الترميز الدولي / ISSN (P) :2710-2653
ISSN (E) :2960-253X /
رقم الايداع الوطني / 2375 /2019

تاريخ استلام البحث : ٢٠٢٦/٦/٣
تاريخ قبول البحث : ٢٠٢٦/٨/١٢
تاريخ النشر : ٢٠٢٦/٩/٣٠

# القدرات السيبرانية الإيرانية وأثرها في اليقظة الرقمية: المواجهة الإيرانية–الأمريكية–الإسرائيلية أنموذجًا (٢٠٢٣–٢٠٢٦)

# Iranian Cyber Capabilities and Their Impact on Digital Vigilance: The Iranian–American–Israeli Confrontation as a Case Study (2023–2026)

م.د. آيات احمد سلمان الحسيني
**Lecturer . Dr Ayat Ahmed Salman Al-Husseini**

الجامعة المستنصرية- كلية العلوم السياسية
Al-Mustansiriya University - College of Political Science
Ayat-ahmed@uomustansiriyah.edu.iq

**IRAQI**
Academic Scientific Journals
https://iasj.rdd.eedu.iq/journals/journal/view/229

**الملخص:**

تتناول الدراسة القدرات السيبرانية الايرانية وإنعكاساتها على الحرب الصهيو– امريكية على الجمهورية الاسلامية الايرانية للفترة ٢٠٢٣–٢٠٢٦ بدءاً من الحرب بالوكالة عن طريق محور الممانعة والذي يشمل كل من لبنان واليمن والعراق وفلسطين بإوجهها المتعددة وصولاً للدخول في المواجهة المباشرة مع الولايات المتحدة الامريكية والكيان الصهيوني، فضلاً عن ضرب المصالح الامريكية في بعض الدول الخليجية، تسعى الدراسة الاجابة عن إشكالية محورية مفادها: كيف طورت إيران قدرتها السيبرانية الاستباقية في الاطار الاستراتيجي، وما آثرها على موازين القوى الاقليمية؟ وتنظلق من فرضية أيران تحولت خلال السنوات المنصرمة من نموذج الردع السيبراني الدفاعي – الانتقامي لنموذج الاستباق الهجومي متعدد المساحات، مستثمرةً بذلك شبكة وكلائها الاقليميين لتجاوز القيود التقنية وتحقق افضلية استراتيجية خاصة بها، إعتمد الدراسة المنهج التاريخي والوصفي التحليلي فضلاً عن منهج دراسة الحالة المقارن والمؤسسي، وتوصلت لجملة من النتائج ابرزها: القدرات السيبرانية تعمل وفق منطق " الكفاءة الانتقائية غير المتكافئة" وشبكة وكلائتها الرقميين تجسد ميزتها الاستراتيجية الحقيقية على الرغم من الحدود التشغيلية، أما معضلة الاسناد القانون تبقى سلاحاً ذو حدين.

**الكلمات المفتاحية:** القدرات السيبرانية، اليقظة الرقمية، الولايات المتحدة الامريكية، الكيان الصهيوني ، الجمهورية الاسلامية .

## Abstract:

The study examines the Iranian cyber capabilities and their implications for the Zionist war- The study seeks to answer a central problem: How has Iran developed its proactive cyber capability in

the strategic framework, and what impact has it had on the regional balances of power in the region, starting with the proxy war through the axis of resistance, which includes Lebanon, Yemen, Iraq and Palestine in its multiple directions, to enter into direct confrontation with the United States and the Zionist entity, as well as Iran has shifted over the past years from a defensive cyber deterrence model – The study adopted the historical and descriptive analytical approach as well as the comparative and institutional case study approach, and reached a set of results, the most prominent of which are: cyber capabilities operate according to the logic of "selective unequal efficiency" and its network of digital agents embodies its real strategic advantage despite operational limits, but the dilemma of attribution law remains a double-edged sword.

**Keywords:** Cyber capabilities, digital vigilance, the United States of America, the Zionist entity, the Islamic Republic.

**المقدمة:**

منذ عام ١٩٧٩ وقيام الثورة الاسلامية، واجهت ايران العديد من الازمات التي أثرت على امنها القومي، إلا إنها عبر سنوات من الاجتهاد تمكنت من تطوير إمكانياتها المادية و مواكبة الدول المتطورة في الفضاء السيبراني من خلال إنشاء منظومة متشابكة لقدراتها السيبرانية واستطاعت من توظيف تلك القدرات مجال اليقظة الاستخباراتية الرقمية و وصلت لمراحل مهمة في هذا المجال وحققت الكثير من المكاسب، وبدا ذلك جلياً خلال الحرب الصهيو– امريكية على ايران منذ ٢٠٢٣ ولغاية ٢٠٢٦، إذ تمكنت من استخدام الفضاء السيبراني وجمع المعلومات ورصد الهجمات والتاثير على الراي العام وإنشاء مجموعات خاصة تعمل ضمن نطاق الحرس الثوري لتنفيذ علميات تعنى بمتابعة العملاء

خارجياً وداخلياً وتحديد مواقعهم الجغرافية، واظهرت تلك الفترة التطور الكبير في حجم تلك القدرات إلا إنها تحتوي في طياتها مكامن اخفاق يسهل تحديده، خاصة في مجال التوازن والمقارنة مع قدرات الولايات المتحدة الامريكية و(الكيان الصهيوني) الذي تمكنوا من ربط القدرات السيبرانية بالذكاء الاصطناعي مما ولد لهم كفاءة عالية متميزة ولم تتمكن الجمهورية الاسلامية الايرانية من الوصول لعتبة التفوق الاستراتيجي، إلا إنها مازالت تمتلك صفة القوة الاقليمية التي لايمكن الاستهانة بها على الرغم من ان الخصم يحاول أثبات بإنهم تمكنوا من اسقاط قوتها الاقليمية.

## اهمية البحث:

تكمن اهمية الدراسة من خلال محاولتها لملئ فجوة بحثية حقيقية في الادبيات الاكاديمية من خلال تقديم دراسة تربط ثلاثة متغيرات بإطار موحد ( القدرات السيبرانية واثرها في تحقيق التفوق السيبراي الايراني خلال المواجهة الحالية ضد الهجمات الصهيو– امريكية بتوظيفها إطارة نظرياً مزدوجاً يجمع بين نظرية الردع والحرب الهجينة لتحليل ظاهرة سيبرانية إقليمية متشابكة.

## إشكالية البحث:

تنطلق إشكالية الدراسة من الفجوة التحليلية في الادبيات الاكاديمية بين مستوى النشاط السيبراني الايراني الموثق وغياب الدراسة الرابطه له ولأثره بتحقيق التفوق في ميادين الحرب ومجالاتها للفترة ٢٠٢٣–٢٠٢٦ تحديداً، لذا تطرح إشكالية محورية تتمثل بـ: كيف وظفت الجمهورية الاسلامية الايراني قدراتها السيبرانية كأداة أستباق إستراتيجي وردع

إحترازي في أطار الحرب الفعلية ٢٠٢٣–٢٠٢٦ وماهو حجم أثر ذلك على ديناميكيات الامن الاقليمية؟ مُشْكلةً بذلك أسئلة فرعية مثل:

١. بماذا تتميز القدرة السيبرانية الاستباقية للجمهورية الاسلامية على نموذج الردع الدفاعي في الفترة المنصرمة؟
٢. ماهو أثر إغتيال قائد فيلق قدس الجنرال قاسم سليماني بعام ٢٠٢٠ وطوفان الاقصى على الاستراتيجية السيبرانية الايرانية؟
٣. مادور شبكة الوكلاء الرقميين لأيران في تضخيم قدرتها الاستباقية وتوزيعها على الاقاليم المتعددة؟
٤. ماهي حدود الفاعلية التشغيلية للمنظومة السيبرانية الايرانية وأثرز ثغراته البنية التي تكشف عنها شواهد الفترة المحددة بالدراسة؟
٥. كيف اسهمت اليقظة السيبرانية الايرانية بتوجيه و صد الهجمات الامريكية تجاهها؟

## فرضية البحث:

تنطلق الدراسة من فرضية مفادها إن الجمهورية الاسلامية الايرانية غيرت في إطار الحرب الممتدة للفترة مابين ٢٠٢٣ ولغاية ٢٠٢٦ من نموذجها الخاص بالردع السيبراني الدفاعي – الانتقامي للاستباق السيبراني الهجومي متعدد المساحات، مستثمرة بذلك شبكة وكلائها الاقليميين لتجاوز القيود التقنية وتحقيق ميزة أستراتيجية اتصفت بالكفاءة الانتقائية غير المتكافئة.

## منهجية البحث:

إنطلاقاً من السعي لتحقيق النتائج البحثية المرجوة إستكمالاً للحالة المدروسة يتحتم علينا الاستعانة بمزيج منهجي يقوم على مناهج متعددة، بدءاً من المنهج التاريخي ومروراً

بالوصفي التحليلي و وصولاً بالمنهج المؤسسي الذي يعتمد على تحليل المؤسسات السيبرانية الايرانية.

**حدود البحث:**

-**الحدود الزمانية :** الفترة من ٢٠٢٣ ولغاية ٢٠٢٦.

- **الحدود المكانية :** منطقة الشرق الاوسط بإعتبارها الساحة الجيوسياسية للحرب.

## المبحث الاول : الاطار النظري والمفاهيمي:

تعتبر الاطر النظرية المفاهيمية في حقل العلوم السياسية وتحديداً النظم السياسية من ابرز الادوات المعرفية لفهم وتفكيك المصطلحات السياسية الخاصة بالدراسة، لما لها من خصوصية لتشريح الربط الحاصل بين المتغيرات الدراسة مما يضفي معرفة أساسية للمتلقي.

**المطلب الاول: مفهوم القدرات السيبرانية:**

أصبحت القوة السيبرانية إحدى الركائز الرئيسة للقوة الوطنية الشاملة في القرن الحادي والعشرين، بعد أن فرض الفضاء السيبراني نفسه بوصفه ميداناً جديداً للتنافس والصراع بين الدول. ولم تعد عناصر القوة التقليدية وحدها كافية لتفسير موازين القوى الدولية، بل أضحت القدرة على امتلاك البنية التحتية الرقمية وحمايتها واستثمارها في تحقيق الأهداف السياسية والعسكرية والاقتصادية معياراً أساسياً لقياس مكانة الدولة ونفوذها في النظام الدولي. (زروقة.٢٠١٩)

وتعرف القدرات السيبرانية بأنها "خليط من الامكانيات البشرية والتقنية المؤسسية التي يمتلكها الفاعل وتمكنه من حفظ البنية الرقمية الخاصة به من خلال إدارة العمليات

السيبرانية الاستخباراتية الدفاعية والهجومية فضلاً عن أدارة تلك المخاطر، الامر الذي يحقق الاهداف الامنية والقومية" (Klimburg 2012) .

يعد جوزيف.س ناي( Nye.S Joseph) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها ": القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لايجاد مزايا للدولة، والتأثير على الاحداث المتعلقة بالبيئات التشغيلية الاخرى وذلك عبر أدوات سيبرانية". (زروقة. 2019)

وتعرف وزارة الدفاع الأمريكية القدرات السيبرانية بأنها "مجموعة الإمكانات التقنية والبشرية والتنظيمية التي تُستخدم لتنفيذ العمليات في الفضاء السيبراني أو من خلاله، بهدف تحقيق الأهداف العسكرية والاستراتيجية، وتشمل القدرات الهجومية والدفاعية، فضلاً عن تشغيل وحماية شبكات المعلومات العسكرية". (Department of Defense 2018,)

ومن الناحية العملية، تُعرف القوة السيبرانية بأنها" قدرة الدولة أو الفاعل على التحكم في البنية التحتية للمعلومات والاتصالات، وتأمينها ضد الهجمات الإلكترونية، وإدارة المخاطر السيبرانية، وتوظيف الفضاء السيبراني لتحقيق الأمن الوطني وحماية المصالح الحيوي"، وقد أصبحت هذه القدرة إحدى أهم ركائز القوة السياسية والاقتصادية والتكنولوجية في العصر الرقمي، لما تؤديه من دور في حماية البنى التحتية الحيوية وتعزيز القدرة على الردع والمنافسة الدولية. (زيتون اذار ٢٠٢٥)

أما من الناحية الأكاديمية، فبعد جوزيف ناي( Joseph S. Nye) من أبرز منظري القوة السيبرانية، إذ يعرفها بأنها "القدرة على تحقيق النتائج المرجوة من خلال استخدام موارد المعلومات المترابطة إلكترونيًا ضمن الفضاء السيبراني، موضحا أن هذه القوة تتجسد في

توظيف المعلومات والتكنولوجيا الرقمية للتأثير في سلوك الفاعلين وتحقيق أهداف سياسية أو اقتصادية أو عسكرية أو اجتماعية". (زيتون ٢٠٢٥،)

وانطلاقًا من مفهوم القوة السيبرانية، سعت إيران إلى تحويل هذا المفهوم إلى قدرات سيبرانية عملية من خلال بناء مؤسسات متخصصة، وتطوير البنية التحتية الرقمية، وتأهيل الموارد البشرية، وتوظيف الهجمات السيبرانية والعمليات المعلوماتية ضمن استراتيجيتها الأمنية، بما عزز قدرتها على الردع وحماية مصالحها والتأثير في البيئة الإقليمية. وعليه، فإن القدرات السيبرانية الإيرانية تمثل التطبيق العملي للقوة السيبرانية، إذ تُترجم موارد الدولة التقنية والبشرية إلى أدوات دفاعية وهجومية واستخباراتية تخدم أهداف السياسة الخارجية والأمن القومي.(النصيري ومري، ٢٠٢٢)

أظهرت التطورات التي شهدتها المواجهة الإيرانية–الأمريكية–الإسرائيلية خلال المدة (٢٠٢٣–٢٠٢٦) تصاعداً ملحوظاً في توظيف إيران لقدراتها السيبرانية، إذ انتقلت هذه القدرات من التركيز على الردع الدفاعي التقليدي إلى تبني نهج أكثر مرونة يقوم على العمليات الاستباقية متعددة المجالات، من خلال دمج الهجمات السيبرانية مع العمليات المعلوماتية واستخدام الوكلاء وأدوات الحرب الهجينة، بما يعكس تطور العقيدة السيبرانية الإيرانية في إطار استراتيجية الردع غير المتماثل.( ابو عليان، ٢٠٢٤)

**المطلب الثاني: نظرية الردع السيبراني والحرب الهجينة**

فرضت التحولات في البيئة الأمنية المعاصرة بروز الفضاء السيبراني والحرب الهجينة بوصفهما من أبرز مجالات الصراع بين الدول. ومن ثمّ، تمثل نظرية الردع السيبراني ونظرية الحرب الهجينة إطارًا نظريًا مناسبًا لتفسير توظيف القدرات السيبرانية في تحقيق الأهداف الاستراتيجية.

**أولاً: نظرية الردع السيبراني(Cyber Deterrence Theory):** تمثل نظرية الردع السيبراني امتداداً لنظرية الردع التقليدية في الدراسات الأمنية والعلاقات الدولية، إلا أنها أُعيدت صياغتها بما يتلاءم مع طبيعة الفضاء السيبراني وخصائصه المختلفة. ويقوم الردع السيبراني على منع الخصم من تنفيذ الهجمات الإلكترونية أو الحد من فاعليتها، سواء بحرمانه من تحقيق أهدافه أو بفرض تكاليف مرتفعة تفوق المكاسب المتوقعة من الهجوم. وتواجه هذه النظرية تحديات جوهرية ناتجة عن طبيعة البيئة السيبرانية، وفي مقدمتها صعوبة إسناد الهجمات إلى الجهة المنفذة، وتعدد الفاعلين من الدول وغير الدول، وانخفاض كلفة تنفيذ العمليات السيبرانية، فضلاً عن أن آثارها قد لا تظهر بصورة فورية، الأمر الذي يجعل تطبيق آليات الردع السيبراني أكثر تعقيدًا مقارنة بالردع العسكري التقليدي.(حسين، ٢٠٢٦)

ويقوم الردع السيبراني على بعدين رئيسيين:

١. **الردع بالعقاب (Deterrence by Punishment)** : يرتكز الردع السيبراني، بوصفه أحد أنماط الردع الحديثة، على مبدأ الردع بالعقاب، الذي يقوم على إقناع الخصم بأن أي هجوم سيبراني سيترتب عليه ثمن سياسي أو اقتصادي أو قانوني أو تقني يفوق المكاسب المتوقعة من تنفيذه. إلا أن نجاح هذا النمط من الردع لا يعتمد على امتلاك القدرة على الرد فحسب، وإنما يتطلب أيضًا توافر مجموعة من المقومات الأساسية، من أبرزها القدرة على إسناد الهجوم إلى الجهة المنفذة بدرجة عالية من الموثوقية، وامتلاك أدوات ردع فعالة، إلى جانب تبني استراتيجية واضحة تحدد توقيت وآليات استخدام تلك الأدوات بما يضمن تحقيق الردع المطلوب.( العلي، ٢٠٢٠)

٢. **الردع بالمنع أو الحرمان (Deterrence by Denial)** : ويتمثل في تعزيز القدرات الدفاعية وتقليل فرص نجاح الهجمات السيبرانية، من خلال رفع مستوى الحماية التقنية، وتطوير أنظمة المراقبة والكشف المبكر، ومعالجة الثغرات الأمنية، والحد من فرص الاختراق. وتنبع أهمية هذا النمط من أنه يدفع الخصم إلى العدول عن تنفيذ الهجوم عندما يدرك أن احتمالات نجاحه محدودة، وأن العوائد المتوقعة لا تبرر الكلفة والمخاطر المترتبة عليه.( عبد الواحد، ٢٠١٦)

وتبعًا لذلك، يمكن تفسير السلوك السيبراني الإيراني بوصفه يجمع بين الردع بالمنع عبر تعزيز دفاعاته الرقمية، والردع بالعقاب من خلال تطوير قدراته الهجومية وتوظيف شبكات الوكلاء السيبرانيين، وهو ما يعكس انتقالاً من الردع الدفاعي إلى الردع الاستباقي.(Klimburg 2012,)

**ثانياً: الحرب الهجينة وعلاقتها بالهجمات السيبرانية**

ويمكن تعريفها بانها "استخدام تكتيكات غير متكافئة للكشف واستكشاف نقاط الضعف باستخدام وسائل غير عسكرسة سياسية أو اعلامية فضلاً عن ذلك الوسائل العسكرية التقليدية وغير التقليدية ويعكس هذا التعريف شمولية واضحة، فهو يعترف بتفاوت القدرات والاساليب بين الاطراف المتصارعة، ويدمج بين الابعاد السياسية والاعلامية والعسكرية في صياغة الحرب الهجينة، كما يبرز الدور الاستراتيجي للكشق عن الضعف كخطوة اولى في النزاع".(ابراهيم، ٢٠٢٦)

وفي هذا الإطار، تؤدي الهجمات السيبرانية دورًا محورياً في الحرب الهجينة من خلال جمع المعلومات الاستخباراتية، وتعطيل البنى التحتية الحيوية، والتأثير في الرأي العام،

ودعم عمليات الوكلاء، بما يحقق أهداف الدولة مع المحافظة على قدر من الإنكار السياسي.(Hoffman, 2007,)

كما يرى توماس ريد( Thomas Rid) أن الفضاء السيبراني أصبح أحد أهم ميادين المنافسة الاستراتيجية، إذ تُستخدم العمليات السيبرانية بصورة متزايدة ضمن حملات التأثير والتجسس والإكراه السياسي، أكثر من استخدامها كحروب مستقلة، الأمر الذي يعزز ارتباطها بالحرب الهجينة.(Rid, 2013,)

وبناءً على ذلك، فإن النموذج الإيراني ينسجم مع منطق الحرب الهجينة، إذ يعتمد على التكامل بين القدرات السيبرانية، وشبكات الوكلاء، والعمليات المعلوماتية، بما يحقق الردع والتأثير الاستراتيجي في البيئة الإقليمية.(Klimburg, 2012,)

**المطلب الثالث : اليقظة الرقمية( السيبرانية)**

تعد اليقظة الرقمية كأداة تحليلية تسهل عمل المختصين من فهم السلوك الاستراتيجي لوحدات النظام الدولي في الفضاء السيبراني على أعتبارها شكلاً معيارياً يشكل أضافة لمفاهيم ومصطلحات العلوم السياسية.

**أولاً: تعريف اليقظة السيبرانية (الرقمية) وعناصرها**

ويمكن تعريفها بإنها " النهج الاستراتيجي للدول من أجل الحفاظ على المراقبة المستمرة للبنية المعلوماتية والسيبرانية من أجل التنبؤ بالتهديد وتمكين إدارة العمليات الدفاعية والهجومية في الوقت نفسه مع بناء أستراتيجية فهم الخصم ضمن منطقة ضبابية قابعة بين السلم والحرب الفعلية(Onwubiko 2022) ، ومن خلال ذلك تبرز عناصر محورية لاتختزل وهي:

١. الديمومة: وتمثل حالة استراتيجية مستدامة.

٢. الازدواجية (هجومية ودفاعية): توظف في الفضاء السيبراني للطرفين.

٣. البعد الادراكي: تكون قائمة على استراتيجية فهم الخصم من خلال استهداف الوعي والقرارات.

**ثانياً: أبعاد اليقظة السيبرانية**

تكمن ابعاد مفهوم اليقظة السيبرانية في(Endsley 1995,) :-

- اليقظة الاستخباراتية الرقمية الخاصة برصد الفضاء الرقمي للعدو بطريقة استباقية من اجل جمع المعلومات والتنبؤ بالتوجهات قبل حدوثه ، وبدورها تعبر الاستخبارات الكلاسيكية بعملها في مجال مفتوح مستمر غير قابل للاستهداف المادي،
- اليقظة العملياتية الرقمية من خلال دمج الامكانيات مع العسكرية والامنية بطريقة تجعلها موازية للمادية والتي بدورها تميزها عن الامن السيبراني،
- اما البعد الاخير هو اليقظة الادراكية الرقمية والمبنية على فهم الخصم والربط بين الحرب والهجمات الرقمية.

وعليه تضيف اليقظة الرقمية قيمة معرفية نظرية لإجابتها على مالم تستطع المفاهيم التقليدية عليه إذ إنها تفسر كيفية أدارة الدول لصراعاتها السيبرانية المستمرة بغياب إعلان الحرب الرسمية مع الحفاظ على الردع وإدارته في الوقت نفسه.

## المبحث الثاني : التطور التأريخي للقدرات السيبرانية الايرانية والركائز المؤسسية

لمعرفة كيف استطاعت الجمهورية الاسلامية الايرانية من بناء قدراتها السيبرانية على الرغم من ماتمر فيه من عقوبات اقتصادية وتصاعد وتيرة التهديدات مع الولايات المتحدة الامريكية والكيان الصهيوني وصول سياسة التنافس إلى مرحلة الحرب الفعلية بعام ٢٠٢٥ يجب أولاً التعمق في مسارات قدراتها السيبرانية وعلى ماذا اعتمدت و ارتكزت تلك القدرات للتمكن من التحول من الدفاع إلى الاستباق الهجومي والتنبؤ بالهجمات.

**المطلب الاول: القدرات السيبرانية الايرانية ومسار تطورها**

تعود البدايات الفعلية لتطوير القدرات السيبرانية الإيرانية إلى حدثين مفصليين؛ الأول تمثل في الاحتجاجات التي أعقبت الانتخابات الرئاسية الإيرانية عام ٢٠٠٩، والتي كشفت لطهران الدور المتنامي للفضاء الرقمي وشبكات الإنترنت في التعبئة السياسية وتحدي السلطة، أما الثاني فتمثل في الهجوم الإلكتروني بفيروس ستوكسنت **(Stuxnet )** عام ٢٠١٠ الذي استهدف منشأة نطنز النووية، وأظهر حجم الثغرات التي تعاني منها البنية السيبرانية الإيرانية. وقد شكل هذان الحدثان نقطة تحول استراتيجية دفعت صناع القرار الإيراني إلى الاستثمار المكثف في بناء منظومة سيبرانية وطنية تجمع بين القدرات الدفاعية والهجومية، باعتبار الفضاء السيبراني أحد مجالات الأمن القومي وأداة لتعويض اختلال موازين القوة التقليدية في مواجهة الخصوم الإقليميين والدوليين ( Citrinowicz 2022.)

وبتتبع مسار القدرات السيبرانية نجد إن هناك مراحل بنيوية مختلفة لها ويمكن تقسيمها على ثلاثة مراحل :

**المرحلة الاولى: ٢٠٠٩–٢٠١١ الاستجابة الاولى:-**

تكرست جهود حكومة طهران على أستيعاب الحوادث التي شهدتها تلك المرحلة كما اسلفنا، فضلاً عن التركيز على إنشاء منصات الدفاع الداخلية والتمكن من إدارة الفضاء السيبراني المحلي وكانت الجمهورية الاسلامية لا تمتلك القدرة البشرية والبنية المؤسسية التي تمكنها من مجابهة او مسايرة التنافس السيبراني الخارجي.(Article19 2024)

**المرحلة الثانية: ٢٠١٢– ٢٠١٨: الهيكل التأسيسي والتحول الهجومي:-**

وتمثل كنقطة محورية في المسار السيبراني الايرانية وذلك لأسباب محورية متزامنة(Citrinowicz 2022):

١. تشريع البنى التحتية و المؤسسية: بعام ٢٠١٢ إنطلق المجلس الاعلى للفضاء السيبراني الايراني بموافقة المرشد الاعلى الشهيد على خامنئي بإعتباره محوراً تنسيقياً لصنع السياسة والقرار ويمتلك المجلس حق وضع الاستراتيجية السيبرانية القومية وإدارة تنفيذها، اما المركز الوطني للفضاء الالكتروني فيتولى توفيق الانشطة الايرانية الرقمية ورصد المعلومات الاستخباراتية ونشر التوجيهات السياسية.
٢. التحول الفعلي نحو الهجوم: إستطاعت الجمهورية الاسلامية بعام ٢٠١٢ توظيف مشروع مادي " Madi" كتجربة لنظامها الهجومي، من خلال إستهداف مواقع خارج حدودها لغرض جمع المعلومات الاستخباراتية في منطقة الشرق الاوسط.
٣. العمليات التأسيسية الكبرى: وتجسدت بهجمات "أبابيل" للفترة مابين ٢٠١٢–٢٠١٣ والتي إستهدفت مؤسسات امريكية والذي خلف أضراراً كبيرة وتكاليف لتطوير أنظمة الدفاع الخاصة بتلك المؤسسات، ولم تقتصر الهجمات على "ابابيل" فقط، إذ شملت هجوم أخر بمسمى " شامون" والذي استهدف محطات شركة أرامكو السعودية مخلقاً

توقفاً مؤقتاً بمحطات العمل للشركة، الامر الذي أرسل شارةً جيوسياسية صارمة بمسار احتدام التنافس الاقليمي.

**المرحلة الثالثة: ٢٠١٩– ٢٠٢٦ الاتقان والانتشار الاستراتيجي:**

خلال هذه الفترة أنشأت الجمهورية الاسلامية الايرانية مستودعاً معرفياً من عملياتها السيبرانية المحدثة وتمكنت من توليد رصيد لقدراتها الهجومية التوسعية من خلال التفاهمات مع كل من روسيا الاتحادية والجمهورية الصينية، وعليه إنتقلت لمستوى الفاعل الاستراتيجي العابر للاقليمية، فضلاً عن ربط قدرته السيبرانية بالمؤسسات العسكرية والاستخباراتية بشكل رسمي مع زيادة مستودعاتها التقنية لتضم اختراق سلاسل التوريد والتملص من البيئة السحابية والحروب النفسية الخاصة بمنظومات الاختراق والتلاعب التقني.(FalconFeeds.io 2026)

**المطلب الثاني: ركائز القدرات السيبرانية الايرانية:-**

للقدرات السيبرانية الايرانية ركائز أربعة مؤسسية مكنتها من التحول من محور الدفاع السيبراني إلى الهجومي والتنبؤ والانتشار الرقمي وهي:

١. **الحرس الثوري** : تنتظم القدرة السيبرانية الهجومية الايراني بمظلة الحرس الثوري بطابعه العسكرية و وزارة الاستخبارات والامن المدنية، ويشمل الحرس الثوري اقسام تخصصة معينة مثل منظمة الحرب الالكترونية والدفاع السيبراني والخاصة بعمل دورات تدريبية رقمية و فرض الرقابة على المحتويات الرقمية، و المجلس السيبراني الباسيج والذي يمثل قوة اقرب للعسكرية تستند على مجاهدي الحرب السيبرانية من المتطوعين، فضلاً عن منظمة الدفاع سلبي الوطني الخاصة بحفظ البنى التحتية المهمة.(Center for strategic and international studies 2026)

٢. **وزارة الاستخبارات والامن** : تتأرجح صلاحيات الاستخبارات السيبرانية بين أستخبارات الحرس الثوري و وزارة الامن، وتقوم الوزارة بالتعاون مع الاجهزة الاستخباراتية الاجنبية كمثال على ذلك مع روسيا الاتحادية.(Mossad 2025)

٣. **مجموعات التهديد المتقدم الدائم ( APTs):** تعتمد الجمهورية الاسلامية على مجموعات التهديد المتقدم الدائم متباينة الاهداف وتشارك في الاعمال التكتيكية والتشغيلية لممارسة عمليات التجسس الاستراتيجي و تنفيذ اخرى ضد الخصوم والمعارضين. (Center for strategic and international studies 2026)

٤. **شركات الواجهة والمقاولون:** ركيزة الانكار المقبول:– وتكمن اهمية تلك الركيزة لما لها من بعد واسع لتشريح آليات اليقظة الرقمية وفهمها، وتتكون من أكاديمية رافيين وسراج للفضاء الالكتروني ومجموعة (CyberAv3ngers) ويمكننا تقديم شرح مبسط لكل منها كمايلي(TDR 2023):

– أكاديمية رافين: أُنشأت عام ٢٠١٩ من قبل سيد مجتبى مصطفوي وفرزين كريمي عضوي وزارة الاستخبارات الايرانية بهدف التدريت والتجنيد لصالح الوزارة الامر الذي جعل منها موقعاً لتجهيز الجيل القادم من القراصنة الحكوميين.

– منظمة سراج للفضاء الالكتروني: ووتكون مهامها ضمن مضلة الباسيج وتعتبر لاعباً مهماً بشكل محوري في حروب المعلومات من خلال جمعها بين التأثيرات السيبرانية والعمليات نفسية وحملات الدعاية الرقمية، فضلاً عن توليد آلعاب قومية مؤدلجة.

– مجموعة (CyberAv3ngers): وهي مجموعة تمارس نشاطاً سيبرانية سياسياً معيناً، إلا إن الدول الغربية وبالتحديد الولايات المتحدة الامريكية تتهم الجمهورية الاسلامية بتوظيف تلك المجموعات وتعتبرها فاعلاً حكومياً أيرانياً، الامر الذي يكشف أستراتيجية

الانكار المقبول الايرانية من خلال توكيل تلك الجماعات لتنفيذ عملياتها الخارجية . (Margin research 2026)

## المبحث الثالث: اثر القدرات السيبرانية في اليقظة الاستخباراتية الايرانية:

إن تغيير النهج المتعارف عليه عن اليقظة الاستخباراتية بنموذج وعي ظرفي مستمر من خلال توظيف القدرة السيرانية يمثل ظاهرة تستحق التحليل، وتمكنت الجمهورية الاسلامية الايرانية من ربط الفضاء السيبراني باليقظة الاستخباراتية وتحويلها لمنظومة استخبارية و وسيلة رئيسية لصناعة التصور الاستخباري عن الخصوم والامن الاقليمي المحيط، لذا سينصب المبحث على تشريح التحول وأثاره.

**المطلب الاول : مستويات تعزيز اليقظة الاستخباراتية للجمهورية الاسلامية :**

يتجسد التحول في توظيف القدرات السيبرانية الايرانية بمستويات متواترة مكنت ايران من السير نحو ذلك التحول وهي:

**اولا: توسيع دائرة اليقظة الجغرافية**

يعتبر التجسس الاستراتيجي السيبرانية بعيد المدى من المستوى الاول لتعزيز اليقظة الاستخباراتي في الجمهورية الاسلامية، ويختلف بشكل كبير عن التجسس الكلاسيكي بمحور مهم جدا وهو البعد الجغرافي اللامتناهي وغياب كلفة الانتشار، ويمكنها هذا المستوى من أمتلاك قدرة معلوماتية لمراجعة ماتم إنجازه من قبل العدو وماسيقوم به مستقبلاً من خلال الفضاء السيبراني ويمثل المستوى المؤسسي والبنيوي لليقظة الاستخبارية ، ومن خلال تتبع حرب عام ٢٠٢٥ والتي عرفت بحرب الاثنا عشر يوماً بأن الجمهورية

الاسلامية و ( الكيان الصهيوني) قد وظفوا القدرات السيبرانية بطريقة إحترافية ساعية لإستهداف الفضاءات الاستخباراتية قبل العسكرية.(Csis 2026)

**ثانياً: الاستخبارات البشرية الرقمية والاستهداف الادراكي**

يمكننا القول بأن المستوى الثاني هو الاكثر تعقيداً، خاصة بوجود مجموعات تجسسية رفيعة المستوى موظفة من قبل الحرس الثوري الايراني ومتخصصة بعمليات المتابعة البشرية والمنظمات المهمة للحكومة فضلاً عن جمع ورصد المعلومات، ومن أبرز تلك المجموعات هي (APT42) والتي قامت بمهام مميزة من عام ٢٠١٥ منها متابعة الخوادم لأجهزة الاندرويد وتحديد الموقع الجغرافي للمعارضين داخل الجمهورية الاسلامية. (hedgehogsecurity 2024)

**ثالثاً: المتابعة العابرة للجغرافية**

يمثل هذا البعد من مستويات اليقظة الاستخباراتية المتطورة للدول، والتي تتمكن من خلاله بمتابعة المعارضين والعملاء ومثيري الشغب القانطين خارج حدود الدول ومتابعتهم ومعرفة مواقعهم والتعامل معهم، وتمكنت ايران من الوصول لهذا المستوى المتطور من اليقظة الاستخباراتية إذ تمكنت من ملاحقة المعارضين والعملاء حتى خارج حدودها. Loft) 2026)

**رابعاً: الاستطلاع الرقمي**

ويمثل البعد الرابع لتوظيف القدرات السيبرانية وتعزيز اليقظة من خلال جعل الفضاء السيراني منظومة إستطلاع موازية وللمسيرات والاقمار الصناعية، وتمكنت الجمهورية الاسلامية من توظيف الاستطلاعات الرقمية ودمجها بعمليات الحرب المعلوماتية الخاصة بالتضليل والمواقع الاخبارية ومجابهة التدخل الخارجي الذي يستهدف الرأي العام الداخلي

في أيران، فضلاً عن إن تلك المزايا التي توصلت إليها الجمهورية الاسلامية تبين بأنها تستخدم الاستخبارات الرقمية كنظام توزيع شبكي يصل لمدى ابعد من حدودها. (Khorrami 2025)

**المطلب الثاني : اثر توظيف القدرات السيبرانية في اليقظة الاستخباراتية:**

بعدما تطرقنا عن كيفية إستخدام إيران لقدراتها السيبرانية، يجب متابعة ذلك التوظيف من خلال دراسة اثره، والذي بدوره يعتبر أكثر تعقيداً على المستوى التحليلي.

١. منظومة الردع الايرانية:- أن توظيف القدرة السيبرانية أثر بشكل كبير على منظومة الردع الايرانية وأكسب الجمهورية الاسلامية حس المناورة في المساحات الرمادية بين السلم والحرب، وخلال فترة الحرب الممتدة نجد بأنها تمكنت من أستهداف الامن الداخلي والعالمي بحملات ممنهجة لإظهار تبعات الهجمات على الاراضي الايرانية، إلا إن في عام ٢٠٢٦ نجد بإن منظومة الردع السيبراني تراجعت بشكل كبير ولم تتمكن من تفادي الحرب الفعلية،(Centrella 2026)

٢. التوازن الاستخباراتي مع كل من امريكا و( الكيان الصهيوني): على الرغم من القدرات السيبرانية الكبيرة للجمهورية الاسلامية الايرانية إلا إنها ضلت بموازين الاستخبارات السيبرانية في منطقة الرخوة مقارنة مع كل من الولايات المتحدة الامريكية و( الكيان الصهيوني) إذ أن مراحل التطور الذي وصلوا إليه يفوق قدراتها (ايران) السيبرانية من خلال ربطها بإنظمة الذكاء الاصطناعي مما اسكبها كفاءة عالية في امكانية الاندماج بين المعلومات الرقمية والذكاء الاصطناعي، الامر الذي مثل تطوراً على مستويات ايران السيبرانية.(GOSWAMI 2026)

٣. استدامة النظام: بدى التأثير على استدامة النظام في الجمهورية الاسلامية الايرانية كسلاح ذو حدين، إذ إن القدرات السيبرانية صنعت من اجل حمايتها من الخارج لكنها أصبحت ثقلاً داخلياً، خاصة مع بداية الاحتجاجات الداخلية عام ٢٠٢٢–٢٠٢٣ إذ إنصبت توجهات الجمهورية الاسلامية على الامن الداخلي مما ولد ثغرة في الردع الخارجي.(Cyderes 2026)

٤. القوة الاقليمية: توثق بعض الدراسات بأن المحور السيبراني الايراني تأثر بسبب الحرب الاخيرة وفقدت قوتها السيبرانية من خلال تشتت القاعدة الايديولوجية القادرة على شن حملات مؤثرة عبر وسائل التواصل الاجتماعي، إلا أن الواقع يثبت عكس ذلك، إذ إن على الرغم من الضربات التي تلقتها الجمهورية الاسلامية إلا أن قدراتها السيبرانية أُعيد هيكلتها بصورة مغايرة ومكثفة من خلال شعوب اغلب دول العالم الاسلامي وحتى الغربي.(Ribeiro 2026)

وعليه يمكننا الاستنتاج أن الجمهورية الاسلامية الايرانية تمكنت من ضنع منظومة يقظة استخباراتية متشابكة ومعقدة جداً إلا إنها لم تصل لمرحلة التفوق الاستراتيجي، على الرغم من تحقيقها مكاسب على مستوى التكتيكي والعملياتي إلا إنها اخفقت من ترجمته كأستراتيجية تفوق كاملة.

**المطلب الثالث :دراسة حالة: توظيف القدرات السيبرانية الإيرانية خلال حرب حزيران/يونيو ٢٠٢٥**

أظهرت حرب حزيران/يونيو ٢٠٢٥، المعروفة إعلاميًا بـ"حرب الاثني عشر يومًا"، تحولًا واضحًا في توظيف إيران لقدراتها السيبرانية، إذ لم تقتصر العمليات على تنفيذ هجمات إلكترونية منفردة، بل اندمجت مع العمليات العسكرية والاستخباراتية وحملات التأثير

المعلوماتي ضمن إطار الحرب متعددة المجالات .(Multi-Domain Operations) فقد ركزت العمليات السيبرانية الإيرانية على جمع المعلومات الاستخباراتية، وتعطيل بعض الخدمات الرقمية، واستهداف البنية التحتية المدنية والعسكرية، بالتوازي مع استخدام وسائل إعلامية ورقمية لتشكيل الإدراك العام وإرباك الخصم، بما يعكس توظيف الفضاء السيبراني بوصفه عنصرًا رئيسًا في إدارة الصراع وليس مجرد وسيلة مساندة(CSIS 2026, 3–8) .

كما كشفت الحرب أن إيران أصبحت تعتمد بصورة متزايدة على مجموعات التهديد المتقدم (Advanced Persistent Threats – APTs)، ولا سيما APT42، التي ركزت على عمليات الهندسة الاجتماعية، والتصيد الاحتيالي، واختراق الحسابات الشخصية للمسؤولين والباحثين والصحفيين، بهدف جمع المعلومات الاستخباراتية وتعزيز اليقظة الرقمية الإيرانية. وتشير الدراسات إلى أن نشاط هذه المجموعة ازداد بصورة ملحوظة خلال الحرب، بما يؤكد انتقالها من عمليات التجسس التقليدية إلى دعم صنع القرار الاستراتيجي في أثناء الأزمات.(Hedgehog Security 2024, 5–11)

وفي السياق نفسه، برزت مجموعة **(CyberAv3ngers)** بوصفها أحد أبرز الفاعلين المرتبطين بالمصالح الإيرانية، حيث تبنت استهداف أنظمة التحكم الصناعية (ICS/SCADA)، ولا سيما في قطاعات المياه والطاقة، بما وفر لإيران قدرة على ممارسة الضغط غير المباشر مع المحافظة على سياسة "الإنكار المقبول Plausible) " (Deniability، وهو أحد المرتكزات الرئيسة للعقيدة السيبرانية الإيرانية Margin ) Research 2026, 12–18).

وتؤكد هذه الحالة أن القدرات السيبرانية الإيرانية لم تعد تقتصر على الدفاع عن البنية الرقمية، وإنما أصبحت جزءًا من منظومة الردع والحرب الهجينة، إذ يجري توظيفها في

جمع المعلومات، وإدارة العمليات النفسية، والتأثير في الخصم، بما يدعم فرضية الدراسة القائلة بأن القدرات السيبرانية أسهمت بصورة مباشرة في تعزيز اليقظة الاستخباراتية الإيرانية.

## الخاتمة:

إستطاعت الجمهورية الاسلامية الايرانية في بناء قدراتها السيبرانية في الفضاء الرقمي وطورته على مده عقد من الزمن، واتصفت قدراتها السيبرانية بالمتشابكة لربطها في منظومة الامن الاستخباراتي و وصل بها الحال إلى تجاوز حدودها الجغرافية ومتابعة الاهداف والعملاء اقليمياً ودولياً، فضلاً عن تطوير عمليات رصد وجمع المعلومات الرقمية والتاثير على الراي العام داخليا وخارجياً، وعلى الرغم من كل هذه القدرات السيبرانية إلا إنها مازالت من نطاق مقيد قياساً بالامكانيات التي تمتلكها الولايات المتحدة الامريكية و (الكيان الصهيوني)، وكان لتوظيف القدرة السيبرانية في أطار اليقظة الاستخباراتية اثر كبير على الجمهورية الاسلامية الايرانية وحققت مكاسب في بعض الجبهات وطورت من قدراته العسكرية معتمدة على المعلومات المرصودة من قبل مجموعاتها السيبرانة، وأخفقت في نواحي أخرى، أذ انها لم تصل إلى مرحلة التفوق الاستراتيجي.

## الاستنتاجات:

١. أثبتت الدراسة أن الجمهورية الإسلامية الإيرانية نجحت في تطوير قدراتها السيبرانية بصورة تدريجية، إذ انتقلت من مرحلة الاستجابة الدفاعية للهجمات الإلكترونية إلى بناء منظومة سيبرانية متكاملة تجمع بين القدرات الهجومية والدفاعية والاستخباراتية، مستندة إلى بنية مؤسسية متخصصة وإطار تشريعي داعم.

٢. أظهرت نتائج الدراسة أن إيران تبنت نموذجًا متطورًا للردع السيبراني يقوم على الجمع بين الردع بالمنع والردع بالعقاب، بما مكّنها من تعزيز قدرتها على إدارة الصراع في الفضاء السيبراني وتقليل كلفة المواجهة العسكرية المباشرة.

٣. كشفت الدراسة أن القدرات السيبرانية الإيرانية أصبحت أحد المكونات الرئيسة للحرب الهجينة، من خلال دمج الهجمات السيبرانية مع العمليات المعلوماتية والحرب النفسية واستخدام الوكلاء، بما وفر لإيران أدوات تأثير تتجاوز القيود التي تفرضها المواجهة العسكرية التقليدية.

٤. بينت الدراسة أن المؤسسات السيبرانية الإيرانية، ولا سيما المجلس الأعلى للفضاء السيبراني، والحرس الثوري، ووزارة الاستخبارات، ومجموعات التهديد المتقدم(APT) ، أسهمت في بناء منظومة سيبرانية مترابطة عززت من كفاءة التخطيط والتنفيذ والإنكار العملياتي.

٥. توصلت الدراسة إلى أن توظيف القدرات السيبرانية أسهم بصورة واضحة في تعزيز اليقظة الاستخباراتية الإيرانية، من خلال توسيع نطاق جمع المعلومات، وتحسين الإنذار المبكر، ورفع كفاءة متابعة التهديدات داخل إيران وخارجها، بما وفر دعمًا لصناع القرار في إدارة الأزمات.

٦. أثبتت الدراسة أن المواجهات السيبرانية خلال المدة (٢٠٢٣–٢٠٢٦) عكست تحولًا في العقيدة السيبرانية الإيرانية نحو العمليات الاستباقية متعددة المجالات، إلا أن هذا التحول لم ينجح في تحقيق تفوق سيبراني استراتيجي كامل أمام الولايات المتحدة وإسرائيل، بسبب الفجوة التقنية والتكنولوجية المستمرة، خاصة في مجالات الذكاء الاصطناعي والاستخبارات السيبرانية.

٧. خلصت الدراسة إلى أن القدرات السيبرانية الإيرانية حققت نجاحات ملموسة على المستويين التكتيكي والعملياتي، إلا أن قدرتها على تحويل هذه النجاحات إلى تفوق استراتيجي طويل الأمد ما زالت تواجه تحديات مرتبطة بالعقوبات الدولية، والتطور التقني المتسارع، والتنافس مع قوى تمتلك إمكانات سيبرانية أكثر تقدمًا.

## التوصيات:

١. ضرورة أن تعمل الدول العربية، ولا سيما العراق، على بناء استراتيجيات وطنية متكاملة للأمن السيبراني ترتكز على تطوير القدرات البشرية والتقنية والتشريعية، بما يعزز قدرتها على مواجهة التهديدات السيبرانية المتزايدة.

٢. تعزيز الاستثمار في مراكز الأمن السيبراني واليقظة الرقمية، وربطها بالمؤسسات الأمنية والعسكرية والاستخباراتية، بما يسهم في تحسين قدرات الإنذار المبكر والاستجابة السريعة للهجمات الإلكترونية.

٣. تطوير التعاون الإقليمي والدولي في مجال تبادل المعلومات الاستخباراتية السيبرانية، ومكافحة الهجمات العابرة للحدود، بما يسهم في الحد من مخاطر الفضاء السيبراني على الأمن الإقليمي.

٤. الاهتمام بتطوير برامج أكاديمية وبحثية متخصصة في الأمن السيبراني والعلاقات الدولية، لتأهيل كوادر قادرة على تحليل التهديدات الرقمية وصياغة السياسات السيبرانية.

٥. توصي الدراسة بإجراء بحوث مستقبلية تتناول العلاقة بين الذكاء الاصطناعي والقدرات السيبرانية، ودورهما في إعادة تشكيل استراتيجيات الردع والحرب الهجينة في الشرق الأوسط.

٦. ضرورة متابعة التحولات المستمرة في العقيدة السيبرانية الإيرانية، ولا سيما ما يتعلق بتوظيف الوكلاء السيبرانيين، والعمليات المعلوماتية، والهجمات المدعومة بالذكاء الاصطناعي، لما لذلك من انعكاسات مباشرة على الأمن الإقليمي.

٧. توصي الدراسة بإنشاء منظومات وطنية لليقظة الرقمية تعتمد على التكامل بين الأمن السيبراني والاستخبارات الرقمية وإدارة المخاطر، بما يمكن مؤسسات الدولة من التنبؤ بالتهديدات والتعامل معها قبل تحولها إلى أزمات فعلية.

## المصادر العربية والاجنبية:

### اولاً: المصادر العربية :

١. إبراهيم، هناء عبد الحميد. "الحروب الهجينة وتهديداتها الجيواستراتيجية: دراسة اجتماعية تحليلية في الواقع العراقي :مرحلة ما بعد داعش أنموذجًا ".*مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية* 18، العدد ٢ ،٢٠٢٦.

٢. أبو عليان، عبد العزيز محمود" .الحرب السيبرانية والأداء الاستراتيجي الفعال؛ دراسة حالة في الهجمات السيبرانية بين إيران و«إسرائيل ".«مجلة المبادرة، المجلد ٢، العدد ١، ٢٠٢٣.

٣. حسين، محمد جاسم. "استراتيجيات الردع السيبراني في الشرق الأوسط: دراسة في التحديات والفاعلية : إيران–الكيان الصهيوني نموذجًا . *مجلة مركز بابل للدراسات الإنسانية*، مج. ١٦، العدد ٥ ،٢٠٢٦.

٤. زروقة، إسماعيل. ٢٠١٩. "الفضاء السيبراني والتحول في مفاهيم القوة والصراع." مجلة العلوم القانونية والسياسية ١٠ (١): ١٠١٦–١٠٣١. جامعة الشهيد حمه لخضر – الوادي، الجزائر.

٥. زيتون، محمد محمود" .القوة السيبرانية أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدولية ". *المجلة العربية للنشر العلمي*، العدد ٧٧ (آذار ٢٠٢٥)، بحث مكمل لمناقشة رسالة دكتوراه، متاح على الرابط:
https://www.ajsp.net/research/%D8%A7%D9%84%D9%82%D9%88%D ( تاريخ الزيارة 1-6-2025).

٦. زيتون، محمد .عتبة القوة السيبرانية وتأثيرها في العلاقات الدولية المعاصرة ".مجلة خليج العرب للدراسات الإنسانية والاجتماعية، المجلد ٢، العدد ٥ (٣١ آب ٢٠٢٥)، مركز السنابل للدراسات والتراث الشعبي.
٧. عبد الواحد، صالح حيدر .*حروب الفضاء الإلكتروني: دراسة في المفهوم وخصائصها وسبل مواجهتها* .رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، كلية الآداب والعلوم، قسم العلوم السياسية، عمّان، ٢٠١٦.
٨. العلي، علي زياد .الصراع والأمن السيبراني في السياسة الدولية: دراسة استراتيجية في العصر الرقمي .عمّان: دار أمجد للنشر والتوزيع، ٢٠٢٠.
٩. النصيري، هبة عبد الخالق، و مري، مثنى فائق .المؤسسات السيبرانية في الشرق الأوسط: إيران وإسرائيل أنموذجًا ".*مجلة تكريت للعلوم السياسية*، العدد ٣٠، ٢٠٢٢.

## ثانياً: المصادر الاجنبية:

1. Article 19. *Iran's New Phase of Digital Repression*. London: Article 19, 2024.
2. Center for Strategic and International Studies (CSIS). "Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape." Washington, DC: Center for Strategic and International Studies, January 14, 2026.
3. Center for Strategic and International Studies (CSIS). "Demystifying Iranian Cyber Operations in the U.S.-Iran Conflict." Washington, DC: Center for Strategic and International Studies, March 20, 2026.
4. Centrella, Michael R. "Iran and the Expanding Cyber Front: What Government Leaders Need to Know." *SC Media*, March 16, 2026. Accessed May 20, 2026. https://www.scworld.com/perspective/iran-and-the-expanding-cyber-front-what-government-leaders-need-to-know.
5. Citrinowicz, Danny. *Iran's Cyberspace Evolution*. Washington, DC: The Dispatch, 2022.
6. Cyderes. "Iran Cyber Conflict Update and Analysis." Kansas City, MO: Cyderes, March 2, 2026.
7. Endsley, Mica R. "Toward a Theory of Situation Awareness in Dynamic Systems." *Human Factors* 37, no. 1 (1995): 32–64. https://doi.org/10.1518/001872095779049543.
8. FalconFeeds.io. *Inside Iran's APT Network: Profiling the Most Active Iranian State-Linked Threat Actors*. January 20, 2026.

9. Goswami, Archishman Ray. "Intelligence for Hyperwar: Tracking the Intelligence Landscape in the 2026 Iran War." *Observer Research Foundation*, March 9, 2026. Accessed May 20, 2026. https://www.orfonline.org/english/expert-speak/intelligence-for-hyperwar-tracking-the-intelligence-landscape-in-the-2026-iran-war.
10. Hedgehog Security. *APT42: Iran's Social Engineering Specialists—From Journalist Impersonation to Election Interference*. December 18, 2024.
11. Khorrami, Nima. *Digital Frontlines: What the 12-Day War Revealed About the Evolution of Iran's Cyber Strategy*. Washington, DC: Middle East Institute, 2025.
12. Klimburg, Alexander, ed. *National Cyber Security Framework Manual*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012.
13. Loft, Philip. *Iranian State Threat Activities in the United Kingdom*. Research Briefing CBP-10293. London: House of Commons Library, 2026.
14. Margin Research. *Unpacking Russian-Iranian Private-Sector Cyber Connections*. New York: Margin Research, May 6, 2026.
15. Mossad, Marco. *Behind the Bombs: The Israel-Iran Cyberwar*. London: Al Majalla Magazine, 2025.
16. Onwubiko, Cyri. *CyberOps: Situational Awareness in Cybersecurity Operations*. arXiv Preprint. Ithaca, NY: Cornell University, 2022. https://arxiv.org.
17. Ribeiro, Anna. "Resecurity Warns That Iran War Enters Multi-Domain Phase as Cyber and Kinetic Operations Converge." *Security Brief*, March 24, 2026.
18. TDR, Maxime A., and Sekoia. *Iran Cyber Threat Overview*. Rennes: Sekoia, June 5, 2023.
19. *Department of Defense*. **Joint Publication (JP) 3-12: Cyberspace Operations.** Washington, DC: Joint Chiefs of Staff.2018,P ii 5.
20. Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007
21. Rid, T.. *Cyber War Will Not Take Place*. Oxford: Oxford University Press. 2013.
22. Citrinowicz, Danny. *Iran's Cyberspace Evolution*. Washington, DC: The Dispatch, 2022.

23. Center for Strategic and International Studies (CSIS). Demystifying Iranian Cyber Operations in the U.S.-Iran Conflict. Washington, DC: CSIS, 2026.
24. Hedgehog Security. APT42: Iran's Social Engineering Specialists—From Journalist Impersonation to Election Interference. 2024.
25. Margin Research. Unpacking Russian-Iranian Private-Sector Cyber Connections. New York, 2026.