URUK FOR HUMANITIES 2025;18:736–746

RESEARCH ARTICLE

The Geopolitical Analysis of the Cyber War Between Iran and the Zionist Entity

Suhad Jamal Jihad Hamadi [a,*] **Hussein Ali Hadhoud** [b,*]

[a] **AL-MUTHANNA UNIVERSITY, College of Medicine, Iraq.**

[b] **AL-MUTHANNA UNIVERSITY, OLLEGE OF LAW, Iraq .**

ABSTRACT

This study focuses on the fact that cybersecurity has become a fundamental element of state power, adding to its existing dimensions of air, land, and sea power. This is exemplified through a case study of the "cyber war between Iran and Israel," demonstrating how cyber capabilities have become a cornerstone tool that transcends the traditional physical geographical boundaries of state security. This model of warfare is nothing more than an intricate blend linking technology, politics, and security.

This study addresses the main reasons for the conflict between the two states, which included Iran's support for its proxies in the region, as well as the undermining of the Iranian nuclear program. Iran aims to extend its influence in the region by enhancing its technological capabilities through alliances with global powers such as Russia and China. Meanwhile, Israel leverages its technological superiority and its relationship with the United States, its primary backer, to bolster its capabilities as part of its proactive security strategy in the Middle East. Israel lacks strategic depth in the region compared to its adversary, Iran. The study also reveals that the repercussions of the conflict have contributed to destabilizing regional and international security and stability.

KEYWORDS: Cybersecurity, cyber warfare, geopolitics, Iran, the Zionist entity.

مقالة بحثية

التحليل الجيوسياسي للحرب السيبرانية بين إيران والكيان الصهيوني

سهاد جمال جهاد حمادي[1] ، حسين علي هدهود [2]

جامعة المثنى ، كلية الطب ، قسم الفسلجة والفيزياء الطبية ، العراق [1]

جامعة المثنى ، كلية القانون ، القسم العام ، العراق [2]

الملخص:

تركز هذه الدراسة على ان الأمن السيبراني بات عنصراً اساسياً في قوة الدولة يضاف لا بعاد قوتها " الجوية البرية والبحرية" تجسد ذلك عن طريق دراسة حالة " الحرب السيبرانية بين إيران– والكيان الصهيوني "وكيف باتت القدرات السيبرانية أداة ركيزة تخترق الحدود الجغرافية المادية التقليدية لأمن الدولة هذا النموذج من الحرب ما هو الا مزيج متشابك يربط بين "التكنولوجيا والسياسة والأمن ".

تناولت هذه الدراسة الأسباب الرئيسية للحرب بين الدولتين والتي تمثلت بدعم ايران لوكلائها في المنطقة فضلاً عن تقويض البرنامج النووي الإيراني ،فإيران تهدف لبسط نفوذها في المنطقة بوساطة تعزيز كفاءتها التكنلوجية بالتحالف مع قوى عالمية مثل "روسيا والصين" في حين يوظف الكيان الصهيوني تفوقه التقني وعلاقاته مع "الولايات المتحدة الامريكية "وهي الداعم الرئيس لتعزيز إمكانات الكيان وكجزء من استراتيجيته الأمنية الاستباقية في منطقة الشرق الأوسط ،فالكيان الصهيوني يفتقر للعمق الاستراتيجي في المنطقة مقارنة بخصمه ايران ،كما كشفت الدراسة تداعيات الحرب أسهمت في زعزعة الأمن و الاستقرار الإقليمي والدولي.

الكلمات المفتاحية : الأمن السيبراني، الحرب السيبرانية ، الجيوسياسية ، إيران، الكيان الصهيوني.

Received 30-11- 2025; Revised 08-12- 2025; accepted 14-12- 2025 ; Available online 30-12- 2025 .

*Corresponding author

E-mail Suhad.jamal@mu.edu.iq **(S.J. Hamadi)**, hussain.hadhood@mu.edu.iq **(H.A. Hadhoud).**

https://doi.org/xx.xxxxx/2572-5440.1068

المقدمة

شـــهدت الســـنوات الاخيـــرة مفـــاهيم جديـــدة للحـــرب وتحـــولات كبيـــرة فـــي جوهرهـــا اذ اضـــحت "القـــدرات الســـيبرانية "تمثـــل مصـــدر قـــوة وتنـــافس للدولـــة الحديثـــة لا بـــل ان القـــوة الســـيبرانية اضـــحت عنصـــراً اساســـياً فـــي معادلـــة القـــوى الدوليـــة ومؤشـــراً لقوتهـــا التكنلوجيـــة ومقياســـاً لتفوقهـــا التكنلـــوجي لمـــا يـــوفر للـــدول حمايـــة مصـــالحها فـــي الســـاحة الدوليـــة دون الانـــزلاق الـــى المواجهـــة العســـكرية التقليديـــة وعليـــه بـــرزت الحـــرب الســـيبرانية كـــأداة توظفهـــا الـــدول لتحقيـــق غايـــات واهـــداف جيوسياســـية، لـــذ يعـــد نمـــط العلاقـــة الغيـــر متماثلـــة بـــين إيـــران والكيـــان الصـــهيوني نمـــوذج بـــارز ومعاصـــر للحـــرب السيبرانية والتنافس السيبراني في منطقة الشرق الأوسط.

تنـــاقش هـــذه الدراســـة الابعـــاد الجيوسياســـية للحـــرب الســـيبرانية بـــين "إيـــران والكيـــان الصـــهيوني " فـــي المنطقـــة مـــن خـــلال التعـــرف علـــى الـــدوافع الرئيســـة للحـــرب الســـيبرانية لإيـــران والكيـــان الصـــهيوني و تـــداعياتها علـــى الأمـــن و الاســـتقرار الـــداخلي والاقليمـــي والـــدولي لاســـيما أمـــن دول الخلـــيج خاصـــة يضـــاف اليهـــا التفـــاعلات الإقليميـــة والدوليـــة التـــي اعـــادة رســـم مـــوازين القـــوة الاقليميـــة ،كمـــا تناولـــت هـــذه الدراســـة التعـــرف علـــى ابـــرز الهجمـــات للطـــرفين والتـــي اعـــادة بلـــورة مفهـــوم الـــردع الجيوسياســـي فـــي الحـــرب ممـــا يفـــرض تحـــديات جديدة على الاستراتيجيات الأمنية الإقليمية.

أولاً:- مشكلة البحث

يمكن صياغة مشكلة البحث على النحو الاتي:-

1- ما دوافع الحرب السيبرانية بين إيران والكيان الصهيوني؟

2- بماذا تمثلت تداعيات الهجمات السيبرانية للحرب الإيرانية الصهيونية؟

ثانياً: - فرضية البحث

انطلاقا من المشكلة يفترض الباحثان الآتي:-

1- ثمة دوافع وأهداف جيوسياسية" سياسية وأمنية وايدولوجية " للحرب الإيرانية الصهيونية منها التنافس الجيوسياسي ، التموضع كقوة اقليمية سيبرانية في منطقة الشرق الاوسط.

2- هناك حزمة من التداعيات للحرب السيبرانية بين الدولتين انعكست اثارها على الأمن الإقليمي والدولي تمثلت (بزعزعة الاستقرار الإقليمي، انخراط قوى لتحالفات عالمية سيبرانية، توسع مفهوم الردع العسكري).

ثالثاً:- هدف البحث

تسعى الدراسة الى فهم الابعاد الجيوسياسية من الحرب الإيرانية –الصهيونية مع دراسة انعكاساتها على موازين القوى الإقليمية في منطقة الشرق الأوسط ،فضلاً عن تداعياتها على مستويات الأمن الإقليمي والدولي فهي دراسة تجمع بين (الجغرافية والسياسة والسياد).

رابعاً:- أهمية البحث

تأتي أهمية البحث من خلال تحليل جيوسياسية الحرب الإيرانية الصهيونية في منطقة الشرق الأوسط ولفهم العلاقة المترابطة بين" الجغرافيا ،السياسة والقوة السيبرانية " فالأخيرة أضافت بعداً جديداً لقوة للدولة ، فضلاً عن التعرف على اثر ديناميكيات الحرب السيبرانية على المنطقة.

خامساً:- حدود بحث الدراسة

تجسدت حدود الدراسة بالحدود المكانية لدولة ايران والكيان الصهيوني في منطقة الشرق الأوسط، في حين تمثلت الزمانية منها للمدة (2010-2025) مع التطرق لبعض المراحل التاريخية التي تخدم حدود البحث .

سادساً:- منهج الدراسة

اعتمد الباحثان على منهجين الأول هو المنهج التأريخي لرصد القدرات السيبرانية وتطورها بين إيران والكيان الصهيوني والثاني منهج تحليل القوة لتحليل وتفسير عناصر القوة السيبرانية لإيران والكيان التي تم توظيفها في الحرب.

سابعاً:- هيكلية الدراسة

اشتمل البحث على مقدمة وثلاثة مباحث ركز الاول على الاطار المفاهيمي للأمن السيبراني و اهتم الثاني بالأمن السيبراني في سياق الجغرافية السياسية والاستيراتيجية, في حين استعرض الثالث النطاق الجغرافي للحرب السيبرانية الإيرانية- الصهيونية وتداعيات الحرب اقليمياً ودولياً ثم اختتم البحث بجملة الاستنتاجات.

ثامناً :- الدراسات السابقة

1-أماليا(2025)،الحرب السيبرانية بين إيران والكيان الصهيوني بوصفها امتداد للتنافس الجيوسياسي بينهما، اكدت استخدام الأدوات الرقمية لتعزيز النفوذ والردع في المنطقة الإقليمية.

2- هارون (2024)، دور الذكاء الاصطناعي والحرب السيبرانية في الصراع الصهيوني-الإيراني، بينت تأثيراته على أمن دول الخليج واستراتيجياتها الدفاعية.

3- شانزر(2023)،طبيعة الصراع غير المعلن بين إيران والكيان الصهيوني ،اكد اعتماد الدولتين على العمليات السيبرانية كأدوات غير مباشرة لإدارة التنافس دون الانزلاق إلى مواجهة عسكرية مفتوحة.

يستنتج ان الدراسات اعلاه ركزت على التنافس السيبراني و لم تركز على الفجوة البحثية المتمثلة بالأمن السيبراني قد أضاف بعداً رابعاً لقوة الدولة فضلاً عن بيان نقاط الضعف للكيان الصهيوني ومن هنا تسعى هذه الدراسة الى التركيز على تلك النقاط.

المبحث الأول: الاطار المفاهيمي للأمن السيبراني

أولاً- الاطار المفاهيمي

1- مفاهيم الامن السيبراني

شهد مفهوم الأمن نقلة نوعية من المفهوم التقليدي إلى منظور أكثر نقداً في مناقشات العولمة التي بدأت منذ أوائل التسعينيات تعزز هذا التطور بظهور مفهوم" الأمن السيبراني" فهو لا ينحصر على أمن الدولة وانما وثيق الصلة وجزءاً

لا يتجزأ من(الأمن الانساني، السياسي ،الاقتصادي ،الصحي ،الغذائي ،البيئي والمجتمعي). [1،ص504]. فمن المعروف ان الدولة تنمي قدراتها الأمنية العسكرية من خلال تعزيز امكانياتها التقليدية كـ (الجيوش ،البحرية والقوات الجوية) أما حالياً وفي العصر الرقمي تتم من خلال تعزيز قدراتها السيبرانية [2،ص524]. وعليه تجسدت مفاهيم الأمن السيبراني بالاتي:-

أ- الامن السيبراني: يُشير هذا المصطلح إلى فرض الحماية الوطنية على كافة أنظمة (الشبكات ،الأجهزة ،البيانات) ازاء الوصول غير القانوني للهجمات الخبيثة واتلافها ،اذ ان تطور العالم الرقمي جعل الأمن السيبراني مجالاً أساسيًا لحماية البيانات الشخصية والبنية التحتية الحيوية للدولة وامنها القومي فضلاً عن الاستقرار العالمي اذ يضم هذا المفهوم في جوهره حزمة متنوعة من التدابير والبروتوكولات المعدة لتصدي الهجمات السيبرانية واختراق البيانات والأنظمة [3،ص 257-258]. فضلاً عن ذلك فقد عرفته المنظمة الدولية للمعايير **(ISO)** على انه : (نهج يعمل على إدارة مخاطر أمن المعلومات الرقمية لدى أجهزة الحاسوب ووحدات التخزين، والشبكات) [4 ،ص 436].

تكمن أهمية الامن السيبراني على ارتكاز معظم الخدمات والصناعات الأساسية كـ (شبكات الطاقة ،الأنظمة المالية والرعاية الصحية)على البنية التحتية الرقمية المتضمنة (أمن الشبكات، أمن المعلومات، أمن التطبيقات، فضلاً عن خطط التعافي من الكوارث) [3،ص257-258]. يضاف الى ما ذكر فهو يحد من (الوصول غير المصرح به، اختراق الحواسيب فضلاً عن سرقة المعلومات من أنظمة الحاسوب والشبكات وقواعد البيانات) [5،ص29]. ففي وقتنا الحاضر اصبح إلا من السيبراني لا يقتصر على حماية الأفراد أو الشركات أو المؤسسات اذ تصاعد الآن إلى تكتيكات الحرب أو التجسس او كلاهما وهوما يُعرف الآن بـ (الحرب السيبرانية) الامر الذي يهدد الأمن القومي للدولة بالخطر[6،ص48] .

ب - الحرب السيبرانية: تعنى باستخدام القدرات السيبرانية لأغراض عسكرية وهي جزء من حرب المعلومات[5،ص31].

ج- الفضاء الجيوسيبراني : يمثل العلاقة الرابطة بين كل من(الانترنيت ،الجغرافيا ،الديموغرافيا فضلاً عن الاقتصاد والسياسة الداخلية والخارجية للدولة) [7، ص239].

د- القوة السيبرانية: يعد جوزيف ناي عام (2011) هو أول من اسس مفهوم "القوة السيبرانية" كبعد جديد لقدرات الدولة يُشبه القوة الاقتصادية والعسكرية أكد على ضرورة فهم الدول للأشكال "الصارمة والناعمة" للقوة السيبرانية[8،ص 1397] . فهي تعنى بالابتكار والابداع والاختراع فضلاً عن امتلاك المعرفة التكنلوجية ومدى إمكانية استخدامها[9،ص12].

2- ابعاد الامن السيبراني

أدت الطبيعة المترابطة للفضاء الإلكتروني إلى تشابك الأبعاد الجيوسياسية والتقنية والعسكرية لتشكل بعداً آخر من المنافسة كـ (الاقتصاد الإلكتروني ،الثقافة الإلكترونية والدبلوماسية الإلكترونية) .تجسد الابعاد السيبرانية بالاتي:-

أ- البعد العسكري : انتقل نهج العمليات العسكرية باتجاه التركيز على العمليات الذكية الاخيرة دعمت تطبيقات الاستخبارات والمراقبة والاستطلاع عبر دمج الرادار والأنظمة الموجهة بدقة وأجهزة الاستشعار والكشف بالأشعة تحت الحمراء في المقابل أن الأسلحة السيبرانية تبقى سريةً لخلق التهديدات. اذ ادى الترابط عند جمع المعلومات الاستخبارية، اختراق الشبكات، العمليات الهجومية والدفاعية الى عرقلة تحديد مصدر الهجمات السيبرانية وعليه ارتفع خطر نشوب صراعات عرضية كالردع النووي والعمليات الاستخباراتية مما قد ينجم عنه انهيار محطة نووية أو إطلاق مياه من سد ما فوق منطقة مأهولة بالسكان أو تعطيل مراقبة الملاحة الجوية[10،ص8-11].

ب- البعد السياسي : يعنى بالتوازن بين قطاعي الدولة العام والخاص أزاء آلية تأمين الفضاء السيبراني اذ يسعى كلا الطرفين لأولوية التنافس باكتساب النفوذ السياسي وعليه تعد هذه الآلية هي سياسات مشتركة بين القطاعين[11،ص406-407] .

ج- البعد القانوني : ان التنظيم القانوني للسلوك في ميدان الفضاء الإلكتروني وردع إساءة استخدام تكنولوجيا المعلومات والاتصالات هو جزءًا لا يتجزأ من استراتيجية الأمن السيبراني للدولة إزاء حماية البنى التحتية الرقمية وتعزيز امنها السيبراني[12،ص9] .

د- البعد التقني : يضم الأنشطة الأساسية المتمثلة بـ (التجسس الإلكتروني، والهجمات الإلكترونية، والحرب الإلكترونية) [10،ص8].

هـ- البعد الاقتصادي: عاملًا مهمًا ازاء قرارات الاستثمار في الدولة فالحوادث السيبرانية تعد عامل مؤثر على تخصيص الموارد و تطوير قطاعات معينة فحجم الحوادث اعلاه يُعدّ أكثر صعوبة من جمع البيانات[13,ص10].

و- البعد الاجتماعي (الأخلاقي): يهتم بـ توفير الحماية وفق إطار من الشفافية لـ خصوصية الأفراد واستقلاليتهم أزاء توظيف البيانات بالطريقة التطفلية الغير أخلاقية[14،ص14].

3- فواعل الامن السيبراني

ان المعركة الرقمية تعد ساحة للجهات الفاعلة الحكومية وغير الحكومية مما تسمح بإجراء عمليات ذكية هدفها زعزعة استقرار البنى التحتية الوطنية بأكملها دون إطلاق قذيفة مادية واحدة [2،ص515].

أ- فواعل دولية : تلعب الدول القومية دورًا حاسمًا في الدبلوماسية السيبرانية فهي تعمل على مواجهة المخاطر السيبرانية من خلال مشاركتها في الجهود الدبلوماسية ،التفاوض على اتفاقيات المعايير السيبرانية اذ تُصوغ الدول خططًا وسياساتٍ سيبرانية وتُناقش الشؤون السيبرانية مع الدول الأخرى اذ يُمثّل الدبلوماسيون والسلك الدبلوماسي حكوماتهم في المنتديات الدولية والمحادثات

عبر الإنترنت ذات الصلة بالفضاء الإلكتروني .

اما المنظماتٌ كـ الأمم المتحدة، الاتحاد الأوروبي، الاتحاد الدولي للاتصالات، الدبلوماسية السيبرانية فهي تُيسّر المحادثات والمبادرات العالمية أزاء المعايير والحوكمة السيبرانية فضلاً عن منتديات الإنترنت كحوكمة الإنترنت **(IGF)** الذي يعد منبرًا للحكومات والقطاع التجاري والمجتمع المدني والأوساط الأكاديمية لمناقشة سياسات الفضاء الإلكتروني يضاف الى ما ذكر دور وسائل الإعلام على الرأي العام فـ الاولى تعمل على زيادة الوعي بمخاطر السيبرانية ومن ثَمة تؤثر على آراء وتصرفات الجمهور والحكومات . [5،ص34-35].

ب- فواعل غير دولية: تتمثل بمنظمات المجتمع المدني كالمؤسسات الأكاديمية، جماعات المناصرة، مجتمعات الأمن السيبراني والشركات الخاصة لدورها الفعال في مجال الإنترنت وتبادل معلومات استخباراتية ازاء التهديدات اذ تُعزز الوعي وتُشارك الخبرات من خلال تُنظيم حملات للحفاظ على الحقوق والحريات الرقمية وعليه تسهم الجهات غير الحكومية من خلال إجراء البحوث وتقديم تحليلات الخبراء والدعوة إلى ممارسات سيبرانية آمنة واقتراحات سياسية وتتعاون مع الحكومات والوكالات الدولية في حوارات الدبلوماسية السيبرانية عبر تبادل خبراء الأمن السيبراني والباحثون والمتخصصون التقنيون أفكارهم وخبراتهم [5،ص34-35].

ثانياً: تهديدات الامن السيبراني

يشكل الأمن السيبراني مصدر قلق عالمي متزايد إزاء تفاقم الهجمات السيبرانية واختراقات البيانات[15،ص75]. اذ يعتمد مستوى التهديدات على التوزيع النسبي للقوة، القرب الجغرافي ،القدرات الهجومية فضلاً عن النوايا المخطط لها[16،ص14].فالتهديدات اتخذت أشكالًا مختلفة تمثلت بأهمها:-

أ- اختراقات (تجسس): هجمات غايتها سرقة معلومات حكومية أو عسكرية أو مؤسسية حساسة تنفذها جماعات التهديد المتقدم المعروفة باسم **(APT)** ذات خروقات أمنية طويلة الأمد تُؤدي إلى خروقات أمنية مثال/ حملات تجسس إلكتروني لدى (الصين وروسيا وكوريا الشمالية) [3،ص 258].

من اثارها هي تكلفة الاقتصاد العالمي مليارات الدولارات سنويًا فقد بينت شبكة (إنفاذ قوانين الجرائم المالية) بلغت الخسائر عام (2023) نحو (1.4) مليار دولار أمريكي بنسبة (30%) لارتفاع عدد الجرائم الإلكترونية مقارنةً بالعام الذي يسبقه. وفي ذات الصدد توقعت شركة **(CybersecurityVentures)** عام (2024)ان ألاضرار قد تتجاوز نحو (10.5) تريليون دولار أمريكي سنويًا مطلع هذا العام (2025) مما تزيد عن إجمالي الاضرار التي تخلفها الكوارث الطبيعية ،الإرهاب والحروب التقليدية [3،ص258] .

ب- التضليل : وهي الدعاية الإلكترونية تستهدف جمهور معين بغية تغيير وجهات نظرها لليقين بمعلومات محددة[6،ص49-50].مثال/ عمدت روسيا لحملات تضليل منسقة كسلاح لـ خلق خلافات بين دول الناتو وتشويهها وانقسامها وإضعافها من خلال التأثير على الرأي العام في أوروبا الشرقية[17،ص352].

ج- (DDoS): تعد من الخدمات الحديثة نسبياً تسمى بـ هجمات الحرمان طُوّرت عام (2010) من قبل الولايات المتحدة وإسرائيل استخدمت لمهاجمة البنية التحتية النووية لإيران دون استخدام أي أسلحة تقليدية[6،ص49-50].

د- الفدية: هي احد انواع الهجمات الخبيثة اذ يعتمد المهاجمون على تشفير بيانات المؤسسة المعنية ثم يطالبون بدفع فدية لاستعادة الوصول للبيانات[18،ص280] .

ثالثاً- المعاهدات والاتفاقيات الدولية السيبرانية

ان التعاون الدولي أمرًا بالغ الأهمية لمواجهة التهديدات الإلكترونية السيبرانية الذي يضم اتفاقيات ومعاهدات لإرساء معايير ولوائح وبروتوكولات منها اتفاقية **بودابست** وهي أول معاهدة دولية صادقت علها أكثر من (65) دولة ومنها الولايات المتحدة الأمريكية [19،ص57]. فضلاً عن الاتحاد الأفريقي عام (2014) للبيانات الشخصية في الدول الأفريقية، **باليرمو** لتجريم استخدام أجهزة الكمبيوتر لغسل الأموال،تقارير للأمم المتحدة المعنية بالقانون والمعايير الدولية، لائحة **(GDPR)** لمواطني الاتحاد الأوروبي، **واسينار** لمراقبة الصادرات يُنظّم تجارة الأسلحة التقليدية والتقنيات ذات الاستخدام المزدوج، برنامج الدول الامريكية للأمن السيبراني، خطة العمل للمنشآت النووية الإيرانية، دليل تالين لكيفية تطبيق القانون الدولي على العمليات السيبرانية [5،ص37].

وفي ما يلي ملخص لأهم المعاهدات والاتفاقيات الدولية في مجال الأمن السيبراني يلخصها **جدول (1)(ص 5).**

المبحث الثاني- الأمن السيبراني في سياق الجغرافية السياسية والجيوسياسية

اولاً - علاقة الامن السيبراني بالجغرافية السياسية.

تركز الجغرافية السياسية على دراسة الأنظمة السياسية للدول فضلاً عن اهتمامها بدراسة التفاعل بين كل من المنطقة الجغرافية والعملية السياسية وعلاقتها المكانية وعليه يـ عرفها **"بومان"** بانها:" الوجه السياسي للجغرافية الذي يحدد العوامل الجغرافية المؤثرة في السلوك السياسي للإنسان"[20،ص277].

مما لا شك فيه ان الجغرافيا السياسية شهدت تحولاً عميقاً مع ظهور الفضاء السيبراني بخلاف الحدود الإقليمية التقليدية، يُمثل الفضاء الإلكتروني مجالًا غير ملموس وإن كان ذا أهمية استراتيجية اذ يتزايد التنافس على السلطة الوطنية فقد بات المشهد الرقمي ساحة معركة معقدة تتلاشى فيها القيود الجغرافية وتنخرط الدول في عمليات متطورة تتجاوز القيود المادية كساحة حاسمة للصراع الدولي[2،ص515]. اذ ان مخاطر الإنترنت لا تقتصر على نطاق جغرافي محدد إذ يمكن للقراصنة استهداف أي دولة أو منظمة بغض النظر عن موقعها الجغرافي[5،ص32]. في حين تتمثل العلاقة بين عناصر الجغرافيا السياسية وعلاقتها بالأمن السيبراني كالتي:-

1- السيادة السيبرانية: تشير السيادة السيبرانية إلى سلطة الدولة على الإنترنت ودورها في حماية المواطنين من مختلف التحديات فهي تعنى ومن خلال الانترنت بإدارة الأنشطة المحلية وحماية البنية التحتية لتكنولوجيا المعلومات فضلاً عن التصدي للإجراءات الساعية لـ تقويض نظام الدولة من خلال شبكات تكنولوجيا المعلومات

2- التنافس الجيوسياسي: هناك ارتباطًا وثيقًا بين الأهداف الجيوسياسية وعسكرة الفضاء الإلكتروني فالأولى تسعى إلى تأمين مصالحها الوطنية وفرض نفوذها وقوتها في الفضاء الإلكتروني [10،ص3،7].

3- الأمن القومي: تُعدّ القدرات السيبرانية اليوم جزءًا أساسيًا من استراتيجيات الأمن القومي للدولة في حين ان الحرب الرقمية تصنف كأداةً أساسيةً من أدوات قوة الدولة ونفوذها فغياب القدرات الدفاعية السيبرانية سيهدد (البنى التحتية الوطنية وانظمتها المالية الحديثة فضلاً عن شبكات الاتصالات).

4- الحدود السيبرانية: ليس هناك ارتباط بين الهجمات السيبرانية والحدود المادية للجغرافية اذ بإمكان أي دولة أن تشن هجومها عن بعد دون عبور تلك الحدود [17،ص346-352].

وعليه يمكن القول ان الأمن السيبراني غدا بعداً رابعاً لقوة الدولة الحديثة وموازياً لا بعادها التقليدية "الجوية والبرية والبحرية" المتعارف عليها فالأمن السيبراني يتفاعل مع الميادين الجغرافية والسياسية وهو تحول نوعي في طبيعة سيادة الدولة وقوتها الدولية.

ثانياً- دور الإستراتيجية في سياسات الامن السيبراني

مما لا شك فيه ان الدولة القوية إلكترونيًا توظف براعتها التكنولوجية لاكتساب مزايا استراتيجية (عسكرية ،اقتصادية،سياسية واجتماعية) لـتتجاوز بـذلك الحدود المادية وعليه يمكنها ذلك من فرض هيمنتها عالميًا اذ ان أي دولة بإمكانها تنفيذ عملياتها السيبرانية مثل (التجسس الإلكتروني، حرب المعلومات، والهجمات السيبرانية التخريبية) دون اللجوء إلى القوة العسكرية التقليدية [5،ص72].

ان توجه الدول لاستخدام الأساليب الرقمية بغية الوصول لأهداف جيوسياسية التي لم تلمس عادة في الاجراءات العسكرية التقليدية تعد مهارة و تحديًا كبيرًا لقواعد الاشتباك الدولية المعمول بها اذ وفق هكذا آلية يتلاشى التمييز بين الهجوم والدفاع في المجال الرقمي[6،ص64].

جدول (1) المعاهدات والاتفاقيات الدولية للأمن السيبراني

ت	الوصف	الهدف
1	اتفاقية بودابست عام 2001	الجرائم الإلكترونية مواءمة القوانين الوطنية
2	اتفاقية الاتحاد الأفريقي عام2014	حماية البيانات الشخصية في الدول الأفريقية
3	اتفاقية باليرمو عام2000	الجرائم السيبرانية التي ترتكبها الجماعات الإجرامية المنظمة
4	تقارير الأمم المتحدة UN (GGE) عام2000	إرشادات وتوصيات بشأن الفضاء السيبراني
5	لائحة GDPR للاتحاد الأوروبي عام 2016	حماية البيانات الشخصية في الاتحاد الأوروبي
6	نظام واسينار عام1995	نظام لمراقبة صادرات المواد المتعلقة بالأمن السيبراني
7	مذكرات خطة عمل مشتركة	أحكامًا تتعلق بالأمن السيبراني للمنشآت النووية الإيرانية
8	دليل تالين عام2013	إرشادات الفضاء السيبراني عن السيادة والدفاع عن النفس وقانون النزاعات المسلحة
9	برنامج الامن السيبراني لمنظمة الدول الأمريكية عام2010	مواجهة التهديدات السيبرانية في الأمريكيتين

Source:- Radanliev, Petar. "Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." Journal of Cyber Security Technology, Vol. 9,No.1(2025), p.37.

الا انه في ظل السيناريو الجيوسياسي الحالي هناك آثار ومخاطر يولدها التقدم التكنولوجي على الاستقرار الجيوسياسي للدولة فالمنافسة العالمية لا تنحصر على التقدم الاقتصادي وانما تمتد لتشمل الأمن السيبراني، الردع العسكري والحوكمة الدولية يضاف اليها مخاطر تقنيات الجيل الخامس والذكاء الاصطناعي. [21،ص3-6،21].

1- تحديد مصادر التهديدات السيبرانية: الجيوسياسية من شأنها تساعد على فهم من اين تأتي منبع التهديدات ولماذا فالجهات الفاعلة الحكومية مثل(روسيا ،الصين ،كوريا الشمالية) وتكتيكاتها الجيوسياسية وقدراتها السيبرانية تعد وسيلة لتحقيق خططها من قوة ونفوذ عالمي دون صراع مباشر اذ ليس من الضرورة ان تستند لمساعي تقنية بل قد تستند لصراعات إقليمية. [21،ص3-6،21].

2- تشكيل تحالفات دفاعية سيبرانية: ان السباق المستمر للتقدم التكنولوجي يعمل على تفاقم التوترات الجيوسياسية بل يُجبر الدول على إعادة النظر في آلية صياغة التحالفات، السياسات الاقتصادية وتأمين الدولة [21،ص3-6،21].مثال/ تعاون اسرائيل مع تحالفات قوية كـ الولايات المتحدة لتعزز أهدافها ونفوذها في المنطقة [16،ص17]. تعد الولايات المتحدة والصين وروسيا، هي في سباق تسلح رقمي فضلاً عن ذلك يعد الفضاء الإلكتروني ميداناً لتحالفات حلف

شمال الأطلسي (الناتو) فهو يمكن أعضائه التصدي الجماعي للتهديدات السيبرانية [17،ص348].

3- التأثير على سياسات الرقابة والسيادة الرقمية: ان السباق التكنلوجي الساعية اليه الدول جعل تحديات الحوكمة العالمية أكثر تعقيدًا فمن نتائج هذا السباق هو صعود السيادة السيبرانية اذ تسعى الدول لفرض سيادتها على فضاءاتها الرقمية بغية حماية مصالحها الوطنية ازاء النفوذ الاجنبي من خلال القدرات السيادية اذ لا ترى الفضاء الإلكتروني منطقةً بلا حدود تمامًا [21،ص15]. مثال/ جدار الحماية العظيم الصيني (GFW) وهو جزء مشروع الدرع الذهبي" العمود الفقري لأكبر نظام رقابة صارمة على الانترنت في العالم[22،ص2] .

4- التحكم في البنية التحتية الرقمية العالمية: من الامور التي تعقد العلاقات الجيوسياسية المعاصرة هو ما ينطوي عليه عسكرة الفضاء في ظل احتدام التنافس بين الدول على بسط نفوذها على الأرض وفي المدار مثال/ مساعي الصين لترسيخ مكانتها الدولية وتعزيز نطاقها الجيوسياسي يتجسد ذلك من خلال التكنلوجيا في مبادرة الحزام والطريق الصينية (BRI) وما تتضمنه هذه البنية التحتية الرقمية كاداة فعّالة لبسط نفوذها من خلال ضخ استثماراتضخمة في مشاريع رقمية في قارّات (آسيا ،أفريقيا وأوروبا) ومن ثمة فهو تفوقاً سيبرانياً واستيراتيجياً. [21،ص36،13].

5- تشجيع التنافس التقني والاقتصادي : ان التحول التكنولوجي عاملًا أساسيًا في بناء السياسة العالمية في السياق الجيوسياسي الحالي فـ صعود شركات تقنية عملاقة كـ (Google and Facebook) وغيرها بمثابة جهات فاعلة رئيسية في الشؤون الجيوسياسية من خلال الادوار الفعالة التي تلعبها في بناء الآراء العامة وتأثيرها على سير الانتخابات مما ولد عدم اليقين في سلطة الدولة وعليه ارتبطت التكنولوجيا ارتباطًا وثيقًا بالجغرافيا السياسية فـ أدوات هذه الشركات تتجسد بـ (مراقبة وتحليلات بيانات) سابقاً كانت حكرًا على الوكالات الحكومية وعليه ولد مخاوف بشأن الخصوصية وسرية المعلومات متجاوزة بذلك الجهات الحكومة لذا يُعد فهم دور هذه الشركات في تشكيل الدبلوماسية والأمن الدوليين أمرًا أساسيًا في الجغرافيا السياسية في وقتنا المعاصر فـ التنافس هو من اهداف هذه الشركات مثال/ المنافسة الأمريكية - الصينية في الذكاء الاصطناعي وتقنية الجيل الخامس والذي يعزز امنها الوطني وتفوقها الاقتصادي. [21،ص2-19].

6- تصاعد الحرب السيبرانية كأداة جيوسياسية: إن تصاعد الهجمات الإلكترونية التي ترعاها البعض من دول العالم تعد أدوات غير مباشرة للأعمال الدبلوماسية والعدائية بغية اضعاف الخصوم دون الخوض في صراع الحروب التقليدية هذه الأنشطة الإلكترونية تُركز على البنية التحتية الحيوية للخصم ، البيانات الحساسة مثال/الانتخابات الرئاسية الأمريكية لعام (٢٠٢٠)[21،ص2-19]. وهذا ما سيتم التطرق اليه لاحقاً ضمن التداعيات على المستوى الدولي.

7- بلورة قوانين دولية جديدة للأمن السيبراني: هناك أهمية قصوى لصياغة القوانين والتعاون الدولي فغياب الأطر القانونية أزاء الحوادث السيبرانية العابرة للحدود تعمل على تفاقم التحديات للدولة او حتى امام المنظمات كجهات فاعلة غير حكومية ساعية لمعالجة تهديدات الأمن السيبراني [23،ص10].

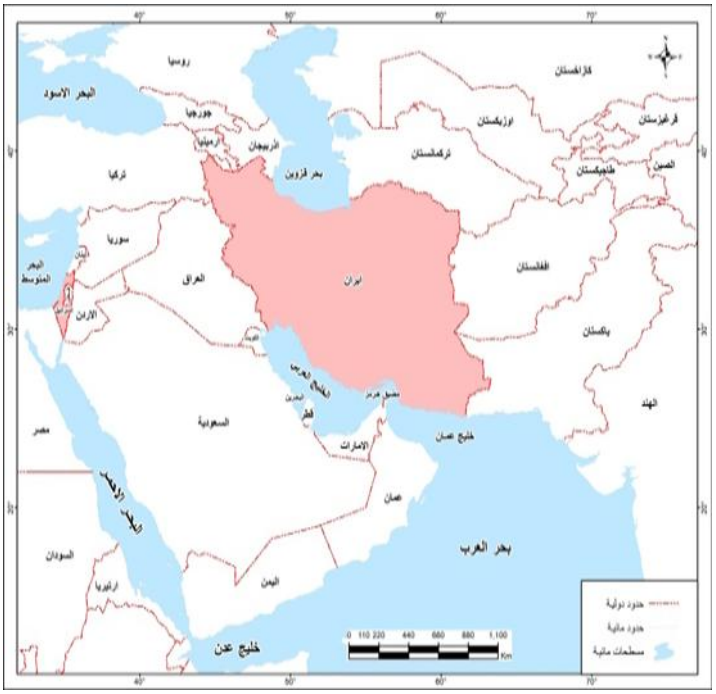
المبحث الثالث: النطاق الجغرافي للحرب السيبرانية الايرانية – الصهيونية

اولاً- الموقع الجغرافي لإيران والكيان الصهيوني في الشرق الأوسط واهميته الاستراتيجية

يمثل الموقع الجغرافي لأي دولة أهمية بالنسبة للدول المجاورة فضلاً عن موقعها بالنسبة للبحار والمحيطات التي تقع عليها تلك الدولة. في حين يمنح الموقع الاستراتيجي الدولة أهمية (محلية، إقليمية ودولية) [24،ص122].وعليه فموقع الدولة الجغرافي يشكل أهمية كبيرة في سلوك الدولة سيما في أوقات السلم والحرب اذ يمكن من خلاله تحديد موقع الدولة المطلق والنسبي[25،ص1].

جغرافياً تقع جمهورية إيران الإسلامية في الشرق الأوسط أي في قارة آسيا[26،ص1]. تبلغ مساحتها الاجمالية حوالي (1.75)مليون كيلومتر مربع، تحدها من الشمال أرمينيا ،أذربيجان ،بحر قزوين وتركمانستان ومن الشرق أفغانستان وباكستان اما من الجنوب خليج عُمان ومضيق هرمز والخليج العربي والعراق وتركيا من الغرب[27،ص1]. **خريطة (1)(ص7).**

خريطة (1) الموقع الجغرافي لإيران والكيان الصهيوني في الشرق الاوسط



المصدر:- من عمل الباحثين بالاعتماد على برنامج ال (GIS) لخرائط رقمية متاحة على مواقع الكترونية عبر شبكة الانترنت.

https://commons.wikimedia.org/wiki/File%3AIran_and_Israel_%28

without_West_Bank_and_Gaza%29.pn

اما فيما يخص الكيان الصهيوني وعلى السياق ذاته الجغرافي اذ تبلغ مساحته الاجمالية حوالي (22,072) كيلومتر مربع فقط اي(8,522) ميلامربعاً ، يحده من الشمال لبنان ومن الشرق سوريا والأردن ومن الجنوب كل من مصر والأردن[28،ص6] .

الا ان الكيان الصهيوني يواجه العديد من المشاكل فجغرافياً يعد دولة صغيرة نسبيًا وافتقاره الكبير للعمق الجغرافي مقارنة بباقي الدول في المنطقة ،فضلا عن وقوع العديد من تجمعاته السكانية بالقرب من الحدود ومن ثَم يجعله عرضة للهجمات، اضف الى ذلك ما يعانيه من مشاكل ديموغرافية كالهجرة العكسية وعدم التوازن السكاني [29 ،ص17-49,19].

اما الأهمية الجيوسياسية للمنطقة وعلى المستوى الاقتصادي يتجسد بامتلاك إيران نسبة (20%) من بحر قزوين ذو الاحتياطيات الهائلة من (النفط والغاز الطبيعي) . ومن زاوية أخرى ان الدول المُطلة على بحر قزوين تُعارض الإيراني لحوالي(12)جزيرة في الخليج العربي[26،ص12]. فإيران تعد لاعبًا رئيسيًا وحيويًا في الشرق الأوسط لامتلاكها ثروة اقتصادية ضخمة فهي تمثل رابع أكبر احتياطيات مؤكدة من النفط الخام في العالم فضلاً عن عضويتها الرئيسية في منظمة الدول المصدرة للنفط (أوبك) حيث تنتج تاريخيًا حوالي(3-4) ملايين برميل يوميًا وفي ذات الصدد هناك علاقات إقليمية ودية تربط بين قطر و إيران من خلال خط أنابيب نفط المعروف باسم (حقل غاز القبة الشمالية) اذ يبلغ انتاج الدولتان يومياً بين(650 -700 ألف) برميل من مكثفات الغاز (النفط الخفيف جدًا) [30،ص148,156].

الأهمية الأخرى تتجسد بأهداف السياسة العسكرية للولايات المتحدة الامريكية في المنطقة اذ أنشأت العديد من القواعد العسكرية والجوية لإقامتها في دول(الخليج العربي كعمان والعراق) وذلك لقرب القواعد من مواقع التهديد الأمني المباشر في منطقة الشرق الأوسط [31،ص2].

يضاف الى ما ذكر انفاً جغرافياً يعد الكيان الصهيوني دولة قريبة من دول الخليج العربي فالأخيرة تُقيم تحالفات مع قوى عالمية كالولايات المتحدة الأمريكية ومؤخرًا مع الكيان. الاولى تدعم حلفائها من دول الخليج بأدوات سيبرانية متطورة مدعومة بالذكاء الاصطناعي مثال/ أُنشئت جامعة محمد بن زايد للذكاء الاصطناعي لتعزيز البحث والتطوير بغية مواجهة التهديدات الأمنية. [30،ص148-149].

فمن خلال ما ذكر انفاً يتضح ان الدولتين كلاهما يقعان في ذات النطاق الجغرافي في قارة اسيا فالكيان الصهيوني يقع في منطقة مهمة وهي منطقة قلب الشرق الأوسط ولكون الكيان يعاني من صغر المساحة وعزلة في العلاقات لذا عمدت تبني سياسة الأمن السيبراني لتعويض خلل التوازن هذا وهذا ما سيتم تناوله في مسار البحث .

ثانياً- الهجمات السيبرانية الإيرانية –الصهيونية

يُعدّ الصراع الإيراني- الصهيوني صراعًا متعدد الأوجه من حيث (الهجمات الالكترونية ، التجسس الإلكتروني وتعطيل البنية التحتية الحيوية والرقمية ... الخ) وعليه فهو احد الدوافع الرئيسية للتوترات الجيوسياسية في الشرق الأوسط الاخير يمثل عاملًا مهمًا في الجغرافيا السياسية للمنطقة اذ ان الدولتين كقوتين فاعلتين تسعيان لبسط نفوذهما في المنطقة من خلال تعزيز تقنياتهما المتمثلة بالأمن السيبراني والذكاء الاصطناعي [30،ص148-149]. فهما يتبادلان الهجمات في الفضاء الإلكتروني الا انه يصعب تحديد مصدرها على اعتبار انها تتم دون تبني احدهما مسؤوليتها أو إنكارها[32،ص46].

هناك خصومًا رئيسيين من الدول تستهدفهم الهجمات الإلكترونية الإيرانية الاول يتجسد بالكيان الصهيوني ومالكي النفط في شبه الجزيرة العربية على الصعيد الإقليمي الشرق اوسطي ، والثاني الولايات المتحدة على صعيد الامن العالمي وهذا ما سيتم التطرق اليه ضمن التداعيات على مستوى النطاق العالمي [18،ص281].

فإيران عززت نهجها الاستراتيجي لدى الشرق الأوسط الأخير يضم(حماس ،حزب الله والحوثيين يضاف اليهم الحرس الثوري الإسلامي) [30،ص154]. ناهيك عن الفصائل الفلسطينية هؤلاء تم توظيفهم كـ جماعات **بالوكالة** لغرس القواعد الايرانية في اللعبة الدولية فهم فواعل غير دولية غالبًا ما تزاول نشاطها من ميادين أخرى تحظى بعلاقات سلمية وودية مع الكيان الصهيوني مثل (مصر والأردن) الامر الذي يعيق الكيان من الحد من هكذا جماعات [16،ص22-28].

ايران وابان الحرب الأهلية السورية دعمت حزب الله ونظام الأسد اذ منحت الجماعات الخارجة عن القانون رواتب تصل لـ (200 -300) دولار في حين رواتب الفصائل المحلية مثل لواءي نبل والزهراء تصل الى دون (100) دولار شهريًا هذا التواجد الايراني في سوريا يعد بوابةً إلى لبنان لـ إمداد ودعم حزب الله بالأسلحة و بقوة ومدربة تدريبًا جيدًا تتوافق مع الاستراتيجية الإيرانية [30،ص 156].

ان المصدر الرئيسي للتوتر بين الدولتين **الأول** يتجسد بالدعم (المالي والعسكري واللوجستي لجماعات مثل حزب الله في لبنان وحماس في غزة) ،في حين ان **الثاني** كان أزاء البرنامج النووي الإيراني على اعتباران ايران ساعية لتطوير أسلحتها النووية لاكتساب نفوذها على الصعيد الإقليمي فديناميكيات الحروب الإلكترونية بين الدولتين لها مخلفاتها الكبيرة على الجغرافيا السياسية للشرق الأوسط فهي ذات علاقة معقدة بين قوتين عظميين تتنافسان على النفوذ والهيمنة في المنطقة [32،ص 50]. وفيما يلي ابرز الهجمات التي شنها الجانبين للمدة (2010-2025) وكالاتي :-

1- نموذج الهجمات السيبرانية الإيرانية

الكيان الصهيوني يمتاز بقلة عدد وكثافة سكانهاه وعليه فإن نجاح أي هجوم إيراني سيبراني على البنية التحتية الحيوية فيها له تأثير مضاعف عما لو حدث في

الدول الأكبر فضلاً عن موقعها من الشرق الأوسط مما يجعلها في مرمى للنفوذ الإيراني [33،ص1141]. فمن ابرز الهجمات الإلكترونية الايرانية كانت على البنية التحتية للمياه والصرف الصحي **"نظام المياه"** التابعة للكيان نفذ يومي(24 و25) أبريل عام (2020) [32،ص46].ثم في عام (2018) اخترق قراصنة إيرانيون الهاتف المحمول لرئيس أركان جيش الدفاع الصهيوني "غانتس"[34،ص 2].

اما عام (2020) شنت ايران هجومًا إلكترونيًا على نظام التحكم **(SCADA)** في الكيان الصهيوني المسؤول عن مستويات الكلور في المياه و معالجتها لجعلها آمنة للاستهلاك البشري بهدف الهجوم لرفع مستوى الكلور وهو مادة كيميائية فلو أُضيف بتركيز عالٍ سيُشكل ذلك تهديدًا صحيًا للسكان الا ان حكومة الكيان الصهيوني اتخذت إجراءات آنية للحد منه [30،ص154] . وفي ابان عام (2021) تم استهداف (باحثين طبيين صهاينة، وكالات حكومية، وأوساطًا أكاديمية) [34،ص2]. فضلاً عن الحملة الإلكترونية المتتالية ضد (البنوك والمؤسسات المالية الصهيونية) بالاعتماد على البرمجيات الخبيثة التقليدية وهجمات حجب الخدمة الموزعة **(DDos)** بغية فرض ضغوط كحرب اقتصادية [33،ص1143].

عام (2023) استهدفت إيران **أنظمة رادار** تابعة للكيان بعد الحرب مع حماس فضلاً عن أنشاء الاستخبارات الإيرانية عمليات **لانتحال حسابات** في التواصل الاجتماعي مثال/ حساب يُدعى **"دموع الحرب"** لناشطين صهاينة ينتقدون تعامل رئيس الوزراء بنيامين نتنياهو مع أزمة احتجاز حماس لعشرات الرهائن و حساب يُدعى "كارما" لإسرائيليين يمثلون وهم يطالبون استقالة نتنياهو[32،ص53].

مؤخراُ اندلع صراع متبادل في13 حزيران من هذا العام (2025) الا ان الهجمات كانت ذو **مردود نفسي** تضمنت رسائل تضليل إلكترونية مثال/ ان محطات الوقود ستنفد ابان (24) ساعة فضلاً عن تفجير ملجأ للكيان [35،ص3] .

2- نموذج الهجمات السيبرانية للكيان الصهيوني

نفذ الكيان الصهيوني عام (2010) عملية ستاكسنت **"Stuxnet"** الاكترونية استهدفت مصنع اليورانيوم الإيراني لردع وانذار إيران[30،ص153]. منشأة نطنز لتخصيب اليورانيوم احدى المنشآت المتضررة من دودة ستوكسنت في منطقة الشرق الأوسط دمرت حوالي (984) جهاز طرد مركزي لتخصيب اليورانيوم أدى لانخفاض بنسبة(30%) من كفاءة التخصيب [32،ص46] . وفي ذات المقام قام الموساد عام (2018) بتسريب مئات الآلاف من الوثائق من أرشيف نووي سري سعياً لتعطيل المفاوضات النووية بين إيران والقوى العالمية الخمس زائد واحد (الولايات المتحدة وروسيا والصين وفرنسا وبريطانيا، فضلاً عن ألمانيا)[34،ص3] .

وفي عام (2020) شنت الكيان الصهيوني هجومًا إلكترونيًا آخر على ميناء الشهيد رجائي في بندر عباس جنوب إيران في (9 مايو عام 2020) وهو رداً على الهجوم الإلكتروني الإيراني المشار اليه انفاً أزاء البنية التحتية للمياه والصرف الصحي "نظام المياه" لدى الكيان الصهيوني[32،ص46].

في 17 من الشهر حزيران عام (2025) اخترقت إسرائيل ومن خلال **"العصفور المفترس" بنك "سباه"** الإيراني الحكومي نجم عنه تلف بياناته وانقطاع في الخدمة. وبعد يوم تم اختراق منصة "نوبيتكس" لتداول العملات الرقمية اذ سرق حوالي(81.7) مليون دولار [35،ص1-2]. الغاية هي إحداث (فوضى مجتمعية، زرع القلق للحكومة المعنية فضلاً عن الضغط عليها لاتخاذ قرار معين) وهو أداة ابتزاز لفرض تنازلات (سياسية أو اقتصادية أو استراتيجية) [18،ص282].

ثانياً- تداعيات الحرب السيبرانية الإيرانية -الصهيونية على الأمن الإقليمي

شهدت منطقة الشرق الأوسط تصاعداً مقلق للتوترات الإقليمية حيث تعد إيران والكيان الصهيوني قوتين مُهيمنتين تتنافسان لامتلاك أسلحة نووية [16،ص25] .نجم تفاقم هذا التنافس جراء الموقع الجغرافي الذي تتمتع به المنطقة ولقربها من أهمّ احتياطيات النفط والغاز في العالم اذ بلغت الهجمات الالكترونية نسبة(800%) للمدة (2016 -2020) بحسب تحليل شركة رايثيون الامريكية للاستخبارات والفضاء [36،ص393] .وفيما يلي اهم التداعيات:-

1- باتت الهجمات السيبرانية المتبادلة تزعزع الامن الاقليمي اذ تشكل مصدر قلق وتوتر واستنفار امني لدول الخليج والدول المجاورة اذ ومن البديهي ان تكون عرضة أمام الهجمت الإلكترونية مثال/ الهجوم السيبراني الإيراني "شمعون" على شركة **(أرماكو)** السعودية عام (2012) اذ اخترق الفيروس حوالي (30) ألف جهاز كمبيوتر سعودي [30،ص146-154]. الذي اوقف أكبر شركة منتجة للنفط في العالم[18،ص 280].

2- عززت دول الخليج تعاونها مع قوى عالمية ك (بريطانيا ،فرنسا والولايات المتحدة)في مجال الأمن السيبراني .مثال /التعاون الرقمي الإماراتي- الصهيوني للتصدي لفيروس الفدية لمهاجمته المؤسسات المالية الإماراتية (البنوك)وشركة النفط الإماراتية. مثال آخر / اتفاقية "إبراهيم" عام(2020) المبرمة ايضاً بين الإمارات العربية المتحدة يضاف اليها البحرين مع الكيان الصهيوني تحت ذريعة دعم التطبيع العربي الإسرائيلي وحماية أمن واستقرار المنطقة الا انها في واقع الأمر تسعى **اولاً** لـ تسهيل التنمية الاقتصادية لتعويض مصادر التدخل الدولي مثل (روسيا ،الصين وإيران) **وثانياً** التعاون بمجالات (الزراعة ،الدفاع ،الذكاء الاصطناعي والأمن السيبراني) دفع ايران لتكثيف تحالفها الاقتصادي والتكنولوجي مع (الصين وروسيا) فضلاً عن النفط و أمن الطاقة مما اسهم بربط الصراع السيبراني بالمحاور الجيوسياسية في المنطقة .

3- عسكرة الفضاء السيبراني الذي اضحى ساحة للصراع دفع دول المنطقة لتوسيع قدراتها الدفاعية الاستثمارات الضخمة للتقنيات السيبرانية عوضاً عن التوجه لمعالجة التحديات المحلية داخل الدولة مما يولد استياء محلي مثال/ الميزانية العسكرية للمملكة العربية السعودية هي الأعلى في العالم المخصصة حتى (2030) بدلاً من انفاقها في البنى التحتية الرئيسية في المقابل تفتقر دول ك (سوريا

واليمن) للقدرات السيبرانية ومن ثمة فهي عرضة للتهديدات السيبرانية مما يخلق سباق للتسلح السيبراني [30،ص147-156].

4- استهداف البنى التحتية الحيوية الأساسية شبكات الكهرباء والاتصالات والنقل والأنظمة المالية وغيرها من الخدمات الأساسية ومن ثمة يولد هذا قلق للمدنيين من ان يكون ضحايا غير مباشرين[18،ص 275-280].

5- الفضاء السيبراني اسلوب ردع بدل المواجه العسكرية اذ باتت ايران والكيان الصهيوني تتبنى الأساليب السيبرانية مثل(هجماتDDOS،مقاطع فيديو مفبركة لشخصيات سياسية ومؤثرة) وهذا يعد تحول واضح في طبيعة الصراع. [30،ص156].

6- الاقتصاد الرقمي وتقويض ثقة المستثمرين الأجانب مثال/ تعاون الإمارات العربية المتحدة مع الشركة الصينية لتقنيات الذكاء الاصطناعي(G42) في أبوظبي الا ان الشركة سحبت استثماراتها بالكامل ومن ذلك حصة تُقدر بـ (100) مليون دولار لدى شركة (ByteDance) المطورة لتطبيق (TikTok) ازاء اختراق برنامج التجسس الصهيوني "بيغاسوس" لبيانات مجموعة من الصحفيين والمحامين المشهورين والمؤسسات الإعلامية[30،ص151].

ثالثاً- تداعيات الحرب السيبرانية الإيرانية-الصهيونية على الأمن الدولي

يخضع الأمن الدولي لمهددات العمليات الإيرانية السيبرانية إلى جانب (روسيا ،الصين وكوريا الشمالية) فهؤلاء جميعاً يسعون لتعميق نفوذها والحفاظ عليه لتحقيق عدم استقرار النظام السياسي الأمريكي والدول الحليفة له [18،ص 272].

1- عملية 'Stuxnet' برعاية الـ جهود الإسرائيلة- الأمريكية لتدمير مجمع التخصيب النووي الإيراني حفزت إيران لـ تطوير اساليبها السيبرانية الانتقامية [37،ص2042]. حملة من الهجمات الإلكترونية الايرانية ضد القطاع المالي الأمريكي فضلاً عن سيطرتهم على احد سدود نيويورك الا ان الولايات المتحدة الامريكية ، فضلاً عن تهديدات الفدية في ديسمبر(2015) استمرت (34) شهرًا و بخسائر حوالي (30مليون دولار) استهدفت (مائتي كيان ،مستشفيات ،هيئات حكومية محلية ومؤسسات عامة) لدى الولايات المتحدة[18،ص 281].

حزمة أخرى للهجمات امتدت بين الاعوام (2013 – 2017)اذ شملت (300جامعة لـ 22 دولة، 47شركة قطاع خاص، منظمات حكومية وفيدرالية والأمم المتحدة فضلاً عن اليونيسف) الهجمات تعود لـمعهد مابنا الإيراني اخترقت بيانات أكثر من (31تيرابايت) من حسابات أساتذة الضحايا في قطاعات علمية مختلفة .تضليل إعلامي استهدف الانتخابات الرئاسية الأمريكية لعام (2020) بغية تقويض الثقة في نزاهة النظام الانتخابي الأمريكي يعمل القراصنة مع شركة "إمينيت باسارغاد" الامريكية ومحاولتهم اختراق مواقع التصويت [18،ص 281].

2- تعد الولايات المتحدة الامريكية والدول الأوروبية دول داعمة للكيان الصهيوني على الصعيد (العسكري ،الاستخباري ،الصناعي والتقني السيبراني) [30،ص 153].الامر الذي دفع ايران الى تعزيز تعاونها السيبراني مع دول أخرى مثل (روسيا والصين) لزيادة كفاءتها التقنية [16،ص 41] .

3- التهديدات السيبرانية ولدت حوافز للتعاون متجاوزة الانقسامات السياسية التقليدية انخرطت القوى الخارجية بتعاون إقليمي متعدد الاطراف منها (الولايات المتحدة، روسيا والصين) مثال/الشراكة الإسرائيلية- الامريكية للتعاون الإقليمي في مجال الأمن السيبراني[33،ص1151-1153].

الاستنتاجات: -

1- بات الامن السيبراني بعداً جديداً يضاف لأبعاد قوة الدولة التقليدية " الجوية والبرية والبحرية".

2- ان تقنية الأمن السيبراني تعد ميدانًا للحروب الجيوسياسية عبر هجمات رقمية عابرة للحدود الجغرافية التقليدية .

3- بإيران والكيان الصهيوني قوتان تمتلكان "برامج نووية" متطورة وعليه لهما ثقلهما في موازين القوى اقليماً ودولياً اذ يسعى كل طرف منهما للتغلغل في الاخر واضعافه من خلال التفوق في القدرات السيبرانية.

4- يسعى الكيان الصهيوني لقطع الامدادات العسكرية والمالية مع وكلاء ايران في المنطقة مثل (سوريا ،حزب الله في لبنان وجماعات في غزة) فضلاً عن سعيه للإضعاف البرنامج النووي الايراني.

5- ايران ذات عمق استراتيجي في المنطقة مقارنة بخصمها الكيان الصهيوني الذي يفتقد لهذا العمق لذا لجئ الكيان لتبني القوة السيبرانية لمعالجة هذا الفقد وبسط نفوذه.

6- يستمد الكيان الصهيوني تفوقه التكنولوجي من تحالفاته الامريكية في المقابل ايران تعزز قوتها وكفاءتها مع دول منافسة لهذه التحالفات .

7- تسعى ايران من خلال تبنيها للقوة السيبرانية هو بهدف الضغط الغير مباشر لرفع العقوبات الاقتصادية المفروضة عليها.

المصادر:-

1- Akyesilmen, Nezir, Geopolitical Implications of Cyberspace on International Relations: Anindepth Analysis, Selçuk University.
https://www.tuba.gov.tr/files/yayinlar/bilim-ve-dusun/TUBA-978-625-6110-04-
https://doi.org/10.53478/TUBA.978-625-6110-04-5.ch36
5_ch36.pdf?utm_source=chatgpt.com
2- Khan, Zeeshan Faisal, "Cyber Warfare and International Security: A New Geopolitical Frontier." The Critical Review of Social Sciences Studies

CONTEMPORARY SECURITY POLICY, Geschwister-Scho, LMU, Munich, Germany,Vol. 46, No. 3(2025).
https://doi.org/10.1080/13523260.2025.2474867

12- Appazov, Artur , Legal Aspects of Cybersecurity, University of Copenhagen, Faculty of Law, (2014).
https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf?utm_source=chatgpt.com

13- Cobos ,Estefania Vergara, Cakir, Selcen , A Review of the Economic Costs of Cyber Incidents, Washington, DC: World Bank,(2024).
https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf?utm_source=chatgpt.com

14- Andrade, Tiago Negrão ,de et al, "Cybersecurity in the Digital Era: Geopolitical Impacts and Structural Challenges", IOSR Journal Of Humanities And Social Science,No.30, Issue 1,(2025)
https://DOI: 10.9790/0837-3001063044

15- Iqbal, Muhammad Jawed, et al, "The Role of China-Pakistan Relations in the Global Tech Competition, Especially in Areas like 5G, AI, and Cybersecurity." Review of Education, Administration & Law ,Vol. 8,No.1 ,(2025). DOI: https://10.47067/real.v8i1.404

16- Vilinskiy , Egor Nikolaevich, Defence strategies in the digital space: the case of Israel. MS thesis. Universidad do Minho (Portugal), (2024).
https://repositorium.uminho.pt/bitstreams/6623e9c2-1ae9-4d40-abac-2f648a297031/download?utm_source=chatgpt.com

17- Khan, Aneel Waqas, et al,"CYBERSECURITY AS A GEOPOLITICAL TOOL: THE GROWING INFLUENCE OF DIGITAL WARFARE IN STATECRAFT." International Research Journal of Social Sciences and Humanities, Vol. 03, Issue.02, (2024).
https://doi.org/10.5673/irjssh.2024.0302.0201

18- Stachoń, Monika , "IRANIAN CYBER Vol.3.No.2, (2025).
DOI: https://doi.org/10.59075/k9cbhz04

3- Shakeelm, Muhammad Bilal, et al ,"THE ROLE OF CYBER SECURITY IN INDO-PACIFIC GEOPOLITICS, Journal of Media Horizons, Vol. 6, Issue. 2, May (2025).
https://doi.org/10.5281/zenodo.15401012

4- BOUKARRITA, Badreddine, "National Cybersecurity: A New Evolving Concept." Legal and Political Research, University of Jijel (Algeria, Vol .10, N°0.1,(2025).

5-Radanliev, Petar,"Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." Journal of Cyber Security Technology ,Vol.9.No.1 (2025).
https://doi.org/10.1080/23742917.2024.2312671

6- Aryasatya ,Idden , Daryanto Eko, "Cyber Warfare And Its Place In Modern Geopolitics And War." Security Intelligence Terrorism Journal (SITJ) Vol.2.No.1, (2025).
doi: https://doi.org/10.70710/sitj.v2i1.31

7 - المشهدي ،تغريد معين حسن ،الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، جامعة الكوفة كلية الآداب مجلة البحوث الجغرافية، العدد 3، 2020.

8- Muhammad, Hatim, et al,"Bridging Firewalls and Foreign Policy: The Role of Cybersecurity in Shaping International Diplomacy." Social Science Review Archives ,Vol. 3.No.2, April-June, (2025).
DOI: https://doi.org/10.70670/sra.v3i2.752

9- المحمود ،خالد وليد ، الفضاء السيبراني وتحولات القوة في العلاقات الدولية، المركز العربي للأبحاث ودراسة السياسات ,ط 1، بيروت، 2025.

10- Singh, Nistha Kumari, et al, "Navigating the nexus: geopolitical, international relations and technical dimensions of US-China cyber strategic competition." Cogent Social Sciences ,Vol. 11,No.1, May (2025).
https://doi.org/10.1080/23311886.2025.2499171

11- Weiss, Moritz and Nicolas Krieger, The political economy of cybersecurity :Governments, firms and opportunity structures forbusiness power,

2018/en/English_ABOUT_ISRAEL_PDF_Israel-the%20Land%202018.pdf
29- Shelah, Ofer , et al ,The State of Israel's National Security: Doctrine and Policy Guidelines for 2025–2026, The Institute for National Security Studies, Tel Aviv,2025.
30- Haroon, Ayesha "AI and Cyber Drove Warfare in the Israeli-Iran Conflict and its Impact on Gulf States' Security." Journal of Politics and International Studies ,Vol. 10,No.2, (2024).
https://doi.org/10.46601/jpis.2024.10.2.1387
31- brahim, Abdul-Jabbar Ismael, THE AMERICAN MILITARY PRESENCE IN THE ARAB GULF REGION, International Journal of Research in Social Sciences and Humanities, Vol. No. 10, Issue No. II,(2020).
32- Amaliya, Laila Rizky,"A Cyber War of Iran-Israel: A Geopolitical Rivalry." International Conference on Strategic and Global Studies (ICSGS 2024). Atlantis Press,(2025).
https://doi.org/10.2991/978-94-6463-646-8_4
33- Arshad, Muhammad Hammad, "US-Iran Cyber war and its impact on Israel." Wah Academia Journal of Social Sciences ,Vol.4,Issue.1, (2025).
34- Schanzer , Jonathan,"The quiet war between Israel and Iran." Middle East Quarterly ,Vol.3,No.1, (2023).
35- Radware, Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel-Iran War, (2025).
https://www.radware.com/getattachment/5e4a87dc-39db-46ff-914c-92086def7c64/Threat-Advisory-June-18-Israel_Iran-Cyberthreat-update-June-2025.pdf.aspx
36- Othman, Srbaz Nidham, et al. "The impact of cybersecurity law in the middle east." Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico ,No.23, (2025).
https://doi.org/10.5281/zenodo.14291287
37- Umar, Muhammad ,Iran and Israel Cyber Warfare and Interference of US, SOCIAL SCIENCE REVIEW ARCHIVES, Department of Political Science University of Management and Technology, Volume. 3, No. 2,(2025).
CAPABILITIES AS A TOOL OF DOMESTIC AND FOREIGN POLICY." Scientific Reports of Fire University ,Vol.2,No.89 ,(2024).
https://DOI: 10.5604/01.3001.0054.4537
19- Israfilov Anar,"Geopolitical aspects of cybersecurity: international cooperation and conflicts." Холодная наука,Vol. 8, (2024).
20- عبد المحسن, ضياء محمد ، الجغرافية البوليتيكية، مطبعة المناهل،2016
21- Chari, Srinivasan Gopal, "Power, Pixels, and Politics: The Geopolitics of Emerging Technologies in the Digital Age." London Journal of Research In Humanities and Social Sciences ,Vol.25,Issue.2, (2025). https://doi.org/10.9790/0837-2502063044
22- Tang, Chao, In-depth analysis of the Great Firewall of China,(2016).
https://www.cs.tufts.edu/comp/116/archive/fall2016/ctang.pdf?utm_source=chatgpt.com
23- Aisha, Adeyeri and Abroshan, Hossein ,"Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era." Information, Vol. 15.No.11, (2024).
https://doi.org/10.3390/info15110682
24 -المومني, محمد أحمد عقلة ، استراتيجيات سياسة القوة مقومات الدولة في الجغرافية السياسية، دار الكتاب الثقافي، الأردن- اربد،(2008).
25- W. Wile ,David ,Introduction to World Regional Geography ,(2019).
https://pressbooks.pub/worldgeography/chapter/12/?utm_source=chatgpt.com
26- Rob Gilmore,(2014).
https://bpb-us-w2.wpmucdn.com/u.osu.edu/dist/9/1401/files/2014/03/Iran-1lpu29s.pdf
27- FAO Country profile – Iran (Islamic Republic of),food and Agriculture Organization of the United Nations ,(2008).
https://openknowledge.fao.org/server/api/core/bitstreams/e0d3e709-26fc-43c4-910b-9ee29b588e69/content
28- Facts About Israel – Israel in Perspective, State of Israel, Ministry of Foreign Affairs, (2018).
https://www.gov.il/BlobFolder/generalpage/facts-about-israel-