استراتيجيات الردع السيبراني في الشرق الاوسط: دراسة في التحديات والفاعلية(ايران – الكيان الصهيوني نموذجاً)

م.د محمد جاسم حسين

وزارة التعليم العالي والبحث العلمي/ جامعة القادسية/ كلية الزراعة

Mohmmed_J@qu.edu.iq

الكلمات المفتاحية: الردع السيبراني، ايران، الكيان الصهيوني، التحديات، الفاعلية

كيفية اقتباس البحث

حسين ، محمد جاسم ، استراتيجيات الردع السيبراني في الشرق الاوسط: دراسة في التحديات والفاعلية(ايران – الكيان الصهيوني نموذجاً)،مجلة مركز بابل للدراسات الانسانية، آيار ٢٠٢٦، المجلد:١٦ ،العدد:٥ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Cyber Deterrence Strategies in the Middle East: A Study of Challenges and Effectiveness — (Iran and the Zionist Entity as a Model)

Lecturer Dr. Mohammed Jasim Hussein
Ministry of Higher Education and Scientific Research / University of Al-Qadisiyah / College of Agriculture
Mohmmed_J@qu.edu.iq

Keywords : Cyber Deterrence, Iran, the Zionist Entity, Challenges, Effectiveness

How To Cite This Article
Hussein ، Mohammed Jasim ، Cyber Deterrence Strategies in the Middle East: A Study of Challenges and Effectiveness — (Iran and the Zionist Entity as a Model) ,Journal Of Babylon Center For Humanities Studies, May 2026,Volume:16,Issue 5.

Abstract

This study examines cyber deterrence strategies in the Middle East, focusing on Iran and Israel as a model of regional cyber rivalry. It argues that cyber deterrence is not limited to offensive capabilities, but also depends on protecting critical infrastructure, identifying threats, ensuring rapid response, and controlling escalation. Iran uses cyberspace as an asymmetric tool to compensate for military and technological gaps through espionage, influence operations, and political pressure. In contrast, Israel relies on technological superiority, intelligence capabilities, and advanced institutional structures in cybersecurity. The study shows that cyber deterrence in the region remains relatively limited because of attribution difficulties, proxy actors, legal ambiguity, and the overlap between civilian and military targets. It concludes that effective

cyber deterrence requires the integration of technical defense, institutional readiness, political signaling, and rapid recovery capacity.
The study was divided into three main sections, in addition to an introduction, conclusion, and findings. The first section addressed the conceptual and theoretical framework of cyber deterrence, and was divided into three key points: first, the concept of cyber deterrence and its development in contemporary strategic thought; second, patterns of cyber deterrence strategies; and third, the characteristics of the cyber environment and their impact on the effectiveness of deterrence. The second section, titled "Cyber Deterrence Strategies of Regional Actors," was divided into three parts: first, the Iranian cyber strategy; second, the Israeli cyber strategy; and third, a comparison of the capabilities of these actors. The third section, titled "Challenges and Effectiveness of Cyber Deterrence in the Middle East," addressed the following: first, the challenges of cyber deterrence; second, an evaluation of the effectiveness of cyber deterrence; and third, the prospects for cyber deterrence in the Middle East.

الملخص

تبحث هذه الدراسة في استراتيجيات الردع السيبراني في الشرق الأوسط، مع التركيز على إيران والكيان الصهيوني نموذجاً للصراع السيبراني الإقليمي. وتنطلق الدراسة من أن الردع السيبراني لم يعد مقتصراً على امتلاك القدرات الهجومية، بل يرتبط بقدرة الدولة على حماية بنيتها التحتية، وكشف مصادر التهديد، والاستجابة السريعة، وإدارة التصعيد. تعتمد إيران على الفضاء السيبراني كأداة غير تقليدية لتعويض الفجوة العسكرية والتقنية، من خلال عمليات التجسس والتأثير والضغط السياسي. في المقابل، يستند الكيان الصهيوني إلى تفوق تقني واستخباراتي وبنية مؤسسية متقدمة في الأمن السيبراني. وتوضح الدراسة أن فاعلية الردع السيبراني في المنطقة تبقى نسبية بسبب صعوبة إسناد الهجمات، وتعدد الفاعلين، واستخدام الوكلاء، وغموض قواعد القانون الدولي. وتخلص إلى أن الردع السيبراني الفعال يتطلب تكاملاً بين الدفاع التقني، والجاهزية المؤسسية، والردع السياسي، والقدرة على التعافي السريع.

قسمت الدراسة الى ثلاث محاور رئيسة، فضلا عن، مقدمة وخاتمة واستنتاجات، اذ تناول المحور الاول الاطار المفاهيمي والنظري للردع السيبراني، وقسم الى ثلاث نقاط محورية وهي اولاً: مفهوم الردع السيبراني وتطوره في الفكر الاستراتيجي المعاصر، وثانياً: انماط استراتيجيات الردع السيبراني، وثالثا: خصائص البيئة السيبرانية وتأثيرها على فاعلية الردع. اما المحور الثاني فقد جاء بعنوان استراتيجيات الردع السيبراني لدى الفاعلين الاقليميين، وقسم الى

اولاً: الاستراتيجية السيبرانية الايرانية، وثانيا: الاستراتيجية السيبرانية للكيان الصهيوني، وثالثاً: مقارنة القدرات لدى الفاعلين. كما جاء المحور الثالث بعنوان التحديات وفاعلية الردع السيبراني في الشرق الاوسط، الذي تناول اولاً: تحديات الردع السيبراني، وثانيا: تقييم فاعلية الردع السيبراني، وثالثاً افاق الردع السيبراني في الشرق الاوسط.

المقدمة

يشهد الشرق الأوسط تصاعداً كبيراً في توظيف الفضاء السيبراني ضمن معادلات القوة والصراع، إذ لم تعد المواجهة بين الدول تقتصر على الأدوات العسكرية التقليدية، بل امتدت إلى المجال الرقمي بوصفه ساحة مؤثرة في الأمن القومي والاستقرار الإقليمي.

وفي هذا السياق، تبرز استراتيجيات الردع السيبراني بوصفها مدخلاً لفهم كيفية منع الخصوم من تنفيذ هجمات إلكترونية أو الحد من ثارها عبر الدفاع، والتهديد بالرد، وبناء القدرة على التعافي. وتكتسب دراسة إيران والكيان الصهيوني أهمية خاصة نظراً لطبيعة الصراع الممتد بينهما، وما يتضمنه من عمليات سيبرانية مباشرة وغير مباشرة، وحملات تأثير، واستخدام للوكلاء، واستهداف للبنى التحتية والمجالات الحيوية. كما تكشف هذه الحالة عن إشكاليات جوهرية تواجه الردع السيبراني، منها صعوبة تحديد مصدر الهجوم، وغموض قواعد الاشتباك، وتداخل الأهداف المدنية والعسكرية. لذلك يسعى هذا البحث إلى تحليل تحديات الردع السيبراني وقياس فاعليته في البيئة الشرق أوسطية، من خلال دراسة النموذج الإيراني–الصهيوني بوصفه أحد أبرز نماذج الصراع السيبراني المعاصر.

اهمية الدراسة

تنبع أهمية هذه الدراسة من كونها تتناول موضوعاً معاصراً يرتبط مباشرة بتحولات الأمن القومي في الشرق الأوسط، أصبح الفضاء السيبراني ساحة رئيسة للتنافس والصراع بين الدول. وتزداد أهمية البحث من خلال تركيزه على إيران والكيان الصهيوني بوصفهما نموذجين بارزين في توظيف القدرات السيبرانية ضمن استراتيجيات الردع والتأثير والضغط السياسي.

وتكتسب الدراسة أهميتها العلمية من سعيها إلى سد جانب من النقص في الدراسات العربية المتعلقة بالردع السيبراني، وربط المفهوم النظري بالتطبيق العملي في الشرق الأوسط. أما أهميتها العملية فتتمثل في تقديم رؤية تحليلية يمكن أن تفيد صانعي القرار والباحثين في تطوير سياسات أكثر كفاءة لمواجهة التهديدات السيبرانية وتعزيز الأمن الرقمي والاستقرار الإقليمي.

هدف الدراسة:

تهدف هذه الدراسة إلى تحليل استراتيجيات الردع السيبراني في الشرق الأوسط، وبيان طبيعة التحديات التي تواجه فاعليتها في ظل بيئة إقليمية تتسم بالصراع والتنافس الأمني. كما تسعى إلى دراسة النموذج الإيراني–الصهيوني بوصفه حالة تطبيقية تكشف اليات توظيف الفضاء السيبراني في الردع، والضغط، والتأثير السياسي والأمني.

وتركز الدراسة على توضيح مفهوم الردع السيبراني وأبعاده الدفاعية والهجومية والمؤسسية، وبيان مدى قدرة هذه الاستراتيجيات على منع الهجمات السيبرانية أو الحد من اثارها. كما تهدف إلى الكشف عن أبرز المعوقات التي تحد من فاعلية الردع السيبراني.

اشكالية الدراسة

تتمحور إشكالية الدراسة حول مدى قدرة استراتيجيات الردع السيبراني على تحقيق الفاعلية في بيئة الشرق الأوسط، ولا سيما في ظل الصراع بين إيران والكيان الصهيوني، اذ يتسم الفضاء السيبراني بالغموض، وتعدد الفاعلين، وصعوبة تحديد مصادر الهجمات، وتداخل الأدوات التقنية مع الأهداف السياسية والأمنية. ومن هنا لابد من الاجابة على السئلة الاتية:

١–ما المقصود بالردع السيبراني، وما ابرز الياته؟

٢–كيف توظف إيران والكيان الصهيوني الفضاء السيبراني ضمن استراتيجيات الردع؟

٣–ما التحديات التي تحد من فاعلية الردع السيبراني في الشرق الأوسط؟

٤–ما مدى فاعلية الردع السيبراني في في الشرق الاوسط، في ظل افاق معقدة ومتسارعة؟

فرضية الدراسة

تنطلق الدراسة من فرضية رئيسة مفادها أن فاعلية استراتيجيات الردع السيبراني في الشرق الأوسط تبقى نسبية ومحدودة، على الرغم من تطور القدرات السيبرانية لدى إيران والكيان الصهيوني، وذلك بسبب طبيعة الفضاء السيبراني القائمة على الغموض، وصعوبة اسناد الهجمات، وتعدد الفاعلين، واستخدام الوكلاء، وغياب قواعد قانونية واضحة تنظم السلوك السيبراني بين الدولتين.

منهجية الدراسة

اعتمدت هذه الدراسة على عدة مناهج اذ استخدم المنهج الوصفي التحليلي لوصف مفهوم واليات الردع السيبراني، كما استخدم المنهج الاستنتاجي والاستنباطي لدراسة استراتيجيات الردع لدى ايران والكيان الصهيوني. في حين، استخدم المنهج الاستشرافي في بيان افاق الردع السيبراني في الشرق الاوسط.

هيكلية الدراسة

قسمت الدراسة الى ثلاث محاور رئيسة، فضلا عن، مقدمة وخاتمة واستنتاجات، اذ تناول المحور الاول الاطار المفاهيمي والنظري للردع السيبراني، وقسم الى ثلاث نقاط محورية وهي اولاً: مفهوم الردع السيبراني وتطوره في الفكر الاستراتيجي المعاصر، وثانياً: انماط استراتيجيات الردع السيبراني، وثالثا: خصائص البيئة السيبرانية وتأثيرها على فاعلية الردع. اما المحور الثاني فقد جاء بعنوان استراتيجيات الردع السيبراني لدى الفاعلين الاقليميين، وقسم الى اولاً: الاستراتيجية السيبرانية الايرانية، وثانيا: الاستراتيجية السيبرانية للكيان الصهيوني، وثالثاً: مقارنة القدرات لدى الفاعلين. كما جاء المحور الثالث بعنوان التحديات وفاعلية الردع السيبراني في الشرق الاوسط، الذي تناول اولاً: تحديات الردع السيبراني، وثانيا: تقييم فاعلية الردع السيبراني، وثالثاً افاق الردع السيبراني في الشرق الاوسط.

المحور الاول: الاطار المفاهيمي والنظري للردع السيبراني

دأبت الادبيات الاستراتيجية في تناول الردع السيبراني، واضحت العديد من مراكز الفكر والمؤسسات الرسمية وغير الرسمية تبحث عن تأطير لمفهوم الردع السيبراني والياتة وانماطة، ومن هنا جاءت الرؤية لدراستة بشئ من التفصيل. اذ قسم هذا المحور الى: مفهوم الردع السيبراني وتطوره في الفكر الاستراتيجي المعاصر، وانماط واستراتيجيات الردع السيبراني، وكذلك خصائص البيئة التي يعمل بها.

اولاً: مفهوم الردع السيبراني وتطوره في الفكر الاستراتيجي المعاصر

يعد الردع السيبراني أحد المفاهيم الحديثة في الدراسات الاستراتيجية والأمن الدولي، وقد ظهر نتيجة التحول المتزايد في طبيعة التهديدات من المجال العسكري التقليدي إلى المجال الرقمي[١]. ويقصد بالردع السيبراني قدرة دولة أو منظمة أو فاعل ما على منع الخصم من تنفيذ هجوم إلكتروني، أو تقليل احتمالية إقدامه عليه، من خلال التأثير في حساباته المتعلقة بالكلفة والعائد. فالمهاجم، وفق هذا التصور، لا يتخذ قراره بمعزل عن توقعاته لنتائج الهجوم، بل يوازن بين ما يمكن أن يحققه من مكاسب وما قد يتعرض له من خسائر أو عقوبات أو فشل تقني[٢].

ينطلق مفهوم الردع السيبراني من فكرة الردع التقليدي التي عرفت فيها الدراسات الاستراتيجية والعلاقات الدولية، ولا سيما خلال مرحلة الحرب الباردة، حين ارتبط الردع بمنع الخصوم من استخدام القوة العسكرية عبر التهديد بعواقب شديدة. غير أن نقل هذا المفهوم إلى البيئة السيبرانية لم يكن انتقالاً مباشراً أو بسيطاً، لأن الفضاء السيبراني يختلف جذرياً عن المجالات التقليدية للحرب والصراع. ففي المجال الرقمي يصعب أحياناً تحديد هوية المهاجم، كما أن الهجمات قد

تنفذ من دول أو جماعات أو أفراد، وقد تتم بسرعة وبكلفة منخفضة نسبياً، فضلاً عن أن آثارها قد تكون غير واضحة في لحظتها الأولى(٣).

وفي هذا السياق، يمكن فهم الردع السيبراني بوصفه عملية استراتيجية تهدف إلى تشكيل سلوك الخصم قبل وقوع الهجوم، وذلك عبر إقناعه بأن الهجوم لن يكون مجدياً أو أن نتائجه ستكون مكلفة. ولا يقتصر الردع هنا على التهديد بالرد، بل يشمل أيضاً بناء قدرات دفاعية قوية تجعل الهجوم صعب التنفيذ أو محدود التأثير. ولهذا أصبح المفهوم في الأدبيات الاستراتيجية أكثر اتساعاً من مجرد العقاب، إذ بات يشمل منع النجاح، وتقليل الفائدة، ورفع الكلفة، وإضعاف الدافع لدى الخصم(٤).

وقد مر مفهوم الردع السيبراني بعدة مراحل من التطور. ففي بداياته، خلال تسعينيات القرن العشرين، لم يكن المفهوم واضحاً أو مستقلاً، بل كان يندرج ضمن نقاشات أوسع حول حرب المعلومات وأمن الشبكات والبنية التحتية الرقمية. في تلك المرحلة، كان التركيز منصباً على حماية الأنظمة المعلوماتية من الاختراق والتخريب، ولم تكن نظرية الردع السيبراني قد اكتسبت بعد إطاراً مفاهيمياً مستقلاً. اذ كان الاهتمام منصباً بصورة أكبر على الجانب التقني، أي كيفية منع الاختراق أو الحد من آثاره، أكثر من الاهتمام بالسلوك الاستراتيجي للخصوم(٥).

ومع بداية القرن الحادي والعشرين، بدأ المفهوم يكتسب أهمية أكبر مع ازدياد اعتماد الدول والمؤسسات على البنية الرقمية. فقد أصبحت الشبكات الإلكترونية جزءاً أساسياً من إدارة الاقتصاد، والطاقة، والاتصالات، والخدمات الحكومية، والقدرات العسكرية. وبذلك لم تعد الهجمات السيبرانية مجرد أعمال تقنية محدودة، بل تحولت إلى تهديدات محتملة للأمن القومي والاستقرار السياسي والاقتصادي. هذا التحول ساعد على إدخال الردع السيبراني في النقاشات الأمنية والاستراتيجية بوصفه أداة لفهم كيفية منع الخصوم من استغلال نقاط الضعف الرقمية(٦).

ومع مرور الوقت، أصبح الردع السيبراني مفهوماً أكثر تعقيداً وأقل يقيناً من الردع التقليدي. فالردع النووي، على سبيل المثال، يقوم على وضوح نسبي في هوية الخصوم وحجم الدمار المتوقع، بينما يعمل الردع السيبراني في بيئة يغلب عليها الغموض والتغير السريع. كما أن الهجمات السيبرانية لا تصل كلها إلى مستوى الحرب، فقد تكون عمليات تجسس، أو تعطيل محدود، أو ابتزاز، أو تأثير سياسي وإعلامي. لذلك يصعب وضع قاعدة واحدة تنطبق على جميع أشكال السلوك العدائي في الفضاء السيبراني(٧).

وفي الأدبيات الاستراتيجية الحديثة، لم يعد الردع السيبراني ينظر إليه باعتباره وسيلة قادرة على منع جميع الهجمات، بل باعتباره أداة لتقليل المخاطر وضبط سلوك الخصوم في حدود معينة.

فالهجمات الصغيرة أو منخفضة الكلفة قد تستمر رغم وجود سياسات ردع، بينما يكون الردع أكثر فاعلية في مواجهة الهجمات الكبرى التي تستهدف البنية التحتية الحيوية أو الأمن القومي. وهذا يعني أن الردع السيبراني يعمل بدرجات متفاوتة، ولا يمكن التعامل معه كحل شامل أو نهائي لجميع التهديدات الرقمية[٨].

ثانيا: انماط واستراتيجيات الردع السيبراني

يرتكز الردع السيبراني في أحد انماطة الأساسية على مبدأ العقاب، أي إقناع الخصم بأن أي هجوم سيبراني سيترتب عليه ثمن سياسي أو اقتصادي أو قانوني أو تقني يفوق المكاسب المتوقعة منه. غير أن فاعلية هذا النمط لا تتحقق بمجرد امتلاك القدرة على الرد، بل تتطلب توافر عناصر مترابطة، أبرزها القدرة على إسناد الهجوم إلى فاعله بدرجة مقبولة من الموثوقية، وامتلاك أدوات مناسبة للرد، وامتلاك رؤية استراتيجية واضحة لاستخدام هذه الأدوات عند الضرورة[٩]. وفي المقابل، يظهر الردع بالإنكار بوصفه نمطاً أكثر ارتباطاً بالبنية الدفاعية، إذ يهدف إلى تقليل قدرة الخصم على تحقيق أهدافه من خلال رفع مستوى الحماية التقنية، وتحسين أنظمة المراقبة، وتطوير قدرات الكشف المبكر، وإغلاق الثغرات، وتقليل فرص الاختراق. وتنبع أهمية هذا النمط من أن الفاعل المعادي قد يتراجع عن الهجوم إذا أدرك أن احتمالات نجاحه محدودة أو أن النتائج المتوقعة لا تبرر الجهد والمخاطرة[١٠].

ولا ينفصل الردع بالإنكار عن مفهوم المرونة السيبرانية، إذ تفترض هذه المقاربة أن منع جميع الهجمات بصورة مطلقة أمر غير واقعي في بيئة رقمية شديدة التعقيد. لذلك تصبح القدرة على امتصاص الصدمة، واستمرار تقديم الخدمات الحيوية، واستعادة الأنظمة بسرعة بعد التعرض للهجوم، جزءاً لايتجزء من عملية الردع. كما يتخذ الردع السيبراني نمطاً اخر من خلال التشابك والاعتماد المتبادل، اذ إن ارتباط المصالح التقنية والاقتصادية بين الدول والشركات والبنى التحتية العابرة للحدود قد يجعل الهجوم على طرف معين ذا نتائج عكسية تطال المهاجم ذاته أو بيئته الاقتصادية والسياسية[١١].

ويبرز كذلك الردع القائم على المعايير والقانون بوصفه أحد المداخل الحديثة لتنظيم السلوك في الفضاء السيبراني. فالهدف هنا لا يقتصر على منع الهجوم من خلال القوة، بل يمتد إلى بناء تصور دولي مشترك حول السلوك المقبول وغير المقبول في البيئة الرقمية. وتؤدي المعايير الدولية، والاتفاقات السياسية، وآليات التعاون القانوني، والإدانة العلنية، دوراً مهماً في رفع الكلفة السياسية والمعنوية للهجمات السيبرانية [١٢].

وهنالك العديد من المدارس الاستراتيجية دأبت على تبني مفهوم الدفاع الأمامي، الذي يقوم على التحرك المبكر لاكتشاف التهديدات وتعطيلها قبل أن تصل إلى الشبكات الوطنية أو الأنظمة الحيوية. وتعكس هذه المقاربة تحولاً من الدفاع السلبي إلى الدفاع الاستباقي. وتعد حماية البنية التحتية الحرجة من أكثر مجالات الردع السيبراني أهمية، لأن استهداف قطاعات مثل الطاقة والمياه والصحة والاتصالات والنقل والخدمات المالية قد يؤدي إلى آثار تتجاوز المجال التقني لتطال الأمن الوطني والاستقرار الاجتماعي والاقتصادي(١٣).

كما أن الردع السيبراني يزداد فاعلية عندما يستند إلى التعاون والتحالفات، لأن التهديدات السيبرانية بطبيعتها عابرة للحدود، ولا تستطيع دولة واحدة مواجهتها بكفاءة كاملة. ويمنح الرد الجماعي الاستجابة وزناً استراتيجياً أكبر، كما يعزز القدرة على الإسناد، وتبادل المعلومات، وتنسيق العقوبات، وتقديم الدعم الفني للدول أوالمنظمات المتضررة. وكلما أدرك الخصم أن الهجوم على طرف واحد قد يستدعي رداً من أطراف متعددة، ارتفعت كلفة الهجوم وتراجعت احتمالات الإقدام عليه(١٤).

ثالثا: خصائص البيئة السيبرانية وتأثيرها على فاعلية الردع

تؤثر طبيعة البيئة السيبرانية بصورة مباشرة في فاعلية الردع، لأنها تختلف عن البيئات التقليدية التي يكون فيها مصدر التهديد أوضح، وحدود الفعل العدائي أكثر تحديداً. فالردع يقوم أساساً على جعل الخصم يقتنع بأن الهجوم لن يحقق له فائدة كافية، أو أن كلفته ستكون أكبر من عائده. غير أن البيئة السيبرانية تجعل هذه المعادلة أكثر تعقيداً، بسبب ما تحمله من خصائص فنية وسياسية وأمنية خاصة(١٥).

وتعد صعوبة تحديد مصدر الهجوم او مايسمى بمشكلة اسناد الهجمات من أهم خصائص البيئة السيبرانية. ففي الهجمات التقليدية يمكن غالباً معرفة الجهة المعتدية من خلال الموقع الجغرافي أو حركة القوات أو نوع السلاح المستخدم، أما في الهجمات السيبرانية، يستطيع المهاجم أن يخفي هويته، أو يستخدم خوادم وسيطة، أو ينفذ الهجوم عبر دول أخرى، أو يستعمل أدوات برمجية لا تدل عليه مباشرة. وهذا يضعف الردع؛ لأن الدولة لا تستطيع توجيه عقوبة رادعة ما لم تكن قادرة على إثبات هوية الفاعل. لذلك، كلما زادت صعوبة الإسناد، قلت قدرة الردع على التأثير في حسابات الخصم(١٦).

اما خاصية إمكانية التخفي والإنكار هي سمة سائدة في البيئة السيبرانية، فالفاعل السيبراني قد ينفذ الهجوم ثم ينكر علاقته به، أو يدعي أن العملية نفذت من طرف مستقل لا يخضع لسيطرته. هذه القدرة على الإنكار تمنحه هامشا للمناورة وتقلل شعوره بالخطر(١٧).

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

كما تتميز البيئة السيبرانية بـ السرعة العالية في التنفيذ والتأثير، وانخفاض كلفة الهجوم، فالهجوم قد يقع خلال دقائق أو ثوان، وقد تنتشر اثاره بسرعة داخل الشبكات والأنظمة. هذه السرعة تضغط على الطرف المستهدف، لأنه يحتاج إلى وقت لاكتشاف الهجوم، وفهم طبيعته، وتحديد مصدره، ثم اختيار الرد المناسب. وكلما كان الهجوم أسرع من قدرة الدولة على التحليل والاستجابة، ضعفت فاعلية الردع القائم على الرد اللاحق. لذلك يصبح الدفاع المسبق والكشف المبكر جزءاً من الردع في البيئة السيبرانية(١٨).

وتبرز أيضاً خاصية تعدد الفاعلين في البيئة السيبرانية، فالتهديد السيبراني لا يصدر عن الدول فقط، بل قد يصدر عن جماعات إجرامية، أو قراصنة مستقلين، أو شركات، أو جماعات تعمل بالوكالة لصالح دول. هذا التعدد يجعل الردع أكثر صعوبة، لأن كل فاعل يفكر بطريقة مختلفة. فالدولة قد تخشى العقوبات أو التصعيد السياسي، بينما قد لا تتأثر الجماعة الإجرامية بالتهديدات نفسها. لذلك لا يمكن استخدام أسلوب ردع واحد مع جميع الفاعلين، بل يجب أن يكون الردع مرناً ومتنوعاً(١٩).

وكذلك غموض الخطوط الحمراء او مايسمى بالادبيات الاستراتيجية بالغموض الاستراتيجي، ففي المجال التقليدي قد يكون عبور الحدود أو قصف هدف عسكري فعلاً واضحاً يستدعي رداً، أما في المجال السيبراني فالأمر أقل وضوحاً. فقد يصعب التمييز بين التجسس، والاختراق، والتخريب، والهجوم العدائي. هذا الغموض يشجع الخصم على اختبار حدود الطرف الآخر من خلال عمليات محدودة ومتكررة(٢٠).

وفي هذا السياق، تتيح البيئة السيبرانية تنفيذ عمليات دون الوصول إلى مستوى الحرب. فقد تقوم جهة ما بتعطيل موقع حكومي، أو سرقة بيانات، أو التأثير في الرأي العام، دون أن يؤدي ذلك إلى حرب مباشرة. هذه المساحة الرمادية تضعف فاعلية الردع، لأن الرد القوي قد يبدو مبالغاً فيه، بينما الرد الضعيف قد يشجع على تكرار الهجمات. وهنا تكمن المشكلة: الخصم يستطيع تحقيق مكاسب تدريجية دون تحمل كلفة مواجهة مفتوحة.

المحور الثاني: استراتيجيات الردع السيبراني لدى الفاعلين الاقليميين

البيئة السيبرانية في الشرق الاوسط تمتاز بالغموض والتعقيد بسبب طبيعة المواجهة بين القطبين الاقليميين، ولهذا نجد ان كلا الطرفين الايراني والصهيوني يعملان على بناء عقيدة سيبرانية للردع وبناء القدرات وفق رؤية تصارعية مستمرة. وقد قسم هذا المحور الى: الاستراتيجية الايرانية للردع السيبراني، والاستراتيجية السيبرانية للكيان الصهيوني، فضلاعن، مقارنة القدرات بين الطرفين.

اولاً: الاستراتيجية الايرانية للردع السيبراني

تقوم الاستراتيجية الايرانية للردع السيبراني على فكرة رئيسة مفادها أن الدولة لا تحتاج بالضرورة إلى امتلاك قدرة تدميرية شاملة لكي تؤثر في حسابات خصومها، فالغاية الأساسية هي رفع كلفة التصعيد، وإقناع الخصم بأن الضغط العسكري، السياسي والاقتصادي عليها قد يقابله رد في المجال الرقمي، سواء عبر التجسس، أو تعطيل الخدمات، أو تسريب المعلومات، أو استهداف البنى التحتية الضعيفة، أو التأثير في الرأي العام. ومن هنا يمكن فهم الاستراتيجية الإيرانية بوصفها نموذجاً من الردع بالعقاب المحدود؛ أي إلحاق أضرار محسوبة لا تصل غالباً إلى مستوى الحرب المباشرة [٢١].

وتستند عقيدة الردع السيبرانية الإيرانية إلى تصور أمني واسع يرى أن المعلومات والاتصال والفضاء الرقمي ليست مجالات محايدة، بل ساحات صراع تمس الامن القومي واستقراره. لذلك تجمع هذه العقيدة بين بعدين متلازمين: بعد داخلي يركز على الامن الداخلي والسيطرة على المجال الرقمي الوطني، وتبلور هذا البعد بعد احتجاجات عام ٢٠٠٩ . وبعد خارجي يهدف إلى ردع الخصوم والتأثير في بيئاتهم السياسية والأمنية، وهذا تعزز بعد هجوم Stuxnet الذي استهدف منشأة نطنز النووي[٢٢].

وفي هذا السياق، بدأت الرؤية الايرانية للردع السيبراني مع إنشاء المجلس الأعلى للفضاء السيبراني عام ٢٠١٢، وهو ما عكس انتقال الملف السيبراني من مستوى المعالجة الأمنية المتفرقة إلى مستوى الحوكمة المركزية. فقد أصبح الفضاء السيبراني مجالاً تشارك فيه مؤسسات سياسية وأمنية وعسكرية واستخبارية، بما ينسجم مع رؤية إيرانية تعد السيطرة على المجال الرقمي شرطاً لحماية الامن الوطني، وفي الوقت نفسه أداة لردع الخصوم[٢٣].

كما يمكن فهم قدرات الردع الإيرانية من خلال أربع وظائف رئيسة وهي[٢٤]:

١- التجسس والاستطلاع، اذ تقوم المؤسسات السيبرانية بإيران إلى جمع المعلومات من الحكومات، والمؤسسات الأكاديمية، والشركات، والمعارضين، والبنى التحتية.

٢- التخريب المحدود، وتشمل هذه الوظيفة تعطيل الخدمات، ومسح البيانات، واستهداف الأنظمة الصناعية الضعيفة، واستخدام البرمجيات المدمرة عندما يحقق ذلك أثراً سياسياً أو نفسياً.

٣- التأثير السياسي والإعلامي، فقد طورت إيران نمطاً يعتمد على الربط بين الاختراق والتسريب والتضخيم الإعلامي. وبذلك لا تكون العملية السيبرانية مكتملة بمجرد الوصول إلى الشبكة أو سرقة البيانات، بل تكتمل عندما تتحول إلى سردية سياسية تستهدف ثقة الجمهور بمؤسساته أو تكشف هشاشة الخصم أمام الرأي العام.

٤- السيطرة الداخلية، فإيران تستخدم أدواتها الرقمية لمراقبة المعارضة، وضبط المجال العام، وحجب الخدمات عند الأزمات، وتطوير شبكات وبنى رقمية وطنية تقلل اعتمادها على المنصات الخارجية.

وتعتمد إيران في تنفيذ هذه الوظائف على بنية مرنة ومتعددة المستويات. فهناك مؤسسات رسمية، وجهات مرتبطة بالحرس الثوري ووزارة الاستخبارات، وشركات واجهة، ومتعاقدون تقنيون، ومجموعات هاكتيفست أو شخصيات سيبرانية تعمل تحت أسماء مختلفة. ويوفر هذا التعدد ميزة استراتيجية مهمة، هي الإنكار المعقول. كما أظهرت الأحداث الاخيرة أن الكيان الصهيوني أصبح هدفاً مركزياً للنشاط السيبراني الإيراني، ويعود ذلك إلى طبيعة الصراع المباشر وغير المباشر بين الطرفين، وإلى رغبة إيران في استخدام الردع السيبراني كأداة دعم لمحورها الإقليمي. فالعمليات ضد إسرائيل لا تهدف دائماً إلى تحقيق ضرر تقني كبير، بل إلى إظهار قدرة إيران وحلفائها على نقل المواجهة إلى الداخل الإسرائيلي، وإرباك الجمهور، وإضعاف الثقة بالمنظومات الأمنية[٢٥].

فقد تزايد الاهتمام الغربي بمخاطر امتداد النشاط السيبراني الإيراني إلى البنية التحتية الحيوية، لاسيما في الحرب الاخيرة وتصاعد التوتر الإقليمي. اذ يرون ان الردع السيبراني الإيراني بوصفه قدرة مندمجة مع منظومة الأمن القومي الإيراني، فهو جزء من نمط أوسع يعتمد على ادوات متعددة داخلية وخارجية، يركز على عناصر متعددة هي: انخفاض الكلفة، صعوبة الاسناد، الاثر الاعلامي، والتحكم في مستوى التصعيد.

ثانياً: استراتيجية الكيان الصهيوني للردع السيبراني

تتبع الخصوصية الاستراتيجية للكيان الصهيوني في مجال الردع السيبراني من طبيعة البيئة الأمنية التي يتحرك فيها. فهو ينظر إلى نفسه بوصفه كيان محاط ببيئة امنية معقدة وغير مستقرة، ويواجه تهديدات تقليدية وغير تقليدية في آن واحد. فهو لا يتعامل مع الفضاء السيبراني باعتباره مجالاً منفصلاً عن الصراع السياسي والعسكري، بل يراه امتداداً للبيئة الأمنية التي يعمل فيها[٢٦].

ويمكن فهم الردع السيبراني للكيان الصهيوني من خلال تتبع تطور الاستراتيجيات الرسمية. ففي الاستراتيجية الوطنية للأمن السيبراني لعام ٢٠١٧، ركزت على بناء منظومة دفاعية قائمة على ثلاث ركائز رئيسة: المتانة السيبرانية، والمرونة السيبرانية، والدفاع السيبراني الوطني[٢٧].

ومن هذا المنطلق، فإن الردع السيبراني للكيان لا يقتصر على حماية الشبكات الحكومية أو البنى التحتية الرقمية، بل يشمل حماية الاقتصاد، والخدمات الحيوية، والقطاع الخاص، والثقة

العامة، والقدرة على إدارة الأزمات. فالتهديد السيبراني، من وجهة نظره، لا يسبب أضراراً تقنية فقط، بل يمكن أن يتحول إلى تهديد استراتيجي إذا أدى إلى تعطيل الخدمات الأساسية، أو إرباك المؤسسات، أو التأثير في الرأي العام، أو إضعاف صورة الدولة وقدرتها على الرد[٢٨].

وقد أظهرت الاستراتيجية الوطنية السيبرانية للكيان للفترة ٢٠٢٥–٢٠٢٨، التي ترى الفضاء السيبراني ميداناً للأمن القومي، لاسيما بعد تصاعد الهجمات السيبرانية خلال حرب السيوف الحديدية وماتلتها. وتشير الوثيقة إلى أن الهجمات السيبرانية الكبيرة ضد الكيان ارتفعت بصورة ملحوظة خلال تلك المرحلة، وأن الأضرار الاقتصادية للهجمات الرقمية أصبحت تمثل عبئاً على الاقتصاد والمجتمع. وهذا يعكس انتقال الأمن السيبراني من كونه مسألة تقنية إلى كونه قضية استراتيجية تمس القدرة على الاستمرار والعمل في ظروف الحرب والصراع[٢٩].

ويعتمد الكيان في تنفيذ استراتيجيته السيبرانية على بنية مؤسسية تجمع بين الطابع المدني والعسكري والاستخباري. منها وحدات استخبارية وتقنية متخصصة، وفي مقدمتها الوحدة ٨٢٠٠، التي تعد من أهم الوحدات المرتبطة بالاستخبارات الإشارية والعمليات التقنية في الجيش. ولا تكمن أهمية هذه الوحدة في الجانب العسكري فقط، بل تمتد أيضاً إلى القطاع التكنولوجي المدني؛ إن هذا التداخل بين الدولة والجيش والاستخبارات والقطاع الخاص يمنح الكيان قدرة عالية على بناء ردع سيبراني مركب[٣٠].

وتتمثل قوة استراتيجية الردع للكيان في شموليتها وتعدد أدواتها. فهي لا تعتمد على الدفاع التقني وحده، ولا على الرد العسكري وحده، بل تمزج بين الوقاية، والمرونة، والاستخبارات، والرد، والتعاون، والابتكار. وهذا يمنحها قدرة على التعامل مع مستويات مختلفة من التهديد، بدءاً من الهجمات منخفضة الشدة، وصولاً إلى العمليات التي تنفذها دول أو جماعات منظمة[٣١].

كما أن قرب المؤسسات السيبرانية من مركز القرار السياسي يمنح إسرائيل قدرة على التنسيق السريع بين المستويات المختلفة. وتوفر العلاقة بين الدولة والقطاع الخاص ميزة إضافية، إذ تسمح بتبادل المعلومات والاستفادة من الابتكار المدني في خدمة الأمن القومي[٣٢].

ثالثاً: مقارنة القدرات لدى الفاعلين

تتشابه إيران والكيان في إدراكهما لأهمية المجال السيبراني بوصفه ساحة مناسبة للعمل تحت مستوى الحرب التقليدية. غير أن هذا التشابه لا يلغي الفوارق الجوهرية بين النموذجين. فالكيان يمتلك منظومة ردع سيبرانية أكثر نضجاً من حيث البناء المؤسسي والتكامل بين الفاعلين، ويظهر ذلك في العلاقة الوثيقة بين المؤسسات الأمنية والعسكرية، وأجهزة الاستخبارات، والقطاع الخاص، والجامعات، ومراكز البحث والتطوير[٣٣].

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

في المقابل، يقوم الردع السيبراني الإيراني على منطق مختلف يرتبط بطبيعة العقيدة الأمنية الإيرانية القائمة على العمل غير المتماثل. فإيران لا تعتمد بالدرجة نفسها على التفوق التقني النوعي، بل تسعى إلى تعويض الفجوة مع إسرائيل من خلال توظيف أدوات منخفضة الكلفة، ومتكررة الاستخدام، وقابلة للإنكار السياسي. ويشمل ذلك الاعتماد على مجموعات مرتبطة بالدولة أو قريبة منها، وتنفيذ عمليات اختراق، وتسريب بيانات، وتشويه مواقع، وهجمات حجب خدمة، وحملات تأثير نفسي وإعلامي. وتمنح هذه الأدوات إيران قدرة على الاستنزاف والإزعاج المستمر، حتى عندما لا تكون قادرة على تحقيق ضرر استراتيجي واسع أو طويل الأمد[٣٤].

وتكشف المقارنة بين أدوات الطرفين عن اختلاف واضح في طبيعة الاستخدام والغاية. فأدوات الكيان تبدو أكثر اندماجا ضمن استراتيجية وطنية شاملة تجمع بين الحماية، والاستخبارات، والقدرات الهجومية، والتعاون الدولي، والصناعة السيبرانية المتقدمة. وبذلك لا يعمل المجال السيبراني للكيان بصورة معزولة، بل يتداخل مع الأدوات العسكرية والدبلوماسية والاقتصادية والتكنولوجية. أما الأدوات الإيرانية، فتتسم بدرجة أكبر من اللامركزية والمرونة، وتعتمد على تعدد الفاعلين، ولا سيما الحرس الثوري، ووزارة الاستخبارات، والجماعات السيبرانية العقائدية المقاومة مع الدولة. ويجعل هذا النمط إيران قادرة على تكثيف الضغط السيبراني على الخصوم[٣٥].

أما من حيث الفاعلية، فإن الكيان يبدو أكثر قدرة على تحقيق ردع سيبراني متقدم، لاسيما في جانبي المنع والعقاب. في المقابل، تكمن فاعلية إيران في قدرتها على إنتاج تهديد مستمر ومنخفض الكلفة. فهي وإن كانت أقل تفوقاً من الكيان من حيث الجودة التقنية والتكامل المؤسسي، فإنها قادرة على استخدام الفضاء السيبراني بوصفه وسيلة لاستنزاف الخصم وإرباكه وإظهار بعض جوانب هشاشته الأمنية. ومن ثم فإن فاعلية الردع الإيراني لا تقاس فقط بحجم الضرر المادي المباشر، بل أيضاً بقدرته على توليد أثر نفسي وإعلامي وسياسي، وعلى إبقاء الخصم في حالة استنفار أمني دائم[٣٦].

المحور الثالث: التحديات وفاعلية الردع السيبراني في الشرق الاوسط

ان جوهر الردع السيبراني يتمثل في قدرة الدولة في التعامل مع التحديات وكيفية صياغة رؤية استراتيجية للفاعلية التي تستطيع من خلالها التأثير في سلوكيات الخصم، ومن هنا قد قسم هذا المحور الى: تحديات الردع السيبراني اولاً، وتقييم فاعلية الردع السيبراني ثانياً، كذلك افاق الردع السيبراني في الشرق الاوسط ثالثاً.

اولاً: تحديات الردع السيبراني

يمثل الردع السيبراني بين إيران والكيان الصهيوني أحد أكثر نماذج الردع تعقيداً في الشرق الأوسط، لأنه لا يتحرك داخل إطار عسكري تقليدي واضح، بل داخل فضاء رمادي تتداخل فيه الاستخبارات، التخريب الرقمي، التأثير النفسي، استهداف البنى التحتية، والحرب غير المعلنة. فالردع في المجال السيبراني لا يعني منع الهجمات كلياً، لأن ذلك يكاد يكون غير ممكن عملياً، وإنما يعني جعل الهجوم أقل جدوى، وأكثر كلفة، وأشد غموضاً من حيث نتائجه السياسية والعسكرية[٣٧].

ان اكبر التحديات التي تواجه الردع السيبراني في الشرق الاوسط هو صعوبة تحديد عتبة الرد. ففي شهر نيسان من عام ٢٠٢٠ نسبت إلى إيران محاولة اختراق لأنظمة مياه إسرائيلية، وهي واقعة بالغة الحساسية لأنها مست قطاعاً حيوياً. وبعد أسابيع، وتحديداً في أيار من العام نفسه تعرض ميناء شهيد رجائي الإيراني في بندر عباس لهجوم سيبراني نسب إلى إسرائيل، وهو ميناء يتعامل مع نسبة كبيرة من حركة الواردات والصادرات الإيرانية. تكشف هذه الحادثة أن الردع السيبراني بين الطرفين يعمل غالباً بمنطق الرد غير المعلن، لا بمنطق الإعلان الرسمي عن المسؤولية[٣٨].

كما يعد تداخل الأهداف المدنية والعسكرية من اهم تحديات الردع بين الطرفين، فالمنشآت التي تستهدف سيبرانياً قد تكون مدنية في ظاهرها، لكنها ذات قيمة استراتيجية للدولة. المصارف، الموانئ، شركات الاتصالات، شركات الطاقة، المستشفيات، ومنصات البيانات لا تعمل كخدمات عامة فحسب، بل تشكل جزءاً من قدرة الدولة على الصمود في الأزمات. لهذا السبب، يصبح الردع السيبراني بين إيران والكيان أكثر خطورة؛ لأن ضرب هدف مدني قد يقرأ من الطرف الآخر بوصفه اعتداءً على الأمن القومي[٣٩].

اما من حيث عدم التماثل بين الطرفين، فالكيان يمتلك بنية متقدمة في الأمن السيبراني، وخبرة استخبارية وتقنية عالية، وقطاعاً تكنولوجياً قادراً على إنتاج أدوات دفاعية وهجومية متطورة. في المقابل، تعتمد إيران على مقاربة مختلفة تقوم على الكلفة المنخفضة، وتعدد الفاعلين، واستغلال الثغرات المعروفة، والتصيد الإلكتروني، وهجمات حجب الخدمة، والتسريبات، وبرمجيات المسح والتخريب. هذا الاختلاف لا يعني أن إيران عاجزة عن الردع، بل يعني أنها تمارس ردعاً غير متماثل؛ أي إنها لا تحتاج إلى مساواة إسرائيل تقنياً، بقدر ما تحتاج إلى امتلاك قدرة كافية على الإزعاج، والتعطيل، وخلق كلفة سياسية أو اقتصادية مستمرة. وهنا تصبح كثافة الهجمات وتكرارها بديلاً عن النوعية العالية في بعض الحالات[٤٠].

من جانب اخر، فكثير من العمليات لا تعلن باسم الدولة مباشرة، وهنا يأتي تحدي بروز الوكلاء السيبرانيين والقدرة على الانكار، وإنما تظهر عبر جماعات تحمل أسماء مستقلة أو شعارات أيديولوجية، مما يمنح الدولة مساحة للإنكار ويصعب عملية الرد القانوني أو العسكري(٤١).

بناءً على ذلك، يمكن القول إن الردع السيبراني بين إيران والكيان يقوم على معادلة مزدوجة وهي: ان الكيان يسعى إلى استخدام التفوق التقني لاحتواء القدرات الإيرانية وإرباك بنيتها الاستراتيجية، بينما تستخدم إيران الأدوات السيبرانية لتعويض اختلال ميزان القوة التقليدي وإبقاء الكيان تحت ضغط دائم. غير أن هذه المعادلة تظل غير مستقرة، لأن غياب قواعد واضحة للاشتباك، وتداخل المدني بالعسكري، وصعوبة الإسناد، وتعدد الوكلاء، كلها عوامل تجعل أي هجوم محدود قابلاً للتحول إلى أزمة أوسع وهذا مالوحظ في الحرب الاخيرة.

ثانياً: تقييم فاعلية استراتيجيات الردع السيبراني

إن تقييم فاعلية الردع السيبراني بين إيران والكيان لا ينبغي أن ينطلق من سؤال بسيط مفاده: هل توقفت الهجمات أم لا؟ لأن الفضاء السيبراني بطبيعته لا يسمح بالمنع الكامل، ولا يوفر حدوداً واضحة بين الهجوم، التجسس، التخريب، والتأثير النفسي. لذلك، فإن المعيار الأدق لقياس الفاعلية يتمثل في مدى قدرة الردع على تعديل حسابات الخصم، وخفض المكاسب المتوقعة من الهجوم، ومنع انتقال العمليات السيبرانية من مستوى الإزعاج والاستنزاف إلى مستوى الشلل الاستراتيجي أو المواجهة العسكرية المباشرة. ومن هذه الزاوية، يمكن وصف الردع السيبراني بين إيران والكيان بأنه ردع احتوائي غير حاسم؛ فهو قادر على ضبط مستوى الصراع، لكنه غير قادر على إنهائه أو منع تجدده(٤٢).

ولهذا تقوم الفاعلية النسبية للكيان على الجمع بين التفوق التقني، والقدرة الاستخبارية، والردود السيبرانية العقابية. فالكيان لا يسعى فقط إلى حماية شبكاته، بل يعمل على إيصال رسالة ردعية مفادها أن البنى الإيرانية الحساسة، سواء كانت نووية أو لوجستية أو مالية، قابلة للاختراق عند تجاوز حدود معينة. غير أن أثر هذه الاستراتيجية يبقى محدوداً إذا قيس بقدرتها على تغيير السلوك الإيراني بصورة دائمة، فالهجمات النوعية قد تفرض كلفة عالية على إيران، لكنها في المقابل لا تلغي دوافعها لاستخدام الفضاء السيبراني بوصفه أداة تعويضية في مواجهة التفوق الصهيوني التقليدي والتكنولوجي. ولذلك، فإن الردع يحقق نجاحاً تكتيكياً في رفع الكلفة، لكنه لا يحقق نجاحاً استراتيجياً في وقف السلوك السيبراني الإيراني(٤٣).

في المقابل، لا تقوم فاعلية الردع الإيراني على امتلاك تفوق تقني مماثل، بل على إنتاج ضغط مستمر ومنخفض الكلفة. ويهدف هذا النمط إلى إقناع الكيان بأن أمنه السيبراني سيبقى مكلفاً ومفتوحاً على الاستنزاف، حتى في ظل تفوقها الدفاعي والهجومي(٤٤).

بناءً على ما تقدم، يمكن القول إن فاعلية الردع السيبراني في النموذج الإيراني–الصهيوني تتوزع على ثلاثة مستويات، فعلى مستوى منع الحرب السيبرانية الشاملة، تبدو الفاعلية متوسطة إلى مرتفعة نسبياً، لأن الطرفين ما زالا يحرصان على إبقاء العمليات دون حد الانفجار الكامل. وعلى مستوى تقليل الهجمات اليومية، تبدو الفاعلية ضعيفة، لأن محاولات الاختراق والتأثير لم تتوقف، بل أخذت أشكالاً أكثر تنوعاً. أما على مستوى تغيير سلوك الخصم، فالفاعلية محدودة؛ إذ لم تتخل إيران عن أدواتها السيبرانية، ولم تتوقف إسرائيل عن استخدام الردع الهجومي والاختراق الوقائي.

ثالثاً: افاق الردع السيبراني في الشرق الاوسط

تتجه افاق الردع السيبراني في الشرق الأوسط نحو مزيد من التعقيد، نظراً لتداخل العوامل التقنية مع التحولات الجيوسياسية والأمنية في المنطقة. فالفضاء السيبراني لم يعد مجالاً تقنياً منفصلاً، بل أصبح امتداداً للصراع السياسي والعسكري، وأداة من أدوات التأثير والضغط. ومن ثم، فإن مستقبل الردع السيبراني في المنطقة لن يقوم على القدرة الهجومية وحدها، بل على مزيج من الحماية، والمرونة، والإسناد، والتعاون، وإدارة التصعيد(٤٥).

ومن المرجح أن يزداد الاعتماد على الردع بالمنع والمرونة بدلاً من الردع القائم فقط على العقاب. ويقصد بذلك أن تسعى الدول إلى تقليل فرص نجاح الهجمات السيبرانية من خلال تعزيز أمن البنية التحتية الحيوية، وتطوير أنظمة الإنذار المبكر، ورفع كفاءة الاستجابة للحوادث، وضمان استمرارية الخدمات الأساسية. فكلما انخفضت قدرة الخصم على إحداث ضرر فعلي أو طويل الأمد، تراجعت جدوى الهجوم السيبراني كأداة للضغط أو الابتزاز(٤٦).

وفي هذا السياق، ستبقى المنطقة مرشحة لاستمرار نمط الصراع السيبراني منخفض العتبة. فالهجمات السيبرانية توفر للدول والفاعلين غير الدوليين وسيلة لممارسة الضغط، أو الرد، أو جمع المعلومات، أو التأثير في الخصوم دون تجاوز عتبة الحرب التقليدية. وهذا يجعل الفضاء السيبراني مجالاً مثالياً للصراعات الرمادية، اذ يمكن تنفيذ عمليات مؤثرة مع قدر من الغموض السياسي والقانوني حول المسؤولية والرد المناسب(٤٧).

كما سيؤدي تطور الذكاء الاصطناعي والتقنيات الناشئة إلى إعادة تشكيل معادلة الردع السيبراني. فمن جهة، يمكن لهذه التقنيات أن تزيد من سرعة الهجمات ودقتها، وأن توسع نطاق

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 5
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

التصيد الإلكتروني، والتضليل، وتحليل الثغرات. ومن جهة أخرى، تتيح للدول قدرات دفاعية متقدمة في رصد الأنماط غير الطبيعية، وتحليل التهديدات، والاستجابة الآلية. وبذلك سيصبح التفوق في توظيف الذكاء الاصطناعي عاملاً مهماً في تحديد ميزان الردع السيبراني مستقبلاً[٤٨].

وسوف يتعزز الاتجاه نحو التعاون الإقليمي، لاسيما بين دول الخليج، بعد الحرب الاخيرة بين ايران والكيان الصهيوني في مجالات تبادل معلومات التهديدات، وتنسيق الاستجابة للحوادث، وتوحيد معايير حماية البنية التحتية الحيوية. فالطبيعة العابرة للحدود للهجمات السيبرانية تجعل الردع الوطني المنفرد غير كافٍ. لذلك، فإن بناء منظومات إقليمية للإنذار المبكر والاستجابة المشتركة قد يشكل أحد أهم مسارات الردع السيبراني في المستقبل[٤٩].

من جهة اخرى، ستبرز الدبلوماسية السيبرانية كأداة مكملة للردع. فمع تزايد احتمالات سوء الفهم والتصعيد غير المقصود، ستحتاج دول الشرق الأوسط إلى الانخراط في وضع قواعد سلوك وضوابط تمنع استهداف الخدمات المدنية الأساسية. وقد لا تؤدي هذه القواعد إلى إنهاء الصراع السيبراني، لكنها قد تساعد في ضبطه وتقليل مخاطره، خاصة في الأزمات السياسية والعسكرية الحادة[٥٠].

بناءً على ذلك، يمكن القول إن مستقبل الردع السيبراني في الشرق الأوسط سيتجه نحو نموذج مركب، لا يعتمد على عنصر واحد، بل يجمع بين القدرة الدفاعية، والمرونة التشغيلية، والإسناد الفني، والضغط السياسي، والتعاون الإقليمي. وستكون الدول الأكثر قدرة على دمج هذه العناصر هي الأكثر امتلاكاً لردع سيبراني فعال.

الخاتمة والاستنتاجات

أن الفضاء السيبراني أصبح مجالاً مركزياً في إدارة الصراع الإقليمي، لا يقل أهمية عن المجالات العسكرية والاستخبارية والسياسية. فالردع السيبراني لم يعد يقوم على منع الهجوم بصورة مطلقة، بل على تقليل فاعليته، ورفع كلفته، والحد من قدرة الخصم على تحقيق مكاسب استراتيجية من خلاله. وتكشف حالة إيران والكيان الصهيوني أن الردع السيبراني يتخذ طابعاً غير متماثل؛ إذ توظف إيران قدراتها السيبرانية لتعويض اختلال ميزان القوة التقليدي، عبر عمليات الاختراق، والتسريب، والتأثير النفسي، واستخدام الفاعلين غير المباشرين. في المقابل، يعتمد الكيان الصهيوني على تفوق تقني ومؤسسي، يقوم على الدمج بين القدرات الدفاعية والهجومية، وتوظيف التكنولوجيا والاستخبارات في تعزيز أمنه السيبراني.

ومع ذلك، فإن فاعلية الردع السيبراني تبقى نسبية ومحدودة، بسبب صعوبة تحديد مصدر الهجمات، وتعدد الفاعلين، وإمكانية الإنكار، وضعف القواعد القانونية الدولية المنظمة لهذا

المجال. لذلك فإن الردع السيبراني في هذه الحالة لا يؤدي إلى إنهاء الصراع أو منع الهجمات، بل يسهم في ضبط مستويات التصعيد وإدارة الصراع ضمن حدود محسوبة.

ومن هنا، يمكن القول إن الردع السيبراني في الشرق الأوسط يمثل أداة استراتيجية فعالة جزئياً، لكنه غير حاسم بذاته. فنجاحه يتوقف على قدرة الدولة على الجمع بين الدفاع المتقدم، والردع الهجومي، والمرونة المؤسسية، وسرعة التعافي، فضلاً عن وضوح العقيدة السيبرانية وقدرتها على التكيف مع طبيعة التهديدات المتغيرة. ومن هنا يمكن اضافة العديد من الاستنتاجات التي توصلنا اليها وهي:

١–إن الردع السيبراني في الشرق الأوسط يعكس تحولاً في طبيعة الصراع، من المواجهة العسكرية المباشرة إلى صراع مركب يعتمد على التكنولوجيا والمعلومات والضغط غير المباشر.

٢– لا تتحقق فاعلية الردع السيبراني من خلال امتلاك القدرة الهجومية فقط، بل من خلال منظومة متكاملة تشمل الوقاية، والكشف، والاستجابة، والتعافي، والرد المتناسب.

٣–إن أبرز تحديات الردع السيبراني تتمثل في صعوبة الإسناد، وتعدد الفاعلين، واستخدام الوكلاء، وضعف الضوابط القانونية، وهو ما يجعل الردع أقل يقيناً من الردع التقليدي.

٤– أن الردع السيبراني بين إيران والكيان الصهيوني ردع نسبي وغير مستقر، ينجح في إدارة التصعيد أكثر مما ينجح في منعه، ويظل مرتبطاً بتطور التكنولوجيا وطبيعة الصراع السياسي والأمني في المنطقة.

الهوامش

[١] – حسين قوادرة، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للامن والتنمية، العدد٩، ٢٠٢٠، ص٥١٩.

[٢] – رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، برلين،العدد١، ٢٠١٧، ص٤٩.

[3] - MartinC.Libicki, cyberdeterrence and cyberwar, RAND Corporation, 2009, p239.

[٤] – علاء الدين فرحات، من الردع النووي الى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، مجلد ١٦، عدد١، ٢٠٢١، ص٢٦٤.

[5]- Stefan Soesanto and Max Smeets, cybar deterrence:the past,present,and future,in NL ARMS Netherlands Annual Review of Military studies2020, Asser press, 2021, p387.

[٦] – ايهاب خليفة، القوة الالكترونية وابعاد التحول في خصائص القوة، مكتبة الاسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٤، ص٢٣.

[٧] – عبد الغفار الدويك، استراتيجية الردع السيبراني.. التجربة الامريكية، مجلة السياسة الدولية، القاهرة، المجلد٥٣، العدد٢١٣، ٢٠١٨، ص١٩٦.

[8]- STEFAN SOESANTO, Cybar Deterrence Revisited, Air University press,2022, p4.

[٩] – علي حسن هويدي، تحديات الامن السيبراني في الاستراتيجية الامنية الصينية، مجلة حمورابي للدراسات، بغداد، العدد٥٦، ٢٠٢٥، ص١٨٢.

[10] - Joseph S. Nye, Deterrence and Dissuasion in cyberspace, International security,vol.41, 2017, p45.

[١١] – ايهاب خليفة، الامن السيبراني: الماهية والاشكاليات، سلسلة اوراق مصرية، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠١٩، ص٦.

[١٢] – عبد القادر بوغازي، الردع السيبراني: مقاربة لطبيعة الفواعل وقيود القانون الدولي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد١٠، العدد١، ٢٠٢٥، ص٨٦٠.

[13] - Thomas Rid, cyber war will not take place, oxford University press, 2013, p165.

[١٤] – علي زياد العلي، الصراع والامن الجيوسبراني في السياسة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، دار امجد للنشر والتوزيع، عمان، ٢٠٢٠، ص٩٩.

[١٥] – صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير غي منشورة، جامعة الشرق الاوسط، كلية الاداب والعلوم، قسم العلوم السياسية، عمان، ٢٠٢١، ص٤٢.

[16] - Jon R. Lindsay, Tipping the scales: the Attribution problem and the feasibility of deterrence against cyberattack, journal of cybersecurity, vol.1, 2015,p55.

[١٧] – شيماء معروف فرحات، التحول في مفهوم القوة والصراع: دراسة في الحروب السيبرانية، مجلة قضايا سياسية، جامعة النهرين، بغداد، العدد٧٥، ٢٠٢٣، ص٥٠٤.

[١٨] – محمد منذر جلال، سرى غضبان، تكنولوجيا الحروب السيبرانية واستراتيجية المواجهة الدولية، دار ومكتبة عدنان، بغداد، ط١، ٢٠٢١، ص١٧٠.

[١٩] – تقى اياد خليل القيسي، حروب الجيل السادس واستراتيجية المواجهة: السيبرانية نموذجاً، مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، بغداد، العدد٢٧، ٢٠٢٥، ص٤٠٥.

[٢٠] – منى الاشقر جبور، السيبرانية: هاجس العصر، المركز العربي للبحوث، جامعة الدول العربية، القاهرة، ط١، ٢٠١٨، ص٣٠.

[٢١] – انيس عبد الوهاب ابن احسن، القوة السيبرانية الايرانية واثرها على الاستقرار الاقليمي، مجلة السياسة العالمية، جامعة الجزائر، المجلد٦، العدد٢، ٢٠٢٢، ص٧٣٥.

[22] - Chuck Freilich, The Iranian cyber threat, Memorandum no.230, institute for national security studies, 2024, p10.

[٢٣] – كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مجلة حمورابي للدراسات، بغداد، العدد٤٠، ٢٠٢١، ص٢١٣.

[24]- Collin Anderson, Karim Sadjadpour, Irans cyber theat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International peace, 2018, pp35-36.

[٢٥] – هبه عبد السلام خطاب، مثنى فائق مرعي، مؤسسات الفضاء السيبراني في منطقة الشرق الاوسط: ايران واسرائيل نموذجا، مجلة تكريت للعلوم السياسية، العدد٣٠، ٢٠٢٢، ص٣٦٥.

[26] - Gabi Siboni, at al, Israel and the cyber threat: How the startup nation Became a global cyber power, oxford University press, 2023,p365.

[27]- Mehmet Emin Erendor, The cyber security strategy of Israel, Zhurnal voprosy istoril, vol11, 2021, p238.

[28]- Gil Baram, Israeli defense in the age of cyber war, Middle East Quarterly, at: https://www.researchgate.net/publication/316960053_Israeli_defense_in_the_age_of_cyber_war .

[29]- ISRAEL NATIONAL CYBER SECURITY STRATEGY2025, at: https://www.gov.il/en/pages/cyber_strategy_2025 .

[٣٠]– السلاح السيبراني في حروب اسرائيل المستقبلية: دراسات لباحثين اسرائيليين كبار، اعداد: رندة حيدر، مؤسسة الدراسات الفلسطينية، بيروت، ٢٠١٨، ص١٠٣.

[31] - Lior Tabansky, Isaac Ben Israel, cybersecurity in Israel, springerbriefs in cybersecurity, springer cham, 2015,p52.

[32]- Eviatar Matania, at al, Structuring the national cyber defence: in evolution towards a central cyber authority, journal of cyber policy, vol2, 2017, pp17-18.

[33]- Matthew S. Cohen, at el, Israel and cyberspace: Unique Threat and Response, International studies perspectives, vol17, 2016,p310.

[34] - Gawdat Bahgat, Anoushiravan Ehteshami, Irans Defense strategy The Navy:Ballistic Missiles and cyberspace, Middli East policy, vol24, 2017, p105.

[٣٥] – عبد العزيز محمود عبد العزيز، الحرب السيبرانية والاداء الاستراتيجي الفعال: دراسة حالة في الهجمات السيبرانية بين ايران واسرائيل، مركز المبادرة الاستراتيجية فلسطين – ماليزيا، فلسطين، العدد٢، ٢٠٢٣، ص٢٠.

[٣٦] – عفيف حيدر، واخرون، حرب الفضاء السيبراني في الاستراتيجية الايرانية، مجلة مدارات ايرانية، المركز الديمقراطي العربي، برلين، المجلد٦، العدد١٩، ٢٠٢٣، ص–ص٥٦–٥٨.

[37]- Kristina Kausck, Cheap Havoc: How cyber- Geopolitics will Destabilize the Middle East, The German Marshall fund of the United States, policy Brief, 2017, p9.

[38] - Ahmed bin Ali Al-Maymouni, The Active front: Consequences of cyberwarfare Between Iran and Israel, Journal for Iranian studies, 2020, p76.

[٣٩] – مجموعة مؤلفين، الحروب السيبرانية في الشرق الاوسط والعالم، تحرير: رغدة البهي، المركز المصري للفكر والدراسات الاستراتيجية، ٢٠٢٥، ص٩٢.

[40]- Gawdet Dahgt, Iranian- Israeli confrontation: the cyber Domain, Middle East policy, vol27, 2020,p120.

[٤١]– احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران واسرائيل، مجلة الدراسات الايرانية، العدد١٢، ٢٠٢٠، ص٨١.

[42] - Veronika Netolicka, Miroslav Mares, Arms Race in cyberspace:A case study of Iran and Israel, comparative strategy, vol37, 2019, p420.

[43]- Sam Cohen, Iranian cyber capabilities: Assessing the threat to Israeli financial and security Interests, cyber Intelligence and security, vol 3, 2019, p82.

[٤٤] – احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران واسرائيل، مصدر سبق ذكره، ص٨٠.

[٤٥] – كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجيات الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مصدر سبق ذكره، ص١٩٥.

[46]- Jams Shires, the politics of cybersecurity in the Middle East, Oxford University press, 2022, p101.

[٤٧] – محمد معن محسن، مستقبل مكانة القوة السيبرانية في استراتيجيات القوى الاقليمية: ايران نموذجا، مجلة قضايا سياسية، جامعة النهرين، بغداد، العدد٨١، ٢٠٢٥، ص١٤٠.

[٤٨] – سيماء علي مهدي، دور الامن السيبراني في استقرار الدولة، مجلة السياسة الدولية، العدد٦٤، ٢٠٢٥، ص٣٩١.

[٤٩] – محمد معن محسن، المصدر السابق، ص١٥٠.

[٥٠] – خالد الجابر، ديناميكيات مابعد الحرب: الخليج في قلب نظام عالمي جديد، مجلس الشرق الاوسط للشؤون الدولية، ٢٠٢٦، متوافر على الرابط:https://mecouncil.org/ar/publication/

قائمة المصادر

المصادر العربية

١–حسين قوادرة، الردع السيبراني بين النظرية والتطبيق، المجلة الجزائرية للامن والتنمية، العدد٩، ٢٠٢٠، ص٥١٩.

٢–رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، برلين،العدد١، ٢٠١٧، ص٤٩.

٣– علاء الدين فرحات، من الردع النووي الى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، مجلد ١٦، عدد١، ٢٠٢١، ص٢٦٤.

٤–ايهاب خليفة، القوة الالكترونية وابعاد التحول في خصائص القوة، مكتبة الاسكندرية، وحدة الدراسات المستقبلية، مصر، ٢٠١٤، ص٢٣.

٥-عبد الغفار الدويك، استراتيجية الردع السيبراني.. التجربة الامريكية، مجلة السياسة الدولية، القاهرة، المجلد٥٣، العدد٢١٣، ٢٠١٨، ص١٩٦.

٦-علي حسن هويدي، تحديات الامن السيبراني في الاستراتيجية الامنية الصينية، مجلة حمورابي للدراسات، بغداد، العدد٥٦، ٢٠٢٥، ص١٨٢.

٧-ايهاب خليفة، الامن السيبراني: الماهية والاشكاليات، سلسلة اوراق مصرية، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠١٩، ص٦.

٨- عبد القادر بوغازي، الردع السيبراني: مقاربة لطبيعة الفواعل وقيود القانون الدولي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد١٠، العدد١، ٢٠٢٥، ص٨٦٠.

٩-علي زياد العلي، الصراع والامن الجيوسبراني في السياسة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، دار امجد للنشر والتوزيع، عمان، ٢٠٢٠، ص٩٩.

١٠- صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير غي منشورة، جامعة الشرق الاوسط، كلية الاداب والعلوم، قسم العلوم السياسية، عمان، ٢٠٢١، ص٤٢.

١١-شيماء معروف فرحات، التحول في مفهوم القوة والصراع: دراسة في الحروب السيبرانية، مجلة قضايا سياسية، جامعة النهرين، بغداد، العدد٧٥، ٢٠٢٣، ص٥٠٤.

١٢-محمد منذر جلال، سرى غضبان، تكنولوجيا الحروب السيبرانية واستراتيجية المواجهة الدولية، دار ومكتبة عدنان، بغداد، ط١، ٢٠٢١، ص١٧٠.

١٣- تقى اياد خليل القيسي، حروب الجيل السادس واستراتيجية المواجهة: السيبرانية نموذجاً، مجلة كلية القانون والعلوم السياسية، الجامعة العراقية، بغداد، العدد٢٧، ٢٠٢٥، ص٤٠٥.

١٤-منى الاشقر جبور، السيبرانية: هاجس العصر، المركز العربي للبحوث، جامعة الدول العربية، القاهرة، ط١، ٢٠١٨، ص٣٠.

١٥-انيس عبد الوهاب ابن احسن، القوة السيبرانية الايرانية واثرها على الاستقرار الاقليمي، مجلة السياسة العالمية، جامعة الجزائر، المجلد٦، العدد٢، ٢٠٢٢، ص٧٣٥.

١٦-كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مجلة حمورابي للدراسات، بغداد، العدد٤٠، ٢٠٢١، ص٢١٣.

١٧–هبه عبد السلام خطاب، مثنى فائق مرعي، مؤسسات الفضاء السيبراني في منطقة الشرق الاوسط: ايران واسرائيل نموذجا، مجلة تكريت للعلوم السياسية، العدد٣٠، ٢٠٢٢، ص٣٦٥.

١٨–السلاح السيبراني في حروب اسرائيل المستقبلية: دراسات لباحثين اسرائيليين كبار، اعداد: رندة حيدر، مؤسسة الدراسات الفلسطينية، بيروت، ٢٠١٨، ص١٠٣.

١٩–عبد العزيز محمود عبد العزيز، الحرب السيبرانية والاداء الاستراتيجي الفعال: دراسة حالة في الهجمات السيبرانية بين ايران واسرائيل، مركز المبادرة الاستراتيجية فلسطين – ماليزيا، فلسطين، العدد٢، ٢٠٢٣، ص٢٠.

٢٠–عفيف حيدر، واخرون، حرب الفضاء السيبراني في الاستراتيجية الايرانية، مجلة مدارات ايرانية، المركز الديمقراطي العربي، برلين، المجلد٦، العدد١٩، ٢٠٢٣، ص–ص٥٦–٥٨.

٢١–مجموعة مؤلفين، الحروب السيبرانية في الشرق الاوسط والعالم، تحرير: رغدة البهي، المركز المصري للفكر والدراسات الاستراتيجية، ٢٠٢٥، ص٩٢.

٢٢–احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران واسرائيل، مجلة الدراسات الايرانية، العدد١٢، ٢٠٢٠، ص٨١.

٢٣–احمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران واسرائيل، مصدر سبق ذكره، ص٨٠.

٢٤–محمد معن محسن، مستقبل مكانة القوة السيبرانية في استراتيجيات القوى الاقليمية: ايران نموذجا، مجلة قضايا سياسية، جامعة النهرين، بغداد، العدد٨١، ٢٠٢٥، ص١٤٠.

٢٥– سيماء علي مهدي، دور الامن السيبراني في استقرار الدولة، مجلة السياسة الدولية، العدد٦٤، ٢٠٢٥، ص٣٩١.

٢٦– خالد الجابر، ديناميكيات مابعد الحرب: الخليج في قلب نظام عالمي جديد، مجلس الشرق الاوسط للشؤون الدولية، ٢٠٢٦، متوافر على الرابط: https://mecouncil.org/ar/publication/

المصادر الاجنبية

1–MartinC.Libicki, cyberdeterrence and cyberwar, RAND Corporation, 2009, p 239.

2–Stefan Soesanto and Max Smeets, cybar deterrence:the past,present,and future,in NL ARMS Netherlands Annual Review of Military studies2020, Asser press, 2021, p387.

3– STEFAN SOESANTO, Cybar Deterrence Revisited, Air University press,2022, p4 .

4- Joseph S. Nye, Deterrence and Dissuasion in cyberspace, International security,vol.41, 2017, p45.

5- Thomas Rid, cyber war will not take place, oxford University press, 2013, p165.

6- Jon R. Lindsay, Tipping the scales: the Attribution problem and the feasibility of deterrence against cyberattack, journal of cybersecurity, vol.1, 2015,p55.

7- Chuck Freilich, The Iranian cyber threat, Memorandum no.230, institute for national security studies, 2024, p10.

8- Collin Anderson, Karim Sadjadpour, Irans cyber theat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International peace, 2018, pp35-36.

9- Gabi Siboni, at al, Israel and the cyber threat: How the startup nation Became a global cyber power, oxford University press, 2023,p365.

10-Mehmet Emin Erendor, The cyber security strategy of Israel, Zhurnal voprosy istoril, vol11, 2021, p238.

11- Gil Baram, Israeli defense in the age of cyber war, Middle East Quarterly, at: https://www.researchgate.net/publication/316960053_Israeli_defense_in_the_age_of_cyber_war.

12-- ISRAEL NATIONAL CYBER SECURITY STRATEGY2025, at: https://www.gov.il/en/pages/cyber_strategy_2025.

13- Lior Tabansky, Isaac Ben Israel, cybersecurity in Israel, springerbriefs in cybersecurity, springer cham, 2015,p52.

14- Eviatar Matania, at al, Structuring the national cyber defence: in evolution towards a central cyber authority, journal of cyber policy, vol2, 2017, pp17-18.

15- Matthew S. Cohen, at el, Israel and cyberspace: Unique Threat and Response, International studies perspectives, vol17, 2016,p310.

16- Gawdat Bahgat, Anoushiravan Ehteshami, Irans Defense strategy The Navy:Ballistic Missiles and cyberspace, Middli East policy, vol24, 2017, p105.

17- Kristina Kausck, Cheap Havoc: How cyber- Geopolitics will Destabilize the Middle East, The German Marshall fund of the United States, policy Brief, 2017,p9.

18- Ahmed bin Ali Al-Maymouni, The Active front: Consequences of cyberwarfare Between Iran and Israel, Journal for Iranian studies, 2020,p76.

19- Gawdet Dahgt, Iranian- Israeli confrontation: the cyber Domain, Middle East policy, vol27, 2020,p120.

20- Veronika Netolicka, Miroslav Mares, Arms Race in cyberspace:A case study of Iran and Israel, comparative strategy, vol37, 2019, p420.

21- Sam Cohen, Iranian cyber capabilities: Assessing the threat to Israeli financial and security Interests, cyber Intelligence and security, vol 3, 2019,p82.
22- Jams Shires, the politics of cybersecurity in the Middle East, Oxford University press, 2022,p101.

List of Sources

Arabic Sources

1- Hussein Qawadra, Cyber Deterrence: Between Theory and Practice, Algerian Journal of Security and Development, Issue 9, 2020, p. 519.

2- Ragda Al-Bahy, Cyber Deterrence: Concept, Problems, and Requirements, Journal of Political Science and Law, Arab Democratic Center, Berlin, Issue 1, 2017, p. 49.
3- Alaa El-Din Farhat, From Nuclear Deterrence to Cyber Deterrence: A Study of the Extent of Achieving the Principle of Deterrence in Cyberspace, Al-Mufakker Journal, Faculty of Law and Political Science, Mohamed Khider University of Biskra, Algeria, Volume 16, Issue 1, 2021, p. 264.
4- Ihab Khalifa, Electronic Power and the Dimensions of the Transformation in Power Characteristics, Bibliotheca Alexandrina, Future Studies Unit, Egypt, 2014, p. 23.
5. Abdul Ghaffar Al-Duwaik, "Cyber Deterrence Strategy: The American Experience," International Politics Journal, Cairo, Vol. 53, No. 213, 2018, p. 196.
6. Ali Hassan Huwaidi, "Cybersecurity Challenges in the Chinese Security Strategy," Hammurabi Journal of Studies, Baghdad, No. 56, 2025, p. 182.
7. Ihab Khalifa, "Cybersecurity: Its Nature and Problems," Egyptian Papers Series, Al-Ahram Center for Political and Strategic Studies, Cairo, 2019, p. 6.
8. Abdul Qader Bughazi, "Cyber Deterrence: An Approach to the Nature of Actors and the Constraints of International Law," Algerian Journal of Law and Political Science, Vol. 10, No. 1, 2025, p. 860.
9. Ali Ziad Al-Ali, "Conflict and Geocyber Security in International Politics: A Study in Digital Engagement Strategies," Amjad Publishing and Distribution House, Amman, 2020, p. 99.
10- Salah Haider Abdul Wahid, Cyber Warfare: A Study of its Concept, Characteristics, and Countermeasures, Unpublished Master's Thesis, Middle East University, Faculty of Arts and Sciences, Department of Political Science, Amman, 2021, p. 42.

11- Shaimaa Marouf Farhat, The Transformation in the Concept of Power and Conflict: A Study in Cyber Warfare, Political Issues Journal, Al-Nahrain University, Baghdad, Issue 75, 2023, p. 504.

12- Muhammad Munther Jalal and Sara Ghadhban, Cyber Warfare Technology and the Strategy of International Confrontation, Adnan Publishing House and Library, Baghdad, 1st Edition, 2021, p. 170.

13- Tuqa Ayad Khalil Al-Qaisi, Sixth-Generation Warfare and the Strategy of Confrontation: Cyber Warfare as a Model, Journal of the College of Law and Political Science, Iraqi University, Baghdad, Issue 27, 2025, p. 405.

14- Mona Al-Ashqar Jabour, Cybersecurity: The Obsession of Our Time, Arab Center for Research, League of Arab States, Cairo, 1st ed., 2018, p. 30.

15- Anis Abdel Wahab Ibn Ahsan, Iranian Cyber Power and Its Impact on Regional Stability, Journal of World Politics, University of Algiers, Vol. 6, No. 2, 2022, p. 735.

16- Karrar Abbas Mutab, Cyber Warfare: A Study of Cyber Attack Strategies Between the United States and Iran, Hammurabi Journal of Studies, Baghdad, No. 40, 2021, p. 213.

17- Heba Abdel Salam Khattab and Muthanna Faiq Marai, Cyberspace Institutions in the Middle East: Iran and Israel as Case Studies, Tikrit Journal of Political Science, No. 30, 2022, p. 365.

18. Cyber Warfare in Israel's Future Wars: Studies by Leading Israeli Researchers, edited by Randa Haidar, Institute for Palestine Studies, Beirut, 2018, p. 103.

19. Abdul Aziz Mahmoud Abdul Aziz, Cyber Warfare and Effective Strategic Performance: A Case Study of Cyber Attacks between Iran and Israel, Palestine-Malaysia Strategic Initiative Center, Palestine, Issue 2, 2023, p. 20.

20. Afif Haidar et al., Cyber Warfare in Iranian Strategy, Iranian Perspectives Journal, Arab Democratic Center, Berlin, Volume 6, Issue 19, 2023, pp. 56-58.

21. A group of authors, Cyber Wars in the Middle East and the World, edited by Ragda El-Bahy, Egyptian Center for Thought and Strategic Studies, 2025, p. 92.

22- Ahmed bin Ali Al-Maimouni, The Active Front: The Repercussions of the Cyber Confrontation between Iran and Israel, Journal of Iranian Studies, Issue 12, 2020, p. 81.

23- Ahmed bin Ali Al-Maimouni, The Active Front: The Repercussions of the Cyber Confrontation between Iran and Israel, previously cited source, p. 80.

24- Muhammad Maan Mohsen, The Future of Cyber Power's Position in the Strategies of Regional Powers: Iran as a Model, Political Issues Journal, Al-Nahrain University, Baghdad, Issue 81, 2025, p. 140.

25- Sima Ali Mahdi, The Role of Cybersecurity in State Stability, International Politics Journal, Issue 64, 2025, p. 391.

26- Khaled Al-Jaber, Post-War Dynamics: The Gulf at the Heart of a New World Order, Middle East Council on International Affairs, 2026, available at: https://mecouncil.org/ar/publication/

Foreign Sources

1−MartinC.Libicki, cyberdeterrence and cyberwar, RAND Corporation, 2009, p 239.

2−Stefan Soesanto and Max Smeets, cybar deterrence:the past,present,and future,in NL ARMS Netherlands Annual Review of Military studies2020, Asser press, 2021, p387.

3− STEFAN SOESANTO, Cybar Deterrence Revisited, Air University press,2022, p4 .

4− Joseph S. Nye, Deterrence and Dissuasion in cyberspace, International security,vol.41, 2017, p45.

5− Thomas Rid, cyber war will not take place, oxford University press, 2013, p165.

6− Jon R. Lindsay, Tipping the scales: the Attribution problem and the feasibility of deterrence against cyberattack, journal of cybersecurity, vol.1, 2015,p55.

7− Chuck Freilich, The Iranian cyber threat, Memorandum no.230, institute for national security studies, 2024, p10.

8− Collin Anderson, Karim Sadjadpour, Irans cyber theat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International peace, 2018, pp35-36.

9− Gabi Siboni, at al, Israel and the cyber threat: How the startup nation Became a global cyber power, oxford University press, 2023,p365.

10−Mehmet Emin Erendor, The cyber security strategy of Israel, Zhurnal voprosy istoril, vol11, 2021, p238.

11− Gil Baram, Israeli defense in the age of cyber war, Middle East Quarterly, at: https://www.researchgate.net/publication/316960053_Israeli_defense_in_the_age_of_cyber_war.

12-- ISRAEL NATIONAL CYBER SECURITY STRATEGY2025, at: https://www.gov.il/en/pages/cyber_strategy_2025.

13- Lior Tabansky, Isaac Ben Israel, cybersecurity in Israel, springerbriefs in cybersecurity, springer cham, 2015,p52.

14- Eviatar Matania, at al, Structuring the national cyber defence: in evolution towards a central cyber authority, journal of cyber policy, vol2, 2017, pp17-18.

15- Matthew S. Cohen, at el, Israel and cyberspace: Unique Threat and Response, International studies perspectives, vol17, 2016,p310.

16- Gawdat Bahgat, Anoushiravan Ehteshami, Irans Defense strategy The Navy:Ballistic Missiles and cyberspace, Middli East policy, vol24, 2017, p105.

17- Kristina Kausck, Cheap Havoc: How cyber- Geopolitics will Destabilize the Middle East, The German Marshall fund of the United States, policy Brief, 2017,p9.

18- Ahmed bin Ali Al-Maymouni, The Active front: Consequences of cyberwarfare Between Iran and Israel, Journal for Iranian studies, 2020,p76.

19- Gawdet Dahgt, Iranian- Israeli confrontation: the cyber Domain, Middle East policy, vol27, 2020,p120.

20- Veronika Netolicka, Miroslav Mares, Arms Race in cyberspace:A case study of Iran and Israel, comparative strategy, vol37, 2019, p420.

21- Sam Cohen, Iranian cyber capabilities: Assessing the threat to Israeli financial and security Interests, cyber Intelligence and security, vol 3, 2019,p82.

22- Jams Shires, the politics of cybersecurity in the Middle East, Oxford University press, 2022,p101.