دراسة

أثر الحرب السيبرانية الإسرائيلية-الإيرانية على الأمن الإقليمي

ليلى الدوسري
مساعدة باحث

RASANAH
المعهد الدولي للدراسات الإيرانية
International Institute for Iranian Studies

المحتويـــات

المقدمة:

أصبحت الحرب السيبرانية واحدةً من أخطر أدوات الصراع بين الدول والجهات الفاعلة غير الحكومية في القرن الحادي والعشرين، حيث تعتمد هذه الحرب على الهجمات الإلكترونية التي تستهدف شبكات الدول، وبنيتها التحتية، وبياناتها الحيوية، بهدف التجسس والتخريب وتعطيل الخدمات، أو التأثير في الرأي العامّ والاقتصاد. وتُستخدم بوعيٍ بالغ لإعادة تشكيل قواعد الاشتباك الإقليمي، من دون اللجوء إلى الحرب التقليديةّ. ولَم يَعُد الهدف فقط تجميع المعلومات أو استنزاف موارد الخصم، بل التأثير في القدرة على الدولة ذاتها في لحظات الأزمات، ما يعني أن السيبرانية أصبحت أداة لـ«تعطيل الدولة» وليس فقط إرباكها. وتُعَدّ الحرب السيبرانية بين إسرائيل وإيران واحدًا من أكثر الصراعات الرقمية تعقيدًا وامتدادًا في الشرق الأوسط، وهذه الحرب ليست جديدة، بل تطوّرت خلال أكثر من 15 عامًا، ويُعَدّ هجوم Stuxnet نقطة فارقة في الحرب السيبرانية بين الطرفين. وعلى الرغم من الفارق النوعي في القدرات بين البلدين، فإنّ إيران استطاعت أن تعزز موقفها في موجهة إسرائيل، وهو ما حوَّل الصراع السيبراني بين إيران وإسرائيل إلى أحد نماذج التنافس الجيوسياسي. وفي هذه الدراسة سوف نتعرَّف هذا النموذج وتداعياته على الأمن القومي في القرن الحادي والعشرين.

وبناءً على ذلك، تناقش هذه الدراسة الصراع السيبراني الإسرائيلي-الإيراني وتأثيره في الأمن السيبراني لدول الإقليم، وآفاقه المستقبلية. وتطرح في هذا الإطار عددًا من الأسئلة، أبرزها: ما القدرات السيبرانية لكل من إيران وإسرائيل؟ وما تأثيرات الحرب السيبرانية في الطرفين الإيراني والإسرائيلي؟ وما تداعيات هذه الحرب على دول الإقليم؟ وما التوقعات المستقبلية للحرب السيبرانية الإيرانية-الإسرائيلية؟ وللإجابة عن هذه الأسئلة ستُناقَش عدة محاور، حيث سيكون المحور الأول هو القدرات السيبرانية في البنية الإستراتيجية الإسرائيلية-الإيرانية، أما المحور الثاني فسيتحدث عن طبيعة وتأثيرات الهجمات السيبرانية المتبادلة بين إيران وإسرائيل، ويأتي المحور الثالث حو تداعيات الحرب السيبرانية الإسرائيلية-الإيرانية على دول الإقليم، وأخيرًا المحور الرابع سوف يعرض الآفاق المستقبلية للحرب السيبرانية الإسرائيلية-الإيرانية.

أولًا: القدرات والأهداف السيبرانية في البنية الإستراتيجية الإسرائيلية والإيرانية

تطوّرت قدرات الحرب السيبرانية الإسرائيلية بشكل كبير منذ بزوغ العصر الرقمي، مما يجعل إسرائيل لاعبًا رئيسيًّا في مجال الحرب السيبرانية داخل الشرق الأوسط. وبالمقابل أسهم تعرُّض إيران لعديد من التهديدات الإلكترونية الداخلية والخارجية إلى تحولها نحو تدعيم قدراتها الإلكترونية الدفاعية والهجومية بقوة وكثافة غير مسبوقة. على هذا النحو يمكن تناول القدرات السيبرانية على الجانبين على النحو الآتي:

1. إسرائيل:

أصبحت قدرات الحرب السيبرانية الإسرائيلية عنصرًا أساسيًّا في ترسانة الدفاع الإستراتيجي الوطنية، وتعكس مزيجًا متطوّرًا من الابتكار التكنولوجي والإتقان التكتيكي. يأتي في مقدمة هذه القدرات القبة الإلكترونية، وهي مصممة لحماية البنية التحتية الوطنية الحيوية. وقد أعلنت تل أبيب عن هذه المنظومة للمرة الأولى عام 2022م للحد من تأثير الهجمات الإلكترونية واسعة النطاق باستخدام الذكاء الصناعي والبيانات الضخمة، ولتمكين الكشف عن التهديدات والتخفيف منها في الوقت الفعلي، والحفاظ على البنية التحتية الحيوية للبلاد آمنة من الهجمات الإلكترونية التي تشنها الدول المعادية والجهات المعادية على الإنترنت[1].

من جهة ثانية تأتي أنظمة استخبارات الإشارات (SIGINT)، التي تلعب دورًا حيويًّا في الدفاع السيبراني من خلال اعتراض وتحليل الإشارات الرقمية لجمع المعلومات الاستخباراتية. تم تصميم هذه الأنظمة لمراقبة وجمع المعلومات من قنوات الاتصال المختلفة، بما في ذلك حركة الراديو والأقمار الصناعية والإنترنت. من خلال التقاط الإشارات الرقمية، يمكن لأنظمة SIGINT اكتشاف التهديدات السيبرانية المحتملة، وتتبُّع الأنشطة الخبيثة، وتوفير رؤى قيِّمة حول عمليات العدوّ[2].

هذا بالإضافة إلى الشركات الناشئة المتخصصة، وتميُّز القطاع الخاص في إسرائيل بوصفها «أم الشركات الناشئة»، حيث تحتضن إسرائيل مئات الشركات المتخصصة في الأمن السيبراني، التي تقدم حلولًا عالمية للحماية من الهجمات الرقمية وإدارة الوصول إلى الحسابات الحساسة. من هذه الشركات تشك بوينت (Check Point Software Technologies Ltd) التي تُعَدّ من أبرز الشركات العاملة في مجال الأمان الإلكتروني. وهي شركة إسرائيلية تأسست عام 1993م، يقع مقرُّها الرئيسي في تل

(1) إندبندنت عربية، القبة الإلكترونية تعكس القدرات السيبرانية الدفاعية لإسرائيل، (18 سبتمبر 2024م)، تاريخ الاطلاع: 5 يناير 2026م، https://tinyurl.com/24ta8yal

(2) Startup Central, , , August 2024 ,11. Accessed January 2026 ,5. https://tinyurl.com/28t74z89

أبيب، ولها مكاتب في كاليفورنيا أيضًا. تشتهر الشركة بتطوير برامج وحلول أمنية لحماية الشبكات والمعلومات، وتُعتبر من أكبر الشركات الإسرائيلية في هذا المجال[1]. كذلك هناك شركة CyberArk، وتأسست في عام 1999م، وهي شركة متخصصة في الأمن السيبراني[2]، وتركز على تأمين الحسابات المميزة التي غالبًا ما تُستهدَف بهجمات إلكترونية[3].

وتأتي المديرية الوطنية للسيبران الإسرائيلية قدرة إضافية أخرى، وهي الوكالة الأمنية الوطنية والتكنولوجية المسؤولة عن الدفاع عن الفضاء السيبراني الوطني الإسرائيلي وعن تأسيس وتطوير القوة السيبرانية الإسرائيلية. تعمل المديرية على المستوى الوطني لتعزيز مستوى الدفاع المستمر عن المنظمات والمواطنين، ومنع والتعامل مع الهجمات الإلكترونية، وتعزيز قدرات الاستجابة للطوارئ[4].

كما أن لدى إسرائيل وحدة تُعرف باسم C4I والدفاع السيبراني، وتُعتبر الهيئة المركزية في جيش الاحتلال الإسرائيلي المسؤولة عن تخطيط الاتصالات، والنقل اللا سلكي، والحوسبة، والقيادة والتحكم، والدفاع عن المعلومات العسكرية والاستخباراتية، وقد أنشئت في 2003م[5].

هذا علاوة على برامج التعليم والتدريب في الدفاع السيبراني، التي تقام عبر برامج مخصصة للشباب بالتعاون مع وزارة الدفاع الإسرائيلية (IDF) ووزارة التعليم، برنامجان بعد المدرسة (Magshimim) لتشكيل واكتشاف المواهب السيبرانية، حيث يلتحق 75% من الطلاب في ما بعدُ بالوحدات السيبرانية والاستخبارات في الجيش[6].

واستكمالًا لهذه القدرات تبني إسرائيل علاقات تحالف إلكتروني مع شركات التكنولوجيا العملاقة، حيث يشير بعض التقارير الأمنية إلى أن إسرائيل أدركت من خلال الصراع المستمر أنها بحاجة إلى بناء علاقات تحالف إلكتروني مع شركات التكنولوجيا العملاقة، وهي بذلك تسعى إلى بناء علاقات إستراتيجية مع شركات «أمازون» و«مايكروسوفت» و«غوغل»[7]. وتهدف إلى تأمين الفضاء الإلكتروني،

---

(1) شهيرة بدري، رئيس شركة إسرائيلية: المستثمرون الأجانب يخشون الاستثمار في بلد غير مستقر، البوابة نيوز، (15 أغسطس 2024م)، تاريخ الاطلاع: 5 أبريل 2026م، https://tinyurl.com/25lbep6y

(2) أخبار أورورا إسرائيل، شركة أمن سيبراني إسرائيلية تستحوذ على شركة ناشئة أمريكية مقابل 175 مليون دولار، (15 فبراير 2025م)، تاريخ الاطلاع: 5 أبريل 2026م، https://tinyurl.com/2crghau3

(3) Startup Nation Central, Israel's Cyber Defense Capabilities, Ibid.

(4) Gov.il, About Gov.il, (21 February 2024), accessed Apr 21, 2026. https://tinyurl.com/2d9mdp8p

(5) الخنادق، مديرية تكنولوجيا المعلومات والاتصالات والدفاع السيبراني، (20 يونيو 2025م)، تاريخ الاطلاع: 10 يناير 2026م، https://tinyurl.com/2d7gqbxa

(6) Jasper Frei, Israel's National Cybersecurity and Cyberdefense Posture. CSS Cyberdefense Report. Zürich: Center for Security Studies (CSS), ETH Zürich, (September 2020), Accessed January 2, 2026. https://tinyurl.com/2ck6yycv

(7) سامي خليفة، القبة الإلكترونية تعكس القدرات السيبرانية الدفاعية لإسرائيل، (18 سبتمبر 2024م)، تاريخ الاطلاع: 1 يناير 2026م، https://tinyurl.com/279sq8fm

مستفيدةً من ارتباطها بعلاقات وثيقة مع أكثر من 20 دولة في مجال تبادل المعلومات اليومي.

استخدمت إسرائيل هذه القدرات لإظهار القوة لحماية الدولة جزئيًّا ولإبراز قوّتها في المنطقة، ويمكن تحديد ثلاثة أهداف هجومية إسرائيلية، الهدف الأول هو التجسس وجمع المعلومات الاستخباراتية، وفي هذا السياق برزت «الوحدة 8200» بمثابة منظومة استخباراتية تقنية، وهي الحاضنة لعشرات الشركات الناشئة المتخصصة في التجسس السيبراني والهجمات الإلكترونية. وتُعرف «الوحدة 8200» بكونها الذراع الاستخباراتية الإلكترونية الأهم في الجيش الإسرائيلي، وتشتهر بقدرتها على اعتراض الاتصالات وتحليل البيانات واختراق الشبكات وشن الهجمات السيبرانية[1].

وبرنامج «غرافيت» (Graphite) ليس مجرد أداة تجسس عادية، بل يمثل مستوى متقدمًا من التحكم السيبراني، فهو قادر على اختراق أي هاتف محمول، سواء يعمل بنظام «أندرويد» أو «آي أو إس»، والوصول الكامل إلى الرسائل والمحادثات داخل التطبيقات المشفرة[2]. وأُنشئت البرمجيات الخبيثة المتطوّرة Flame بشكل مشترك بين الولايات المتحدة وإسرائيل، وهي سلاح تجسس إلكتروني متطوّر ومعقَّد وغامض صُمِّم لجمع بيانات حساسة. اكتشفها باحثو الأمن نحو عام 2012، وتُعتبر من أكثر أشكال البرمجيات الخبيثة تهديدًا التي ظهرت في عالم السيبران[3]. كما جرى تطوير «دوكو»، وهو برنامج خبيث متقدم وسرِّي للغاية مصمم خصيصًا للتجسس الإلكتروني وسرقة البيانات[4].

والهدف الثاني يتمثل في التخريب الإلكتروني للبنية التحتية الحيوية، ويظهر من تصاعد حدة الحرب السيبرانية خلال الفترة الأخيرة، حيث إنّ القدرات السيبرانية الإسرائيلية مكّنتها من استهدف منشآت حسّاسة تشمل مواقع نووية وأهدافًا عسكرية ومدنية، بالإضافة إلى مجموعة من الاختراقات المالية كاستهداف البنوك وتعطيل واسع للخدمات[5]. وشهدت الساحة أيضًا هجومًا كبيرًا على إحدى كبرى

---

(1) أحمد عنتر، «من الوحدة 8200 إلى باراغون: كيفية صناعة التجسس السيبراني الإسرائيلي، الجزيرة، (20 يوليو 2025م)، تاريخ الاطلاع: 1 يناير 2026م، https://tinyurl.com/27uww842

(2) نسرين كارة، «في قرار مثير للجدل.. برنامج التجسس الإسرائيلي غرافيت بين يدي وكالة الهجرة الأميركية، ، (9 سبتمبر 2025م). تاريخ الاطلاع: 2 يناير 2026م، https://tinyurl.com/2bqd9f45

(3) Cyberpedia, ReasonLabs, What is Flame malware? The Massive and Sophisticated Flame Malware: An Advanced Cyber Attack Targeting Political Figures in the Middle East Accessed January 2, 2026. https://tinyurl.com/24pctcyx

(4) Duqu, VPN Unlimited Help – Cybersecurity Terms and Definitions, KeepSolid Inc. Accessed January 2, 2026. https://tinyurl.com/28f79hyq

(5) ديانا استيفانيا روبيو، «أدوات وجبهات الحرب السيبرانية بين إيران وإسرائيل، المجلة، (24 يونيو 2025م)، تاريخ الاطلاع: 2 مارس 2026م، https://tinyurl.com/2yux24c2

منصات تداول العملات الرقمية في إيران (نوبتكس)[1]. وفي حادثة أخرى، اختُرقت شبكات محطات الوقود، ما أدى إلى تعطيل خدماتها في طهران ومدن أخرى.

أما الهدف الأخير فهو تأجيج الرأي العام (الحرب السيبرانية النفسية/المعرفية)، إذ أصبحت الهجمات السيبرانية جزءًا من الحرب على الوعي بين الأطراف المتصارعة. التأثير لم يَعُد تقنيًّا فقط (تعطيل أنظمة أو بنى تحتية) بل تحوَّل إلى إستراتيجية إعلامية-نفسية تهدف إلى تأجيج الرأي العام، وإضعاف الثقة الداخلية بالحكومات، وخلق إحساس بعدم الأمان. تسلحت الدعاية الإسرائيلية وحلفاؤها ومؤيدوها بالأكاذيب والتلاعب بالمعلومات بوصفها سلاحًا إلى جانب عملياتها العسكرية على الأرض، وتعامل مدققو المعلومات مع أشكال جديدة من التلاعب الجماعي بالمعلومات خلال الحروب لم يسبق لهم التعامل معها، خصوصًا في ظل استخدام تقنيات الذكاء الصناعي في توليد المحتوى المضلل، الذي يصعب تفنيده بالأدلة القاطعة مقارنة بالادعاءات الأخرى[2]. وهناك أمثلة واضحة تبين قدرات إسرائيل السيبرانية في التأثير في الرأي العام للدولة المعادية مثل «العصفور المفترس»، وهي مجموعة قرصنة مؤيدة لإسرائيل ولديها ارتباطات محتملة مع الحكومة الإسرائيلية[3]، تتميز حملاتهم بتدمير البيانات المتعمد، والرسائل العامة الاستفزازية المصممة لتعظيم التأثير النفسي إلى جانب الاضطراب الجسدي[4].

2. إيران:

على نفس المنوال تشكل القدرات الدفاعية السيبرانية جزءًا أساسيًّا من إستراتيجية إيران الوطنية للأمن، حيث تسعى إلى حماية بنيتها التحتية الحيوية ومؤسساتها الحكومية وشبكاتها الرقمية من الهجمات الخارجية، في ظل بيئة إقليمية ودولية تشهد تصاعدًا مستمرًّا للتحديات السيبرانية.

ويأتي في مقدمة هذه القدرات قيادة الدفاع السيبراني، وقد تأسست في نوفمبر 2010م تحت إشراف منظمة الدفاع الوقائي، بغرض التعامل مع الحركات المحلية والدولية المنظمة وسوء استخدام منصة الإنترنت (ضد الجمهورية الإسلامية الإيرانية) وأنظمة الاتصال الأخرى لتنفيذ أعمال إرهابية والتجسس عبر الإنترنت وغسل

---

(1) A.J. Vicens, Iran Crypto Exchange Hit by Hackers, $90 Million Destroyed, Reuters, (June 18, 2025), Accessed January 2, 2026. https://tinyurl.com/2c8l3npn

(2) شيماء العيسائي، «ازدواجية التغطية الإعلامية الغربية لمعاناة النساء في العالم الإسلامي، معهد الجزيرة للإعلام، (19 نوفمبر 2024م)، تاريخ الاطلاع: 2 يناير 2026م، https://tinyurl.com/2btsvgjd

(3) Joe Tidy, Predatory Sparrow: Who are the hackers who say they started a fire in Iran?), BBC News, (11 July 2022, Accessed January 2, 2026, https://tinyurl.com/275mu9dt

(4) Tushar Subhra utta, Predatory Sparrow Group Attacking Critical Infrastructure to Destroy Data and Cause Disruption Cyber Security News, (January 11, 2026), Accessed January 2, 2026. https://tinyurl.com/23utwmbk

الأمـوال والهجمـات الثقافيـة[1]. وأُنشـئت المنظمـة الوطنيـة للدفـاع السـلبي لحمايـة البنيـة التحتيـة، وتتمثـل إحـدى المهـام الرئيسـية لمحلليهـا في «اسـتخدام جميـع المـوارد السـيبرانية الوطنيـة وغيرالسـيبرانية لـردع، ومنـع، وردّ، واكتشـاف، ومواجهـة أي هجـوم إلـكتروني مـن أي جهـة أجنبيـة معاديـة (دولـة أو مجموعـة) ضـد إيـران»[2].

ومـن جهـة ثانيـة، هنـاك برنامـج الإنترنـت المنعـزل، ويُعـتبرأحـد المشـروعات الإلكترونيـة الإيرانيـة الإسـتراتيجية التي بـدأت أوائـل عـام 2009م بهـدف تحويـل النشـاط الإلـكتروني بالدولـة إلى شـبكة اتصـالات داخليـة منعزلـة عـن الشـبكة العالميـة للإنترنـت، بمـا يُمكِّـن الحكومـة، مـن جهـة، مـن إحكام رقابتهـا وتعزيـز إشـرافها علـى محتـوى الشـبكة والبيانـات المتاحـة بهـا وتقويـض اسـتخدام شـبكة الإنترنـت العالميـة، وتطويـر عـدد مـن التكنولوجيـات الجديـدة، مـن بينهـا: تأسيـس نظـام تشـغيل آمِـن مُصمَّـم خصيصًـا لإنهـاء الاعتمـاد الإيـراني علـى نظـم التشـغيل الأمريكيـة.

هـذا بالإضافـة إلى تعزيـز إجراءاتهـا الدفاعيـة داخـل أجهزتهـا الحكوميـة، مـن خلال الاعتمـاد علـى الحـرس الثـوري في إجـراء عـدد مـن التدريبـات المُكثَّفـة للمدنـيين والعسـكريين علـى السـواء لمواجهـة مثـل تلـك الهجمـات في حـال حدوثهـا، كان آخرهـا في نهايـات عـام 2015م[3]. ويبـدو أن معظـم الأفـراد والجنـود المشـاركين في الهجـوم السـيبراني يمتلكـون خبرات وتخصصـات سـابقة في مجـالات مثـل الأمـن، والحاسـوب، والاتصـالات، والتخصصـات الحسـابية والفنيـة[4].

وإلى جانـب ذلـك هنـاك التعـاون الـدولي في مجـال الحـرب السـيبرانية، حيـث تمـت أول صفقـة تعـاون إلكترونيـة روسـية-إيرانية في عـام 2015م، قـال رئيـس منظمـة الدفـاع المـدني الإيرانيـة إنهـا ضروريـة لأن البلديـن يواجهـان أعـداء مشـتركين في الفضـاء الإلـكتروني. وفي عـام 2017م وقّعـت موسـكو وطهـران مذكـرة تفاهـم للتعـاون بشـأن القضايـا المتعلقـة بتكنولوجيـا المعلومـات والاتصـالات، بمـا في ذلك «حوكمـة الإنترنـت»، و«أمـن الشـبكة» و«الاتصـال الـدولي بالإنترنـت»، ومـن المرجـح أن تقـوم روسـيا بتزويـد طهـران بأنظمـة الدفـاع الإلـكتروني وتدريـب كوادرهـا، وليـس مـن المسـتبعد أن يضـم

(1) Ibid.

(2) سـایت وزارت امـور خارجـه ودیپلماسـی جمهـوری إسلامـی ایـران، توانایی‌هـای سـایبری ایـران؛ چگـونـه اسـت، تاریـخ الاطلاع: 11 مـارس 2026م www.irdiplomacy.ir.

(3) باسـم راشـد، «نمـو متصاعـد للقـدرات الإيرانيـة في مجـال الحـرب الإلكترونيـة»، المعهـد الدولي للدراسـات الإيرانيـة (رصانـة)، (20 أبريـل 2016م)، تاريـخ الاطلاع: 11 يناير 2026م، https://tinyurl.com/25efhx2u

(4) داود آذر، راهبردهـای قـدرت سـایبری ارتـش جمهـوری اسـالمی ایـران، دراسـات مسـتقبل دفـاع، تاریـخ الاطلاع: 11 ینایـر 2026م، https://tinyurl.com/23wpmhpn

اتفاق التعاون الإستراتيجي بين الصين وإيران في بعض بنوده ما يتعلق بالسيطرة على الفضاء الإلكتروني أيضًا[1].

وأخيرًا هناك الجيش السيبراني الإيراني، وهو المسؤول عن مهمة الهجوم في الفضاء السيبراني. يعمل تحت إشراف الحرس الثوري/قيادة القوات السيبرانية. بفضل القراصنة المحترفين والقدرات العالية في مجال تكنولوجيا المعلومات، يهاجم المعارضون قواعد الإعلام ومصالح الدول الغربية[2]. ويضم مجاميع من الميليشيات والفصائل الرقمية والقراصنة، ومتطوعين من مؤسسات أكاديمية وبحثية، تحت رئاسة الحرس الثوري الإيراني. وتشكَّل ما يُعرف بـ«جيش فضاء إيران الإلكتروني»، الذي تحوَّل إلى الذراع الرقمية للنظام الإيراني في استهداف الدول الأخرى وهز استقرارها.

ولم تغفل إيران إدماج الذكاء الصناعي في الأمن السيبراني الإيراني، إذ استثمرت إيران بشكل كبير في الذكاء الصناعي للأمن السيبراني في السنوات الأخيرة. بعض تطبيقات الذكاء الصناعي في هذا المجال يتمثل في:

- الكشف الآلي عن التهديدات: يمكن للأنظمة الذكاء الصناعي اكتشاف أنماط حركة المرور غير العادية على الشبكة والتنبؤ بالهجمات.
- زيادة دقة تحليل البرمجيات الخبيثة: استخدام التعلم الآلي لتحليل واكتشاف الهجمات المجهولة.
- الاستجابة الآلية للهجمات: يمكن لأنظمة الذكاء الصناعي توفير ردود فورية وآلية على الهجمات المعقدة.
- أنظمة EDR (الكشف والاستجابة لنقاط النهاية): للدفاع ضد البرمجيات الخبيثة والهجمات المستهدفة. EDR هو نظام أمني متقدم يراقب ويحلل سلوك المستخدمين والنظام باستمرار، ويكتشف ويحيد التهديدات في الوقت الحقيقي. تلعب أنظمة EDR دورًا في الدفاع السيبراني الإيراني، إذ تقوم أولًا باكتشاف هجمات متقدمة مثل البرمجيات الخبيثة المخفية (البرمجيات الخبيثة دون ملفات)، وثانيًا بتحليل مفصل لسلوك المستخدمين والأجهزة المتصلة بالشبكة، وثالثًا بالاتصال بأنظمة الذكاء الصناعي لاتخاذ قرارات تهديدية آلية، وأخيرًا القدرة على الاستجابة بسرعة وعزل الأنظمة المصابة[3].

---

(1) عزي، محمد فريد، «النشاط السيبراني الإيراني: ما بين السرية والعلن»، مركز ترينداز للبحوث والاستشارات، (5 ديسمبر 2021م)، تاريخ الاطلاع: 11 يناير 2026م، https://tinyurl.com/2ag7gb7g

(2) المرجع السابق.

(3) بهرامی، کتایون. «افشای برنامه حمله سایبری اسرائیل به ایران؛ راهکارهای دفاعی وتوانمندی‌های سایبری ایران». سلام دیجی (قسم تکنولوژی)، (19 اسفند 1403)، تاریخ الاطلاع: 11 يناير 2026م، hellodigi.ir

وهكذا يبدو أن إيران طوّرت قدرات هجومية سيبرانية متقدمة مكّنتها من تنفيذ عمليات اختراق وتعطيل تستهدف قطاعات حيوية لدى خصومها. وتُستخدم هذه القدرات كأداة إستراتيجية لتعزيز النفوذ والضغط السياسي ضمن إطار الصراع غير المباشر. وغاية إيران في المقام الأول من وراء هذا هي شن الحملات الإلكترونية الإيرانية، وفي هذا الإطار نفذت الجهات السيبرانية الإيرانية حملات كبيرة تهدف إلى إلحاق أضرار اقتصادية وتقويض الاستقرار السياسي، وزعزعة استقرار النظام المالي وانتهاك نظام الرقابة في عدد من البلدان[1].

وغاية إيران الثانية هي تنفيذ عمليات التسلل والاستخبارات في الشبكات والبنية التحتية، التي تشمل مجموعة من هجمات التسلل على شبكات حكومية، وأعمال تدميرية. تشمل مزيجًا من هجمات القرصنة وعمليات الدعاية والحرب النفسية، وتسريب البيانات المسروقة والتشويه من خلال استخدام الشبكات الاجتماعية ووسائل الإعلام، لخلق الخوف وانعدام الثقة بالدولة المستهدفة، كما تضع إيران وثائق مزيفة أو معدلة على مواقع مخترقة لتعزيز سردها الخاص، مثل نشر أخبار كاذبة عن الفساد في وسائل الإعلام المحلية المخترقة[2].

والغاية الأخيرة هي جمع المعلومات التكتيكية من خلال الاستطلاع السيبراني. وفي سياق ذلك تولى عملاء إيرانيون السيطرة على أنظمة كاميرات المراقبة المتصلة بالإنترنت في إسرائيل لاستخدامها لمعرفة ساحة المعركة، وتقييم الأضرار، وأهداف الصواريخ. مثل هذا الاستخدام للبنية التحتية المدنية لأغراض الاستخبارات والاستطلاع والمراقبة يُعَدّ نهجًا أكثر تطوّرًا للتجسس السيبراني التكتيكي، مما سمح لإيران بتعميق رؤيتها العملياتية دون استخدام أدوات الاستطلاع التقليدية في أراضي العدوّ[3]. وكجزء من جهود إيران للوصول إلى المعلومات الاستخباراتية، استُحدث في عام 2014م كيان إلكتروني مرتبط بالحرس الثوري الإسلامي، يُعرف باسم «فريق أياكس» أو «قطة الصواريخ»، لاستهداف كيانات وأفراد معينين بهدف جمع المعلومات الاستخباراتية وسرقة معلومات مهمة[4].

---

(1) Legal Clarity Team, Iran Hack Operations: Cyberattacks and Legal Consequences, Legal Clarity, (December 14, 2025), Accessed January 14, 2026. https://tinyurl.com/296gusec

(2) سرویس مشرق، «ارزیابی توان سایبری ایران در اندیشکده آمریکایی: ایران در حملات دیجیتال صبور است اما تردید نمی‌کند»، (28 شهریور 1404)، تاریخ الاطلاع: 11 يناير 2026م، www.mashreghnews.ir

(3) سجاد عابدي، «جنگ 12 روزه چه چیزی درباره تحول راهبرد سایبری ایران فاش کرد؟ رفتار سایبری تهران بازتابی از بلوغ فزاینده دکترینال آن اس، خبرآنلاین، (14 مرداد 1404)، تاریخ الاطلاع: 2 يناير 2026م، https://tinyurl.com/26mtwz9v

(4) أحمد علي الميموني، «جبهه فعال: پیامدهای رویارویی سایبری بین ایران واسرائیل» موسسه بین‌المللی مطالعات ایران (رصانة) – مرکز مطالعات وپژوهش‌ها، (25 مايو 2021م)، تاریخ الاطلاع: 22 يناير 2026م، https://tinyurl.com/2aykx5ql

ثانيًا: نتائج الهجمات السيبرانية المتبادلة بين إيران وإسرائيل

شهدت العلاقة بين إيران وإسرائيل تصاعدًا في النزاعات السيبرانية خلال السنوات الأخيرة، حيث أصبحت الهجمات الرقمية أداة إستراتيجية لكل طرف لتحقيق أهدافه دون اللجوء إلى الحرب التقليدية. تأثير هذه الحرب يمتد إلى الاقتصاد، والبنية التحتية، والأمن الوطني، والمجتمع المدني، مما يعكس أهمية الأمن السيبراني بوصفه عنصرًا حاسمًا في الصراع بين البلدين. ومن هذه التأثيرات:

1. العواقب والمكتسبات بالنسبة إلى إسرائيل:

تفرض الحرب السيبرانية عواقب عديدة على إسرائيل، لا سيَّما على الجانب الأمني والعسكري، بالنظر إلى اعتماد إسرائيل الكبير على التكنولوجيا العسكرية الحديثة والاقتصاد الرقمي، فإنها تواجه خطرًا أكبر من الهجمات السيبرانية مقارنةً بإيران التي تحدّ من انخراطها في الفضاء الرقمي العالمي بشكل مُفرط. هذا يجعل الجبهة السيبرانية تحديًا أمنيًّا متزايدًا لإسرائيل، حيث يمكن لأي هجوم بسيط التكلفة أن يؤثر بشكل كبير على البنية التحتية الحيوية والشبكات الاجتماعية لديها، حيث أدت الهجمات الإلكترونية إلى تعطيل المستشفيات، من بينها مركز شامير الطبي في وسط إسرائيل خلال أكتوبر 2025م[1]، وطالت الهجمات عديدًا من الشركات التي تقدم خدمات حوسبة للقطاع الاقتصادي[2].

وعلى الجانب الاقتصادي، يُقدِّم تقرير جديد صادر عن المديرية الوطنية للسيبران، للمرة الأولى، تحليلًا اقتصاديًّا للتكلفة الاقتصادية التراكمية للاقتصاد الإسرائيلي نتيجة الأضرار الناتجة عن الهجمات الإلكترونية. تُظهِر البيانات، ولأول مرة، العبء الاقتصادي الكبير على الناتج المحلي الإجمالي للبلاد الذي تسببه الهجمات الإلكترونية والأضرار المتراكمة للاقتصاد[3]. وتُقدَّر الخسائر الاقتصادية الإجمالية لإسرائيل بعد الحرب التي استمرت 12 يومًا مع إيران بنحو 6 مليارات دولار، مع تعرُّض البنية التحتية للضرر بشكل خاص، ومن المرجح أن تكلف الحرب إسرائيل نحو 1% من الناتج المحلي الإجمالي[4]. وكذلك التأثير الاجتماعي الذي يخلق شعور بالقلق والخوف بين المواطنين بسبب احتمال اختراق البيانات أو انقطاع الخدمات

---

(1) Jay Hilotin, IranIsrael War: The Rise and Risks of Hybrid Warfare, Gulf News, (June 25, 2025), Accessed January 2, 2026. https://tinyurl.com/2da8m2fd

(2) موقع MSN العربي، طالت شراكات وكيانات حيوية.. موجة هجمات إلكترونية تضرب إسرائيل وتفاصيل، (22 أكتوبر 2025م)، تاريخ الاطلاع: 9 أبريل 2026م، https://tinyurl.com/25v9l3zs

(3) (האתר הרשמי של ממשלת ישראל, העלות הכלכלית של מתקפות סייבר בישראל: 12 מיליארד ש"ח בשנה, (May 8, 2024). Accessed (January 13, 2026(. https://tinyurl.com/2b2zykm9

(4) Fareed Rahman, Israel's Economic Losses as a Result of Iran War Estimated at $6bn, The National, (June 26, 2025), Accessed January 13, 2026. https://tinyurl.com/22zm3e2m

الأساسية، والتأثير في الحياة اليومية نتيجة تعطّل الخدمات الرقمية، مثل البنوك والاتصالات[1].

ومع هذه المخاطر والتكاليف المرهقة للاقتصاد الإسرائيلي فإنَّ هذه الحرب السيبرانية توفر فرصًا ومزايا، أهمها: أولًا، ضمان التفوق العسكري والأمني، ويشار في هذا الصدد إلى أن إسرائيل حرصت خلال العقود الماضية على تطوير مجال التكنولوجيا العسكرية، من أجل تعزيز قدرتها على التصدي لأي تهديدات أمنية، خصوصًا من جانب إيران وأذرعها في المنطقة الممثلة في حزب الله اللبناني، وحركة حماس، والحوثيين، فقد طوَّرت عديدًا من الأنظمة التكنولوجية المتقدمة التي تلعب دورًا حاسمًا في إدارة دفاعاتها الجوية والبرية. وتستخدم إسرائيل بشكل متزايد تقنيات الذكاء الصناعي في عملياتها العسكرية، حيث تعتمد على قواعد بيانات مدعومة بهذه التقنيات لتحليل الأهداف العسكرية بدقة، وتحديد الأهداف الأكثر أهمية ضمن محيطٍ مُعيَّنٍ. على سبيل المثال، تُعَدّ منصة تحديد الأهداف «غوسبل» مثالًا بارزًا على هذا النهج، إذ تقترح المنصة الأهداف بناءً على أولويات إستراتيجية، وتحسب كمية الذخيرة اللازمة للهجوم، مما يزيد دقة وفاعلية الضربات العسكرية[2].

من جهة ثانية، تبرز المشاركة وتعزيز الفرص الاجتماعية والخبرات كأحد المكتسبات، حيث أصبح الأمن السيبراني دفاعًا في الخط الأمامي لكل من الأمن القومي واستقرار الأعمال. لذلك، أجبرت هذه الحروب الدول على الاستثمار في تدريب الكوادر في الأمن السيبراني وتعزيز قدرة البلاد على حماية نفسها في مواجهة الهجمات السيبرانية. تأسَّس الحرم الإلكتروني الإسرائيلي في عام 2022م، ويُعَدّ الطلاب لمهن في مجال الأمن السيبراني، سواء كمدافعين مسؤولين عن الدفاع ضد الهجمات أو كمطورين. يحصل طلاب الحرم الإلكتروني الإسرائيلي على خبرة عملية ويتعلمون من أفضل خبراء الأمن السيبراني في إسرائيل[3].

وعلى صعيد، متصل اكتسبت إسرائيل قدرات أكبر في ما يتعلق بالردع وتقوية الشراكات والدفاعات في هذا المجال، لا سيما أن الحرب السيبرانية أصبحت بشكل متزايد أداة حيوية في الدبلوماسية الحديثة. تستخدم الدول القدرات السيبرانية، ليس

---

(1) Shweta Sharma, Mental Health Impact of Cyberattacks and Data Breaches, ICliniq (Emotional and Mental Health), (July 19, 2024), Accessed January 13, 2026. https://tinyurl.com/2d77h7n9

(2) دينا إيهاب محمود، قراءةٌ في التطوّر التكنولوجي العسكري الإسرائيلي: إستراتيجيات وآفاق، ، (22 سبتمبر 2024م)، تاريخ الاطلاع: 13 يناير 2026م، https://tinyurl.com/2ca56t8e

(3) Nurit Yohanan, and ToI Staff. How the Israel Cyber Campus Is Preparing the Next Generation of Cyber Warriors, The Times of Israel, (August 25, 2024), Accessed January 13, 2026. https://tinyurl.com/2c5aslta

فقط للعمليات الهجومية، بل أيضًا لممارسة النفوذ وتحقيق الأهداف الإستراتيجية دون المشاركة العسكرية التقليدية. يمكن للدول الاستفادة من القدرات السيبرانية لإرسال رسائل بشكل خفي، أو ردع الخصوم، أو فرض هيمنة[1]، بالإضافة إلى تعزيز الشراكات الدولية، فالتعاون مع شركات ودول كبرى في مجال الأمن السيبراني عزّز المكانة الدبلوماسية. وقّعت «وحدة السايبر الوطنية» الإسرائيلية في عام 2022م على اتفاقيتَي تعاون لتعميق التعاون بمجالات دفاع السايبر والتكنولوجيا المتطوّرة مع «وزارة الأمن الوطني الأمريكية» بهدف تقوية الدفاع السيبراني عن الاقتصاد والبنية التحتية الحيوية، ومكافحة التهديدات المشتركة مثل هجمات الفدية، وتعزيز الأبحاث وتطوير التكنولوجيا المتطوّرة، والتعاون مع القطاع الخاص والعام وحوار الخبراء. يهدف الاتفاق إلى تعزيز تقنيات متطوّرة للحماية السيبرانية، وتعزيز تعاون المعلومات بالمجال، والقدرة على تشكيل قوة عاملة وتبادل خبراء[2].

2. العواقب والمكتسبات بالنسبة إلى إيران:

من جانب إيران، الحرب السيبرانية قد فرضت عليها تحديات عديدة، من بينها: أولًا، تحدٍّ إستراتيجي لقدرات البلاد وبنيتها النووية. ومن أبرز نماذجه هجوم ستوكسنت على البرنامج النووي الإيراني في 2010م، وهو برنامج سيبراني صُمم خصيصًا للتخريب الصناعي، مشترك بين الولايات المتحدة وإسرائيل. وقد تسبب في أضرار مادية، وضَعف البنية الإلكترونية الإيرانية، وأدى إلى صدمة وطنية شديدة. وردًّا على ذلك، سرعت إيران تطوير قدراتها السيبرانية الناشئة آنذاك[3]. ومن الناحية السياسية، الاتهامات المتكررة لإيران بتنفيذ هجمات سيبرانية ضد دول غربية وأهداف دولية ساهمت في فرض عقوبات من قبل الولايات المتحدة ضد أفراد وشركات إيرانية، فأصدرت وزارة الاستخبارات الإيرانية إرشادات سرّية تحذّر الوزارات والشركات الكبرى للاستعداد لاحتمال عودة عقوبات الأمم المتحدة[4].

كما قادت الحرب السيبرانية إلى التأثير في الاستقرار الداخلي والتماسك المجتمعي، فبسبب هذه الحرب قُطع ملايين الإيرانيين عن العالم الخارجي بسبب انقطاع شبه كامل للإنترنت في طهران ومدن أخرى، فيما قال المسؤولون إنه محاولة للحد من

---

(1) Alpha Maneuver, Cyber Warfare and International Relations, (2025), Accessed January 13, 2026. https://tinyurl.com/26pr48rz

(2) i24NEWS، وحدة السايبر الإسرائيلية تعزز تعاونها مع الولايات المتحدة، (3 مارس 2022م)، تم الوصول إليه في 13 يناير 2026م. https://tinyurl.com/29yyaqkg

(3) Chuck Freilich, The Iranian Cyber Threat, Memorandum No. 230, Institute for National Security Studies (INSS), (February 2024), Accessed January 13, 2026. https://tinyurl.com/229yzqtu

(4) Iran International, Sanctions Are Coming: Iranian Intel Warns Ministries, Firms on Snapback', (August 11, 2025), Accessed January 15, 2026. https://tinyurl.com/2a4u82wt

الهجمات الإلكترونية. أثر ذلك في قدرة الجمهور على البقاء على اتصال[1]، بالإضافة إلى أن الحرب لم تعُد تقتصر على البنية التحتية، بل امتدت إلى المجال المعنوي، حيث اختُرقت هيئة الإذاعة والتليفزيون الإيرانية، وبُثت رسائل تحريضية تدعو للاحتجاج، وانتشرت مقاطع فيديو معارضة على منصات التواصل الاجتماعي[2]. ومن الناحية الاقتصادية، قامت حكومة طهران بتحديث ميزانيتها الوطنية لتخصيص 71,4 مليون دولار إضافية لبرامج الفضاء السيبراني لمنظمتين تسيطر عليهما الحكومة، رغم التحديات الاقتصادية.

مع ذلك، ورغم هذه التحديات، منحت قدرات إيران السيبرانية بعض الفرص والمكتسبات، أبرزها تطوير البنية التحتية السيبرانية لمواجهة التحديات، ويُحسب لإيران أنها كانت من أوائل الدول التي وضعت إستراتيجية وطنية للسيبران، شملت تطوير المؤسسات الحكومية اللازمة والقدرات التكنولوجية. وأظهرت هجمات إيران السيبرانية القدرة على تعطيل وتخريب وتدمير الأهداف المدنية والتجارية، والبنية التحتية الوطنية الحيوية والقدرات العسكرية، وكانت عمليات التجسس السيبراني والمعلومات لديها واسعة بشكل خاص. كانت إسرائيل والولايات المتحدة هما الهدفين الرئيسيين للهجمات السيبرانية الإيرانية[3]. وتعتمد إيران على الحرب غير المتماثلة عبر شن هجمات سيبرانية منخفضة التكلفة وعالية التأثير دفاعًا عن نفسها في مواجهة استعدادها العسكري المتفاوت مع الخصوم[4].

هذا بالإضافة إلى تعزيز التعاون السيبراني مع روسيا والصين، الذي جاء في إطار سياسة التوجه شرقًا، حيث سعت إيران إلى توطيد أركان سياستها (خلال السنوات الأخيرة) بالتحوّل نحو الشرق من خلال توطيد علاقاتها مع روسيا والصين والهند في مختلف المجالات لترسيخ الأواصر. وكانت مسائل التعاون في مجال الأمن السيبراني من المسائل والقضايا التي حرصت إيران على الزج بها ضمن مفردات وفقرات هذه الاتفاقيات. وقد أعلنت وزارة الخارجية الإيرانية أن هذه الاتفاقية تهدف إلى التنسيق المشترك للكشف عن عمليات التسلل السيبراني (Cyber Intrusion) والتنسيق لضمان مستوى أمني-سيبراني جيِّد لإيران وحلفائها[5].

---

(1) Financial Times, Iranians Adapt to Wartime Life with No Internet, (June 21, 2025), Accessed January 13, 2026. https://tinyurl.com/272c5quy

(2) محمد مخلوف، ذكاء صناعي وهجمات سيبرانية.. أسلحة جديدة بين إيران وإسرائيل، العربية نت، (20 يونيو 2025م)، تاريخ الاطلاع: 13 يناير 2026م، https://tinyurl.com/2apvavzm

(3) Chuck Freilich, The Iranian Cyber Threat, Ibid.

(4) محمد معن محسن، «مستقبل موقع القوة السيبرانية في إستراتيجيات القوى الإقليمية: إيران نموذجًا». قضايا سياسية، العدد 81، (أبريل-يونيو 2025م)، ص 135-150. تاريخ الاطلاع: 15 يناير 2026م، https://tinyurl.com/27j6x3uz

(5) المركز الديمقراطي العربي، تأثير تحولات إيران إلى الشرق في إستراتيجيتها، (26 ديسمبر 2023م)، تاريخ الاطلاع: 15 يناير 2026م، https://tinyurl.com/2bkggdkj

كما عززت الحرب السيبرانية القدرات التقنية وساعدت على إدماج الذكاء الصناعي ضِمن قدرات إيران السيبرانية، فعلى الرغم من القيود الدولية المفروضة عليها في مختلف جوانب البحث العلمي والتكنولوجي خلال العقود الماضية، فإنّ النظام الإيراني يستخدم تقنيات الذكاء الصناعي على نطاق واسع لتعزيز قدراته في مجال الحرب السيبرانية، وإنتاج محتوى مزيف، وتنفيذ عمليات اختراق وتسلل عن طريق خطط وطنية واستثمارات رسمية. والتطوّر السريع في الذكاء الصناعي يغيّر ميزان القوى في ميدان الأمن السيبراني العالمي[1]، والاعتماد على تكنولوجيا متقدمة يحفّز البحث والتطوير التقني داخل البلاد. ومن الناحية الاجتماعية، الحرب السيبرانية دفعت إيران إلى التركيز على بناء خبرات وطنية في التكنولوجيا والأمن الرقمي، فقد استحدثت أكاديمية سيبرانية سرّية تُعرف باسم «راوين» في طهران، تُديرها جهات مقربة من الدولة (وزارة الاستخبارات)، وتستهدف تجنيد الشباب الموهوبين وتدريبهم على الأمن السيبراني وحتى على تنفيذ هجمات إلكترونية[2]، والتدريب في مجال رفع الوعي من الاختراق (IT Security Awareness) الذي يرفع وعي الموظفين والمجتمع بأساسيات الأمن السيبراني[3].

ولا يفوت التنويه إلى دور الحرب السيبرانية في الحرب التي جرت بين الجانبين في 2025م و2026م، والتي شهدت تصاعدًا ملحوظًا في الهجمات السيبرانية، حيث أصبحت الشبكات الرقمية ساحة حرب موازية للعمليات العسكرية التقليدية. وتتبادل الجهتان عمليات اختراق وتعطيل تستهدف البنى التحتية والاتصالات، في صراع تقني يعكس عمق التوتر الجيوسياسي بينهما.

وقد حملت الضربات الأمريكية والإسرائيلية على إيران، التي أُطلق عليها اسم عملية «الغضب الملحمي»، عدة تداعيات سيبرانية مهمة، حيث إنّ هجومًا سيبرانيًّا واسعًا عطّل الاتصالات الإيرانية قبل الضربة العسكرية، وأسهم تحليل بيانات ضخم في تحديد الأهداف، وعملت الاستخبارات الإسرائيلية لسنوات على جمع معلومات عن المرشد الإيراني علي خامنئي باستخدام أدوات سيبرانية، بما في ذلك اختراق شبكة كاميرات في طهران ومتابعة تحركاته، مقابل تصاعد الهجمات الرقمية المضادة، وسيطرت على نحو 12 برج اتصالات، بالإضافة إلى هجوم على تطبيق ديني منتشر يستخدمه الإيرانيون لتتبع أوقات الصلاة. ومكّن هذا الاختراق السيبراني من

---

(1) إيران إنترناشيونال، مايكروسوفت: إيران تستخدم الذكاء الصناعي لتعزيز الهجمات السيبرانية، (17 أكتوبر 2025م)، تاريخ الاطلاع: 15 يناير 2026م، https://tinyurl.com/2b9rjggh

(2) العربية نت، أكاديمية إيرانية سرية تستدرج الموهوبين وتخرجهم قراصنة إنترنت، (13 أكتوبر 2024م)، تاريخ الاطلاع: 15 يناير 2026م، https://tinyurl.com/25ykemrq

(3) Training Cred, IT Security Awareness and Employee Training Course, Accessed January 15, 2026. https://tinyurl.com/2alrrd89

إيصال رسائل مستهدفة مباشرة إلى المستخدمين[1]، واختُرقت عدة مواقع إخبارية رسمية إيرانية.

بالمقابل، تعتمد حملة إيران السيبرانية «الملحمة الكبرى» الموجهة من الدولة، كجزء من الإطار الأيديولوجي الأوسع للمقاومة الإسلامية السيبرانية، على الهجمات النفسية والتجسس وتعطيل الخدمات بهدف إرباك المجتمع الإسرائيلي وجمع المعلومات، إذ نفذت هجمات حجب قطاعَي المياه والطاقة والخدمات، والتلاعب بأنظمة التحكم الصناعية، ودخلت إلى شبكات التشفير ومسح وتسريب البيانات وهجمات تصيّد ومحاولات جمع معلومات عن مواقع سقوط الصواريخ داخل البلاد[2]. وقالت مديرية الأمن السيبراني الإسرائيلية إنها رصدت «عشرات الاختراقات الإيرانية لكاميرات المراقبة لأغراض التجسس»[3]، ورصدت أكثر من 1300 محاولة هجوم إيراني منذ بداية الحرب على إيران، استهدفت الإسرائيليين عبر مكالمات ورسائل نصية مزيفة[4].

وتُعتبر مجموعة «حنظلة» الإيرانية جهة قرصنة سيبرانية مرتبطة بإيران، نشطت منذ نهاية عام 2025م وحتى 2026م، وركزت على تنفيذ هجمات متعددة ضد أهداف إسرائيلية وغربية. شملت أنشطتها استهداف مسؤولين إسرائيليين باختراق هواتفهم ونشر معلومات حساسة، وتهديد جهاز المخابرات الإسرائيلي (الموساد) بهجوم سيبراني مفاجئ يوصف بأنه صدمة كبيرة، إضافة إلى إطلاق موقع إلكتروني جديد ونشر أكثر من 100,000 مستند سرّيّ مرتبط بمصادر استخباراتية إسرائيلية[5].

ثالثًا: ارتدادات الحرب السيبرانية الإسرائيلية-الإيرانية على الإقليم

يُعَدّ الصراع السيبراني بين إيران وإسرائيل أحد أهم مظاهر التنافس غير التقليدي في الشرق الأوسط، إذ تجاوز تبادل الهجمات الإلكترونية حدود الطرفين ليؤثر في الأمن والاستقرار الإقليمي. ومن هذه التأثيرات:

---

(1) Center for Strategic and International Studies (CSIS), How Will Cyber Warfare Shape the U.S.–Israel Conflict with Iran?, (March 3, 2026), accessed March 12, 2026. https://tinyurl.com/2c4pf999

(2) Government of Canada, Canadian Centre for Cyber Security, Cyber Threat Bulletin: Iranian Cyber Threat Response to US/Israel Strikes, (February 2026), accessed March 10, 2026. https://tinyurl.com/29wuxds3

(3) «الشرق الأوسط»، إسرائيل ترصد اختراقًا إيرانيًا لكاميرات المراقبة، (12 مارس 2026م)، تاريخ الاطلاع: 10 مارس 2026م، https://tinyurl.com/2dmp9oou

(4) يورونيوز، هل تصاعدت الهجمات السيبرانية مع اندلاع الحرب ضد إيران؟ إسرائيل تتحدث عن 1300 هجوم، (10 مارس 2026م)، تاريخ الاطلاع: 10 مارس 2026م، https://tinyurl.com/2xzkhdey

(5) Safir, New website of the Hanzalah cyber group launched, 100,000 confidential documents of former Mossad deputy exposed, (Apr 9, 2026), accessed Jun 10, 2026. https://tinyurl.com/23rvhyqa

1. التنافس ومحاولة تعزيز القدرات في غياب الاكتفاء الذاتي الرقمي:

يعتمد تطوير القدرات السيبرانية على المستوى الإقليمي في الأساس على المشاركة في الفاعليات والتكتلات الدولية وإبرام اتفاقيات الشراكة والاستثمار ومذكرات التعاون في ما بين دول الإقليم، وبينها وبين دول العالم في مجال الفضاء السيبراني[1]. لذلك شاركت المملكة العربية السعودية -ممثلة بالهيئة الوطنية للأمن السيبراني- في مجلس التعاون لدول الخليج العربية الذي عُقِد في دولة الكويت، التي تختص بجميع موضوعات الأمن السيبراني، وتعقد اجتماعًا سنويًّا على مستوى وزراء الأمن السيبراني في دول المجلس، وتهدف إلى الإسهام في تهيئة فضاء سيبراني خليجي آمِن، ومواءمة الجهود ورفع كفاءة التنسيق والتعاون بين دول المجلس، وحماية مصالحها في المنظمات الدولية ذات الصلة بمجال الأمن السيبراني[2]. ووقَّع الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز مذكرة تفاهم مع المنظمة العربية للتربية والثقافة والعلوم للتعاون في مجال الامن السيبراني[3].

وفي سياق المنافسة الرقمية، يشهد الاستثمار في الأمن السيبراني في دول الشرق الأوسط تحولًا إستراتيجيًّا مهمًّا، حيث أصبحت الحكومات تولي هذا القطاع أهمية متزايدة ضِمن خُطَطها الوطنية لحماية البنى التحتية الرقمية ومواجهة التهديدات الإلكترونية المتصاعدة. ومن المتوقع أن يتضاعف الإنفاق على الأمن السيبراني في منطقة الخليج بحلول عام 2030م، ليصل إلى أكثر من 120 مليار درهم إماراتي (ما يعادل نحو 32,7 مليار دولار أمريكي)[4]. وقد بلغ حجم سوق الأمن السيبراني في المملكة 15,2 مليار ريال، وهو ما يمثل إجمالي الإنفاق الذي تنفذه الجهات الحكومية والخاصة على منتجات وخدمات الأمن السيبراني في عام 2024م بزيادة قدرها 14%[5]. واحتلَّت مصر المركز الأول على مستوى الشرق الأوسط وشمال إفريقيا في عدد الصفقات الموجهة لتمويل شركات الأمن السيبراني الناشئة خلال عام 2023م[6].

---

(1) أحمد محيي محمد أحمد علي، «أثر الحرب السيبرانية الإسرائيلية-الإيرانية في الأمن الإقليمي العربي»، مجلة المعهد العالي للدراسات النوعية، مجلد 3، العدد 8، (يوليو 2023م)، تاريخ الاطلاع: 17 يناير 2026م، https://tinyurl.com/245jsqv2

(2) الهيئة الوطنية للأمن السيبراني، المملكة تشارك في الاجتماع الرابع للجنة الوزارية للأمن السيبراني في مجلس التعاون لدول الخليج العربية، (9 سبتمبر 2025م)، تاريخ الاطلاع: 17 يناير 2026م، https://nca.gov.sa/ar/news/1930/

(3) Government of Canada, Canadian Centre for Cyber Security, Ibid.

(4) Kath Young, Gulf cybersecurity spend to exceed AED120bn by 2030, Arabian Business, (November 21, 2025), accessed January 17, 2026. https://tinyurl.com/2yv3nzep

(5) National Cybersecurity Authority, Saudi National Cybersecurity Authority released Key Economic Indicators in the Cybersecurity Sector in the Kingdom 2025', (September 17, 2025), accessed January 17, 2026. https://tinyurl.com/24h8lq52

(6) أحمد غنيم، «المخاطر الإلكترونية» تدعم نمو شركات الأمن السيبراني الناشئة، البورصة، (3 فبراير 2025م)، تاريخ الاطلاع: 17 يناير 2026م، https://tinyurl.com/22ksrdpx

2. التأثير الممتد في الأمن وميزان القوة الإقليمي:

ينظر البعض إلى أن إسرائيل هي الدولة الأكثر تقدمًا في الشرق الأوسط من حيث الأمن السيبراني، وقد ظهر ذلك في الحروب التي خاضتها منذ السابع من أكتوبر على جبهات متعددة، حيث ضَمن لها التفوق في المجال التقني والسيبراني تفوقًا عسكريًّا مما أثَّر في مسارات حروبها. ولا شك أن هذا التفوق هو أحد مظاهر القوة التي تعطي إسرائيل تفوقًا في المنطقة، وقد تمنحها فرصًا أكبر من أجل تنفيذ طموحاتها في تغيير ميزان القوة الإقليمي لصالحها، وذلك على حساب القوى العربية التي تبدو قدراتها مستورَدة ومتواضعة مقارنة بإسرائيل[1].

وقد أدى استخدام الأدوات السيبرانية إلى تخطي الطبيعة الثنائية للصراع (إسرائيل – إيران)، إذ لوحظت هجمات استهدفت بيئات رقمية في دول عربية مجاورة، سواء بشكل مباشر أو عن طريق وكلاء غير حكوميين (هاكتيفست)، ففي قطر مثلًا أفاد عدد من سكان الدوحة بوقوع تغييرات غريبة في مواقعهم على هواتفهم المحمولة، حيث جرى تحديد موقعهم خطأً كنشاط داخل إيران، وفي الإمارات سُجِّلَت محاولات هجمات رقمية واسعة تستهدف جهات حكومية وشركات[2]، وهناك تقارير تشير إلى أن جهات مرتبطة بإيران سرَّبت بيانات لزوّار وألعاب مرتبطة بفاعلية في السعودية، ما يشير إلى نشاط تجسس معلوماتي أو اختراق بيانات[3]. هذا الامتداد يعني أنّ أيّ اشتباك مستقبليّ بين القوى الإقليمية الكبرى قد تتسرب آثاره بسرعة إلى دول ثالثة دون تحذير أو استعداد مسبق، مما يخلق واقعًا أمنيًّا جديدًا يُظهِر أن الحياد لم يعُد يوفر حماية ضد التورط الرقمي[4].

3. تحوُّل الإقليم إلى ساحة للاختبار السيبراني ومسرح لحرب وكالة رقمية:

يتعرض بعض دول الإقليم لتهديدات مستمرة في مجال الأمن السيبراني نتيجة ضَعف البنية التحتية ونقص التنسيق الوطني، ما جعله عرضة للتجسس الرقمي والهجمات بالوكالة، لا سيَّما من إسرائيل، حيث إنّ الموقع الإستراتيجي للبنان جعله أيضًا ساحة اختبار لتكتيكات الأمن السيبراني الإقليمية من قِبل إسرائيل. وبعض الهجمات على شبكاتها الوطنية كان بمثابة تجارب لعمليات أوسع، بالإضافة إلى أجهزة الاستخبارات الإسرائيلية التي تعاملت مع لبنان باعتباره ميدان اختبار حي

---

(1) Government of Canada, Canadian Centre for Cyber Security, ibid.

(2) صحيفة الخليج، الأمن السيبراني.. الإمارات تحبط 200 ألف هجمة سيبرانية يوميًّا غالبيتها مدعومة من دول، (18 فبراير 2026م)، تاريخ الاطلاع: 12 مارس 2026م، https://tinyurl.com/24ng7nmk

(3) Resecurity, IranLinked Threat Actors Leak Visitors and Athletes' Data from Saudi Games, (June 22, 2025), accessed March 2, 2026. https://tinyurl.com/2dh28nnp

(4) أحمد فتحي، مستقبل الصراعات السيبرانية في الشرق الأوسط: التداخل بين الجيوسياسية والأمن، مركز آتون للدراسات، (30 أبريل 2025م)، تاريخ الاطلاع: 17 يناير 2026م، https://tinyurl.com/2ctdhm7r

للعمليات السيبرانية. وإنَّ الموقع الجغرافي للأردن قد يحوله إلى مركز لنقل البيانات، وقد يُستغَل في النزاعات الإقليمية الأوسع، مما يعزز الحاجة إلى تعاون إلكتروني قوي داخليًّا وإقليميًّا[1]. وبسبب الحروب السيبرانية تم إحياء الصراعات بالوكالة في دول ضعيفة مثل لبنان وسوريا والعراق، وأخلَّ بشكل خطير بالتوازن الهش في الشرق الأوسط، كما نشطت إيران في الاعتماد على مجموعات قرصنة (هاكتيفست) موالية أو مدعومة من الدولة لأداء هجمات سيبرانية، خصوصًا في أعقاب الضربات الإسرائيلية والأمريكية، وذلك بهدف زيادة نطاق تأثيرها السيبراني، مع إنكار مباشر لمسؤوليتها الرسمية.

4. تهديد البنى التحتية وتعطيل إمدادات الطاقة الإقليمية:

في حال اتسع نطاق الحرب، فإنَّ العلاقات التجارية القائمة مع طهران أو حتى تل أبيب قد تتأثر سلبًا كما قد تتأثر دول المنطقة ككل[2]، ففي سياق الأزمة الإيرانية – الإسرائيلية شهدت ثلاثة قطاعات اقتصادية رئيسية، الطاقة والنقل والأسواق المالية، أكبر قدر من الهشاشة، ففي قطاع الطاقة أدت الهجمات على البنية التحتية الإيرانية الحيوية إلى انخفاض حاد في صادرات النفط والغاز، فيما أدى توقف الإنتاج في حقلَي ليفياثان وكاريش الإسرائيليين، اللذين كانا من الموردين الرئيسيين للغاز إلى مصر والأردن، إلى تعطيل إمدادات الطاقة الإقليمية[3]. وتلعب البنية الإلكترونية دورًا مهمًّا في استهداف تلك القطاعات أو الدفاع عنها.

5. تغيير نمط العلاقة بين دول المنطقة وإسرائيل:

الحرب السيبرانية ما بين إسرائيل وإيران أثَّرَت في نمط العلاقة ما بين دول الإقليم، حيث إنَّ ارتفاع الهجمات السيبرانية ضد أهداف دول مجلس التعاون، والتفوق الإسرائيلي في المجال السيبراني، أدّيا إلى تسريع عملية إنشاء إطار عمل تعاون بين بعض الدول وإسرائيل[4]. وبعد الاتفاق الإبراهيمي بين إسرائيل وكل من الإمارات والبحرين بدأ التعاون بين هذه الدول في مجال الأمن السيبراني يتسع بشكل ملموس، خصوصًا في ظل التهديدات السيبرانية الإيرانية المشتركة التي تستهدف البنية التحتية للدول الإقليمية، ففي مؤتمر CyberTech الذي عُقِد في تل أبيب، التقى كبار المسؤولين عن الأمن السيبراني من إسرائيل والإمارات والبحرين والمغرب، وتباحثوا

---

(1) Shafaq News. Middle East Cyber War: Strategy Failures Leave Arab States Vulnerable, Shafaq News, (January 16, 2026), Accessed January 16, 2026. https://tinyurl.com/2ar7v25y

(2) زيد اسليم، ما تداعيات تعليق تركيا علاقاتها التجارية مع إسرائيل؟، الجزيرة نت، (3 مايو 2024م)، تاريخ الاطلاع: 17 يناير 2026م، https://tinyurl.com/2yw49ljz

(3) يورونيوز فارسی، جنگ ايران واسرائيل چه تاثيرات ژئوپليتيکی بر امنيت منطقه‌ای واقتصاد جهانی می‌گذارد؟، (21/06/2025)، تاريخ الاطلاع: 1 مارس 2026م، https://tinyurl.com/2732lv7c

(4) Government of Canada, Canadian Centre for Cyber Security, ibid.

حول توسيع التعاون الأمني السيبراني ضِمن إطار الاتفاق الإبراهيمي لحماية البنى التحتية الحيوية وتبادل المعلومات حول التهديدات السيبرانية. هذا النوع من التعاون يُظهِر بوضوح كيف أن التحديات السيبرانية المشتركة دفعت الدول إلى تعزيز الشراكات التقنية والأمنية مع إسرائيل بعد تطبيع العلاقات الدبلوماسية[1]. ولإحداث تغيير في توازنات القوى السيبرانية في المنطقة والتخفيف من حدة نقاط الضعف السيبراني لبعض الدول، كان الحصول الخبرة الإسرائيلية في الاستخبارات والحرب السيبرانية عاملًا مهمًّا.

6. الاستثمار السيبراني في ظل تفاوت الإمكانيات المادية:

وفي ظل تصاعد الهجمات السيبرانية وتعقيد التهديدات الرقمية، أصبح الاستثمار في القدرات البشرية السيبرانية إحدى الركائز الأساسية للأمن الرقمي في الدول. يركز هذا الاستثمار على تأهيل الكوادر وتدريبها وتزويدها بالمهارات المتقدمة لمواجهة الاختراقات وحماية البنى التحتية الحيوية. مثال على ذلك البرنامج السعودي «تأهيل خبراء المستقبل في مجال الأمن السيبراني»، وهو برنامج يوفر للقدرات الوطنية مسارات تدريبية وعملية لهم على رأس العمل، للإسهام في حماية الفضاء السيبراني السعودي وتعزيز مسيرة الأمن السيبراني في المملكة. ويأتي ذلك في إطار الأهداف الإستراتيجية للهيئة الوطنية للأمن السيبراني الرامية إلى تنمية القدرات البشرية في مجال الأمن السيبراني[2]. كما أطلقت مصر مبادرة «مهارات سيبرانية» التي تستهدف إعداد جيل جديد من الكوادر في مجال الأمن السيبراني[3].

مع ذلك فإن الأمن السيبراني في بعض دول الإقليم يواجه ثغرات مالية، مما يجعل البلاد أكثر ضَعفًا أمام التهديدات الرقمية مقارنة بدول لديها ميزانيات أكبر وبرامج متقدمة، ما يتطلب زيادة الاستثمار، فميزانية الأمن السيبراني في الأردن مثلًا تبلغ نحو 70 مليون دولار سنويًّا، وهي ميزانية صغيرة جدًّا مقارنة بميزانيات الدول المتقدمة في المجال مثل الإمارات التي تخصص نحو 1,5 مليار دولار للأمن السيبراني، مما يؤثر في قدرة الأردن على بناء دفاعات قوية ضد الهجمات الإلكترونية[4]. وفي ظل ميزانية محدودة للأمن السيبراني، فإنّ مقارنة هذه الميزانية بالدول التي تخصص مبالغ كبيرة للقطاع قد تؤدي إلى ضغوط اقتصادية على الدولة الصغيرة، نتيجة

---

(1) Department of Homeland Security (DHS), DHS Expands Abraham Accords to Cybersecurity, (February 2, 2023), Accessed January 17, 2026. https://tinyurl.com/25ejx85w

(2) الهيئة الوطنية للأمن السيبراني، برنامج تأهيل خبراء المستقبل في مجال الأمن السيبراني، تاريخ الاطلاع: 17 يناير 2026م، https://tinyurl.com/2bogjtmq

(3) مصراوي، وزارة الاتصالات وتكنولوجيا المعلومات، وزير الاتصالات: تأهيل 1000 طالب جامعي سنويًا من خلال مبادرة مهارات سيبرانية، (4 مايو 2025م)، تاريخ الاطلاع: 1 أبريل 2026م، https://tinyurl.com/253qpx5j

(4) National Cybersecurity Authority, Saudi National Cybersecurity Authority.. Ibid.

الحاجة إلى استثمار موارد إضافية لتعزيز الدفاعات الرقمية ومواجهة الهجمات، مما قد يؤثر في القطاعات الأخرى ويزيد الأعباء المالية.

رابعًا: الآفاق المستقبلية للحرب السيبرانية

من خلال التحليل السابق يمكن استنتاج حدوث تحوّل إستراتيجي في طبيعة الصراع، حيث يتضح أن إسرائيل وإيران نقلتا الصراع من المجالات العسكرية التقليدية إلى الفضاء السيبراني بوصفه ساحة منخفضة الكلفة وعالية التأثير ويمكن إنكاره بسهولة، مع تداخل واضح بين الدفاع والهجوم والحرب النفسية. والصراع يُعيد توزيع توازن القوى السيبرانية في الشرق الأوسط، خصوصًا مع تصاعد دور إسرائيل اعتبارها قوة تقنية رائدة، ودفع بعض دول الخليج على تعزيز التعاون معها في مجال الأمن السيبراني.

كما تعطي الحرب السيبرانية انطباعًا بوجود تفوُّق سيبرانيّ إسرائيليّ نوعيّ إقليميّ ودوليّ، حيث تمتلك إسرائيل قدرات سيبرانية هائلة تضمن لها تفوقًا نوعيًّا قائمًا على الابتكار، والذكاء الصناعي، وتكامل القطاعين العسكري والخاص (وحدات مثل 8200، وشركات مثل Check Point وCyberArk)، علاوة على إثبات حقيقة اندماج الحرب السيبرانية مع الحرب النفسية/المعرفية وتأثيرها في الصراع، إذ لم تعُد العمليات تقتصر على تعطيل الأنظمة، بل باتت تستهدف الوعي العام عبر التضليل، وتسريب البيانات، والتلاعب بالمعلومات، واستخدام الذكاء الصناعي لتضخيم الأثر النفسي. فالهجمات السيبرانية على البنية التحتية الحيوية تسببت بأزمات إنسانية، بما في ذلك تعطّل الخدمات الأساسية وظهور موجات لجوء جديدة، ما يضع ضغوطًا مضاعفة على الدول المجاورة والخدمات الإنسانية.

ولا جدال في أن الحرب السيبرانية الإيرانية-الإسرائيلية أحدثت تحولًا عميقًا في أساليب الصراع، حيث امتدت التأثيرات من البنية التحتية إلى المجتمع والاقتصاد والسياسة، مع تعزيز القدرات الوطنية لدى الطرفين.

والأهم أن الحرب السيبرانية لم تعُد ثنائية (إيران-إسرائيل)، بل امتدت لتشمل دولًا عربية مجاورة سواء بشكل مباشر أو عبر وكلاء رقميين، ما يعكس مخاطر تورط دول ثالثة وتأثر أمنها الرقمي، ويجعل الحياد التقليدي غير كافٍ للحماية والمشاركة في التكتلات والمنتديات الدولية (مثل مجلس التعاون لدول الخليج)، ومذكرات التفاهم الإقليمية تساعد الدول على رفع كفاءة التنسيق وحماية مصالحها الرقمية.

ومع تصاعد الاعتماد على التكنولوجيا والرقمنة، أصبحت إسرائيل وإيران تتصارعان في الفضاء السيبراني امتدادًا للصراع الإقليمي، مستهدفين البنى التحتية الحيوية

والأنظمة الرقمية، ولذا فإنَّ دراسة آفاق هذا الصراع ضرورية لفهم تأثيره في الأمن الإقليمي والقدرات الدفاعية للطرفين. ويظهر أنّ لآفاق الحرب السيبرانية ما بين إسرائيل وإيران ثلاثة سيناريوهات:

السيناريو الأول: استمرار الوضع القائم (استمرار حرب الاستنزاف السيبرانية الحالية)

يفترض هذا السيناريو استمرار الوضع القائم من خلال توجيه ضربات محدودة ومتبادلة بين النظامين الإيراني والإسرائيلي، بهدف احتواء الصراع ومنع انزلاقه إلى حرب سيبرانية إقليمية. ويواصل الطرفان استخدام وسائل غير مباشرة للإضرار بمصالح بعضهما بعضًا، وتنفيذ عمليات استخباراتية تهدف إلى إحباط تحركات الطرف الآخر. وفي هذا الإطار، تأخذ المواجهة طابع حرب استنزاف طويلة الأمد، دون أن يتمكن أي من الجانبين من تحقيق حسم واضح، ما يؤدي إلى أضرار تراكمية متزايدة لدى الطرفين، إذ تعاني إيران في ظل أزمة اقتصادية خانقة من ضغوط متزايدة لتلبية الاحتياجات الأساسية للسكان، وعدم الاستقرار الاجتماعي. وفي المقابل، ورغم امتلاك إسرائيل قدرات اقتصادية أقوى، فإنها تتحمل كلفة مرتفعة نتيجة استمرار القتال، والإنفاق الضخم على المنظومات الدفاعية، فضلًا عن تراجع ثقة المستثمرين الأجانب بفعل تصاعد حالة عدم اليقين. ولا يقتصر تأثير هذا السيناريو على الطرفين المباشرين، بل تمتد تداعياته إلى الإقليم بأسره، إذ قد يؤدي تدهور الأوضاع داخل إيران إلى موجات نزوح واسعة نحو دول الجوار مثل تركيا والعراق وباكستان، ما ينذر بأزمة إنسانية وإقليمية معقدة. كما أن استمرار حالة الفوضى وعدم الاستقرار قد يهيئ بيئة مواتية لعودة الجماعات المتطرفة، وتصاعد أنشطة التمرد من قِبل بعض الأقليات العرقية المعارضة لإيران، كالأكراد والبلوش. ويثير هذا السيناريو قلق القوى الدولية الكبرى، باعتباره نموذجًا لحالة عدم استقرار مزمن في الشرق الأوسط، مع احتمالات توسع الصراع وتداخله عبر ساحات متعددة، وما يحمله ذلك من مخاطر أمنية وسياسية بعيدة المدى. وتُعَدّ احتمالية تحقق هذا السيناريو مرتفعة نسبيًّا، ومن المرجح أن يمتد هذا السيناريو لفترة زمنية طويلة مع تذبذب حدة الصراع بين التصعيد المحدود والتهدئة المؤقتة، بما يعكس حالة عدم الاستقرار المزمن في الإقليم.

السيناريو الثاني: تصاعد الهجمات والانتقال إلى حرب سيبرانية إقليمية تشمل دول مجلس التعاون الخليجي

قد يؤدي تصعيدٌ غير مقصود ناجم عن سوء التقدير أو دوامات عسكرية غير مخطط لها إلى مواجهة إقليمية مكلفة يعارضها معظم الفاعلين الدوليين والإقليميين.

ولهذا التصعيد ثلاثة مؤشرات: أولًا، البرنامج النووي الإيراني، إذ قد تجعل الحماية الجيدة التي توفرها إيران لمنشآتها النووية، إلى جانب ارتفاع مستويات تخصيب اليورانيوم، إسرائيل أكثر عدوانية. كما أن التقدم في الذكاء الصناعي وأتمتة العمليات قد يؤدي إلى هجمات أكثر تعقيدًا، تشمل قرصنة تلقائية، وتحليلًا مكثفًا للبيانات، وهجمات خفية يصعب كشف مصدرها أو التصدي لها بسهولة. ومن شأن ذلك أن يدفع الولايات المتحدة، بوصفها القوة الأبرز، إلى الانضمام إلى الحرب، بما يزيد حدَّة الصراعات. ومن المحتمل أيضًا أن يشارك بعض الدول العربية والخليجية في الحرب. ومن الصعب تصور انتهاء هذه الحرب قبل أن تشن الولايات المتحدة وإسرائيل هجومًا على المواقع النووية الإيرانية المتبقية، وهو ما قد يُفضي بدوره إلى تغيير النظام خلال سنوات قليلة. أما المؤشر الثاني فهو انهيار النظام الإيراني، إذ إنّ انهيار إيران سيُحدِث فراغًا كبيرًا في المنطقة، بما ينعكس سلبًا على توازناتها السياسية والأمنية. كما أن تصعيد الحرب الإلكترونية بين إسرائيل وإيران يحمل تداعيات كبيرة على الاستقرار الإقليمي والدولي. وأما المؤشر الثالث فيتمثل في ضَعف إيران عسكريًّا، وهو ما قد يدفعها إلى التركيز بصورة أكبر على الهجمات السيبرانية بوصفها أداة أقل كلفة وأكثر مرونة في التصعيد والمواجهة.

ويُقدَّر احتمال حدوث هذا السيناريو بأنه متوسط، في حين يُصنَّف مستوى الخطر بأنه عالٍ، ما يجعله من السيناريوهات متوسطة الوقوع وعالية التأثير.

السيناريو الثالث: السيطرة على الحرب السيبرانية عبر تعديل سلوك النظام الإيراني

يشمل السيناريو الثالث استمرار النظام الحاكم في إيران في السلطة، إذ لا يفترض إسقاط النظام أو إحداث تغيير جذري في القيادة، بل يركز على إجراء تعديل تكتيكي أو إصلاحي في سلوك النظام مع استمراره. توجد مجموعة من المؤشرات التي قد تدفع نحو تعديل هذا السلوك، من أبرزها: أولًا تصاعد الضربات السيبرانية التي تستهدف البنية التحتية الإيرانية، ثانيًا تراجع فاعلية الأدوات الهجومية السيبرانية الإيرانية، ثالثًا تنامي الضغوط الاقتصادية والتقنية المفروضة على الدولة، أمّا المؤشر الرابع فهو تزايد الضغوط الداخلية والإعلامية. قد تؤدي هذه العوامل مجتمعة إلى دفع النظام الإيراني نحو إعادة ضبط سلوكه بدلًا من انهياره أو إسقاطه، مع احتمال أن يوافق مجتبى خامنئي، المرشد الأعلى الإيراني الجديد، على تقديم تنازلات تتعلق بالبرامج النووي والصاروخي، إضافة إلى تقليص أو وقف دعم بعض الوكلاء الإقليميين مثل حزب الله، بما يسهم في احتواء الحرب السيبرانية وإبقائها ضمن

حدود يمكن التحكم بها. ومع ذلك، يظل احتمال تحقق هذا السيناريو مستبعدًا في المدى القريب والمتوسط.

خاتمة

وختامًا يمكن استشراف أن سيناريو الحفاظ على الوضع القائم يُعَدّ الأكثر ترجيحًا، وذلك لعدة اعتبارات بنيوية وإستراتيجية، فاحتمالية توسع الحرب من مواجهة إيرانية-إسرائيلية إلى حرب إقليمية شاملة تظل محدودة نسبيًّا، ويعود ذلك إلى الطبيعة الخاصة للفضاء السيبراني، حيث يصعب في كثير من الأحيان تحديد الجهة المسؤولة عن الهجوم بدقة، أو إثباته بشكل قاطع، الأمر الذي يقلل فرص الرد العسكري المباشر ويحدّ من منطق التصعيد التقليدي. إضافة إلى ذلك، تشهد الدول المنخرطة في هذا النوع من الصراع، وفي مقدمتها إسرائيل وإيران، مستوى متزايدًا من الوعي بخطورة الحرب السيبرانية وتداعياتها الإستراتيجية، وهو ما دفعها إلى الاستثمار المكثف في تطوير قدراتها الدفاعية والهجومية السيبرانية. وقد أسهم هذا التطوّر في تعزيز مناعة البنى التحتية الحيوية وتقليص قابليتها للتأثر بالهجمات، مقارنة بالمراحل الأولى من هذا النوع من الصراعات، مما يجعل تحقيق اختراقات حاسمة أكثر صعوبة من السابق. ولا يقتصر هذا الإدراك على أطراف الصراع المباشرين فحسب، بل يمتد أيضًا إلى الدول الإقليمية، التي باتت أكثر وعيًا بخطورة تداعيات الحرب السيبرانية على أمنها الوطني واستقرارها الداخلي، الأمر الذي دفعها إلى تكثيف جهودها في تعزيز أمنها السيبراني، وتطوير قدراتها الدفاعية، ورفع جاهزية مؤسساتها الحيوية لمواجهة أي ارتدادات محتملة لهذا النوع من الصراعات. أمّا في ما يتعلق بسيناريو السيطرة على الحرب من خلال تعديل النظام الإيراني القائم، فيبدو أنه احتمال غير وارد، خصوصًا في المدى القريب، كما أن تعيين مجتبى خامنئي مرشدًا أعلى لإيران يبعث برسائل واضحة تعكس التحدي والاستمرارية، في إشارة إلى أن النظام الإيراني اختار شخصية مقرّبة من الحرس الثوري الإيراني لتأكيد هيمنة هذا الجهاز على مفاصل الدولة، لا سيَّما في ظل حالة المواجهة المستمرة مع الولايات المتحدة وإسرائيل.

info@rasanahiiis.com
@rasanahiiis
www.rasanah-iiis.org