القوة السيبرانية الإيرانية و أثرها على الاستقرار الإقليمي

Iranian cyber power and its impact on regional stability

أنيس عبد الوهاب بن أحسن

جامعة الجزائر 3 –مخبر البحوث الاستراتيجية حول السياسة الخارجية الجزائرية نحو محيطها الجيوسياسي، ، (الجزائر)

Benahsene1515@gmail.com

تاريخ الاستلام: 2022/03/06 تاريخ القبول للنشر: 2022/12/08 تاريخ النشر: 2022/12/29

ملخص:

تسعى الدراسة إلى إبراز أثر تنامي القدرات السيبرانية الإيرانية على الاستقرار الإقليمي، وذلك عبر التطرق إلى أهم الفواعل السيبرانية الإيرانية النظامية وغير النظامية، وأهم أشكال الدور الذي تؤديه هذه الفواعل في الفضاء السيبراني على المستوى الاقليمي، وقد اعتمدت الدراسة في تحليل الموضوع على المنهج الوصفي التحليلي والمنهج الاستقرائي، لتخلص إلى اعتبار أن الهدف من استخدام إيران لقوتها السيبرانية يكمن في إيجاد نوع من الردع السيبراني مع القوى الدولية والإقليمية المؤثرة في المشهد الأمني والاستراتيجي الإقليمي حفاظا على أمنها القومي أولا ومصالحها الاستراتيجية الاقليمية ثانيا .

الكلمات المفتاحية: *القوة السيبرانية الإيرانية؛الفضاء السيبراني؛ الفواعل السيبرانية؛ النشاط السيبراني، الاستقرار الإقليمي.*

Abstract:

The study aims to emphasize the impact of Iranian cyber capabilities on regional stability by examining the most important regular and irregular Iranian cyber actors, as well as the most essential types of cyberspace role that these actors play at the regional level. Experimentally, the study argues that Iran's purpose in using cyber power is to create a form of cyber deterrence with international and regional forces that influence the regional security and strategic landscape, in terms of protecting its national security first and regional strategic interests second.

key words: *Iranian cyber force, Cyber space, Cyber actors, Cyber activity, Regional stability.*

مقدّمة:

سعت إيران منذ تمكن الثورة الإسلامية من إسقاط حكم نظام الشاه محمد رضا بهلوي سنة 1979م للتأثير على المشهد الاستراتيجي لمنطقة جنوب غرب آسيا، وأمام التسارع الذي عرفته ديناميات الأمن والاستقرار الإقليميين بعد حرب الخليج الثانية سنة 1991م والغزو الأمريكي للعراق سنة 2003م والذي واكبتهما ثورة كبرى في مجال تكنولوجيا المعلومات تمخضت عنها بروز ساحة جديدة للصراع متمثلة في الفضاء السيبراني، عملت طهران على بناء قوة سيبرانية قادرة على زيادة فعالية أدائها الاستراتيجي بما يلبي متطلبات أمنها القومي.

تعد القوة السيبرانية الإيرانية حديثة النشأة، حيث لم تؤسس إيران وحدات تعنى بمجال الأمن السيبراني إلا مع نهاية العقد الأول من الألفية الجارية، وذلك نتاج لتزايد استغلال المعارضة للفضاء السيبراني، فضلا عن الهجمات السيبرانية الأمريكية على أنظمة تحكم مفاعلاتها النووية، ومنذ ذلك الحين عملت طهران على الرفع من قدراتها السيبرانية بما يخدم أهدافها الاستراتيجية، فقد عرفت الفترة الممتدة من سنة 2012م إلى غاية سنة 2021م تنامي نشاط الفواعل السيبرانية النظامية وغير النظامية في الفضاء السيبراني، ما جعل العديد من المراكز البحثية وشركات الأمن السيبراني تحذر من التهديد الذي تشكله القوة السيبرانية الإيرانية على الاستقرار الإقليمي.

- إشكالية الدراسة

إلى أي مدى يمكن اعتبار القوة السيبرانية الإيرانية مهددة للاستقرار الإقليمي ؟

- فرضيات الدراسة

- يتهدد الاستقرار الإقليمي حينما يتزايد النشاط الهجومي للفواعل السيبرانية الإيرانية غير النظامية.
- توجد هناك علاقة وثيقة بين تآكل مصالح إيران الإقليمية واستخدام قوتها السيبرانية لتهديد الاستقرار الإقليمي .

- مناهج الدراسة

من أجل المساعدة على التحليل العلمي لموضوع الدراسة تم الاستعانة بالمناهج التالية:

- منهج دراسة الحالة: يعد هذا المنهج أهم منهج استعانت به الدراسة، ذلك أنها اختارت القوة السيبرانية الإيرانية وسعت لتبيين أثرها على استقرار منطقة جنوب غرب آسيا .
- المنهج الاستقرائي: تم الاستعانة بهذا المنهج من خلال استقراء وتحليل بعض الجزئيات المرتبطة بالقوة السيبرانية للوصول إلى نتائج يمكن تعميمها .
- المنهج الوصفي التحليلي: تم الاستعانة بهذا المنهج لوصف الأنشطة السيبرانية على المستوى الاقليمي وتحليلها لتبيين أثرها على الاستقرار الإقليمي .

- أهمية الدراسة

تكمن أهمية الدراسة في معالجتها لأحد أهم فضاءات علم الاستراتيجية، والمتمثل في الفضاء السيبراني الذي يسهم في زيادة فعالية الأداء الاستراتيجي للدول التي تسعى للعب دور إقليمي أو دولي مؤثر مثل حالة الدراسة.

كما يكتسب الموضوع أهميته من تزايد نشاط الفواعل السيبرانية المحسوبة على إيران، ردا على الاستهداف المتكرر لأنظمة تحكم مفاعلاتها النووية، الأمر الذي يستدعي البحث في القوة السيبرانية الإيرانية ومدى قدرتها في التأثير على الاستقرار الإقليمي.

- أهداف الدراسة

تسعى الدراسة لبلوغ مجموعة من الأهداف، منها:

- إبراز بشكل حيادي وموضوعي مدى تأثير القوة السيبرانية على الاستقرار الإقليمي .
- فهم الاستراتيجية السيبرانية التي تنتهجها إيران على المستوى الاقليمي .
- التعرف على أهم الفواعل السيبرانية الإيرانية.

- هيكلة الدراسة

تسعى الدراسة لمعالجة الموضوع وفق الخطة التالية:

1- بنية القوة السيبرانية الإيرانية.

2- أشكال توظيف إيران لقوتها السيبرانية على المستوى الإقليمي.

1- بنية القوة السيبرانية الإيرانية

تتسم بنية القوة السيبرانية الإيرانية بالغموض الشديد، إلى درجة يصعب معها تحديد أهم الفواعل السيبرانية والجهات التي تتبع لها، لكن وبالنظر إلى نشاط هذه القوة خلال العقد الثاني من الألفية الجارية يتبين أنها تتشكل من فواعل سيبرانية نظامية وأخرى غير نظامية.

1.1- الفواعل السيبرانية الإيرانية النظامية

استجابة لبروز الفضاء السيبراني كتهديد جديد يواجه طموح الدولة الإيرانية الإقليمي، قامت إيران باستحداث مجموعة من القوى والهيئات التي تعنى بهام الدفاع السيبراني عن منشآتها الحيوية والاستراتيجية، وقوى أخرى قادرة على خوض الحروب السيبرانية، وتخضع هذه القوى لقيادة أو إشراف كبرى المؤسسات الأمنية والعسكرية، على غرار: حرس الثورة الاسلامية، جيش الجمهورية الإسلامية الإيرانية ووزارة المخابرات، وتتمثل أهم القوى والهيئات المكلفة بمهام الدفاع والهجوم السيبراني فيما يلي:

- منظمة الدفاع المدني "Passive Defence Organisation":أنشأت المنظمة سنة 2003م، غير أن ذروة نشاطها كانت منذ إصدار المرشد على خامنئي لتعليماته الرامية إلى تطويرها سنة 2014م. تلعب المنظمة دورا رئيسيا في مكافحة التهديدات السيبرانية الداخلية والخارجية (Free Word Centre, 2017, p. 9)

- شرطة الإنترنت الإيرانية "Iranian Cyber Police": أنشأت شهر أفريل من سنة 2011م، وتهدف إلى رصد ومتابعة المجرمين السيبرانيين (Free Word Centre, 2017, p. 9)

- المجلس الأعلى للفضاء السيبراني "Supreme Coouncil of Cyberspace":أنشأ المجلس في سنة 2011م بأمر من المرشد الأعلى علي خامنئي بهدف تنسيق الجهود في مجال الدفاع والهجوم السيبرانيين، ويضم في عضويته كبار المسؤولين في الأجهزة الأمنية والاستخباراتية ووزراء الثقافة والاتصالات (Lewis, 2014, p. 2).

- الجيش السايبيري الإيراني "Iranian cyber army": يقدر عدد أفراده بـ2500 فرد، وتخصص له ميزانية سنوية تقدر قيمتها بنحو 80 لامليون دولار أمريكي، هذا ويقوم هذا الجيش بمهام داخلية تهدف أساسا إلى حماية النظام السياسي القائم، وأخرى خارجية تتمثل أساس في القيام بهجمات سيبرانية ضد أهداف حيوية للدول المعادية لإيران (الرزو، 2020، صفحة 289)

- قوة الباسيج السيبرانية: أنشأت قوة الباسيج منذ مطلع العقد الثاني من الألفية الجارية وحدات خاصة تعنى بمواجهة القوى المعادية لإيران (Free Word Centre, 2017, p. 9)، وفي شهر سبتمبر من سنة 2019م أعلن قائد الباسيج غلام رضا سليماني عن تعزيز قدرات قوة الباسيج السيبرانية عبر استحداث كتائب سيبرانية تماشيا مع التحديات التي تواجه بلاده في الفضاء السيبراني (Gabi Siboni, 2020, pp. 36-37)

1-2الفواعل السيبرانية الإيرانية غير النظامية

عملت إيران على تجنيد مجموعة من الفواعل غير النظامية في صراعها مع القوى الدولية والإقليمية، وهو ما عبر عنه اللواء "غلام رضا جلالي" قائد منظمة الدفاع السلبي بقوله: "نخطط لمحاربة أعدائنا بقوة في الفضاء السيبراني عبر تجنيد قراصنة مهرة" (Arakelian, 2013, p. 56)، وفي حقيقة الأمر توجد صعوبة كبيرة في تحديد مجاميع القرصنة السيبرانيين الإيرانيين، نتاج لفوضوية البيئة السيبرانية الإيرانية وديمومة تغيرها (Cilluffo, 2018, p. 13)، ورغم ذلك يمكن تحديد أشهر مجاميع القرصنة الإيرانيين فيما يلي:

- مجموعة عز الدين القسام : تضم المجموعة عدد معتبر من القراصنة السيبرانيين الإيرانيين الذين يعتقد قيامهم بعملية "أبابيل"، التي تم على إثرها اختراق كبرى البنوك الأمريكية بين عامي 2012 و2013م ردا على العقوبات الأمريكية (Baezner, 2019, pp. 11-12).

- مجموعة Ashiyane : تعد من أهم مجموعات القرصنة في إيران، يعمل لحسابها حوالي 363.949 قرصان ، كما تتعاون المجموعة مع العديد من الجامعات لإنتاج البرامج السيبرانية، مثل الاتفاق الذي أبرمته سنة 2015 م مع جامعة شريف الصناعية لإنجاز برامج الأمن السيبراني (Free Word Centre, 2017, p. 34)

- إيران هاكIran Hack : أنشأت في سنة 2009 من طرف مجموعة من الطلاب الباحثين، تتمثل وظيفتها الأساسية في العمل على مواكبة التطورات المتسارعة في الفضاء السيبراني، فضلا عن تنسيق العمل مع مجموعات القرصنة الأخرى (Free Word Centre, 2017, p. 51)

- جيش حزب الله السيبرانيHezbollah Cyber Army : تعرف المجموعة عن نفسها بأنها يد الله للانتقام من الكفار، متوعدة القوى الامبريالية العالمية وعملائها بخوض حرب لا هوادة فيها، وذلك بعد حشد المضطهدين والعالم الإسلامي ضدها (Free Word Centre, 2017, p. 51)

- مجموعةAPT33 : تعرف أيضا باسم Elfin Espionage group, يعتقد أن المجموعة بدأت في العمل سنة 2015م، وقد استهدفت العديد من الهيئات الحكومية والشركات الاقتصادية والمراكز البحثية في الولايات المتحدة الأمريكية والسعودية ودول شرق أوسطية أخرى (Intsights defend forward, p. 5)

- مجموعةAPT34 : تعد المجموعة أكثر مجموعات القرصنة شهرة في إيران، وأكثرها نشاطا في منطقة الشرق الاوسط خاصة منذ سنة 2015م، حيث قامت باستهداف العديد من الأهداف الحيوية في الدول الإقليمية التي تعتبرها إيران دولا معادية (Intsights defend forward, p. 5)

- مجموعةAPT35 :تعرف المجموعة أيضا بتسميات مختلفة منها: "Phosphorus;" "Newscaster Team;" "Ajax Security Team;" and "Charming Kitten;"تعمل المجموعة على جمع المعلومات الاستخباراتية عبر التجسس السيبراني على عسكريين يشتغلون في الولايات المتحدة الأمريكية وفي منطقة الشرق الأوسط، فضلا عن التجسس على المنظمات الدولية ووسائل الاعلام (Intsights defend forward, p. 6)

- مجموعةAPT39 : تتميز المجموعة عن نظرائها من مجموعات القرصنة الأخرى بتركيز نشاطها في أعمال مراقبة الأنشطة السيبرانية للشخصيات البارزة في منطقة الشرق الأوسط والعالم، والتي يحتمل أن تشكل تهديدا للدولة الإيرانية .(Intsights defend forward, p. 6)

وإضافة إلى الفواعل السيبرانية الإيرانية غير النظامية قامت إيران بدعم القوة السيبرانية لأهم شركائها ووكلائها الاستراتيجيين الإقليميين، مثل:

- الجيش السوري السيبراني " The Syrian Electronic Army (SEA)":يعتبره الجنرال الأمريكي مايكل هايدن "Michael Hayden"بأنه امتداد للدولة الإيرانية، وقد أدت هذه القوة السيبرانية دورا نشطا في استهداف البنية التحتية السيبرانية للولايات المتحدة الأمريكية و((((إسرائيل)))) ودول مجلس التعاون الخليجي .(Connell, 2014, p. 11)

- مؤسسة الفضاء السيبراني لحزب الله: ظهرت في مسرح العمليات السيبرانية في شهر جوان من سنة 2011م، وتعد المؤسسة أحد أهم الوكلاء السيبرانيين لإيران في منطقة الشرق الأوسط، وتعمل هذه القوة السيبرانية على القيام بهجمات سيبرانية ضد أهداف ((((إسرائيلية)))) (الرزو، التهديد السيبراني الإيراني: الملف المضاف إلى برنامجها النووي ودوره في تأجيج صراع من نمط جديد ، 2020، الصفحات 296-297)

- جيش فضاء اليمن السيبراني " Yemen Cyber Army": ظهر في مسرح العمليات السيبرانية في شهر أفريل من سنة 2015م، تزامنا مع اشتداد المواجهات العسكرية بين التحالف العربي لإعادة الشرعية في اليمن الذي تقوده السعودية وجماعة أنصار الله الحوثية، وفي حقيقة الأمر لا توجد أدلة قاطعة تثبت تبعية هذه القوة السيبرانية لجماعة الحوثي، لكن هناك أدلة استطاع فريق The Intelligence الأمريكي جمعها، والتي تشير إلى وجود تحالف وشراكة وطيدة بين قراصنة معلومات من اليمن مع مجاميع القرصنة السيبرانيين الإيرانيين (الرزو، التهديد السيبراني الإيراني: الملف المضاف إلى برنامجها النووي ودوره في تأجيج صراع من نمط جديد ، 2020، الصفحات 304-305)

يتضح من خلال العرض السابق اعتماد إيران بشكل كبير على الفواعل السيبرانية غير النظامية، وذلك بسبب إمكانية إفلاتها من المتابعة القضائية الدولية، كما يمكنها من القيام بالهجمات السيبرانية بشكل مكثف ما يجعلها قادرة إلى حد ما على تغطية فارق التكنولوجيا الموجود بينها وبين خصومها وأعدائها الإقليميين والدوليين، غير أن الاعتماد المتزايد على الفواعل السيبرانية غير النظامية يحمل في طياته تهديدا محتملا للأمن إيران القومي مستقبلا، ذلك أن كثرة هذه الفواعل والرفع من كفاءاتها من الممكن أن تستخدم ضد الدولة الإيرانية نفسها في حال حدوث انشقاق بين كبار رجال الدولة، يأتي هذا لما يتم الأخذ بالحسبان كبر سن المرشد " علي خامنئي" وعدم وجود شخصية توافقية يمكن أن تخلفه في حالة وفاته.

2- أشكال توظيف إيران لقوتها السيبر انية على المستوى الإقليمي

انشغلت التشكيلات السيبرانية الإيرانية قبل سنة 2012م في مهام القضاء على الدعم الجماهيري للمعارضة حماية للنظام السياسي الإيراني وسلطة المرشد الأعلى، لكن بعد الهجوم السيبراني الأمريكي الذي استهدف مفاعلاتها النووية ببرنامج Stuxnet سنة 2010م وظفت إيران قدراتها السيبرانية للتصدي للهجمات السيبرانية التي تستهدف منشآتها الحيوية والاستراتيجية، فضلا عن الرد على القوى المعادية (United Against Nuclear Iran, 2020, pp. 7-8)، وفي هذا الاطار اتسم النشاط السيبراني الإيراني على المستوى الاقليمي في أشكال ثلاث، هي: استهداف المنشآت الحيوية والبنية التحتية، عمليات التجسس والمراقبة فضلا عن الدعاية السيبرانية

1.2- استهداف المنشآت الحيوية والبنية التحتية.

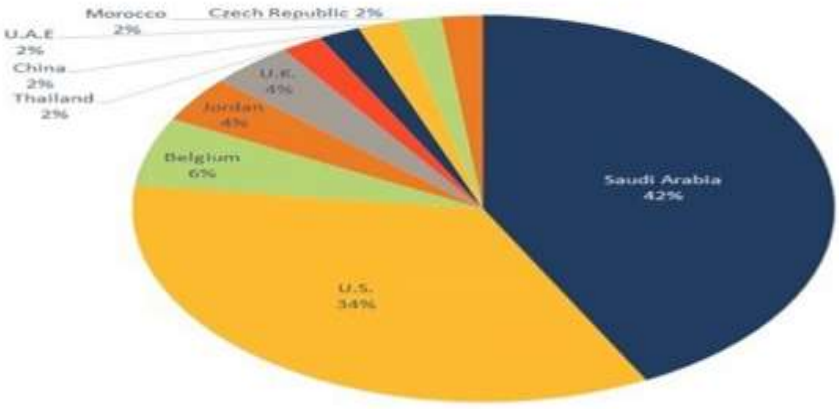
تعمل الفواعل السيبرانية الإيرانية منذ سنة 2012م على القيام بهجمات سيبرانية ضد المنشآت الحيوية والبنية التحتية الموجودة في منطقة الشرق الأوسط، وذلك بهدف إثبات قدرتها على الانتقام من السلوكيات العدائية لبعض القوى الدولية والإقليمية الفاعلة في المنطقة، وكذا للتعامل مع التهديدات والأزمات الإقليمية (Sadjadpour, 2018, p. 29).

قامت مجموعة سيبرانية تطلق على نفسها "سيف العدالة" في شهر رمضان من سنة 2012م باستهداف الحواسب المكتبية لشركة النفط السعودية آرمكو، ورغم أن هذا الهجوم لم يستهدف الحواسب المرتبطة بالتشغيل التقني للمنشآت النفطية، إلا أنها تسببت في إعطاب 30.000 حاسوب وإخراجها عن الخدمة، وقد استخدمت في هذه الهجمة برامج شمعون، واعتبرت المجموعة أن الهجوم يندرج في إطار الرد على استخدام النظام الحاكم في السعودية لموارده المالية النفطية لتمويل القيام بانتهاكات في عدد من دول منطقة جنوب غرب آسيا حسبها (United Against Nuclear Iran, 2020, p. 9)، وتشير بعض التقديرات إلى أن الخسائر السعودية الناجمة عن هذا الهجوم تقدر بين 10 و100 مليون دولار أمريكي (Baezner, 2019, p. 15)، وفي سنة 2014م أطلقت عدد من مجاميع القرصنة السيبرانيين الإيرانيين عملية كليفر "Operation Cleaver"، أين استهدفت عدد من المؤسسات النفطية والمطارات ومواقع حكومية حساسة

وكذا شركات الاتصال (الرزو، النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي، 2019م، صفحة 6) .

عرفت الفترة الممتدة من سنة 2016 إلى غاية سنة 2019م تنفيذ مجموعة القرصنة APT33 للعديد من الهجمات السيبرانية، حيث استهدفت أزيد من 50 مؤسسة وشركة تعمل أغلبها في مجالات حيوية كالطاقة، وتتوزع أغلبها في السعودية والولايات المتحدة الأمريكية ودول أخرى (أنظر الشكل رقم -1-) (قدور، 2021، صفحة 13)

الشكل رقم 1: الهجمات السيبرانية لمجموعة APT33 بين عامي 2016 و2019م



المرجع: (قدور، 2021، صفحة 13)

تمكنت مجموعة القرصنة السيبرانية APT34 سنة 2019 من برمجة برنامج يدعى Zero Cleare يعمل على حذف بيانات حواسب شركات الطاقة الشرق أوسطية، وذلك في سياق قصف الولايات المتحدة الأمريكية لوكلاء إيران في العراق (United Against Nuclear Iran, 2020, p. 11).

يتضح من خلال العرض السابق، تمكن إيران من تطوير حرب سيبرانية لا تماثلية، حيث أن جل الهجمات السيبرانية التي قامت بها نفذتها فواعلها السيبرانية غير النظامية، كما أن هذه الهجمات جاءت في سياق استراتيجي معقد، نتاج للأزمات الإقليمية المتلاحقة التي عرفتها البيئة الإقليمية الشرق أوسطية خلال العقد الثاني من الألفية الجارية، وبالتالي سعت طهران لزيادة فعالية أدائها الاستراتيجي السيبراني تعزيزا لقدراتها على ردع الخصوم والأعداء.

2.2- عمليات التجسس والمراقبة

تعود أولى كبرى عمليات التجسس السيبرانية الإيرانية إلى صيف سنة 2012م حينما كشفت شركتي security firms Kaspersky Lab and Seculert uncovered المتخصصتين في مجال الأمن السيبراني عن قيام الفواعل السيبرانية المحسوبة على إيران بحملة تجسس استهدفت 800 شخص، استهدفت الحملة في المقام الأول رجال الأعمال التنفيذيين في مجالات البنية التحتية الحيوية والخدمات المالية، وكذلك المسؤولين الحكوميين في منطقة الشرق الأوسط وموظفي السفارات، وقد كان من بين المستهدفين 387

شخص في إيران نفسها، و 54 شخص في (((إسرائيل)))، اعتمدت القوى السيبرانية الإيرانية في هذه الحملة على برامج تجسس تسمى مادي "Madi" (United Against Nuclear Iran, 2020, p. 8)، وفي شهر فيفري من سنة 2014م أطلقت إيران عملية سيبرانية أطلق عليها اسم "Thamar Reservoir"، قامت خلالها بالتجسس على مراكز الأبحاث وعدد من النشطاء في منطقة الشرق الأوسط، وقامت في الفترة الممتدة من شهر نوفمبر سنة 2016م وشهر جانفي من سنة 2017م بالتجسس على العديد من الوزارات السعودية، في حين ركزت حملة التجسس السيبراني التي قامت بها مجموعة APT-33 بين عامي 2016 و2019م على المنظمات العاملة في مجالات الفضاء والطاقة والكيمياء (قدور، 2021، صفحة 15)،

وفي سياق متصل، أوردت مجلة "جينز إنتليجنس ريفيو" في شهر جوان من سنة 2018م تحليلا عن نشاط إيران في مجال استخبارات الإشارات من خلال سعيها لتطوير منشأة لجمع بيانات الأقمار الصناعية، حيث يشير تحليل المجلة لمكان الموقع وتكوينه إلى أنه يستهدف أقمار الاتصالات في المدارات المتزامنة، بما في ذلك تلك الموجودة في دول بعض الدول الشرق أوسطية، مثل: (((إسرائيل))) والمملكة العربية السعودية، وفضلا عن ذلك تمتلك إيران أيضا إمكانية الوصول إلى الاتصالات واعتراضها من عدد من الكابلات البحرية التي تمر عبر إقليمها، على غرار الكابلات البحرية التي تعتبر كابلات اتصالات ممتدة في قاع البحر بين المحطات الأرضية لنقل إشارات الاتصالات عبر المحيطات والبحار، وتستخدم هذه الكابلات تقنية الألياف الضوئية لنقل البيانات الرقمية، ويتعزز هذا الطرح بوجود محطات أرضية للكابلات في المدن الإيرانية التالية: بندر عباس، جاسك وشابهار، ومن أشهر هذه الكابلات كابل "فالكون" الذي يتصل بعشر دول أخرى من بينها المملكة العربية السعودية (مركز الملك فيصل للبحوث والدراسات الإسلامية، 2020م، صفحة 20)، وعلى إثر جائحة كورونا ذكرت وكالة رويترز أن قراصنة سيبرانيين يعملون لصالح إيران قاموا منذ مطلع شهر مارس من سنة 2020م بتوظيف تقنيات التصيد المتقدمة لمحاولة سرقة كلمات مرور البريد الإلكتروني لموظفي منظمة الصحة العالمية للوصول - على الأرجح- إلى معلومات استخباراتية من شأنها المساعدة في مكافحة فيروس كوفيد-19 (United Against Nuclear Iran, 2020, p. 11)، ومما لا شك فيه أن تجسس إيران على موظفي منظمة الصحة العلمية ساهم في معرفة أن فيروس كورونا ما هو إلى أداة جيدة من أدوات الصراع بين القوى العالمية الكبرى، خاصة وأنها تعد من أوائل الدول الإقليمية التي أعلنت عن إنتاج لقاح مضاد للفيروس، يأتي هذا رغم الحصار الدول المفروض عليها بفعل برنامجها النووي.

ومن خلال العرض السابق يستنتج وبوضوح سعي إيران لجمع المعلومات عبر العمل على التجسس على من الشخصيات الدولية والإقليمية المؤثرة في عملية صنع القرار والسياسات، وكذلك التجسس على المنظمات الدولية الحكومية وغير الحكومية والعديد من الهيئات الرسمية وغير الرسمية في دول العالم، وتسمح عمليات التجسس الواسعة التي تقوم بها الفواعل السيبرانية الإيرانية النظامية وغير النظامية بتعزيز اليقظة الاستراتيجية الإيرانية بما يمكن صناع القرار الإيرانيين من اتخاذ القرارات وبلورة السياسات والاستراتيجيات التي تسهم في الدفاع عن المصالح الاستراتيجية للأمة الإيرانية وأمنها القومي.

3.2- الدعاية السيبرانية

يدرك صناع القرار الإيرانيين أهمية ودور الفضاء السيبراني في حشد الرأي العام المحلي والدولي إزاء مختلف المواقف والسياسات التي يمكن تتبناها الجمهورية الإسلامية الإيرانية، لذلك عملوا على بذل جهود كبيرة في سبيل إنشاء آلة دعائية سيبرانية تمجد سلوك النظام السياسي وتنتقد خصومه وأعدائه الداخليين والخارجيين (Kronenfeld, 2012, p. 80)

سعت إيران لاستغلال شبكات التواصل الاجتماعي من أجل الترويج لسياستها الإقليمية، وحشد الرأي العام الإقليمي والدولي ضد سياسات الدول الإقليمية من أمثال السعودية وإسرائيل (United Against Nuclear Iran, 2020, p. 10)، وفي هذا الصدد كشفت شركة الأمن الإلكتروني "فايراي" عن وجود عدد كبير من الحسابات على التويتر باللغة الانجليزية تنتحل صفة شخصيات أمريكية، من أجل تبني وجهات نظر مؤيدة لإيران، ونشر محتوى سلبي ومعلومات غير صحيحة عن ((((إسرائيل)))) والمملكة العربية السعودية (مركز الملك فيصل للبحوث والدراسات الإسلامية، 2020م، صفحة 34)، كما نبهت في بيان لها من التهديد الذي يمكن أن يشكله تنامي دور طهران السيبراني في شبكات التواصل الاجتماعي في تعزيز مصالحها الإقليمية، وأمام هذا الوضع قامت كل من شركتي فيسبوك وتويتر سنة 2018م بحجب المئات من الحسابات والمجموعات التي تتخذ من إيران مقرا لها، ورغم ذلك ظلت الولايات المتحدة الأمريكية متوجسة من تمكن إيران ودول أخرى من تأجيج الغضب الشعبي إزاء سياساتها حيال منطقة الشرق الأوسط، وهو ما أكده وزير الخارجة الأمريكي "مايك بومبيو" في 20 مارس سنة 2020 حينم حذر من إمكانية قيام كل الصين، روسيا وإيران بحملة تضليل ودعاية في الفضاء السيبراني بهدف إذكاء المخاوف من الولايات المتحدة الأمريكية والخلاف معها (United Against Nuclear Iran, 2020, pp. 10-11)، ويعتبر الخوف من الدعاية السيبرانية الإيرانية نتاج لقدرة طهران في التأثير على أعداد كبيرة من شيعة منطقة الشرق الأوسط والعالم، ما يمكنها من تهديد السلم الأهلي في العديد من الدول التي تستقر بها، وبالتالي يتيح لها التأثير على سياسات تلك الدول بشكل غير مباشر، على غرار ما حصل في العراق بعد اغتيال الولايات المتحدة الأمريكية لقائد فيلق القدس في الحرس الثوري الجنرال "قاسم سليماني".

ومن خلال العرض السابق، يستنتج أن الدعاية السيبرانية تساهم في فعالية الاستراتيجية الإقليمية الإيرانية، وذلك نظرا لطبيعة التكوين الطائفي لمجتمعات الشرق الأوسط، وعليه فإن هذه الدعاية من شأنها التأثير على الاستقرار الإقليمي في حال ما إذا رأت إيران أن مصالحها الإقليمية تتعرض لتهديد جدي ومستدام.

الخاتمة:

تتكون بنية القوة السيبرانية الإيرانية من فواعل سيبرانية نظامية وأخرى غير نظامية، تضم المجموعة الأولى مجموعة من القوى السيبرانية المتصلة بكبرى المؤسسات الأمنية والعسكرية، وفي مقدمتها حرس الثورة الإسلامية، في حين تضم المجموعة الثانية مجموعة من القراصنة السيبرانيين الإيرانيين

بالإضافة إلى وكلاء سيبرانيين إقليميين، وقد تجلى توظيف إيران لقوتها السيبرانية على المستوى الاقليمي في أشكال ثلاث، هي: استهداف المنشآت الحيوية والبنية التحتية، التجسس السيبراني والدعاية السيبرانية، كما توصلت الدراسة إلى النتائج التالية:

-لا يمتلك صناع القرار الاستراتيجي الإيرانيين نية في تهديد الاستقرار الإقليمي عبر استخدام القوة السيبرانية، ذلك أن إيران أحجمت عن السعي لاختراق منشآت استراتيجية مثل المفاعلات النووية، كما أنها تدرك التكاليف الباهظة لمتطلبات الأمن والحرب السيبرانية في ظل معناة اقتصادها من تبعات العقوبات الاقتصادية الدولية.

-تصبوا إيران من جراء توظيف قوتها السيبرانية على المستوى الإقليمي إلى إيجاد نوع من الردع السيبراني مع القوى الدولية والإقليمية المؤثرة في المشهد الأمني والاستراتيجي الإقليمي، حفاظا على أمنها القومي أولا ومصالحها الاستراتيجية الإقليمية ثانيا .

-تمكنت إيران بفضل دعمها لوكلائها وشركائها الاستراتيجيين الإقليميين من تفعيل الحرب بالوكالة في الفضاء السيبراني، وحتى إن لم ترقى الهجمات السيبرانية التي يشنها هؤلاء إلى مستوى خلق تهديد استراتيجي جدي، إلا أنها تعتبر عنصرا داعما للسياسات الإقليمية الإيرانية.

قائمة المراجع

أولا: باللغة العربية

الكتب

حسن مظفر الرزو. (2020). *التهديد السيبراني الإيراني: الملف المضاف إلى برنامجها النووي ودوره في تأجيج صراع من نمط جديد* . برلين: المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية.

الدراسات

ضياء قدور. (01 فيفري, 2021). القدرات السيبرانية الإيرانية (الحرب الأخرى بين إيران وخصومها). فيينا-النمسا: مركز أبحاث ودراسات مينا.

مركز الملك فيصل للبحوث والدراسات الإسلامية. (2020م). *قدرات القرصنة السيبرانية الإيرانية*. الرياض: مركز الملك فيصل للبحوث والدراسات الإسلامية.

التقارير

حسن مظفر الرزو. (2019م). *النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي*. الدوحة: مركز الجزيرة للدراسات.

ثانيا: باللغة الإنجليزية

Articles published in scientific journals

Arakelian, J. P. (2013, Winter/ Spring). What does Iran's cyber capability mean for future conflict? *The wbitebead journal of diplomacy and international relations*, pp. 49-65.

Gabi Siboni, L. A. (2020, March). Iran activity in cyberspace : Identifying patterns and understanding the strategy. *Cyber, Intelligence, and Security*, pp. 21-40

Kronenfeld, G. S. (2012, December). Iran and cuberspace warfare. *Military and strategic affairs*, pp. 77-99.

Reports

Sadjadpour, C. A. (2018). *Iran's cyber threat.* Washington: Carneggie endowment for international peace.

United Against Nuclear Iran. (2020). *The Iranian cyber threat* . London: United Against Nuclear Iran.

Free Word Centre. (2017). *Tigtening the net, Part2 : The soft war and cyber tactics in Iran.* London: Free Word Centre.

Intsights defend forward. (s.d.). *Threat brief: Iranian cyber warfare.* Dallas, New York: Intsights defend forward.

Cilluffo, A. F. (2018). *Evolving menace Iran's use cyber-enabled economic warfare.* washington: FDD press.

Connell, M. (2014). *Deterring Iran's use of offensive cyber : Acase study.* Washington: CNA Corporation.

Analytics

Baezner, M. (2019, May). Hotspot analysis : Iranian cyber-activities in the context of regional rivalries and international tensions. Zurich: Center for security studies (CSS).

Lewis, J. A. (2014, Januray). Analysis about Cybersecurity and Stability in the Gulf. Washington: Center for strategic and international studies.