https://doi.org/10.61353/ma.0260365

التهديدات السيبرانية وأثرها في الاستراتيجية الأمنية الإيرانية

Cyber threats and their impact on Iran's security strategy

الباحث: كرار حيدر علي
معهد العلمين للدراسات العليا
karaar.iraq.h94@gmail.com

ا.د. علي هادي حميدي
معهد العلمين للدراسات العليا
ali.hadi.alshukrawy@gmail.com

تاريخ استلام البحث 2025/6/16 تاريخ ارجاع البحث 2025/7/13 تار يخ قبول البحث 2025/7/28

أثرت التطورات التكنولوجية في طبيعة التهديدات الأمنية، وظهور أشكال جديده منها، والمتمثلة بالتهديدات السيبرانية، ما نجم عنها مخاطر كبيرة على الأمن القومي لجميع الدول، ودفع إلى تعزيز عمليات بناء القدرات في جميع مجالات الأمن القومي عامة، والأمن السيبراني خاصة، ومن بين أهم تلك الإجراءات التي تتخذها الدولة هي وضع استراتيجيات أمنية في مجال الفضاء السيبراني وتطويرها.

لقد أدت التهديدات السيبرانية المتزايدة التي تعرضت لها إيران بعد العام 2010 إلى تطوير استراتيجية أمنية شاملة تدمج البعد السيبراني بوصفه عنصراً أساسياً في منظومة الأمن القومي الإيراني، إذ ساهمت الهجمات السيبرانية التي استهدفت البرنامج النووي الإيراني ومؤسسات أمنية وساندة، وقيادات سياسية وأمنية وعلمية، في تسريع وتيرة تطوير القدرات السيبرانية الإيرانية الدفاعية والهجومية، إذ تعتمد إيران استراتيجية متكاملة في مواجهة التهديدات السيبرانية تجمع بين الإجراءات الوقائية والردعية ضد المصادر الرئيسة للتهديدات السيبرانية الموجهة ضد إيران من قبل الولايات المتحدة الأمريكية والكيان الصهيوني. وكلما تزايدت التهديدات السيبرانية الصادرة عن الكيان الصهيوني والولايات المتحدة الأمريكية، كلما قامت إيران بتطوير استراتيجيتها الأمنية السيبرانية.

الكلمات المفتاحية: التهديدات السيبرانية، الهجمات السيبرانية، القدرات السيبرانية، الاستراتيجيات الأمنية.

Technological developments have influenced the nature of security threats, giving rise to new forms—most notably cyber threats—which pose significant risks to the national security of all states. This has prompted the strengthening of capacity-building processes across all domains of national security in general, and cybersecurity in particular. Among the most vital measures undertaken by states in this context is the formulation and development of national cybersecurity strategies.

The escalating cyber threats facing Iran post-2010 have led to the development of a comprehensive security strategy that integrates the cyber dimension as a core pillar of the Iranian national security apparatus. Cyberattacks targeting the Iranian nuclear program, security and auxiliary institutions, as well as political, military, and scientific leadership, have accelerated the development of Iran's defensive and offensive cyber capabilities. Iran adopts an integrated strategy to counter cyber threats, combining preventive and deterrent measures against the primary sources of threats directed at it, namely the United States and the Zionist entity. Furthermore, as cyber threats emanating from the United States and the Zionist entity increase, Iran continuously refines and develops its cybersecurity strategy.

Keywords: Cyber Threats, Cyberattacks, Cyber Capabilities, Security Strategies.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

المقدمة

يُعد الأمن السيبراني من أبرز المهام التي تسعى الدول إلى تحقيقها عملياً وإجرائياً في الوقت الراهن، ولاسيَّما في ظل التطور التكنولوجي السريع وتأثيره الكبير على جوانب الأمن القومي، وقد أدى ذلك إلى ضرورة وضع استراتيجيات وقائية ودفاعية وهجومية لمواجهة الهجمات السيبرانية، بالإضافة إلى الاستمرار بعمليات تعزيز القدرات السيبرانية وتطويرها.

أولاً: موضوع البحث

تبنت جمهورية إيران الإسلامية استراتيجية وطنية معاصرة لمواجهة التحديات الآنية والمستقبلية، والتهديدات السيبرانية خاصةً. وبفضل القدرات المتنوعة التي تتمتع بها، يُعد العامل الأساسي في هذه الاستراتيجية هو استخدام أدوات أو وسائل الأمن السيبراني في عمليات ردع الخصوم من جهة، ودرء التهديدات السيبرانية الخارجية والداخلية من جهة أخرى، فضلا عن كونها أداةً للتجسس على قدرات الدول المعادية، لا سيَّما الولايات المتحدة الأمريكية، والكيان الإسرائيلي الذي نفذ أقوى هجمات سيبرانية على المنشآت النووية الإيرانية في عام 2010، وعام 2025.

إنَّ ردع مصادر التهديد الداخلية والخارجية للنظام السياسي الإيراني، وإجراءات التحدي في سياق الهيمنة الإقليمية، دفع إيران إلى مراعاة وضع الاستراتيجيات التي تتضمن الإجراءات الوقائية والدفاعية والهجومية ضمن إطار استراتيجيتها الشاملة للأمن السيبراني. ويهدف ذلك إلى منع تعطيل البنية التحتية الحيوية الإيرانية، وإثارة الفوضى، وزعزعة الثقة بين عناصر النظام السياسي، وتعزيز عمليات دعم أو قيادة العمليات النفسية التي تردع الأنشطة العدائية أو تحقق أهدافا استراتيجية أو تكتيكية، من خلال تطوير القدرات السيبرانية التي تُعتبر ركيزة أساسية للردع والدفاع والهجوم.

إنَّ تطور الاستراتيجية الأمنية السيبرانية الإيرانية لا يمكن فهمها بمعزل عن طبيعة وحجم التهديدات التي تواجهها البلاد في هذا الفضاء، إن البيئة السيبرانية العالمية بطبيعتها تتسم بالتشابك والتعقيد وغياب الحدود الواضحة، مما يجعل الدول عرضة لمجموعة واسعة من التهديدات التي قد تأتي من فاعلين متنوعين، سواء كانوا دولاً معادية، أو مجموعات إجرامية، أو قراصنة يعملون بدوافع سياسية أو أيديولوجية. بالنسبة لإيران، تتضاعف هذه التهديدات بفعل موقعها الجيوسياسي، وسياساتها الإقليمية، وبرنامجها النووي المثير للجدل، وعلاقاتها المتوترة مع عدد من القوى الكبرى والإقليمية.

يتناول هذا البحث تحليل أبرز التهديدات التي تواجه إيران في الفضاء السيبراني، وكيف أثرت هذه التهديدات في تشكيل استراتيجيتها الأمنية السيبرانية، مع التركيز على الحاجة الملحة للدفاع عن النفس ومنع الاختراقات، والسعي لبناء قدرات ردع فعّالة وتنفيذ إجراءات استباقية لمواجهة المخاطر المحتملة.

ثانياً: أهمية البحث

1-إنَّ دراسة التهديدات السيبرانية الموجهة ضد إيران، لا تنحصر آثارها السلبية عليها فقط، بل تمتد إلى الدول المجاورة لها، ولاسيَّما العراق ودول مجلس التعاون الخليجي، واليمن، ودول شرق المتوسط.

2-بيان أهمية بناء قدرات الردع السيبراني والإجراءات الاستباقية ضد التهديدات المحتملة.

3-بيان تزايد تأثير التهديدات والهجمات السيبرانية في تطوير الاستراتيجية الأمنية الإيرانية.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

4-جذب انتباه صناع القرار في العراق لتفادي الآثار السلبية الناجمة عن تنفيذ التهديدات السيبرانية ضد إيران، وما يتبعها من عمليات الرد عليها والسجالات المستمرة.

ثالثاً: إشكالية البحث

ينطلق البحث من إشكالية مفادها أنه: شكلت التهديدات السيبرانية، ولا تزال، دافعاً رئيسياً وراء سعي إيران لتطوير قدراتها الدفاعية والهجومية في الفضاء السيبراني. فالهجمات المتكررة التي استهدفت بنيتها التحتية الحيوية، ومحاولات التجسس وسرقة المعلومات، وحملات التضليل الإعلامي، كلها عوامل دفعت طهران إلى إيلاء أهمية قصوى للأمن السيبراني بوصفه جزءاً لا يتجزأ من أمنها القومي.

ومن هنا فإنه كلما زادت التهديدات السيبرانية كمّاً ونوعاً، كان لها تأثير تطويري واضح في الاستراتيجية الأمنية السيبرانية الإيرانية.

وعليه، ينطلق السؤال المركزي الآتي: هل أثرت التهديدات السيبرانية في تطوير الاستراتيجية الأمنية الإيرانية؟ كما تبرز الأسئلة الفرعية الآتية:

1-هل تطوير الاستراتيجية الأمنية السيبرانية الإيرانية يستلزم الحاجة إلى الدفاع عن النفس ومنع اختراق أنظمتها الإلكترونية؟

2-هل تطوير الاستراتيجية الأمنية السيبرانية الإيرانية يستلزم الحاجة إلى بناء قدرات ردع سيبراني وتنفيذ إجراءات استباقية ضد التهديدات المحتملة؟

رابعاً: فرضية البحث

يفترض الباحث أنه كلما تصاعدت التهديدات السيبرانية الموجهة ضد جمهورية إيران الإسلامية، فإنها تواجه بمزيد من إجراءات التحديث المستمر للتشريعات لعل في مقدمتها الاستراتيجية الأمنية السيبرانية الإيرانية، وتعزيز عمليات بناء القدرات البشرية والتقنية والتنظيمية، وتعزيز مجالات التعاون الدولي.

خامساً: منهجية البحث

تم اعتماد منهج البحث العلمي الاستقرائي كونه من المناهج التي تلائم البحث في هذا الموضوع الهام، وهو يشتمل على مستويات الملاحظة والوصف، والفرضية والتحليل، والتقييم والاستنتاج. وهذا المنهج يستخدم بصفة عامة في العلوم الاجتماعية والعلوم السياسية بصفة خاصة.

سادساً: هيكلية البحث

اشتمل البحث على ملخص ومقدمة وخاتمة وتم تقسيم هذا البحث على مبحثين، تناول المبحث الأول؛ بعنوان (الحاجة إلى الدفاع عن النفس ومنع اختراق أنظمتها الإلكترونية)، وقسم إلى مطلبين، المطلب الأول بعنوان (الحاجة إلى الدفاع عن النفس)، أما المطلب الثاني بعنوان (منع اختراق الأنظمة الإلكترونية) أما المبحث الثاني؛ بعنوان (الحاجة إلى بناء قدرات ردع سيبراني وتنفيذ إجراءات استباقية ضد التهديدات المحتملة). وقسم على مطلبين تناول الأول (الحاجة إلى بناء قدرات ردع سيبراني) أما المطلب الثاني تناول (تنفيذ إجراءات استباقية ضد التهديدات المحتملة).

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

المبحث الأول

الحاجة إلى الدفاع عن النفس ومنع اختراق أنظمتها الإلكترونية

يتناول هذا المبحث أهمية الجهود الإيرانية للدفاع عن النفس في الفضاء السيبراني من واقع التهديدات المستمرة التي تواجهها من قبل خصومها، وتسعى إيران من خلال تطوير قدراتها الدفاعية إلى حماية بنيتها التحتية المعلوماتية من الاختراق والتجسس، وضمان استمرارية عمل المؤسسات الحيوية في حالة التعرض لهجمات سيبرانية.

المطلب الأول - الحاجة إلى الدفاع عن النفس:

تعدّ إيران من أكثر الدول استهدافاً بالهجمات السيبرانية على مستوى العالم، خاصة من قبل وكالات الاستخبارات الأمريكية وحلفائها وتتنوع هذه الهجمات بين هجمات تستهدف البنية التحتية الحيوية مثل منشآت الطاقة والاتصالات، وهجمات تستهدف المنشآت النووية والعسكرية، وهجمات تستهدف المؤسسات الحكومية والمالية، إذ تنبع الحاجة الإيرانية للدفاع عن النفس في الفضاء السيبراني من إدراكها للتهديدات الوجودية التي يمكن أن تشكلها الهجمات السيبرانية المنظمة والمتطورة، فقد أثبت هجوم "STUXNET" أن الهجمات السيبرانية قادرة على إحداث أضرار مادية حقيقية في البنى التحتية الأكثر حساسية، وأنها يمكن أن تستخدم سلاحاً فعّالاً لتحقيق أهداف سياسية واستراتيجية دون الحاجة إلى مواجهة عسكرية تقليدية (مركز الملك فيصل للبحوث والدراسات الإسلامية، 2020، الصفحات 5-6).

هذا الإدراك دفع إيران إلى تبني موقف دفاعي في المقام الأول في استراتيجيتها السيبرانية المعلنة، مؤكدة على حقها في حماية بنيتها التحتية وشبكاتها من أيّ عدوان خارجي. وتتجلى الحاجة إلى الدفاع عن النفس في الاستثمارات الكبيرة التي وجهتها إيران نحو تعزيز أمن شبكاتها، وتطوير قدراتها على كشف الهجمات والتصدي لها، وتدريب الملاكات البشرية المتخصصة في الدفاع السيبراني. كما يندرج مشروع شبكة المعلومات الوطنية (SHOMA) ضمن هذا السياق الدفاعي، إذ يُنظر إليه كوسيلة لتقليل الاعتماد على الشبكة العالمية وزيادة القدرة على الصمود في وجه الهجمات الخارجية (كوهون، 2022، الصفحات 3-5).

وفي اطار الدفاع عن النفس، حددّت الجمهورية الإسلامية ثمانية مجالات ذات أولوية قصوى للحماية من الهجوم الإلكتروني للعدو بوصفها خط الدفاع الأول عن مصالحها الوطنية العليا (Assoudeh, 2020, p. 181):

1. **ولاية الفقيه:** تعتقد النخب الدينية والعسكرية في الجمهورية الإسلامية أن مؤسسة ولاية الفقيه، وهي المصدر المرجعي للمرشد الأعلى، هي الركيزة الأيديولوجية الرئيسة للدولة التي تمنع النظام من الانهيار. لذلك، فإن أحد الأهداف الرئيسة للحرب الناعمة الأمريكية هو نزع الشرعية عن ولاية الفقيه كلها، والمرشد الأعلى على وجه الخصوص، وتشويه سمعتها.
2. **المجتمع الإيراني الإسلامي:** تؤكد الجمهورية الإسلامية بان العلمانية هي أكبر تهديد لثقافتها؛ إذ تجرد المجتمع الإيراني من القيم الإسلامية الحقيقية وتستبدله بإسلام أمريكي.
3. **الإعلام:** ساحة المعركة الرئيسة للحرب الناعمة هي الإعلام والاتصالات، ولا يمكن لدولة ذات منافذ وهياكل إعلامية ضعيفة أن تنجو في هذه الحرب.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

4. الطلاب: يجب على الشباب بشكل عام والطلاب بشكل خاص أن يظلوا متفائلين فيما يتعلق بالثورة وإنجازاتها.

5. الجامعات: تسلل الأعداء إلى أفكار ومعلومات الحرم الجامعي.

6.حقوق الإنسان: تسلل الأعداء باسم قضايا حقوق الإنسان.

7. الأقليات العرقية والدينية: تسلل الأعداء باسم حقوق الأقليات العرقية والدينية.

8. التوعية العامة: توفير التثقيف العام حول كيفية تحديد الأعداء.

ووظّفت إيران تقدمها في مجال الأمن السيبراني لوضع استراتيجية تهدف إلى كشف وصد الهجمات السيبرانية. وقد تم إعداد هذه الاستراتيجية وتطوير هيكليتها على وفق رؤية وأهداف وضعتها النخبة الحاكمة، وقد أصبحت عقيدة الأمن السيبراني جزءاً أساسياً من استراتيجية الأمن القومي الإيراني بشكل عام، إذ تستند هذه العقيدة إلى ركيزتين رئيسيتين (صيوح وآخرون، 2022، صفحة 377) :

الركيزة الأولى: تركز على حماية الأمن القومي الإيراني من خلال إنشاء بنية تحتية علمية وتكنولوجية تعتمد على استراتيجية وقائية في الدفاع واستراتيجية استباقية في الهجوم في المجال السيبراني.

الركيزة الثانية: تهدف إلى تطوير مجموعة من المفاهيم والتقاليد القتالية السيبرانية عبر شبكة معقدة من الجيوش السيبرانية القادرة على تنفيذ هجمات سيبرانية متعددة على أهداف محددة في الوقت نفسه.

ومع ذلك، فإن مفهوم الدفاع عن النفس في الفضاء السيبراني لا يقتصر على الإجراءات الدفاعية السلبية فقط، ففي ظل صعوبة تحديد مصدر الهجمات بشكل قاطع وسرعة تطور التهديدات، قد يتضمن الدفاع عن النفس أيضاً القدرة على الردع النشط والقيام بعمليات استباقية لتحييد التهديدات قبل وقوعها.

إنَّ التحدي الذي تواجهه إيران، والعديد من الدول الأخرى، هو كيفية الموازنة بين الحاجة المشروعة للدفاع عن النفس وبين خطر التصعيد غير المقصود في الفضاء السيبراني.

المطلب الثاني- منع اختراق الأنظمة الإلكترونية الإيرانية:

يمثل منع اختراق الأنظمة الإلكترونية هدفاً محورياً ضمن استراتيجية الدفاع السيبراني الإيرانية. فالأنظمة الإلكترونية الحكومية والعسكرية والاقتصادية تحتوي على معلومات حساسة وبيانات حيوية، وأي اختراق لها يمكن أن يؤدي إلى تسريب هذه المعلومات، أو تعطيل الخدمات الأساسية، أو حتى التلاعب بالبيانات لإحداث أضرار. لقد واجهت إيران محاولات اختراق متعددة استهدفت وزاراتها ومؤسساتها الحيوية، مما يؤكد أهمية تعزيز أمن هذه الأنظمة، وتتبنى في هذا السياق مجموعة متنوعة من التدابير التقنية والتنظيمية، تهدف إلى تعزيز أمن هذه الأنظمة وحمايتها من التهديدات الخارجية والداخلية.

تتخذ إيران مجموعة من الإجراءات لمنع الاختراقات، تشمل ما يأتي (الجزيرة نت، د.ت.):

1- تعزيز الأمن التقني: يمكن تعزيز الأمن التقني عن طريق استخدام جدران الحماية المتقدمة، وأنظمة كشف ومنع التسلل (IDPS)، وتقنيات التشفير القوية لحماية البيانات والاتصالات، وتطبيق سياسات أمنية صارمة على مستوى الشبكات والتطبيقات. إذ عملت إيران على تطوير أنظمة متقدمة للكشف عن التطفل والاختراق، تعتمد على تقنيات الذكاء الاصطناعي والتعلم الآلي، وتتميز هذه الأنظمة بقدرتها على تحليل أنماط حركة البيانات، وتحديد السلوكيات المشبوهة، والكشف عن محاولات الاختراق في مراحلها المبكرة .

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

2-إدارة الثغرات والتحديثات: إجراء مسح دوري للثغرات الأمنية في الأنظمة والشبكات، وتطبيق التحديثات الأمنية اللازمة بشكل فوري لسد هذه الثغرات قبل استغلالها من قبل المهاجمين. كما تتبنى إيران استراتيجية لتنويع أنظمة الحماية الإلكترونية، بحيث لا تعتمد على نظام واحد أو منتج واحد، مما يقلل من مخاطر الاختراق الناتجة عن ثغرات محددة في أحد الأنظمة. وتتضمن هذه الاستراتيجية أيضاً تحديث الأنظمة والبرمجيات بشكل دوري، وتطبيق أفضل الممارسات العالمية في مجال الأمن السيبراني.

3- **رفع مستوى الوعي الأمني:** تدريب الموظفين والمستخدمين على التعرف على التهديدات السيبرانية الشائعة، مثل رسائل التصيد الاحتيالي والبرمجيات الخبيثة، وتوعيتهم بأهمية اتباع الممارسات الأمنية السليمة. إذ تتضمن الاستراتيجية الإيرانية لمنع اختراق الأنظمة الإلكترونية أيضاً تدابير تنظيمية وإجرائية، مثل تطوير سياسات وبروتوكولات موحدة للأمن السيبراني، وتدريب العاملين في المؤسسات الحيوية على أفضل الممارسات الأمنية، وإجراء اختبارات دورية لتقييم مستوى الأمن السيبراني في هذه المؤسسات.

4- مر اقبة الشبكات وتحليل السلوك: استخدام أدوات متقدمة لمراقبة حركة المرور على الشبكات وتحليل سلوك المستخدمين والأنظمة للكشف عن أيّ أنشطة مشبوهة أو مؤشرات على حدوث اختراق. كما تعمل إيران على تطوير نظام وطني للتنبيه المبكر بالهجمات السيبرانية، يعتمد على شبكة من أجهزة الاستشعار الموزعة في مختلف أنحاء البنية التحتية المعلوماتية. ويهدف هذا النظام إلى الكشف عن الهجمات السيبرانية في مراحلها المبكرة، وتمكين فرق الاستجابة من التعامل معها قبل أن تتسبب في أضرار واسعة النطاق.

5- **تقسيم الشبكات والعزل:** تطبيق مبدأ تقسيم الشبكات (Network Segmentation) وعزل الأنظمة الحساسة (Air-gapping) لتقليل الأضرار المحتملة في حال نجاح المهاجم في اختراق جزء من الشبكة. وتولي إيران اهتماماً خاصاً بحماية أنظمة التحكم الصناعي في المنشآت الحيوية، التي تعتبر من أكثر الأهداف جاذبية للهجمات السيبرانية. وتتبنى في هذا السياق استراتيجية للعزل المادي والمنطقي لهذه الأنظمة عن شبكة الإنترنت العالمية، وتطوير بروتوكولات أمنية خاصة بها، وإنشاء فرق متخصصة لمراقبتها وحمايتها.

وتولي الاستراتيجية الأمنية السيبرانية الإيرانية اهتماماً متزايداً بالتهديدات المرتبطة بالاستشعار عن بعد والتنصت على الاتصالات، وتتبنى في هذا السياق تدابير متطورة لتشفير الاتصالات وحماية البيانات المنقولة عبر الشبكات المختلفة، كما تسعى إلى تطوير أنظمة للكشف عن عمليات التنصت الإلكتروني، والتصدي لها بفعالية (مركز الملك فيصل للبحوث والدراسات الإسلامية، 2020، الصفحات 5-6).

وعلى الرغم من هذه الجهود، فإن منع الاختراقات بشكل كامل يظل تحدياً صعباً في ظل التطور المستمر لتقنيات الهجوم والعدد الهائل من نقاط الضعف المحتملة في الأنظمة المعقدة، تشير بعض التقارير إلى أن إيران لا تزال تعاني نقصاً في القدرات الدفاعية المتقدمة مقارنة بخصومها، كما أن التركيز الكبير على المراقبة الداخلية قد يأتي أحياناً على حساب تعزيز الدفاعات ضد التهديدات الخارجية.

إنَّ السعي المستمر لمنع اختراق الأنظمة الإلكترونية يعكس إدراك إيران لأهمية حماية معلوماتها وبنيتها التحتية الرقمية بوصفها جزءاً أساسياً من أمنها القومي. ويتطلب هذا السعي استثماراً متواصلاً في التكنولوجيا والموارد البشرية، وتبني نهج شامل لإدارة المخاطر السيبرانية على المستويات كافة.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

المبحث الثاني

الحاجة إلى بناء قدرات ردع سيبراني

وتنفيذ إجراءات استباقية ضد التهديدات المحتملة

يتناول هذا المبحث الحاجة المتزايدة لدى إيران لبناء قدرات ردع سيبراني قادرة على ثني الخصوم عن شن هجمات ضدها، وكذلك الحاجة إلى تطوير وتنفيذ إجراءات استباقية لمواجهة التهديدات المحتملة بناءً على المعلومات الاستخباراتية أو تقييم المخاطر.

المطلب الأول - الحاجة إلى بناء قدرات ردع سيبراني:

يرتكز مفهوم الردع السيبراني في الاستراتيجية الإيرانية على فكرة أساسية مفادها أن امتلاك قدرات هجومية متطورة في الفضاء السيبراني يُعدّ الوسيلة الأساسية لثني الخصوم عن مهاجمتها. ويهدف الردع السيبراني، في جوهره، إلى منع الخصوم من شنّ هجمات سيبرانية من خلال التهديد بفرض تكاليف باهظة عليهم تفوق المكاسب المتوقعة من الهجوم. بالنسبة لإيران، يمثل بناء قدرة ردع سيبراني فعّالة هدفاً استراتيجياً هاماً لعدة أسباب (عزي، د.ت.):

1- يمكن للردع أن يساعد في موازنة التفوق العسكري والتكنولوجي التقليدي الذي يتمتع به بعض خصومها، إذ يوفر الفضاء السيبراني ساحة للمواجهة غير المتماثلة.

2- يمكن للردع أن يساهم في حماية المصالح الوطنية الحيوية، بما في ذلك البرنامج النووي والبنية التحتية الحيوية، من خلال جعل تكلفة مهاجمتها مرتفعة للغاية.

3- يمكن للقدرة على الردع أن تعزز مكانة إيران بوصفها قوةً إقليميةً فاعلةً في الفضاء السيبراني.

تسعى إيران لبناء قدرات الردع السيبراني من خلال تطوير قدراتها الهجومية المتضمنة مجموعة متنوعة من الأدوات والتقنيات، بما في ذلك برمجيات التجسس، وبرمجيات الفدية، وبرمجيات مسح البيانات، وبرمجيات تعطيل الخدمات. وتتميز هذه البرمجيات بقدرتها على استهداف أنظمة متنوعة، بما في ذلك أنظمة التحكم الصناعي، والبنية التحتية للاتصالات، والأنظمة المالية والمصرفية.

كما تطور إيران قدراتها في مجال الهندسة الاجتماعية والتلاعب بالمعلومات، بهدف تنفيذ عمليات تأثير في الفضاء السيبراني، يمكن استخدامها للرد على الهجمات التي تستهدف مصالحها. وتتضمن هذه القدرات تطوير تقنيات وأدوات لنشر المعلومات المضللة، واختراق حسابات وسائل التواصل الاجتماعي، والتأثير على الرأي العام في الدول المستهدفة، ويعتبر التوصل إلى نسخة إيرانية من فيروس "ستوكسنت" أحد الأهداف الاستراتيجية للقدرات الردعية السيبرانية الإيرانية، ويتطلب تحقيق هذا الهدف تطوير قدرات متقدمة في مجال هندسة البرمجيات الخبيثة، وفهم عميق لنقاط الضعف في أنظمة التحكم الصناعي، والقدرة على تنفيذ عمليات معقدة في الفضاء السيبراني (مركز الملك فيصل للبحوث والدراسات الإسلامية، 2020، الصفحات 40-43).

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

وتعتمد إيران في بناء قدرات الردع السيبراني على مجموعة من المؤسسات المتخصصة، أبرزها وحدات الحرب السيبرانية التابعة للحرس الثوري، والتي تضم خبراء ومتخصصين في مختلف مجالات الأمن السيبراني. كما تستفيد من التعاون مع دول أخرى، ولاسيَّما روسيا والصين، في تطوير قدراتها الهجومية في الفضاء السيبراني.

تشير العديد من التقارير إلى أن إيران تمتلك مجموعات قراصنة متطورة قادرة على شن هجمات معقدة ضد أهداف متنوعة، وأنّ امتلاك هذه القدرات الهجومية، والقدرة على إظهارها أو استخدامها بشكل محدود، يمكن أن يرسل رسالة ردع للخصوم المحتملين. يتماشى هذا مع مفهوم "الدفاع المتقدم" الذي تتبناه طهران في استراتيجيتها الأمنية الأوسع، والذي يتضمن نقل المواجهة إلى أرض الخصم أو الفضاءات التي ينطلق منها التهديد ترى القيادة الإيرانية في العمليات السيبرانية وسيلة "لتسوية الفرص، وتعطيل الأنظمة الاقتصادية والسياسية الغربية، وردع الأعمال الانتقامية العلنية" (فريحات، 2024)

يصنف رضا غلامي، رئيس مركز صدرا للأبحاث حول العلوم الإنسانية الإسلامية، في نهج بناء القدرات السيبرانية للجمهورية الإسلامية الإيرانية - حول بناء القدرات الرئيسية للأمن السيبراني تستند عليها إيران في ردع خصومها إلى ست فئات: إطلاق شبكة المعلومات الوطنية، وتشكيل شبكة إنترنت ثانية، وتشكيل تحالف عالمي لتحدي القيادة والهيمنة الأمريكية، وخلق خطاب مهيمن لنموذج حوكمة بديل، والاستثمار في صناعات التكنولوجيا الفائقة المحلية، وتعبئة عامة الناس في الفضاء الإلكتروني لحماية الثقافة والتقاليد، والتي سوف نوضحها في الآتي (الرزو، د.ت.، الصفحات 67-68):

1- شبكة المعلومات الوطنية: تتكون شبكة المعلومات الوطنية من ثلاث طبقات: البنية التحتية، والمحتوى، والخدمات. وقد أكملت وزارة الاتصالات وتكنولوجيا المعلومات الإيرانية جزءاً كبيراً من الطبقة الأولى، وهذه ستوفر طبقة البنية التحتية وحدها، وإلى حد كبير الأمن القومي إضافة إلى أمان المستخدم، من الناحية التكنولوجية والمالية والثقافية. إضافة إلى ذلك، سيستمتع المستخدمون بسرعات أعلى وبأسعار أكثر معقولية. ووفقا لغلامي، فإن شبكة المعلومات الوطنية تحمي القيم الوطنية والدينية لإيران في الفضاء الإلكتروني وتسعى إلى ازدهار التجارة الإلكترونية، في حين تساعد أيضا في تنقية محتوى الفضاء الإلكتروني.

2- **شبكات إنترنت بديلة:** للحد من قوة التحالف الأمريكي الصهيوني، تسعى إيران إلى تشجيع الدول الأخرى على تشكيل شبكة إنترنت ثانية. لدى الصين وروسيا ودول أخرى الدافع اللازم للقيام بهذا المسعى، وكذلك الجمهورية الإسلامية. من خلال السعي لتحقيق مصالحها المشتركة مع الآخرين، وبالطبع من خلال الحفاظ على شبكة الإنترنت الوطنية بوصفها أساساً للإنترنت الثاني أو شبكة المعلومات العابرة للحدود الوطنية، تلعب الجمهورية الإسلامية دوراً مهماً في خلق وتوسيع الفجوة الأيديولوجية بين الولايات المتحدة والدول الأخرى. لا يقبل خامنئي قيادة الولايات المتحدة في حوكمة الفضاء الإلكتروني، وقد أصدر تعليماته للحكومة بالدفاع عن مجموعتها الخاصة من القواعد والمعايير الإلكترونية من أجل رفاهية العالم.

3-التحالفات: تعتقد الجمهورية الإسلامية أن الفضاء الإلكتروني يحكمه حالياً شريط وظيفي (الغرب بقيادة الولايات المتحدة)، ولا تواجه سلطته سوى مساءلة محدودة. كانت هناك محاولات عديدة من قبل دول مختلفة، بما في ذلك الصين وروسيا، لإثارة قضايا الفضاء الإلكتروني مع الأمم المتحدة والمنظمات التابعة لها، لكن هذه المحاولات قوبلت بمعارضة وقوضتها الولايات المتحدة. لذلك، بدأت إيران تحركا نحو

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

إنشاء وتعزيز تحالفات تسعى إلى تقليص السلطة غير المحدودة للأمريكيين في الفضاء الإلكتروني. يجادل غلامي بأن خطوة كبيرة لتشكيل مثل هذا التحالف، يجب إنشاء منصب نائب وزير الفضاء الإلكتروني في وزارة الخارجية وتدريب ضباط مهرة وشجعان على الدبلوماسية الإلكترونية.

4- الدعم المعنوي: يجادل غلامي بأن تحقيق قدرات سيبرانية ناجحة يتطلب إنشاء سردية كبرى موحدة - سردية خطابية مهيمنة واسعة بما يكفي لتكون شاملة للجهات الفاعلة المحلية والدولية، إضافة إلى أن طبيعة الناس السياسة الواعية مع سياسات الجمهورية الإسلامية يمكن أن تسهل بناء المعايير والقدرات بشكل أكبر. حالياً، وتفتقر الجمهورية الإسلامية إلى هذه السرديات الكبرى وترى وجهات نظر متنافسة، حتى الخطابات التي تعارض سياسات النظام، تنمو في المجتمع. ومع ذلك، تحدد الوثيقة أن الخطوة الأولى لإنشاء سردية أوسع هي خلق توافق في الآراء بين النخب.

5- الدعم المادي: يحث غلامي الجمهورية الإسلامية على تسهيل الأساس المالي للشركات الناشئة في مختلف صناعات التكنولوجيا الفائقة وتكنولوجيا المعلومات المحلية لتعزيز بناء القدرات السيبرانية.

6- الثقافة المجتمعية: يزعم غلامي أن أحد العناصر المهمة لبناء القدرات السيبرانية هو تعبئة وتثقيف عامة الناس للدفاع عن القيم الوطنية والدينية من خلال إنشاء محتوى قائم على القيم ومواجهة المحتوى المناهض للنظام والمناهض للقيم: "يجب أن نكون يقظين في دعم القيم الإسلامية والثورية في الفضاء الإلكتروني وإحباط الهجمات على هذه القيم. ومع ذلك، في السنوات الأخيرة، كانت إحدى النقاط المحورية لأعدائنا هي العمليات النفسية التي تهدف إلى التأثير على الرأي العام". لا تقتصر الوثيقة على التعبئة الإلكترونية للشعب الإيراني، وتوصي النظام بتوسيع جهوده للوصول إلى الأشخاص ذوي التفكير المماثل الذين يتمثل اهتمامهم الأهم في حماية القيم الإلهية في جميع أنحاء العالم.

وتجدر الإشارة إلى أن الاستراتيجية الإيرانية لبناء قدرات للردع السيبراني تواجه تحديات متعددة، أبرزها الفجوة التكنولوجية بين إيران والقوى الغربية، والقيود المفروضة على وصول إيران إلى التكنولوجيا المتقدمة بسبب العقوبات الدولية. إذ إن صعوبة الإسناد (Attribution)، أي تحديد مصدر الهجوم بشكل قاطع وموثوق، وهو أمر ضروري لتوجيه الردع أو الانتقام. كما أن إظهار القدرات (Signaling) دون الكشف عن تفاصيل قد يستغلها الخصم، وبناء المصداقية (Credibility) بأن التهديد بالرد سيتم تنفيذه فعلاً، كلها تحديات معقدة في الفضاء السيبراني. إضافة إلى ذلك، فإن خطر سوء التقدير والتصعيد غير المنضبط يظل قائماً في ظل غياب قواعد سلوك دولية واضحة ومتفق عليها في هذا المجال (مركز المستقبل للأبحاث والدراسات المتقدمة، د.ت.).

وعلى الرغم من هذه التحديات، يبدو أن إيران ماضية في تطوير قدراتها الهجومية بوصفها جزءاً أساسياً من استراتيجيتها للردع السيبراني، ويتحقق تنامي قدراتها، وارتفاع تصنيفها ضمن القوى السيبرانية، من خلال تطوير قدراتها الذاتية، والاستفادة من التعاون مع الدول الصديقة، وتبني نهج غير تقليدي في مجال الحرب السيبرانية.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

المطلب الثاني - تنفيذ إجراءات استباقية ضد التهديدات المحتملة:

تتبنى الاستراتيجية الأمنية السيبرانية الإيرانية نهجاً استباقياً في التعامل مع التهديدات السيبرانية، لا يكتفي بالانتظار حتى وقوع الهجمات ثم الرد عليها، بل يسعى إلى استباق هذه الهجمات والتعامل معها قبل وقوعها. ويتضمن هذا النهج الاستباقي مجموعة متنوعة من الإجراءات والعمليات، تهدف في مجملها إلى تحييد مصادر التهديد المحتملة، وتعطيل قدرات الخصوم في الفضاء السيبراني.

وتعتمد الإجراءات الاستباقية الإيرانية على استخدام تقنيات متقدمة في مجال الاستطلاع والتجسس السيبراني، تمكنها من جمع معلومات استخباراتية حول التهديدات المحتملة، وتحديد نقاط الضعف في أنظمة الخصوم، ورصد التحضيرات للهجمات السيبرانية المستقبلية. كما تستخدم إيران تقنيات متطورة لتحليل البيانات الضخمة واستخلاص المؤشرات والتنبيهات التي تشير إلى وجود تهديدات محتملة.

يمكن أن تتخذ الإجراءات الاستباقية أشكالاً متنوعة على المستوى الداخلي وعلى المستوى الخارجي، أهمها:

1- الإجراءات الداخلية:

أ- **الرقابة على الإنترنت:** تُعد إيران واحدة من الدول التي لديها أعلى معدل رقابة في العالم. في مؤشر حرية الإنترنت العالمي السنوي لعام 2021، الذي أعدته منظمة فريدوم هاوس غير الحكومية ومقرها الولايات المتحدة، حصلت إيران على وضع "غير حرة"، حيث حصلت على 16 نقطة فقط من أصل 100 نقطة، على الرغم من أن دستور جمهورية إيران الإسلامية وقانون الصحافة يضمنان حرية التعبير والإعلام، إلا أنّه يُحظر في إيران نشر مقالات والصور والمواد التي تنتهك قيم الإسلام وتضر بأسس الجمهورية الإسلامية. وان القيود المفروضة تشكل ذريعة، أو ما يشبه التبرير، لفرض رقابة على الصحافة والإنترنت وكذلك لمقاضاة ومعاقبة نشطاء الإنترنت. تنشط الحكومة الإيرانية في المجال الرقمي، بحجة حماية مصالح الدولة وفضيلة مواطنيها (Stachon, 2024, p. 275).

في السنوات الأخيرة، انخرطت إيران بشكل خاص في استخدام المعلومات والمراقبة عبر الإنترنت ضد المعارضين للسيطرة على الخطابات الاجتماعية والسياسية وتشويه سمعتهم في نظر الرأي العام العالمي. وكان ضحايا الهجمات في المجال الرقمي بشكل رئيسي أعضاء رئيسيين في الشتات الإيراني، بمن فيهم الصحفيون والنشطاء الاجتماعيون والفنانون، من بين آخرين (كوهون، 2022، صفحة 4).

ب- **عمليات إغلاق واسعة النطاق للإنترنت:** تُعد عمليات إغلاق الإنترنت الجماعية طريقة جديدة نسبيا للحكومة الإيرانية للتعامل مع تفشي السخط العام والرد على الأنشطة السيبرانية المناهضة للحكومة من قبل الإيرانيين عبر الإنترنت، وهناك عدة أنواع من عمليات إغلاق الشبكة، تتراوح من عمليات إغلاق واسعة النطاق، على المستوى الوطني إلى المحلي، إلى تعطيل مجالات مختارة فقط، مثل منصات الاتصال أو وسائل التواصل الاجتماعي، تُظهر الأبحاث أنه بين عامي 2010 و2022، كانت هناك ثماني حالات من انقطاع سعة الشبكة في إيران، اثنتان منها كانتا الأكثر أهمية. كانت الأولى خلال ما يسمى بالربيع العربي (نوفمبر 2011 إلى أغسطس 2012)، عندما انخفض النطاق الترددي بنسبة 77%، والثانية كانت خلال الاحتجاجات التي أعقبت وفاة مهسا أميني (أكتوبر - نوفمبر 2022)، مع انخفاض بنسبة 69% في النطاق الترددي (Stachon, 2024, p. 276).

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

ج- **التطبيقات الوطنية:** إنَّ البرامج المحلية والوطنية التي أُجبر الإيرانيون على استخدامها خوفاً من التهديدات السيبرانية من اختراق المجتمع، لسنوات عدّة، لم يتمكن المواطنون الإيرانيون من الوصول إلى تطبيقات مثل فيسبوك وتويتر ويوتيوب وإنستغرام وواتساب نتيجة للحظر الوطني للوصول إلى التطبيقات والبرامج الدولية، كما تم حظر تطبيق تيك توك ومتجر آبل وجيت هب والعديد من الوظائف من google ومئات المواقع الإلكترونية الأخرى، ومع ذلك، تجدر الإشارة إلى أن الحكومة أنشأت وأتاحت أيضا للاستخدام برمجياتها الوطنية الخاصة، والتي تغطي عدداً من المجالات، بما في ذلك أنظمة التشغيل (Ghasedak و Sharif Linux) وخدمة البريد الإلكتروني (Chaapaar) ومحركات البحث (Fajr وYooz وParsijoo أو Gorgor). كما تم تطوير برامج المراسلة الفورية الإيرانية (TD Messenger)، وبوابة للتجارة الإلكترونية (Digikala)، وحتى وسائل التواصل الاجتماعي الداخلية (Cloob أو Camera) (ديكي، 2023، صفحة 78).

ومن أهم الأنظمة المستخدمة محلياً لتنفيذ إجراءات استباقية ضد التهديدات المحتملة نظام SIEM، وهو نظام حاسوبي يُمكّن مشغلي شبكات الهاتف المحمول في إيران من مراقبة وتغيير وتعطيل استخدام العملاء للهواتف على شبكة معينة، إذ يمتلك النظام أيضا أدوات أكثر دقة وتطورا للسيطرة على الجمهور بل يحتوي أيضا على وظائف تسمح بالتلاعب عن بُعد بمجموعات البيانات الفردية، ويقدم البرنامج ما يقرب من ثلاثين وظيفة مختلفة، أهمها (Stachon, 2024, p. 238): الحد من سرعات البيانات على الهاتف و تحويل الجهاز الطرفي من شبكات الجيل الثالث والرابع إلى الجيل الثاني و تتبع موقع مستخدم الهاتف وتحركاته المستمرة. إلى جانب جمع البيانات الوصفية الأخرى، ويُسهّل هذا تحديد مواقع مجموعات كبيرة من الأشخاص وتحليل اتجاهاتهم في الوقت الفعلي القدرة على الحصول على معلومات حول جميع الهواتف الموجودة. إضافة إلى ذلك، يُتيح برنامج SIEM أيضا تحليل جميع جهات اتصال المستخدم، والحصول على الفواتير، بما في ذلك تاريخ ومكان آخر مكالمة وعدد المكالمات الخارجية، أو معلومات حول الخدمات الخاصة التي يستخدمها المستخدم، مثل VPN أو مكالمات الفيديو.

2- الإجراءات الخارجية:

1- الهجمات على البنية التحتية الحيوية:

تشمل البنية التحتية الحيوية المرافق أو المعدات أو المنشآت التي تدعم الأداء الطبيعي للمجتمع الحديث والاقتصاد. وتشمل هذه الخدمات والمرافق الأساسية مثل شبكة الكهرباء والاتصالات والنقل والأنظمة المالية وغيرها من الخدمات الأساسية ويتم تنفيذ العديد من الإجراءات الاستباقية السيبرانية من قبل قراصنة يحملون الجنسية الإيرانية أو تابعين لحكومة الجمهورية الإسلامية ومنها كيانات تابعة للحرس الثوري الإسلامي، متهمين بتنفيذ حملة منسقة من الهجمات الإلكترونية ضد القطاع المالي الأمريكي كما اتُهم أحدهم بالوصول غير المصرح به إلى أنظمة التحكم في سد في نيويورك. وعلى الرغم من أن الحكومة الإيرانية لم تعترف رسميا بتنفيذ الهجمات، إلا أنه يُعتقد على نطاق واسع أنها لعبت دورا غير رسمي على الأقل في توجيهها ضربات استباقية (بن أحسن، 2022، صفحة 738).

لا تقتصر الهجمات الإلكترونية الإيرانية على الولايات المتحدة. ففي مايو 2020، على سبيل المثال، وردت تقارير عن حادثة تهدف إلى إتلاف أجهزة الكمبيوتر التي تتحكم في تدفق المياه ومحطات معالجة مياه الصرف

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

الصحي في الكيان الإسرائيلي، مما كان من شأنه أن يعطل إمدادات المياه لموقعين على الأقل في الكيان الإسرائيلي، وأيضاً إلى واحدة من أشهر الهجمات الإلكترونية على البنية التحتية الحيوية التي تُتهم بها الجمهورية الإسلامية. في عام 2012، تعرضت شبكة حواسيب أرامكو السعودية لهجوم بفيروس ذاتي التكاثر (Stachon, 2024, pp. 280-281).

2- التجسس الإلكتروني :

يكمن نشاط إيران في المجال الرقمي في التجسس إذ إن إحدى أكبر حملات التجسس الإلكترونية التي نفذها مواطنون إيرانيون مرتبطون بحكومة الجمهورية الإسلامية من عام 2013 إلى عام 2017. اتُهم تسعة إيرانيين بتنفيذ حملة منسقة لاختراق أنظمة تكنولوجيا المعلومات والتجسس عليها التابعة لأكثر من 300 جامعة في 22 دولة، و47 شركة من القطاع الخاص، ومنظمات حكومية وفيدرالية، والأمم المتحدة، واليونيسف. وكانت جميعها مرتبطة بمعهد مابنا الإيراني.وقد استخدم المتسللون بيانات اعتماد مسروقة للوصول غير المصرح به إلى حسابات الضحايا وتجسس عليهم، ثم سرقوا أكثر من 31 تيرابايت من البيانات من وثائق و مجالات علمية مختلفة. ثم تم استخراج البيانات إلى خوادم خارج الولايات المتحدة. ويُعتقد أن حملة القرصنة نُفذت نيابة عن الحرس الثوري الإسلامي أو ممثلين رفيعي المستوى من الحكومة الإيرانية وقطاع الأعمال والأوساط الأكاديمية (Stachon, 2024, p. 281).

يهدف هذا النوع من الأنشطة إلى (Anderson & Sadjadpour, 2018, pp. 14-15):

أ- جمع المعلومات الاستخباراتية عن الخصوم (سواء كانوا دولاً، مؤسسات، أو أفراداً).

ب- اختراق الأنظمة الحكومية والعسكرية للدول المعادية بهدف مراقبة التحركات والتخطيط المسبق.

ت- سرقة الملكية الفكرية والتقنية من شركات التكنولوجيا أو الجامعات ومراكز الأبحاث.

ث- تعزيز القدرات الدفاعية والهجومية من خلال فهم نظم الأعداء واستخدام البيانات لاحقاً في عمليات هجومية دقيقة.

3- عمليات النفوذ الإيراني:

أصبحت إيران خبيرة في تنفيذ إجراءات استباقية غير تقليدية ضد التهديدات المحتملة لتحقيق أهداف إقليمية. فهي تشن حرباً هجينة باستخدام مزيج من الوسائل العسكرية وشبه العسكرية، بما في ذلك الأدوات الرقمية. وتجدر الإشارة إلى أن أحد الأنشطة الرئيسة للجمهورية الإسلامية هو العمليات المعلوماتية التي تهدف إلى تشكيل الجهات الفاعلة الحكومية والضغط عليها، وتُعد عمليات التأثير أحد عناصر القوة الناعمة الإيرانية، وبالتالي، غالبا ما تشمل الهجمات الإلكترونية الإيرانية خصوما رئيسيين من الدول. وكما هو الحال في التجسس الإلكتروني وتعطيل البنية التحتية الحيوية (Baezner, 2019, p. 17).

كانت إحدى أكثر القضايا شهرة في السنوات الأخيرة حملة تضليل إعلامي تهدف إلى التأثير على الانتخابات الرئاسية الأمريكية لعام 2020. ونشروا مواد تضليل إعلامي حول ثغرات أمنية مزعومة، أو حاولوا الوصول غير المصرح به إلى مواقع التصويت (Baezner, 2019, p. 18).

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

4- الدعاية السيبرانية:

يدرك صُنّاع القرار الإيرانيون أهمية ودور الفضاء السيبراني في حشد الرأي العام المحلي والدولي إزاء مختلف المواقف والسياسات التي يمكن أن 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، إذ سعت إيران لاستغلال شبكات التواصل الاجتماعي من أجل الترويج لسياستها الإقليمية، وحشد الرأي العام الإقليمي والدولي ضد سياسات الدول الإقليمية من أمثال السعودية و الكيان الإسرائيلي (بن أحسن، 2022، صفحة 741).

وفي هذا الصدد كشفت شركة الأمن الإلكتروني "فايراي" عن وجود عدد كبير من الحسابات على التويتر باللغة الإنجليزية تنتحل صفة شخصيات أمريكية، من أجل تبني وجهات نظر مؤيدة لإيران، ونشر محتوى سلبي ومعلومات غير صحيحة عن الكيان الإسرائيلي والمملكة العربية السعودية، وإن الدعاية السيبرانية تُسهم في فعالية الاستراتيجية الإقليمية الإيرانية، وذلك نظراً 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 (مؤسسة اليوم الثامن للإعلام والدراسات، د.ت.).

ومن أبرز الإجراءات الاستباقية التي تتبناها إيران في مجال الأمن السيبراني: إنشاء شبكات وهمية (Honeypots) لجذب المهاجمين المحتملين وكشف تقنياتهم وأساليبهم، وتنفيذ عمليات استطلاع إلكتروني لرصد التحضيرات للهجمات السيبرانية، واختراق شبكات الخصوم لجمع معلومات استخباراتية حول قدراتهم ونواياهم، كما تتضمن الإجراءات الاستباقية الإيرانية تنفيذ عمليات تأثير في الفضاء السيبراني، تهدف إلى التأثير على المشهد المعلوماتي في الدول المستهدفة، وتشتيت انتباه الخصوم، وخلق حالة من الارتباك والتشويش تعيق قدرتهم على تنفيذ هجمات سيبرانية ضد المصالح الإيرانية، فتعتمد الاستراتيجية الاستباقية الإيرانية أيضاً على تطوير قدرات في مجال الهجمات الإلكترونية، تمكنها من تنفيذ ضربات استباقية ضد مصادر التهديد المحتملة. وتتضمن هذه القدرات تطوير برمجيات خبيثة متطورة، وأدوات لاختراق الأنظمة والشبكات، وتقنيات لتعطيل الخدمات الإلكترونية في الدول المستهدفة (العربية نت، 2024).

وتجدر الإشارة إلى أن الإجراءات الاستباقية الإيرانية تواجه تحديات قانونية وسياسية على المستوى الدولي، حيث يمكن عدّها انتهاكاً للسيادة الرقمية للدول الأخرى. ومع ذلك، تنظر إيران إلى هذه الإجراءات بوصفها ضرورة استراتيجية لحماية مصالحها الوطنية العليا، في ظل التهديدات المتزايدة التي تواجهها في الفضاء السيبراني.

ويتضح من التحليل السابق أن الحاجة إلى بناء قدرات ردع سيبراني وتنفيذ إجراءات استباقية ضد التهديدات المحتملة تشكل محوراً أساسياً في الاستراتيجية الأمنية السيبرانية الإيرانية. وتسعى إيران من خلال هذه القدرات والإجراءات إلى تحقيق توازن استراتيجي مع خصومها في الفضاء السيبراني، وبناء منظومة أمنية متكاملة قادرة على حماية مصالحها الوطنية العُليا في العصر الرقمي.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

https://doi.org/10.61353/ma.0260365

الخاتمة

تُعد قضية التهديدات السيبرانية وتأثيرها العميق في تطوير الاستراتيجية الأمنية الإيرانية بعد عام 2010 من الموضوعات البارزة خاصة بعد الهجوم على المنشآت النووية . فقد أظهرت الأهمية المتزايدة للفضاء السيبراني بوصفه ساحةً رئيسةً للصراع والتنافس الدولي، مما جعل حماية هذا الفضاء جزءاً أساسياً من الأمن القومي للدول، بما في ذلك الجمهورية الإسلامية الإيرانية.

وتسعى إيران جاهدة لفهم طبيعة التهديدات السيبرانية المتنوعة وتحديد مصادرها، مع التركيز بشكل خاص على التحديات التي تمثلها القدرات السيبرانية للولايات المتحدة والكيان الإسرائيلي، وفي مواجهة تلك التهديدات، لم تقتصر الاستجابة الإيرانية على الجانب الدفاعي فحسب، بل شملت أيضاً بناء قدرات هجومية وردعية تهدف إلى حماية المصالح الوطنية الحيوية، مثل البرنامج النووي والمؤسسات الحساسة، وهو ما اتضح في حرب الـ(12) يوماً السيبرانية والصاروخية ضد الكيان الإسرائيلي التي اندلعت في حزيران 2025 بسبب فشل مفاوضات البرنامج النووي مع الولايات المتحدة.

وتتجلى الاستراتيجية الأمنية السيبرانية الإيرانية كنتيجة لتفاعل معقد بين إدراك التهديدات، وتطوير القدرات البشرية والتكنولوجية، ووضع الأطر التشريعية والتنظيمية اللازمة، إذ تسعى إيران ليس فقط إلى صد الهجمات ومنع اختراق أنظمتها، بل أيضاً إلى تطوير إمكانيات لتنفيذ إجراءات استباقية واستخدام الفضاء السيبراني بوصفه أداةً لتحقيق أهدافها الاستراتيجية.

وتشمل الاستعدادات الإيرانية لمواجهة تلك التهديدات جوانب متعددة، منها العلمية والأكاديمية والأمنية والعسكرية والاستخباراتية والإعلامية، بالإضافة إلى تعزيز التعاون الدولي. وتمتلك إيران أبعاداً هجومية في استراتيجيتها، بما في ذلك استخدام أدوات سيبرانية متطورة ومهاجمة البنى التحتية الحيوية للخصوم، كما حصل في حرب الـ(12) يوماً ضد الكيان الإسرائيلي .

أولاً-الاستنتاجات:

1-التطور الاستراتيجي المتسارع: شهدت الاستراتيجية الأمنية السيبرانية الإيرانية تطوراً ملحوظاً ومتسارعاً بعد عام 2010، استجابة مباشرة لتصاعد وتيرة ونوعية التهديدات السيبرانية التي استهدفت بنيتها التحتية الحيوية ومصالحها الوطنية، وعلى رأسها الهجمات التي طالت برنامجها النووي.

2-محورية القدرات السيبرانية: أصبحت القدرات السيبرانية ركيزة أساسية في منظومة الأمن القومي الإيراني، إذ تستثمر الدولة بشكل كبير في تطوير القدرات البشرية والتكنولوجية، وسنّ التشريعات القانونية اللازمة، لتعزيز مكانتها في الفضاء السيبراني.

3-عمليات الاستراتيجية (الدفاع والهجوم): تتبنى إيران استراتيجية سيبرانية مزدوجة تجمع بين الدفاع والهجوم. فبينما تركز على بناء دفاعات قوية لحماية أنظمتها ومنشآتها الحيوية، تعمل في الوقت ذاته على تطوير قدرات هجومية وردعية لردع الخصوم ومواجهة التهديدات بشكل استباقي عند الضرورة.

4-تحديد مصادر التهديد: تعد إيران كلاً من الولايات المتحدة والكيان الصهيوني المصدرين الرئيسيين للتهديدات السيبرانية الموجهة ضدها، وهو ما يوجه بشكل كبير طبيعة استعداداتها واستراتيجياتها الدفاعية والهجومية.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

5-أهمية الردع السيبراني: تسعى إيران جاهدة لبناء قدرات ردع سيبراني ذات مصداقية، بهدف منع الخصوم من شن هجمات واسعة النطاق، وذلك عبر إظهار قدرتها على إلحاق أضرار مضادة ومؤثرة.

ثانياً-التوصيات:

لا شك في أنَّ لموضوع الدراسة تأثيرا سلبيا كبيرا على أمن العراق وسيادته، إذ إنَّ أي تفوق استراتيجي سيبراني لأيّ دولةٍ من دول المنطقة عامة، ودول الجوار خاصة، يعد مصدر تهديدٍ أمنيّ كامنٍ للعراق، وفي حالة استخدام القدرات السيبرانية بين أيٍّ من دول المنطقة سوف يضر بالمصالح العليا للعراق، لاسيَّما في المجال الأمني والتنموي، وقد يجعل إقليم العراق ساحةً للصراع السيبراني والصاروخي، ولاسيَّما في المجال الجوي.

وعلى أساس ذلك، يمكن تقديم توصيات عدة إلى صُنّاع القرار السياسي في العراق، وكما يأتي:

1-تعزيز الاستثمار السيبراني المستمر: ضرورة مواصلة الاستثمار في بناء وتطوير القدرات السيبرانية الوطنية، سواء البشرية عبر برامج التدريب والتأهيل المتخصصة، أو التكنولوجية عبر البحث والتطوير وتبني أحدث التقنيات الدفاعية والهجومية.

2-تطوير الأطر القانونية والتنظيمية: أهمية استكمال وتحديث الأطر التشريعية والتنظيمية المتعلقة بالأمن السيبراني، بما يضمن مواكبة التطورات التكنولوجية وطبيعة التهديدات المتغيرة، وتحديد المسؤوليات والصلاحيات بوضوح.

3-تعميق التعاون الدولي: استكشاف فرص التعاون الدولي في مجال الأمن السيبراني مع الدول الصديقة أو ذات التوجهات المماثلة، لتبادل الخبرات والمعلومات حول التهديدات المشتركة وأفضل الممارسات الدفاعية، مع الحفاظ على المصالح الوطنية العليا.

4-**تطوير استراتيجيات الردع:** العمل على تطوير استراتيجيات ردع سيبراني أكثر تطوراً ومرونة، لا تقتصر على القدرات التقنية فحسب، بل تشمل أيضاً الجوانب النفسية والإعلامية والدبلوماسية.

5-دعم البحث العلمي والأكاديمي: تشجيع ودعم البحث العلمي والدراسات الأكاديمية المتخصصة في مجال الأمن السيبراني، لفهم أعمق للتهديدات الناشئة وتطوير حلول مبتكرة واستراتيجيات فعالة للمواجهة.

6-تعزيز الوعي المجتمعي: رفع مستوى الوعي بأهمية الأمن السيبراني ومخاطر التهديدات السيبرانية لدى مختلف شرائح المجتمع والمؤسسات، لتعزيز ثقافة الأمن السيبراني بوصفه جزءاً من المسؤولية الوطنية الشاملة.

7-مواصلة البحث في هذا المجال: مواصلة البحث، ولاسيَّما فيما يتعلق بتأثير التقنيات الناشئة كالذكاء الاصطناعي على مستقبل الأمن السيبراني الإيراني واستراتيجياته المتطورة.

ويؤكد هذا البحث على أن الفضاء السيبراني قد أصبح ساحة مواجهة رئيسة في العلاقات الدولية، وأن تطوير استراتيجية أمنية سيبرانية قوية ومتكاملة يعد ضرورة حتمية للدول للحفاظ على أمنها القومي ومصالحها الحيوية في عالم يزداد ترابطاً وتعقيداً يوماً بعد يوم.

ومن هنا نقترح على الباحثين والمختصين البحث في أسباب حرب الـ(12) يوماً التي اندلعت بين إيران والكيان الإسرائيلي وتداعياتها الإقليمية والدولية.

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0

المراجع

1. بن أحسن، أنيس عبد الوهاب. (2022). القوة السيبرانية الإيرانية وأثرها على الاستقرار الإقليمي. *مجلة السياسة العالمية*، (2)، جامعة محمد بوقرة بومرداس، الجزائر.
2. الجزيرة نت. (د.ت.). أبرز الإجراءات الوقائية الإيرانية لسد الثغرات الأمنية. استُرجع في 7 مايو 2025، من https://nabdapp.com/t/143808379
3. ديكي، إسراء. (2023). الإصلاح في مجال تكنولوجيا المعلومات والاتصالات في الجمهورية الإسلامية الإيرانية: المبادرات. *مجلة كلية الاقتصاد والعلوم الإدارية*، (1)، جامعة طرسوس، تركيا.
4. الرزو، حسن مظفر. (د.ت.). تأثير تحولات إيران إلى الشرق على استراتيجيتها السيبرانية وانعكاساتها المحتملة على المجال الجيوسياسي-السيبراني في منطقة الشرق الأوسط. *مجلة مدارات إيرانية*، (22). المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين.
5. صيوح، لؤي، وآخرون. (2022). دور الأمن السيبراني في الاستراتيجية الأمنية الإيرانية. *مجلة جامعة تشرين*، 44(5)، جامعة تشرين، سوريا.
6. العربية نت. (2024، 29 أغسطس). للإيقاع بجواسيس في لبنان وسوريا.. إيران أدارت شبكة وهمية. https://www.alarabiya.net/iran/2024/08/29
7. عزي، محمد فريد. (د.ت.). النشاط السيبراني الإيراني: ما بين السرية والعلن. ترينذز للبحوث والاستشارات. استُرجع في 5 مايو 2025، من https://trendsresearch.org/ar/insight
8. فريحات، معاذ. (2024، نوفمبر). أنشطة إيران السرية: هجمات خبيثة عبر الويب المظلم. الحرة. https://www.alhurra.com/iran/2024/11/2
9. كوهون، مليندا. (2022). *عمليات ضبط المعلومات في الفضاء السيبراني الإيراني: استراتيجية الحرب الناعمة*. المركز العربي للأبحاث ودراسة السياسات، وحدة الدراسات الإيرانية.
10. مركز المستقبل للأبحاث والدراسات المتقدمة. (د.ت.). بين الدفاع والهجوم: التطورات الإيرانية في مجال الحرب الإلكترونية. استُرجع في 10 مايو 2025، من https://futureuae.com/ar/Mainpage/Item/783/
11. مركز الملك فيصل للبحوث والدراسات الإسلامية. (2020). *قدرات القرصنة السيبرانية الإيرانية*. الرياض.
12. مؤسسة اليوم الثامن للإعلام والدراسات. (د.ت.). "ذباب مايو".. مصنع أكاذيب إيراني على الإنترنت. استُرجع في 9 مايو 2025، من https://alyoum8.net/posts/46839
13. Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat: Espionage, sabotage, and revenge*. Carnegie Endowment for International Peace.
14. Assoudeh, M. (2020). *Shaping cybersecurity strategy: China, Iran, and Russia in a comparative perspective* [Doctoral dissertation, University of Nevada, Reno].
15. Baezner, M. (2019). *Iranian cyber-activities in the context of regional rivalries and international tensions*. Center for Security Studies (CSS), ETH Zürich.
16. Stachon, M. (2024). Iranian cyber capabilities as a tool of domestic and foreign policy. *Zeszyty Naukowe SGSP*, (89).

هذا العمل مرخص بموجب الاسناد/ غير تجاري/ 4.0 دولي. CC BY-NC 4.0