استراتيجيات الحروب السيبرانية بعد العام ٢٠١٠: الحرب الإيرانية – (الإسرائيلية) أنموذجا

Cyber Wares Strategies after 2010: The Iranian-Israeli War As model

أ.م.د. دنيــا جواد مطلك

جامعة بغداد – كلية العلوم السياسية

donia.col@copolicy.uobaghdad.edu.iq.

https://orcid.org/0000-0003-3423-5206

تاريخ استلام البحث: ٢٠٢٥/١/٧ تاريخ قبول النشر: ٢٠٢٥/٤/١٠

الملخص:

على الرغم من تنامي المخاوف الدولية من الهجمات السيبرانية التي تهدد الامن القومي للدول وسيادتها واستقرارها وقدراتها الاقتصادية والعسكرية، الا انه حتى اللحظة لم يتحقق الإجماع الدولي لوضع قانون دولي يحظر الهجمات والحروب السيبرانية التي تهدد البنية التحتية للدول والاصول الوطنية مما يرتب تهديدها للسلم والامن الدوليين، على الرغم من امتلاك الكثير من الدول لا سيما المتقدمة منها استراتيجيات امن سيبراني متطورة، الا انها لم تستطع صياغة استراتيجيات ردع افتراضي متكاملة وفاعلة في ضوء التقدم المتسارع لتقنيات الهجمات السيبرانية بشكل مضطرد، اذ اتجه الفكر الاستراتيجي العسكري الى دمج القدرات السيبرانية مع الأدوات والاقتصادية والدبلوماسية والعسكرية لتحقيق ما يعرف بالردع السيبراني، لمنع الهجمات السيبرانية ضد الاهداف الوطنية للدولة مثل البنى التحتية وشبكات المعلومات والملفات المعنية بالأمن القومي، في ضوء ثورة المعلومات والاتصالات التي غيرت الكثير من استراتيجيات الحروب السيبرانية وأضافت ابعاد هجومية ودفاعية في الفضاء الافتراضي بل وغيرت من طبيعة العلاقات الدولية في العموم.

وبقدر تعلق الامر بموضوع البحث فان أهم تحدي يواجه منطقة شرق المتوسط يتمثل بتزايد التوتر في العلاقات الإيرانية – (الإسرائيلية) بعد العام ١٩٧٩، اذ تحولت إيران من حليف للكيان الصهيوني قبل هذا التاريخ الى تهديد وجودي للدولة العبرية، حيث وظفت كل أدوات القوة الصلبة والناعمة لإحاطة(إسرائيل) بطوق ناري من البحر الى البحر عبر إقامة منظومة من التحالفات مع الفواعل من دون الدول، فضلا عن بناء قوة سيبرانية متميزة للارتقاء بإدائها الاستراتيجي لضمان امنها القومي، في الوقت الذي حرصت فيه(إسرائيل) على الارتقاء بقدراتها السيبرانية انطلاقا من ادراكها بإن من يملك القدرات السيبرانية الفاعلة سيكون اكثر تأثيرا على المستخدمين للقوة السيبرانية في الفضاء الرقمي الذي اصبح مسرحا للتفاعلات الدولية في القرن الحادي والعشرين ذات الطابع الصراعي والتعاوني. وعليه يهدف البحث الى شرح وتحليل استراتيجيات الحرب السيبرانية الإيرانية مع الكيان (الإسرائيلي)، في ضوء اتجاه كلا من إيران و(إسرائيل) الى اعتماد الهجمات السيبرانية بدلا من الصدام المباشر الذي يبدوا مكلفا لكليهما لكنها لن تمنعه مستقبلا.

الكلمات المفتاحية: الحروب السيبرانية، الفضاء الافتراضي، الردع السيبراني، القوة السيبرانية.

Abstract:

Despite growing international fears of cyber-attacks to national security as threats to countries' sovereignty, stability and economic and military capabilities, but so far it has not International consensus is achieved to develop international law prohibiting cyber-attacks and wars that threaten infrastructure States and national assets. These developments threaten international peace and security, especially as States have not been able to date develop integrated and effective cyber deterrent strategies. In addition, military strategic thinking has turned to integrate cyber capabilities with economic, diplomatic, and military tools to achieve the so-called response cyber.

This response ensures that the opponent realizes that any cyber threat will be met with a retaliation that involves employing all means available to the state. These practices include counter-cyber retaliation, international legal procedures allowing for the imposition of punitive sanctions and diplomatic measures, directly using and employing military capabilities, or threatening to use such capabilities to prevent cyber-attacks against the state's national targets such as infrastructure, flag networks, and national security files. These variables have led countries to upgrade their cyber deterrence capabilities. In light of the information and communication revolution, which has changed many war strategies. These challenges added some offensive and defensive dimensions to the virtual space and even changed the nature of international relations in general. As far as the topic of research is concerned, the most important challenge facing the Eastern Mediterranean region is the increasing tension in Iran-Israel relations after 1979.

Iran transformed from an ally of Israel before this date into an existential threat to Israel,. Hence, Iran employed all hard and soft power tools to encircle Israel with a firewall from sea to sea. This encirclement included a system of alliances with actions without countries and building a distinct cyber force to upgrade its strategic performance to ensure its national security. At the same time, Israel focused on the sophistication of its cyber capabilities from the fact that those who possess effective cyber capabilities will be more influential for users of cyber power in the digital space. Outer space has become the scene of interactions the twenty-first century is of a conflict and cooperative nature. Therefore, this research aims to explain and analyze this war based on cyber strategies in light of both Iran and Israel's trend towards cyber-attacks rather than direct clashes that appear costly to both but will not be possible in the future.

Keywords: Cyber Wars, Virtual Space, Cyber Deterrence, Cyber Power.

المقدمة

مع تعدد طبيعة واشكال التهديدات السيبرانية لسيادة الدول وامنها واستقرارها لتشمل الحرب الرقمية (Digital Warfare) والإرهاب الرقمي(Digital Terrorism) فضلا عن التجسس الرقمي (Digital Espionage) وغيرها من التحديات السيبرانية في ظل الانكشاف الاستراتيجي، تتزايد اثار وتحديات الحروب السيبرانية التي تهدد البنى التحتية والامن القومي للدول في ضوء التطور المتسارع لثورة المعلومات والاتصالات التي ازالت الحدود وقربت المسافات بين الافراد والجماعات والدول، وللحيلولة دون تكرار تلك الهجمات من خلال تهديد المهاجم بالانتقام، ولحماية الأمن القومي للدول الذي البنى بات رهنًا بالفضاء السيبراني سارعت الدول الى الارتقاء بقدراتها السيبرانية لتتمكن من القيام بهجمات افتراضية بوصفها شكل من اشكال الردع لمنع الهجمات الرقمية التي تنال من امنها ورفاهيتها وبناها التحتية مثل شبكات نقل الطاقة الكهربائية والاستثمارات والبنوك وغيرها من الملفات التي تهم الامن القومي، بعد ان اصبح الفضاء مجالا رابعا لحروب المستقبل، واصبح تصنيف تراتيبة القوى الدولية في النظام الدولي يرتكز على ما تملكه من قدرات فضائية، تمكنها من صياغة استراتيجيات ردع سيبرانية فاعلة تضمن لها امنها وتحقق مصالحها في ضوء تعدد الاستخدامات المدنية والعسكرية للفضاء الافتراضي.

ولعل (إسرائيل) من أوائل الدول التي أدركت أهمية الارتقاء بقدراتها العسكرية للحفاظ على الاختلال في توازن القوى العسكرية في المنطقة لصالحها بوصفه شكلا من اشكال الردع، عبر امتلاك القدرة على توجيه ضربة استباقية – وقائية لاي هجوم محتمل متى ما استشعرت التهديد، اذ حرصت على امتلاك السلاح النووي لتعويض افتقارها الى ميزة العمق الاستراتيجي الذي يمكنه ان يمتص زخم الضربات الصاروخية المحتملة أولا، ويعوضها عن افتقارها للعدد الكافي من المقاتلين مقارنه بما تملكه الدول المحيطة بها ثانيا. اذ حرصت ومنذ قيامها على امتلاك ممكنات الفعل الاستراتيجي عسكريا واقتصاديا وتقنيا اعتمادا على الدعم الكبير الذي تلقته من الدول التي أسهمت في انشائها، الامر الذي سهل لها انشاء قاعدة اقتصادية وتكنلوجية وعسكرية واسعة ومتينة مكنتها من الولوج الى عصر الفضاء ومنذ وقت مبكر مقارنه بدول المنطقة، لاسيما وإنها أدركت خطورة التحديات الإقليمية التي تهدد امنها القومي. وقد تفاقم هذا الهاجس الامني مع تبلور ثورة المعلومات والاتصالات التي ربطت الابعاد الاقتصادية والجغرافية والسياسية، في الوقت الذي حرصت هي فيه على إقامة الاطواق الضامنة لأمنها القومي بوصفها مرتكزا من مرتكزات استراتيجية الردع للكيان (الإسرائيلي)، لا سيما بعد تداعيات ما عرف بالربيع العربي الذي احاطها بالتحديات اللامتماثلة التي ابتدأت بالتحديات الإرهابية والدول الفاشلة، فضلا عن القوى المناوئة لها واهمها إيران وحلفائها من دون الدول، لا سيما وانها استطاعت توظيف واستخدام التكنلوجيا العسكرية منخفضة الكلفة بالرغم من العقوبات الاقتصادية المفروضة عليها منذ عام ١٩٧٩، مما رتب تزايد الفجوة السيبرانية في قدراتهما السيبرانية اثرت بشكل كبير في استراتيجيات الردع السيبراني. ومع تزايد التصعيد ومساعي إيران الى اقامة اطواق من النار للإحاطة ب(إسرائيل) من كل الجهات لتهديد امنها القومي وتهديد مصالحها لتحقيق غايتين تتمثل الاولي بالوصول الى

حوض شرق المتوسط وتفعيل فرص تصدير النفط الإيراني الى اوربا عبر الاراضي السورية والعراقية وتجاوز العقوبات الامريكية المفروضة عليها منذ العام ١٩٧٩. في ما تتمثل الثانية بالضغط على حلفاء الولايات المتحدة في المنطقة لإتاحة الفرصة لإكمال برنامجها النووي، وهو ما تعده (إسرائيل) تهديدا وجوديا لأمنها، مما يرتب زيادة التصعيد السيبراني بين إيران وحلفائها من جهة و(إسرائيل)وحلفائها من جهة ثانية.

أولا:- أهمية البحث:-تكمن أهمية البحث في أهمية الفضاء الافتراضي الذي اصبح ميدانا للتفاعلات الدولية بكل مظاهرها واشكالها، الامر الذي جعل الحروب السيبرانية احد اهم التحديات للامن القومي للدول، مما دفع الدول الى تخصيص مبالغ هائلة لارتقاء بقدراتها الرقمية لضمان امنها القومي واستثمار الفضاء السيبراني في تعاملاتها التعاونية والتجارية، إذ تخصص الكثير من الدول أقساما ومرافق خاصة بالحرب السيبرانية ضمن اجهزه الأمن الوطني الخاصة بها، لتضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، القرصنة الالكترونية والاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية، بعد ان اصبح الفضاء الافتراضي ميدان للاستخدامات العسكرية والمدنية. كما يهتم البحث بتحديد طبيعة وحجم الفجوة في القدرات السيبرانية بين إيران و(إسرائيل) وأثرها في استراتيجيات الحرب السيبرانية المستعرة بينهما منذ عام ٢٠١٠، عندما استهدف البرنامج النووي الإيراني فايروس افتراضي سبب عطل ملفات الطرد المركزي للمفاعلات النووية الإيرانية وتعطيل المشروع لسنوات تالية، وبيان أثر التصعيد السيبراني بين إيران وحلفائها من جهة و(إسرائيل) وحلفائها من جهة ثانية على الاستقرار الإقليمي والتوازن الاستراتيجي في منطقة جنوب غرب آسيا.

ثانيا: أهداف البحث: وهي تتمثل بما يأتي:-

١. التعرف على سمات الحروب السيبرانية وخصائصها وتحدي استراتيجيات مواجهة الهجمات الافتراضية.
٢. تحليل العلاقة بين الاستراتيجية العسكرية والقوة السيبرانية.
٣. المساعدة في تطوير استراتيجيات الردع السيبراني.
٤. معرفة القدرات الهجومية السيبرانية لكل من إيران والكيان (الإسرائيلي).

ثالثا:- مشكلة البحث:- وهي تتمثل بالتساؤل الآتي:- ما هي استراتيجيات الحرب السيبرانية بين إيران و(إسرائيل) بعد استهداف البرنامج النووي الإيراني بفايروس ادى الى تعطيله لسنوات، وكيف تؤثر فجوة القدرات السيبرانية بين إيران و(إسرائيل) على استراتيجيات الحرب السيبرانية بينهما؟؟ ويتفرع من هذا التساؤل التساؤلات الفرعية الآتية:-

١. ما المقصود بالفضاء الافتراضي؟
٢. ما هي المفاهيم المقاربة للحروب السيبرانية؟؟ مثل الامن السيبراني، الردع السيبراني، الهجمات الافتراضية؟
٣. ما هي القدرات الافتراضية الإيرانية و(الاسرائيلية)؟
٤. كيف وظفت كلا من إيران و(إسرائيل) قدراتهما السيبرانية في عملياتهما العسكرية ضد بعضهما البعض.
٥. هل يمكن ان تؤدي الهجمات السيبرانية المتبادلة الى حرب تقليدية بينهما؟؟وكيف؟؟.

رابعا:- فرضية البحث:-يرتكز البحث على افتراض مؤداه (كلما ادرك كلا من إيران والكيان (الإسرائيلي) اثار الدمار الذي ينتج عن اي صدام عسكري مباشر بينهما كلما اتجها الى صياغة استراتيجيات لحروب سيبرانية اكثر فتكا وتدميرا للبنى التحتية لكلاهما، مما يحمل معه احتمالات حدوث صدام عسكري تقليدي مباشر بينهما عبر توجيه ضربات صاروخية محدودة متبادلة او القيام بعمليات عسكرية خاصة في العمق الاستراتيجي لكل منهما وبشكل محدود).

خامسا:- الفجوة البحثية:- تتحدد الفجوة البحثية بتناول اهداف ووسائل استراتيجيات الحروب السيبرانية بين إيران و(اسرائيل)، ودورها في تزايد احتمالات اندلاع حرب تقليدية مباشرة، لا سيما وان استراتيجيات الردع السيبراني غير فاعلة ما لم تقترن باستراتيجيات عسكرية فاعلة، في ضوء التصعيد العسكري بين (اسرائيل) وحلفائها من جهة وإيران وحلفاءها من دون الدول الاوربية والولايات المتحدة الامريكية فضلا عن حلفائها في منطقة جنوب غربي آسيا من ناحية ثانية، لا سيما مع تداعيات احداث غزة ٢٠٢٣، وتبلور العديد من الاستقطابات والمحاور الاقليمية والدولية حولها، فضلا عن تنامي القدرات الافتراضية لكل من إيران و(اسرائيل) بشكل متسارع وتنامي التطورات في الفضاء السيبراني عموما.

سادسا:- مناهج البحث وهيكليته:- اعتمد البحث للوصول الى النتائج النهائية على المنهج التحليلي والاستشرافي.

سابعا:- هكيلية البحث:- قسم البحث الى مقدمة ومطلبين وخاتمة واستنتاجات كالأتي:-

المبحث الأول:- الحرب السيبرانية:اطار مفاهيمي. وهو يضم المحورين الاتيين: -

المطلب الاول:- مفهوم السايبر والمصطلحات ذات العلاقة.

المطلب الثاني: - الحرب السيبرانية: المفهوم والمخاطر.

المبحث الثاني:- استراتيجيات الحرب السيبرانية الإيرانية -(الإسرائيلية): وهو يضم المحورين الآتيين:-

المطلب الاول:- القدرات السيبرانية الإيرانية و(الإسرائيلية).

المطلب الثاني: - اهداف ووسائل استراتيجيات الحرب السيبرانية الإيرانية(الإسرائيلية)، وآفاقها المستقبلية.

الخاتمة والاستنتاجات.

المبحث الأول: الحرب السيبرانية/ إطار مفاهيمي

مما لا شك فيه ان القوة تمثل أحد اهم أدوات ضمان تحقيق المصالح القومية للدول[1]، ولها أنماط متعددة تبتدأ بالقوة الصلبة التي ترتكز على عناصر القوة الاقتصادية والعسكرية، والقوة الناعمة التي حدد مفهومها وأبعادها (جوزيف ناي) لتشمل منظومة القيم السياسية والثقافية والاداة الدبلوماسية الفاعلة والخطاب الإعلامي الذي يتمتع بالمصداقية والشرعية. ثم ظهر مصطلح القوة الذكية مع العقد الاول من القرن الحالي ليشير الى استراتيجيات توظيف مقومات القوة الصلبة والناعمة معا لضمان الاكراه والردع لتحقيق المصالح القومية، واخيرا ظهرت القوة الافتراضية او السيبرانية بعد ان ظهر الفضاء الافتراضي بوصفه مجالا آخر للتفاعلات الدولية، وأعاد ترتيب القوى الدولية وفق هيكلية جديدة، لتعرف بوصفها (القدرة على استخدام الفضاء

السيبراني لضمان المصالح القومية والتأثير في مصالح ومناطق النفوذ، عبر توظيف أدوات القوة التكنلوجية)[٢]. او استهداف البنى التحتية للدولة والملفات الوطنية المعنية بالأمن القومي للدول واصابتها بالعطب والضرر، عبر استهداف أنظمة المعلومات والملفات التي تضمها بشكل يؤدي الى اتلافها وتدميرها[٣]، اذ لم تعد القوة ترتكز على التحكم في الموارد فقط بل تعتمد على التحكم بفعلية النتائج والاثار المترتبة على توظيفها لضمان تحقيق المصالح العليا[٤].وفي تموز من عام ٢٠٠٩ شهد العالم أول حالة (معروفة) للهجوم السيبراني بالتزامن مع النزاع المسلح الفعلي خلال الحرب الروسية الجورجية[٥]، وعليه سيتناول هذا المطلب مفهوم السايبر والمصطلحات ذات العلاقة السيبرانية (الفضاء الافتراضي، القوة السيبرانية، الامن السيبراني، الردع السيبراني، الهجمة السيبرانية، في أولا، واستراتيجيات الحروب السيبرانية ثانيا.

المطلب الأول/ مفهوم السايبر والمصطلحات ذات العلاقة

مع نهايات مرحلة الحرب الباردة وتزايد اعتماد الدول في ضمان امنها القومي على تقنيات حديثة مستثمرة التقدم المتسارع في ثورة المعلومات والاتصالات تبلورت معضلة امنية جديدة كانت من نتاجات الانكشاف الأمني الذي شهده العالم بفعل ظهور مجموعة من الفواعل الدولية من دون الدول، فضلا عن التحول في أنماط القوة وظهور ما عرف بالقوة الافتراضية او السيبرانية التي مثلت إيذانا ببدء عصر جديد للتنافس في الفضاء الافتراضي. اذ اشتقت مفردة السايبر (Cyber) ابتداءا من مفردة (cyber) اليونانية، او مصطلح (Keybernetes)، وتعني التحكم عن بعد[٦]، وفي العموم تطلق مفردة سيبراني على كل ما له علاقة بتطبيقات الحاسوب وبرمجياته[٧].لذا سيتناول هذا المحور المفردات القريبة من مفهوم الحرب السيبرانية وكما يأتي:-

١. **الفضاء السيبراني:** حيث عرف (ويليام جيبسون) في كتابه "النيورومانسر" الصادر عام ١٩٨٤ الفضاء الالكتروني بوصفه (هلوسة يتم التعبير عنها عبر رسوم بيانية وبيانات مستخرجة من الحواسيب التي يمتلكها ملايين البشر)[٨]. بمعنى انها عبارة عن واقع تخيلي وافتراضي لمخرجات أنظمة الاتصال والمعلومات والشبكات العنكبوتية للتحكم بنتائجها وآثارها، وفي اللغة العربية تستخدم مفردة القوة الالكترونية للدلالة على القوة السيبرانية[٩]. اذ شهدت العقود الأخيرة من القرن الحادي والعشرين تبلور فضاء او مجال جديد للتفاعلات الدولية والإنسانية اضيف الى (الأرض، الجو، البحر، والفضاء الخارجي) تمثل بالفضاء الافتراضي، الذي اصبح احد مرتكزات تحديد هيكلية النظام الدولي او تراتبية توزيع القوة فيه، لما يوفره من مقومات بإمكان الدول استثمارها للأغراض المدنية والعسكرية، الامر الذي كان له انعكاسات مباشره على الادراك الاستراتيجي للدول لأمنها القومي في ظل تنامي التهديدات الناجمة عن ثورة المعلومات الرقمية، ما دفع الدول الى الدخول المتسارع لانشاء بنية تحتية رقمية، بعد ان ظهر الفضاء الافتراضي، ساحة جديدة للصراع الدولي[١٠]، بعد ان طرح تحديات جدية للسيادة الإقليمية للدولة أولا، وهدد احتكار الدولة للقوة ثانيا، في ضوء عدم وجود قيود قانونية تحد من الهجمات السيبرانية ثالثا[١١]، فضلا عن ان الفضاء السيبراني طرح فرصا اكبر للتعاون كما يرى اتباع النظرية الليبرالية بتوجهاتها الفكرية المختلفة.

وقد عرَّف قاموس المصطلحات العسكرية (DOD)، الفضاء الإلكتروني بوصفه مجال عالمي للمعلومات الرقمية، يضم شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات والبيانات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات وأجهزة التحكم المدمجة[١٢]. في ما عرفت استراتيجية الامن القومي الألماني الفضاء الافتراضي بوصفه المجال او الفضاء الذي يضم أنظمة وتقنيات الاتصال ونقل المعلومات والبيانات على نطاق عالمي، ومن جانب آخر عرَّفت استراتيجية الامن القومي الامريكية الفضاء السيبراني بوصفه احد اهم المجالات الضامنة لاستقرار وأمن الشعب الأمريكي، وهي ترتكز على بنية تحتية ومؤسسات حيوية معلوماتية [١٣]، كما عرفته الوكالة الفرنسية لأمن الاعلام بوصفه الربط البيني لتقنيات المعالجة الآلية للمعلومات الرقمية [١٤]. ومع تسارع الدول للتحول نحو الرقمنة او الأتمتة في بنيتها التحتية، لاستثمار الفرص التي يتيحها الفضاء السيبراني للأغراض العسكرية والمدنية وتزايد الترابط والاشتباك في المصالح الدولية في الفضاء الافتراضي أصبح هذا الفضاء المجال الرئيس للأمن القومي والنمو الاقتصادي والتنمية الاجتماعية للدول[١٥]، الامر الذي جعله ساحة للصراع والتعاون الدولي معا.

ويتكون الفضاء الافتراضي في العموم من عدة طبقات تتمثل الأولى بالطبقة المادية التي تشمل البنية التحتية الرقمية والبيانات والأنظمة التي تحكمها وهي تخضع للقيود القانونية والسياسية، فضلا عن الطبقة الافتراضية ويراد بها المعلومات والتطبيقات الالكترونية وهي لا تخضع لأي قيود من أي شكل[١٦]، فضلا عن مقوم او مرتكز التفاعل بين البشر والمعلومات في الفضاء الافتراضي، ليتضمن عدة عناصر تتمثل بكل من أجهزة الكومبيوتر، الحواسيب، شبكات الاتصال، التطبيقات والبرامج المعلومات والبيانات[١٧]. واخيرا يمكن القول ان الفضاء السيبراني هو بيئة تفاعلية حديثة تتضمن المجال المادي وغير المادي يضم مجموعة من الاجهزة الرقمية وانظمة الشبكات والبرمجيات والمستخدمين سواء اكانوا مستخدمين او مشغلين [١٨].

٢. **القوة السيبرانية:** قبل تعريف القوة السيبرانية لابد من التفريق بين مصطلحي الفضاء السيبراني والقوة السيبراني، اذ ان الفضاء السيبراني هو المجال الذي تتم فيه العمليات السيبرانية، في ما يراد بالقوة السيبرانية مجموع التأثيرات الاستراتيجية الناتجة عن العمليات السيبرانية داخل الفضاء السيبراني ومنه[١٩]. ويمكن تعريف القوة السيبرانية بوصفها القدرة على توظيف واستخدام الفضاء السيبراني لخلق المزايا والتأثير في الاخرين[٢٠]. في ما تعرف الاستراتيجية السيبرانية بوصفها تطوير وتوظيف قدرات العمل في الفضاء السيبراني، متكاملة ومنسقة مع العمليات الأخرى لتحقيق الأهداف والمصالح القومية اعتمادا على عناصر القوة الوطنية[٢١]، لتشمل كلا من المرتكز المادي الذي يضم البنية المعلوماتي التحتية للقوة السيبرانية، والمرتكز المعنوي المتمثل بالمعلومات والتطبيقات في الفضاء السيبراني، والمرتكز الاخر المتمثل بالتفاعل بين البشر والبرمجيات والمعلومات الموجودة في الفضاء السيبراني، بوصفها استخدام تكنلوجيا المعلومات والطيف الكهرومغناطيسي لتخزين البيانات وتعديلها وتبادلها عبر شبكات الاتصال العنكبوتية من قبل

الفواعل الدولية من الدول او دون الدول للتحكم بمخرجات الفضاء السيبراني سواء كان للأغراض المدنية او العسكرية دفاعا او هجوما[٢٢]، وقد عرف جوزيف ناي القوة السيبرانية بوصفها السيطرة على البنية التحتية الرقمية من أنظمة تشغيل وتطبيقات رقمية وحواسيب ومعلومات وشبكات الكترونية ومعلومات وبيانات وكفاءات بشرية توظيف هذه البنية الرقمية بما يحقق مصالح الدولة القومية[٢٣].

ووفقا لما سبق يمكن القول ان القوة السيبرانية تفيد القدرة على استحداث الفرص في الفضاء السيبراني او الافتراضي لضمان المصالح القومية للدول[٢٤]، وعليه فأن الجهات التي تستطيع توظيف القوة السيبرانية تتمثل بكل من الدولة أولا، حيث تعد فاعلا رئيسا في الفضاء الافتراضي، لما تملكه من مقومات مادية وغير مادية، ومنها احتكارها القانوني للقوة وعبر العديد من الأجهزة والمؤسسات التي تملكها، والفاعلون من غير الدول ثانيا من افراد وجماعات من غير الدول تملك مقومات القوة وان كان بمستويات تختلف عن ما تملكه الدول، فضلا عن الشركات العابرة للقوميات ثالثا، والتي بإمكانها تحقيق المصالح الاقتصادية للدولة في الأسواق الدولية وحتى تهديد المقومات الاقتصادية للخصوم، والمنظمات غير الحكومية التي بإمكانها تعبئة الرأي العام العالمي والضغط على الحكومات لتحقيق مصالح معينه من خلال الحملات الاعلانية التي تقوم بها. فضلا عن المنظمات الاجرامية والجريمة الالكترونية رابعا لا سيما الجرائم المنظمة، والتي تسعى لتحقيق منافع مادية خاصه بها مستثمرة اهم ما يتمتع به الفضاء الافتراضي من مزايا أهمها إمكانية إخفاء الهوية وصعوبة اكتشافها، والتنظيمات الإرهابية خامسا التي توظف موارد القوة السيبرانية للإضرار بالأمن القومي لدول بعينها لتحقيق اجندات سياسية عبر التهديد والإرهاب او تدمير البنى التحتية الرقمية للدول لتحقيق اهداف معينه، وجماعات القرصنة الالكترونية سادسا، والتي غالبا ما تسعى لتحقيق اهداف ربحية او منافع اقتصادية او سياسية او ايدلوجية، وأخيرا الافراد القادرين على توظيف مزايا الفضاء السيبراني مثلمارك زوكربارغ والذي استقطب اكثر من مليار شخص في العالم عبر تطبيق الفيسبوك، وتتمثل مرتكزات القوة السيبرانية بكل من البنية التحتية لتكنلوجيا المعلومات وأجهزة الحاسوب وإدارة ومعالجة قواعد البيانات والمعلومات وشبكات الاتصال من هواتف محمولة ووسائل اتصال لا سلكية وخطوط البث التلفزيوني عبر الأقمار الصناعية والكابلات وأجهزة التوجيه، والأسلحة السيبرانية التي تضم كلا من الفيروسات، الديدان، واحصنة طروادة والقنابل المنطقية وغيرها من الأسلحة[٢٥].

٣. الامن السيبراني:- ان الامن ابتداءا هو ضد الخوف، في ما يفيد الامن السيبراني اتخاذ الاجراءات والوسائل التنفيذية والتنظيمية والإدارية لمنع الوصول الى المعلومات التي تهم الامن القومي للدولة واستقرارها وأصولها الوطنية، واستغلالها بطرق غير مشروعة تهدد بإتلافها او مسحها او سرقتها، والمحافظة على سريتها، او انه يفيد مجموعة التدابير المضادة التي تتخذها الدولة لصد الهجمات السيبرانية او احتواء اثارها ونتائجها في ما بعد، بمعنى انه يفيد مجموع السياسيات الامنية التي تتخذها الدولة لإدارة المخاطر لصد هجمات قراصنة الكومبيوتر، والتدابير المضادة لاحتواء اثار الهجمات

السيبرانية [٢٦]. وهو يتميز بمجموعة من السمات يتمثل اهمها بمنع الوصول غير المصرح به للمعلومات التي تمس امن الدولة واستقراراها ورفاهيتها اولا، الارتقاء بقدرات حماية انظمة واجهزة معالجة المعلومات، بما فيها البنى التحتية الافتراضية للدولة واجهزة المستخدمين من الهجمات والمخاطر السيبرانية ثانيا، حماية وادارة امن المعلومات وشبكات الاتصال الرقمية الحديثة ثالثا، سرية وسلامة المعلومات والبيانات من الاختراقات السيبرانية رابعا[٢٧]. وفي العموم يفيد الامن السيبراني مجموع الساسيات الامنية التي تتضمن مجموعة من الاجراءات والتدابير الامنية التي تهدف الى حماية المعلومات الرقمية المعنية بالامن القومي للدولة من الاختراق والجرائم السيبرانية.

وتتمثل اهدافه بالحفاظ على امن المجتمع واستقراره اولا، والحفاظ على نظم المعلومات الرقمية الحيوية او المهمه في الدولية ثانيا، حفظ المعلومات والبيانات الرقمية ثالثا، حماية شبكة المعلومات الرقمية رابعا، فضلا عن ذلك فإن للأمن السيبراني ابعادا عدة يتنثل اهمها بالبعد العسكري، الذي يعني بالاوامر العسكرية وتبادل المعلومات وصد اي اختراق قد يستهدف الملفات المعنية بالامن القومي. فضلا عن البعد الاقتصادي وهو يتمثل بضمان امن التعاملات الاقتصادية والتجارية والمالية والصناعية للدولة في الفضاء الافتراضي، والبعد امن البعد الاجتماعي بما يتضمنه من وسائل الرقمية التي قد تكون مصدرا في تهديد الهوية الوطنية للدولة او تعريضها للغزو الثقافي ما لم يتم ضمان امنها، بالاضافة الى البعد السياسي الذي يعنى بحماية معلومات حساسة للدولة والوثائق المهمه لعمل قطاعات الدولة، اذ قد ينشب اشتباك عسكري مباشر بسبب تسريب معلومات حساسة كا حصل في الحرب الروسية الاوكرانية، واخيرا فإن للامن السيبراني بعدا قانونيا يتمثل بالقواعد القانونية التي تحاول السيطة على الفضاء الافتراضي وحماية امن الدولة[٢٨].

٤. **الجريمة السيبرانية:** وهو من المصطلحات الحديثة التي ظهرت مع ثورة المعلومات والاتصالات والثورة الرقمية لوسائل الاتصال ليفيد عمل اجرامي ينفذ عبر الحواسيب والشبكات الالكترونية بقصد الاضرار بالطرف الاخر، بمعنى انها جريمة تنفذ على الحاسوب او وسائل الاتصال الرقمية الحديثة. وهناك من يعرفها بوصفها السلوك غير المشروع والمنافي للأخلاق يتم تنفيذه عبر الشبكة العالمية للمعلومات يستهدف المعلومات او البيانات الخاصة بدولة او مؤسسه عبر اتلافها او سرقتها او تشويهها، وقد يستهدف السمعة ايضا[٢٩]. وهي تتميز بعد سمات يتمثل اهمها بانها تتم في الخفاء اولا، وتتم عن بعد ثانيا، فضلا عن ذلك فهي تتم بسرعة ثالثا، وهي جرائم عابرة لحدود رابعا، والاهم من ذلك كله يصعب اثباتها ولا تترك اثرا بعد تنفيذها لا سيما وانها تعد من الجرائم الناعمة اخيرا [٣٠].

٥. **الهجمات السيبرانية:** وهي تفيد الاجراءات التي تتخذها الدول لمهاجمة نظم المعلومات الرقمية للخصوم بهدف تشويهها او اتلافها او سرقتها، عبر تنفيذ سلسة من الهجمات الكترونية تقوم بها دولة ضد دولة اخرى[٣١].واصبحت هذه الهجمات اليوم اداه للصراع والتنافس الدولي واظهار النفوذ[٣٢].

٦. **الردع السيبراني:** ولما كان الردع يفيد منع الخصم من الاقدام علي عمل عدائي لإدراكه بإن التكاليف

المترتبة على العمل العدواني تفوق المكاسب التي يتوقعها [٣٣]، وعليه فإن الردع السيبراني يفيد الوسائل والإجراءات التي تعمل على منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السبراني، وهو يرتبط جذريًا بسياسات القوى الكبرى من جانب، والأبعاد الأمنية للفضاء السيبراني من جانبٍ آخر[٣٤]. والردع نوعان ردع بالمنع، ويكون عبر الارتقاء بالنظم الدفاعية لتمتع بالمصداقية، مما يجعل المهاجم يفكر بالاكلاف المترتبة على هجومه، واقناعه بإن الخسائر اعلى من المكاسب التي يتوقعها، في ما يتمثل النوع الثاني بالردع بالتهديد او العقاب عبر البدء بهجمات سيبرانية فيما يُعرف بـ(الردع بالانتقام)[٣٥]. واجمالا يتطلب الردع السيبراني استراتيجية معلنة متكاملة [٣٦]. ففي سنه ٢٠١٣ اصدر وزير الخارجية للملكة المتحدة بيانا اكد فيه ان ان بريطانيا ماضية باتجاه بماء وصياغة استراتيجيات للهجوم السيبراني المضاد في الفضاء الالكتروني، لتتبنى الولايات المتحدة والدول الاوربية ذات الموقف وتتجه الى صياغة استراتيجيات ردع سيبرانية [٣٧]، لتتعدد وتتنوع استراتيجيات الردع السيبراني[٣٨]، لأسباب عدة يتمثل اهمها بكل من ظهور فواعل جديدة من دون الدول اولا، وما يتسم به الفضاء السيبراني من طبيعة ثانيا، مثل تجاوز الحدود الجغرافية والزمنية ما يصعب تحديد وقت الهجوم وطبيعته، وتحديد السيادة الاقليمية لكل دولة في الفضاء السيبراني، فضلا عن استحالة عرض الاسلحة السيبرانية التي تستخدم للردع ثالثا كما هو الحال مع استراتيجيات الردع التقليدي [٣٩]، لا سيما مع صعوبة تحديد هوية المهاجم رابعا. وفي العموم لا يمكن ترصين استراتيجية ردع سيبرانية مالم تمتلك الدوله مصداقية للتهديد والدفاع والقدرة على الانتقام والرغبة في الانتقام، والقدرة على تكييف مفاهيم الردع التقليدية لتطبيق طرق وأساليب جديدة تتناسب مع هذا المجال الجديد، والتي قدد تتطلب توظيف مجموعة من الاستراتيجيات والوسائل التقليدية وغير التقليدية مثل الاحتجاج الدبلوماسي، والقدرة على إتخاذ التدابير القانونية، والعقوبات الاقتصادية، والانتقام في الفضاء الافتراضي التي يجب ان تقترن بالقدرة على الانتقام العسكري.

ومع تنامي ادراك الدول للتحديات السيبرانية وصعوبة صياغة استراتيجية سيبرانية شاملة للتصدي للمخاطر التي ترتبها الحروب السيبرانية وصعوبة التوصل الى رؤية مشتركه بإمكانها ان تحدد القيود القانونية لمنع الهجمات السيبرانية التي من شأنها تهديد امن الدول واستقراراها، فضلا عن تباين القدرات الاقتصادية والتكنلوجية للدول، وتناقض مصالحها واهدافها وطموحاتها تتسع الفجوات السيبرانية في ما بينها، لا سيما وان ميثاق الامم المتحدة لم يتطرق للهجمات السيبرانية بالرغم مما ترتبه من تحديات للسلم والامن الدوليين، خاصة من الفاعلين من غير الدول والذين قد يمتلكون قدرات تقنية اكثر مما تملكه الدول وتبلور ساحات افتراضية جديدة للصراع الدولي بأدوات تقنية جديدة. وما زاد من تعقد الامور وخروجها عن السيطرة اتجهت الدول الى ربط بنيتها التحتية من مصارف وشبكات طاقة كهربائية ومياه واتصالات ببنيتها التحتية الرقمية التي تضم اقمار صناعية وشبكات الكترونية وحواسيب مما زاد من التأثر الشبكي بين الدول داخل الدول وخارجها ورتب تزايد الفجوة في قدراتها السيبرانية، نجم عنه تزايد التحديات السياسية والمتمثلة بالحاق الضرر بشبكة المعلومات الوطنية والتي ترتبط بمؤسسات

لها علاقة بالأمن القومي للدول، مثل تدميرها او سرقة بياناتها او الوصول الى البريد الالكتروني للصناع القرار وعتك اسراراهم ومعلوماتهم او تهديدهم لحملهم على القيام بسلوكيات تتنافي وضمان مصالح دولهم. فضلا عن التحديات الامنية التي تطرحها الفجوة في القدرات السيبرانية بين الدول متمثلة بالحاق الضرر بمنظومات القيادة والسيطرة والاتصالات، او قطع الاتصالات بين القيادات المركزية والميدانية، واخراج الاسلحة عن مساراتها او التحكم بمنظومات تشغيلها او تدميرها مما يهدد الامن القومي للدول، فضلا عن التحديات الاقتصادية المتأتية من تزايد الفجوة في القدرات السيبرانية والمتمثلة بالآثار السلبية المترتبة على العولمة والانفتاح الاقتصادي وما قد يترتب عنه من تزايد عمليات النصب والاحتيال الالكتروني والسرقات والجرائم الاقتصادية[٤٠].

المطلب الثاني/ الحرب السيبرانية: المفهوم والمخاطر

مما لا شك فيه مثلت الحرب الافتراضية او السيبرانية أحد اهم التحديات للامن القومي للدول والسلم والامن الدوليين، لا سيما وإنها تحدث اضرارا تكافي او تساوي الاضرار التي تحدثها الحروب التقليدية، ومع تنامي وتطور الثورة الرقمية في وسائل الاتصال الحديثة اصبحت الحروب الرقمية أخطر اشكال الحروب واكثرها دمارا مما دفع الدول الى وضع استراتيجيات عسكرية وامنية للتصدي لأي هجوم سيبراني[٤١].

وتعرف الحرب السيبرانية بوصفها اختراق دولة لحواسيب دولة اخرى وبشكل غير مشروع وغير مصرح به بهدف الحصول على معلومات حساسة معنية بالأمن القومي، او تدمير الاقتصاد او شبكات الطاقة الكهربائية وغيرها من الاهداف التي تمس سيادة الدولة وامنها واستقرارها[٤٢]، بمعنى انها تفيد تلك الاجراءات التي تتخذها دولة للهجوم على نظم المعلومات للعدو بقصد الاضرار بها [٤٣]، او استخدام الحواسيب وشبكة المعلومات مما يجعلها الاداة المناسبة لفرض الاكراه والتأثير في الفواعل الدولية في الفضاء الافتراضي[٤٤]. اذ بإمكان الحروب السيبرانية اشعال الحروب التقليدية، او تدمير البني التحتية الرقمية للدول، والقواعد الاقتصادية والصناعية، وتحدث اختلالا في ميزان القوى العسكرية بين الدول في ضوء هذا التسارع المضطرد في اتجاه الدول نحو الارتقاء بقدراتها السيبرانية للانسجام مع المتغيرات التكنلوجية والاقتصادية والدولية الجديدة من قبيل تبلور فواعل دولية جديدة من غير الدول، فضلا عن ظهور ابعاد غير تقليدية وعابرة للحدود القومية للدول غيرت من اشكال التحديات التي تواجه امنها القومي مثل الفقر والاوبئة والمجاعات، بالاضافة الى تداعيات الاحتباس الحراري وما ترتبه من التغيير المناخي الذي بات يمثل تحديا عابرا للحدود، لتضاف الى الجرائم السيبرانية والتحديات السيبرانية التي بأمكانها النيل من مصالح الدول مثل تعطيل قدراتها العسكرية او الاقتصادية. لهذا عرَّفت منظمة التعاون الاقتصادي والتنمية الحرب السيبرانية بوصفها كل فعل يستهدف الاصول المادية والمعنوية للدولة عبر توظيف تكنلوجيا المعلومات وشبكات الاتصال الرقمي، في ما عرفتها لجنة الصليب الاحمر بوصفها الاعمال التي يقوم بها اطراف في نزاع ما للتفوق على خصومهم في الفضاء السيبراني [٤٥].

وعليه يمكن القول ان الحروب السيبرانية تفيد توظيف دولة لقدراتها الرقمية لاستهداف نظم المعلومات لخصومها في الفضاء السيبراني بهدف الاضرار بها او التأثير عليها لإرغامها على تنفيذ مصالح الدولة المهاجمة (بكسر الجيم)، مع تراجع قدرات الدول في تحقيق الردع في الفضاء الافتراضي او على الاقل السيطرة على الفضاء الدولي، لا سيما وان الجرائم السيبرانية عابرة للحدود ولا يمكن اكتشاف اوقات الهجمات السيرانية وتحديد هوية المهاجم او على الاقل التغلب على حالة الفوضى التي تسوء الفضاء السيبراني.

وتتسم الحرب السيبرانية بإنها حرب غامضة الاهداف، لا يمكن تحديد هوية او جنسية الفاعل، وهي حرب عابرة للحدود، لا توجد قواعد قانونية تحول دون تنفيذها او منع المهاجمين منها[٤٦]، ويمكن تصنيفها على انها حروب لا متماثلة اذا يمكن لدولة من دول العالم الثالث استطاعت امتلاك القدرات السيبرانية مهاجمة دولة متقدمة بسبب انخفاض تكاليف امتلاك ادوات الهجوم والحرب السيبرانية[٤٧]، فضلا عن تنوع اشكال الهجمات السيبرانية في هذه الحرب لتأخذ اشكال الارهاب الرقمي، والتجسس السيبراني، الاحتيال الرقمي وغيرها من الاشكال، ما يرتب تنوع وتعدد النتائج المترتبة على هذه الحرب.

وتجدر الاشارة الى ان هناك فارقا بين الحرب الالكترونية والحرب السيبرانية على الرغم من ان البعض يخلط بينهما، ففي الوقت الذي تعرف فيه الحرب الالكترونية بوصفها استخدام حزم الطيف الكهرومغناطيسي لتشويش أو تعطيل الاتصالات وأنظمة التحكّم والتوجيه الخاصة بقطعات جيش العدو لتعطيل نظام اتصالاته ودحره في المعارك وعبر الحواسيب الالكترونية، فإن الحرب السيبرانية تعرف بوصفها استهداف الشبكات الحاسوبية والأنظمة الرقمية للدولة الخصم والتي تشمل منشآت حيوية معنية بأمن الدولة واستقرارها ورفاهيتها وعبر الهجمات الافتراضية في الفضاء الافتراضي، وهذه الهجمات قد تشمل سرقة البيانات الحساسة وتعطيل البنية التحتية الرقمية، مثل محطات الطاقة أو شبكات الاتصالات، اذا تستخدم في الحروب الالكترونية الحواسيب الالكترونية بينما تستخدم الحرب السيبراني الفضاء الافتراضي الذي يعد اليوم احد مجالات السيادة بالاضافة الى البر والبحر والجو والفضاء، حيث تستخدم في الحروب السيبرانية الفضاء الرقمي وشبكات المعلومات الدولية، بينما تستخدم في الحروب الالكترونية الكيف الكهرومغناطيسي والاتصالات، اذ ان الحرب السيبرانية تستخدم الفيروسات، والبرمجيات، لتعطيل البنية التحتية كالمياه والكهرباء، مما يشل عصب الاقتصاد وقد يرتب ضحيا من الافراد، اما الحرب الإلكترونية يمكن أن توقف حركة البنوك والمطارات والبورصات[٤٨].

المبحث الثاني:- استراتيجيات الحرب السيبرانية الإيرانية – (الإسرائيلية):- ادركت كلا من إيران و(إسرائيل) اهمية الارتقاء بقدرات الردع السيبراني لكلا منهما مع التسارع المضطرد لتطورات الفضاء السيبراني، الذي ظهر بوصفه فضاءا جديدا فضاءات الصراع والتعاون الدولي الاخرى، ولا يمكن ادراك اثار وتداعيات استراتيجيات الردع السيبراني بين إيران و(إسرائيل) ما لم ندرك مرتكزات استراتيجيات الردع السيبراني لكلا منهما، لذا سيتناول هذا المطلب القدرات السيبرانية لكل من إيران و(اسرائيل) في اولا، والاستراتيجيات الإيرانية و(الاسرائيلية)في ثانيا، والافاق المستقبلية لاستراتيجيات هذه الحرب في ثالثا، وكما يأتي:-

المطلب الاول: القدرات السيبرانية الإيرانية و(الإسرائيلية)

تتنوع القدرات السيبرانية لكل من إيران و(إسرائيل) لا سيما بعد تزايد التصعيد بينهما بعد عام ٢٠١٠ لتشمل كلا مما ياتي:

أ. القدرات السيبرانية الإيرانية: أدركت إيران اهمية بناء قوة سيبرانية متميزة مع عام ٢٠٠٣ وتموضع القوات الامريكية في العراق منذ العام ٢٠٠٣، وابرام اتفاقية الاطار الاستراتيجي معه، فضلا عن تسارع (إسرائيل) الى الارتقاء بقدراتها العسكرية عموما وقدراتها السيبرانية على وجه الخصوص، اذ انها ادركت اهمية امتلاك قوة سيبرانية متميزة تحقق متطلبات امنها القومي[٤٩]، في الوقت الذي اتجهت فيه الى ترصين منظومه من الحلفاء من دون الدول للوصول الى شرق المتوسط لتصدير النفط والغاز الإيراني بعيدا عن العقوبات الامريكية المفروضة عليها. واجمالا أدركت إيران خطورة الهجمات السيبرانية منذ العام ٢٠١٠ بعد ان هوجمت المفاعل النووية الإيرانية، وبعد تداعيات التظاهرات التي اندلعت في إيران عام ٢٠٠٩ والتي استخدمت الاف المنصات الالكترونية للترويج لأفكارها المعارضة لنهج النظام السياسي الإيراني لتسارع الى الارتقاء بقدراتها السيبرانية، لا سيما وإنها تدرك ان الفضاء السيبراني بمكن ان يعوضها عن الافتقار لبعض الاسلحة مثل انظمة الدفاع الجوي والطائرات الحربية الحديثة، اذ يوفر الفضاء السيبراني قدرات عابرة للحدود[٥٠].

وعلى الرغم من محدودية التقنيات المتقدمة التي استطاعت إيران الحصول عليها منذ العام ١٩٧٩ بسبب العقوبات الدولية المفروضة عليها، الا انها استطاعت تحقيق تفوق عسكري كبير في قدراتها العسكرية غير المتماثلة عبر منظومة من الحلفاء من غير الدول والتي استطاعت تمكينها من امتلاك قوة سيبرانية، استطاعت بمرور الوقت تطويرها حتى تمكنت من التجسس على خصومها وشنّ الهجمات السيبرانية عليها[٥١]، لا سيما وانها تدرك الاهمية الاستراتيجية لمنطقة الخليج بما فيها العراق الذي يمثل حدودها الشمالية بالاضافة الى منطقة شرقي حوض المتوسط، حيث تملك مفاتيح الصراع الجيوبولتيكي والجيو–استراتيجي العالمي، اذ لا تقتصر مقومات القدرة التي تملكها هذه المنطقة على امتلاكها لمصادر الطاقة العالمية فحسب، بل انها تطل على ممرات بحرية تتحكم في السلسلة البحرية الاهم في العالم، والمتجهة من منطقه الخليج وحوض المتوسط الى اوربا، واهمها مضيق هرمز الذي يعد شريان الطاقة العالمي، ومضيق باب المندب وصولا الى قناه السويس لتشكل هاتين المنطقتين عنق الزجاجة للسلسلة البحرية الاهم في نصف الكره الغربي، وتكاد الاهمية الجيوبولتيكية لهذه المنطقة تتفوق على الاهمية الجيوبولتيكية الجيواستراتيجية لإيران بل وحتى تركيا. فضلا عن ذلك فهي تدرك عمق القضايا الخلافية بينها وبين الولايات المتحدة الامريكية، التي ترى في منطقة جنوب غرب آسيا والشرق الاوسط في العموم أحد اهم مناطق الامن القومي الامريكي لاعتبارات ضمان امن الطاقة ومعابر امداداتها. وتتسم البنية التحتية للقوة السيبرانية بالغموض والتعقيد، لا سيما وإنها ترتكز على فواعل سيبرانية نظامية وغير نظامية[٥٢]، اذ طورت إيران قدرات الحرب الالكترونية لتحييد القدرات التقنية لخصومها ومعارضيها في

الداخل والخارج، وفق استراتيجية اعدت لهذا الغرض منذ سنوات تقودها قيادات الحرس الثوري الإيراني كونوا فضاءا افتراضيا طوروا من خلاله قدرات الصواريخ الباليستية التي تملكها إيران ومهاجمة الدول التي ترفض البرنامج النووي الإيراني وتعارضه[٥٣]. وتشمل القوة السيبرانية الإيرانية ما يأتي[٥٤]:-

١. **البنى المؤسساتية الإيرانية المسؤولة عن التصدي للتهديدات الافتراضية:** وهي تضم منظمة الدفاع المدني اولا، وقد انشات عام ٢٠٠٣، ويتمثل دورها في التصدي للهجمات السيبرانية الداخلية والخارجية، وقد تزايد دورها عام ٢٠١٤، وشرطة الانترنيت ثانيا، وقد تم انشائها عام ٢٠١١، وهي تعمل لمتابعة والتصدي للمجرمين السيبرانين، فضلا عن المجلس الأعلى للفضاء السيبراني ثالثا، وهو يضم قيادات عسكرية من الجيش والحرس الثوري وكبار المسؤولين في الاجهزة الامنية، يتولى مهمه التنسيق للدفاع والهجوم السيبراني. بالاضافة الى والجيش السيبيري الإيراني رابعا، بقوام (٢٥٠٠) فرد يتولى مهمه حماية النظام السياسي الإيراني في الداخل والقيام بهجمات سيبرانية في الدول المعادية في اخارج بميزانية تربوا على (٨٠) مليون دولار سنويا. واخيرا كتائب الباسيج الإيرانية والتي تتكون من وحدات خاصة مسلحة بأحدث القدرات السيبرانية مهمتها التصدي لقوى معادية للنظام السياسي الإيراني[٥٥]، ومن الجدير بالذكر ان هذه الكتائب تملك العديد ن التقنيات الافتراضية وتكنلوجيا الحروب الالكترونية للتصدي لرموز المعارضة الإيرانية في الداخل مثل بث الاشاعات ضدهم وانشاء المدونات الالكترونية التي تتصدى لهم.

٢. **الفواعل الرقمية غير الرسمية:** وهي تضم كلا من مجموعة عز الدين القسام اولا، والتي تضم مجموعة من القراصنة الإيرانيين المهرة، استطاعت هذه المجموعة اختراق البنوك الامريكية عامي ٢٠١٢ و٢٠١٣ ردا على العقوبات الامريكية، فضلا عن مجموعة ايشيان ثانيا وهي تضم مجموعة من أمهر جماعات الهاكرز والقراصنة الإيرانيين، تتعامل مع الجامعات الإيرانية لحماية الامن السيبراني الإيراني، فضلا عن إيران هاك ثالثا، تعمل على التنسيق مع المجاميع السيبرانية الاخرى، ومواكبة التطورات في الفضاء السيبراني. بالاضافة الى مجموعة APT33 رابعا، والتي تستهدف المراكز البحثية الامريكية والشرق اوسطية. ومجموعة APT34 خامسا، والتي تعد أكثر المجاميع السيبرانية الإيرانية شهرة في الشرق الاوسط لقيامها بالعديد من الهجمات على دول معادية لها في الشرق الاوسط، ومجموعة الAPT35 سادسا تضم مجموعة من المخترقين السيبرانين تعمل على جمع المعلومات عن العسكريين الامريكان في الولايات المتحدة ودول الشرق الاوسط، ومجموعة ال APT39، ومهمتها مراقبة الشخصيات العالمية والتي قد نشكل تهديد للامن القومي الإيراني[٥٦]، فضلا عن مجموعة من المنتديات الرقمية الإيرانية[٥٧].

ومن جانب آخر فإن إيران دعمت القوى السيبرانية لحلفائها الاقليمين مثل الجيش السوري السيبراني الذي استهدف البنية التحتية السيبرانية الامريكية و(الإسرائيلية) وحلفاء الولايات المتحدة في منطقة الخليج، ومؤسسة الفضاء لحزب الله التي هاجمت سيبرانيا اهداف (إسرائيلية) اكثر من مره، وجيش فضاء اليمن السيبراني الذي اتضح دوره في الحرب في اليمن مع المملكة العربية السعودية، واجمالا يمكن القول ان

إيران تركز في قدراتها السيبرانية على الفواعل غير النظامية لسهولة افلاتها من الملاحقة القضائية[٥٨]، ووفقا لخبراء اوربيون في الامن السيبراني فإن إيران تعد من الدول الاكثر نشاطا سيبرانيا في السنوات الاخيرة. وعلى الرغم من الانفاق الهائل الإيراني في سبيل الارتقاء بقدراتها السيبرانية الا انها ما تزال حتى اللحظة لم تستطع موازاة القوة السيبرانية الصينية، إذا يمكن اكتشاف الهجوم السيبراني الإيراني بنسبة (٧٥%)بينما امكانية اكتشاف العجوم السيبراني الصيني تصل الى (٣٣%)[٥٩].

ب. القدرات السيبرانية (الإسرائيلية): ادركت (إسرائيل) ومنذ عام ١٩٤٨ اهمية ترصين استراتيجياتها الامنية لمواجهة التحديات المعقدة التي تحيط بها، لا سيما وانها وجدت نفسها معزولة في محيط اقليمي لا تنتمي اليه ولا يقيم معها علاقات طبيعية[٦٠]، وهو ما دفع (ديفيد بن غوريون) اول رئيس وزراءها الى تبني استراتيجية نقل الحرب الى اراضي الخصوم كما كان يخطط[٦١]، لافتقارها الى العمق الاستراتيجي اولا فضلا افتقارها الى القدرات الديموغرافية التي تمكنها من الصمود في اي حرب متوقعه مع دول جوارها، وهي ذات الاسباب التي دفعتها الي تبني استراتيجية الضربة الوقائية والطوق الامن او الحدود الآمنة وغيرها من الإستراتيجيات ذات الابعاد العسكرية. وبعد الحرب الباردة واحداث سبتمبر ٢٠٠١ حرصت على تكييف قدراتها العسكرية بما فيها قدراتها الافتراضية وبما ينسجم مع التحديات المستحدثة في العلاقات الدولية، والتي نقلت الامن القومي الى افاق وابعاد غير تقليدية عابرة للحدود مثل التغييرات المناخية وتزايد ادوار الفواعل من غير الدول لا سيما الفواعل المتطرفة منها.

ويعد عام 2010 عاماً مفصلياً لدى (إسرائيل)، حيث بدأت تداعيات ما عرف بالربيع العربي تحيطها بالدول الفاشلة التي مكنت الجماعات الاصولية الارهابية من الاقتراب من الحدود (الإسرائيلية) من جهة، فضلا عن تنامي الدور الاقليمي الإيراني المرتكز على مجموعة القوى الناعمة متمثلة بإمبراطوريتها الاعلامية، وعمقها الحضاري، والتراجع الكبير في الاداء العربي الفاعل في تسوية ازمات المنطقة، بالاضافة الى مقوماتها الصلبة متمثلة بقدراتها الصاروخية، ومنظومة الحلفاء من الفواعل من دون الدول وبرنامجها النووي والطائرات المسيرة التي بإمكانها نقل رؤوس تفجيرية غير تقليدية الى الاراضي (الإسرائيلية)، الامر الذي شكل دافعا قويا ل(إسرائيل) للارتقاء بقدراتها السيبرانية حتى ظهرت بوصفها القوة السيبرانية الثالثة عالميا، بعد اطلاق المبادرة السيبرانية (الإسرائيلية)عام ٢٠١٠، برعاية المجلس(الإسرائيلي) للبحث والتطوير للتصدي للتحديات والتهديدات العسكرية والمدنية على حد سواء، لا سيما وانها كانت من اكثر الدول تعرضا للهجمات السيبرانية على مستوى العالم، لكن بعد العام ٢٠٢٠ لم تعد تظهر (إسرائيل) في قائمة الدول العشرة الاولى الاكثر تعرضا لتلك الهجمات[٦٢]. حيث سعت هذه المبادرة الى الارتقاء بالقدرات (الإسرائيلية) لإدارة تحديات الفضاء الافتراضي الحالية والمستقبلية اولا، الارتقاء بقدراتها الدفاعية لحماية البنى التحتية (الإسرائيلية)ثانيا، تعزيز استراتيجياتها التعاونية مع الدول في الفضاء الافتراضي متعدد التخصصات ثالثا، الظهور بوصفها قوه سيبرانية متميزة ومحط انظار دول العالم في مجال تعزيز الامن السيبراني رابع[٦٣]ا.

وفي العموم استطاعت (إسرائيل) احتلال المرتبة السادسة عالميا عام ٢٠٢٠ بعد كلا من الولايات المتحدة الامريكية والصين والمملكة المتحدة وروسيا وهولندا في مؤشر النوايا السيبرانية، وتصدرت الدول الاعضاء في منظمة التعاون الاقتصادي في نسبة انفاقها على البحث والتطوير عام ٢٠١٨، وبما يصل الى (٤,٩%) من اجمالي دخلها القومي[٦٤]، ويمكن اجمال اهم مرتكزات القدرات السيبرانية (الإسرائيلية) بما يأتي:

١. **برنامج الفضاء الخارجي(الإسرائيل):** حيث طورت (إسرائيل) ومنذ العام ١٩٦٣ برنامجها للفضاء الخارجي، عبر انشاء لجنتها القومية لبحوث الفضاء، والتي كان لها الدور في دخول (إسرائيل) الى نادي الفضاء العالمي، والارتقاء بقدراتها الصناعية في مجال الفضاء والتكنلوجيا المتقدمة[٦٥].

٢. **محطات لانتاج وبرمجة الاقمار الاصطناعية:** حيث تم انشائها لغزو الفضاء لخارجي، وتم انشائها بأبعاد عسكرية وامنية ورقمية، ولها قدرة على تعطيل شبكات الاتصال في المنطقة لا سيما العربية والتركية والإيرانية[٦٦]:-

أ. هيئة تطوير الاسلحة (رافائيل) وهي واحدة من أكبر الشركات المعنية بتطوير الاسلحة (الإسرائيلية).

ب. القمر أفق١ (Ofeq 1) والذي تم انطلاقة عام ١٩٨٨، وقد أطلق لاغراض تجسسية.

ت. القمر افق ٢(Ofeq 2) وقد أطلق لأغراض استكشافية عام ١٩٩٠.

ث. القمر تكسات ١(Tksat 1) أطلق عام ١٩٩٥ بالتعاون بين مجموعة من الطلبة (إسرائيليين) والروس لاغراض علمية الا ان تجربتهم باءت بالفشل.

ج. القمر افق ٣ (Ofeq 3) وقد أطلق عام ١٩٩٥ بقدرات رقمية متطورة للتصوير ومن مسافات بعيدة عن الارض.

ح. حالقمر عاموس (Amos) تم اطلاقه عام ١٩٩٦ لأغراض الاتصالات ونقل المعلومات والبيانات الى القواعد الارضية وادراة استراتيجيات الجيش (الإسرائيلي) في ما يتعلق برصد المعلومات والاختراقات المعلوماتية.

خ. القمر افق ٥(Ofeq 5)، تم اطلاقه عام ٢٠٠٢ بتقنيات متقدمة لاستخدامه لأغراض الاستطلاع العسكري والتجسس ولأغراض امنية الاخرى.

د. القمر بولاريس (Polares) وهو يكافئ الاقمار الاصطناعية الامريكية في قدراته التقنية مخصص للأغراض العسكرية.

ذ. القمر افق ٩(Ofeq 9) تم اطلاقه عام ٢٠١٠ لاغراض التجسس على إيران، علما إن (إسرائيل) تملك العديد من الاقمار الاصطناعية المخصصه لأغراض التجسس في الفضاء الإيراني.

س. وأخطر الاقمار الاصطناعية التي أطلقتها (إسرائيل) يتمثل بالقمر افق ١٦ (Ofeq16) والذي أطلقته في شهر تموز من عام ٢٠٢٠ بقدرات متطورة جدا، اشترك في تصنيعه عدة شركات(إسرائيلية) بقيادة هيئة الصناعات الجوية (الاسرائيلية)، واهم اغراضه يتمثل بالتجسس، لا سيما وانه أطلق بعد التصعيد الإيراني –(الاسرائيلي) في الشرق الاوسط[٦٧].

٣. **البنية التحتية لعصر الانترنيت:** حيث أنشأت (إسرائيل) عام ١٩٩٧ البنية التحتية لعصر الانترنيت في وزارة المالية (الإسرائيلية)عبر اقامة مركز حماية المعلومات بهدف التنسيق بين الوزارات والمؤسسات الحكومية وحماية المعلومات، ومتابعة تطور وسائل حماية المعلومات والبيانات في العالم[٦٨].

٤. **القوة السيبرانية للجيش (الاسرائيلية):** حيث تم انشاء هذه القوة بوصفها ذراعا رابعا بالاضافة الى سلاح الجو (الإسرائيلي) والقوات البحرية والبرية (الإسرائيلية)، واصبحت في ما بعد هذه القوة خامس قوة سيبرانية في العالم، بسبب ما تملكه من قدرات سيبرانية وتقنية متفوقة، واصبحت الان احد اهم ادوات الاستراتيجية العسكرية (الاسرائيلية) في حروبها دفاعا وهجوما واحد اهم ادواتها في العمليات العسكرية الخاصة اليت تقوم بها [٦٩].

٥. اقتناء التكنلوجيا المتقدمة في المجال العسكري:- لا سيما وان (إسرائيل) منذ قيامها حرصت على الارتكاز على استراتيجيات ذات ابعاد امنية وعسكرية لمواجهة التحديات المعقدة التي تواجهها، اذ حرصت على شراء كل ما تنتجه الصناعات العسكرية التكنولوجية في العالم من قدرات تقنية ذات بعد عسكري لحماية بنيتها التحتية من أي اختراقات أو هجمات قرصنة[٧٠].

٦. حرصت (إسرائيل) على استضافة المؤتمرات التي تعالج قضايا التعاون في مجال الامن السيبراني الافتراضي، حيث تعقد سنوياً مؤتمر التكنلوجيا السيبرانية، وابرمت العديد من اتفاقيات التعاون في مجال الامن السيبراني، مثل اتفاقياتها مع الهند والامارات العربية المتحدة[٧١]، التي اضيفت الى اتفاقيات التعاون السيبراني مع الولايات المتحدة الامريكية وغيرها من الدول المتطورة في هذا المجال.

٧. بالاضافة الى ما سبق فإن اسرائيل انشأت وحدة او جهاز يعتمد التقنيات الرقمية للحصول علة المعلومات الجغرافية والسياسية والاقتصادية عن خصومها في المنطقة العربية هو جهاز (آمان)، لتأمين المعلومات العسكرية والامنية والاستخبارية عن خصومها[٧٢].

٨. الوحدة (٨٢٢٠)، وهي تضم الاف من الجنود والضباط (الإسرائيليين) تأسست عام ١٩٥٢، مهمتها اعداد الخبراء السيبرانيين ذوي الكفاءات، وتشفير المعلومات والتجسس، ومتابعة التهديدات السيبرانية، بالتعاون مع وحدات اضافية للامن السيبراني[٧٣].

٩. انشأت (اسرائيل) العديد من الاجهزة الاستخبارية والمخابراتية الامنية التي ضمت العديد من القدرات الرقمية للتصدي للهجمات السيبرانية ولأغراض تجسسية مثل جهاز الشاباك والموساد

المطلب الثاني: أهداف ووسائل استراتيجيات الحرب السيبرانية الإيرانية – (الاسرائيلية)

لا يمكن فهم استراتيجيات الحرب السيبرانية بين إيران و(اسرائيل) ما لم نفهم اهداف كل واحدة منهما في هذه الحرب ووسائلهما وهذا ما سيوضحه المحور الثاني، لذا سنتناول اهم الاهداف والوسائل الإيرانية السيبرانية، والاهداف والوسائل السيبرانية (الاسرائيلية) في هذه الحرب بينهما.

أ. **الاهداف السيبرانية الإيرانية:** حرصت إيران ومنذ وقت مبكر على الاستعداد للتصدي للتحديات السيبرانية، حتى تمكنت من امتلاك قدرة على شن الهجمات الافتراضية على دول جوارها دون دفعهم باتجاه شن حرب تقليدية عليها[٧٤]. ويمكن اجمال اهم الاهداف الإيرانية وراء الارتقاء بقدراتها السيبرانية:

١. **حماية النظام السياسي الإيراني:** ادرك النظام السياسي الإيراني التحديات السياسية التي تواجهه والقضايا الخلافية بينه وبين القوى الدولية الفاعلة منذ العام ١٩٧٩، وتزايدت الهواجس الامنية التي تواجهه منذ عام ٢٠٠٩، في ضوء تبلور الفضاء الافتراضي الذي يمكن الجماعات والقوى المعارضة له من استخدامه بشكل يهدد وجوده، لا سيما وانها تطالب بالبديل، وظهر ذلك جليا في الدعوات التي رفعها المعارضون في الثورة الخضراء عام ٢٠٠٩، لتنطلق اول عملية سيبرانية في إيران عام ٢٠٠٩، لا سيما وان القوى القابضة على السلطة في إيران ادركت ان شبكة المعلومات الدولية ستكون متاحه للمعارضين لترتب تهديدات وتحديات خطيرة للنظام السياسي الإيراني والامن والاستقرار في إيران(٧٥). لتبدأ إيران في توظيف قدراتها السيبرانية لأغراض التجسس على المعارضين داخل إيران وخارجها، وبدأت باختراق التطبيقات التي تسهل التواصل بين قيادات الثورة الخضراء مثل تويتر وفيسبوك وغيرها من التطبيقات وتعطيلها وحرمان المستخدمين في إيران من الوصول اليها وقطع وسائل التواصل بين المعارضين الإيرانيين في الخارج والداخل، ولم تكتف بهذه الاجراءات والتدابير، اذ انها طردت وسائل الاعلام الغربية، والتجسس على اجهزه الهاتف المحمول واعتقال المعارضين(٧٦).

٢. **البحث عن دور اقليمي فاعل:** على الرغم من القضايا الخلافية بين إيران والولايات المتحدة الامريكية وحلفائها في الشرق الاوسط واهمهم اسرائيل، الا ان إيران لم تتخلى عن طموحها الاقليمي في دور اقليمي واعد لتأمين مجال حيوي ضامن لأمنها القومي عبر الهيمنة على الاطلالات البحرية في جنوب غربي آسيا ومصادر الطاقة فيها، مما دفعها للارتقاء بقدراتها العسكرية على الدوام واهمها قدراتها الافتراضية لأغراض الدفاع والهجوم، فضلا عن استهداف المنشآت الاقتصادية لخصومها التقليدين واهمهم الولايات المتحدة الامريكية وحلفائها (٨٠).

٣. **الارتقاء بقدراتها العسكرية عبر امتلاك تقنيات رقمية واطئة الكلفة:** لا شك ان العقوبات الاقتصادية المفروضة على إيران حدت من الكثير من قدراتها العسكرية الامر الذي تراه انه يشكل تهديدا لأمنها القومي، مثل تراجع اداء قدراتها الجوية الحربية، الامر الذي دفعها للارتقاء بقدراتها غير المتماثلة مثل الصواريخ الباليستية، وقدراتها السيبرانية، لتحييد القدرات الافتراضية المتقدمة لمنافسيها في المنطقة، لترتفع الموازنة الإيرانية للارتقاء بقدراتها السيبرانية بنسبة (١٢٠٠%) للمدة (٢٠١٣ –٢٠١٧) فقط، كما حرصت على توظيف قدراتها السيبرانية في استراتيجيتها العسكرية (٨١)، مما يمكنها من القيام بعمليات انتقامية ضد خصومها، وتحييد معارضيها في الخارج، لا سيما وإنها تدرك ان الد خصومها المتمثل ب(اسرائيل) يهيمن على الفضاء الافتراضي في منطقة الشرق الاوسط عبر ما تملكه من اقمار صناعيه متقدمة بما تملكه من قدرات وبرمجيات حديثة.

٤. **الارتقاء بقاعدتها الصناعية والاقتصادية:** اذ حرصت إيران على اختراق مراكز الابحاث الدولية والإقليمية لاقتناص المعلومات والبيانات التي بإمكانها للارتقاء بقدراتها الصناعية والاقتصادية (٨٢).

٥. **امتلاك القدرة على تحييد الخصوم:** يتمثل اهم الاهداف وراء مساعي إيران لتطوير قدراتها الافتراضية هو تعزيز ادائها الاستراتيجي وامتلاك قدرات الردع السيبراني لخصومها التقليدين واهمهم (اسرائيل) في ضوء تفاقم الازمات الاقليمية التي شهدتها منطقة جنوب غرب آسيا وشرق المتوسط، لا سيما وان إيران امتلكت منظومة من الفواعل من دون الدول مكنتها من الوصول الى شرق المتوسط، املا في تصدير الغاز الإيراني عبر الاراضي العراقية والإيرانية بعيدا عن العقوبات المفروضة عليها من قبل الولايات المتحدة الامريكية، قبل احداث غزة عام ٢٠٢٣، مما رتب تزايد التحديات العسكرية للامن القومي الإيراني تطلب معه الارتقاء بقدراتها السيبرانية. فضلا عن ذلك حرصت إيران على توظيف قدراتها الافتراضية للتصدي لهجمات خصومها وقدراتهم الاقتصادية والصناعية لأثبات قدراتها على القيام بأعمال انتقامية للردع او تحييد الخصوم، وبالفعل رتبت الهجمات السيبرانية الإيرانية الثير من الخسائر للملكة العربية السعودية في منشآتها النفطية عام ٢٠١٢، فضلا عن الهجمات السيبرانية التي قامت بها مجموعة (APT 33) الإيرانية للمدة من ٢٠١٦- ٢٠١٩ على بعض المصالح السعودية والامريكية[٨٣].

٦. **امتلاك قدرات تجسسية سيبرانية تدعم ادائها الاستراتيجي في المنطقة:** حرصت إيران على الارتقاء بقدراتها الافتراضية لتعزيز قدراتها في التجسس والمراقبة على الشخصيات المتنفذة اقليميا دوليا بهدف بلورة رؤية واضحه لصناع القرار الإيرانيون تمكنهم من صياغة استراتيجيات الامن القومي الإيراني بشكل يتناسب وطموحاتها الاقليمية للظهور بوصفها قوة اقليمية متميزة وقدراتها المتاحة، كما استطاعت الفواعل النظامية وغير النظامية السيبرانية الإيرانية التجسس على المنظمات الدولية الحكومية وغير الحكومية بما يرفدها برؤية واضحه لضمان مصالحها الحيوية خارج إيران [٨٤].

٧. **توظيف قدراتها الرقمية للترويج لمشروعها الاقليمي:** ركزت إيران لا سيما بعد العام ٢٠٠٩ على الترويج لمشروعها الاقليمي عبر توظيف قدراتها الرقمية، لحشد رأي عام محلي واقليمي ودولي يساند توجهاتها السياسية ويدعمها، ويوجيه الانتقادات لخصومها الإقليمين والدوليين عبر وسائل التواصل الاجتماعي، وبما يعزز مصالحها الاقليمية ودورها الاقليمي، وهو ما نجحت فيه حتى احداث غزة عام٢٠٢٣، مستثمرة التنوع الاثني والعرقي في منطقة جنوب غربي آسيا وشرق المتوسط، مما اثار الهاجس الامني لدى الولايات المتحدة الامريكية وحلفائها من تنامي الدور الافتراضي الإيراني واحتمالية تهديده للمصالح الامريكية في الشرق الاوسط الذي يعد احد اهم مناطق الامن القومي الامريكي لاعتبارات ضمان امن الطاقة ومعابر امداداتها، فضلا عن تهديد الدور السيبراني الإيراني مصالح حلفاء الولايات المتحدة الامريكية، عبر تهديد الاستقرار الاقليمي[٨٥].

٨. **ضبط نقل وتداول المعلومات لحماية العمق الإيراني من الغزو الحضاري الوافد:** تسعى إيران عبر توظيف حربها الناعمة في الداخل الى الحفاظ على نمط الثقافة الإيرانية من الغزو الاجنبي، ونشر الافكار ونمط الثقافة الغربية سبيلا لضمان هيمنتها على المجتمع الإيراني بعيدا عن التأثيرات الاجنبية، من خلال منع تداول الافكار الغربية الى المواطنين الإيرانيين، والهيمنة على الثقافة الإيرانية، والعمل على

ربط نظامها السياسي بإرثها الحضاري الفارسي وبما يؤدي في نهاية المطاف الى عزل الإيرانيين عن الفضاء الافتراضي العالمي، وما سهل لها ذلك هو العقوبات الامريكية والدولية المفروضة على إيران والتي تحول دون وصول الإيرانيين الى المنصات الرقمية الغربية مثل غوغل وامازون والالقاب الالكترونية الغربية [٨٦]، وعلى هذا الاساس تم انشاء شبكة المعلومات الإيرانية لمنع الغرب والخصوم التقليدين لإيران من الوصول الى افضاء الافتراضي الإيراني، وتم الزام المواطنين الإيرانيين باعتماد المنصات الرقمية الإيرانية، والتي انشأت تحت اشراف الحرس الثوري الإيراني عام ٢٠١١، اطلق على هذه المنصة شبكة الانترنيت الحلال ردا على احتجاجات الثورة الخضراء عام ٢٠٠٩ [٨٧]، كما حرصت إيران على السيطرة على نظم الاتصالات في إيران بهدف مراقبة نقل المعلومات وضبطها وعرقلتها او اغلاقها عند تصاعد حملات الاحتجاجات المعارضة.

ب. الاهداف السيبرانية الاسرائيلية: مما لا شك فيه فإن اهم اهداف (إسرائيل) للارتقاء بقدراتها الرقمية يتمثل ضمان دور مهيمن على الفضاء الافتراضي سبيلا لتأمين قوة هجمية سيبرانية وقوة ردع سيبراني في ظل التحديات المحيطة بها ويمكن اجمال اهم الأهداف (الإسرائيلية) للارتقاء بقدراتها الرقمية وكما يأتي:

١. **ضمان أمنها القومي:** مما لاشك فيها ان الهاجس الامني الاخطر لإسرائيل يتمثل بضمان امنها القومي في ظل وجود تحديات وجودية تحيط بها في بيئتها الاقليمية، وعلى هذا الاساس انشات العديد من الاجهزة اهمها تمثل (بسلطة الدفاع السيبراني الاسرائيلي) عام ٢٠١٦ لتوفر لها ردع متوازع بإمكانه ان يضمن امن (إسرائيل) واستقرارها في كل الاوقات والتصدي للهجمات السيبرانية ايا كان مصدرها او حجمها، وجمع الملومات وتحليلها لرصد التحديات في الفضاء الافتراضي (الاسرائيلي)، وضمان امن البنى التحتية (الإسرائيلية) والمؤسسات في كل الاوقات والاحتمالات[٨٨]، لا سيما وان الاستراتيجية ا(الاسرائيلية) الشاملة تغلب عليها الابعاد العسكرية والامنية ما يدفعها على الدوام للارتقاء بقدراتها السيبرانية التي تعد مكونا اصيلا في عناصر ومتركزات الاستراتيجية العسكرية والامنية (الاسرائيلية) في السلم والحرب، لتوفر لها ردعا فاعلا ضد الهجمات السيبرانية وقدرات للهجوم السيبراني وبكفاءة عالية[٨٩]، لا سيما وان العقيدة العسكرة الاسرائيلية لا تفرق بين الحروب التقليدية والحروب السيبرانية[٩٠].

٢. **الارتقاء بقدراتها الاقتصادية:** حرصت (اسرائيل) منذ ولوجها الى الفضاء الافتراضي على توظيف قدراتها الرقمية في تعزيز قاعدتها الاقتصادية، اذ ان الاقتصاد الرقمي فيها يرتكز على صناعة تقنيات الاتصالات ونقل المعلومات من خلال تصنيع التطبيقات والمعدات عالية التقنية اولا وعلى التجارة الالكترونية ثانيا، حيث تجاوز حجم التجارة الألكترونية في (اسرائيل) (٥٠) مليار شيكل في عام ٢٠٠٩، ما يضعها في مصاف الاقتصاديات الرقمية في العالم[٩١]. فضلا عن ذلك حرصت (اسرائيل) على جذب الاستثمارات العالمية في مجال تكنلوجيا المعلومات، حيث تعمل أكثر من (٥٠٠) شركه (اسرائيلية) في ميدان تقنيات المعلومات استطاعت تحويل(اسرائيل) الى اهم بلد يصنع ويصدر برمجيات تقنيات التجسس العالمية وبأسعار باهضه [٩٢].

٣. **الحصول على الدعم المحلي والدولي لشرعية وجودها:** اذ تحرص (إسرائيل) على حشد دعم محلي ودولي يؤمن لها شرعية الوجود عبر توظيف ما تملكه من وسائل تواصل رقمية بما فيها الدبلوماسية السيبرانية(الاسرائيلية)، للانفتاح على شعوب الدول الفاعلة في النظام الدولي ومجتمعاتها، فضلا عن شعوب منطقة الشرق الاوسط، لا سيما وانها تسعى الى الظهور بوصفها حلقة الوصل الاهم بين دول الشرق الاوسط الذي تنتمي اليه جغرافيا والدول الفاعلة في اوربا والولايات المتحدة التي تنتمي لها فكريا وسياسيا مستثمرة منظومة تحالفاتها الاستراتيجية مع الولايات المتحدة الامريكية واوربا وبريطانيا وفرنسا وغيرها من الدول الفاعلة، فضلا عن علاقاتها مع دول المنطقة لا سيما بعد ابرام اتفاقيات ابراهيم عام٢٠٢٠.

٤. **كسر عزلتها الجغرافية في الشرق الاوسط:** اذ أدركت (اسرائيل) ومنذ عام ١٩٤٨ انها محاطة بدول معادية لوجودها وامنها القومي، لذا حرصت على الارتقاء بقدراتها الرقمية لتؤمن سهولة التواصل مع كل دول العالم.

٥. **استعراض القوة:** عملت (اسرائيل) على الظهور بوصفها قوة سيبرانية عملاقة بهدف ضمان وسائل فاعلة لاستراتيجيات الردع من خلال العمل لتغطية الضاء السيبراني (الاسرائيلي) بالوسائل التي تمكنها من جمع المعلومات عن القوى الإقليمية المناوئة في منطقة الشرق الاوسط، والاستعداد لخوض حروب افتراضيه معها مستقبلا وهو ما تروج له دوائر المخابرات ووسائل الاعلام (الاسرائيلية)[٩٣].

٦. **توظيف التقنيات السيبرانية في الاستراتيجيات العسكرية (الاسرائيلية):** وهو ما قامت به اسرائيل في حروبها في فلسطين لا سيما في احداث غزه عام ٢٠٢٣، لتامين الحصول على المعلومات للتصدي للقوى المناوئة لها، وشن الحروب الناعمة ضد خصومها في المنطقة.

٧. **جمع المعلومات والتجسس على القوى الاقليمية المناوئة:** من خلال استخدام منظومة الاقمار الاصطناعية التي تملكها لجمع المعلومات الأمنية والاستخباراتية عن الدول المناوئة لها، مثل إيران التي تمثل تهديدا وجوديا للدولة العبرية، وتحقيق اهدافها القومية.

استهداف مجتمعات الدول المناوئة: من خلال توظيف القدرات السيبرانية لنشر الشائعات او توجيه الانتقادات للنظم السياسية المعادية وتحريض الراي العام المحلي فيها ضد الحكومات المناوئة لها، وحشد الراي العام الاقليمي والدولي ضد هذه النظم السياسية، ودعم التوجهات الاقليمية والدولية (لإسرائيل).

اما الوسائل الإيرانية و(الاسرائيلية) في هذه الحرب فتتمثل بتوظيف إيران قدراتها السيبرانية ومنصاتها الالكترونية لتوجيه رسائل الى وسائل التواصل الاجتماعي (الاسرائيلية) لزعزعة الاستقرار في الداخل (الاسرائيلي)، لا سيما بعد تداعيات السابع من اكتوبر عام ٢٠٢٣ [٩٤]. اذ حرصت إيران ومنذ العام ٢٠١٠ بعد استهداف البرنامج النووي الإيراني، والذي اتهمت فيه كلا من الولايات المتحدة الامريكية واسرائيل، والذي تسبب بتعطيل محركات الطرد المركزي في البرنامج النووي الإيراني ولسنوات، حرصت على دعم منتديات القرصنة في الفضاء الافتراضي الإيراني، وتجنيد آخرين ممن ينتمون الى منظومة حلفائها من دون الدول الاقليميين في اليمن وسوريا ولبنان، فضلا عن تشكيل كيانات رقمية تعمل على توجيه التهديدات والتجسس الالكتروني والهجمات الالكترونية والاحتيال السيبراني بوما يساهم في بسط

هيمنتها الاقليمية علي جنوب غربي آسيا[٩٥]. واهم الدول التي استهدفتها إيران تمثلت ب(إسرائيل)، حيث استمرت الهجمات السيبرانية بينهما لترتب مزيد من التصعيد في العلاقات الإيرانية –(الاسرائيلية)لا سيما وإنها ترافقت مع حروب الظل الدائرة في العمق الإيراني من اغتيالات لعلماء نوويين إيرانيين وضربات صاروخية متبادلة. ولعل اهم هجوم وجهت فيه اصابع (اسرائيل) اصابع الاتهام لإيران تمثل بالهجوم على محطات تحليه المياه (الاسرائيلية) عام ٢٠٢٠، وقد ردت عليه (اسرائيل) بهجوم رقمي على حواسيب ميناء بندر عباس الإيراني رتب تعطيل حركة الملاحة في الممرات المائية القريبة منه، ومع نهاية عام ٢٠٢١ اقدمت (اسرائيل) على هجوم على محطات الوقود الإيرانية ادت الى تعطيلها لأكثر من عشرة ايام دفعت إيران الى الهجوم على مشفى اسرائيلي كبير[٩٦]، ما دفع إيران الى استهداف سفينه(اسرائيلية) في بحر العرب بصاروخ[٩٧]، وهو ما دعى عضو الشاباك(الاسرائيلي) (أريك بريبنج) الى القول بإن التوتر الإيراني – (الاسرائيلي) بدء مرحلة جديدة من الحرب بينهما، وقد تؤدي الهجمات السيبرانية الى حرب شاملة، اذ وجدت (اسرائيل) ان هذه الهجمات تمثل خط احمر وتهدد الامن القومي (الاسرائيلي) بشكل مباشر [٩٨]، لا سيما وان إيران تمثل تهديدا وجوديا للدولة العبرية في ضوء منظومة تحالفاتها وبرنامجها النووي فضلا عن توجهات سياستها الخارجية والايدلوجية التي يؤمن بها النظام الإيراني، فضلا عن مساعيه المستمرة للبحث عن دور اقليمي واعد في المنطقة.

واستمرت إيران في التصعيد من الهجمات السيبرانية ضد (اسرائيل) بعد التي قامت بها الاخيرة بالتعاون مع الولايات المتحدة الامريكية عام ٢٠٢٠ علي منشأة نطنز النووية الإيرانية، وهو ما رتب زيادة التصعيد في التوتر الإيراني –(الاسرائيلي) لا سيما وانه ترافق مع حرب الظل التي تدور بينهما من تفجيرات وحوادث اغتيال غامضه لعلماء نوويين إيرانيين، لترد إيران بالمزيد من الهجمات الرقمية المعقدة على سلسلة من الشركات (الاسرائيلية) عام ٢٠٢١، احدها كانت شركة أمنية، مما احرج الحكومة (الاسرائيلية) امام الراي العام المحلي، الامر الذي دفعها للمزيد من الهجمات (الاسرائيلية) ضد الفضاء الافتراضي الإيراني، ما دفع إيران الى توجيه المزيد من الجمات السيبرانية انتقاما لما تواجهه، ما ترتب معه تهديد الامن السيبراني الإيراني، لتسارع إيران الى مهاجمة سلاسل التوريد الاسرائيلية والخدمات اللوجستية[٩٩]. ومع بدء الحرب في غزة عام ٢٠٢٤ صعدت إيران من هجماتها ضد (اسرائيل)، حيث وضفت مواقع التواصل الاجتماعي لأرسال رسائل ضد (اسرائيل) بهدف زعزعة الاستقرار في الداخل (الاسرائيلي) [١٠٠]، كما أنشأت إيران حسابات رقمية بأسماء(اسرائيلية) وهمية تطالب باستقالة (حكومة بنيامين نتنياهو)، وحسابات اخرى انشاتها الاستخبارات الإيرانية في تطبيق التليغرام تهدد (الإسرائيليين) وتصور الاوضاع المأساوية للرهائن في قطاع غزه[١٠١]، مما يؤكد امتلاك كلا الطرفين ادوات ووسائل الحرب السيبرانية التي بإمكانها النيل الامني السيبراني لكلا منهما، وتهديد البنى التحتية كلاهما مع تطور وسائل وادوات الحرب السيبرانية مع تطور ثورة المعلومات والاتصالات، وتزايد ابعاد التنافس الامريكي – الصيني، لا سيما حول الفضاء الافتراضي، وتسارع الخطوات الامريكية لإكمال طريق الازدهار والتنمية

من الهند الى اوربا عبر الشرق الاوسط، واكمال الصين لمبادرة الحزام والطريق، مما يفرض تزايد التنافس بينهما، ذلك التنافس الذي يأخذ ابعادا عده منها التنافس حول الفضاء الافتراضي، مما يرتب انعكاسات مباشرة على ابعاد الصراع الإيراني –(الاسرائيلي)، بما فيه البعد السيبراني والعمليات الخاصة لاتي تقوم بها (اسرائيل) في العمق الإيراني.

ثالثا:– الآفاق المستقبلية للحرب السيبرانية الإيرانية –(الاسرائيلية):– لكي نفهم الافاق والمشاهد المستقبلية لهذه الحرب علينا العودة الى مراحل تاريخية سابقة، حيث ارتكزت (إسرائيل) ومنذ قيامها على مقومين في استراتيجيتها العسكرية والامنية يتمثلان بامتلاك القدرة على توجيه ضربات وقائية وشن حروب استباقية لتعويض افتقارها الى العمق الاستراتيجي والقدرات الديموغرافية من المقاتلين مقارنه بدول جوارها، لتظهر إيران بعد عام ١٩٧٩بوصفها خطر وجوديا (للأمن القومي الاسرائيلي). ومع التطور المتسارع للقدرات السيبرانية اصبحت الهجمات السيبرانية تهدد البنى التحتية للدول والملفات المعنية بأمنها القومي ما ينذر بتحولها الى حروب مباشرة في ضوء تشابك المصالح الدولية وتزايد الاعتمادية المتبادلة التي رتبت تعقد منظومات التحالف الاقليمي والدولي، فضلا عن تزايد الاعتماد على مصادر الطاقة المحدودة اساسا ما يفرض ثلاثة مشاهد مستقبلية محتملة للحرب السيبرانية الإيرانية (الاسرائيلية) كما هي في ادناه:–

المشهد الاول:– تصاعد الهجمات السيبرانية الإيرانية –(الاسرائيلية):– يفترض هذا السيناريو او المشهد ان كلا من إيران و(اسرائيل) لن يقدما على حرب تقليدية مباشرة، فعلى الرغم من ان إيران تظهر عدائها لإسرائيل وبشكل معلن، وبالرغم من تصاعد الهجمات السيبرانية الإيرانية على (اسرائيل) بعد السابع من اكتوبر عام ٢٠٢٣، حيث وجهت إيران اكثر من نصف هجاتها السيبرانية ضد شركات (اسرائيلية)، واستخدمت منصاتها الالكترونية لتوجيه رسائل للداخل (الاسرائيلي) بهدف زعزعه الاستقرار والدعوة الى اقالة رئيس الوزراء (بنيامين نتنياهو) على خلفية احداث غزة، وعلى الرغم من الهجمات الصاروخية المحدودة بين اسرائيل وإيران لعام ٢٠٢٤، الا إن اسرائيل وحتى الان تبدو غير راغبة بالدخول بصدام عسكري مباشر لإدراكها القدرات العسكرية الاسرائيلية، ومنظومة التحالفات الاستراتيجية بين (اسرائيل) والقوى الفاعلة في النظام الدولي واهمهم الولايات المتحدة الامريكية التي تملك العديد من القضايا الخلافية مع إيران، مما يؤكد ان إيران ستعول على الهجمات السيبرانية على (اسرائيل) للتحريض ضد الحكومة الاسرائيلية. وبالمقابل تبدو (اسرائيل) اليوم غير مستعدة للدخول في صدام عسكري مباشر مع إيران، لا سيما بعد الحرب التي استنزفت قدراتها في غزة وجنوب لبنان والهجمات الجوية ضد نظام بشار الاسد في سوريا. وما يعزز هذا السيناريو المؤشرات الاتية:–

اولا:– تزايد الرغبة الإيرانية في الحصول على المعلومات الاستخبارية او التسبب بضرر عبر السيطرة على انظمة التحكم الالية، او تداول معلومات خاطئة بغية التضليل الاعلامي، عبر برامج الفدية الرقمية من اسرائيل، لاسيما وانها تدرك انه لا يمكن التمييز بسهولة بين الهجمات الافتراضية التي تشنها دول ونظيراتها التي تشنها الجماعات الاجرامية، وهو ما رتب تزايد الهجمات الإيرانية السيبرانية ضد

(اسرائيل) لا سيما بعد تداعيات حرب غزة، وهو ما اكده (افرام اتزابا) في تصريح لوكالة فرانس برس، وهو المسؤول عن التعاون الدولي في المديرية الوطنية الإسرائيلية للأمن السيبراني، اذ اكد ان هناك حربا صامته تجري في الفضاء الافتراضي بين (اسرائيل) من جهة وإيران وحلفائها من جهة ثانية بشكل متسارع ومضاعف، حيث تضاعفت الهجمات بعد احداث غزه عام ٢٠٢٣[١٠٢].وذات الامر ينطبق على اسرائيل.

ثانيا:– يدرك كلا من إيران واسرائيل ان من يملك المعلومات يملك القوة والتمكين على الارض في اي صدام عسكري محتمل ومباشر بينهما، فمن يمك المعلومات البيانات الصحيحة سيكون قادرا على حماية جنوده على الارض ويحمي امنه الداخلي في هذا الصراع الدائر بينهما منذ العام ١٩٧٩، والذي شهد مراحل من التصعيد، لا سيما وان إيران حرصت على احاطة (اسرائيل) بمنظومة من الحلفاء الاقليمين من دون الدول للضغط على الامن (الاسرائيلي) اولا، والضغط مناطق نفوذ ومصالح وحلفاء الولايات المتحدة الامريكية، والتنصل من العقوبات التي فرضتها الولايات المتحدة الامريكية عليها، عبر الوصول الى البحر الابيض المتوسط وتصدير الغاز الإيراني مرورا بالأراضي العراقية والسورية. في ما حرصت (اسرائيل) على الارتقاء بقبتها السيبرانية لحمايتها من الهجمات السيبرانية الإيرانية التي تضاعفت بعد تداعات غزه عام ٢٠٢٣، كما ان الهجمات السيبرانية اخذت تستهدف الاستيلاء على معلومات.

ثالثا:– يدرك كلا من إيران و(اسرائيل) اهمية الارتقاء بقدراتها السيبرانية لضمان دور اقليمي واعد في المنطقة، لا سيما مع تسارع خطوات الدول العربية في المنطقة واهمها المملكة العربية السعودية للارتقاء بقدراتها السيبرانية من خلال تطوير البنية التحتية للاتصالات وتكنلوجيا المعلومات والاطار التشريعي لقدراتها السيبرانية مما يمهد الطريق لبناء قوة سيبرانية متميزة لا سيما بعد تعرضها لهجمات سيبرانية إيرانية على منشآت ارامكو النفطية السعودية وقطاع الغاز الطبيعي في قطر. فضلا عن ذلك سارعت دول مجلس التعاون الخليجي الى تنسيق التعاون في ما بينها في الامن السيبراني وتكنلوجيا الاتصالات بعد الهجمات التي يعتقد انها من إيران، حيث سارعت الى بناء اطار تعاوني للتنسيق بالتصدي للهجمات السيبرانية التي تتعرض لها [١٠٣]. وبالمقابل، تم تشكيل تحالف إلكتروني آخر في المنطقة بين إيران وروسيا. ففي ٢٦ يناير ٢٠٢١، وقعت إيران وروسيا اتفاقية تعاون مشترك في هذا المجال الأمن السيبراني، بما في ذلك نقل التكنولوجيا والتدريب وتبادل المعلومات، والتعاون الثنائي. وبموجب هذه الاتفاقية زودت روسيا إيران بأنظمة الدفاع السيبراني، وبما يجعل الهجمات السيبرانية المحتملة ضد الاهداف السيبرانية الإيرانية أكثر صعوبة وتكلفه مستقبلا، كما سارعت إيران الى توفير التقنيات السيبرانية الى حلفائها في جنوب لبنان وسوريا واليمن لتنسيق الهجمات السيبرانية ضد (اسرائيل)، مما يرجح الرغبة الإيرانية باستمرار الهجمات السيبرانية ضد (اسرائيل) ومصالحها في المنطقة دون الدخول في اشتباك عسكري مباشر قد يكون غير محسوب النتائج والاثار.

رابعا:– صعوبة تحديد الطرف المهاجم يساهم في ضبط مستويات الصراع في الفضاء الافتراضي، وبما يحول دون الرد بهجمات افتراضية انتقامية مباشرة، لا سيما وان بعض الهجمات تضمن توجيه فايروسات تعمل على تدمير نفسها ذاتيا بعد الهجوم كما حصل مع الهجوم على البرنامج النووي الإيراني،

فعلى الرغم من الاتهامات الإيرانية للولايات المتحدة الامريكية و(اسرائيل) بهذا الهجوم الا انها لم تتمكن حتى بعد من تحليل الهجوم من تثبيت الاتهام ضد خصومها، لا سيما وان معظم الدول تحاول ضبط هجماتها السيبرانية بمستوى معين يحول دون تحولها الى حروب كبرى قد تؤدي الى اندلاع.

خامسا:- لا يمكن تطبيق استراتيجيات الردع الافتراضي بسبب صعوبة تحديد الطرف الهاجم مما يرجح صعوبة التصعيد بناءا على قراءات خاطئة لما قد يرتب البدء هجمات سيبرانية انتقامية تحمل في طياتها فرصا لاندلاع حروب سيبرانية.

سادسا:- ولا ننسى هنا الدور الامريكي في منع التصعيد بين (اسرائيل) وإيران في نيسان عام ٢٠٢٤ وتحوله الى حرب مفتوحة في الشرق الاوسط، حيث مارست ادارة الرئيس الامريكي (جو بايدن) ضغوط كبيرة على (اسرائيل) لمنعها من الرد العنيف على إيران بعد هجماتها الصاروخية، وبالفعل كان الرد الاسرائيلي على إيران محدودا في شهر نيسان من عام ٢٠٢٤، كما حرصت كذلك الولايات المتحدة بالتعاون مع حلفائها على تحجيم واحتواء الضربة الإيرانية على اسرائيل[١٠٤]، اذ تدرك الولايات المتحدة الامريكية ان اي تصعيد سيرتب تهديد مباشر لمصالحها في الشرق الاوسط.

سابعا:- وفي العموم اكدت مراحل التصعيد الإيراني – الاسرائيلي منذ استهداف القنصلية الإيرانية في سوريا في نسان من عام ٢٠٢٤، على ادراك إيراني – (اسرائيلي) على تجنب الاصطدام العسكري المباشر وتجنب الانجرار لحرب شاملة بينهما، في ضوء الادراك الإيراني باختلال التوازن العسكري في المنطقة لصالح (اسرائيل) فضلا عن الدعم الامريكي اللامحدود (لإسرائيل) في الوقت الذي تعاني هي فيه من العقوبات الاقتصادية عليها والتي فرضتها الولايات المتحدة الامريكية بعد انسحاب الرئيس الامريكي السابق (دونالد ترامب) من الاتفاق النووي عام ٢٠١٨.

المشهد الثاني:- تحول الحرب السيبرانية الإيرانية –(الاسرائيلية) الى صدام عسكري مباشر:- بعد تزايد التنافس الامريكي –الصيني الاقتصادي من جهة واندلاع الحرب الروسية الاوكرانية وتداعيات غزة عام ٢٠٢٣ من جهة ثالثة، امكن القول انه لا يمكن الفصل بين الهجمات السيبرانية بين إيران و(اسرائيل) وبين المتغيرات الاقليمية والدولية التي تشهدها منطقة شرق المتوسط، لا سيما وانها تتمحور حول المصالح الاقليمية والدولية للقوى الفاعلة في المنطقة مثل تجارة البترول والغاز الطبيعي فضلا عن تزايد التنافس حول الاطلالات البحرية في المنطقة، فضلا عن تزايد التنافس بين الصين والولايات المتحدة الامريكية حول العديد من القضايا الخلافية ويتمثل اهمها مباردة الحزام والطريق الصينية التي تمر عبر منطقة شرق المتوسط من جهة، وطريق التنمية والازدهار الذي تدعمه الولايات المتحدة الامريكية والمار من الهند عبر المحيط الهندي الى الامارات العربية المتحدة ومنها الى شرق المتوسط عبر الاراضي السعودية والاردنية و(الاسرائيلية)، وعليه يفترض هذا السيناريو ان قد تؤدي الهجمات السيبرانية المتبادلة بين إيران و(اسرائيل) الى تطورها الى حرب سيبرانية استراتيجية تقوض البنى التحتية لكلا منهما مما يؤدي الى الكثير من القتلى واستهداف المؤسسات المرتبطة بالأمن القومي لكلاهما وما يعزز هذا المشهد المؤشرات الاتية:-

اولا:– تصريحات عضو الشاباك السابق (اريك بريبنج) يقول بعد موجات الهجمات السيبرانية الإيرانية والتي تجاوزت فيها الخطوط الحمراء تعلن عن بدء حقبة امنية جديدة، وقد تتحول هذه الهجمات الى حرب عالمية خطيرة على البنى التحتية المستهدفة، بل ان (عاموس يدلين)الرئيس السابق لشعبة الاستخبارات العسكرية يؤكد ان الحروب السيبرانية بين إيران و(اسرائيل) اصبحت تمثل البعد الرابع اضيف الى الحروب البرية والجوية والبحرية بينهما منذ العام ١٩٧٩[١٠٥].

ثانيا:– اقترنت هذه الهجمات بالرد الانتقامي (الاسرائيلي) على الموانئ الإيرانية، مما يرتب تهديد الملاحة في مضيق هرمز، فضلا عن ذلك فان الهجمات الإيرانية السيبرانية لم تقتصر على (اسرائيل) بل استهدفت المصالح الامريكية في الشرق الاوسط، مما يرتب تزايد التصعيد السيبراني واحتمالية تحوله الى حرب حقيقية.

ثالثا:– ما يعزز هذا السيناريو هو وصول الرئيس (دونالد ترامب) الى البيت الابيض، مع رغبته بإزاحة النفوذ الإيراني من منطقة شرق المتوسط فضلا عن عدم العودة الى الملف النووي الإيراني بعد انسحابه من اتفاق فينا حول البرنامج النووي الإيراني عام ٢٠١٥.

رابعا:– تزايد الرغبات الإيرانية في الانتقام من الولايات المتحدة الامريكية بعد انسحاب الاخيرة من الاتفاق النووي وتزيد العقوبات الاقتصادية التي فرضتها الاخيرة على إيران، فضلا عن الدعم الامريكي اللامحدود (لإسرائيل) في ضربها لمنظمة الحلفاء الاقليمين لإيران بعد احداث غزة بدأ من ضرب قيادات واستهداف حزب الله التي كانت تهدد الشمال (الاسرائيلي) وصولا الى اسقطا نظام بشار الاسد مما يرتب خسارة إيران لمنظمة الحلفاء الذين كانت تروم فيها محاصرة (اسرائيل) للضغط على الولايات المتحدة الامريكية في للعودة الى الاتفاق النووي، مما يرجح تزايد الهجمات السيبرانية الإيرانية على (اسرائيل) والولايات المتحدة واحتمالية تحولها الى حرب تقليدية مباشرة بين إيران وحلفائها من جهة و(اسرائيل) وحلفائها من جهة ثانية.

خامسا –الادراك الصيني لما تتمتع به (اسرائيل) من موقع جيوبولتيكي يجعلها تشرف على المنطقة الوسطي بين قارات آسيا وافريقيا واوربا اولا، فضلا عن انها ترى إن الاستثمار الصيني في (اسرائيل) لن يتعرض لمخاطر كبرى كما هو الحال في الدول الاخرى التي تستثمر فيها الصين ثانيا، فضلا عن ذلك ترى الصين ان (اسرائيل) تعد منفذا مهما للحصول على التكنلوجيا الغربية والامريكية، نظرا للشراكات الاستراتيجية التي تربط الاخيرة مع الولايات المتحدة الامريكية والدول الغربية ثالثا، واهم من هذا وذاك فأن الصين تطمح للوصل الى احتياطات الغاز الطبيعي المكتشفة على السواحل (الاسرائيلية) رابعا [١٠٦]، الامر يرجح المساعي الصينية لمد الاستثمارات الصينية الى اسرائيل في اطار مبادرة الحزام والطريق الذي يزيد من التنافس الامريكي – الصيني على (اسرائيل) واطلالتها على سواحل المتوسط في ضوء المساعي الامريكي لإكمال مبادرة طرق الازدهار والتنمية الامريكية التي تمتد من الهند الى اسرائيل عبر المحيط الهندي والاراضي العربية وصولا الى اطلاله (إسرائيل) على المتوسط وصولا الى اوربا، مما يرجح دخول اطراف دولية في الصراع الإيراني (الاسرائيلي) قد يتحول في اية لحظة الى حرب تقليدية مباشرة.

سادسا:- تخوض كلا من إيران و(اسرائيل) منذ عقود طويله حروب ظل تم اجتياز الخطوط الحمراء فيها لمرات عديدة وكادت تسبب حروبا مباشرة، لكن الحرب في غزة عام ٢٠٢٣، حرص فيها الطرفين على الارتقاء بقدراتها العسكرية لا سيما السيبرانية منها، فضلا عن امتلاك إيران صواريخ بالستية شكلت اهم مصادر التهديد لإسرائيل، لا سيما وان بإمكانها الوصول الى قاعدة نفاتيم (الاسرائيلية) التي تعد الحظيرة الرئيسة لمقاتلات إف-٣٥ الإسرائيلية، وتعتقد إيران أن الهجوم(الاسرائيلي) على القنصلية الإيرانية في سوريا في نسان عام ٢٠٢٤ انطلق منها[١٠٧]، وعليه فأن اي سوء تقدير للموقف قد يؤدي الى اندلاع حرب شامله تشعل المنطقة برمتها.

واخيرا وليس آخرا ترجح الباحثة السيناريو الثاني، فعلى الرغم من الضغوط الامريكية لمنع اسرائيل من التصعيد العسكري المباشر ضد إيران، الا إن وصول الرئيس (دونالد ترامب) للبيت الابيض وهيمنه صقور المحافظين من الجمهوريين على الكونغرس الامريكي بشقية النواب والشيوخ يزيد من التوتر والتصعيد بين إيران من جهة والولايات المتحدة الامريكية وحلفائها واهمم (اسرائيل) من جهة ثانية، لاسيما وان الرئيس الامريكي يعلن مرارا وتكرارا عن رغبته بعدم امتلاك إيران طاقة نووية والعودة الى الاتفاق النووي، فضلا عن ذلك فإن إيران لم تتواني عن استخدام قدراتها السيبرانية لاستهداف المصالح الامريكية في المنطقة، بالاضافة الى تماهيها مع المصالح الروسية والصينية ضد النفوذ الامريكي في المنطقة، فضلا عن المساعي الإيرانية لجمع معلومات استخبارية عن المصالح والقواعد الامريكية وقيادات عسكرية في حلف شمال الاطلسي وقادة أمريكان و(اسرائيليون)، فضلا عن استهداف إيران لشركات امريكية لسرقة ابحاثها[١٠٨]، ولما كانت الاستراتيجية الإيرانية السيبرانية تتكيف مع مصالحها الجيوسياسية فأنها تنشط بعد كل حزمة من العقوبات الامريكية تفرض عليها فانه من المتوقع انها ستعمل على استهداف المصالح الامريكية ومنظومة حلفاء الولايات المتحدة في المنطقة واهمهم (اسرائيل) سيبرانيا وقد تتحول هذه الحرب السيبرانية من هجمات سيبرانية محدودة الى حرب سيبرانية استراتيجية تستهدف المنشآت الحيوية في كلا من إيران و(اسرائيل) بعد العقوبات الاقتصادية القصوى التي يفرضها الرئيس الامريكي(دونالد ترامب) عليها اخيرا، اذا انها ادت الى انهيار كبير في العملة الإيرانية لم تشهده منذ عام ١٩٧٩.

الخاتمة والاستنتاجات:

لا شك ان الحروب السيبرانية اضافت بعدا خامسا لأبعاد الحروب التقليدية المتمثلة بالأبعاد البرية والبحرية والجوية والفضائية تمثل بالبعد الافتراضي الذي أصبح أحد اهم ساحات التنافس الاستراتيجي بين الدول، لا سيما وانه حتى الان لم يتم الاتفاق على قواعد قانونية تمنع الهجمات السيبرانية التي من شأنها تهديد السلم والامن الدوليين، ولم تستطع الدول على الرغم من امتلاكها قدرات تقنية فائقة لم تستطع صياغة استراتيجيات ردع سيبراني فاعلة بإمكانها ضمان امنها القومي وسيادتها واستقرارها. وعليه توصل البحث الى الاستنتاجات الاتية:-

اولا:– مع التطور المتسارع للثورة الرقمية في وسائل الاتصال والمواصلات مع بدايات القرن العشرين باتت الدول تعاني من انكشاف استراتيجي هائل جعلها عرضه للهجمات السيبرانية والتهديدات السيبرانية الاخرى مثل التجسس الالكتروني والإرهاب الرقمي وغيرها من التحديات التي تهدد امنها القومي واستقرارها، بعد ان ظهر الفضاء الافتراضي بوصفه مجالا جديدا للتفاعل الدولي ببعديه التعاون والصراع.

ثانيا:– مع تنامي قدرات الدول على توظيف التطور التكنولوجي في المجال السياسي زادت التهديدات السيبرانية، مما أدى إلى ظهور مفهوم جديد تمثل الأمن السيبراني، والذى تحاول الدول من خلاله الحد من المخاطر والتهديدات فى الفضاء السيبراني.

ثالثا:– مع تنامي استراتيجيات الحروب السيبرانية لم تعد نتائج الحروب تعتمد على ما تملكه الدول من جيوش جراره وطائرات ودبابات وسفن حربية بقدر ما تعتمد على مهندسي حواسيب تعمل على استهداف الاصول الوطنية والملفات المعنية بالأمن القومي للخصوم من الدول، بعد ان تحولت التكنلوجيا الى قوة تدميرية هائلة غير مرئية.

رابعا:– وفي الوقت الذي تعرف فيه الحرب الالكترونية بوصفها استخدام حزم الطيف الكهرومغناطيسي لتشويش أو تعطيل الاتصالات وأنظمة التحكّم والتوجيه الخاصة بقطعات جيش العدو لتعطيل نظام اتصالاته ودحره في المعارك وعبر الحواسيب الالكترونية، فإن الحرب السيبرانية تعرف بوصفها استهداف الشبكات الحاسوبية والأنظمة الرقمية للدولة الخصم والتي تشمل منشآت حيوية معنية بأمن الدولة واستقرارها ورفاهيتها وعبر الهجمات الافتراضية في الفضاء الافتراضي، وهذه الهجمات قد تشمل سرقة البيانات الحساسة وتعطيل البنية التحتية الرقمية، مثل محطات الطاقة أو شبكات الاتصالات.

خامسا:– شهدت العلاقات الإيرانية –(الاسرائيلية) موجات من التوتر والتصعيد المتبادل منذ عام ١٩٧٩ بعد ان ظهرت إيران بوصفها تهديد وجودي للدولة العبرية، ومع تنامي ثورة المعلومات والاتصالات الرقمية تصاعدت الهجمات السيبرانية بين الطرفين في الوقت الذي اتجه كلا منهما للارتقاء بقدراته الافتراضية لفرض جزءاً من نفوذه وهيمنته على منطقة شرق المتوسط.

سادسا:– اشتركت (اسرائيل) مع الولايات المتحدة الأمريكية في شن هجمات سيبرانية بالغة التعقيد على أنظمة الكمبيوتر التي تشغل منشآت تخصيب اليورانيوم النووية في إيران في مفاعل نطنز، مما رتب تعطيل أجهزة الطرد الإيرانية، حيث استطاعت هذه الهجمات في تعطيل نحو ١٠٠ جهاز طرد في منشأه نطنز بجعلها تدور بسرعة عالية تسبب تلفها، فكان هذا أول هجوم كبير يُستخدم فيه سلاح إلكتروني لإنزال دمار مادي عام ٢٠١١، على اثره انشأت إيران المجلس الأعلى للامن السيبرانية يتولى مهمه صياغة الاستراتيجية السيبرانية الإيرانية.

سابعا:– تعرضت إيران لهجوم سيبرانيً كبير آخر في ٨ شباط عام ٢٠٢٠م، رتب انقطاعاً جزئياً في خدمة الإنترنت توقف على اثره (٢٥%) من خدمات الانترنيت في إيران، وخللاً في نظم الاتصالات في الهواتف الأرضية وبعض شركات الهواتف المحمولة، والبنية التحتية لنظم الاتصالات الإيرانية، اتهمت على اثره إيران كلا من (اسرائيل) والولايات المتحدة الامريكية بهذا الهجوم الافتراضي.

ثامنا:- تزايدت الهجمات السيرانية بين إيران و(اسرائيل) بعد تداعيات غزة عام ٢٠٢٣، لاسيما وان (اسرائيل) بدأت بالإعلان عن مشروع شرق اوسط جديد لا يتواجد فيه حلفاء إيران مع الاعلان عن طريق الازدهار والتنمية الذي يبتدأ في الهند وينتهي في الشواطئ (الاسرائيلية) وصولا الى اوربا مما يجعله يتقاطع مع مبادرة الحزام والطريق الصينية الامر الذي يرتب دخول اطراف دولية جديدة في الإيراني – (الاسرائيلي)، مع زيادة التنافس على مصادر الطاقة ومناطق النفوذ بين القوى الكبرى في النظام الدولي.

تاسعا:- تشير الادلة والقرائن على احتمالات تحول الحرب السيبرانية الإيرانية –(الاسرائيلية) الى حرب سيبرانية استراتيجية يتم استهداف البنى التحتية لكل منهما ترتب اندلاع حرب تقليدية بين الطرفين، لا سيما وان هناك الكثير من القضايا الخلافية بين إيران من جهة واهم حلفاء (اسرائيل) من جهة ثانية ممثلا بالولايات المتحدة الامريكية، خاصة وان (اسرائيل) ربطت بين الارتقاء بقدرات الافتراضية بالتهديد الوجودي الذي تمثله إيران في ضوء التهديدات العلنية الإيرانية لها، فضلا عن الربط (الاسرائيلي) بين المساعي (الاسرائيلية)وبين الابعاد الايدلوجية، حيث تسارع (اسرائيل) للارتقاء بقدراتها السيبرانية بسبب وجود تهديد اسلامي وعربي لها، مما رتب نجاح (اسرائيل) في توظيف قدراتها السيبرانية في سياستها الخارجية مع محيطها العربي والاسلامي والرافض لوجودها.

عاشر:- لا شك ان اهم سمه تميزت بها الحرب السيبرانية ممثلة بسهوله التنصل من الهجمات السيبرانية، فضلا عن عدم وجود روادع قانونية تحول دون تنفيذها يسهل على كلا من إيران و(اسرائيل) من شن العديد من الهجمات السيبرانية واستهداف البنى التحتية مما يزيد من مستويات التصعيد الإيراني – (الاسرائيلي).

احد عشر:- واخيرا وليس آخر فإن الصراع السيبراني بين إيران وإسرائيل سيزداد حدة في الايام القادمة بسبب التفوق السيبراني الهائل والإمكانيات التي تؤهل كل من الدولتين لخوض هجمات سيبرانية انتقامية تجاه الآخر، مما يدفع نحو حرب تقليدية واسعة النطاق والاهداف وربما تكون حرب وجودية بالنسبة لكلاهما في ضوء منظومة التحالفات التي يمتلكانها والقدرات الهائلة لكلا منهما. وعليه توصي الباحثة بما يأتي:-

١. العمل على انشاء جدار ناري يمكن العراق من امتلاك حدود سيبرانية آمنه.

٢. العمل على استثمار الموارد الوطنية في الارتقاء بالقدرات العراقية ووضع استراتيجيات الامن السيبراني بأيادي عراقية ادارة واشرافا ومتابعه.

٣. تأمين وسائل وتقنيات الردع الافتراضي بما يحقق التكافؤ مع دول الجوار الاقليمي.

٤. على العراق عدم الانخراط في صراع المحاور الاقليمية والدولية، بل عليه ان يكون عنصر توازن واستقرار اقليمي في المنطقة.

٥. على العراق رعاية الكفاءات والمواهب العراقية لمواكبة دائرة الصناعة الالكترونية وبقدرات وطنية لتحقيق السرية التامة في تتملكه المؤسسات الامنية العراقية من اجهزة وتقنيات تستخدم في استراتيجيات الردع السيبراني.

٦. على العراق توظيف وكالات التنشئة الاجتماعية بداءا من الاسرة والمدرسة والجامعة للارتقاء بالوعي الجمعي حول خطورة التوظيف الخاطئ للتكنلوجيا ووسائل التواصل الاجتماعي، لتوظيفها بما يعزز الوحدة الوطنية والامن السيبراني العراقي.

٧. على الحكومة العراقية الارتقاء بإداء الاجهزة الامنية لا سيما المعنية منها بالأمن السيبراني عبر ادخالهم في دورات تأهليه داخل وخارج العراق.

٨. على العراق استثمار منظومة التحالفات الدولية لتعزيز امنه السيبراني عبر ابرام الاتفاقيات التي تعزز متابعة الجريمة المنظمة والارهاب الرقميين واي تهيدي افتراضي محتمل.

الهوامش

(١) تغريد صفاء ولبنى خميس، اثر السيبرانية في تطور القوة، العراق، مجلة حمورابي للدراسات، العدد ٣٣– ٣٤، السنة الثامنة، ٢٠٢٠، ص ١٤٧.

(٢) سماح عبد الصبور، القوة السيبرانية في العلاقات الدولية: دراسة في الحروب السيبرانية بالتطبيق على عام ٢٠٢٠، شبكة المعلومات الدولية، آخر دخول ٢٠٢٥/١/٥:- https://hadaracenter.com.

(3) Marco Benatar, The Use of Cyber Force: Need for Legal Justification?, Goettingen Journal of International Law 1 (2009) 3, p:379.

(٤) سماح عبد الصبور، القوة السيبرانية في العلاقات الدولية، https://hadaracenter.com.

(5) 377 Marco Benatar, The Use of Cyber Force, p:

(٦) بزير آمال، الاستجابة الدولية للتهديدات السيبرانية، الجزائر، جامعة محمد الصديق بن يحيى:قطب تاسوست: جيجل، كلية الحقوق ولعلوم السياسية، قسم العلوم السياسية، رسالة ماجستير، ٢٠٢٢، ص أ، وص ١١.

(٧) منى عبد الله السمحان، متطلبات تحقيق الامن السيبراني لانظمة المعلومات الادارية بجامعة الملك سعود، مصر، جامعة المنصورة، كلية التربية، مجلة كلية التربية، العدد ١١١، يوليو ٢٠٢٠، ص ٩.

(8) Dr. Stuart H. STARR1, Towards an Evolving Theory of Cyber power, a Center for Technology and National Security Policy (CTNSP) National Defense University (NDU), the U.S. Government, https://ccdcoe.org/uploads/2018/10/02_STARR_Cyberpower.pdf..

(٩) بزير آمال، الاستجابة الدولية للتهديدات، مصدر سبق ذكره، ص ١١–ص١٢.

(١٠) علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، الجزائر، جامعة الوادي، مجلد ١، العدد ٣، ٢٠١٩، ص ٨٨ –٨٩.

(١١) عمران طه عبد الرحمن عمران، الفضاء السيبراني إطار مفاهيمي في ضوء نظريات العلاقات الدولية، المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٩: https://www.democraticac.de/?p=96508.

(١٢) المصدر نفسه.

(١٣) عمران طه عبد الرحمن عمران، الفضاء السيبراني إطار مفاهيمي في ضوء نظريات العلاقات الدولية، المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٩: https://www.democraticac.de/?p=96508

(١٤) نور الدين حامد علي إبراهيم، الفضاء السيبراني: المفاهيم والابعاد، المجلة العلمية للبحوث والدراسات السيبرانية، مصر، جامعة حلوان، كلية التجارة وتجارة الاعمال، المجلد ٣٨، العدد ٢، ٢٠٢٤، ص ٧٢٦.

(١٥) عمران طه عبد الرحمن عمران، الفضاء السيبراني إطار مفاهيمي في ضوء نظريات العلاقات الدولية، المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٩ https://www.democraticac.de/?p=96508.

(١٦) نور الدين حامد علي إبراهيم، الفضاء السيبراني: المفاهيم والابعاد، المجلة العلمية للبحوث والدراسات السيبرانية، مصر، جامعة حلوان، كلية التجارة وتجارة الاعمال، المجلد ٣٨، العدد ٢، ٢٠٢٤، ص ٧٢٢.

(١٧) علاء الدين فرحات، الفضاء السيبراني، مصدر سبق ذكره، ص ٩١.

(١٨) اسامة سالم محمد الفرجاني، العقوبات السيبرانية ومشروعيتها في ضوء قواعد القانون الدولي، مصر، جامعة دمياط، كلية القانون، مجلة حقوق دمياط للدراسات القانونية والاقتصادية، العدد العاشر، يوليو ٢٠٢٤، ص٥٩.

(١٩) عمران طه عبد الرحمن عمران، الفضاء السيبراني إطار مفاهيمي في ضوء نظريات العلاقات الدولية، المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٩: https://www.democraticac.de/?p=96508.

(20) Dr. Stuart H. STARR1, Towards an Evolving Theory of Cyber power,https://ccdcoe.org/uploads/2018/10/02_STARR_Cyberpower.pdf.

(21) Dr. Stuart H. STARR1, Towards an Evolving Theory of Cyber power,https://ccdcoe.org/uploads/2018/10/02_STARR_Cyberpower.pdf.

(٢٢) ياسين محمد، الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية، ليبيا، مجلة شمال افريقيا للنشر العلمي، المجلد الرابع، العدد ١، ٢٠٢٣، ص١٥٦.

(٢٣) فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى: دراسة حالة الصين، الجزائر، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، رسالة ماجستير، ٢٠١٧/٢٠١٨، ص٢٣.

(٢٤) احمد محمود صفي الدين، رؤية تحليلية للثورة السيبرانية، مصر، جامعة بور سعيد، كلية التجارة، مجلة البحوث المالية والتجارية، المجلد ٢٥، العدد٢، ٢٠٢٤، ص ١٢٤.

(٢٥) فريدة طاجين، تاثير القوة السيبرانية، مصدر سبق ذكره، ص ٢٢، ص٢٣، ص٢٤، ص٢٥.

What are Cyber-Threats, Cyber-Attacks and how to defend our Systems, See discussions, stats, and author profiles for this publication at:.https://www.researchgate.net/publication/349043516

(٢٦) منى عبد الله السمحان، متطلبات تحقيق الامن السيبراني، مصدر سبق ذكره، ص ٩ – ص١٠.

(٢٧) فاطمة علي ابراهيم ورحاب يوسف ووليد، الامن السيبراني والرقمية، مصر، المجلة المصرية لعلوم المعلومات، المجلد ٩، العدد ٢، اكتوبر ٢٠٢٢، عيد ص٣٩٨.

(٢٨) شويرب جيلالي ودمراد فائزة، مفهوم الحروب السيبرانية والامن السيبراني، الجزائر، جامعة محمد حيدر، مجلة الحقوق، المجلد ١١، العدد١، ص١٦٦– ص١٦٧.

(٢٩) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المملكة العربية السعودية، جدة المجلة الالكترونية الشاملة متعددة التخصصات، العدد ٢٤، ٢٠٢٠، ص ٨– ص٩.

(٣٠) المصدر نفسه، ص ١١– ص١٣.

(٣١) فاطمة على ابراهيم ورحاب يوسف ووليد عيد، الامن السيبراني، مصدر سبق ذكره، ص ٤٠١.

(32) Ahmed Al-Zaidy, Research Proposal Paper: Final Term Project Paper

What are Cyber-Threats, Cyber-Attacks and how to defend our Systems, See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/349043516

[٣٣] ايهاب خليفه، اليات تحقق الردع في الفضاء السيبراني، المركز المصري للفكروالدراسات الاستراتيجية، ص٥٣، شبكة المعلومات الدولية، أخر ظهور ٢٠٢٥/١/٩: https://www.researchgate.net/publication/366965740

[٣٤] رغدة البهي، الردع السيبراني المفهوم والاشكاليات، القاهرة، المركز المصري للفكر والدراسات الاستراتيجية، شبكة المعلومات الدولية، اخر ظهور ٢٠٢٥/١/١٤: https://ecss.com.eg/6203.

[٣٥] ايهاب خليفه، اليات تحقق الردع في الفضاء السيبراني، المركز المصري للفكر والدراسات الاستراتيجية، ص٥٣، شبكة المعلومات الدولية، أخر ظهور ٢٠٢٥/١/٩: https://www.researchgate.net/publication/366965740

[٣٦] رغدة البهي: الردع السيبراني، مصدر سبق ذكره: https://ecss.com.eg/6203.

[٣٧] حسين قوادرة، الردع السيبراني: بين النظرية والتطبيق، الجزائر، المجلة الجزائرية للامن والتنمية، المجلد ٩، العدد١٦، ٢٠٢٠، ص ٥١٩.

[٣٨] رغدة البهي، الردع السيبراني المفهوم والاشكاليات، القاهرة، المركز المصري للفكر والدراسات الاستراتيجية، شبكة المعلومات الدولية، اخر ظهور ٢٠٢٥/١/١٤:- https://ecss.com.eg/6203/

[٣٩] حسين قوادرة، الردع السيبراني: بين النظرية والتطبيق، مصدر سبق ذكره، ص ٥٢١، ص٥٢٢، ص٥٢٣.

[٤٠] اسامة سالم محمد الفرجاني، العقوبات السيبرانية، مصدر سبق ذكره، ص٣٠، ص٣١، ص٣٢.

[٤١] نبيلة عبد الفتاح قشطي، الحرب السيبرانية وسبل مواجهتها، الجزائر، مجلة شؤون استراتيجية، العدد ١٧، مارس ٢٠٢٤، ص ٤٨٣.

[٤٢] علاء الدين فرحات، الحرب السيبرانية ومستقبل الامن العالمي، الجزائر، مجلة الناقد للدراسات السياسية، المجلد ٦، العدد ٢، ٢٠٢٢، ص ٦٨٠.

[٤٣] شويرب جيلالي ومارد فائزة، مفهوم الحروب السيبرانية، مصدر سبق ذكره، ص ١٥٧.

[٤٤] علاء الدين فرحات، الحرب السيبرانية، مصدر سبق ذكره، ص ٦٨٣.

(٤٨) مايسة السروي، حروب عصر الرقمنة. كيف يمكن أن تصيب العالم بالشلل؟، شبكة المعلومات الدولية، نشر ٢٠٢٤/٩/٢٠، آخر ظهور ٢٠٢٥/٢/٧:- https://www.alarabiya.net/science/2024/09/20..

[٤٥] جيهان احمد عبد العال وسلوى السعيد ورشا عطوة عبد الحكيم، الحروب السيبرانية: دراسة في المفهوم والنشأة ومعدلات النجاح، مصر، جامعة قناة السويس، كلية التجارة، المجلة العلمية للدراسات التجارية والبيئية، المجلد الثالث عشر، العدد الثاني، ٢٠٢٢، ص٢٩١.

[٤٦] شويرب جيلالي ودمراد فائزة، مفهوم الحروب السيبرانية والامن السيبراني، مجلة الحقوق والحريات، المجلد ١١، العدد١، ص١٦٠.

[٤٧] جيهان احمد عبد العال وسلوى السعيد ورشا عطوة عبد الحكيم، الحروب السيبرانية، مصدر سبق ذكره، ص ٣٠٢.

[٤٨] مايسة السروي، حروب عصر الرقمنة. كيف يمكن أن تصيب العالم بالشلل؟، شبكة المعلومات الدولية، نشر ٢٠٢٤/٩/٢٠، آخر ظهور ٢٠٢٥/٢/٧:-. https://www.alarabiya.net/science/2024/09/20..

[٤٩] انيس عبد الوهاب، القوة السيبرانية الايرانية وأثرها على الاستقرار الاقليمي، الجزائر، مجلة السياسة العالمية، المجلد ٦، العدد٢، ٢٠٢٢، ص ٧٣٤.

[٥٠] احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران و(إسرائيل)، الرياض، مجلة الدراسات الايرانية، معهد الدراسات الايرانية (رصانه)، العدد الثاني عشر، ٢٠٢٠، ص ٦٨.

[٥١] مركز الملك فيصل للدراسات والبحوث الاسلامية، قدرات القرصنة السيبرانية الايرانية، تقرير خاص، يناير ٢٠٢٠، ص٥.

[٥٢] انيس عبد الوهاب بن أحسن، القوة السيبرانية، مصدر سبق ذكره ص٧٣٥.

(٥٣) احمد بن علي الميموني، الجبهة النشطة، مصدر سبق ذكره، ص ٦٨.

(٥٤) انيس عبد الوهاب بن أحسن، القوة السيبرانية، ص ٧٣٥.

(٥٥) المصدر نفسه، ص ٧٣٦.

(٥٦) المصدر نفسه، ص ٧٣٧.

(٥٧) احمد بن علي الميموني، الجبهة النشطة، مصدر سبق ذكره، ص ٧١.

(٥٨) أنيس عبد الوهاب بن احسن، القوة السيبرانية، مصدر سبق ذكره، ص ص٧٣٧- ص٧٣٨.

(٥٩) احمد بن علي الميموني، الجبهة النشطة، مصدر سبق ذكره، ص ٧٢.

(٦٠) حسين قوادرة، الردع السيبراني: بين النظرية والتطبيق، الجزائر، المجلة الجزائرية للامن والتنمية، المجلد ٩، العدد١٦، ٢٠٢٠، ص ٥١٩.

(٦١) المصدر نفسه، ص ٥١٩.

(٦٢) تينا الجلاد، الدبلوماسية السيبرانية الالكترونية ل(إسرائيل)، مجلة شؤون فلسطينية، مركز الابحاث: منظمة التحرير الفلسطينية، العدد ٢٨٥، ٢٠٢١، ص ٢٤-ص ٣١.

(٦٣) المصدر نفسه، ص ٣٢.

(٦٤) المصدر نفسه ص ٣٣.

(٦٥) صينية قحايرية ومنية قحايرة، الاستراتيجية الامنية (الإسرائيلية) في مواجهة التهديدات السيبرانية، الجزائر، جامعة التبسي – تبسة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، رسالة ماجستير، ٢٠١٨، ص ٥٨.

(٦٦) المصدر نفسه، ص ٥٩- ص٦٠.

(٦٧) قناة TRT العربية، القمر الصناعي الإسرائيلي "أفق ١٦" ما علاقته بالتجسس واستهداف إيران؟، شبكة المعلومات الدولية آخر دخول ٢٠٢٥/١/٢٧: https://www.trtarabi.com/now

(٦٨) محمود محارب، (إسرائيل) والحرب الالكترونية: قراءة في كتاب حرب في الفضاء السيبراني اتجاهات وتأثيرات على (إسرائيل)، الدوحة، المركز العربي للأبحاث ودراسة السياسات، ٢٠١١، ص ٥.

(٦٩) صينية قحايرية ومنية قحايرة، الاستراتيجية الامنية، مصدر سبق ذكره، ص ٦٢.

(٧٠) المصدر نفسه، ص ٦٢- ص٦٣.

(٧١) تينا الجلاد، الدبلوماسية(السيبرانية)الالكترونية، مصدر سبق ذكره، ص ٣٣.

(٧٢) صينية قحايرية ومنية قحايرية، الاستراتيجية الامنية، مصدر سبق ذكره، ص ٦٥.

(٧٣) المصدر نفسه، ص ٦٧.

(٧٤) ضياء قدرور، القدرات السيبرانية الإيرانية (الحرب الأخرى بين إيران وخصومها)، شبكة المعلومات الدولية، ٢٠٢١/٢/١، اخر دخول ٢٠٢٥/١/٢٧:- https://www.mena-researchcenter.org..

(٧٥) المصد نفسه.

(٧٦) المصدر نفسه.

(٨٠) المصدر نفسه.

(٨١) احمد بن علي الميموني، الجبهة النشطة، مصدر سبق ذكره، ص ٦٨، ص٧١.

(٨٢) المصدر نفسه، ص ص٧٢.

(٨٣) انيس عبد الوهاب بن احسن، القوة السيبرانية الايرانية، مصدر سبق ذكره، ص ٧٣٨- ص٧٣٩.

(٨٤) المصدر نفسه، ص ٧٤٠.

(٨٥) المصدر نفسه، ص٧٤١.

(٨٦) مليندا كوهون، عمليات ضبط المعلومات في الفضاء السيبراني الايراني: استراتيجية الحرب الناعمة، الدوحة، المركز العربي للأبحاث ودراسة السياسيات، وحدة الدراسات الايرانية، ايار ٢٠٢٢، ص١.

(٨٧) المصدر نفسه، ص٧.

(٨٨) احمد بن علي الميموني، تداعيات المواجهة السيبرانية، مصدر سبق ذكره، ص٧٣.

(٨٩) المصدر نفسه، ص٧٣.

(٩٠) مريم سيد محمد حسن علي علام، القوة السيبرانية في السياسة الخارجية الإسرائيلية تجاه إيران (٢٠١٠– ٢٠٢٠)، المانيا، المركز الديمقراطي العربي، ١٥/نوفمبر /٢٠٢٣، شبكة المعلومات الدولية، المركز العربي الديمقراطي، آخر ظهور ٢٧/ ١/ ٢٠٢٥:– https://democraticac.de/?p=93046..

(٩١) المصدر نفسه.

(٩٢) المصدر نفسه.

(٩٣) المصدر نفسه.

(٩٤) قناة الحرة الفضائية، تقرير: تصاعد الهجمات الإلكترونية الإيرانية ضد إسرائيل بعد حرب غزة، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٥/١/٢٩: https://www.alhurra.com/israel/2024/10/16

(٩٥) احمد بن علي الميموني، تداعيات المواجهة، مصدر سبق ذكره، ص ٦٩– ص٧٠.

(٩٦) شادي عبد الوهاب، السيناريو الكارثي: متى تتحول الحرب السيبرانية إلى حرب شاملة؟، المستقبل للأبحاث والدراسات المتقدمة، ابو ظبي ٢/ يناير / ٢٠٢٢، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٣٠: https://futureuae.com/ar/Mainpage/Item/6992.

(٩٧) شبكة المعلومات الدولية، الحرب الإلكترونية بين إسرائيل وإيران "مستترة" لكنها مؤذية، آخر ظهور ٢٠٢٥/١/٣٠: https://mdeast.news/ar/2021

(٩٨) لأحمد بن علي الميموني، تداعيات المواجهة، مصدر سبق ذكره، ص ٧٤.

(٩٩) شبكة المعلومات الدولية، الحرب الإلكترونية بين إسرائيل وإيران "مستترة" لكنها مؤذية، آخر ظهور ٢٠٢٥/١/٣٠: https://mdeast.news/ar/2021..

(١٠٠) قناة الحرة الفضائية، تقرير: تصاعد الهجمات الإلكترونية الإيرانية ضد إسرائيل بعد حرب غزة، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٥/١/٢٩: https://www.alhurra.com/israel/2024/10/16

(١٠١) قناة الحرة الفضائية، تقرير: تصاعد الهجمات الإلكترونية الإيرانية ضد إسرائيل بعد حرب غزة، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٥/١/٢٩: https://www.alhurra.com/israel/2024/10/16

(١٠٢) مركز الجزيرة للدراسات، إسرائيل تطور "قبة سيبرانية" في وجه الهجمات المعلوماتية الإيرانية، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٤/٢/٤: https://www.aljazeera.net/tech/2024/5/3.

(103) Ibd,p 12

(١٠٤) وحدة الدراسات السياسية، هل نجحت الولايات المتحدة الأمريكية في كبح التصعيد بين (اسرائيل) وايران، الدوحة، المركز العربي للأبحاث ودراسة السياسات، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٤/٢/٧: https://www.dohainstitute.org/ar/PoliticalStudies/Pages/has-the-united-states-succeeded-in-curbing-the-escalation-between-iran-and-israel.aspx

(١٠٥) احمد بن علي الميموني، الجبهة النشطة، مصدر سبق ذكره، ص ٧٤.

[١٠٦] وليد عبد الحي، المكانة الاسرائيلية في مشروع مبادرة الحزام والطريق الصينية، فلسطين، مركز الزيتونه للدراسات والاستشارات، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٤/٢/٧:- https://www.alzaytouna.net/2019.

[١٠٧] وحدة الدراسات السياسية، هل نجحت الولايات المتحدة الأميركية في كبح التصعيد بين إيران وإسرائيل؟ مصدر سبق ذكره.

[١٠٨] احمد بن علي الميموني، الجبهة النشطة، مصدر سبق ذكره، ص ٨٠.

المصادر والمراجع

اولا: المصادر العربية

١) احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران و(إسرائيل)، الرياض، مجلة الدراسات الإيرانية، معهد الدراسات الإيرانية (رصانه)، العدد الثاني عشر، ٢٠٢٠.

٢) احمد محمود صفي الدين، رؤية تحليلية للثورة السيبرانية، مصر، جامعة بور سعيد، كلية التجارة، مجلة البحوث المالية والتجارية، المجلد ٢٥، العدد٢، ٢٠٢٤.

٣) اسامة سالم محمد الفرجاني، العقوبات السيبرانية ومشروعيتها في ضوء قواعد القانون الدولي، مصر، جامعة دمياط، كلية القانون، مجلة حقوق دمياط للدراسات القانونية والاقتصادية، العدد العاشر، يوليو ٢٠٢٤.

٤) انيس عبد الوهاب، القوة السيبرانية الإيرانية وأثرها على الاستقرار الاقليمي، الجزائر، مجلة السياسة العالمية، المجلد ٦، العدد٢، ٢٠٢٢.

٥) ايهاب خليفه، اليات تحقق الردع في الفضاء السيبراني، المركز المصري للفكر والدراسات الاستراتيجية، ص٥٣، شبكة المعلومات الدولية، أخر ظهور ٢٠٢٥/١/٩:
https://www.researchgate.net/publication/366965740...

٦) بزير آمال، الاستجابة الدولية للتهديدات السيبرانية، الجزائر، جامعة محمد الصديق بن يحيى: قطب تاسوست: جيجل، كلية الحقوق ولعلوم السياسية، قسم العلوم السياسية، رسالة ماجستير، ٢٠٢٢.

٧) حسين قوادرة، الردع السيبراني: بين النظرية والتطبيق، الجزائر، المجلة الجزائرية للامن والتنمية، المجلد ٩، العدد١٦، ٢٠٢٠.

٨) رغدة البهي، الردع السيبراني المفهوم والاشكاليات، القاهرة، المركز المصري للفكر والدراسات الاستراتيجية، شبكة المعلومات الدولية، اخر ظهور ٢٠٢٥/١/١٤:https://ecss.com.eg/6203

٩) تغريد صفاء ولبنى خميس، اثر السيبرانية في تطور القوة، العراق، مجلة حمورابي للدراسات، العدد ٣٣- ٣٤، السنة الثامنة، ٢٠٢٠.

١٠) تينا الجلاد، الدبلوماسية السيبرانية الالكترونية واهميتها ل(إسرائيل)، مجلة شؤون فلسطينية، مركز الابحاث: منظمة التحرير الفلسطينية، العدد ٢٨٥، ٢٠٢١.

١١) جيهان احمد عبد العال وسلوى السعيد ورشا عطوة عبد الحكيم، الحروب السيبرانية: دراسة في المفهوم والنشأة ومعدلات النجاح، مصر، جامعة قناة السويس، كلية التجارة، المجلة العلمية للدراسات التجارية والبيئية، المجلد الثالث عشر، العدد الثاني، ٢٠٢٢.

١٢) روان بنت عطية الله الصحفي، الجرائم السيبرانية، المملكة العربية السعودية، جدة المجلة الالكترونية الشاملة متعددة التخصصات، العدد ٢٤، ٢٠٢٠.

١٣) سماح عبد الصبور، القوة السيبرانية في العلاقات الدولية: دراسة في الحروب السيبرانية بالتطبيق على عام ٢٠٢٠، شبكة المعلومات الدولية، آخر دخول ٢٠٢٥/١/٥:- https://hadaracenter.com..

١٤) شادي عبد الوهاب، السيناريو الكارثي: متى تتحول الحرب السيبرانية إلى حرب شاملة؟، المستقبل للأبحاث والدراسات المتقدمة، ابو ظبي ٢/ يناير / ٢٠٢٢، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٣٠:- https://futureuae.com/ar/Mainpage/Item/6992...

١٥) شويرب جيلالي ودمراد فائزة، مفهوم الحروب السيبرانية والامن السيبراني، الجزائر، جامعة محمد خيدر، مجلة الحقوق والحريات، المجلد ١١، العدد١.

١٦) صينية قحايرية ومنية قحايرة، الاستراتيجية الامنية (الإسرائيلية) في مواجهة التهديدات السيبرانية، الجزائر، جامعة التبسي – تبسة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، رسالة ماجستير، ٢٠١٨.

١٧) ضياء قدرور، القدرات السيبرانية الإيرانية (الحرب الأخرى بين إيران وخصومها)، شبكة المعلومات الدولية، ٢٠٢١/٢/١، اخر دخول ٢٠٢٥/١/٢٧:-https://www.mena-researchcenter.org .

١٨) فاطمة علي ابراهيم ورحاب يوسف ووليد، الامن السيبراني والرقمية، مصر، المجلة المصرية لعلوم المعلومات، المجلد ٩، العدد ٢، اكتوبر ٢٠٢٢.

١٩) فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى: دراسة حالة الصين، الجزائر، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، رسالة ماجستير، ٢٠١٧/٢٠١٨.

٢٠) علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، الجزائر، جامعة الوادي، مجلد ١، العدد ٣، ٢٠١٩.

٢١) علاء الدين فرحات، الحرب السيبرانية ومستقبل الامن العالمي، الجزائر، مجلة الناقد للدراسات السياسية، المجلد ٦، العدد ٢، ٢٠٢٢.

٢٢) عمران طه عبد الرحمن عمران، الفضاء السيبراني إطار مفاهيمي في ضوء نظريات العلاقات الدولية، المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية والاقتصادية، شبكة المعلومات الدولية، اخر دخول ٢٠٢٥/١/٩: -https://www.democraticac.de/?p=96508.

٢٣) مايسة السروي، حروب عصر الرقمنة. كيف يمكن أن تصيب العالم بالشلل؟، شبكة المعلومات الدولية، نشر ٢٠٢٤/٩/٢٠، آخر ظهور ٢٠٢٥/٢/٧:https://www.alarabiya.net/science/2024/09/20.

٢٤) محمود محارب، (إسرائيل) والحرب الالكترونية: قراءة في كتاب حرب في الفضاء السيبراني اتجاهات وتأثيرات على (إسرائيل)، الدوحة، المركز العربي للأبحاث ودراسة السياسات، ٢٠١١.

٢٥) مركز الملك فيصل للدراسات والبحوث الاسلامية، قدرات القرصنة السيبرانية الإيرانية، تقرير خاص، يناير ٢٠٢٠.
٢٦) مريم سيد محمد حسن علي علام، القوة السيبرانية فى السياسة الخارجية الإسرائيلية تجاه إيران (٢٠١٠-٢٠٢٠)، المانيا، المركز الديمقراطي العربي، ١٥/نوفمبر /٢٠٢٣، شبكة المعلومات الدولية، المركز العربي الديمقراطي، آخر ظهور ٢٧/ ١/ ٢٠٢٥: https://democraticac.de/?p=93046
٢٧) منى عبد الله السمحان، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، مصر، جامعة المنصورة، كلية التربية، مجلة كلية التربية، العدد ١١١، يوليو ٢٠٢٠.
٢٨) مليندا كوهون، عمليات ضبط المعلومات في الفضاء السيبراني الإيراني: استراتيجية الحرب الناعمة، الدوحة، المركز العربي للأبحاث ودراسة السياسيات، وحدة الدراسات الإيرانية، أيار ٢٠٢٢.
٢٩) نبيلة عبد الفتاح قشطي، الحرب السيبرانية وسبل مواجهتها، الجزائر، مجلة شؤون استراتيجية، العدد ١٧، مارس ٢٠٢٤.
٣٠) نور الدين حامد علي إبراهيم، الفضاء السيبراني: المفاهيم والابعاد، المجلة العلمية للبحوث والدراسات السيبرانية، مصر، جامعة حلوان، كلية التجارة وتجارة الاعمال، المجلد ٣٨، العدد ٢، ٢٠٢٤.
٣١) وحدة الدراسات السياسية، هل نجحت الولايات المتحدة الأمريكية في كبح التصعيد بين (اسرائيل) وإيران، الدوحة، المركز العربي للأبحاث ودراسة السياسات، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٤/٢/٧: https://www.dohainstitute.org/ar/PoliticalStudies/Pages/has-the-united-states-succeeded-in-curbing-the-escalation-between-iran-and-israel.aspx..
٣٢) وليد عبد الحي، المكانة الاسرائيلية في مشروع مبادرة الحزام والطريق الصينية، فلسطين، مركز الزيتونة للدراسات والاستشارات، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٤/٢/٧: https://www.alzaytouna.net/2019.
٣٣) ياسين محمد، الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية، ليبيا، مجلة شمال افريقيا للنشر العلمي، المجلد الرابع، العدد ١، ٢٠٢٣.

ثانيا المصادر الاجنبية:

1) Marco Benatar, the Use of Cyber Force: Need for Legal Justification? Goettingen Journal of International Law 1 (2009) 3.
2) Dr. Stuart H. STARR1, Towards an Evolving Theory of Cyber power, a Center for Technology and National Security Policy (CTNSP) National Defense University (NDU), the U.S. Government, https://ccdcoe.org/uploads/2018/10/02_STARR_Cyberpower.pdf.
3) Dr. Stuart H. STARR1, Towards an Evolving Theory of Cyber power,https://ccdcoe.org/uploads/2018/10/02_STARR_Cyberpower.pdf.
4) What are Cyber-Threats, Cyber-Attacks and how to defend our Systems, See

discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/349043516.

5) Ahmed Al-Zaidy, Research Proposal Paper: Final Term Project Paper. Annegret Bendiek, und Tobias Metzger, Deterrence theory in the cyber-century.Lessons from a state-of-the-art literature reviewLecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 201

6) Ahmad Mohee Mohammed Ahmad Ali, The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security. Institute of Arab Research & Studies , https://www.researchgate.net/publication/369573139...

ثالثا: مصادر الانترنيت

١) قناة TRT العربية، القمر الصناعي الإسرائيلي "أفق ١٦" ما علاقته بالتجسس واستهداف إيران؟، شبكة المعلومات الدولية آخر دخول ٢٠٢٥/١/٢٧:- https://www.trtarabi.com/now.

٢) قناة الحرة الفضائية، تقرير: تصاعد الهجمات الإلكترونية الإيرانية ضد إسرائيل بعد حرب غزة، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٥/١/٢٩: https://www.alhurra.com/israel/2024/10/16.

٣) شبكة المعلومات الدولية، الحرب الإلكترونية بين إسرائيل وإيران "مستترة" لكنها مؤذية، آخر ظهور ٢٠٢٥/١/٣٠: https://mdeast.news/ar/2021.

٤) شبكة المعلومات الدولية، الحرب الإلكترونية بين إسرائيل وإيران "مستترة" لكنها مؤذية، آخر ظهور ٢٠٢٥/١/٣٠: https://mdeast.news/ar/2021.

٥) قناة الحرة الفضائية، تقرير: تصاعد الهجمات الإلكترونية الإيرانية ضد إسرائيل بعد حرب غزة، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٥/١/٢٩: https://www.alhurra.com/israel/2024/10/16.

٦) مركز الجزيرة للدراسات، إسرائيل تطور "قبة سيبرانية" في وجه الهجمات المعلوماتية الإيرانية، شبكة المعلومات الدولية، آخر ظهور ٢٠٢٤/٢/٤: https://www.aljazeera.net/tech/2024/5/3.