurich, Switzerland, 2017, p 9.

(37) فايروس ضرب برنامج ايران النووي، عربي bbc news، بتاريخ 22/ نوفمبر/ 2010، الشبكة الدولية للمعلومات:
https://www.bbc.com/arabic/middleeast/2010/11/

(38) كيف هوجمت المنشأة النووية الإيرانية في «نطنز» المعزولة من الانترنت، العربية، بتاريخ 6/ يوليو/2019، الشبكة الدولية للمعلومات:
https://www.alarabnet/iran/2019/07/06/

(39) president Donald J.Trump, national cyber strategy of the united states of American, the white house, Washington, dc, September, 2018, p 3.

4- توسيع النفوذ الأمريكي لتوسيع المبادئ الأساسية لوجود انترنت آمن وموثوق وقابل للتشغيل المتبادل.

5- تعزيز قدرات الشركاء في مجال الأمن السيبراني للحفاظ على النفوذ الأمريكي ضد المنافسين الإقليميين والعالميين.[40]

(40) president Donald J. Trump, Ibid, p 26.

وأكد (جون بولتون) مستشار الرئيس الأمريكي (دونالد ترامب) سابقاً أن هذه الاستراتيجية هي أول استراتيجية مفصلية بالكامل خلال السنوات الـ (15) عشر الماضية إذ دخلت حيّز التنفيذ وهذه الاستراتيجية جاءت في أعقاب قرار (ترامب) لإلغاء قواعد حدّدها سلفه (أوباما) قد قيَّد العمليات السيبرانية

أن أي دولة تقوم بعمل أو نشاط سيبراني ضد الولايات المتحدة الامريكية يجب أن تتوقع أننا سنرد بطريقة هجومية ودفاعية فعالة ومؤثرة

وأكد (جون بولتون): «أن أي دولة تقوم بعمل أو نشاط سيبراني ضد الولايات المتحدة الامريكية يجب أن تتوقع أننا سنرد بطريقة هجومية ودفاعية فعالة ومؤثرة» ، وشددت وزيرة الأمن الداخلي الأمريكي (كيرستين نيلسن) على تحديث قوانين المراقبة الالكترونية وجرائم الكمبيوتر بهدف مواصلة ومواكبة التطورات السريعة في العالم الرقمي.[41]

(41) استراتيجية أمريكية شرسة للأمن الالكتروني تستهدف الصين وروسيا، عربية sky news، ابوظبي، بتاريخ 21/سبتمبر/2018، الشبكة الدولية للمعلومات: https://www.skynewsarabia.com/world/1184165

وضمن الحفاظ على الأمن القومي الأمريكي أمر الرئيس الأمريكي السابق (دونالد ترامب) بتوسيع سلطة وكالة المخابرات المركزية (CIA) بأن تشن هجمات سيبرانية وأنَّ تكثف جهودها السيبرانية ضد إيران.[42]

(42) ـوقائع الحرب السيبرانية «الخفية» بين الولايات المتحدة وإيران، المصدر نفسه.

وأكّد الرئيس الحالي (جو بايدن) قبل تنصيبه رئيساً للولايات المتحدة الأمريكية في 20/يناير/2021 , إذ أكّد في ديسمبر/ 2020 أن الأمن السيبراني هو أولويّة قصوى لإدارته القادمة وضمن خطته على إثر تعرّض الولايات المتحدة الأمريكية لهجوم سيبراني واسع ووفقاً لصحيفة (وول ستريت جورنال) الأمريكية أن الحواسب المخترقة تواجدت بأكثر من (20) مؤسسة أمريكية وانتقد (جو بايدن) (دونالد ترامب) باعتباره رئيساً للولايات المتحدة الأمريكية لغاية قبل التنصيب أنه مقصّراً في تعزيز الأمن السيبراني وأنّه كان غير يقظ في ذلك وأنّه سيأخذ الأمر بجدية خلال ادارته القادمة تعزيزاً وحمايةً للأمن القوميً الأمريكي من خلال الرد على الهجمات السيبرانية ضد منطلقيها.[43]

(43) مواجهة 2020 خطة بايدن للحرب السيبرانية، قناة الحرة، بتاريخ 29/ديسمبر/2020، الشبكة الدولية للمعلومات: https://www.alhurra.com/episode/2020/12/29/801626

وفي مارس/ 2021 بدأت استراتيجية (جو بايدن) في الفضاء السيبراني والحرب السيبرانية ولمواجهة التهديدات السيبرانية بالتشكل، إذ تعكس الاستراتيجية السيبرانية لإدارة (جو بايدن) الركائز الآيديولوجية والجيوسياسية والتكنلوجية والدبلوماسية لرؤية الرئيس (جو بايدن) الشاملة للسياسة الخارجية والأمن القومي للولايات المتحدة الأمريكية، وأكد وزير الخارجية الامريكي (انتوني بلينكن) مع الرئيس (جو بايدن) أن الأنشطة السيبرانية المناهضة للولايات المتحدة الامريكية والضارة لها تتوجب علينا أنَّ نعيد النظر في علاقة الديمقراطية بالفضاء السيبراني وهو جزء من مشروع تجديد الديمقراطية وتخطط إدارة (جو بايدن) لتحسين الدفاعات السيبرانية وردع العمليات السيبرانية المعادية ومواجهتها.[44]

(44) David p. fidler , america's place in cyber pace: the biden administration cyber strategy. Takes shape, council foreign re_lation, foreign affairs, march, 11, 2021, international information network: https://www.cfr.org/blog/americas_place_cyberspace

وتأكيداً لاستراتيجية (جو بايدن) لتعزيز الأمن السيبراني ومواجهة التهديدات السيبرانية كانت قمة (جو بايدن) مع الرئيس الروسي (فلاديمير بوتين) في 16/ يوليو/2021 حاضرة فيها الهجمات السيبرانية في اعلى قمة المحادثات بين الطرفين ويجب ابعاد شبح الخطر النووي السيبراني ومواجهة الدول التي تنطلق منها الهجمات السيبرانية أو أنها تشكل مصدر تهديد سيبراني لها وشيك في إشارة لإيران، ناهيك انه تم ذكر كلمة (سيبراني) (25 مرة) في البيان النهائي لقمة دول شمال الأطلسي (الناتو) التي عقدت في الشهر نفسه من هذا العام والتي أكدت على الهجوم السيبراني قد يكون سبباً لتفعيل البند الخامس من ميثاق الحلف، والذي يعد أي هجوم على عضو في الحلف بمثابة هجوم على الحلف بأكمله وهذا يصب في مصلحة استراتيجية الولايات المتحدة الامريكية السيبرانية باعتبارها عضواً في حلف شمال الاطلسي.[45]

وفي يوليو/2021 أكد الرئيس الأمريكي (جو بايدن) أنه من المنطقي أن تشن الولايات المتحدة الامريكية هجمات سيبرانية على الخوادم المستخدمة في الهجمات السيبرانية ضد الولايات المتحدة الأمريكية وفي السياق نفسه أكد مسؤول أمريكي رفيع في الإدارة الأمريكية أن الولايات المتحدة الامريكية ستتخذ الخطوات الضرورية لحماية بنيتها التحتية وأمنها القومي من الهجمات السيبرانية.[46]

فضلاً عمّا تقدم من طرح للتوجهات الاستراتيجية للولايات المتحدة الامريكية السيبرانية خلال الادارة الحالية والادارات السابقة حيال الدول التي تشكل منطلق للهجمات السيبرانية ضدها وبصورة خاصة ايران، سنطرح الهجمات السيبرانية للولايات المتحدة الامريكية حيال ايران، وكما في الجدول الآتي:-

(45) ريتشارد ووكر، قمة بايدن وبوتين ... وشبح الخطر النووي السيبراني، موقع DW، بتاريخ 16/ يونيو/2021، الشبكة الدولية للمعلومات: https://www.dw.com/ar/%D,%85%D8

(46) بايدن: من المنطقي مهاجمة الخوادم التي تنطلق منها الهجمات السيبرانية، موقع RT عربي، بتاريخ 9/يـولـيـو/2021، الشبكة الدولية للمعلومات: https://www.arabic.rt.com/world/1250247

جدول رقم (1) يوضح الهجمات السيبرانية للولايات المتحدة الامريكية حيال إيران

ت	تاريخ الهجمات السيبرانية	نوع الهجمات السيبرانية
1	يوليو/2010	تم التعرف على فايروس (stuxnet) إذ أظهرت التحليلات الفنية اللاحقة أن هذا الفايروس تم انشاؤه لاستهداف المنشآت الصناعية الايرانية وخاصة النووية منها من قبل الولايات المتحدة الامريكية كما أدى إلى تدمير أكثر من (1000) جهاز طرد مركزي وإعاقة التقدم النووي لأكثر من عام.
2	25/سبتمبر/2010	قالت منظمة الطاقة الذرية الإيرانية أنها تحارب البرمجيات الخبيثة التي تستهدف منشآتها النووية وقال مسؤول إيراني أن (30) ألف جهاز كمبيوتر أصيب بفايروس ستوكسنت.

3	25/ابريل/2011	اكتشفت وكالة الدفاع السيبرانية الايرانية فيروساً يطلق عليه اسم (النجوم) والذي تم تصميمه للتسلل إلى منشآتها النووية وإلحاق الضرر بها.
4	23/ابريل/2012	اجبرت الهجمات السيبرانية ايران على ايقاف العديد من محطات النفط وانتشر الفيروس الملقب (بالمسحة) عبر وزارة النفط الايرانية وشركة النفط الوطنية الايرانية.
5	9/مايو/2012	أقرّت إيران بأن فيروساً يطلق عليه اسم (فليم/ flame) اصاب اجهزة الكمبيوتر الحكومية وكان قادراً على سرقة البيانات.
6	19/مايو/2012	قال مسؤولون غربيون لصحيفة واشنطن بوست انَّ الولايات المتحدة الامريكية و(إسرائيل) قد نشرتا فيروس (فليم / flame) لجمع معلومات استخبارية عن شبكات الكمبيوتر الايرانية من أجل الاستعداد لحملة حرب سيبرانية.
7	سبتمبر/2018	سمحت ادارة دونالد ترامب لوكالة المخابرات المركزية الامريكية بشن هجمات سيبرانية واسعة ضد البنية التحتية الحيوية الايرانية.
8	ابريل/ 2019	تسبب اختراق سيبراني لمراكز البيانات الايرانية في ترك العلم الامريكي على شاشات الكمبيوتر الايرانية الى جانب رسالة بعدم التدخل في الانتخابات الامريكية.
9	17/يونيو/2019	اكتشفت طهران شبكة تجسس سيبرانية تديرها وكالة المخابرات المركزية الامريكية وفككتها، وهذا نوع من التدخل السيبراني الموجه ضد ايران.
10	20/يونيو/2019	شنت الولايات المتحدة الامريكية هجوماً سيبرانياً على ايران بعد هجمات ايران على ناقلات النفط في مضيق هرمز واسقاط طائرة امريكية بدون طيار وقال مسؤولون امريكيون أن هذه الهجمات مسحت البيانات المستخدمة للتخطيط لهجمات الناقلات.
11	26/يونيو/2019	ابلغت (net black) عن تعطل واسع النطاق للأنترنت في ايران.
12	سبتمبر/2019	شنت الولايات المتحدة الامريكية هجوماً سيبرانياً على ايران ردّاً على هجوم بطائرة بدون طيار على منشآت سعودية وقال مسؤولون امريكيون ان هذه الهجمة استهدفت قدرة ايران على نشر الدعاية.

13	25/يناير/2020	منعت الولايات المتحدة الامريكية الوصول الى (.farsnews com) وهو عنوان الويب باللغة الانجليزية لوكالة انباء فارس التابعة للحرس الثوري.
14	8/فبراير/2020	ذكرت ايران انَّ الاتصال الوطني بالانترنت فيها انخفض الى (75%) بعد أنَّ قامت ايران بتفعيل (net black) الاجراءات السيبرانية المضادة لهجوم (DDOS).
15	14/فبراير/2020	ألقى رئيس منظمة الدفاع المدني الايرانية باللوم على الولايات المتحدة الامريكية في هجوم سيبراني (DDOS) ادى الى انقطاع الخدمة لساعات.
16	7/اكتوبر/2020	صادرت الولايات المتحدة الامريكية (92) اسم مجال تستخدمها ايران ضدها وعلى أنَّها منافذ اخبارية حقيقة لكنها وفق ما رأت الولايات المتحدة الامريكية أنَّها تستهدفها لنشر الدعاية الايرانية.
17	15/اكتوبر/2020	أكدت ايران أنَّ هجومين سيبرانيين استهدفا اهداف حكومية في الفترة من (12 الى 13 اكتوبر) وقالت هيئة الموانئ الايرانية أنَّها احبطت هجوماً سيبرانياً على الانظمة الالكترونية للوكالة وقامت وكالات عدة تعليق الخدمات مؤقتاً واجرت اختبارات فنية بعد الابلاغ عن الهجمات.
18	3/نوفمبر/2020	استهدفت القيادة السيبرانية الامريكية ووكالة الامن القومي الامريكي قراصنة ايرانيين قبل الانتخابات الرئاسية الامريكية.
19	4/نوفمبر/2020	اغلقت الولايات المتحدة الامريكية (29) موقعاً على شبكة الانترنت تستخدمها ايران بهدف التأثير على سياسة الولايات المتحدة الامريكية والرأي العام.
20	23/فبراير/2021	ازال موقع (تويتر) (238) حساباً يعمل من ايران بعد استكمال التحقيق عن التدخل الايراني في الانتخابات الرئاسية الامريكية عام 2020.
21	22/يونيو/2021	صادرت الولايات المتحدة الامريكية وهذا يقع ضمن الحرب السيبرانية ضد ايران (30) عنواناً على شبكة الانترنت تابعة لإيران بما في ذلك محطة الاذاعة الرائدة (برس تي في) مع (33) موقعاً على الانترنت على أنَّها تنفذ حملات تضليل وتأثر داخل الولايات المتحدة الامريكية.

الجدول من إعداد الباحث بالاعتماد على المصادر الآتية:

Sources:

1- Andrew Hanna, the invisible U.S. – Iran cyber war, The iran primer, united states institute of peace , 29/july/2021, p-4-8: https://www.iranprimer.usip.org
2- Michael Connell, deterring Iran; use of offensive cyber: a case study, report C N A, Analysis and solutions, Washington, october2014 , p – 5 - .
3- Iran's cyber attacks capabilities, king Feisal center for research and Islamic studies, special report, January, 2020, p- 10.
4- Collin Anderson, Karim Sadjad pour, Iran's cyber threat: espionage, sabotage, and revenge, Carnegie endowment for international peace, Washington, 2018, p – 9.

وللتوضيح اكثر عن مستوى وعدد الهجمات السيبرانية للولايات المتحدة الامريكية حيال ايران ضمن استراتيجيتها السيبرانية، سنطرح مخططاً بيانياً يوضح ذلك، وكالآتي:

مخطط رقم (1) يوضح مستوى وعدد الهجمات السيبرانية بيانياً للولايات المتحدة الامريكية حيال ايران.

المخطط البياني من اعداد الباحث، بالاعتماد على المصادر الآتية:

Sources:

1- Idrees ali, phil stewart, exclusive: us. Carried out secret cyber strike on iran in wak of Saudi oil attack: official – 16/ Octo-

ber/2019;
1. https://www.reuters.com/article/us-usa-iran.
2- Us launched cyber – attack on iran weapons systems , 23/ june/2019:
2. https://www.bbc.com/news/world-us-canada.
3- Andrew Hanna, the invisible U.S. – Iran cyber war, The iran primer, united states institute of peace , 29/july/2021, p-4-8: https://www.iranprimer.usip.org
4- Collin Anderson, Karim Sadjad pour, Iran's cyber threat: espionage, sabotage, and revenge, Carnegie endowment for international peace, Washington, 2018, p – 9.

المطلب الثاني: استراتيجية الهجمات السيبرانية الايرانية حيال الولايات المتحدة الامريكية

عملت ايران لبناء قدرات سيبرانية واستطلاعية لتحييد القدرات التقنية العالمية لمنافسيها في منطقة الشرق الاوسط وخاصة الولايات المتحدة الامريكية من خلال الاستفادة من الثورة التقنية قليلة الكلفة والتي يمكن الحصول عليها واستعمال تلك القدرات لتعزيز أمنها السيبراني وشن الهجمات السيبرانية ضد اعدائها، وقد اعتمدت ايران استراتيجية سيبرانية تم الاعداد لها والتجهيز منذ سنوات عدة ووفق هذه الاستراتيجية تقود مؤسسة الحرس الثوري وقوات الباسيج القوة شبه العسكرية الايرانية البالغ تعدادها ما يقارب (900.000) تسعمائة ألف التابعة للحرس الثوري الايراني مع الفاعلين الرقميين الآخرين يشكلون كياناً افتراضياً تأسس منذ العام 2005 واطلق عليه اسم (جيش فضاء ايران السيبراني) الذي يعد أحد الأدوات الرقمية الفاعلة التي تستخدمها ايران لشن هجمات سيبرانية ضد الدول التي تقف عائقاً امام البرنامج النووي الايراني وتطوير الصواريخ الباليستية أو في المجالات الاستخبارية وجمع المعلومات وخاصة الولايات المتحدة الامريكية.[47]

اعتمدت ايران استراتيجية سيبرانية تم الاعداد لها والتجهيز منذ سنوات عدة

وأخذت عقيدة الأمن السيبراني تفرض نفسها في اطار استراتيجية الأمن القومي الايراني بشكل عام وأنَّ هذه العقيدة تستند على ركيزتين مهمتين: **الركيزة الأولى:** تتمثّل بحماية الأمن الوطني الايراني من خلال بناء بنية تحتية علمية تكنلوجية واستخبارية تستند على استراتيجية وقائية في الدفاع واستراتيجية استباقية في الهجوم في المجال السيبراني. **أمّا الركيزة الثانية:** فتتمثّل بتطوير العديد من المفاهيم والتقاليد القتالية السيبرانية عن طريق تشكيل شبكة معقدة من الجيوش السيبرانية القادرة على شن هجمات سيبرانية متعددة على اهداف محددة في آن واحد, فضلاً عن تفعيل قدراتها الاستخبارية في نشر المعلومات المضللة واجهاض المسيرات

(47) احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران وإسرائيل، مجلة الدراسات الإيرانية، المعهد الدولي للدراسات الإيرانية، السنة 4، العدد 12، اكتوبر ,المملكة العربية السعودية ، 2020، ص 68 – 69.

المناهضة لإيران، وفي مايو/2009 ادخلت شركة (American security) اسم ايران بين الدول الخمسة التي تتمتع بأقوى قدرات انترنت في العالم.[48]

وتتكون القدرات السيبرانية الايرانية من قدرات بشرية ومادية ذات كفاءة عالية المستوى في المجال السيبراني ترتبط بأعلى المستويات في الدولة، وهي[49]:

1- المجلس الأعلى للسايبر.

وتم تشكيله بأمر من المرشد الأعلى (علي خامنئي) عام 2012، ويضم في عضويته المسؤولين في الجهات الحكومية الرئيسة برئاسة رئيس الجمهورية ويتولى الاشراف على جميع الجهات التي لها علاقة بالمجال السيبراني ويحدد السياسات ومجالات العمل.

2- قيادة الدفاع السايبر.

وظيفتها دفاعية تهدف لحماية المنشآت الوطنية ضد أي هجوم سيبراني وتتبع الدفاع المدني الذي يعد فرعاً من أفرع القوات المسلحة الايرانية.

3- الجيش السيبراني الايراني.

ويهتم بالجانب الهجومي في المجال السيبراني ويتبع لقيادة الحرس الثوري/ القوات السيبرانية، ويضم خبرات عالية المستوى في مجال تقنية المعلومات لمهاجمة وسائل الإعلام ومصالح الدول الغربية والمعادية وخاصة الولايات المتحدة الامريكية وأيضاً جمع المعلومات.

4- دعم الفاعلين المعلوماتيين.

يعمل الكثير من الفاعلين السيبرانيين تحت مظلة النظام الايراني في الفضاء الرقمي الايراني، وعمدت ايران الى تشكيل شبكة كيانات رقمية من أجل صد الهجمات السيبرانية من القوات الدولية المنافسة وشن الهجمات السيبرانية أيضاً خاصة ضد الولايات المتحدة الامريكية.

وعمدت ايران الى تشكيل شبكة كيانات رقمية من أجل صد الهجمات السيبرانية من القوات الدولية المنافسة

وبدأت الهجمات السيبرانية الايرانية ضد الولايات المتحدة الامريكية في عام 2009 عندما قام (الجيش السيبراني الايراني) بتشويه صفحة (تويتر) الرئيسية رداً على احتجاجات ما يسمى بـ (الثورة الخضراء) التي اندلعت في ايران احتجاجاً على اعادة انتخاب الرئيس الايراني الأسبق (محمود احمدي نجاد).[50]

وأصبحت ايران ذات هجمات سيبرانية فعالة خاصة بعد الهجوم السيبراني عليها من قبل الولايات المتحدة الامريكية بفايروس (ستوكسنت / stuxnet) في عام 2010 اذ تحسنت تلك القدرات السيبرانية بشكل مطرد واعتبرت ايران قوة سيبرانية من الدرجة الثالثة كونها قادرة على شن هجمات اكثر تعقيداً وتدميراً خاصة ضد الولايات المتحدة الامريكية وفي الاستراتيجية الامنية الايرانية تعمل القدرات السيبرانية كركيزة فعالة خاصة بما تسمى (عقدة الردع) اذ تهدف القدرات السيبرانية الايرانية الى معاقبة السلوك غير المرغوب فيه للخصوم وردع الجهات التي تنوي القيام بتلك الهجمات[51].

(48) فـراس الياس، عقيدة الأمن السيبراني فـي إيــران ومـعـادلات المواجهة مع أمريكا، موقع ن بوست، بتاريخ 14/ أغسطس/ 2019، الشبكة الدولية للمعلومات: https://www.noonpost.com/content/28950

(49) -احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايـران و(إسرائيل)، مصدر سبق ذكره، ص 69.

(50) وقائع الحرب السيبرانية «الخفية» بين الولايات المتحدة الامريكية وايران، المصدر نفسه.

(51) mattias schulze, Josephine kerscher, paul bochtler, cyber escalation, Ibid, p 6 – 7.

وقد زادت ايران من مخصصات الميزانية للأنشطة السيبرانية بحوالي (12) ضعفاً للفترة (2013 - 2021) بنسبة (1200%) من أجل الارتقاء بالقدرات السيبرانية وتعزيزها وأن لإيران الاستعدادات الكاملة لتعطيل الخدمة ضد آلاف الشبكات الكهربائية ومحطات المياه وشركات الرعاية الصحية والتكنلوجية وخطوط الغاز والبترول في الولايات المتحدة الامريكية واختراق البريد الالكتروني والاتصالات ايضاً.[52]

وبعد تسلم الرئيس الايراني الجديد (ابراهيم رئيسي) السلطة في 3/اغسطس/2021 ورغم تعرض ايران للهجمات السيبرانية قبل تسلمه السلطة استطاعت ايران أنْ تصد تلك الهجمات والكشف عنها وتجسيدها وعدم التأثير على مجريات الاحداث بشكل عام، خاصة بعد احداث سفينة (أم تي مير سيرستريت) التابعة (لإسرائيل) إذ اشتد التصعيد الأمريكي – (الإسرائيلي) وبعض الدول الأوروبية منها لكن استطاعت ايران أنْ تقوض تلك الاحداث خدمة لمصالحها العليا وسترد على اي هجمات ضدها سواء كانت سيبرانية او تقليدية برد سيبراني او تقليدي ضمن ما تراه مناسباً.[53]

وفضلاً عمّا تقدم, سنطرح الهجمات السيبرانية الايرانية حيال الولايات المتحدة الامريكية استكمالاً لما تقدم من طرح التوجهات الاستراتيجية الايرانية السيبرانية، وكما هي:

جدول رقم (2) يوضح الهجمات السيبرانية الايرانية حيال الولايات المتحدة الامريكية

ت	تاريخ الهجمات السيبرانية	نوع الهجمات السيبرانية
1	18/سبتمبر/2009	قام الجيش السيبرانية الايراني بهجمة سيبرانية قامت بتشويه موقع (تويتر) الامريكي مما جعله غير متصل بالانترنت لعدة ساعات رداً على الموقف الامريكي من الاحتجاجات التي حدثت في ايران في عام 2009.
2	اغسطس/2012	مسح فيروس (شمعون) ثلاث ارباع جميع اجهزة كمبيوتر الشركة المملوكة لشركة (ارامكو) السعودية واستبدل البيانات بصورة علم امريكي مخترق، وأكد المسؤولون الأمريكيون أنَّ ايران وراء هذا الهجوم، وإنَّ هذا الهجوم هدفه موجه للولايات المتحدة الامريكية في اشارة لها.
3	11/سبتمبر/2012	قامت ايران بهجوم سيبراني (رفص الخدمة) ضد البنوك الامريكية فيما يعرف باسم (عملية أبابيل).
4	12/اكتوبر/2012	قامت ايران بهجمات سيبرانية عن طريق متسللين ايرانيين لهم صلات بالحكومة ضد بنوك امريكية.
5	8/يناير/2013	قامت ايران بهجمات سيبرانية باسم (عملية أبابيل) ضد الجهاز المصرفي الامريكي.

(52) مهدي مبارك عبد الله، الجيش السيبراني الايـران القوة السرية الـمـدمـرة، موقع جـرس، بتاريخ 22/ ابـريـل/2019، الشبكة الدولية للمعلومات:
https://www.ga-rasanews.com/article/325741

(53) محمد محمد السادة، الضرورة والمحظورات في «حرب الظل» بين ايـران والـعـدوّ (الإسـرائيـلي)، موقع الميادين نت، بتاريخ 11/ أغسطس/2021، الشبكة الدولية للمعلومات:
https://www.almaya-deen.net/articles/%D8%A7%D9

6	27/سبتمبر/2013	اخترق فاعلين سيبرانين ايرانيين اجهزة كمبيوتر غير سرية للبحرية الامريكية في خضمّ المحادثات حول البرنامج النووي الايراني.
7	فبراير/2014	استهدف فاعلين سيبرانيين ايرانيين شركة (لاس فيجاس ساندز) التابعة لشركة (شيلدون اديلسون) اذ أدى الهجوم الى اغلاق انظمة الاتصالات ومسح محركات الاقراص الثابتة.
8	نوفمبر / 2015	قامت ايران باستهداف وزارة الخارجية الامريكية ومسؤولين آخرين في (ادارة باراك اوباما.)
9	24/مارس/2016	وجهت وزارة العدل الامريكية لائحة اتهام ضد ايران بشن هجمات سيبرانية ضد بنوك امريكية وسد في نيويورك.
10	22/مارس/2018	ادى هجوم سيبراني ببرنامج (الفدية) يعرف باسم (sam sam) إلى شل حكومة مدينة (اتلانتا) الامريكية
11	9/مايو/2018	حذرت شركة الامن السيبراني الامريكي من زيادة ملحوظة في النشاط السيبراني الايراني في غضون (24) ساعة من انسحاب (ادارة ترامب) من خطة العمل الشاملة المشتركة.
12	12/يوليو/2018	حذر كبار المسؤولين الامريكيين من أنَّ ايران استعدت لهجمات سيبرانية واسعة النطاق ضد الولايات المتحدة الامريكية.
13	5/ديسمبر/2018	وجهت وزارة العدل الامريكية لائحة اتهام الى فاعلين ايرانيين سيبرانيين بشأن هجوم (sam sam ransam ware) على مدينة اتلانتا الامريكية.
14	يناير/ 2019	قامت شركة (fire eye) للأمن السيبراني بتفصيل حملة استمرت عامين من قبل ايران لسرقة بيانات اعتماد تسجيل الدخول وتفاصيل العمل في الولايات المتحدة الامريكية.
15	6/مارس/2019	قالت شركة مايكروسوفت انَّ الهجمات السيبرانية الايرانية استهدفت اكثر من (200) شركة في عامي 2017 و 2018
16	22/يونيو/2019	قالت وزارة الامن الداخلي الايرانية أنَّ ايران زادت من نشاطها السيبراني ضد الوكالات الحكومية الامريكية والصناعات الخاصة.
17	4/اكتوبر/2019	قالت شركة (مايكروسوفت) أنَّ ايران حاولت اختراق الحسابات المتعلقة بحملة اعادة انتخاب الرئيس الامريكي (دونالد ترامب) والمسؤولين الامريكيين.
18	22/اكتوبر/2019	كشفت المحكمة الموثقة ان مكتب التحقيقات الفدرالي الامريكي تعقب فاعلين ايرانيين سيبرانيين انتهكوا شركات تكنلوجيا الاقمار الصناعية الامريكية.

19	ابريل/2020	هاجم فاعلين ايرانيين سيبرانيين هجوماً سيبرانياً تصيداً احتيالياً ضد كبار المسؤولين التنفيذيين في شركة (جلعاد ساينسز)وهي شركة امريكية لصناعة الادوية.
20	4/يونيو/2020	قالت (google) أنَّ فاعلين ايرانيين سيبرانيين يستخدمون (apt35) قاموا بهجوم تصيد ضد حملة اعادة انتخاب الرئيس الامريكي (دونالد ترامب).
21	16/يوليو/2020	قالت شركة (IBM) أنَّ فاعلين ايرانيين سيبرانيين مع (APT35/ charming kitten) قاموا باختراق حساب (google) لمسؤول في البحرية الامريكية واستهدفوا موظفي وزارة الخارجية الامريكية بهجمات تصيد.
22	30/سبتمبر/2020	ازال موقع تويتر (150) حساباً منشؤها إيران كانوا يحاولون تعطيل المحادثة العامة خلال المناظرة الرئاسية الامريكية لعام 2020.
23	30/اكتوبر/2020	استهدفت مجموعة سيبرانية ايرانية مواقع انتخابات الولايات المتحدة الامريكية وحصلت بنجاح على بيانات تسجيل الناخبين في ولاية واحدة على الاقل وفقاً لمكتب التحقيقات الفيدراي (FBI) ووكالة الامن السيبراني والبنية التحتية (CISA)
24	3/ديسمبر/2020	اصدرت (CISA) تنبيهاً وعياً متزايداً للهجمات السيبرانية الايرانية وحذروا من نطاق قدرات ايران بما في ذلك تشويه موقع الويب، وهجمات رفض الخدمة الموزعة (DDOS) وسرقة معلومات التعريف الشخصية.
25	16/مارس/2021	قال مكتب المخابرات الوطنية ان ايران سمحت بحملة تأثير سيبراني خلال الانتخابات الرئاسية الامريكية لعام 2020 كان الهدف منها تقويض احتمالات اعادة انتخاب الرئيس السابق (دونالد ترامب).
26	30/مارس/2021	استهدف (charming kitten) المعروف باسم (الفوسفور) اكثر من عشرين باحثاً طبياً في الولايات المتحدة الامريكية حسبما افادت مجموعة (Proof point) للأمن السيبراني.
27	15/يوليو/2021	ازال موقع (facebook) ما يقرب من (200) حساب مزيف استخدمه فاعلين ايرانيين سيبرانيين لاستهداف افراد الجيش والدفاع الامريكي اذ سعى المتسللون الى اصابة اجهزة الكمبيوتر الخاصة بالمستهدفين ببرامج ضارة وسرقة معلومات تسجيل الدخول الخاصة بهم.

28	26/يوليو/2021	تم تسريب وثائق في الولايات المتحدة الامريكية حول كيفية قيام ايران باختراق البنية التحتية الحيوية للولايات المتحدة الامريكية بما في ذلك تنقية المياه وأنظمة امداد الوقود والاتصالات البحرية وكيفية اكتشاف انظمة ادارة المباني الذكية في الولايات المتحدة الامريكية.

الجدول من اعداد الباحث بالاعتماد على المصادر الآتية:

Sources:

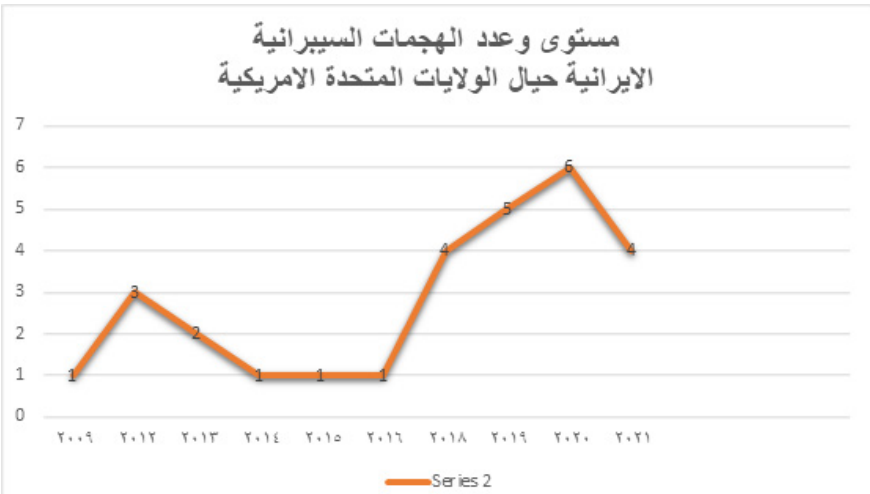
1- Collin Anderson, Karim Sadjad pour, Iran's cyber threat: espionage, sabotage, and revenge, Carnegie endowment for international peace, Washington, 2018, p – x – xi.

2- Andrew Hanna, the invisible U.S. – Iran cyber war, The iran primer, united states institute of peace , 29/july/2021, p-4-8: https://www.iranprimer.usip.org

3- Annie fixler and frank cilloffo, evolving menace: iran's use of cyber – enabled economic war fare, report, FDD press, adivision of the foundation for deense of democracies, November, Washington, DC, 2018, p – 7.

4- Quentin E.Hogson, logon ma, krystna marcinek schwindt, fighting shadows in the dork, understanding and countering coercion in cyber space, published by the rand, corporation, santa monica, calif, 2019, p 23 – 24 - .

وللتوضيح اكثر عن مستوى وعدد الهجمات السيبرانية الايرانية حيال الولايات المتحدة الامريكية ضمن استراتيجيتها السيبرانية، سنطرح مخططاً بيانياً يوضح فيه ذلك، وكالآتي: مخطط رقم (2) يوضح مستوى وعدد الهجمات السيبرانية الايرانية بيانياً حيال الولايات المتحدة الامريكية



المخطط من اعداد الباحث، بالاعتماد على المصادر الآتية:

Sources:

1- Annie fixler and frank cilluffo, evolving menace iran's use of cyber – enabled economic war fare, report, FDD press, adivision of the foundation for deense of democracies, November, Washington, DC, 2018, p – 7 – 8 -.
2- Marie baezner, hotspot analysis: Iranian cyber – activities in the context of regional rivalries and international tensions, center for security studies (css), version – 1 - , Switzerland, may/2019, p - 6 - 8 -.
3- Andrew Hanna, the invisible U.S. – Iran cyber war, The Iran primer, united states ,institute of peace , 29/july/2021, p-4-8: https://www.iranprimer.usip.org
4- Ilan berman, the Iranian cyber threat ,Revisited, u.s. house of representatives committee on homeland security, American foreign policy council, 20 march, 2013, p – 3 -.

الخاتمة

نستنتج من كل ما تقدم أنَّ الحرب السيبرانية هي احدى أدوات الجيل الخامس من الحروب التي ميدان صراعها وعملها هو الفضاء السيبراني إذ تستخدم عبر هذا الفضاء الأسلحة السيبرانية من برامجيات وفايروسات ذات قدرة تدميرية ضد الجهة المستهدفة لذا سعت الدول ذات القدرات السيبراينة الى تفعيل ذلك وخاصة الولايات المتحدة الامريكية وايران (محط الدراسة) الدولتان ذات التاريخ الحافل بالصراعات، اذ استخدمت الولايات المتحدة الامريكية أولى هجماتها ضد ايران كان في عام 2006 عبر حملة الألعاب الأولمبية واستمرت بتلك الهجمات عبر استراتيجية سيبرانية خاصة لها عبر الإدارات الامريكية المتعاقبة وحتى وقتنا الحاضر ساعية من ذلك لتدمير وإنهاك وابطاء القدرات الحيوية لإيران والبنى التحتية خاصة في اطار قدراتها النووية متمثلاً بالبرنامج النووي الإيراني وصولاً لما مخطط له ضمن استراتيجيتها الخارجية، مع رد إيراني استراتيجي سيبراني ضد الولايات المتحدة الامريكية بدأ في عام 2009 واستمر حتى وقتنا الحاضر عبر استراتيجية سيبرانية خاصة شكلت مؤسسات عاملة لذلك عبر أسلحة سيبرانية هدفها الحاق اكبر ضرر داخل المواقع الحيوية والبنى التحتية للولايات المتحدة الامريكية لإثبات أنَّ ايران لها القدرة السيبرانية على الرد والهجوم الاستباقي أيضاً، وهذه الهجمات السيبرانية لكلا الطرفين تدخل ضمن النطاق الاستراتيجي غير المعلن، وعليه طرحنا مخططاً بيانياً يوضح مسار الهجمات السيبرانية لكلا الطرفين لمعرفة ما دار بينهما ضمن النطاق الاستراتيجي السيبراني التي في المستقبل قد تمهد لمرحلة تصعيد

لحرب شاملة بين الطرفين إلّا إذا بقيت تحت نطاق التحكم الاستراتيجي، فضلاً عن ذلك تم طرح الحرب السيبرانية كنشأة ومفهوم والمفاهيم المقاربة لها مع الوسائل والأهداف للضرورة العلمية البحثية .

قائمة المصادر

- المصادر العربية

أولاً الكتب:

1-إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، العربي للنشر والتوزيع، ط1، القاهرة، 2019.

ثانياً: البحوث العلمية.

1- اميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد 35، الجزء 3، كلية القانون، جامعة الامارات العربية المتحدة، 2020.

2- حيدر كاظم عبد علي، رباب محمود عامر، التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة، مجلة الكوفة، العدد47، جامعة الكوفة، 2019.

3- زينب شنوف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد2، جويلية (يوليو)، الجزائر، 2020.

4- يحيى ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، العدد 4, جامعة القاهرة – كلية الحقوق – فرق الخرطوم، 2018.

5- إسماعيل زروقـة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، منشورات جامعة الشهيد حمة لخضر بالوادي، المجلد10، العدد1، الجزائر، 2019.

6- علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد 57، جامعة النهرين – كلية العلوم السياسية، 2019.

7- نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني «التهديد المتصاعد لأمن الدول» ، مجلة مركز بابل للدراسات الإنسانية، المجلد8، العدد2، جامعة بابل، 2018.

8- محمد وائل القيسي، مستقبل الامن الاستراتيجي العالمي في ظل التحديات التكنو – معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، مركز الدراسات الإقليمية، السنة14، العدد44، نيسان، جامعة الموصل، 2020.

9- تغريد صفاء، لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي للدراسات، مركز حمورابي للبحوث والدراسات الاستراتيجية، العدد 33 – 34،

السنة 8، شتاء -ربيع، بغداد، 2020.
10- زهراء عماد مجيد كلنتر، احمد عبيس نعمة الفتلاوي، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 1، العدد 44، آذار، جامعة الكوفة – كلية القانون، 2020.
11- حيدر أدهم الطائي، علي محمد كاظم، المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية، مجلة كلية الحقوق، المجلد 21، العدد 2، جامعة النهرين، 2019.
12- صلاح مهدي هادي الشمري، زيد محمد علي إسماعيل، الامن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، السنة 12، العدد 62، جامعة النهرين، كلية العلوم السياسية، 2020.
13- احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران و(إسرائيل)، مجلة الدراسات الإيرانية، المعهد الدولي للدراسات الإيرانية، السنة 4، العدد 12، اكتوبر ,المملكة العربية السعودية، 2020.

ثالثاً الانترنت

1- الحروب السيبرانية – نتائج ملموسة لمعارك غير مرئية، الجندي، بتاريخ 1/ ابريل/2021، ص1، الشبكة الدولية للمعلومات:
https://www.aljundi.ae%d8%a7%84%d9
2- غيث علاو، الهجمات السيبرانية أكبر من حروب نووية بوسائل الكترونية، موقع جادة ايران، بتاريخ 5/يوليو/2020، الشبكة الدولية للمعلومات:
https://www.jadehiran.com/archives/16835
3- وقائع الحرب السيبرانية «الخفية» بين الولايات المتحدة وإيران، الحرة، ترجمات – واشنطن، بتاريخ 25/فبراير/2021، الشبكة الدولية للمعلومات:
https://www.alhurra.com/iran/2021/02/25
4- فايروس ضرب برنامج ايران النووي، عربي bbc news، بتاريخ 22/ نوفمبر/ 2010، الشبكة الدولية للمعلومات:
https://www.bbc.com/arabic/middleeast/2010/11
5- كيف هوجمت المنشأة النووية الإيرانية في «نطنز» المعزولة من الانترنت، العربية، بتاريخ 6/ يوليو/2019، الشبكة الدولية للمعلومات:
https://www.alarabia.net/iran/2019/07/06
6- استراتيجية أمريكية شرسة للأمن الالكتروني تستهدف الصين وروسيا، عربية sky news، ابوظبي، بتاريخ 21/سبتمبر/2018، الشبكة الدولية للمعلومات:
https://www.skynewsarabia.com/world/1184165
7- مواجهة 2020 خطة بايدن للحرب السيبرانية، قناة الحرة، بتاريخ 29/ ديسمبر/2020، الشبكة الدولية للمعلومات:
https://www.alhurra.com/episode/2020/12/29/801626

8- ريتشارد ووكر، قمة بايدن وبوتين ... وشبح الخطر النووي السيبراني، موقع DW، بتاريخ 16/ يونيو/2021، الشبكة الدولية للمعلومات:
https://www.dw.com/ar/%D,%85%D8
9- بايدن: من المنطقي مهاجمة الخوادم التي تنطلق منها الهجمات السيبرانية، موقع RT عربي، بتاريخ 9/يوليو/2021، الشبكة الدولية للمعلومات:
https://www.arabic.rt.com/world/1250247
10- فراس الياس، عقيدة الأمن السيبراني في إيران ومعادلات المواجهة مع أمريكا، موقع ن بوست، بتاريخ 14/ أغسطس/ 2019، الشبكة الدولية للمعلومات:
https://www.noonpost.com/content/28950
11- مهدي مبارك عبد الله، الجيش السيبراني الايراني القوة السرية المدمرة، موقع جرس، بتاريخ 22/ ابريل/2019، الشبكة الدولية للمعلومات:
https://www.garasanews.com/article/325741
12- محمد محمد السادة، الضرورة والمحظورات في «حرب الظل» بين ايران والعدوّ (الإسرائيلي)، موقع الميادين نت، بتاريخ 11/ أغسطس/ 2021، الشبكة الدولية للمعلومات:
https://www.almayadeen.net/articles/%D8%A7%D9

- المصادر باللغة الإنجليزية

first: books

1- tim Jordan, cyber power: the culture and politics of cyber space and the internet, routledge, London, 1999.

2- Athina karatzogianni, cyber conflict and global politics, London and new York, 2009..Routledge

3- jeetendra pande, introduction to cyber security (fcs), published by: uttarkhand open university, haldwani, 2017 .

4- Collin Anderson, Karim Sadjad pour, Iran's cyber threat: espionage, sabotage, and revenge, Carnegie endowment for international peace, Washington, 2018.

5- Quentin E-Hogson, logon ma, krystna marcinek schwindt, ,fighting shadows in the dark, understanding and countering coercion in cyber space, published by the rand, corporation, santa monica, calif, 2019.

6- Marie baezner, hotspot analysis: Irani an cyber – activities in the context of regional rivalries and international tensions, center for security studies (css), version – 1 - , Switzerland, may/2019 .

Secondly: : research, priodecals and reports

1- Michael Robinson, Kevin jones, helge janicke , cyber war fare: issues and challenges, article in computer and security, Elsevier volume – 49 -, march, united kingdom, 2015 .

2-Andrea bendovschi, cyber – attacks – trends, patterns and security counter measures, article in procedia economics and finance, Elsevier, volume 28, 2015 .

3-p.s. seema, s.nandhini, m.sowmiya, over view of cyber security, international journal of advanced research in computer and communication engineering, article in ijarcce, volume 7, issue 11, November, 2018 .

4- darko galince, darko mozink and boris guberina, cyber security and cyber defence: national level strategic approach, journal for control, measurement, electronics, computing and communications, article in automatika, volume 58, number3, july, 2017 .

5- g.n reddy, g.j.u.reddy, a study of cyber security challenges and its emerging trends on latest technologies, computer science, arxiv, 8 February, 2014.

6- Robert "Jake" bebber, cyber power and cyber effectiveness: an analytic framework, comparative strategy an international journal, routledge, taylor & francis group, volume 36, November 5, 2017 .

7- alexander kosenkov, cyber conflict a new global threat, future internet, mdpi, 8, 45, 2016 .

8- Stefan soesanto and max smeets, cyber deterrence: the past, present, and future, center for security studies (css), Switzerland, 2021 .

9- tim stevens, cyber weapons: power and the governance of the invisible, article in international politics, springer, king's collage London, may, 2018 .

10- mattias schulze, joseph kerscher, Paul bochtler, cyber escalation: the conflict dyad USA / Iran as a test case, working paper, swp, german institute for international and security affairs, December, 2020 .

11- marie baezner, Patrice robin, stuxnet, publisher(s) :cene

ter for security studies (css), issue 4, E T H Zurich, Switzerland, 2017.

12- president Donald J.Trump, national cyber strategy of the united states of American, the white house, Washington, dc, September, 2018 .

Third: internet

1-Andrew Hanna, the invisible U.S. – Iran cyber war, The iran primer, united states institute of peace , 29/july/2021,international information network : https://www.iranprimer.usip.org/blog/2019/oct/25/invisible

2- David p. fidler , america's place in cyber pace: the biden administration cyber strategy Takes shape, council foreign relation, foreign affairs, march, 11, 2021, international information network: https://www.cfr.org/blog/americas-place-cyberspace