

الاتحاد الأوروبي والحد من انتشار أسلحة الدمار الشامل: البرنامج النووي الإيراني إنموذجاً

*شهد حسن علي

باحثة من العراق - سياسة دولية

ملخص :

* Shahadhassanali@gmail.com

يعد الاتحاد الأوروبي من أبرز وأهم التكتلات والمنظمات الإقليمية الكبرى كونه يمتاز ببنية مؤسسية قوية، وكذا امتياز به حسن تسييره للمهام، هذا ما جعله يبرز كأحد أبرز القوى العالمية سواء من الناحية السياسية أو الاقتصادية على وجه التحديد، حيث ارتبطت العلاقات الأوروبية بمنطقة الشرق الأوسط بالمصالح الاقتصادية إذ يسعى إلى حماية هذه المصالح من التهديدات والتحديات التي تواجهها هذه المنطقة، إذ يسعى إلى إيجاد عالم أكثر أمناً فضلاً عن دوره الفعال في مجال إرساء الاستقرار وتحقيق السلم والأمن الدوليين، مما جعله يقوم بدعم عدة معاهدات في مجال حظر وانتشار الأسلحة النووية، حيث بات الحد من انتشار الأسلحة النووية أكثر من ضرورة خاصة خلال الحرب الباردة واحتدام الصراع بين الكتلتين الشرقية والغربية، وخطورة الأسلحة التي كانت تمتلكها، مما أدى إلى إنشاء معاهدات هادفة إلى حظر ومنع الانتشار النووي وكذلك انضمام الاتحاد الأوروبي إلى المنظمات الدولية الرامية لحظر انتشار ومنع ما يعرف بأسلحة الدمار الشامل خاصة الأسلحة حيث تبرز جهود الاتحاد الأوروبي في هذا المجال من خلال سعيه الدائم في حل وتسوية الملف النووي الإيراني بطرق سلمية، وذلك عن طريق القوة الناعمة وكذلك السماح لإيران باستخدام الطاقة النووية لكن لأغراض سلمية، فالإتحاد الأوروبي بسياسته الخارجية والأمنية المشتركة يهدف إلى إرساء الأمن والسلم الدوليين.

كلمات مفتاحية : أسلحة الدمار، البرنامج النووي، الاتحاد الأوروبي.

The European Union and the proliferation of weapons of mass destruction: the Iranian nuclear program as a model

Shahd Hassan Ali

researcher from Iraq

PhD students at Al-Nahrain University / Department of International Politics

ABSTRACT

The European Union is considered to be one of the most prominent, important and major regional organizations unions. This is why it is the greatest political and economic power in particular. European relations with the Middle East have been linked to economic interests. It intends to protect those interests from threats and challenges in the region. It seeks to create a safer world in addition to its role in establishing stability and international peace and security. This has led to support several treaties in the prevention and proliferation of the nuclear weapons it which led to the establishment of nuclear non-proliferation treaties and the accession of the European Union to international organizations to prohibit and prevent the proliferation of mass destruction weapons, in particular nuclear weapons, in order to establish security and stability in the world and to defy the Middle East. The efforts of the European Union in this area are highlighted through its constant efforts to resolve the nuclear issue in a peaceful manner, through its soft power and by allowing Iran to use nuclear energy but for the most peaceful was purposes. The European Union's foreign and security policy is aimed at establishing international peace and security.

KEY WORDS: weapons of mass destruction, nuclear program, European Union.

المقدمة:

عند البحث في التحديات الدولية التي تواجه القوى الفاعلة في النظام السياسي الدولي لا بد من تناول انتشار أسلحة الدمار الشامل التي تعد تحدياً ليس أمام القوى الفاعلة في النظام الدولي فقط وإنما أمام العالم اجمع لما تحتويه هذه الأسلحة من اضرار مادية ليس لوقت وقوعها فقط وإنما لفترات زمنية طويلة جداً فعلى سبيل المثال ان الأرض التي يقع عليها انفجار نووي تصبح غير صالحة للزراعة ولا للعيش لانها أصبحت مشعة وغير صالحة للزراعة وهذا بالطبع هو ابسط النتائج التي تخرج عن الانفجار النووي.

باختصار، فإن اتخاذ حكومة لقرار خوض حرب نووية كبرى يعادل انتحار

الحضارة كما نعرفها. وفي وجود الأسلحة النووية الحديثة - التي تبلغ قوة بعضها ٢٠٠ ميغا طن حيث أصبح قيام حرب نووية هو السبيل الذي قد يبدأ به الزعماء السياسيون بضغطة زر ربما عن غير قصد) الانزلاق في هوة فناء البشرية) ينبغي أن يتضح جلياً مما سبق أن المجتمع الدولي برمته لديه مصلحة جماعية في أعمال سياسات وتدابير أكثر فعالية لمنع انتشار الأسلحة النووية، وللترويج لنزع السلاح العام الكامل ومن ضمن هذه القوى الدولية الاتحاد الأوروبي الذي يعد أحد المؤثرين في عملية الحد من انتشار أسلحة الدمار الشامل.

أهداف الدراسة:

تهدف الدراسة لتوضيح أهمية ودور القوى الدولية الفاعلة التي لها تأثير في عملية منع انتشار أسلحة الدمار الشامل ومن بينها الاتحاد الأوروبي الذي يسعى الى الحد من انتشار أسلحة الدمار الشامل لكن هذا المنع يأتي فقط في المناطق التي تعد مهمة وحيوية بالنسبة للاتحاد والدول الأعضاء ومن بينها إيران التي تعد احدى القوى الإقليمية الفاعلة في منطقة الشرق الأوسط.

إشكالية الدراسة:

تنطلق إشكالية الدراسة من كون ان انتشار أسلحة الدمار الشامل تمثل احد اهم التحديات الدولية بالنسبة للقوى الدولية التي تحاول جاهدة للحد من انتشارها بمختلف المستويات وعليه ستكون الإشكالية على مجموعة تساؤلات هي: ماهي المساعي الدولية المبذولة للحد من انتشار أسلحة الدمار الشامل؟ وماهو دور الاتحاد الأوروبي في هذه الجهود؟ وهل الاستراتيجية الأوروبية للحد من انتشار أسلحة الدمار الشامل هي استراتيجية فاعلة؟ وماهي سياسة الاتحاد الأوروبي تجله انتشار أسلحة الدمار الشامل؟ وكيف تم التعامل مع البرنامج النووي الإيراني؟

فرضية الدراسة:

ومن إشكالية البحث تنطلق الدراسة من فرضية مفادها ان (الاتحاد الأوروبي كفاعل دولي يحاول ان يثبت وجوده من خلال المشاركة الفعلية في القضايا الدولية المهمة ومن بينها الانتشار النووي والذي يعد البرنامج النووي الإيراني هو أفضل مجال للاتحاد الأوروبي لاثبات دوره وتطبيق استراتيجيته.

منهجية الدراسة:

تم تناول أكثر من منهج خلال الدراسة وهي المنهج التاريخي: والذي تم استخدامه من خلال تناول مجموعة من الاحداث التاريخية المهمة للدراسة والمنهج الاستقرائي الذي يعتمد على دراسة الجزء للانتقال الى الكل من خلال دراسة تفاصيل الانتشار النووي والانطلاق الى النتائج النهائية

وتم تقسيم الدراسة على أربعة مطالب **المطلب الأول**: المساعي والجهود الدولية الذي تم البحث فيه عن مستوى الجهد الدولي للحد من انتشار أسلحة الدمار الشامل **والمطلب الثاني**: يوضح تطور دور الاتحاد الأوروبي في السعي للحد من انتشار أسلحة الدمار الشامل اما **المطلب الثالث** استراتيجية الاتحاد الأوروبي

للحد من انتشار أسلحة الدمار الشامل وتوضح مدى فعاليتها وقدرتها على تحقيق هذا الغرض والمطلب الرابع سياسة الاتحاد الأوروبي والبرنامج النووي الإيراني الذي يوضح مدى فعالية هذه السياسة وهل هي فاعلة في البرنامج النووي الإيراني؟ والانتهاج بالخاتمة.

المطلب الأول: المساعي والجهود الدولية

عند البحث في الحد من انتشار أسلحة الدمار الشامل ينبغي توضيح انه ثمة نوعان أساسيان للانتشار: الرأسي، وفيه تزيد الدول الحائزة للأسلحة النووية ترسانتها النووية الخاصة وربما ترسانات حلفائها أيضاً بتطوير أسلحة نووية وناقلات للأسلحة النووية أكثر قوة ودقة من خلال البحث والتطوير الأفقي: وفيه يحصل عدد متزايد من الدول على أسلحة نووية على الرغم من الجهود حسنة النية التي بذلها مبتكرو نظام معاهدة عدم الانتشار النووي وأولئك المسؤولون حالياً عن تفعيله، فما زال النوعان من الانتشار مستمرين.

وكانت هناك جهود دولية واسعة للحد من انتشار الأسلحة النووية وسيتم توضيحها بصورة مختصرة في بداية الأمر في تموز من عام 1957 اقترحت الحكومة الأمريكية على لجنة الطاقة الذرية التابعة للامم المتحدة خطة باروخ التي وافقت من خلالها الولايات المتحدة على ازالة الاسلحة النووية

**وفي تموز من عام 1957 تأسست
الوكالة الدولية للطاقة الذرية بقرار
بالاجماع من الامم المتحدة**

كافة شريطة ان تتعهد الدول الاخرى بعدم انتاجها ودعم اقامة نظام للتفتيش والعقوبات. وفي تموز من عام 1957 تأسست الوكالة الدولية للطاقة الذرية بقرار بالاجماع من الامم المتحدة، وتهدف الوكالة الى التفتيش على المنشآت

النووية الحالية وتعزيز الاستخدام السلمي للطاقة النووية وقد انضمت 150 دولة لعضوية الوكالة الدولية للطاقة الذرية حتى نهاية يونيو. واصبحت الصين دولة عضوا في عام عام 1984.⁽¹⁾ وفي اب عام 1963 وقع الاتحاد السوفيتي والمملكة المتحدة والولايات المتحدة معاهدة الحظر الجزئي للتجارب النووية لابطاء سباق التسلح ووقف الانتشار المكثف لتساقط الغبار النووي في الجو الا ان المعاهدة استثنت التجارب النووية تحت الارض فتركتها دون تحديد.

وفي تموز 1968 افتتحت معاهدة منع انتشار الاسلحة النووية للتوقيع عليها وفي الوقت الحالي يوجد 189 دولة وقعت عليها. وتدعو المعاهدة الدول الى نزع عام وشامل للسلاح النووي والى الاستخدام السلمي للطاقة النووية للاغراض المدنية.⁽²⁾ اذ يذكر ان سولت 1 وسولت 2 وقعتا للحد من نمو الترسانتين الأمريكية والسوفيتية وتخفيف العبء الاقتصادي لسباق التسلح. وحددت معاهدة الحد من الصواريخ المضادة للصواريخ بالستية عدد انظمة الصواريخ المضادة للصواريخ باليستية المستخدمة في المجالات الدفاعية ضد الصواريخ ذات الرؤوس النووية. ومنذ منتصف فترة السبعينات انصب التركيز الاساسي لجهود منع الانتشار على زيادة الحد من المواد الانشطارية خاصة ذات التخصيب العالي لليورانيوم والبلوتونيوم.

(1) [https://www.wikipedia.org/nuclear weapons](https://www.wikipedia.org/nuclear%20weapons)

(2) جامعة مينيسوتا , مكتبة حقوق الانسان , معاهدة عدم انتشار الأسلحة النووية 2021/6/13
<http://hrlibrary.umn.edu/arabic/TNPNW.html>

وفي عام 1975 اجتمعت سبع دول في لندن في سلسلة من المحادثات وتم تأسيس مجموعة الموردين النوويين. من اجل مهمة مشابهة لتلك الخاصة بلجنة زانجير وهو جهاز متعدد الجنسيات معنى بتخفيض انتشار الاسلحة النووية عن طريق الحد من تصدير وإعادة نقل المواد التي على مستوى الاسلحة النووية، وقد انضمت الصين الى المجموعة عام 2004. وفي عام 1987 تم التوصل الى معاهدة القوى النووية متوسطة المدى بين الولايات المتحدة والاتحاد السوفيتي. وقد خفضت عدد الصواريخ النووية والصواريخ الباليستية التقليدية الأرضية وتم السماح باجراء تفتيش من الناحيتين. وفي عام 1991 و 1993 تم التوقيع على معاهدي خفض الاسلحة الاستراتيجية 1 و 2 المعروفتين باسم ستارت 1 وستارت 2 على التوالي. ولم يتم تفعيل معاهدة ستارت اثنين على الاطلاق. وفي 2002 وقعت الولايات المتحدة وروسيا معاهدة موسكو التي تنص على ان تخفض كلتا الدولتين رؤوسهما النووية بمقدار الثلثين في غضون عشرة اعوام. وتم التوقيع على معاهدة الحظر الشامل للتجارب النووية في عام 1996 إلا أنها لم تصبح سارية المفعول بعد. وهي معاهدة دولية وقعت عليها 181 دولة تحظر كافة التفجيرات النووية في كل البيئات.

وفي عام 1991 و 1993 تم التوقيع على معاهدي خفض الاسلحة الاستراتيجية 1 و 2 المعروفتين باسم ستارت 1 وستارت 2 على التوالي.

ولكن ابرز المعاهدات الدولية للحد من أسلحة الدمار الشامل هي معاهدة الحد من انتشار الأسلحة النووية أو معاهدة عدم انتشار الأسلحة النووية (Treaty on the Non-Proliferation of Nuclear Weapons) والمعروفة اختصاراً (NPT) وهي تهدف إلى منع انتشار الأسلحة النووية وتكنولوجيا الأسلحة، لتعزيز التعاون حول الاستخدامات السلمية للطاقة النووية، وتهدف بشكل ابعدي إلى نزع الاسلحة النووية ونزع الاسلحة العام والكامل. تم التفاوض على المعاهدة بين عامي 1965 و 1968 من قبل لجنة مؤلفة من ثماني عشرة دولة برعاية من الأمم المتحدة في مدينة جنيف السويسرية⁽³⁾.

(3) سعد حقي توفيق ، الاستراتيجية النووية بعد انتهاء الحرب الباردة ، دار زهران للنشر والتوزيع ، عمان - الأردن ، 2008 ، ص ص 190 - 200

تم إتاحة المعاهدة للتوقيع عليها عام 1968 ودخلت حيز التنفيذ في 1970 بعد خمسة وعشرين عاماً اجتمع أعضاء المعاهدة، كما تنص عليه المعاهدة، واتفقوا على تمديدها إلى ما لا نهاية ضمت هذه المعاهدة أكبر عدد من الدول مقارنة مع باقي المعاهدات الخاصة بالحد من أو نزع الاسلحة الاخرى مما يؤكد على أهمية هذه المعاهدة في آب 2016 وقع على المعاهدة 191 دولة على الرغم من أن كوريا الشمالية التي وقعت على المعاهدة عام 1985 إلى أنها لم تلتزم بها، وأعلنت انسحابها من المعاهدة في 2003 أربعة من الدول الأعضاء في الأمم المتحدة لم توافق أبداً على المعاهدة ثلاثة منهم تمتلك أسلحة نووية وهي الهند وباكستان وإسرائيل فضلا عن جنوب

ابرز المعاهدات الدولية للحد من أسلحة الدمار الشامل هي معاهدة الحد من انتشار الأسلحة النووية أو معاهدة عدم انتشار الأسلحة النووية

السودان المنضمة إلى الأمم المتحدة عام 2011 ولم تنضم إلى المعاهدة. تعترف المعاهدة بوجود خمس دول نووية قامت ببناء واختبار أجهزة انفجارات نووية قبل 1 كانون الثاني 1967 وهي الولايات المتحدة، روسيا، المملكة المتحدة، فرنسا والصين. هناك ثلاث دول أخرى تم تأكيد حيازتها للأسلحة النووية وهي الهند وباكستان وكوريا الشمالية حيث أعلنت هذه الدول حيازتها للأسلحة النووية وأنها قامت باختبار هذه الأسلحة، بينما إسرائيل تعتمد الغموض بما يخص وضوح الأسلحة النووية من جانبها.⁽⁴⁾

(4) نفس المصدر السابق

غالباً ما يُنظر إلى معاهدة عدم انتشار الأسلحة النووية على أساس صفقة مركزية: ((الدول غير النووية المنضوية ضمن المعاهدة توافق على أنها لن تقوم بامتلاك أسلحة نووية بالمقابل ستقوم الدول النووية بمشاركة الفوائد السلمية للتقنية النووية وسوف تتابع نزع الأسلحة النووية الذي يهدف إلى القضاء على ترسانتها النووية))⁽⁵⁾

(5) معاهدة عدم انتشار الأسلحة النووية ، سلسلة وقائع التابعة للأمم المتحدة ، نيويورك ، 1985 ، المادة الثالثة

إنَّ المعاهدة تتسم بطبيعتها بالتمييز وتتهم بعض البلدان النامية الدول المتقدمة باستخدام نظام عدم الانتشار للحفاظ على احتكارها للتكنولوجيا النووية المتقدمة

عند تقديم معاهدة الحد من انتشار الأسلحة النووية، كان من المتوقع ظهور 25-30 دولة تمتلك الأسلحة النووية خلال 20 سنة. بالمقابل بعد أربعين عاماً فقط خمس دول لم توقع على المعاهدة منها فقط أربع دول يعتقد بأنها تمتلك أسلحة نووية تم تبني عدة معايير إضافية لتقوية المعاهدة

وتوسيع نظام الحد من الأسلحة النووية وجعل حصول الدول على الإمكانيات لتطوير الأسلحة النووية أصعب، بما في ذلك ضوابط تصدير مجموعة الموردين النوويين وتدابير التحقق المعززة للبروتوكول الإضافي للوكالة الدولية للطاقة الذرية. ولكن هناك الكثير من الانتقادات تدور حول هذه المعاهدة منها⁽⁶⁾.

(6) بول ويكليسن ، العلاقات الدولية مقدمة فصيلر جدا ، ترجمة لبنى عماد تركي ، مصدر سبق ذكره ، ص ص 128-130

- إنَّ المعاهدة تتسم بطبيعتها بالتمييز وتتهم بعض البلدان النامية الدول المتقدمة باستخدام نظام عدم الانتشار للحفاظ على احتكارها للتكنولوجيا النووية المتقدمة. وتدعو هذه البلدان الى وصول حر غير مقيد الى تلك التكنولوجيا دون اعتبار في الغالب ضمان عدم انتشار الاسلحة النووية وبصرف النظر عن احتياجاتها الحقيقية ذاتها، وخاصة الاتفاق بشأن ضوابط نقل المواد النووية.

- إنَّ المعاهدة تحرم على الدول الاطراف فيها وغير الحائزة على الأسلحة النووية تصنيع اي جهاز تفجير نووي آخر او ان تلتمس أو تتلقى اي مساعدة من الدول الحائزة على الاسلحة النووية لصنع المتفجرات النووية او اي جهاز تفجير نووي آخر، بل وقد يكون لها الحق في الابقاء على ما لديها. ولا تشير كذلك الى تحريم نشر الاسلحة النووية على أراضي دولة غير حائزة لاسلحة نووية، أو العبور فوق اجوائها او تحريكها من موقع لآخر في تلك الدولة. وليس بالضرورة ان تكون الدولة خالية تماما من الأسلحة النووية (كإسرائيل والهند وباكستان) وبمعنى آخر فقد كانت المعاهدة تُعد وسيلة لمنع الدول الصناعية الكبرى عن بناء الاسلحة النووية أما الآن فانها تعتبر وسيلة لاحتفاظ الدول

- الحائزة لاسلحة نووية بما لديها من تكنولوجيا نووية، بينما يمنع الفئة الأخرى من الدول من تطوير مثل تلك التكنولوجيا ونشرها خاصة في الدول النامية
- استمرار سباق التسلح وعدم تخلي الدول الكبرى عن ترسانة أسلحتها بل وأصبحت المعاهدة ضمانه للحفاظ على ترسانة الدول الكبرى
- نظام الضمانات ضعيف جدا في المعاهدة ولا يوجد هناك جزاءات في حال الاستخدام الفعلي للأسلحة النووية

اما احداث المساعي الدولية للحد من انتشار الأسلحة النووية وأسلحة الدمار

الشامل هي معاهدة حظر الأسلحة النووية - Treaty on prohibition of nuclear weapons وتختصر إلى (TPNW) وهي أول اتفاقية دولية للإلزام القانوني بحظر الأسلحة النووية على نحو شامل، بهدف المُضي نحو القضاء التام على هذه الأسلحة. مُررت هذه المعاهدة يوم 7 تموز عام 2017 وتحتاج هذه المعاهدة توقيع وتصديق 50 دولة على الأقل حتى تُطبق وبحلول يوم 23 يناير عام 2020، صدقت

35 دولة على هذه المعاهدة. وتمنع هذه المعاهدة الدول المُصدِّقة عليها من (تطوير، واختبار، وإنتاج، وتخزين، وإقامة، ونقل، واستخدام، والتهديد باستخدام الأسلحة النووية، فضلاً عن حظر المساعدة والتشجيع على هذه الأنشطة المحظورة) وتعطي هذه المعاهدة الدول المُصدِّقة عليها، والمالكة للأسلحة النووية، إطاراً زمنياً محدداً لإجراء المفاوضات التي ستؤول إلى قضاء مُحقق، وبلا رجعة، على برنامج الأسلحة النووية⁽⁷⁾.

بدأت المفاوضات على هذه المعاهدة بالأمم المتحدة في آذار عام 2017، طبقاً لتفويض رسمي تبنته الجمعية العامة للأمم المتحدة في ديسمبر عام 2016، واستمرت هذه المفاوضات بين 15 حزيران وحتى 7 تموز عام 2017

وعند التصويت على نص هذه المعاهدة، صوتت 122 دولة لصالحها، وصوتت دولة واحد ضدها دولة هولندا وامتنعت دولة أخرى عن التصويت جمهورية سنغافورة. لم تصوت 69 دولة على هذه المعاهدة، ومن بينهم جميع الدول المالكة للأسلحة النووية وجميع أعضاء حلف شمال الأطلسي الناتو باستثناء هولندا. ستشكل معاهدة حظر الأسلحة النووية، طبقاً لما يتصوره مؤيدوها، «التزاماً سياسياً

واضحاً» لتحقيق عالم خال من السلاح النووي والحفاظ عليه. ومع ذلك، فبخلاف اتفاقية الأسلحة النووية، لم يكن مقصوداً أن تضم هذه المعاهدة كافة الوسائل القانونية والتقنية المطلوبة حتى تحقق القضاء على الأسلحة النووية وستكون بنود هذه المعاهدة مادةً للمفاوضات اللاحقة، لتسمح بالتوصل إلى اتفاقية مبدئية بشكل سريع نسبياً، دون الحاجة إلى اشتراك الدول المالكة للأسلحة النووية إذا استلزم

كانت المعاهدة تُعد وسيلة لمنع الدول الصناعية الكبرى عن بناء الاسلحة النووية أما الآن فانها تعتبر وسيلة لاحتفاظ الدول الحائزة لاسلحة نووية

(7) اللجنة الدولية للصليب الأحمر ،
2018 / 4 / 24
<https://www.icrc.org/ar/document/2017-treaty-prohibition-nuclear-weapons>

كانت المعاهدة تُعد وسيلة لمنع الدول الصناعية الكبرى عن بناء الاسلحة النووية أما الآن فانها تعتبر وسيلة لاحتفاظ الدول الحائزة لاسلحة نووية

الأمر⁽⁸⁾

(8) الوكالة الدولية للطاقة الذرية ،
<https://www.iaea.org/ar/almawadie/mueahadat-edm-alaintishar>

يؤمن مؤيدوا هذه المعاهدة أنها ستؤدي إلى الحد من الأسلحة النووية، وستعمل باعتبارها عاملاً حافزاً للقضاء عليها التي تعهد نحو ثلثي دول العالم على العمل معاً «لغلق هذه الفجوة القانونية» الموجودة عند النظام الدولي القائم الذي يحكم الأسلحة النووية وترى هذه الدول أن معاهدة حظر السلاح النووي هي الخيار الوحيد لتحقيق هذا الهدف

وفي 22 كانون الثاني 2021، دخلت معاهدة حظر الأسلحة النووية حيز التنفيذ وكان قد تم تبنيها من قبل 122 دولة في الولايات المتحدة عام 2017، ووقعت عليها حتى الآن 86 دولة، وصادقت عليها 51 دولة من بين هذه الدول

قد حظيت هذه المبادرة الصادرة عن المجتمع المدني والحائزة على جائزة نوبل للسلام بدعم الأغلبية الساحقة من الدول، باستثناء تلك التي تمتلك أسلحة نووية وحلفائها. وبالتالي، أشارت بعض الأصوات المتقدمة إلى أن

انّ انتشار أسلحة الدمار الشامل يشكل أحد أهم التحديات الأمنية ولعل التحدي الرئيسي الذي يقف امام عملية إدارة انتشار هذه الأسلحة هو مستوى الضغوط التي تواجهها المعاهدات الدولية

المعاهدة الجديدة لن يكون لها أي تأثير على نزع الأسلحة النووية. وفي جميع الأحوال، ينبغي تقييم ما إذا كان حظر الأسلحة النووية سيُسهم في تعزيز القضاء عليها وكيف؟

كانت معظم الدول قد أعربت عن فرحها وارتياحها لتبني معاهدة حظر الأسلحة النووية رابط خارجي (يُشار إليها اختصاراً بـ TPNW) في عام 2017. في حين اقتصرت (ردة فعل) الدول التي تمتلك الأسلحة النووية على

الصمت أو الإعراب عن استيائها من هذه المعاهدة. وجاءت هذه المعاهدة كثمرة للمؤتمرات الدولية حول العواقب الإنسانية لكل تفجير نووي وللمحادثات التي استمرت أسابيع عدة في جنيف. وكانت معظم الدول التي لديها أسلحة نووية قد قاطعت هذه الاجتماعات وعارضت المفاوضات التي جرت في نيويورك⁽⁹⁾.

(9) مارك فينو ، الوحدة الدولية التابعة لهيئة الإذاعة والتلفزيون السويسرية 2021/6/12

<https://www.swissinfo.ch/ara/%-/46314566>

وفي هذا المجال يمكن القول انّ انتشار أسلحة الدمار الشامل يشكل أحد أهم التحديات الأمنية ولعل التحدي الرئيسي الذي يقف امام عملية إدارة انتشار هذه الأسلحة هو مستوى الضغوط التي تواجهها المعاهدات الدولية الرئيسية الهادفة الى وقف انتشار أسلحة الدمار الشامل فعلى سبيل المثال تواجه معاهدة عدم انتشار الأسلحة النووية واتفاقية حظر الأسلحة البيولوجية والسامة واتفاقية حظر الأسلحة الكيميائية طائفة واسعة من الضغوطات الداخلية والخارجية التي تعرقل مهمة إقامة نظام عالمي لمنع الانتشار

المطلب الثاني: تطور دور الاتحاد الأوروبي كفاعل دولي في مجال عدم الانتشار النووي:

وفي ما يخص دور الاتحاد الأوروبي في هذا المجال وباعتبار الاتحاد فاعلاً دولياً مؤثراً في معظم القضايا الدولية المهمة حيث لم يكن الاتحاد الأوروبي عبر مختلف أطوار تطوره كفاعل دولي بمعزل عن الاهتمام بتلك القضية لاسيما في ظل

رغبته للعب دور فاعل فيها لاعتبارات تتعلق بأمنه ومكانته على الساحة الدولية. وقد وجدت الأسس القانونية والسياسية لعدم الانتشار النووي منذ الأيام الأولى للجماعة الأوروبية، من خلال الاتفاقية الأوروبية للطاقة الذرية عام 1957، والتي هدفت في المقام الأول إلى تعزيز تطوير الطاقة النووية ولكنها احتوت أيضاً على نظام متقدم نسبياً من ضمانات وضوابط التصدير، الأمر الذي منحها دوراً واضحاً في مجال عدم الانتشار، إلا أن نطاق عملها كان محدداً للغاية في المجال المدني وذلك نظراً لأن الاتفاقية اعفت جميع السلع المتصلة بالأمن القومي من لوائح الجماعة⁽¹⁰⁾ وبدأ دور الجماعة الأوروبية في مجال عدم الانتشار في التبلور خلال ثمانينات القرن الماضي، عندما قرر المجلس الأوروبي إنشاء مجموعة عمل بشأن المسائل النووية في سياق التعاون السياسي الأوروبي (EPC) عام 1981 وأصدر وزراء خارجية الدول الأعضاء العشر بالجماعة الأوروبية آنذاك اتفاق بشأن المبادئ التوجيهية لسياسة الصادرات النووية.

وفي بداية التسعينات، ومع تراجع فرنسا عن معارضتها التقليدية لمعاهدة عدم انتشار الأسلحة النووية (NPT) وانضمامها إليها عام 1991، أصبح بالإمكان تفعيل سياسة الجماعة الأوروبية بشأن عدم الانتشار، وبدأت أهداف عدم الانتشار تذكر في أعلى مستوى في هيكلها، مع إصدار المجلس الأوروبي أول بياناته حول منع انتشار الأسلحة النووية في قمتي دبلن ولوكسمبورج عامي 1990 و 1991. كما وصل التكامل الأوروبي إلى الحالة التي شعرت الدول الأعضاء فيها أنها مستعدة للشروع في إقامة تنسيق أوثق للسياسات الخارجية، فقد أحدثت معاهدة ماستريخت 1992 المنشأة للاتحاد الأوروبي نقلة نوعية في تنسيق السياسة الخارجية عبر استحداث السياسة الخارجية والأمنية المشتركة، والتي ساعدت تعزيز أدواتها وآلياتها إلى حد كبير على تطوير دور الاتحاد في مجال عدم الانتشار⁽¹¹⁾

خلال عقد التسعينات برزت مبادرات هامة للاتحاد الأوروبي في مجال عدم الانتشار النووي:

- حملة الاتحاد الأوروبي للتمديد اللانهائي لمعاهدة عدم الانتشار النووي (NPT) الذي جرى عام 1995، والذي بموجبه أصبحت جميع الدول التي تمتلك برامج نووية مهمة منضمة إلى معاهدة عدم الانتشار أو إلى إحدى المعاهدات الإقليمية التي تحظر انتشار الأسلحة النووية فيما عدا ثلاث دول وهي (إسرائيل والهند وباكستان).⁽¹²⁾
- التحرك المشترك "Joint Action" بشأن مشاركة الاتحاد الأوروبي في منظمة تنمية الطاقة في شبه الجزيرة الكورية (كيدو) عام 1995 وذلك بالاستناد إلى الاتفاقية الأوروبية للطاقة الذرية. وقد شكل سابقة لتمكين مشاركة أكثر

وجدت الأسس القانونية والسياسية لعدم الانتشار النووي منذ الأيام الأولى للجماعة الأوروبية

(10) سليمان حسين الوادعي ، الأطراف الأوروبية والاتفاق والاتفاق النووي مع إيران : تراجع الأهمية واحتمالات المستقبل ، المعهد الدولي للدراسات ، الرياض ، 2020 ، ص ص 6- 10 .

وبدأت أهداف عدم الانتشار تذكر في أعلى مستوى في هيكلها، مع إصدار المجلس الأوروبي أول بياناته حول منع انتشار الأسلحة النووية

(11) صادق النابلسي ، زياد ناصر الدين ، الاقتصاد المقاوم إيران من صناعة الأباريق إلى تقنية النانو ، شركة المطبوعات للتوزيع والنشر ، بيروت / لبنان ، 2020 ، ص ص 41- 43

(12) سليمان حسين الوادعي ، الأطراف الأوروبية والاتفاق النووي مع إيران ، مصدر سبق ذكره

نشاطا من قبل الاتحاد الأوروبي في قضايا عدم الانتشار في جميع أنحاء العالم، كما أظهر تعاوننا غير مسبوق وتنسيقا للعمل المشترك بين المفوضية الأوروبية والمجلس والبرلمان الأوروبيين بغية تبسيط مواقفهم بشأن تلك القضية الهامة والشائكة .

(13) ديفد فيشر ، الضمانات النووية
الخطوة الأولى ، مجلة الوكالة الدولية
للطاقة الذرية 49/1 ، أيلول 2007 ،
ص 7

• التحرك المشترك بشأن تعزيز الشفافية في ضوابط التصدير في المجال النووي عام 1997، وكان أكثر أهمية سياسيا من سابقه كونه يهدف إلى زيادة الشرعية والطابع الدائم للنظم الرقابة على الصادرات، وهو عنصر هام لبناء الثقة بين البلدان المصدرة للتكنولوجيا النووية والبلدان التي تشتريها.⁽¹³⁾

**أن التقدم نحو المعايير المشتركة
والعمل المشترك فيما يتعلق
بمكافحة الانتشار النووي كان ذو تأثير
محدود للغاية في مواجهة الأزمات
الحقيقية**

وتجدر الإشارة هنا الى أن التقدم نحو المعايير المشتركة والعمل المشترك فيما يتعلق بمكافحة الانتشار النووي كان ذو تأثير محدود للغاية في مواجهة الأزمات الحقيقية، وأبرز مثال على ذلك، أنه مع نشوب الأزمة النووية بين الهند وباكستان عام 1998، جاء رد فعل الاتحاد الأوروبي ضعيفا للغاية

نظرا للانقسامات بين الدول الأعضاء بشأن التعامل مع الأزمة، الأمر الذي جعل الولايات المتحدة الأمريكية في طليعة الجهود الدبلوماسية لاحتوائها. وشكل الحد من المخاطر النووية في أراضي الاتحاد السوفيتي السابق - سواء كانت مدنية أو عسكرية - ساحة رئيسية للجهود التي يبذلها الاتحاد الأوروبي لمكافحة الانتشار، ويرجع ذلك إلي أن هذه الأراض تقع في الجوار المباشر للدول الأعضاء، وهي مصدر رئيسي محتمل لتحويل المواد الانشطارية أو حتى الأسلحة إلى الدول أو الجماعات الإرهابية. وقد تركزت جهود الاتحاد الأوروبي بشأن السلامة والأمن، والتخلص من البلوتونيوم وتوظيف العلماء والمهندسين النوويين، وكان في طليعة تلك الجهود برنامج المساعدة الفنية لرابطة الدول المستقلة (TACIS) فضلا عن المساعدات لدول الاتحاد السوفيتي السابق والتي كانت موضعا للعديد من التحركات المشتركة للدول الأعضاء. وتحت مظلة الشراكة العالمية ضد انتشار أسلحة ومواد الدمار الشامل، تعهد الاتحاد الأوروبي بتخصيص مبلغ مليار يورو في الفترة من (2002-2012)، وقد تم تخصيص ما يقرب من نصف هذا المبلغ للسلامة النووية بشكل عام.⁽¹⁴⁾

(14) هادي زعرور ، توازن الرعب
، القوى العسكرية العالمية ، أمريكا
، روسيا ، إيران ، الكيان الصهيوني ،
حزب الله ، كوريا الشمالية ، شركة
المطبوعات للتوزيع والنشر ، الطبعة
الثانية ، 2017 ، ص 39

**المطلب الثالث: إطلاق استراتيجية الاتحاد
الأوروبي لمكافحة أسلحة الدمار الشامل عام 2003:**
تعد استراتيجية الاتحاد الأوروبي لمكافحة أسلحة الدمار الشامل إلى حد كبير وليدة هجمات 11 سبتمبر 2001 الإرهابية في الولايات المتحدة وتدابيرها، فعلى الرغم من أن أسلحة الدمار الشامل لم تستخدم في الهجمات، إلا أن حجم الدمار

الهائل سلط الضوء على احتمالات وجود صلة بين الإرهاب الدولي وأسلحة الدمار الشامل.

وقد ربط المجلس الأوروبي في أكتوبر 2001 بين احتمال وجود صلة بين التهديد الإرهابي وجهود الاتحاد الأوروبي بشأن عدم الانتشار والسيطرة على صادرات الأسلحة، ما جعله يفتح مسار التطور التدريجي لحقل تلك السياسة الجديدة على المستوى الأوروبي، عبر إطلاق مبادرة في ديسمبر 2001 تستهدف الاستجابة بصورة فعالة لفضايا عدم الانتشار ونزع السلاح والحد من التسليح في ظل التهديد الدولي للإرهاب. كما أعطي اعتماد الولايات المتحدة الأمريكية لاستراتيجية الأمن القومي الجديدة في سبتمبر 2002 واستراتيجية مكافحة أسلحة الدمار الشامل

وقد ربط المجلس الأوروبي في أكتوبر 2001 بين احتمال وجود صلة بين التهديد الإرهابي وجهود الاتحاد الأوروبي بشأن عدم الانتشار والسيطرة على صادرات الأسلحة

في ديسمبر من العام ذاته دفعة قوية للجهود الأوروبية في هذا المجال⁽¹⁵⁾ وفي فبراير 2003، وبناء على مبادرة من السويد، وافق مجلس الشؤون العامة والعلاقات الخارجية (GAERC) رسمياً على إعادة النظر في سياسة الاتحاد الأوروبي لعدم الانتشار. وفي يونيو من العام ذاته، مهد المجلس الأوروبي في اجتماعه في سالونيك باليونان الطريق لحقبة جديدة في استراتيجية الاتحاد الأوروبي لعدم الانتشار، وأعقب ذلك اعتماد المجلس الأوروبي رسمياً في ديسمبر 2003 لاستراتيجية الاتحاد الأوروبي لمكافحة انتشار أسلحة الدمار الشامل، وفي حين لم تضمن هذه النصوص أي اختراقات سياسية أو مفاهيمية الكبرى، إلا أنها شكلت أول نهج منظم وشامل للاتحاد الأوروبي للتصدي لمشكلة انتشار الأسلحة النووية. فضلاً عن اعتماد المجلس الأوروبي استراتيجية الأمن الأوروبية (ESS)، وتعد هذه الوثيقة هي الأولى من نوعها حيث وضع فيها كبار القادة السياسيين في الاتحاد الأوروبي تسلسلاً هرمياً للتهديدات المشتركة، حيث جاء انتشار أسلحة الدمار الشامل في المرتبة الثانية بعد الإرهاب.⁽¹⁶⁾

(15) نفس المصدر السابق، ص 41

(16) EU strategy against proliferation of weapons of mass destruction, the council, the European union office, Brussels, December 2003

وفيما عرفت استراتيجية الأمن الأوروبية، الانتشار النووي بأنه "يحتمل أن يكون أكبر تهديد لأمننا"، أكدت استراتيجية مكافحة أسلحة الدمار الشامل أن "انتشار أسلحة الدمار الشامل ووسائل إيصالها... تشكل تهديداً متزايداً للسلم والأمن الدوليين، وأن مواجهة تحدي

عرفت استراتيجية الأمن الأوروبية، الانتشار النووي بأنه "يحتمل أن يكون أكبر تهديد لأمننا"

الانتشار "يجب أن يكون عنصراً أساسياً في العمل الخارجي للاتحاد الأوروبي". في السياق نفسه، شددت استراتيجية مكافحة انتشار أسلحة الدمار الشامل على ضرورة استغلال الاتحاد الأوروبي جميع ما يتاح له من أدوات لمنع وردع ووقف الانتشار النووي، حيثما كان ذلك ممكناً، والقضاء على البرامج النووية التي تسبب قلقاً على الصعيد العالمي. أما عن أبرز النقاط التي تضمنتها الاستراتيجية الأوروبية لمكافحة انتشار أسلحة

(17) IBID

الدمار الشامل، فتمثل فيما يلي: (17)

1. التشديد على النهج التعاوني المتعدد الأطراف لتعزيز التحقق والامثال واتباع الأنظمة الدولية الموجودة بشأن مكافحة الانتشار النووي مثل معاهدة حظر الانتشار النووي لعام 1969.
2. استخدام الإكراه الاقتصادي أو العسكري للقضاء على تهديدات الانتشار وذلك فقط كخيار أخير، مع التأكيد على أن اللجوء الى التدابير القسرية يكون فقط بموجب الفصل السابع من الأمم المتحدة، وذلك في إشارة لاستبعاد التحركات المنفردة حيث أن الدور المركزي في تلك القضايا يجب أن يضطلع به مجلس الأمن الدولي.
3. التعاون بين الدول الأعضاء في الاتحاد الأوروبي للعمل من أجل إضفاء الطابع العالمي لنزع السلاح وقواعد عدم الانتشار.
4. مساعدة دول العالم الثالث في الوفاء بالتزاماتها بموجب الاتفاقيات المتعددة الأطراف المنظمة لتلك القضايا.
5. التركيز على سياسة تعزيز الامثال والالتزام بالمعاهدات الدولية المنظمة لتلك المجالات، والسعى نحو إستحداث تحسينات في آليات التحقق القائمة وعند الضرورة المساعدة على تطوير تلك الآليات من خلال إجراءات إضافية.
6. تأكيد أن تعزيز وجود بيئة دولية وإقليمية مستقرة شرط هام وضروري لمكافحة انتشار أسلحة الدمار الشامل.

”التعددية الفعالة“، والتي تتسم بالعزم على تحقيق ومتابعة الأهداف الأمنية المشتركة في إطار المؤسسات متعددة الأطراف وبالتحديد

وأطلق الممثل الأعلى للسياسة الخارجية والأمنية المشتركة بالاتحاد الأوروبي آنذاك، خافيير سولانا على هذا النهج الأوروبي الجديد مسمى ”التعددية الفعالة“، والتي تتسم بالعزم على تحقيق ومتابعة الأهداف الأمنية المشتركة في إطار المؤسسات متعددة الأطراف وبالتحديد، (الأمم المتحدة والمنظمات الإقليمية) وسيادة القانون مع التأكيد على أن القوة العسكرية وحدها لا يمكنها التغلب على التحديات والتهديدات الأمنية الرئيسية. وأعد مجلس الاتحاد الأوروبي عام 2008 تقريراً حول تطبيق الاستراتيجية الأمنية الأوروبية، بعد خمس سنوات من إقرارها خلص فيه إلي الحاجة الملحة للعمل على مواضيع محددة، من ضمنها: دعم الاتحاد الأوروبي لتوجه متعدد الأطراف فيما يتعلق بدورة الوقود النووي، مكافحة تمويل الانتشار، اجراءات خاصة بالأمان والأمن البيئي، احتواء انتشار أنظمة الايصال خاصة الصواريخ الباليستية، ووجوب البدء في مفاوضات حول اتفاقية متعددة الأطراف تمنع إنتاج المواد القابلة للانشطار للاستخدام في الأسلحة النووية.

وقد عزز اعتماد استراتيجية مكافحة انتشار أسلحة الدمار الشامل من نشاط الاتحاد الأوروبي في هذا المجال إلى حد كبير وهو ما يتضح في أكثر من مؤشر (18):

(18) الموقع الرسمي لقانون الاتحاد الأوروبي
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A133234>

- تزايد الوعي بأهمية قضايا الانتشار النووي بشكل كبير في أوساط الاتحاد الأوروبي، ما يتضح في تخصيص حوالي 25% من ميزانية السياسة الخارجية والأمنية المشتركة (CFSP) لأنشطة عدم الانتشار.
- اعتماد الدول الأعضاء للاتحاد الأوروبي منذ عام 2003 لأكثر من 20 إجراء مشترك لدعم عمل المنظمات الدولية في مجال منع الانتشار النووي ونزع السلاح، فعلي سبيل المثال يعد الاتحاد الأوروبي أكبر المانحين لصندوق الأمن النووي التابع للوكالة الدولية للطاقة الذرية، إذ يسهم بأكثر من 20 مليون يورو كدعم مالي للصندوق. وقد ساهم ذلك الدعم في توفير الحماية المادية للمرافق النووية، وحماية ومراقبة المصادر المشعة، واتخاذ تدابير لمكافحة الاتجار غير المشروع بالمواد النووية والإشعاعية، والمساعدة التشريعية لغرض تنفيذ البروتوكول الإضافي للوكالة الدولية للطاقة الذرية.

يعد الاتحاد الأوروبي أكبر المانحين لصندوق الأمن النووي التابع للوكالة الدولية للطاقة الذرية

- مساعدة الاتحاد الأوروبي العشرات من البلدان في أفريقيا والبلقان وآسيا الوسطى وجنوب شرق آسيا لمنع الإرهاب النووي من خلال تعزيز الحماية والأمن ومراقبة المواد النووية والمشعة الأخرى، ما جعله لاعباً عالمياً في مجال عدم الانتشار النووي على الأقل من الناحية الجغرافية.
- يعتبر الاتحاد الأوروبي معاهدة حظر الانتشار النووي لعام 1968 بمثابة "حجر الزاوية" لنظام حظر الانتشار النووي العالمي، لذلك فهو ينظر إلى مؤتمرات استعراض المعاهدة بأهمية شديدة، ويتبنى نهج متعدد الأطراف من خلال توفير الدعم السياسي والمالي القوي لمجموعة واسعة من المنظمات الدولية كالوكالة الدولية للطاقة الذرية أو مجموعات مثل لجنة زنجر ومجموعة موردي المواد النووية أو معاهدات و قرارات دولية مثل معاهدة الحظر الشامل للتجارب النووية لعام 1996 و قرار مجلس الأمن (1540).

يعتبر الاتحاد الأوروبي معاهدة حظر الانتشار النووي لعام 1968 بمثابة "حجر الزاوية" لنظام حظر الانتشار النووي العالمي

- بالإضافة إلى التعددية، انتهج الاتحاد الأوروبي عدم الانتشار من خلال أدوات السياسة الخارجية التقليدية، فقد أشار الاتحاد الأوروبي إلى عدم الانتشار في حواراته مع العديد من المنظمات الإقليمية وتعاون في هذا الشأن مع رابطة أمم جنوب شرق آسيا (آسيان) واجتماع آسيا-أوروبا (اسيم). وقدمت "يوراتوم" من خلال أداة التعاون للسلامة النووية نحو 524 مليون يورو بين عامي 2007 و 2013 إلى بلدان خارج الاتحاد الأوروبي لتحسين

(19) هادي زعرور ، توازن الرعب ، مصدر سبق ذكره ، ص 44

السلامة النووية، والحماية الإشعاعية، وضوابط السلامة الفعالة.⁽¹⁹⁾ فضلاً عما سبق، اعتمد مجلس الاتحاد الأوروبي في 13 ديسمبر 2010 مبادئ توجيهية جديدة لعمل الاتحاد الأوروبي في مجال مكافحة انتشار أسلحة الدمار الشامل ووسائل إيصالها بهدف إبراز أهمية تدابير عدم الانتشار داخل الاتحاد الأوروبي عبر تحويل هذه المسألة الأمنية الأساسية إلى أولوية شاملة لعدة قطاعات بالنسبة لسياسات الدول الأعضاء في هذا المجال، فضلاً عن تحديد أفضل الممارسات المتبعة وتعميم هذه الممارسات على الدول الأعضاء.. ويبقى هذا التعاون ربما أقل طموحاً ومؤسسية، ولكنه

اعتمد مجلس الاتحاد الأوروبي في 13 ديسمبر 2010 مبادئ توجيهية جديدة لعمل الاتحاد الأوروبي في مجال مكافحة انتشار أسلحة الدمار الشامل

مع ذلك يستند إلى التزامات سياسية رفيعة المستوى، وحتى لو كانت هذه الشراكات ليست كلها نفس القدر من الأهمية لمنع انتشار الأسلحة النووية بالنسبة للاتحاد الأوروبي ، إلا أنها تشكل أداة مفيدة في خدمة استراتيجية أكثر فعالية.

المطلب الرابع: السياسة لمكافحة الانتشار النووي والبرنامج النووي الإيراني شكل اعتماد (المبادئ الأساسية بشأن استخدام الإجراءات التقييدية) العقوبات في عام 2004 أول وثيقة محددة بشأن سياسة عقوبات الاتحاد الأوروبي. وتتمحور هذه المبادئ حول ثلاثة موضوعات عامة، وهي⁽²⁰⁾:

(20) Treaty on European union , official publication of the European communities , Brussels - Luxemburg , 1992 p 123

- احترام القانون الدولي بما في ذلك ميثاق الأمم المتحدة.
- الوحدة العضوية لأراضي الاتحاد الأوروبي، وتشجيع السلام والتعاون الدولي.
- تعزيز قيم مثل الديمقراطية وحقوق الإنسان والحريات الأساسية. وكانت هذه الموضوعات الثلاثة ترسخت أيضاً في استراتيجية الأمن الأوروبية لعام 2003، كمبادئ توجيهية لسياسة الأمن والدفاع الأوروبية.

(21) EU strategy against proliferation of weapons of mass destruction , OPCIT ,

وتؤكد وثيقة "المبادئ الأساسية" أن الطرف الرئيسي المخول فرض العقوبات هو الأمم المتحدة، مشيرة لحق الاتحاد الأوروبي أيضاً في استخدام تلك الآلية، مع تفضيل أن يجري ذلك في إطار تأييد دولي واسع.⁽²¹⁾

وتؤكد وثيقة "المبادئ الأساسية" أن الطرف الرئيسي المخول فرض العقوبات هو الأمم المتحدة

وتشير إلى أن فرض العقوبات الأوروبية، يجب أن يكون جزءاً من سياسة أكثر شمولية تشمل حواراً سياسياً وحوافز وشروط، فالعقوبات تبقى خيار أخيراً. وتضمنت الوثيقة أمثلة للمجالات التي قد يستخدم فيها الاتحاد الأوروبي العقوبات ومنها: دعم جهود مكافحة الإرهاب، مكافحة انتشار أسلحة الدمار الشامل، وكذلك استخدامها كإجراء تقييدي لتعزيز احترام حقوق الإنسان والديمقراطية وحكم القانون والحكم الرشيد. ومن الملفت للنظر أن هذه هي المجالات التي تمثل أيضاً التهديدات الرئيسية للدول الأعضاء في الاستراتيجية الأمنية

الأوروبية، فضلاً عن النزاعات الإقليمية والأعمال الإجرامية. إضافة إلى ذلك، لم تهتم الوثيقة فقط بأهداف العقوبات بل أيضاً فصلت معلومات أكثر احكاماً عن نوع العقوبات التي يمكن أن يستخدمها الاتحاد الأوروبي، موضحة أنها يجب أن تكون عقوبات موجهة (أي تستهدف قطاع بعينه) بدلاً من العقوبات الاقتصادية الشاملة، وقدمت ثلاثة أمثلة في هذا الصدد وهي حظر الأسلحة وحظر تأشيرات الدخول أو السفر وتجميد الأرصدة. وجاءت جهود الاتحاد الأوروبي بشأن مسائل عدم الانتشار

**لم تهتم الوثيقة فقط بأهداف
العقوبات بل أيضاً فصلت معلومات
أكثر احكاماً عن نوع العقوبات التي
يمكن أن يستخدمها الاتحاد الأوروبي**

متوازية مع تصاعد دور مجلس الأمن الدولي في هذا المجال، إذ أضحت قضية عدم الانتشار ظاهرة دولية واسعة النطاق، ففي عام 2006، فرضت الأمم المتحدة عقوبات على كل من كوريا الشمالية وإيران للمرة الأولى. وباتت لقضية عدم الانتشار مكانة ثابتة في جدول أعمال مجلس الأمن، فخلال 3 سنوات وتحديداً الفترة من 2006 إلى 2009 كانت نظم الجزاءات الجديدة الوحيدة التي وافق عليها المجلس تلك التي تهدف إلى تحقيق أهداف عدم الانتشار أو مكافحة الإرهاب. بشكل عام، هناك تحديين رئيسيين يواجهان نظام عدم الانتشار النووي، أولهما أنه يمكن لأي دولة تطوير قدرات نووية رغم كونها جزءاً من معاهدة حظر الانتشار النووي، ويكون بإمكانها حينها إما أن تنسحب من المعاهدة أو تبقى مع الحفاظ على قدرتها الكامنة لوضع اللمسات الأخيرة علي نحو سريع لبرنامجها للأسلحة النووية كجزء من استراتيجية دعم قوتها أو كحماية ضد التهديدات المستقبلية، وهو المسار الذي تعتقد الدول الأعضاء في الاتحاد الأوروبي أن كلا من كوريا الشمالية وإيران قد اتبعته.

أما عن التحدي الثاني، فيتمثل في الفاعلين من دون الدولة، مثل الجماعات الإرهابية، التي يمكن أن تسعى للحصول على المواد النووية، وهو تحدي خطير للغاية نظراً لكون الجماعات الإرهابية أكثر ميلاً لاستخدام هذه الأسلحة عن الدول.⁽²²⁾

**لا يزال الاتحاد الأوروبي بعيداً عن كونه
ممثلاً وحدوياً في مجال عدم الانتشار
النووي، فرغم اطلاقه لاستراتيجيته
لمكافحة انتشار أسلحة الدمار الشامل
2003**

وبعبارة أخرى، لا يزال الاتحاد الأوروبي بعيداً عن كونه ممثلاً وحدوياً في مجال عدم الانتشار النووي، فرغم اطلاقه لاستراتيجيته لمكافحة انتشار أسلحة الدمار الشامل 2003، إلا أنه لم يزل بحاجة أولاً إلى تحقيق إجماع داخلي بين الدول الأعضاء بشأن أي حالة من حالات الانتشار النووي، قبل أن يتخذ زمام المبادرة فيها، لذا تركز معظم الأنشطة بشكل كبير على عدم الانتشار، بدلاً من نزع السلاح. ورجح بعض من الباحثين تجاهل مسألة نزع السلاح النووي داخل الاتحاد الأوروبي لتجنب المواجهات مع بريطانيا وفرنسا بوصفهما الدولتان الوحيدتان اللتان تملكان أسلحة نووية بين الدول الأعضاء في المنظمة، وأيضاً للسماح بتمرير

(22) سعد حقي توفيق، الاستراتيجية النووية بعد انتهاء الحرب الباردة، مصدر سبق ذكره، ص 277

هادئ لأجندة الاتحاد والمضي قدما في جهوده للتصدي لتلك القضية الخطيرة. ومع استمرار تهميش مسألة نزع السلاح ، لا تزال سياسة الاتحاد الأوروبي لعدم الانتشار "انتقائية"، وهذا يؤكد عدم العدالة في تنفيذ ما كان من المفترض أن يكون صفقة عادلة وينال من مصداقية تلك السياسة. وعلاوة على ذلك، أدى التوسع الكبير للاتحاد الأوروبي في السنوات الـ 10 الماضية الى أن أصبح بين صفوفه عدد كبير من أعضاء حلف شمال الأطلسي (الناتو) المضيفين لأسلحته النووية.

وان ابرز القضايا الدولية التي عبرت عن دور الاتحاد الأوروبي في منع انتشار أسلحة الدمار الشامل هو البرنامج النووي الإيراني الذي يعد التطبيق الفعلي لدور الاتحاد الأوروبي

ففي عام 2003 كان الاتحاد الأوروبي يضم 11 عضوا في حلف الناتو و دولتان تملكان أسلحة نووية و 4 مضيئة لأسلحة النووية للحلف، أما في عام 2014 أصبح لدى الاتحاد 22 دولة أعضاء في الناتو، وبالتالي هم تحت مظلته النووية، ما يدفع لاستبعاد تحقق دفعة لأي جهد وتنسيق مشترك لنزع السلاح داخل الاتحاد الأوروبي من غير المرجح.

من ناحية أخرى، تأثر دور الاتحاد الأوروبي في قضايا الحد من التسليح بالتقسيم المستقبلي للعمل في هذا المجال مع حلف "الناتو"، وذلك في ضوء العلاقة التنافسية بين المنظمتين بشأن القضايا الخارجية والدفاع. ونظرا لاهتمام البعض داخل حلف الناتو بمنحه دورا أقوى في قضايا منع ومكافحة الانتشار النووي، فقد فرضت تلك الرغبة على الاتحاد الأوروبي حتمية إعادة تأكيد دوره في تلك القضية. ولاشك أن انضمام فرنسا إلى البنية العسكرية المتكاملة لحلف الناتو عام 2009 ، أعطي دفعة جديدة لإعادة تنظيم تلك العلاقة بين المنظمتين. ويتضح مما سبق، أنه لم يتم توجيه جهود الاتحاد الأوروبي لعدم الانتشار عبر استراتيجية طويلة المدى، ولكن وضع الاتحاد لنفسه أهدافاً متوسطة المدى تمثل "طريقاً وسطاً" ما بين الحفاظ على الوضع النووي الراهن ومقترحات بعيدة المدى لدول راغبة في نزع السلاح.

وان ابرز القضايا الدولية التي عبرت عن دور الاتحاد الأوروبي في منع انتشار أسلحة الدمار الشامل هو البرنامج النووي الإيراني الذي يعد التطبيق الفعلي لدور الاتحاد الأوروبي كفاعل دولي مؤثر حيث بحسب وجهة النظر الأوروبية، الاتفاق النووي ذو أهمية فائقة باعتباره يرمي إلى وضع حلول لإحدى أخطر وأطول أزمات الانتشار النووي في الشرق الأوسط، والحيولة دون تسابق دول إقليمية على التسليح النووي ففي حال تطبيق القيود الفيزيائية وأحكام التطبيق المنصوص عليها في الاتفاق، تهدف الدول الأوروبية إلى ترحيل احتمالية تطوير قنبلة نووية إيرانية لفترة من الزمن، من خلال إعاقة إنتاجها لمواد قابلة للانفجار في مرافقها النووية المعلن عنها وللاتحاد الأوروبي مصالح بيئية يمكن سردها في أربعة سياقات أساسية تشمل:⁽²³⁾

أولاً: ضمان الاستقرار في منطقة الخليج العربي، التي تُعد ذات أهمية قصوى لإمدادات الطاقة العالمية وتأرجح أسعارها.

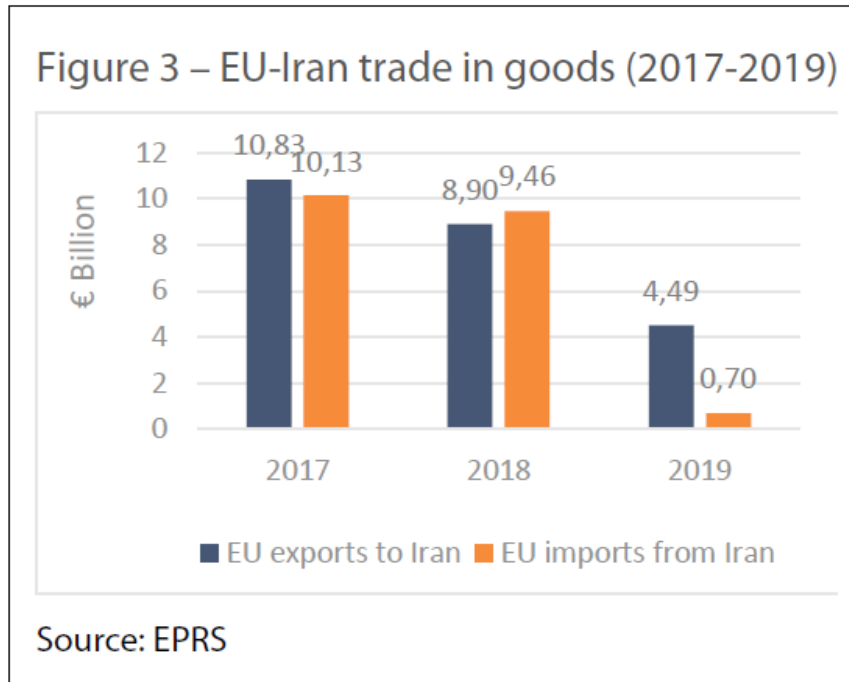
(23) سليمان حسين الوادعي ، الأطراف الأوروبية والاتفاق النووي مع إيران ، مصدر سبق ذكره ، ص 8

ثانياً : وضع حل نهائي للصراعات الإقليمية بُغية تأمين الحماية لأوروبا ضدّ معضلات الهجرة إلى البلدان الأوروبية، على غرار ما حدث نتيجة الأزمة السورية، فضلاً عن موجات الإرهاب التي طالت عدداً من مدن القارة
ثالثاً : تنويع مصادر الطاقة لدول الاتحاد الأوروبي، وتخفيض اعتمادها الكبير على روسيا.

رابعاً : تعزيز صادراتها خصوصاً البضائع لصناعية بتوسيع نطاق الشراكة الاقتصادية مع إيران، كونها تمثل فرصة ذهبية أمام الشركات الأوروبية، في ظلّ اقتناص الشركات الأمريكية لمعظم الفرص الاستثمارية في منطقة الشرق الأوسط.

شكل رقم (1)

التبادل التجاري بين الاتحاد الأوروبي وايران



EU-Iran: The way forward

Can the JCPOA survive the Trump presidency? , European parliament

European Parliamentary Research Service, 2020 ,p6

الشكل السابق يوضح مستوى التبادل التجاري بين الاتحاد الأوروبي وايران وهو أمر يدل على مدى أهمية استقرار العلاقات ورفع العقوبات للطرفين وما يسترعي الانتباه أنّ البرنامج النووي الإيراني، والذي يشكّل خطراً نوعياً على الأراضي الأوروبية لم يُضمّن في الاتفاق النووي، والعلّة تكمن في اعتبارات أوروبية وأخرى متعلّقة بسياسة إدارة الرئيس الأمريكي السابق باراك أوباما والتي

ارتأت في عملية التكامل ما بين الاقتصاد الإيراني ونظيره الغربي والعالمي أُن يكون عاملاً مؤثراً لخلق سياسيات وسلوكاً أكثر اعتدالاً للحكومة الإيرانية ما يفضي إلى تدخُل المصالح الغربية والإيرانية وتوافقها وباستقصاء تاريخي للرجبة الأوروبية في الانفتاح تجاه إيران سياسياً واقتصادياً، نجد أنّ واحداً من أبرز دوافع الاتحاد

الأوروبي يتجلى في جُوحه للعب دور محوري على مسرح العلاقات الدولية، ومزاحمة الهيمنة الأمريكية المتصاعدة من بعد الحرب الباردة وانهيار الاتحاد السوفيتي؛ ما يؤكّد إصرار الاتحاد على عدم ترك الولايات المتحدة تنفرد في معالجة مشكلات المنطقة والاستثمار بمعظم فرصها الاستثمارية على النطاق الاقتصادي، شركات خدمات مالية أوروبية عديدة رحّبت بالاتفاق النووي، معتبرة إياه أهمّ ثروة

من أبرز دوافع الاتحاد الأوروبي يتجلى في جُوحه للعب دور محوري على مسرح العلاقات الدولية

اقتصادية مربحة للقارة الأوروبية منذ انهيار الاتحاد السوفيتي. الوزير الألماني للشؤون الاقتصادية والطاقة آنذاك، زيغمار غابرييل، حطّ الرحال في 14 يوليو 2015 م بعد الإعلان عن الاتفاق مباشرة، في إيران مصطحباً⁽²⁴⁾

معه وفداً كبيراً من رجال الأعمال ومنسوبي القطاعات التجارية، بُعِيه عقد الصفقات والتوقيع على عقود الاستثمار مع الطرف الإيراني. ووزير الخارجية الفرنسي لورنت فابوس، بعد أسبوعين من توقيع الاتفاق، زار طهران للغرض ذاته، كما أرسلت إيطاليا وفداً مكوثاً من

300 رجل أعمال إلى طهران في بداية شهر اب 2015 في ظاهر الأمر استئناف الصلات السياسية والاقتصادية مع إيران، تمّ تسويغه ضمن سياق السياسات العامة في ألمانيا خاصّة، وبالقارة الأوروبية على وجه العموم، كجزء من سياسة التغيير عبر التبادل التجاري والعلاقات الودّية (CTTR) وهو ما منح هذا الاستئناف مناعةً ضدّ أيّ تقييم موضوعي⁽²⁵⁾

في يوليو 2015 ، وقعت إيران ومجموعة الدول الأوروبية الثلاث / الاتحاد الأوروبي + 3 (فرنسا وألمانيا والمملكة المتحدة) والاتحاد الأوروبي فضلاً عن الصين وروسيا والولايات المتحدة الأمريكية) على خطة العمل الشاملة المشتركة ، وهي اتفاقية تاريخية لضمان الطبيعة السلمية لبرنامج إيران النووي. مقابل إنهاء الإجراءات التقييدية ضد إيران. بعد شهادة من الوكالة الدولية للطاقة الذرية بأن إيران امتثلت لالتزاماتها بتفكيك الأسلحة النووية ، بدأ تنفيذ خطة العمل الشاملة المشتركة في 16 يناير 2016. في ذلك اليوم ، المعروف بيوم التنفيذ ، جميع عقوبات الأمم المتحدة والولايات المتحدة والاتحاد الأوروبي المتعلقة بالطاقة النووية عن إيران. ومع ذلك ، فإن الرئيس ترامب ، الذي تولى منصبه في كانون الثاني (يناير) 2017 ، وصف باستمرار خطة العمل الشاملة المشتركة بأنها «صفقة مروعة». في 8 مايو 2018 ، أعلن الرئيس ترامب أن الولايات المتحدة ستسحب من الاتفاق النووي مع إيران وستعيد (فرض) العقوبات. تمنع

(24) Fiedler Radoslaw , Iran and the European union after the nuclear deal , working papers , Alexandru Ioan Cuza University, Poland , 2018 , p 294

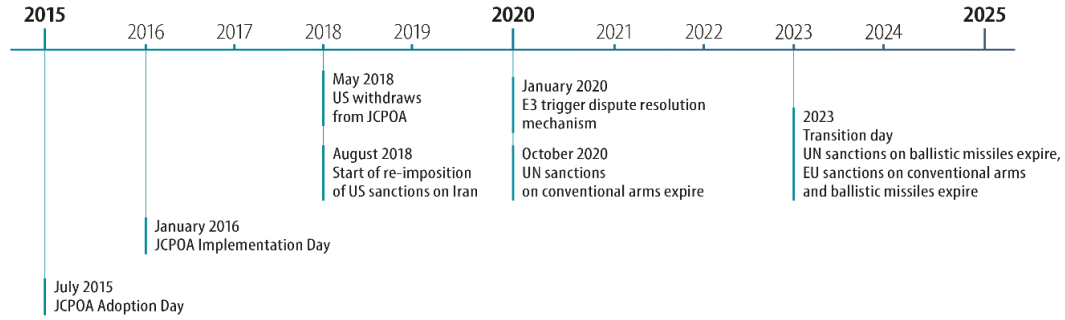
(25) محمد مطاوع ، السياسات الأمريكية - الأوروبية تجاه الاتفاق النووي الإيراني الادراكات والتفسيرات ، مجلة دراسات ، المجلد الحادي والعشرون ، العدد الرابع ، القاهرة /مصر ، 2020 ، ص ص 150 - 153

العقوبات الأمريكية الشركات الأمريكية من ممارسة الأعمال التجارية في إيران ، وتمنع الشركات الأجنبية التي تتعامل مع إيران من الوصول إلى النظام المصرفي والمالي الأمريكي بالكامل⁽²⁶⁾.

(26) نفس المصدر السابق

شكل رقم (2)

الخطة الاستراتيجية للتعامل مع البرنامج النووي الإيراني



EU-Iran: The way forward

Can the JCPOA survive the Trump presidency? , European parliament

European Parliamentary Research Service, 2020 , p 4

يوضح المخطط خطة العمل الشاملة المشتركة التي وضعها الاتحاد الأوروبي للعمل على وصول لحل بخصوص البرنامج النووي الإيراني حيث في يوليو 2015 ، وقعت إيران ومجموعة E3 / EU + 3 (فرنسا وألمانيا والمملكة المتحدة) (المملكة المتحدة) والاتحاد الأوروبي فضلاً عن الصين وروسيا والولايات المتحدة الأمريكية) على خطة العمل الشاملة المشتركة ، وهي اتفاقية تاريخية لضمان الطبيعة السلمية لبرنامج إيران النووي. مقابل إنهاء الإجراءات التقييدية ضد إيران. بعد شهادة من الوكالة الدولية للطاقة الذرية بأن إيران امتثلت لالتزاماتها بتفكيك الأسلحة النووية ، بدأ تنفيذ خطة العمل الشاملة المشتركة في 16 يناير 2016. في ذلك اليوم ، المعروف بيوم التنفيذ ، جميع عقوبات الأمم المتحدة والولايات المتحدة والاتحاد الأوروبي المتعلقة بالطاقة النووية عن إيران. ومع ذلك ، فإن الرئيس ترامب ، الذي تولى منصبه في كانون الثاني (يناير) 2017 ، وصف باستمرار خطة العمل الشاملة المشتركة بأنها «صفقة مروعة». في 8 مايو 2018 ، أعلن الرئيس ترامب أن الولايات المتحدة ستسحب .

من الاتفاق النووي مع إيران وستعيد (فرض) العقوبات. تمنع العقوبات الأمريكية الشركات الأمريكية من ممارسة الأعمال التجارية في إيران ، وتمنع الشركات الأجنبية التي تتعامل مع إيران من الوصول إلى النظام المصرفي والمالي الأمريكي

بالكامل. (27)

الخاتمة:

(27) Can the JCPOA survive the Trump presidency? , European parliament, European Parliamentary Research Service, 2020 ,p4 EU-Iran: The way forward

ومن خلال ماتقدم يتبين لنا أنّ انتشار أسلحة الدمار الشامل تمثل تحدياً بالنسبة للقوى الدولية الفاعلة والتي هي حائزة على السلاح النووي وحاولت قدر المستطاع بذل جهود حثيثة للحد من هذا الانتشار لكنها لم تكن بالمستوى المطلوب الذي من الممكن أن يحد من هذا الانتشار أما أزمة ملف إيران

أنّ انتشار أسلحة الدمار الشامل تمثل تحدياً بالنسبة للقوى الدولية الفاعلة والتي هي حائزة على السلاح النووي وحاولت قدر المستطاع بذل جهود حثيثة للحد من هذا الانتشار

النووي والذي يمكن أن يؤدي الى حرب فايران تصر على سلمية برنامجها النووي لكن المعلومات الاستخباراتية تشير الى أن إيران قادرة على صنع قنبلة نووية وان إيران تحاول شراء الوقت مع العلم انّ الأمور قد تبدو انها اتجهت نحو الهدوء غير أنّ اندلاعها وتفجيرها لايزالان قائمين والخدع السياسية ليست جديدة او حديثة العهد كما يبدو ان الجميع

يستعد وهذه الأزمة تبقى هادئة عسكرياً على الأقل ولكنها احدى الازمات العالمية التي تهدد باشعال حرب إقليمية او حرباً عالمياً اذا تفاقمت الظروف لايزال يتعين على الأوروبيين وإدارة

بايدن المساومة حول كيفية التوصل إلى صفقة أخرى مع إيران تتضمن المصالح الاستراتيجية للاتحاد الأوروبي فيما يتعلق بإيران ثلاثة أهداف مترابطة:

أولاً: دعم النظام الدولي لعدم الانتشار ومنع إيران، أو أي دولة أخرى في هذا الشأن، من تطوير سلاح نووي.

ثانياً: لتجنب حرب شاملة بين الدول تشمل إيران والمخاطرة بمزيد من عدم الاستقرار الإقليمي.

ثالثاً: إظهار قدرة الاتحاد الأوروبي على العمل على الساحة الدولية؛ حيث حقق الاتحاد الأوروبي جميع هذه الأهداف الثلاثة من خلال خطة العمل الشاملة المشتركة لعام 2015، وتشبث صانعو السياسة الأوروبيون بالاتفاق منذ ذلك الحين.

قائمة المصادر:-

1-اللجنة الدولية للصليب الأحمر , 24 / 4 / 2018

<https://www.icrc.org/ar/document/2017-treaty-prohibition-nuclear-weapons>

2- الوكالة الدولية للطاقة الذرية

<https://www.iaea.org/ar/almawadie/mueahadat-edm-alaintishar>

3- الموقع الرسمي لقانون الاتحاد الأوروبي

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A133234>

4- بول ويلكينسن , العلاقات الدولية /مقدمة قصيرة جدا , كلمات عربية للترجمة والنشر , ترجمة لبنى عماد تركي , مصر , 2013

5- جامعة منيسوتا , مكتبة حقوق الانسان , معاهدة عدم انتشار الأسلحة النووية 2021/6/13

<http://hrlibrary.umn.edu/arabic/TNPNW.html>

- 6-ديفيد فيشر , الضمانات النووية الخطوة الأولى , مجلة الوكالة الدولية للطاقة الذرية 49/1 , أيلول 2007
- 7- سعد حقي توفيق , الاستراتيجية النووية بعد انتهاء الحرب الباردة , دار زهران للنشر والتوزيع , عمان - الأردن , 2008
- 8- سعد حقي توفيق , مبادئ العلاقات الدولية , الطبعة الرابعة , المكتبة القانونية للنشر والتوزيع , بغداد , العراق , 2009
- 9- سليمان حسين الوادعي , الأطراف الأوروبية والاتفاق والاتفاق النووي مع ايران : تراجع الأهمية واحتمالات المستقبل , المعهد الدولي للدراسات , الرياض , 2020 ,
- 10- صادق النابلسي , زياد ناصر الدين , الاقتصاد المقاوم ايران من صناعة الاباريق الى تقنية النانو , شركة المطبوعات للتوزيع والنشر , بيروت / لبنان , 2020
- 11- محمد مطوع , السياسات الامريكية - الأوروبية تجاه الاتفاق النووي الإيراني الادراكات والتفسيرات , مجلة دراسات , المجلد الحادي والعشرون , العدد الرابع , القاهرة /مصر ,
- 12- مارك فينو , الوحدة الدولية التابعة لهية الإذاعة والتلفزيون السويسرية 2021/6/12
- 13- معاهدة عدم انتشار الأسلحة النووية , سلسلة وقائع التابعة للأمم المتحدة , نيويورك , 1985 , المادة الثالثة
- 14- هادي زعرور , توازن الرعب , القوى العسكرية العالمية , أمريكا , روسيا , ايران , الكيان الصهيوني , حزب الله , كوريا الشمالية , شركة المطبوعات للتوزيع والنشر الطبعة الثانية , 2017
- 15-Fiedler Radoslaw , Iran and the European union after the nuclear deal , working papers , Alexandru Ioan Cuza University, Poland , 2018
- 16- Can the JCPOA survive the Trump presidency? , European parliament , European Parliamentary Research Service, 2020 ,p4 EU-Iran: The way forward
- 17- EU strategy against proliferation of weapons of mass destruction ,the council ,the European union office , Brussels ,December 2003
- 18-Treaty on European union , official publication of the European communities , Brussels – Luxemburg , 1992
- 19- <https://www.wikipedia.org/nuclear weapon>

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

*أ.م.د. كرار عباس متعب فرج

باحث من العراق

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

ملخص :

تعد الحرب السيبرانية احدى أدوات الجيل الخامس للحروب، إذ أخذت حيزاً واسعاً ومؤثراً في الوقت الحاضر؛ بسبب كلفتها القليلة للجهة المهاجمة بخلاف الجهة المستهدفة التي تكون منشأتها ومواقعها الحيوية وبنائها التحتية في مرمى التدمير والإنهاء والإبطاء، وهذا ما ترجم فعلياً بين طرفي الصراع بين الولايات المتحدة الأمريكية وإيران (محل 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 الأمريكية المتعاقبة من جهة، وعبر الرؤساء الإيرانيين المتعاقبون من جهة أخرى، إذ أنشأت مؤسسات 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 إلا إذا تم التحكم الاستراتيجي بها، فضلاً عن ما تقدم وللضرورة العلمية تم طرح الحرب السيبرانية من حيث نشأتها ومفهومها مع المفاهيم المقاربة لها استكمالاً لموضوع 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 أهمية الموضوع من الحرب السيبرانية نفسها باعتبارها إحدى أدوات الجيل الخامس للحروب التي مجال صراعها هو الفضاء السيبراني وأسلحتها هي البرمجيات والفايروسات ذات الصفة التدميرية الموجهة ضد المواقع الحيوية والبنى التحتية للدول المستهدفة مع أقل كلفة للدول المهاجمة وهذا ما ترجم بين الطرفين الولايات المتحدة الأمريكية وإيران (محط الدراسة) الذي أصبح صراع الهجمات السيبرانية بينها هو السائد بدءاً من عام 2006 وحتى وقتنا الحاضر، من خلال تلك الهجمات الاستراتيجية السيبرانية لكل طرف والرد عليه بالمثل أو بهجوم استباقي، وهذا ما دفعنا للبحث العلمي في هذا الموضوع لمعرفة مسار تلك الهجمات الاستراتيجية السيبرانية لكل طرف لأهمية ذلك لأنه قد يمهد في المستقبل للمواجهة الشاملة بين الطرفين إلا 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 الأمريكية 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 كالاتي:

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 التوجهات الاستراتيجية للولايات المتحدة الأمريكية عبر ادارتها المتعاقبة في طرح استراتيجيتها السيبرانية الخارجية ؟ وما هي الهجمات السيبرانية للولايات المتحدة الأمريكية التي استهدفت فيها ايران منذ انطلاقتها 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 الأمريكية 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 الأمريكية وإيران (محط الدراسة) من خلال طرح استراتيجية الهجمات السيبرانية ضمن التوجهات الاستراتيجية لكل طرف عبر الإدارات المتعاقبة داخل الولايات المتحدة الأمريكية وكذلك في إيران، خاصة منذ انطلاقتها 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: الأول: تناول الحرب السيبرانية بمطلين: المطلب الأول: الحرب السيبرانية (النشأة والمفهوم، المفاهيم المقارنة لها)، اما المطلب الثاني: تناول الحرب السيبرانية (الوسائل والأهداف) اما المبحث الثاني: تناول الحرب السيبرانية (الولايات المتحدة الأمريكية وإيران) بمطلين: المطلب الأول: استراتيجية الهجمات السيبرانية للولايات المتحدة الأمريكية حيال إيران، اما المطلب الثاني: استراتيجية الهجمات السيبرانية الإيرانية حيال الولايات المتحدة الأمريكية.

المبحث الأول: الحرب السيبرانية

تعدّ الحرب السيبرانية إحدى 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 بمطلين:

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

المطلب الأول: الحرب السيبرانية (النشأة والمفهوم - المفاهيم المقارنة لها).
المطلب الثاني: الحرب السيبرانية (الوسائل والأهداف).

المطلب الأول: الحرب السيبرانية (النشأة والمفهوم - المفاهيم المقارنة لها)
اشتُقَّت السيبرانية من الكلمة اللاتينية (cyber) ويقصد بها «افتراضي» أو «تخيُّلي» وتستخدم ضمن مجال الفضاء الذي يضم الشبكات العنكبوتية المحوسبة،

(1) أميرة 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، ص 378 .
(2) حيدر ناظم عبد علي، رباب محمود عامر، التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة، مجلة الكوفة، العدد 47، جامعة الكوفة، 2019، ص 109.

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

(3) الحروب السيبرانية - نتائج ملموسة لمعارك غير مرئية، الجندي، بتاريخ 1/1 أبريل/2021، ص 1، 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 -

**الحرب السيبرانية ميدانها الفضاء
السيبراني وهي غير محدودة
المجال وتكون غامضة الأهداف
لأنها تتحرك عبر شبكة المعلومات
والاتصالات**

(5) زينب شنف، الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش، المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 2، جويلية (يوليو)، الجزائر، 2020، ص 91.

ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد وكل ما يتعلق بأنظمة الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، والسيبرانية هي: علم التحكم الأوتوماتيكي والقيادة والتوجيه عن بعد.⁽¹⁾

وجاء معنى كلمة سايبير (cyber) في قاموس المورد بـ (الكمبيوتر) أو (عصري جداً)، وعند البحث عن مصطلح السايبر في القواميس نجد غالبية القواميس الإنجليزية بصورة عامة والعربية بصورة خاصة تفتقر لهذا المصطلح لحدثه، وان قاموس مايكروسوفت للحاسوب قد تناول هذا المصطلح وبأنه مشتق البادئة (cy-ber) وهو علم التحكم الآلي.⁽²⁾

إذ تعود بداية نشأة الحروب السيبرانية الى مرحلة الحرب الباردة فإن أول حرب سيبرانية وقعت كانت بين الولايات المتحدة الأمريكية والاتحاد السوفيتي في عام 1982، إذ قام جهاز المخابرات السوفيتي (سابقاً) (KGB) بعملية تسمى (Line X) صممت لتساعد الاتحاد السوفياتي على سرقة تكنولوجيا المعلومات لكل أنشطة الغرب، إذ قامت المخابرات السوفيتية

بتدريب جيش من العلماء على التسلل الى الشركات والوكالات لسرقة المعلومات مع تسرب المعلومات إلى وكالة المخابرات الأمريكية (CIA) والتي قامت بدلاً من القاء القبض عليهم تركتهم يواصلون العمل ولكن مع امدادهم بمعلومات مغلوطة، وإذ حصل الجواسيس السوفيت على وثائق تتضمن مخططات ولكن تتضمن خطأ بسيطاً في الشفرة مع استمرار السوفيت باستخدام المعلومات المغلوطة لبناء العمود الفقري لخطوط نقل الغاز الطبيعي والنفط القادم من سيبيريا، وبعد فترة قصيرة تسبب الخطأ المتعمد في الشفرة في حدوث انفجار لخط الأنابيب وكان هذا الانفجار يعادل ثلث حجم انفجار القنبلة النووية في هيروشيما.⁽³⁾

أما الحرب السيبرانية كإطار عام للمفهوم فإنها تُشَنُّ ضد كيانات محددة بهدف تعطيلها والحفاظ على مجال المعلومات من أي اعتداء سيبراني من طرف الخصم باستخدام الوسائل التكنولوجية والمعلوماتية المتطورة.⁽⁴⁾

وعرّفت وزارة الدفاع الأمريكية الحرب السيبرانية بأنها: توظيف القدرات السيبرانية حيث يكون الهدف الأساسي هو تحقيق الأهداف والآثار العسكرية في الفضاء السيبراني أو من خلاله، وهي أيضاً نشاط مماثل أو غير مماثل 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⁾

وإن الحرب السيبرانية ميدانها الفضاء السيبراني وهي غير محدودة المجال وتكون غامضة الأهداف لأنها تتحرك عبر شبكة المعلومات والاتصالات المتعدية للحدود الدولية فضلاً عن اعتمادها على أسلحة إلكترونية 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 توصلت 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⁾

(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، ص 6.

(7) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، ط1، القاهرة، 2019، ص 114.

واستكمالاً لمفهوم الحرب السيبرانية فيعرفها كل من (ريتشارد كلارك) و (روبرت كناكي) بأنها: أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تدميرها، ويعرفها (بولو شاكريان) على أنها: استمرار أو امتداد للسياسة عن طريق

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

الاجراءات المتخذة في الفضاء السيبراني من دول أو فاعلين غير دوليين، إذ تشكل تهديداً خطيراً للأمن القومي.⁽⁸⁾

وتتميز الحرب السيبرانية 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 لشنها.
- 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 جداً على عقلية التحصن لوحدها أن تنجح.
- 4- حرب هلامية الشكل والملمح: فهي متعددة بميادينها، متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوراً وتبدلاً في الحياة المعاصرة للدول وهي تطل 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 الإلكتروني وسع دائرة استهداف المواقع بمستوياتها كافة.

(8) إسماعيل زروق، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، منشورات جامعة الشهيد حمة لخضر بالوادي، المجلد 10، العدد 1، الجزائر، 2019، ص 12.

(9) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلام الدوليين، مجلة قضايا سياسية، العدد 57، جامعة النهريين - 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 بأنه عالم افتراضي يتشارك مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد، إذ تقوم العلاقة بين العالمين على نظرة تكاملية ويوصف بأنه الذراع الرابع للجيش الحديث إلى جوار القوات البرية والجوية والبحرية.⁽¹¹⁾

ويعرف الفضاء السيبراني بأنه عالم افتراضي يتشارك مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد.

ويعرف أيضاً بأنه المستودع الكبير الذي تجري فيه جميع عمليات التواصل الإلكتروني عبر شبكات الحواسيب، وهو منظومة من العناصر المتفاعلة فيما بينها والمكونة من أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات.⁽¹²⁾

كما عرّفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي بأنه فضاء التواصل المشكل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، وأنه لا يقتصر على شبكة الانترنت فقط وإنما 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 التكنولوجي المتسارع والتي تسمح للمخترقين من الاختراق بسهولة سواء من الدول أو من غيرها.⁽¹⁴⁾

الهجمات السيبرانية بأنها الجهود الرامية إلى تغيير، تعطيل أو تدمير أنظمة الحاسوب أو الشبكات أو المعلومات أو البرامج الموجودة عليها

وتعرف الهجمات السيبرانية وفق ما تبنته القيادة الاستراتيجية الأمريكية عام 2007 بأنه تطويع عمليات نظام الكمبيوتر بهدف منع الخصم من الاستخدام الفعال لها فضلاً عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع البيانات التي تحتويها وحيازتها وتحليلها، وعرّفته شميت (Schmitt) المتخصص في القانون الدولي الإنساني بأنه الهجوم السيبراني

هو أي تصرف إلكتروني دفاعي كان أو هجومي يتوقع منه وعلى نحو معقول في التسبب بجرح أو قتل شخص أو الحاق أضرار مادية أو دمار بالهدف المهاجم.⁽¹⁵⁾ ويعرف (Matthew C. Waxman) الهجمات السيبرانية بأنها الجهود الرامية إلى تغيير، تعطيل أو تدمير أنظمة الحاسوب أو الشبكات أو المعلومات أو البرامج الموجودة عليها، والأضرار التي تسببها هذه الهجمات يمكن أن تصيب شبكة

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

(11) نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني «التهديد المتصاعد لأمن الدول»، مجلة مركز بابل للدراسات الإنسانية، المجلد 8، العدد 2، جامعة بابل، 2018، ص 190.

(12) محمد وائل القيسي، مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو - معلوماتية والفضاء السيبراني، مجلة دراسات إقليمية، مركز الدراسات الإقليمية، السنة 14، العدد 44، نيسان، جامعة الموصل، 2020، ص 153 - 154 .

(13) 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، ص 149.

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

(15) 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، 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⁾

وإنّ 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 بأنه التلصص الإعلامي والاستعراض التكنولوجي والمحاكاة

(16) حيدر أدهم الطائي، علي محمد كاظم، المشاركة المباشرة للهيئة 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 ijarccce, volume 7, issue 11, November, 2018, p2.

(18) 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, 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، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، السنة 12، العدد 62، جامعة النهرين، كلية العلوم السياسية، 2020، ص277.

(21) Robert "Jake" bebbber, 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 mozink and boris, I bid, p 4.

الاستراتيجية لإنشاء صورة رقمية مفرطة لهيمنة دولة ما سيبرانياً عبر نطاق الفضاء السيبراني لردع الخصم سيبرانياً.⁽²⁵⁾

7- الاستراتيجية السيبرانية (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 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⁾

وإن 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 لوضع ساعات او أيام ومثال على ذلك ما حدث في عام 2005 عندما قام القراصنة الروس بتشويه العديد من المواقع الحكومية.

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 وإنَّ 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), Switzerland, 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.

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

(28) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الامن القومي، مصدر سبق ذكره، ص 115.

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

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

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 شدة 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 إما بالإزالة أو التعديل أو الحذف أو 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 أو 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 طروادة (Trojan horses): وهي شفرة أو برنامج صغير يختبئ في برنامج كبير من البرامج ذات الشعبية العالية، إذ يقوم على نشر دودة أو 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 أو البرنامج إذ أن البرنامج أو الجهاز مصاباً منذ البدء بالبرنامج الضار أي بالسلح السيبراني اذ يبدأ عمل البرنامج الضار تحت ظروف معينة تكون في المحصلة والهدف النهائي هو التحكم في الجهاز بصورة تامة أو اتلافه.
- 5- البرمجيات الخبيثة مثل «اريد البكاء» (wanna cry): وقد تميزت هذه البرمجيات بأنها تستهدف الكيانات الاقتصادية وليست الافراد وذلك لأن 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 ان 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 ان 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 الأمن 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 ومثل 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 (crysylab) 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⁾

المبحث الثاني: الحرب السيبرانية (الولايات المتحدة الأمريكية وإيران)

تعد الحرب السيبرانية بين الولايات المتحدة الأمريكية وإيران احدي 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 الأول: استراتيجية الهجمات السيبرانية للولايات المتحدة الأمريكية حيال إيران.

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

المطلب الأول: استراتيجية الهجمات السيبرانية للولايات المتحدة الأمريكية حيال إيران.

تعد الولايات المتحدة الأمريكية من القوى العظمى والمستوى الأول في المجال السيبراني إذ أنها 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

(32) غيث علاو، الهجمات السيبرانية أكبر من حروب نووية بوسائل الكترونية، موقع جادة إيران، بتاريخ 5/يوليو/2020، الشبكة الدولية للمعلومات:

<https://www.jadehiran.com/archives/16835>

(33) mattias schulze, joseph ker-scher, 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 التخريب النووية الإيرانية.⁽³⁵⁾

وفي عام 2010 اعترف المسؤولون الإيرانيون بأن أجهزة الكمبيوتر في محطة بوشهر النووية قد أصيبت بفيروس له تأثير بالغ أدى إلى توقف تخريب اليورانيوم في محطة (نطنز) النووية بالكامل جراء الفيروس الموجه لها المعروف باسم (ستوكسنت) التي اتهمت إيران الولايات المتحدة الأمريكية بالوقوف وراءه.⁽³⁶⁾

وقد أكد نائب مدير الوكالة الدولية للطاقة الذرية السابق (أولي هينونن) أن الفيروس الإلكتروني المعروف باسم (ستوكسنت) قد ولد مشاكل تقنية أثرت على البرنامج النووي الإيراني مما أدى إلى إيقاف الآلاف من أجهزة الطرد المركزي الخاصة بتخريب اليورانيوم، وأظهر بحث أجرته شركات الأمن المعلوماتي أن (60%) من الأجهزة المصابة بفيروس (ستوكسنت) توجد في إيران، وعليه جاء تقرير للوكالة الدولية للطاقة الذرية نشر في أيلول عام 2010 أن إيران فصلت (160) جهاز طرد مركزي عن شبكة التحكم.⁽³⁷⁾

ورغم قدرته الفريدة على الانتشار ومعدل الإصابة على نطاق واسع إلا أن برنامج (ستوكسنت) يلحق ضرراً ضئيلاً أو معدوماً لأجهزة الحاسوب غير المستخدمة في تخريب اليورانيوم، أما في حالة إيران فإن الفيروس (ستوكسنت) غير برمجة أجهزة التحكم المنطقي القابلة للبرمجة، مما أسفر عن دوران أجهزة الطرد المركزي بسرعة كبيرة جداً لمدة طويلة مما أدى إلى 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 مؤدياً إلى اهتزازها مسببة ارتفاع درجة الحرارة المؤدية في النهاية إلى تعطل المعدات الحساسة كما أسلفنا.⁽³⁸⁾

أما خلال فترة إدارة الرئيس الأمريكي السابق (دونالد ترامب) فقد طرح استراتيجية سميت بـ (الاستراتيجية القومية السيبرانية) في عام 2018 التي عدت الفضاء السيبراني أمراً أساسياً وأنه جزء لا يتجزأ من جوانب الحياة الأمريكية ومع إصدار هذه الاستراتيجية يكون لدى الولايات المتحدة الأمريكية 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 الأمريكي 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 ومعاينة 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 إيران 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 مفصلة بالكامل خلال السنوات الـ (15) عشر الماضية إذ دخلت حيز التنفيذ وهذه الاستراتيجية جاءت في أعقاب قرار (ترامب) لإلغاء قواعد حددها سلفه (أوباما) قد قيدت العمليات السيبرانية وأكد (جون بولتون): «أن أي دولة تقوم بعمل أو نشاط سيبراني ضد الولايات المتحدة الأمريكية 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⁾

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

(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>

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

(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>

(44) David p. fidler , america's place in cyber pace: the Biden administration cyber strategy. Takes shape, council foreign relations, foreign affairs, march, 11, 2021, international information network: <https://www.cfr.org/blog/americas-place.cyberspace>

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

وأكد الرئيس الحالي (جو بايدن) قبل تنصيبه رئيساً للولايات المتحدة الأمريكية في 20/يناير/2021، إذ أكد في ديسمبر/ 2020 أن الأمن السيبراني هو أولوية قصوى لإدارته القادمة وضمن خطته على إثر تعرض الولايات المتحدة الأمريكية لهجوم سيبراني واسع ووفقاً لصحيفة (وول ستريت جورنال) الأمريكية أن الحواسيب المخترقة تواجدت بأكثر من (20) مؤسسة أمريكية وانتقد (جو بايدن) (دونالد ترامب) باعتباره رئيساً للولايات المتحدة الأمريكية لغاية قبل التنصيب أنه مقصراً في تعزيز الأمن السيبراني وأنه كان غير يقظ في ذلك وأنه سيأخذ الأمر بجديته خلال ادارته القادمة تعزيزاً وحمايةً للأمن القومي الأمريكي من خلال الرد على الهجمات السيبرانية ضد منطلقها.⁽⁴³⁾

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

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 الأمريكية السيبرانية باعتبارها عضواً في حلف شمال الأطلسي.⁽⁴⁵⁾

وفي يوليو/2021 أكد الرئيس الأمريكي (جو بايدن) أنه من المنطقي أن تشن الولايات المتحدة الأمريكية 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 الأمريكية ستتخذ الخطوات الضرورية لحماية بنيتها التحتية وأمنها القومي من الهجمات السيبرانية.⁽⁴⁶⁾ فضلاً عما تقدم من طرح للتوجهات الاستراتيجية للولايات المتحدة الأمريكية السيبرانية خلال الادارة الحالية والادارات السابقة حيال الدول التي تشكل منطلق للهجمات السيبرانية ضدها وبصورة خاصة ايران، سنطرح الهجمات السيبرانية للولايات المتحدة الأمريكية 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/ يوليو/2021، الشبكة الدولية للمعلومات: <https://www.arabic.rt.com/world/1250247>

جدول رقم (1) يوضح الهجمات السيبرانية للولايات المتحدة الأمريكية 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 الأمريكية 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	أقرت 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 ان الولايات المتحدة الامريكية و(إسرائيل) قد نشرتتا 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 ان هذه الهجمات مسحت البيانات المستخدمة للتخطيط لهجمات الناقلات.
11	26/يونيو/2019	ابلغت (net black) عن تعطل واسع النطاق للأترنت 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.

منعت الولايات المتحدة الأمريكية الوصول الى (farsnews.com) وهو عنوان الويب باللغة الانجليزية لوكالة انباء فارس التابعة للحرس الثوري.	25/يناير/2020	13
ذكرت ايران أنَّ الاتصال الوطني بالانترنت فيها انخفض الى (75%) بعد أنَّ قامت ايران بتفعيل (net black) الاجراءات السيبرانية المضادة لهجوم (DDOS).	8/فبراير/2020	14
ألقي رئيس منظمة الدفاع المدني الايرانية باللوم على الولايات المتحدة الأمريكية في هجوم سيبراني (DDOS) ادى الى انقطاع الخدمة لساعات.	14/فبراير/2020	15
صادرت الولايات المتحدة الأمريكية (92) اسم مجال تستخدمها ايران ضدها وعلى أنَّها منافذ اخبارية حقيقية لكنها وفق ما رأته الولايات المتحدة الأمريكية أنَّها تستهدفها لنشر الدعاية الايرانية.	7/اكتوبر/2020	16
أكدت ايران أنَّ هجوماً سيبرانياً استهدفتها 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.	15/اكتوبر/2020	17
استهدفت القيادة السيبرانية الأمريكية ووكالة الامن القومي الأمريكي قراصنة ايرانيين قبل الانتخابات الرئاسية الأمريكية.	3/نوفمبر/2020	18
اغلقت الولايات المتحدة الأمريكية (29) موقعاً على شبكة الانترنت تستخدمها ايران بهدف التأثير على سياسة الولايات المتحدة الأمريكية والرأي العام.	4/نوفمبر/2020	19
ازال موقع (تويتر) (238) حساباً يعمل من ايران بعد استكمال التحقيق عن التدخل الايراني في الانتخابات الرئاسية الأمريكية عام 2020.	23/فبراير/2021	20
صادرت الولايات المتحدة الأمريكية 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 وتأثير داخل الولايات المتحدة الأمريكية.	22/يونيو/2021	21

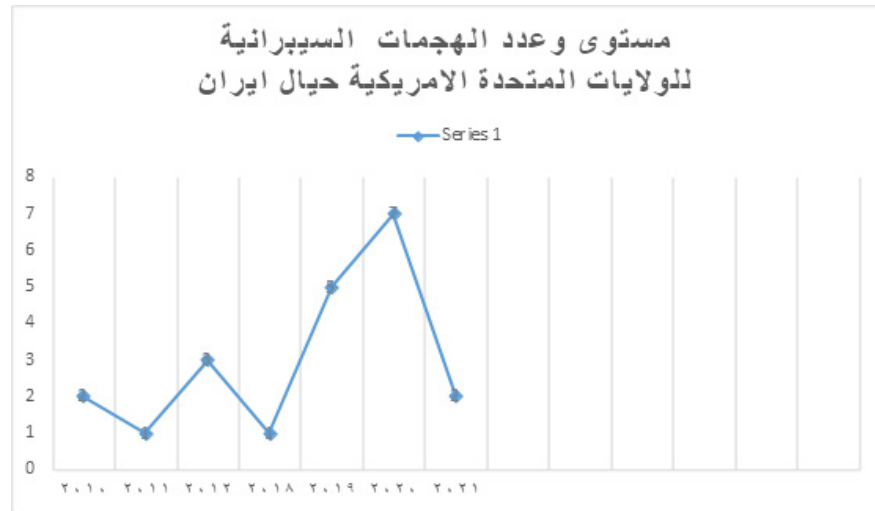
الجدول من إعداد الباحث بالاعتماد على المصادر الآتية:

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، وكالاتي:

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 الإيرانية حيال الولايات المتحدة الأمريكية

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

اعتمدت إيران استراتيجية سيبرانية تم الاعداد لها والتجهيز منذ سنوات عدة

وخاصة الولايات المتحدة الأمريكية.⁽⁴⁷⁾ وأخذت عقيدة الأمن السيبراني تفرض نفسها في اطار استراتيجية الأمن القومي الإيراني بشكل عام وأن هذه العقيدة تستند على ركيزتين مهمتين: الركيزة الأولى: تتمثل بحماية الأمن الوطني الإيراني من خلال بناء بنية تحتية علمية تكنولوجية واستخباراتية تستند على استراتيجية وقائية في الدفاع واستراتيجية استباقية في الهجوم في المجال السيبراني. أما الركيزة الثانية: فتتمثل 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 الاستخباراتية في نشر المعلومات المضللة واجهاض المسيرات

(47) احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران 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 إيران بين الدول الخمسة التي تتمتع بأقوى قدرات انترنت في العالم.⁽⁴⁸⁾ وتتكون القدرات السيبرانية الإيرانية من قدرات بشرية ومادية ذات كفاءة عالية المستوى في المجال السيبراني ترتبط بأعلى المستويات في الدولة، وهي:⁽⁴⁹⁾

(48) 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>

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

1- المجلس الأعلى للساير. 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 الساير. وظيفتها دفاعية تهدف لحماية المنشآت الوطنية ضد أي هجوم سيبراني وتتبع الدفاع المدني الذي يعد فرعاً من أفرع القوات المسلحة الإيرانية.

3- الجيش السيبراني الإيراني. 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 الأمريكية وأيضاً جمع المعلومات.

4- دعم الفاعلين المعلوماتيين.

يعمل الكثير من الفاعلين السيبرانيين تحت مظلة النظام الإيراني في الفضاء الرقمي الإيراني، وعمدت إيران الى تشكيل شبكة كيانات رقمية من أجل صد الهجمات

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

السيبرانية من القوات الدولية المنافسة وشن الهجمات السيبرانية أيضاً خاصة ضد الولايات المتحدة الأمريكية.

وبدأت الهجمات السيبرانية الإيرانية ضد الولايات المتحدة الأمريكية في عام 2009 عندما قام (الجيش السيبراني الإيراني) بتشويه صفحة (تويتر) الرئيسية رداً على احتجاجات ما يسمى

بـ (الثورة الخضراء) التي اندلعت في إيران احتجاجاً على إعادة انتخاب الرئيس الإيراني الأسبق (محمود احمدى نجاد).⁽⁵⁰⁾

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

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

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

(51)

وقد زادت إيران 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 والتكنولوجية وخطوط الغاز والبتروك في الولايات المتحدة الأمريكية واختراق البريد الإلكتروني والاتصالات أيضاً.⁽⁵²⁾ وبعد تسلم الرئيس الإيراني الجديد (ابراهيم رئيسي) السلطة في 3/أغسطس/2021 ورغم تعرض إيران للهجمات السيبرانية قبل تسلمه السلطة استطاعت إيران أن 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 إيران أن تقوض تلك الاحداث خدمة لمصالحها العليا وسترده على اي هجمات ضدها سواء كانت سيبرانية او تقليدية برد سيبراني او تقليدي ضمن ما تراه مناسباً.⁽⁵³⁾ وفضلاً عما تقدم، سنطرح الهجمات السيبرانية الإيرانية حيال الولايات المتحدة الأمريكية استكمالاً لما تقدم من طرح التوجهات الاستراتيجية الإيرانية السيبرانية، وكما هي:

جدول رقم (2) يوضح الهجمات السيبرانية الإيرانية حيال الولايات المتحدة الأمريكية

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

(52) مهدي مبارك عبد الله، الجيش السيبراني الايران القوة السرية المدمرة، موقع جرس، بتاريخ 22 ابريل/2019، الشبكة الدولية للمعلومات:

<https://www.garasanews.com/article/325741>

(53) محمد محمد السادة، الضرورة والمحظورات في «حرب الظل» بين إيران والعدو (الإسرائيلي)، موقع الميادين نت، بتاريخ 11/أغسطس/2021، الشبكة الدولية للمعلومات:

<https://www.almayadeen.net/articles/%D8%A7%D9>

6	27/سبتمبر/2013	اخترق فاعلين سيبرانيين إيرانيين أجهزة كمبيوتر غير سرية للبحرية الأمريكية في خضم المحادثات حول البرنامج النووي الإيراني.
7	فبراير/2014	استهدف فاعلين سيبرانيين إيرانيين شركة (لاس فيجاس ساندز) التابعة لشركة (شيلدون ادلسون) إذ أدى الهجوم إلى إغلاق أنظمة الاتصالات ومسح محركات الأقراص الثابتة.
8	نوفمبر / 2015	قامت إيران باستهداف وزارة الخارجية الأمريكية ومسؤولين آخرين في (إدارة باراك أوباما).
9	24/مارس/2016	وجهت وزارة العدل الأمريكية لائحة اتهام ضد إيران بشأن هجمات سيبرانية ضد بنوك أمريكية وسد في نيويورك.
10	22/مارس/2018	أدى هجوم سيبراني ببرنامج (الفدية) يعرف باسم (sam sam) إلى شل حكومة مدينة (اتلانتا) الأمريكية
11	9/مايو/2018	حذرت شركة الأمن السيبراني الأمريكي من زيادة ملحوظة في النشاط السيبراني الإيراني في غضون (24) ساعة من انسحاب (إدارة ترامب) من خطة العمل الشاملة المشتركة.
12	12/يوليو/2018	حذر كبار المسؤولين الأمريكيين من أن إيران استعدت لهجمات سيبرانية واسعة النطاق ضد الولايات المتحدة الأمريكية.
13	5/ديسمبر/2018	وجهت وزارة العدل الأمريكية لائحة اتهام إلى فاعلين إيرانيين سيبرانيين بشأن هجوم (sam sam ransom ware) على مدينة اتلانتا الأمريكية.
14	يناير / 2019	قامت شركة (fire eye) للأمن السيبراني بتفصيل حملة استمرت عامين من قبل إيران لسرقة بيانات اعتماد تسجيل الدخول وتفاصيل العمل في الولايات المتحدة الأمريكية.
15	6/مارس/2019	قالت شركة مايكروسوفت أن الهجمات السيبرانية الإيرانية استهدفت أكثر من (200) شركة في عامي 2017 و 2018
16	22/يونيو/2019	قالت وزارة الأمن الداخلي الإيرانية أن إيران زادت من نشاطها السيبراني ضد الوكالات الحكومية الأمريكية والصناعات الخاصة.
17	4/أكتوبر/2019	قالت شركة (مايكروسوفت) أن إيران حاولت اختراق الحسابات المتعلقة بحملة إعادة انتخاب الرئيس الأمريكي (دونالد ترامب) والمسؤولين الأمريكيين.
18	22/أكتوبر/2019	كشفت المحكمة الموثقة أن مكتب التحقيقات الفدرالي الأمريكي تعقب فاعلين إيرانيين سيبرانيين انتهكوا شركات تكنولوجيا الأقمار الصناعية الأمريكية.

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

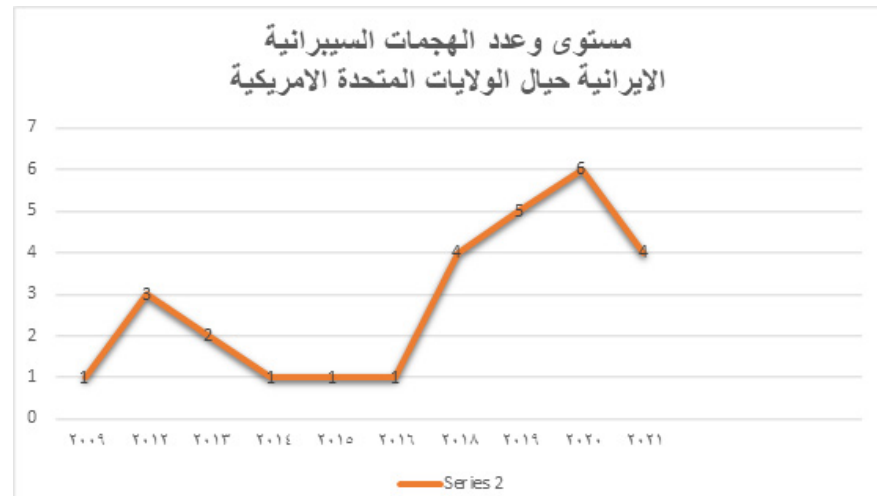
28	2021/ يوليو/26	تم تسريب وثائق في الولايات المتحدة الأمريكية حول كيفية قيام إيران باختراق البنية التحتية الحيوية للولايات المتحدة الأمريكية بما في ذلك تنقية المياه وأنظمة امداد الوقود والاتصالات البحرية وكيفية اكتشاف أنظمة ادارة المباني الذكية في الولايات المتحدة الأمريكية.
----	----------------	--

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 الأمريكية ضمن استراتيجيتها السيبرانية، سنطرح مخططاً بيانياً يوضح فيه ذلك، وكالاتي: مخطط رقم (2) يوضح مستوى وعدد الهجمات السيبرانية الايرانية بيانياً حيال الولايات المتحدة الأمريكية



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 أن الحرب السيبرانية هي احدى أدوات الجيل الخامس من الحروب التي ميدان صراعها وعملها هو الفضاء السيبراني إذ تستخدم عبر هذا الفضاء الأسلحة السيبرانية من برمجيات وفايروسات ذات قدرة تدميرية ضد الجهة المستهدفة لذا سعت الدول ذات القدرات السيبرانية الى تفعيل ذلك وخاصة الولايات المتحدة الأمريكية وإيران (محط الدراسة) الدولتان ذات التاريخ الحافل بالصراعات، اذ استخدمت الولايات المتحدة الأمريكية أولى هجماتها ضد ايران كان في عام 2006 عبر حملة الألعاب الأولمبية واستمرت بتلك الهجمات عبر استراتيجية سيبرانية خاصة لها عبر الإدارات الأمريكية المتعاقبة وحتى وقتنا الحاضر ساعية من ذلك لتدمير وإنهاك وإبطاء 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 الأمريكية 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 الأمريكية لإثبات أن إيران 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 إلا 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 زروقة، 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 كلتري، 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%84%9d>
- 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/%D8%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 الإيراني 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 إيران والعدو (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 Warfare: 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, Overview of Cyber Security, International Journal of Advanced Research in Computer and Communication Engineering, article in IJARCC, 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, number 3, 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” Bebb, Cyber Power and Cyber Effectiveness: An Analytic Framework, Comparative Strategy, 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 College London, May, 2018 .

10- Matthias 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>