E-ISSN : 2790-2404
P- ISSN 2070-9250
Qadaya siyasiyyat

Ministry of Higher Education
& Scientific Research
Al-Nahrain University
College of Political Science

وزارة التعليم العالي والبحث العلمي
جامعة النهرين
كلية العلوم السياسية

قضايا سياسية

Political Issues

مجلة فصلية محكمة

العدد ٨١
Issue 81

نيسان - ايار - حزيران / ٢٠٢٥
Apr. - May. - Jun / 2025

قضايا سياسية
العدد ٨١
٢٠٢٥

جامعة النهرين
كلية العلوم السياسية

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

قضايا سياسية
Political Issues

مجلة فصلية محكمة تعنى بنشر الأبحاث والدراسات السياسية العراقية والعربية والدولية
http://pissue.iq

مجلة قضايا سياسية

pissue.iq

قواعد النشر

- لغة المجلة هي اللغة العربية والانكليزية على أن يراعى الوضوح وسلامة النص.
- ترحب المجلة بنشر البحوث والدراسات السياسية النظرية والتطبيقية ولا سيما التي تجعل من قضايا المنطقة والعالم محط اهتمامها، ماضياً وحاضراً ومستقبلاً، وعلى وفق الآتي:

1. أن لا يزيد عدد صفحات البحث أو الدراسة عن (15) صفحة مطبوعة بحجم خط (14) والتباعد (1,15) ونوع الخط Simplified Arabic تقدم عبر المنصة الاليكترونية للمجلة على الرابط : https://pissue.iq/index.php/pissue/about/submissions
2. أن تتصف البحوث والدراسات بالموضوعية والدقة العلمية.
3. أن تعتمد الترقيم العشري للعناوين الأساسية والفرعية او التنصيف المعياري العام.
4. يرفق مع كل بحث او دراسة ملخصين (احدهما باللغة العربية والآخر باللغة الانكليزية/ يتضمن اهداف البحث ، المنهج والمعالجة ، ابرز النتائج واهم الاستنتاجات والمقترحات) مع ضرورة مراعاة ان الملخص مختلف اختلافا جذريا عن المقدمة وليس تكرارا لها .
5. تخضع جميع البحوث المقبولة للنشر الى نظام الاستلال الالكتروني في كلية العلوم السياسية –جامعة النهرين.
6. يرفق مع كل بحث ودراسة سيرة ذاتية مختصرة للباحث وتعهد .

- تقوم المجلة بإخطار الباحثين بإجازة بحوثهم أو دراساتهم من عدمها بعد عرضها على محكمين تختارهم على نحو سري من بين أصحاب الاختصاص.

مجلة قضايا سياسية

pissue.iq

- يجوز للمجلة أن تطلب إجراء تعديلات شكلية أو شاملة على البحث أو الدراسة قبل إجازتها للنشر بما يتماشى مع أهدافها.
- البحوث المنشورة تعبر عن آراء أصحابها ، ولاتعبر عن راي المجلة .
- ترحب المجلة بالمناقشات الموضوعية لما ينشر فيها أو في غيرها من الدوريات وبأية ردود فكرية أو تصويب، وكذلك ترحب بنشر التقارير عن المؤتمرات والندوات ذات العلاقة ومراجعات الكتب وملخصات الرسائل الجامعية التي تتم إجازتها على أن تكون من إعداد أصحابها.

توجه جميع المراسلات إلى هيأة التحرير على العنوان الآتي
مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين-بغداد – الجادرية.
E.mail: pirj@nahrainuniv.edu.iq

الموقع الاليكتروني
https://pissue.iq/index.php/pissue

E-ISSN 2790-2404
P- ISSN 2070-9250
DOI prefix: 10.58298

جدول المحتويات

مستقبل مكانة القوة السيبرانية في استراتيجيات القوى الإقليمية ايران انموذجا[▽]

The future of the position of cyber power in the strategies of regional forces: Iran as a model.

م.م محمد معن محسن[*] MOHAMMED MAAN MOHSIN

الملخص

تتناول هذه الدراسة مستقبل القوة السيبرانية كأحد العناصر الفاعلة في صياغة استراتيجيات القوى الإقليمية، مع التركيز على إيران كنموذج بارز في هذا المجال ، اذ بات الفضاء السيبراني يشكّل ساحةً جديدة للتأثير والصراع، تستخدمها الدول لتعزيز قوتها، والحد من نفوذ خصومها، وتحقيق مكاسب سياسية وأمنية دون اللجوء إلى القوة التقليدية ، ويبرز هذا البحث كيف أن إيران، في ظل التحديات المتعددة التي تواجهها، تتجه نحو تطوير قدراتها السيبرانية بوصفها أداة استراتيجية لتعويض مكامن الضعف في المجالات الأخرى، ولبناء ردع غير تقليدي يعزّز من مكانتها في محيطها الإقليمي ، ويركّز البحث على تحليل دوافع إيران السيبرانية، وأهدافها، والتحديات التي تواجهها، فضلاً عن السيناريوهات المحتملة لمستقبل استخدامها لهذه القوة في إطار صراعات الشرق الأوسط.

الكلمات المفتاحية: ايران – القوة السيبرانية – الفضاء السيبراني

Abstract

This study addresses the future of cyber power as one of the active elements in shaping the strategies of regional powers, focusing on Iran as a prominent model in this field. The cyber space has become a new arena for influence and conflict, used by countries to enhance their power, limit the influence of their adversaries, and achieve political and security gains without resorting to traditional power. This research highlights how Iran, in light of the multiple challenges it faces, is moving towards developing its cyber capabilities as a strategic tool to compensate for weaknesses in other areas and to build an unconventional deterrent that enhances its position in its regional environment. The research focuses on analyzing Iran's cyber motives, objectives, challenges it faces, as well as the potential scenarios for the future use of this power within the context of conflicts in the Middle East.

Keywords: Iran - Cyber power - Cyberspace .

▽ تاريخ التقديم : 2025/3/13 تاريخ القبول: 2025/4/9 تاريخ النشر: 2025/6/30

* جامعة النهرين / قسم الاستراتيجية Muhammad.Maan@nahrainuniv.edu.iq

المقدمة

تشهد البيئة الدولية تحوّلات متسارعة بفعل الثورة الرقمية والتطورات التكنولوجية، ما أسهم في بروز الفضاء السيبراني بوصفه ميداناً جديداً للتنافس والصراع بين الدول ، ولم تعد القوة السيبرانية مقتصرة على الجانب التقني أو الدفاعي، بل أصبحت أداة استراتيجية تعتمد عليها الدول لتحقيق مصالحها، وفرض تأثيرها في الإقليم والعالم ، وفي هذا السياق، برزت إيران كإحدى القوى الإقليمية التي تولي أهمية متزايدة لتطوير قدراتها السيبرانية ضمن استراتيجياتها الشاملة، لاسيما في ظل التحديات الأمنية والسياسية التي تواجهها.

أهمية البحث

تنبع أهمية الموضوع من تركيزه على بُعدٍ استراتيجي متنامٍ في بنية العلاقات الدولية المعاصرة، وهو القوة السيبرانية، مع تسليط الضوء على إيران كنموذج إقليمي يسعى إلى توظيف هذه القوة في تعزيز مكانته ومصالحه ، كما يسهم في فهم آليات توظيف الفضاء السيبراني كأداة للردع، والتأثير ، وإعادة تشكيل موازين القوة على المستويين الإقليمي والدولي.

هدف البحث

يهدف البحث إلى تحليل الاستراتيجيات السيبرانية لإيران في سياق التنافس الإقليمي، مع التركيز على الدوافع والأساليب (كالهجمات بالبرامج الضارة، التصيد الاحتيالي، وحروب الوكالة) ،إضافة الى تقييم مدى تأثير هذه القدرات على توازن القوى في الشرق الأوسط، خاصةً في ظل تحوُّل الصراع إلى الفضاء الإلكتروني مع استشراف مستقبل الدور السيبراني للقوى الإقليمية في ضوء التطورات التكنولوجية والتحالفات الدولية

اشكالية البحث

تثار إشكالية الموضوع من التساؤل الرئيس (كيف تسهم القوة السيبرانية في إعادة تشكيل المكانة الإقليمية لإيران ضمن استراتيجياتها المستقبلية؟) .

فرضية البحث

فرضية البحث مفادها (تعمل إيران على دمج القوة السيبرانية في استراتيجياتها الإقليمية كوسيلة لتعزيز نفوذها، والتعامل مع التهديدات الأمنية، وموازنة تفوق خصومها في المجالات التقليدية) .

الاطار المنهجي للبحث

سيتم تقسيم هذا البحث الى ثلاث محاور وكالاتي :

أولاً : القوة السيبرانية الإيرانية

تُظهر إيران تطورًا ملحوظًا في مجال التكنولوجيا السيبرانية، خاصة في ظل العقوبات الدولية وضرورة تطوير حلول محلية ، ويهدف هذا المحور إلى تحليل مكونات القوة السيبرانية الإيرانية وقياسها عبر دراسة الجوانب التكنولوجية، الاستراتيجية، والعسكرية.

ولقياس القوة السيبرانية لدولة ما، يتم النظر في عدة معايير، منها:(سليخ ، 2022 ، ص 65)

1. البنية التحتية السيبرانية وتشمل شبكات الاتصالات، مراكز البيانات، والتكنولوجيا المستخدمة.
2. الموارد البشرية أي مدى توفر الكفاءات والخبرات في مجال تقنية المعلومات والأمن السيبراني.
3. القدرات الهجومية والدفاعية وتشمل الأدوات والتقنيات المستخدمة في الهجمات السيبرانية والحماية منها.
4. الإطار القانوني والتنظيمي عبر وجود سياسات وقوانين تنظم الفضاء السيبراني وتحدد مسؤوليات الجهات المختلفة.

وقد بدأ اهتمام إيران بالفضاء السيبراني في أوائل العقد الأول من القرن الحادي والعشرين عبر تعرضها لهجمات سيبرانية كفيروس ستوكسنت في عام 2010 الذي استهدف برنامجها النووي ممادفعها لتعزيز قدراتها في هذا المجال ، ومنذ ذلك الحين، شهدت إيران تطورًا ملحوظًا في قدراتها السيبرانية، مع التركيز على بناء بنية تحتية قوية وتطوير مواردها البشرية. (جاسيم ، 2024 ، ص 195)

واستثمرت إيران في تطوير بنيتها التحتية السيبرانية، بما في ذلك شبكات الاتصالات ومراكز البيانات، كما قامت بتدريب وتأهيل كوادر متخصصة في مجال الأمن السيبراني ، اذ تشير التقارير إلى استخدام إيران لتقنيات وأدوات متقدمة في هجماتها السيبرانية، كالبرمجيات الخبيثة وتقنيات التصيد الاحتيالي ، وعلى الرغم من العقوبات الدولية، تمكنت إيران من تحقيق تقدم ملحوظ في هذا المجال.(فرج ،2022،ص 188)

وتعتمد إيران على استراتيجيات هجومية ودفاعية في الفضاء السيبراني ، فهي تعمل على حماية بنيتها التحتية من الهجمات المحتملة، وفي الوقت نفسه، تنفذ هجمات سيبرانية تستهدف مؤسسات حكومية وخاصة في دول أخرى ، وتُظهر الهجمات المنسوبة إلى إيران تنوعًا في الأهداف والأساليب، مما يعكس مرونة وقدرة على التكيف مع التحديات المختلفة. .(جاد،2020،ص 189)

شهدت إيران عبر العقدين الماضيين تطورًا ملحوظًا في مجال التكنولوجيا السيبرانية، مما جعلها لاعبًا رئيسيًا في الساحة الإلكترونية العالمية ، هذا التطور جاء نتيجة لاستثمارات استراتيجية في البنية التحتية الرقمية، وتطوير القدرات الهجومية والدفاعية، بالإضافة إلى تعزيز الكفاءات البشرية المتخصصة في هذا المجال.

ففي العام 2011، تعرضت إيران لهجمات إلكترونية معقدة، كفيروس ستارز الذي استهدف أنظمة التحكم الصناعية، وفيروس دوكو الذي صُمم لسرقة البيانات الحساسة ، هذه الهجمات كانت بمثابة حافز لإيران لتعزيز قدراتها السيبرانية، اذ قامت بإنشاء هيكل مؤسسي متكامل يضم المجلس الأعلى للفضاء الإلكتروني، وقيادة الدفاع الإلكتروني، والجيش الإلكتروني الإيراني، وكتائب الباسيج الإلكترونية، ووحدة مكافحة الجريمة الإلكترونية ، هذه المؤسسات تعمل بتناغم لتعزيز الأمن السيبراني وحماية البنية التحتية الحيوية للدولة.(إلياس، فراس (2023)، عقيدة الأمن السيبراني في إيران ومعادلات المواجهة مع أمريكا،

(https://www.noonpost.com/content/28950

لذلك ، استثمرت إيران في تطوير قدراتها في مجالات التكنولوجيا المتقدمة كالنانو والذكاء الاصطناعي ، منذ العام 2000، وحققت تقدمًا ملموسًا في تكنولوجيا النانو، اذ تحتل حاليًا المرتبة الرابعة عالميًا في إنتاج أبحاث النانو، مع نشر 8791 مقالة في هذا المجال ، وفي تموز من العام 2024، أطلقت إيران المنظمة الوطنية للذكاء الاصطناعي بهدف وضعها ضمن الدول العشر الأولى التي تستخدم الذكاء الاصطناعي لدعم الحوكمة والاقتصاد الرقمي بحلول عام 2034. .(إلياس، فراس (2023)، عقيدة الأمن السيبراني في إيران ومعادلات المواجهة مع أمريكا، https://www.noonpost.com/content/28950)

اما التطور التكنولوجي السيبراني الإيراني فيمكن تناوله عبر الاتي :

1. البنية التحتية الرقمية ، فقد شهدت إيران تطورًا ملحوظًا في بنيتها التحتية السيبرانية، مما مكّنها من بناء قدرات إلكترونية تنافس الدول الكبرى كالولايات المتحدة والصين وروسيا ، وقد ساهمت العقوبات الدولية في دفع إيران نحو تطوير تقنياتها المحلية لتعزيز أمنها السيبراني ، وكالاتي : (راشد ، 2021 ، ص 188)

أ- شبكات الاتصالات عبر تطوير شبكات G5 محلية بالتعاون مع شركات صينية.

ب- مراكز البيانات عبر إنشاء مراكز كشبكة المعلومات الوطنية (NIN) لعزل الإنترنت المحلي.

ت- الشبكات المحلية ، تعتمد إيران على شبكة الإنترنت الوطنية المُنفصلة جزئيًا عن الإنترنت العالمي، لضبط تدفق المعلومات وتعزيز الأمن السيبراني الداخلي .

ث- التكنولوجيا الناشئة ، تُطور إيران تقنيات مثل الشبكات الذكية وإنترنت الأشياء (IoT) بدعم من مؤسسات كمنظمة الفضاء الإيرانية .

2. القدرات الهجومية: تملك إيران قدرات سيبرانية هجومية متقدمة، اذ أنشأت وحدات متخصصة في شن هجمات إلكترونية على المؤسسات الحكومية والشركات الأجنبية، بالإضافة إلى تنفيذ عمليات تجسس سيبراني ، وتملك إيران تفوقًا كبيرًا في القدرات العسكرية غير المتماثلة، وتستخدم في ذلك وكلاءها عبر تزويدهم بالتكنولوجيا العسكرية المنخفضة التكلفة لموازنة قوى خصومها الأكثر تقدمًا من الناحية التكنولوجية ، وقد نفذت إيران هجمات سيبرانية استهدفت بنى تحتية حيوية في دول منافسة، مما يعكس قدراتها الهجومية المتقدمة. ومن بين أبرز القدرات الهجومية التي طورتها إيران: (فياض ، 2025 ، ص 191-194)

أ- هجمات الفدية ، استُخدمت هذه التقنية لتعطيل أنظمة حيوية في الدول المنافسة.

ب- الهجمات التخريبية ، شملت تعطيل أنظمة البنية التحتية مثل شبكات الكهرباء والمنشآت النووية.

ت- الهجمات على سلاسل التوريد ، استهدفت شركات التقنية الكبرى التي توفر خدمات رقمية للقطاع الحكومي والعسكري في بعض الدول.

ث- مجموعات القرصنة الموالية للحكومة كـ(APT34، Charming Kitten).

ج- وحدة الجيش السيبراني التابعة للحرس الثوري (IRGC)، المسؤولة عن هجمات كتعطيل أنظمة البنوك الأمريكية (2013)

ح- مجموعة APT33 المُتخصصة في استهداف قطاع الطاقة العالمي

3. الدفاع السيبراني : على المستوى الدفاعي ، استثمرت إيران في تعزيز أمن شبكاتها وحماية معلوماتها الحساسة، معترفةً بأهمية الأدوات السيبرانية والذكاء الاصطناعي في سياستها الخارجية، رغم القيود المالية والعلمية التي تواجهها ، كما أنشأت إيران أنظمة متقدمة لحماية شبكاتها الحكومية والعسكرية، إلى جانب تطوير برامج للحماية من الاختراق والتجسس السيبراني، بما في ذلك: (عبد الله، (2023) ،الجيش السيبراني الإيران القوة السرية المدمرة ، https://www.garasanews.com/article/325741)

أ- تعزيز تقنيات التشفير لحماية المعلومات الحساسة.

ب- تطوير جدار ناري وطني لمراقبة حركة البيانات ومنع الاختراقات الخارجية.

ت- إنشاء مراكز متخصصة لمراقبة الفضاء السيبراني والاستجابة السريعة للهجمات.

ث- تطوير أنظمة مراقبة كالدرع الوطني للإنترنت وأنظمة الدرع السيبراني لحماية المنشآت النووية والمالية .

ج- إنشاء قيادة الجيش السيبراني تحت إشراف الحرس الثوري.

ح- تُموّل إيران مشاريع بحثية في جامعات كجامعة شريف التكنولوجية لدمج الذكاء الاصطناعي في الحرب الإلكترونية، كخوارزميات كشف الاختراقات .

وتعمل إيران على تطوير تقنيات الذكاء الاصطناعي لتعزيز قدراتها في مجال الأمن السيبراني، اذ تستخدم هذه التقنيات في تحليل البيانات الضخمة، واكتشاف التهديدات السيبرانية، وتحسين استراتيجيات الدفاع الإلكتروني. وتشمل بعض المجالات التي تركز عليها إيران في هذا الجانب: (المنتظر،2023 ، ص 162)

أ- تطوير برمجيات متقدمة للكشف عن الهجمات السيبرانية والاستجابة لها.

ب- استخدام الذكاء الاصطناعي في عمليات الاختراق والاختراق المضاد .

ت- تحسين تقنيات التشفير وأمن المعلومات لحماية الاتصالات الحكومية والعسكرية.

ويمكن فهم الدوافع الكامنة وراء التطور السيبراني الإيراني عبر حدث محوري، وهو الهجوم الإلكتروني الشهير بفيروس ستوكسنت عام 2010، الذي استهدف المنشآت النووية الإيرانية، اذ كشف هذا الهجوم، الذي نُسب إلى تحالف أمريكي-إسرائيلي، عن نقاط ضعف خطيرة في البنية التحتية الإيرانية، مما دفع بايران إلى إعادة تقييم أولوياتها الأمنية ، ووفقًا لتقرير معهد كارنيغي للسلام الدولي (2021)، تحول هذا الهجوم إلى حافزٍ استراتيجي لإنشاء قيادة الدفاع السيبراني التابعة للحرس الثوري الإسلامي، والتي أصبحت نواةً للقدرات الهجومية والدفاعية الإيرانية. وهكذا، مثلت الأزمة نقطة تحول نحو استثمار غير مسبوق في البحث والتطوير السيبراني.(المنتظر، 2023 ، ص 166.)

فقد أدركت إيران مبكرًا أن تحقيق السيادة الرقمية يتطلب بناء بنية تحتية مستقلة ، وفي هذا الإطار، أطلقت عام 2012 مشروع الشبكة الوطنية للمعلومات، وهو نظام إنترنت محلي يهدف إلى تقليل الاعتماد على الخوادم الدولية، مما يوفر سيطرة أكبر على تدفق البيانات ويحد من مخاطر التجسس الخارجي ، ووفقًا لوثيقة الاستراتيجية السيبرانية الإيرانية (2025)، يعد هذا المشروع ركيزةً للاقتصاد المقاوم الذي تروج له ايران، والذي يركز على الاكتفاء الذاتي في ظل العقوبات ، بالإضافة إلى ذلك، أسست إيران "مركز التنسيق الوطني للفضاء الإلكتروني" لمراقبة التشريعات وتنسيق الجهود بين المؤسسات العسكرية والمدنية، مما يعكس نهجًا شموليًا في إدارة الفضاء الرقمي.

لذا شهدت إيران في العقود الأخيرة تقدمًا ملحوظًا في المجال التكنولوجي السيبراني، مما جعلها واحدة من الدول البارزة في هذا المجال على المستويين الإقليمي والدولي. هذا النمو لم يكن وليد الصدفة، بل جاء نتيجة مجموعة من العوامل التي أسهمت في تعزيز قدراتها السيبرانية وتطوير بنيتها التحتية الرقمية.

وقد تميز النموذج الإيراني بتكامل غير مسبوق بين القطاعات العسكرية والمدنية ، فالحرس الثوري الإسلامي، على سبيل المثال، لا يقتصر دوره على العمليات الأمنية، بل يدير أيضًا حاضنات تكنولوجية تدعم الشركات الناشئة في مجالات كالذكاء الاصطناعي وتحليل البيانات ، هذا التكامل يخلق بيئةً تسمح بتحويل الابتكارات المدنية إلى أدوات استراتيجية. وفقًا لدراسة أجراها مركز الأبحاث التابع للأمم المتحدة فإن هذا النهج يُعد استجابةً لطبيعة الحروب الحديثة، التي تزداد فيها الحدود بين الجبهات العسكرية والاقتصادية غموضًا. (الجبوري ، (2023) ، الحرب السيبرانية في الشرق : ايران واسرائيل نموذجا، https://www.alfalq.com/?p=12120)

وعلى الرغم من التقدم المحرز، لا تزال إيران تواجه تحديات تقنية في بعض القطاعات، خاصة عند مقارنتها بدول متقدمة في المجال السيبراني كالصين ، ومع ذلك، تستمر إيران في تعزيز قدراتها الإلكترونية كجزء من استراتيجيتها للدفاع المتقدم، مستفيدة من تكتيكات الحرب غير المتكافئة لتعزيز موقعها في المشهد الجيوسياسي العالمي ، ويعكس التطور التكنولوجي السيبراني الإيراني التزام الدولة بتعزيز قدراتها التقنية والدفاعية، مع التركيز على الابتكار والتطوير المستمر في مجالات التكنولوجيا المتقدمة ، وعلى الرغم من التقدم الإيراني في مجال القوة السيبرانية ، تواجه إيران تحديات عدة، منها (الماجدي ، 2022 ، ص 195)

1. العقوبات الدولية والتي تحد من قدرتها على الحصول على التكنولوجيا المتقدمة وتطوير بنيتها التحتية ، اذ تؤثر العقوبات الاقتصادية والتكنولوجية على قدرة إيران في الحصول على تقنيات متقدمة وتطوير بنيتها التحتية السيبرانية.
2. الثغرات الأمنية والتحديات الداخلية ، اذ تواجه إيران تحديات في تأمين بنيتها التحتية الرقمية من الهجمات السيبرانية، وقد تعرضت لهجمات استهدفت منشآتها الحيوية، كالهجوم على محطات الوقود في عام 2021.

3. الاستجابة الدولية للهجمات السيبرانية الإيرانية، تؤدي الهجمات السيبرانية المنسوبة إلى إيران إلى ردود فعل دولية، بما في ذلك تعزيز الدفاعات السيبرانية وفرض عقوبات إضافية، مما يزيد من عزلة إيران التقنية.

ختاما تمتلك إيران قوة سيبرانية متوسطة المستوى مع قدرات هجومية متفوقة على الجانب الدفاعي، فعلى الرغم من التحديات، فإن الاستثمار في الكوادر والتكنولوجيا المحلية عزز مكانتها كفاعل رئيسي في الفضاء الإلكتروني مما جعل فهم قوتها السيبرانية يتطلب رصدًا مستمرًا لتحالفاتها وتكتيكاتها المتغيرة ، اذ تمكنت إيران من بناء قوة سيبرانية مؤثرة رغم العقوبات، مع تركيز واضح على الجانب الهجومي ، ومع ذلك، فإن ضعف البنية التحتية الدفاعية واعتمادها على التكنولوجيا الأجنبية يحدان من قدرتها على منافسة دول كإسرائيل ، ويُتوقع أن تستمر إيران في تعزيز تحالفاتها مع روسيا والصين لسد الفجوات التقنية.

ثانياً_ مجالات استخدام القوة السيبرانية الإيرانية وانعكاساتها على الأمن الإقليمي

تُمثل القوة السيبرانية الإيرانية أحد أبرز أدوات الاستراتيجية الإيرانية في تحقيق أهدافها الجيوسياسية، سواء عبر الهجمات التخريبية أو التجسس أو حروب المعلومات ، اذ تُساهم هذه القدرات في تعزيز النفوذ الإقليمي لإيران، لكنها تثير في الوقت نفسه تحديات أمنية جسيمة لدول الشرق الأوسط والعالم.

ومن بين أبرز مجالات استخدام القوة السيبرانية الإيرانية هو المجال العسكري، اذ أصبحت العمليات الإلكترونية جزءًا لا يتجزأ من استراتيجيات إيران الدفاعية والهجومية ، وقد تم تطوير وحدات سيبرانية داخل الحرس الثوري الإيراني ووحدات عسكرية أخرى، تهدف إلى تنفيذ عمليات اختراق وتجسس إلكتروني ضد الخصوم ، وفي أكثر من مناسبة، أشارت تقارير استخباراتية إلى ضلوع إيران في هجمات إلكترونية استهدفت منشآت عسكرية وحكومية في دول الخليج العربي، في إطار ما يُعرف بالحروب غير المتكافئة، اذ تستخدم إيران القوة السيبرانية لتعويض الفجوة في القوة التقليدية مقارنة بخصومها الإقليميين.(الجاسم،2024،ص153) إلى جانب المجال العسكري، تُستخدم القوة السيبرانية الإيرانية في استهداف البنية التحتية الحيوية لدول المنطقة، وهو ما يشكل تهديدًا مباشرًا للأمن الإقليمي ، فالبنية التحتية التي تشمل قطاعات الطاقة، المياه، النقل، والاتصالات، تُعد من الأهداف الرئيسية للهجمات السيبرانية الإيرانية، خاصة في ظل التوترات الجيوسياسية المستمرة ، وفي حالات عدة ، تعرضت منشآت نفطية ومرافق حكومية في دول خليجية لهجمات إلكترونية يُعتقد أنها مرتبطة بمجموعات سيبرانية مدعومة من إيران، بهدف إلحاق الضرر الاقتصادي والضغط السياسي على هذه الدول ، مثل هذه الهجمات لا تهدد فقط الأمن الاقتصادي للدول المستهدفة، وإنما تمتد تأثيراتها إلى الأمن الإقليمي ككل، نظرًا لاعتماد المنطقة الكبير على القطاعات المستهدفة، خصوصًا قطاع الطاقة، الذي يُعد عصب الاقتصاد العالمي. (رؤوف،(2024)، "إسرائيل" على الجبهة الإلكترونية، https://metras.co/)

ومن المجالات الأخرى التي تستغل فيها إيران قوتها السيبرانية هو مجال التجسس الإلكتروني، اذ طورت قدرات عالية في مجال اختراق الأنظمة الحكومية وجمع المعلومات الاستخباراتية عن خصومها الإقليميين والدوليين عبر تنفيذ عمليات قرصنة متطورة، فقد تمكنت وحدات سيبرانية إيرانية من الوصول إلى بيانات حساسة تتعلق بالمؤسسات العسكرية والأمنية والاقتصادية للدول المجاورة ، ولايقتصر التجسس الإلكتروني على سرقة المعلومات فقط، بل يُستخدم أيضًا في تنفيذ عمليات التأثير والتلاعب بالمعلومات بهدف إرباك الخصوم وتضليل صانعي القرار ، وقد كشفت عدة تقارير عن محاولات إيرانية لاختراق أنظمة بعض الوزارات والمنظمات الإقليمية، مما يؤكد اعتمادها على الفضاء السيبراني كوسيلة لتعزيز مكانتها الأمنية والسياسية . (رؤوف،(2024)، "إسرائيل" على الجبهة الإلكترونية، https://metras.co/)

اما على انعكاسات استخدام القوة السيبرانية الإيرانية على الأمن الإقليمي في المنطقة تتجلى في عدة مستويات، أبرزها زيادة حدة الصراعات الإقليمية، اذ أدى تصاعد الهجمات الإلكترونية بين إيران وخصومها الإقليميين إلى نشوء بيئة أمنية غير مستقرة، تجعل من المواجهة السيبرانية عاملًا مؤججًا للتوترات ، كما أن هذا التصعيد يزيد من مخاطر اندلاع صراعات أوسع، خاصة في ظل تزايد اعتماد الدول على البنى التحتية الرقمية، ما يجعلها أكثر عرضة للهجمات السيبرانية التي قد تتسبب في خسائر اقتصادية وأمنية كبيرة. (عبد الحميد ، 2023 ،ص101)

إلى جانب ذلك، تساهم القوة السيبرانية الإيرانية في إعادة تشكيل ميزان القوى في المنطقة، اذ تمنح هذه القدرات لايران أدوات جديدة لتعزيز نفوذها دون الحاجة إلى اللجوء إلى المواجهات العسكرية التقليدية ، عبر تنفيذ عمليات سيبرانية دقيقة ، هذا التحول في طبيعة الصراع يجعل الأمن الإقليمي أكثر تعقيدًا، اذ لم تعد التهديدات تقتصر على المواجهات التقليدية، بل أصبحت تشمل الهجمات الإلكترونية التي يصعب التنبؤ بها أو احتواؤها بسهولة. (عبد الحميد ، 2023 ،ص 102)

ففي ظل التحولات الجيوسياسية التي يشهدها الشرق الأوسط، تبرز التكنولوجيا السيبرانية كأداة محورية لإعادة تشكيل موازين القوى الإقليمية ، اذ تُعد إيران واحدة من الدول التي استثمرت بكثافة في تطوير قدراتها السيبرانية، ليس فقط كآلية دفاعية، بل كأداة هجومية لتعزيز نفوذها الإقليمي. (صالح، 2023، ص97)

وتنبع أولوية التكنولوجيا السيبرانية في الاستراتيجية الإيرانية من إدراك ايران أن الفضاء الإلكتروني بات ساحةً حاسمة لتحقيق أهدافها الأمنية والاستراتيجية ، ففي ظل العقوبات الدولية والضغوط العسكرية المباشرة، تُقدم القدرات السيبرانية بديلًا مرنًا لتنفيذ عمليات استخباراتية وهجمات مضادة دون التورط في مواجهات تقليدية مكلفة ، وفقًا لتقرير مؤسسة راند الامريكية للعام (2022)، فإن إيران تعتمد على الإنكار المُحكم في عملياتها السيبرانية، مما يمكنها من تحقيق أهداف سياسية مع الحفاظ على الغموض حول مسؤوليتها المباشرة. (صالح، 2023، ص 99)

وتتنوع مجالات توظيف إيران لقدراتها السيبرانية بين أهداف استخباراتية وعسكرية واقتصادية: (عزي ،(2024) ، النشاط السيبراني الايراني مابين السر والعلن، https://trendsresearch.org/research.)

1. التجسس الإلكتروني ، اذ تُستخدم التقنيات السيبرانية لاختراق أنظمة الحكومات والشركات في الدول المنافسة، كالسعودية والإمارات وإسرائيل ، ففي العام 2020، كشف تقرير لشركة "كاسبرسكي" عن حملة تجسس إيرانية استهدفت مؤسسات حكومية في الخليج عبر ثغرات في برمجيات إدارة الشبكات.
2. تخريب البنى التحتية الحيوية، تمتلك إيران سجلاً من الهجمات على منشآت الطاقة والنقل، ففي العام 2012، تسببت هجمات إيرانية مزعومة ببرنامج "شمعون" في تعطيل آلاف الحواسيب في شركة أرامكو السعودية، مما كشف عن قدرات متقدمة في إلحاق الضرر المادي عبر الفضاء الرقمي.
3. حروب المعلومات ، تُوظف إيران مجموعات إلكترونية موالية لنشر حملات التضليل الإعلامي، كاختراق حسابات صحفية في دول الخليج لبث رسائل معارضة أو زعزعة الثقة في الحكومات ، وفقًا لدراسة مركز "أطلانتيك كاونسل" (2023)، فإن هذه الحملات تهدف إلى تعميق الانقسامات الداخلية في المجتمعات المستهدفة. وقد أدت الأنشطة السيبرانية الإيرانية إلى تفاقم التوترات الإقليمية عبر آليات متعددة: (جاسب، 2024، ص 124)

1. زعزعة الاستقرار الداخلي للدول اذ تُشكل الهجمات على البنى التحتية، كشبكات الكهرباء أو الأنظمة المالية، تهديدًا مباشرًا لأمن المواطنين واقتصادات الدول. ففي العام 2021، أدى هجوم إلكتروني على ميناء جبل علي في الإمارات إلى شل العمليات اللوجستية لأيام، مما أثار مخاوف من تكرار مثل هذه الحوادث في منشآت استراتيجية أخرى.
2. سباق التسلح السيبراني ، اذ دفع التهديد الإيراني دولًا كإسرائيل والسعودية إلى تعزيز إنفاقها على الأمن السيبراني ، فوفقًا لمؤشر "ستاتيستا" (2023)، تضاعفت ميزانيات الأمن السيبراني في الخليج ثلاث مرات منذ 2015، مع تركيز خاص على تطوير وحدات هجومية ردعية.
3. تأثير التحالفات الدولية، فقد أجبرت الهجمات الإيرانية بعض الدول العربية على تعميق تعاونها مع الولايات المتحدة وحلف الناتو في مجال الدفاع السيبراني، مما أدى إلى إعادة رسم تحالفات إقليمية تقليدية.

وعل الرغم من فعالية الأدوات السيبرانية، فإن استخدامها يثير تساؤلات حول انتهاك القانون الدولي، فالهجمات على البنى التحتية المدنية كالمستشفيات أو محطات المياه، تتعارض مع مبادئ "قانون الحرب" التي تحظر استهداف المنشآت غير العسكرية ، بالإضافة إلى ذلك، تتعرض إيران لانتقادات بسبب استخدامها للقرصنة المالية (كسرقة الأموال عبر اختراق البنوك)، والتي تُعد شكلاً من أشكال الإرهاب الاقتصادي. (الكناني ، 2025، ص236)

وتشير التطورات الأخيرة إلى أن التكنولوجيا السيبرانية الإيرانية ليست مجرد أداة تقنية، بل عاملٌ جيوسياسي يعيد تعريف قواعد الاشتباك في المنطقة ، فمن ناحية، تمكنت ايران من تحويل الفضاء الإلكتروني إلى مجال لتعويض نقاط ضعفها العسكرية والاقتصادية ، ومن ناحية أخرى، أدت هذه الاستراتيجية إلى تفكيك الحدود التقليدية بين الأمن الداخلي والخارجي، اذ أصبحت الهجمات السيبرانية قادرة على عبور الحدود الوطنية في غضون ثوانٍ. (الشرقي ، 2024، ص 200)

ختاما قد يتطلب تعزيز الأمن الإقليمي تطوير آليات تعاون جديدة، كإنشاء منصة إقليمية لتبادل المعلومات حول التهديدات السيبرانية، أو صياغة معاهدات تحظر استخدام الهجمات ضد البنى التحتية الحيوية ، ومع ذلك، يبقى التحدي الأكبر هو بناء الثقة بين دول تتصارع على النفوذ في ظل بيئة إقليمية مُتشظية.

ثالثاً_ مستقبل القوة السيبرانية الايرانية في ظل استراتيجيات القوى الإقليمية في المنطقة

أصبحت القوة السيبرانية أحد أهم أبعاد الصراع الجيوسياسي في الشرق الأوسط، اذ تُعَد إيران من أبرز الفاعلين في هذا المجال ، اذ تبذل إيران جهودًا كبيرة لتطوير قدراتها في هذا المجال كجزء من استراتيجيتها العسكرية والأمنية الأوسع ، ويهدف هذا المحور إلى تحليل مستقبل القوة السيبرانية الايرانية وتأثيرها على الاستراتيجيات الإقليمية في السنوات القادمة ، عبر الاتي :

1- الانكفاء على الذات (السيادة السيبرانية)

تواجه إيران تحديات داخلية قد تُعيد توجيه استراتيجياتهما السيبرانية ، فإيران، تعاني من أزمات اقتصادية حادة بسبب العقوبات، مما يحدُّ من استثماراتها في التكنولوجيا المتطورة، ويجعلها تعتمد على الهجمات منخفضة الجودة التي تركز على الإزعاج الإعلامي أكثر من التأثير الاستراتيجي، كاختراق المواقع الإلكترونية الحكومية.

ويعتمد مفهوم الانكفاء على الذات في المجال السيبراني على سعي الدول إلى تعزيز اكتفائها التكنولوجي، سواء عبر تطوير بنى تحتية محلية أو تقليل الاعتماد على الشركاء الخارجيين ، بالنسبة لإيران، التي تحتل المرتبة العاشرة في مؤشر القوة السيبرانية العالمية وفقاً لتصنيف مركز بيلفر للعام 2024 ، تسعى إلى تعزيز قدراتها عبر الاستثمار في البنية التحتية العسكرية السيبرانية، مدفوعةً بالعقوبات الدولية التي تحدُّ من وصولها إلى التقنيات الغربية. (الكناني ، 2025، ص 245)

وتدفع مجموعة من العوامل إيران إلى تبني نهج الانكفاء على الذات في مجال القوة السيبرانية ، فالتوجه الايراني نحو الانكفاء على الذات ينبع من الضغوط الاقتصادية والسياسية التي تواجهها نتيجة العقوبات الدولية والعزلة الدبلوماسية كما أن تعرض إيران لهجمات سيبرانية متكررة، عزز لديها قناعة بأن تحقيق الاستقلالية في المجال السيبراني ضرورة أمنية وليست مجرد خيار استراتيجي.(جاك، 2024،ص253)

ورغم الفوائد التي قد تجنيها إيران من تعزيز استقلاليتها السيبرانية، إلا أن هذا التوجه لا يخلو من تحديات جوهرية ، أحد أبرز هذه التحديات يكمن في صعوبة تحقيق الاكتفاء الذاتي التام في قطاع شديد التعقيد

كالأمن السيبراني، فبالنسبة لإيران، فالتحديات كبيرة جدا نظرًا للعقوبات التي تقيد وصولها إلى التكنولوجيا المتقدمة والخبرات الأجنبية .(عبدالحي، 2024 ، ص 141)

ويمكن تحديد ابرز التحديات التي تواجها والمحصورة بين القيود الداخلية والضغوط الخارجية بالاتي : .(الكناني، 2025،ص 250)

1. العقوبات الدولية وإشكالات التطوير التكنولوجي ، تُعاني إيران من تحديات جسيمة في تطوير قدراتها السيبرانية بسبب العقوبات الاقتصادية التي تعوق استيراد المكونات التكنولوجية المتطورة ، هذا الواقع يدفعها إلى الاعتماد على حلول محلية قد تكون أقل كفاءة .

2. الاستقطاب السياسي وتقلبات الأولويات : يُهدِّد الاستقطاب السياسي الداخلي وتباين الرؤى بتباطؤ الاستثمار في البنية التحتية السيبرانية .

3. التهديدات العابرة للحدود وتعقيدات الإسناد ، تُواجه ايران صعوبات في إدارة التهديدات السيبرانية المتبادلة بسبب طبيعة الهجمات غير المنسوبة ، مما يُعقِّد عملية الرد وفقاً للقانون الدولي .

اما الفرص التي يوفرها الانكفاء على الذات في المجال السيبراني ، فعلى الرغم من التحديات المرتبطة بمشهد الانكفاء على الذات، إلا أن هذا التوجه يحمل في طياته فرصًا استراتيجية ، اذ إن تعزيز قدراتها المحلية في المجال السيبراني يمنحها أداة قوية للحفاظ على أمنها القومي، خاصة في ظل التهديدات المستمرة من قبل الولايات المتحدة وإسرائيل ودول أخرى . (بلا،(2024) ، استراتيجية اسرائيلية شرسة للأمن الإلكتروني تستهدف ايران، https://www.skynewsarabia.com/world/1184165)

ويؤثر مشهد الانكفاء على الذات في المجال السيبراني بشكل مباشر على التوازنات الإقليمية، اذ يؤدي إلى تعزيز الاستقطاب بين القوى الفاعلة في المنطقة ، اذ تستفيد إيران من علاقتها مع حلفائها الإقليميين، كحزب الله وحماس ، لتعزيز عملياتها السيبرانية في مواجهة خصومها . كما أن التحول نحو مزيد من الاستقلالية السيبرانية قد يؤدي إلى تصاعد حروب الظل (الحروب بالوكالة) بين إسرائيل وإيران، اذ يعتمد الطرفان بشكل متزايد على العمليات السيبرانية كبديل عن المواجهات العسكرية التقليدية ، وقد نشهد في المستقبل مزيدًا من الهجمات على البنى التحتية الحيوية، كشبكات الكهرباء والمواصلات والأنظمة المصرفية، مما يزيد من تعقيد المشهد الأمني في الشرق الأوسط. (عبد العزيز ، (2024)، إدراك التهديد وآفاق الحوار المتوسطي لحلف الناتو، https://emirate.wiki/wiki/Balance_of_threat)

يُهدِّد الانكفاء على الذات بتعزيز ديناميكيات الصراع غير المباشر ، اذ تُصبح الهجمات السيبرانية أداةً رئيسية لزعزعة الاستقرار الإقليمي ، اذ تعاني إيران من تراجع قدراتها بسبب العزلة الدولية، مما يدفعها إلى اعتماد استراتيجيات هجينة تجمع بين الحرب السيبرانية والحروب بالوكالة عبر حلفائها الاقليمين . (عبد العزيز ، (2024) ، إدراك التهديد وآفاق الحوار المتوسطي لحلف الناتو، https://emirate.wiki/wiki/Balance_of_threat)

2- الانغماس المكثف (التوجه الى الخارج)

تعتمد إيران على الحرب غير المتماثلة عبر شن هجمات سيبرانية منخفضة التكلفة وعالية التأثير، كالهجوم على شبكة المياه الإسرائيلية (2020)، الذي استهدف زيادة الكلور في مياه الشرب، مما كشف عن محاولة استغلال الثغرات في البنى التحتية المدنية ، كما تعمل ايران على تعزيز تحالفاتها مع وكلائها في المنطقة لتنفيذ هجمات إلكترونية تُضفي طابعًا إقليميًا على الصراع، وتُعقِّد جهود العزل الدولي ضدها. (الكناني ، 2025، ص 252)

كما يُسهم هذا السباق في تعميق الانقسامات الإقليمية ، اذ تتعاون إيران مع روسيا والصين لتطوير قدراتها التكنولوجية، مستفيدةً من العقوبات الغربية لتعزيز الاكتفاء الذاتي في صناعة البرمجيات الخبيثة،هذا التحول يخلق نظامًا إقليميًا متعدد الأقطاب، اذ تصبح القوة السيبرانية أداة لإعادة رسم التحالفات.(كوهون ، 2024،ص 189)

ويرجع تبني ايران لاستراتيجية الانغماس المكثف في القوة السيبرانية إلى مجموعة من العوامل المرتبطة بالبيئة الأمنية والجيوسياسية المتغيرة في المنطقة ، اذ إن العزلة الدولية والعقوبات الاقتصادية دفعتها إلى عدّ القوة السيبرانية أداة حيوية لتعويض أوجه القصور في قدراتها العسكرية التقليدية ، وقد أدركت ايران أن امتلاك قدرات سيبرانية هجومية يتيح لها التأثير على خصومها دون الحاجة إلى مواجهة مباشرة. .(كوهون ، 2024،ص 192)

وعلى الرغم من المزايا التي يتيحها الانغماس المكثف في المجال السيبراني، إلا أن هذا التوجه يفرض تحديات معقدة عليها، ويمكن تحديد ابرز التحديات التي تواجه ايران والمحصورة بين امن القيود التكنولوجية إلى تعقيدات الصراع بالاتي : (رؤوف (2024) ، الحرب السيبرانية في الشرق : ايران واسرائيل نموذجا ، https://www.alfalq.com/?p=12120)

1. الفجوة التكنولوجية والاعتماد على الخارج ، تواجه إيران تحديات جسيمة في تطوير بنيتها التحتية السيبرانية بسبب العقوبات التي تحدُّ من وصولها إلى المكونات التكنولوجية المتطورة ، هذا الواقع يدفعها إلى الاعتماد على حلول محلية أقل كفاءة .

2. تعقيدات الإسناد وغياب الإطار القانوني ، تتميز الهجمات السيبرانية بطابع غير قانوني مما يُعقِّد عملية الرد وفقًا لقواعد القانون الدولي .

3. تصاعد سباق التسلح السيبراني ، أدَّى التقدم الإيراني في المجال السيبراني إلى تحفيز دول إقليمية أخرى، كتركيا وإسرائيل ودول الخليج، على استثمار موارد ضخمة في تطوير قدراتها السيبرانية ، هذا السباق يُشبه إلى حدٍّ ما سباق التسلح النووي في القرن العشرين، اذ تُصبح الهيمنة التكنولوجية عاملًا حاسمًا في إعادة رسم التحالفات الإقليمية .

ورغم التحديات المرتبطة بهذا المشهد، إلا أن الانغماس المكثف في المجال السيبراني يتيح فرصًا استراتيجية لايران ، اذ إن توسيع قدراتها السيبرانية يمكنها من التأثير على موازين القوى الإقليمية بوسائل غير تقليدية،

مما يتيح لها ممارسة نفوذ أكبر دون الحاجة إلى مواجهة عسكرية مباشرة . ويمكن تحديد ابرز الفرص التي تواجه ايران والمحصورة بين الابتكار وإعادة تشكيل التحالفات بالاتي (الكناني، 2025، ص258)

1. تعزيز الاكتفاء التكنولوجي ، قد يُسرع الانغماس المكثف من وتيرة الابتكار المحلي ، اذ تعمل إيران على تعزيز التعاون مع حلفاء كروسيا والصين لسد الفجوة التكنولوجية .
2. إعادة هيكلة التحالفات الإقليمية ، في ظل التنافس السيبراني، تُعزز إيران تحالفاتها مع حافائها الاقليمين، كأنصار الله في اليمن، لتنفيذ هجمات سيبرانية بالوكالة .
3. استغلال الفجوات في النظام الدولي ، يُتيح الغموض في التشريعات الدولية المتعلقة بالفضاء السيبراني فرصًا للدول لاستخدام أدوات رقمية دون مواجهة عواقب مباشرة .

ويُهدِّد الانغماس السيبراني المكثف بتعزيز ديناميكيات الصراع غير المباشر، اذ تُصبح الهجمات الإلكترونية أداةً رئيسية لزعزعة الاستقرار ، فالهجمات على البنى التحتية الحيوية، كشبكات الطاقة والموانئ، قد تؤدي إلى اضطرابات اقتصادية واجتماعية واسعة النطاق، كما حدث في الهجمات على ميناء الشهيد رجائي الإيراني عام 2020، والتي شلت حركة النقل لثلاثة أيام . (عبد اللطيف، 2023 ، ص 180 .)

ختاما يُشكِّل الانغماس المكثف في القوة السيبرانية تحديًا وجوديًا للدول الإقليمية، اذ تجد نفسها في سباق ضد الزمن لتطوير أدوات دفاعية وهجومية قادرة على مواكبة التهديدات المتطورة ، ومع استمرار غياب الإطار القانوني الدولي، يظل الشرق الأوسط ساحةً لصراع سيبراني معقد، تُعيد فيه القوة الرقمية تعريف مفاهيم السيادة والأمن في عصرٍ يُسيطر عليه الغموض الرقمي .

ثالثا : احتمالية زيادة فاعلية القوة السيبرانية

تستند احتمالية زيادة فاعلية القوة السيبرانية الإيرانية إلى مجموعة من العوامل التي تعزز هذا التوجه وتدفع بها إلى الاستثمار المستمر في تطوير تقنيات الهجوم والدفاع السيبراني ،أذ ان الدافع الرئيسي لايران وراء تعزيز فاعلية قوتها السيبرانية يتمثل في سعيها لمواجهة العقوبات الدولية المفروضة عليها والحد من التفوق العسكري والتكنولوجي الإسرائيلي ، وتعتمد ايران على استراتيجيات غير متناظرة لتعويض أوجه القصور في قدراتها العسكرية التقليدية، اذ أصبحت الهجمات السيبرانية أداة رئيسة تستخدمها لاختراق البنية التحتية الحيوية لخصومها ، ويمكن تحديد ابرز الدوافع التي تواجه ايران ، بالاتي : (كوهون ، 2023،ص 14)

1. التطور التكنولوجي والاستثمارات الضخمة ، تعتمد إيران على الدعم التقني من روسيا والصين لسد الفجوة التكنولوجية، مع التركيز على الهجمات منخفضة التكلفة التي تستهدف البنى التحتية المدنية، كشبكات المياه الإسرائيلية.

2- إعادة تشكيل التحالفات الإقليمية، تعزز إيران تحالفاتها مع حلفائها الاقليمين عبر تزويدها بأدوات قرصنة، مما يُوسع نطاق تأثيرها دون التورط المباشر.

3. الحرب غير المتماثلة وتجنب التصعيد العسكري ، تعتمد على هجمات بالوكالة عبر حلفائها كحماس لزعزعة الاستقرار في إسرائيل، مستفيدةً من صعوبة إسناد الهجمات في الفضاء الرقمي.

ورغم الفرص التي قد توفرها زيادة الفاعلية السيبرانية لإيران، إلا أن هذا السيناريو لا يخلو من تحديات معقدة قد تؤثر على مدى نجاحها في تحقيق أهدافهما الاستراتيجية ، ويمكن تحديد ابرز التحديات التي تواجه ايران بالاتي : (المنتصر، 2024 ، ص 200)

1. الفجوة التكنولوجية والقيود الاقتصادية ، تواجه إيران تحديات جسيمة في تطوير بنيتها التحتية بسبب العقوبات الدولية، مما يحد من وصولها إلى مكونات التكنولوجيا المتطورة، ويجبرها على الاعتماد على حلول محلية أقل كفاءة .

2. تعقيدات الإسناد وغياب الإطار القانوني ، تتميز الهجمات السيبرانية بطابع غير منسوب، مما يُعقِّد الردود وفقًا لقواعد القانون الدولي .

3. سباق التسلح السيبراني وتصاعد المخاطر، ادَّى التنافس بين دول المنطقة إلى تحفيز دول إقليمية أخرى كتركيا لاستثمار موارد ضخمة في تطوير قدراتها، مما يزيد من هشاشة البنى التحتية الحيوية في المنطقة.

ورغم التحديات المرتبطة بزيادة فاعلية القوة السيبرانية لإيران، إلا أن هذا السيناريو يوفر فرصًا استراتيجية قد تعزز من مكانتها على المستوى الإقليمي والدولي ، اذ إن تعزيز القدرات السيبرانية الايرانية يوفر لها فرصة لتعزيز موقعها في المواجهة مع خصومها الإقليميين والدوليين، اذ يمكنها تنفيذ عمليات هجومية تستهدف مصالح أعدائها دون الحاجة إلى الدخول في مواجهات عسكرية مباشرة ، كما أن امتلاك قدرة سيبرانية متقدمة يتيح لها ممارسة الضغط على القوى الكبرى عبر شن هجمات إلكترونية قد تستهدف منشآت حيوية في الغرب، مما قد يدفع بعض الدول إلى إعادة النظر في استراتيجياتها تجاه إيران أو حتى الدخول في مفاوضات معها حول قضايا سياسية واقتصادية. (الشرقي ، 2024، ص 105)

ويُهدِّد تصاعد الفاعلية السيبرانية بتحويل المنطقة إلى ساحة لفوضى رقمية مُمنهجة ، اذ تُستهدف البنى التحتية الحيوية بشكل متكرر، فعلى المستوى الإقليمي، فإن ازدياد فاعلية القوة السيبرانية قد يدفع دول الشرق الأوسط إلى تبني استراتيجيات أكثر تطورًا في مجال الأمن السيبراني، اذ قد تجد العديد من الدول نفسها مضطرة لتعزيز بنيتها التحتية الدفاعية لمواجهة التهديدات المتزايدة .(ريتشلد،2024، ص 98)

ختاما ، يمثل مشهد احتمالية زيادة فاعلية القوة السيبرانية لإيران في المنطقة الإقليمية تطورًا استراتيجيًا بارزًا قد يعيد تشكيل موازين القوى في الشرق الأوسط ، وعلى الرغم من أن هذا السيناريو يوفر فرصة لتعزيز النفوذ وتحقيق ألاهداف الأمنية والسياسية، إلا أنه يحمل في طياته تحديات كبيرة قد تؤدي إلى تصعيد الصراع السيبراني وتفاقم حالة عدم الاستقرار في المنطقة ، وفي ظل التقدم المستمر في مجال التقنيات السيبرانية، فإن هذا المشهد يظل مفتوحًا على عدة احتمالات تتراوح بين تعميق سباق التسلح السيبراني وبين إمكانية نشوء أنظمة جديدة للتعاون الدولي في مجال الأمن السيبراني ، وفي كلتا الحالتين، يبقى الفضاء

السيبراني أحد أبرز ساحات التنافس في الشرق الأوسط، مما يجعل من الضروري متابعة تطوراته وتأثيراته على الأمن الإقليمي والدولي بشكل مستمر.

الخاتمة

يُشكّل التفوق التكنولوجي والمرونة الاستراتيجية عاملين حاسمين في تحديد ملامح الصراع السيبراني المستقبلي ، اذ تُظهر إيران قدرة على التكيف عبر حرب غير متماثلة ، ومع استمرار غياب إطار قانوني دولي، تظل المنطقة عُرضةً لتصعيد غير متوقع، قد يُعيد تعريف مفاهيم الأمن والسيادة في عصرٍ تُهيمن عليه القوة الرقمية ، وقد يكون السبيل الوحيد لاحتواء هذا الصراع هو تعزيز الشفافية وبناء آليات ثقة، لكن تحقيق ذلك يبقى رهينًا بإرادة سياسية غائبة في المدى المنظور.

وهكذا، يُتوقع أن يستمر الصراع السيبراني بين إيران ودول المنطقة خاصة اسرائيل في التصاعد، مع زيادة التركيز على تطوير القدرات الهجومية والدفاعية في هذا المجال. وسيكون لهذا الصراع تأثيرات كبيرة على الأمن الإقليمي والدولي، مما يستدعي تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية المتزايدة.

الاستنتاجات

بناءً على ما تقدم في نتوصل الى الاستنتاجات الآتية:

1- ان الفضاء السيبراني ذات أولية مهمة لدى القوى الدولية والإقليمية.

2- ان الصراعات التي يقودها الفضاء السيبراني يشكل تهديداً مباشر لأمن الدول بشكل عام والدول الصغيرة بشكل خاص.

3- تزايد الهجمات السيبرانية بوصفها أداة للصراع الإقليمي، إذ شهدت منطقة الشرق الأوسط بعد عام 2010 تزايداً كبيراً في الهجمات السيبرانية واذ أصبحت الهجمات الرقمية أداة رئيسية في النزاعات الإقليمية.

4- تعد الاستراتيجيات السيبرانية أداة ردع وعقاب، ففي حال استهداف بنية تحتية حيوية، تقوم الدولتان بتنفيذ هجمات معقدة تهدف إلى التأثير على الاقتصاد، الأمن القومي، والقدرة الدفاعية للدولة المستهدفة.

5- أدت وتؤدي الهجمات السيبرانية إلى زعزعة استقرار الدول الإقليمية ، سواء عبر تعطيل أنظمة حيوية أم نشر المعلومات المضللة التي تؤثر على الرأي العام، مما يؤدي إلى توترات سياسية، ويزيد من حالة عدم الاستقرار الإقليمي ويؤثر على التعاون بين الدول في معالجة القضايا الأمنية المشتركة.

6- ان إيران عمدت إلى التعاون مع القوى الدولية وبالأخص روسيا والصين، في تعزيز قدراتها السيبرانية ، بينما اتجهت إسرائيل الى الولايات المتحدة الامريكية والاتحاد الأوروبي ,

7- ومع استمرار التحولات التكنولوجية والابتكارات الرقمية، ستشهد منطقة الشرق الأوسط مزيداً من الصراعات السيبرانية في المستقبل، لذلك، من المتوقع أن يتم تطوير أطر دولية لضبط هذه الحروب السيبرانية، مع تزايد الحاجة إلى التعاون بين الدول في مجالات الأمن السيبراني لمواجهة التحديات المستقبلية والتخفيف من حدة النزاعات.

References:

1. رؤوف، أسامة ، (2023) ، الاتجاهات الاستراتيجية لمواجهة التهديدات الأمنية اللاتماثلية : مدخل مفاهيمي نظري ، ط1 ، دار ألفا للوثائق، عمان.
2. المنتصر، أحمد سالم ، (2023)، تجليات جديدة في مفهوم الأمن الإلكتروني "السيبراني" (دراسة مقارنة) ، ط1، دار البيان للطباعة والنشر، عمان .
3. الماجدي، أحمد خضير ، (2024)، الحروب الإلكترونية والصراعات الدولية "الواقع، الآفاق"، ط1، دار الابداع للنشر، الإسكندرية .
4. جاك، مارتي ،(2024)، متغيرات ساحة المعركة السيبرانية، ط1، مطبعة الأمن والدفاع السعودية ، المملكة العربية السعودية .
5. ريتشلد ، مليندا،(2024)، عمليات ضبط المعلومات في الفضاء السيبراني الايراني : استراتيجية الحرب الناعمة ، ط 1 ، المركز العربي للابحاث والدراسات والسياسات ، قطر .
6. صالح، أحمد كريم،(2024) ، الحروب الهجينة: ماهيتها، ادواتها ونماذجها التطبيقية ، ط1 ،المطبعة الوطنية ،الجزائر.
7. فرج ، كرار عباس متعب ، 2022 ، " الحرب السيبرانية : دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران" ، مجلة حمورابي للدراسات، 7، (40)،195- 216 .
8. الحائري ،أحمد بن علي ، (2022) ، "الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل"، مجلة الدراسات الإيرانية، 4، (12) ، 75-99.
9. عبد الواحد ، سامر مؤيد ، (2023)، "الحرب في الفضاء الرقمي– رؤية مستقبلية" ، مجلة الدراسات القانونية والدستورية، 7 ، (38) ، 92-118.
10. السعودي ، سعيد احمد سليمان ،(2023) ، "القوة الناعمة الايرانية وتاثيرها على القرارات الاسرائيلية "، مجلة مدارات الايرانية ،3 ، (15) 138-152
11. الشرقي ، هيبت ،(2024) ، "دور القوة الناعمة في السياسة الخارجية الايرانية ومستقبلها في الشرق الأوسط" ، مجلة مدارات الايرانية، 2، (14) 14، 5-22
12. بيرم، فاطمة ، (2024) ، "السيادة الوطنية في ظل الفضاء السيبراني والتحولات الرقمية: الصين نموذجًا"، المجلة الجزائرية للأمن الإنساني، 2، 9 ، 210-233
13. عبد الواحد، فاطمة، (2024) ، "تطور توظيف جماعات العنف للإرهاب السيبراني"، مجلة السياسة الدولية، بلا ،(157) ، 99-125.
14. روتشيلد، فريدة، (2018) ، " تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى: دراسة حالة إسرائيل" ، رسالة ماجستير غير منشورة ، كلية الحقوق والعلوم السياسية، ، جامعة قاصدي مرباح ورقلة، الجزائر.
15. عداي ، فاضل جويد ، (2021) ،" قوة ايران الذكية وتأثيرها في الشرق الاوسط دراسة جيوبولتكية " ، اطروحة دكتوراه غير منشورة ، جامعة القادسية ، كلية الاداب ، العراق .
16. الكناني ، علي موسى فياض ، (2025) ،" مكانة القوة السيبرانية في استراتيجيات القوى الاقليمية (اسرائيل) وايران انموذجا" ، اطروحة دكتوراه غير منشورة ، جامعة النهرين ، كلية العلوم السياسية ، العراق .