الحرب السيبرانية بين إيران وإسرائيل (2010–2025).. قراءة تحليلية في الأهداف الأدوات والانعكاسات الإقليمية

د. صبري عفيف العلوي

مدير تحرير مجلة بريم الصادرة عن مؤسسة اليوم الثامن للإعلام والدراسات

يونيو 2025م

الحرب السيبرانية بين إيران وإسرائيل (2010–2025).. قراءة تحليلية في الأهداف الأدوات والانعكاسات الإقليمية

د. صبري عفيف العلوي

مدير تحرير مجلة بريم الصادرة عن مؤسسة اليوم الثامن للإعلام والدراسات

يونيو 2025م

صادر عن
مؤسسة
اليوم الثامن
alyoum8.net
للإعلام والدراسات

ملخص

تتناول هذه الورقة البحثية تصاعد الحرب السيبرانية بين إيران وإسرائيل خلال الفترة الممتدة من عام 2010 حتى عام 2025، باعتبارها واحدة من أكثر ساحات الصراع تعقيدًا وحداثة في الشرق الأوسط. وقد تحولت هذه الحرب من مجرد اختراقات رقمية محدودة إلى نمط هجومي متكامل يشمل الهجمات السيبرانية، الاغتيالات الذكية، والعمليات الاستخباراتية المترابطة.

تسعى الدراسة إلى تحليل الأهداف الاستراتيجية لكل طرف، واستعراض أبرز الهجمات، ومقارنة الأدوات والتكتيكات المستخدمة، مع تقييم دقيق للانعكاسات السياسية والأمنية على مستوى الإقليم.

تُبرز الورقة كيف مثّل الفضاء السيبراني ميدانًا بديلاً للمواجهة، ووسيلة للردع غير المتناظر، في ظل غياب إطار قانوني دولي حاكم، مما ينذر بإمكانية انزلاق الصراع نحو مستويات أكثر عنفًا وتهديدًا للأمن الإقليمي والدولي.

المقدمة

شهدت الفترة الممتدة من عام 2010 حتى عام 2025 تصاعدًا ملحوظًا في حدة وتكرار الهجمات السيبرانية بين إسرائيل وإيران، لتشكل واحدة من أبرز ساحات الصراع غير التقليدي في الشرق الأوسط، بل وفي النظام الدولي بأسره. فقد انتقل الصراع بين الطرفين من نطاقه العسكري والأمني التقليدي إلى الفضاء الرقمي، حيث باتت الحروب السيبرانية أداة استراتيجية تستخدمها الدول لفرض الإرادة السياسية، وتحقيق أهداف استخباراتية، والتأثير على الخصم دون الحاجة إلى خوض مواجهات ميدانية مباشرة.

وتُعد هذه المرحلة من الصراع السيبراني بين إيران وإسرائيل تجسيدًا لتحول نوعي في أنماط التهديدات الأمنية، حيث تركزت الهجمات في بدايتها على البنى التحتية الحيوية، كالمياه والطاقة والمواصلات، ثم تطورت لتستهدف القطاعات المدنية، والمؤسسات الطبية، والمراكز البحثية، بل وحتى الحياة اليومية للمواطنين. وفي المقابل، تبنّت إسرائيل بدورها سياسة هجومية في المجال السيبراني، مستفيدة من تفوقها التكنولوجي، ومكرسة أدواتها الإلكترونية لضرب المنشآت الإيرانية الحساسة، لا سيما في مجالات الطاقة والنووي والموانئ.

لقد فرض هذا النوع من الحروب واقعًا جديدًا يتجاوز الحدود التقليدية للصراع، ويجعل من كل منشأة رقمية أو شبكة معلوماتية ساحة محتملة للمواجهة. كما أن هذه الهجمات، في كثير من الأحيان، كانت تتم عبر وكلاء إلكترونيين غير حكوميين، ما يمنح الطرفين هامشًا للمناورة والإنكار السياسي، ويعقد في الوقت ذاته مهمة الردع القانوني الدولي.

من هذا المنطلق، تسعى هذه الورقة إلى تحليل مسار الهجمات السيبرانية المتبادلة بين إيران وإسرائيل خلال الفترة (2010–2025)، من حيث تطورها الزمني، وأهدافها الاستراتيجية، ونتائجها العملية، ودلالاتها السياسية، وذلك لفهم مدى تأثير هذا الصراع الرقمي على الأمن الإقليمي والاستقرار الاستراتيجي في الشرق الأوسط.

الأهداف الاستراتيجية لإيران وإسرائيل

في سياق التنافس الإقليمي والدولي بين إسرائيل وإيران، لم تعد الحرب السيبرانية مجرّد أدوات تكميلية ضمن منظومة الردع، بل غدت وسيلة مركزية تسعى من خلالها كل دولة إلى تحقيق أهداف استراتيجية محددة، تُترجم في الغالب ضمن رؤيتها للأمن القومي، وطبيعة تموضعها في المعادلات الإقليمية والدولية. فقد وظّفت إسرائيل قدراتها التكنولوجية المتقدمة لتكريس سياسة "الضربات الاستباقية" تجاه البنى التحتية الإيرانية، خاصة ما يتعلق ببرنامجها النووي وشبكاتها اللوجستية، في حين وظّفت إيران الهجمات السيبرانية كأداة ردع غير متماثلة لتعويض ضعفها التقليدي في مواجهة التفوق الإسرائيلي.

وتكشف طبيعة الأهداف التي اختارها كل طرف عن منطق مغاير في استخدام الفضاء السيبراني: حيث تميل إسرائيل إلى استهداف المنشآت ذات الطابع الاستراتيجي – الأمني والعسكري – بهدف تقويض قدرات إيران وتعطيل مشاريعها بعيدة المدى، بينما تميل إيران إلى استهداف المنشآت المدنية والمؤسسات الخدمية داخل إسرائيل، في محاولة لزعزعة الثقة الشعبية بالمنظومة الحكومية، وإثبات حضورها الإلكتروني كمصدر تهديد فعّال.

وبالتالي، فإن تحليل الأهداف الاستراتيجية للطرفين يُعد مدخلًا حاسمًا لفهم طبيعة هذا الصراع، وحدود تأثيره، وإمكانية تصعيده أو احتوائه في المستقبل.

جدول رقم (1) يوضح

الأهداف الاستراتيجية لطرفي الصراع

أطراف الصراع	إسرائيل	ايران
الأهداف الاستراتيجية	- شلّ البنية التحتية الإيرانية النووية واللوجستية - جمع المعلومات الاستخباراتية - ردع القدرات الإيرانية ومنع تصعيدها الإقليمي - الحفاظ على تفوقها التقني	- التأثير على الداخل الإسرائيلي نفسيًا وسياسيًا - إرباك المؤسسات الحيوية والمدنية - تقويض ثقة الجمهور بالحكومة الإسرائيلية - خلق أدوات ردع غير متماثلة في مواجهة التفوق الإسرائيلي

الهجمات السيبرانية الإسرائيلية ضد إيران (2010–2025)

منذ عام 2010، أصبحت الهجمات السيبرانية أحد أبرز أدوات إسرائيل في تنفيذ استراتيجيتها لاحتواء المشروع النووي الإيراني وعرقلة توسّع نفوذ طهران الإقليمي. وقد مثّلت هذه الهجمات جزءًا مما يُعرف بـ"حرب الظل" بين الجانبين، وهي حرب غير تقليدية، تدور خارج أطر الصدام العسكري المباشر، وتُستخدم فيها أدوات رقمية عالية الدقة، وتُنفّذ غالبًا من خلال أجهزة استخبارات متخصصة، في مقدمتها الموساد ووحدة 8200 التابعة للاستخبارات العسكرية الإسرائيلية.

تميّزت الهجمات الإسرائيلية على إيران بطابعها الاستباقي والانتقائي، إذ ركزت على أهداف نوعية وحساسة تمسّ البنية التحتية النووية والصناعية واللوجستية، كما طالت منظومات القيادة والسيطرة، والموانئ، وحتى وسائل الإعلام الرسمية. وقد تراوحت هذه العمليات ما بين تدمير مادي مباشر (عبر فيروسات مثل "ستاكس نت") إلى شلل تقني شامل في شبكات اتصالات أو أنظمة ملاحة، إضافة إلى عمليات تجسس رقمية واختراق قواعد بيانات إستراتيجية.

وعلى مدار الفترة (2010–2025)، تكشف الهجمات الإسرائيلية ضد إيران عن تطوّر مستمر في الأدوات السيبرانية المستخدمة، وتكاملها مع العمل الاستخباراتي التقليدي والعمليات الميدانية، في إطار استراتيجية ردع مرنة ومتصاعدة تهدف إلى إبقاء إيران تحت الضغط الدائم، ومنعها من بلوغ العتبة النووية أو توسيع قدراتها الهجومية في المنطقة.

وفي هذا المحور، سيتم استعراض أبرز الهجمات السيبرانية الإسرائيلية التي استهدفت إيران، مرتبة زمنيًا، مع توضيح نوع كل عملية، موقع تنفيذها، والجهة المنفذة أو المسؤولة عنها، ما يوفّر رؤية تحليلية شاملة لهذا الجانب الحاسم من الصراع الإسرائيلي–الإيراني في الفضاء الرقمي.

جدول رقم(2) يوضح

الفترة الزمنية للعمليات الإسرائيلية داخل إيران وخارجه (2010–2025)

الوصف	النوع	الموقع	العملية	التاريخ
فيروس سيبراني دمّر آلاف أجهزة الطرد المركزي لتخصيب اليورانيوم.	هجوم سيبراني/ تخريبي	نطنز، إيران	Stuxnet	2010
تشويش الدفاعات الجوية لضرب منشأة نووية سورية سرًا.	تشويش إلكتروني/ غارة جوية	دير الزور، سوريا	عملية أورشارد	2007
حجز سفينة تنقل أسلحة إيرانية لفصائل في غزة.	اعتراض عسكري/ مخابراتي	البحر الأحمر	حجز سفينة إيرانية	2014
اختراق شركة الاتصالات الرسمية للتجسس على مكالمات اللبنانيين.	هجوم سيبراني/ تجسس	لبنان	عملية أوجيرو	2017
الموساد استولى على وثائق نووية سرية عبر 20 عميلاً داخل إيران.	تجسس ميداني/ اختراق استخباراتي	طهران، إيران	سرقة الأرشيف النووي الإيراني	2018

تفجير أدى إلى دمار كبير في المنشأة النووية.	تخريب داخلي/ سيبراني	نطنز، إيران	تفجير أول في منشأة نطنز	2020
تم باستخدام رشاش مثبت على شاحنة ويتحكم به عن بعد.	اغتيال ذكي عبر الذكاء الصناعي	طهران، إيران	اغتيال محسن فخري زاده	2020
عملية خفية عطلت أجهزة الطرد المركزي؛ اتُّهمت إسرائيل رسميًا.	تخريب داخلي/ سيبراني	نطنز، إيران	تفجير ثانٍ في نطنز	2021
كشف أن مسؤول مكافحة الموساد كان عميلًا له.	اختراق استخباراتي	إيران	تصريحات أحمدي نجاد	2021
أكد أن الموساد تسلل إلى مفاصل الدولة الإيرانية.	تقدير استخباراتي	إيران	تصريحات علي يونسي	2022
استهداف مصنع ذخيرة؛ الموساد متهم بالتنفيذ.	هجوم مسير/عمليات خاصة	أصفهان، إيران	هجوم بطائرات مسيرة على أصفهان	2023
استُهدف داخل دار ضيافة تابعة للحرس الثوري بعد حفل تنصيب الرئيس بزشكيان.	اغتيال سياسي خارجي	طهران، إيران	اغتيال إسماعيل هنية	2024
سبق عملية تصعيد كبرى؛ توقيت يثير الشكوك حول اختراق أمني.	حادث غامض/تحرك استخباراتي	إيران	حادث وفاة الرئيس إبراهيم رئيسي	2024
هجوم جوي وصاروخي واسع استهدف منشآت نووية وقيادات عسكرية.	حرب سيبرانية + عسكرية	إيران	بدء الحرب الإسرائيلية–الإيرانية	2025
اغتيال 6 من كبار القادة العسكريين بصواريخ ومسيرات.	اغتيال ميداني بالتوازي مع القصف	إيران	اغتيال كبار القادة العسكريين	2025
سرقة بيانات 42 مليون عميل (12 تيرابايت) وتسريبها لاحقًا.	هجوم سيبراني/ابتزاز مالي	إيران	اختراق بنك "سباه" الإيراني	17 يونيو 2025
تدمير 90 مليون دولار من الأصول الرقمية ونقلها لمحافظ خارجية.	هجوم سيبراني مالي	إيران	اختراق بورصة Nobitex للعملات الرقمية	18 يونيو 2025
شلل شبه تام للبنية الرقمية والاتصالات الداخلية والعسكرية.	شلل سيبراني/هجوم شامل	إيران	انهيار الإنترنت بنسبة 97%	18 يونيو 2025
اغتيال سامي عبد الله، فؤاد شكر، نصر الله وآخرين بضربات دقيقة.	اغتيالات استخباراتية متسلسلة	لبنان	سلسلة اغتيالات لقيادات حزب الله	يونيو–سبتمبر 2025
الأجهزة المستوردة تم تفخيخها مسبقًا وتحولت لعبوات ناسفة في توقيت واحد.	تفجير عبر أجهزة مخترقة	إيران + لبنان	تفجير أجهزة نداء لـ 3000 عنصر من حزب الله	منتصف 2025

مما سبق تبين أن الفترة الممتدة من 2010 حتى 2025 مرحلة حاسمة في الصراع الخفي بين إسرائيل وإيران، حيث اتسمت العمليات الإسرائيلية بتنوع تكتيكاتها وأهدافها، من هجمات سيبرانية معقدة إلى اغتيالات ميدانية دقيقة، مرورًا بعمليات مخابراتية واستخباراتية متقدمة، بالإضافة إلى تدخلات عسكرية خاصة. ويبرز هذا الصراع كأحد أكثر الأمثلة تطوراً على استخدام الأدوات التكنولوجية والاستخباراتية في الحروب الحديثة.

- التحول من الهجمات السيبرانية إلى العمليات المختلطة (2010-2014)
- التوسع الجغرافي والتكتيكي (2014-2018)
- . تصعيد الهجمات السيبرانية والاغتيالات الذكية (2020-2021)
- توسع العمليات إلى حرب هجينة شاملة (2022-2025)

التقييم العام والتوجهات المستقبلية

يظهر من التحليل أن إسرائيل نجحت في تطوير تكامل عالٍ بين القدرات السيبرانية، الاستخباراتية، والعسكرية الميدانية، مما جعلها قوة فاعلة في فرض قواعد الاشتباك في منطقة الشرق الأوسط.

العمليات اتسمت بالتدرج الزمني في التعقيد والجرأة، حيث انتقلت من عمليات تجسس واختراق إلكتروني إلى هجمات مسلحة معقدة واغتيالات ذكية.

استغلال التكنولوجيا الحديثة مثل الطائرات المسيرة، الذكاء الصناعي، والاختراقات السيبرانية المالية يعكس اتجاه إسرائيل نحو حرب هجينة شاملة متعددة الأبعاد.

استمرار هذا النمط من العمليات يُنذر بتصعيد مستمر في المواجهة، ويطرح تحديات كبيرة لإيران وحلفائها، خصوصًا في مجال حماية البنية التحتية الحيوية والمعلوماتية.

الهجمات السيبرانية الإيرانية ضد إسرائيل (2010–2025):

في ظل تصاعد المواجهة غير التقليدية بين إيران وإسرائيل، برز الفضاء السيبراني كساحة مركزية للصراع، تُمارس فيه طهران سياسات هجومية تهدف إلى تحقيق جملة من الأهداف الاستراتيجية دون الدخول في مواجهة عسكرية مباشرة. ومنذ عام 2010، وظّفت إيران – بشكل متزايد – قدراتها السيبرانية كأداة للردع والضغط، خاصة في ضوء القيود المفروضة على أذرعها العسكرية، والعقوبات الدولية التي حدّت من قدرتها على خوض صراعات مفتوحة.

وقد تطورت الهجمات السيبرانية الإيرانية بشكل ملحوظ من حيث التنظيم والاختراق والتأثير، مع توسع استهدافاتها من المنشآت الأمنية والعسكرية إلى البنية التحتية المدنية، مرورًا بالمستشفيات، وقطاعات المياه، والطاقة، ومؤسسات الإعلام وشركات التأمين. وتم تنفيذ هذه الهجمات إما بواسطة وحدات إلكترونية رسمية تابعة للحرس الثوري الإيراني، أو من خلال مجموعات قرصنة موالية مثل "بلاك شادو"، و"عصا موسى"، و"APT35"، بهدف الإرباك، والتجسس، والتشويش على الحياة العامة في الداخل الإسرائيلي، بل وأحيانًا للحصول على فدية.

وقد أظهرت هذه الهجمات تحولًا نوعيًا في العقيدة الإيرانية، التي باتت ترى في الفضاء الرقمي جبهة موازية للميدان العسكري، وسلاحًا فعالًا في زعزعة الجبهة الداخلية للخصوم وفرض قواعد اشتباك جديدة.

وفي هذا السياق، سيتم عرض أبرز الهجمات السيبرانية الإيرانية ضد إسرائيل خلال الفترة (2010–2025)، مرتبة زمنيًا، مع تحليل نوع الهجوم، والجهة المنفذة، وطبيعة الأهداف، والنتائج المترتبة، لفهم أعمق للوظيفة السياسية والأمنية التي تؤديها الحرب السيبرانية في الاستراتيجية الإيرانية تجاه إسرائيل.وامريكا1

(1) الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، أحمد بن على الميمونى، مجلة الدراسات الإيرانية، تصدر عن المعهد الدولى للدراسات الإيرانية، السنة الرابعة، العدد الثانى عشر، أكتوبر 2020، ص77.

جدول رقم(3)

يعرض الهجمات السيبرانية الإيرانية ضد إسرائيل خلال الفترة (2010–2025)

م	التاريخ	الدولة المستهدفة	الهدف	الجهة المنفذة	نوع الهجوم	أبرز النتائج
1	2011– 2013	أمريكا	47 بنكًا ومؤسسة مالية	قراصنة إيرانيون	DDoS	تعطيل وصول العملاء للحسابات، خسائر مادية
2	2013	أمريكا	سد مياه قرب نيويورك	خلايا إلكترونية إيرانية	اختراق نظام التحكم	فشل الهجوم بسبب فصل النظام للصيانة
3	2013– 2017	أمريكا ودول أخرى	جامعات ومؤسسات علمية (176 جامعة)	مجموعة إيرانية	تسلل وسرقة بيانات	سرقة 31 تيرابايت من الوثائق
4	2014	إسرائيل	مواقع عسكرية ومدنية أثناء "الجرف الصامد"	غير محددة	اختراق وتشويش	اختراق حساب وزير الدفاع – ضرر محدود
5	2014	أمريكا	شركة Sands Las Vegas	قراصنة إيرانيون	تعطيل أنظمة	خسائر كبيرة وتعطيل الخدمات
6	أبريل 2020	إسرائيل	شبكة المياه	غير محددة (نسبت لإيران)	اختراق أنظمة تحكم	محاولة تسميم المياه – أضرار محدودة2
7	مايو 2020	إسرائيل	مراكز أبحاث كورونا	قراصنة إيرانيون	هجوم تخريبي	بدون سرقة بيانات – أضرار محدودة
8	ديسمبر 2020	إسرائيل	شركة "شيربيت" للتأمين	Black Shadow	فدية وتسريب	تسريب آلاف الوثائق – طلب فدية مليون دولار
9	2021	إسرائيل	شركات دفاع ومستشفيات	عصا موسى / بلاك شادو	اختراق وتسريب وفدية	شلل بمستشفى، سرقة بيانات، 10 مليون $ فدية
10	ديسمبر 2021	إسرائيل	7 أهداف حكومية	APT35 (Charming Kitten)	استغلال ثغرة Log4j	محاولة اختراق – تم إحباطها3

(2) Raved, Ahiya, Cyber-attack targeted Israel's water supply, internal report claims, Ynet News, 24 April 2020. Availabe at: https://bit.ly/324oLlU

(3) الهجوم السيبراني الإيراني على إسرائيل.. خلفيات ودلالات https://ecss.com.eg/18961/#:~

خروج المواقع عن الخدمة – لا تسريبات مؤكدة	DDoS	غير محددة (نسبت لإيران)	مواقع حكومية (gov.il.)	إسرائيل	14 مارس 2022	11
نشر صور سليماني، رسائل تهديد	اختراق دعائي	بلاك شادو أو جهات موالية	منصات إعلامية	إسرائيل	يناير 2023	12

المصدر:4

أولًا: التحول في الأهداف

من الأهداف الاستراتيجية إلى الأهداف الحيوية والمدنية:

الهجمات في بداية العقد (2011–2014) ركزت على مؤسسات مالية أمريكية أو بنى تحتية محدودة.

بدءًا من 2020، توسعت إيران لاستهداف منشآت حيوية مدنية (مثل شبكات المياه في إسرائيل، والمستشفيات، وشركات التأمين)، ما يعكس تصعيدًا في محاولة الضغط على السكان المدنيين وإرباك الدولة.

استهداف البيانات والمعلومات الحساسة بدلًا من التدمير المادي فقط:

هجمات مثل تلك التي نفذتها مجموعتا "بلاك شادو" و"عصا موسى" ركزت على اختراق وسرقة وتسريب بيانات حساسة، ما يدل على تطور في طبيعة الحرب السيبرانية نحو "الحرب النفسية والمعلوماتية".

ثانيًا: تطور الوسائل والتكتيك

من هجمات بدائية (DDoS) إلى استخدام أدوات متقدمة (مثل استغلال ثغرات Log4j):

يمثل الانتقال من هجمات تعطيل الخدمة إلى هجمات باستخدام ثغرات "يوم الصفر" مؤشرًا على احترافية متزايدة وتقنيات متقدمة.

جماعات مثل APT34 وAPT35 تستخدم تقنيات تجسسية دقيقة تدل على وجود دعم مباشر من أجهزة استخباراتية إيرانية.

اللجوء المتزايد إلى هجمات الفدية (Ransomware):

كما حدث في الهجوم على مستشفى "هيليل يافه"، ما يكشف عن تشابك الأهداف المالية والسياسية في عمليات إيران ووكلائها.

ثالثًا: النتائج والتأثيرات

فعالية محدودة من حيث التدمير المباشر، لكن عالية من حيث التأثير الرمزي والسياسي:

معظم الهجمات لم تؤدِ إلى تدمير مادي كبير (باستثناء بعض التعطيلات المؤقتة)، لكنها نجحت في إثارة الذعر، وكشف ثغرات إسرائيلية وأمريكية.

نجاح تكتيكي لإيران في اختراق العمق المدني الإسرائيلي والأمريكي:

استهداف منشآت طبية، وشبكات مياه، وشركات خاصة، يظهر قدرة إيران على اختراق شبكات محمية نسبيًا.

تصعيد في "الردع السيبراني المتبادل" بين إيران وإسرائيل:

الهجوم على شبكة المياه الإسرائيلية (أبريل 2020) جاء بعد سلسلة هجمات منسوبة لإسرائيل على أهداف داخل إيران (مثل الموانئ والمنشآت النووية)، ما يدل على دخول الطرفين في حرب سيبرانية غير معلنة ولكن مستمرة.

(4) الفضاء السيبرانى كساحة لإدارة التنافس الإيرانى-الإسرائيلى حول النفوذ فى الشرق الأوسط، أميرة صديق، مجلة قضايا اسيوية، تصدر عن المركز الديمقراطى العربى للدراسات الإستراتيجية والسياسية والإقتصادية، (العدد 9، يوليو 2021)، ص125

ضعف واضح في جاهزية بعض القطاعات الإسرائيلية أمام الهجمات المعقدة:

الهجوم على مستشفى "هيليل يافه" كشف عن هشاشة في البنية التحتية السيبرانية الصحية، وأدى إلى اعتراف رسمي بعدم الجاهزية التامة.

استخدام الهجمات كأداة دعائية واستعراضية:

مثل اختراق "جيروزالم بوست" ونشر صور قاسم سليماني، ما يعكس استخدام الحرب السيبرانية كوسيلة رمزية للرد السياسي والمعنوي.

اتساع رقعة الحرب السيبرانية من المجال العسكري إلى المجالات المدنية والاقتصادية والصحية.

توظيف إيران لوكلاء سيبرانيين غير رسميين (مثل مجموعات القراصنة) يمنحها هامش إنكار مرن (Plausible Deniability).

الحرب السيبرانية باتت ساحة ردع استراتيجية جديدة موازية للردع النووي أو التقليدي، وذات آثار تدميرية مستترة وبعيدة الأثر.

تنامي التهديدات المستقبلية في ظل ضعف القوانين الدولية المنظمة للفضاء السيبراني.

جدول رقم (4) يوضح

الإطار التحليلي المقارن للهجمات السيبرانية الإسرائيلية والإيرانية (2010–2025)

محور المقارنة	إيران	إسرائيل	محور المقارنة
الطبيعة العامة للعمليات	هجومية انتقامية أو ردعية، تهدف إلى إرباك المؤسسات الإسرائيلية، وزعزعة الجبهة الداخلية، وتسجيل حضور سيبراني.	هجومية استباقية، دقيقة، تركز على إضعاف البنية التحتية الحساسة وعرقلة البرنامج النووي الإيراني.	الطبيعة العامة للعمليات
الجهة المنفذة	مزيج من جهات حكومية (الحرس الثوري) ووكلاء إلكترونيين (APT34، بلاك شادو، عصا موسى).	وحدات رسمية ضمن هيكل الدولة (الوحدة 8200 – الموساد السيبراني)	الجهة المنفذة
طبيعة الأهداف	شبكات المياه، المستشفيات، شركات التأمين، مواقع حكومية، مراكز بحث، أهداف مدنية.	منشآت نووية، موانئ، أنظمة طاقة، شبكات لوجستية، قواعد بيانات حساسة.	طبيعة الأهداف
أدوات التنفيذ	برمجيات فدية، هجمات تعطيل الخدمة (DDoS)، تسريب البيانات، التصيد الإلكتروني، استغلال ثغرات عامة مثل Log4j.	برامج اختراق متقدمة، أدوات زراعة برمجيات تجسسية، استغلال ثغرات معروفة وغير معروفة (Zero-Day).	أدوات التنفيذ
أهداف الهجوم	التأثير على الرأي العام الإسرائيلي، تعطيل الحياة اليومية، الضغط النفسي، الاستعراض الرمزي، أحيانًا الفدية المالية.	إضعاف القدرات النووية والعسكرية الإيرانية، خلق فوضى تنظيمية، جمع معلومات استخباراتية.	أهداف الهجوم
أثر الهجمات	أثر رمزي أو نفسي، وأحيانًا تعطيل جزئي (مثال: مستشفى هيليل يافه، تسريب بيانات شركة شيربيت).	أثر مباشر عالي التأثير (مثل تعطيل أجهزة الطرد المركزي في نطنز).	أثر الهجمات

التخطيط والتعقيد التقني	متفاوت، يشمل عمليات متقدمة وأخرى هواة أو مجموعات مرتزقة.	عالي التنظيم والسرية، بتنسيق استخباراتي – عسكري.	التخطيط والتعقيد التقني
الخطاب الإعلامي المرافق	دعاية سياسية وإعلامية مباشرة، إبراز الاختراق كإنجاز أيديولوجي أو وطني.	إنكار أو صمت رسمي في الغالب، مع تسريبات دقيقة عبر قنوات غربية.	الخطاب الإعلامي المرافق
تفاعل المجتمع الدولي	يُنظر إلى إيران كطرف مهدِّد للمنظومة السيبرانية، وتُدرج جماعاتها على قوائم المراقبة.	يُنظر إلى إسرائيل كقوة سيبرانية رائدة ضمن الحلف الغربي.	تفاعل المجتمع الدولي
سياق الصراع	امتداد للصراع الإقليمي والنووي، وساحة بديلة عن الحرب المباشرة.	جزء من سياسة ردع شاملة تشمل أذرعًا عسكرية ودبلوماسية واستخباراتية.	سياق الصراع

يُظهر هذا الإطار التحليلي أن الصراع السيبراني بين إسرائيل وإيران لم يعد مجرد مواجهات تكتيكية متفرقة، بل بات يُشكل ميدانًا استراتيجيًا موازٍ للمواجهات العسكرية والأمنية التقليدية. فبينما تميل إسرائيل إلى تبني استراتيجية الضربات الاستباقية النوعية بدقة استخباراتية عالية، فإن إيران تستخدم الحرب السيبرانية كأداة ردع غير متماثلة لتعويض ضعفها التقليدي، مركّزة على الاستهداف الرمزي والضغط النفسي والمعلوماتي5.

وبذلك، فإن الحرب السيبرانية بين الطرفين هي أحد أهم أشكال الصراع غير المتناظر في الشرق الأوسط، وهي مرشحة للاستمرار والتصاعد في ظل غياب قواعد دولية رادعة تنظم الفضاء السيبراني.

النتائج العملية

- فعالية نسبية للطرفين: نجحت إسرائيل في إحداث أضرار حقيقية في المنشآت الإيرانية (مثل نطنز وبندر رجائي)، بينما تمكنت إيران من اختراق مؤسسات إسرائيلية مدنية وتسريب معلومات حساسة.
- تحول الأهداف من عسكرية إلى مدنية: يدل على رغبة الطرفين في توسيع ساحة الصراع لتشمل المجتمع، بما يعزز "الردع الشعبي".
- تصاعد الهجمات الانتقامية: أصبحت الهجمات السيبرانية ردودًا مباشرة على عمليات ميدانية (مثل اغتيال سليماني أو استهداف علماء نوويين).
- توظيف الهجمات للفدية والإرباك الاقتصادي: كما حدث في الهجمات الإيرانية على مستشفيات وشركات تأمين إسرائيلية.

انعكاسات سيبرانية

أسهمت الهجمات السيبرانية الإسرائيلية الأخيرة في إضعاف قدرات إيران بشكل ملحوظ على الساحة الرقمية والعسكرية، حيث أدت إلى شلل جزئي في شبكات التوجيه والتحكم، ما أجبر طهران على تقليص حجم عملياتها الهجومية، خصوصًا فيما يتعلق بالصواريخ والطائرات المسيّرة.

كما تسببت هذه الهجمات في قطع قنوات الاتصال الآمن بين إيران وفصائلها الإقليمية، مثل "حزب الله" في لبنان و"أنصار الله" في اليمن، وهو ما عكس ارتباكًا في التنسيق العملياتي، وتراجعًا في مستوى التناغم الذي كانت تعوّل عليه طهران في المواجهات الإقليمية، وفقدت إيران في هذا السياق عنصر المفاجأة الاستراتيجي واضطرت إلى اتخاذ مواقف دفاعية محصورة ومحدودة التأثير، في وقت تتزايد فيه الخسائر الرقمية والاقتصادية التي تهدد قدرتها على إدارة الحرب والصمود فيها.

(5) - تداعيات التأثير السيبراني على قدرات إيران في المواجهة مع إسرائيل https://alqaheranews.net/news/132

الدلالات السياسية والاستراتيجية

- تآكل الخط الفاصل بين الحرب والسلام: فقد أصبحت الدول تستخدم الهجمات السيبرانية في أوقات "اللا حرب" لتحقيق مكاسب استراتيجية دون تكلفة دبلوماسية علنية.
- الحرب السيبرانية كأداة ردع بديلة: خصوصًا لإيران، التي توظفها لتعويض ضعفها التقليدي أمام التفوق الإسرائيلي التقني والعسكري.
- انعدام الإطار القانوني الدولي: ما يمنح الأطراف منفذًا للإنكار السياسي، ويصعّب تحميل المسؤوليات.
- إعادة تعريف الأمن القومي: أصبح يشمل حماية نظم المعلومات والبيانات والمؤسسات الرقمية لا الجغرافيا فقط.
- احتمالية التصعيد الخطر : في حال أفضت هجمات سيبرانية إلى أضرار بشرية أو بيئية جسيمة، قد يُستخدم ذلك كمبرر لرد عسكري، ما يعني تحول الصراع الرقمي إلى حرب شاملة.
- مدى تأثير الصراع السيبراني على الأمن الإقليمي والاستقرار الاستراتيجي
- أدى الصراع السيبراني إلى توسيع رقعة الصراع بين إسرائيل وإيران إلى خارج حدود الدولتين، مع إدخال أطراف إقليمية ودولية ثالثة في دائرة التأثر والتورط.
- أحدثت الهجمات اضطرابًا في مفهوم الردع الإقليمي، حيث أصبحت الدول تعتمد على "الرد غير المباشر" عبر أدوات إلكترونية بدلًا من المواجهة العسكرية.
- خلقت هذه الحرب بيئة هشة للأمن المعلوماتي في المنطقة، حيث باتت أي أزمة سياسية مرشحة للتطور إلى هجمات إلكترونية واسعة، مما يهدد البنية التحتية الحيوية للدول.
- كما أنها تعمّق الانقسام في الشرق الأوسط بين محورين تقنيين: محور متقدم (إسرائيل وداعموها الغربيون)، ومحور يسعى للحاق والاختراق (إيران وحلفاؤها)، مما يكرس عدم الاستقرار طويل الأمد.

النتائج

1- كشفت الفترة من 2010 إلى 2025 عن تصاعد غير مسبوق في وتيرة الهجمات السيبرانية بين إسرائيل وإيران، ما جعل الفضاء الرقمي ساحة مركزية للصراع الاستراتيجي بين الطرفين. استخدمت إسرائيل تفوقها التكنولوجي في تنفيذ هجمات استباقية استهدفت البرنامج النووي الإيراني والمنشآت اللوجستية، بينما وظّفت إيران الحرب السيبرانية كأداة ردع غير متماثلة لتعويض تفوق إسرائيل التقليدي، مستهدفة المؤسسات المدنية بهدف زعزعة الثقة الشعبية والإرباك الداخلي.

2- اتجهت إسرائيل نحو استهداف القدرات النووية والعسكرية بدقة واختراق عالي المستوى، كما في استخدام فيروس "ستاكس نت" لتعطيل منشأة نطنز، وعمليات الاغتيال التي استُخدم فيها الذكاء الاصطناعي. في المقابل، ركزت إيران على أهداف نفسية ورمزية وإعلامية، من خلال هجمات على شبكات المياه، والمستشفيات، وشركات التأمين، باستخدام أدوات مثل برامج الفدية، وهجمات حجب الخدمة (DDoS)، والتصيد الإلكتروني.

3 - عكست الهجمات تطورًا واضحًا في الأساليب والتكتيكات، حيث انتقل الصراع من اختراقات محدودة (2010–2014)، إلى هجمات مركّزة على البنية التحتية (2015–2021)، ثم إلى عمليات هجينة شاملة (2022–2025) تضمنت اغتيالات رقمية، وابتزازًا ماليًا، وضربات ميدانية منسقة.

4- أظهرت إسرائيل قدرة عالية على تنسيق الهجمات السيبرانية مع العمل الاستخباراتي والميداني، مما مكّنها من شل أنظمة حساسة داخل إيران. في المقابل، نجحت إيران في توسيع قدراتها من خلال مجموعات سيبرانية موالية شبه رسمية، مثل "بلاك شادو" و"عصا موسى"، والتي أتاحت لها هامشًا مرنًا للإنكار السياسي مع تنفيذ هجمات رمزية فعالة.

5 - حققت إسرائيل نتائج ملموسة على الأرض تمثلت في تعطيل شبكات الطاقة، والموانئ، ومنشآت تخصيب اليورانيوم الإيرانية، بالإضافة إلى إضعاف التنسيق بين إيران ووكلائها الإقليميين. في المقابل، أظهرت إيران براعة في اختراق بعض القطاعات المدنية الإسرائيلية وكشف هشاشة البنية الرقمية، لا سيما في مؤسسات الصحة والإعلام والتأمين.

6 - ساهم الصراع في تآكل الخط الفاصل بين حالة الحرب والسلم، حيث أصبحت الهجمات السيبرانية أداة لتحقيق مكاسب استراتيجية دون صدامات عسكرية مباشرة. كما أن غياب التشريعات الدولية المنظمة للفضاء السيبراني منح الطرفين مساحة واسعة للمناورة والإنكار، ما يعزز قابلية التصعيد دون تكلفة قانونية.

7 - لم يقتصر الصراع على إيران وإسرائيل، بل امتدت تداعياته إلى أطراف إقليمية (لبنان، اليمن، سوريا) ودولية (الولايات المتحدة)، مما أسهم في خلق مناخ دائم من التهديد للأمن المعلوماتي والبنية التحتية في المنطقة. كما عزز هذا الواقع الانقسام بين محور تقني متقدم تقوده إسرائيل، وآخر يسعى للاختراق والمشاغبة تقوده إيران، ما يزيد من هشاشة الاستقرار الإقليمي على المدى الطويل.

التوصيات

في ضوء ما توصلت إليه الورقة من نتائج، تبرز مجموعة من التوصيات التي يمكن أن تسهم في تعزيز الأمن السيبراني الإقليمي، وتقليل مخاطر التصعيد الرقمي في بيئة غير مستقرة:

1. رفع مستوى الحماية للبنية التحتية الحيوية، لا سيما في الدول العربية، مع التركيز على القطاعات الصحية، والمالية، والمائية، باعتبارها أهدافًا محتملة للهجمات السيبرانية غير المتناظرة.

2. تعزيز التعاون الإقليمي في مجال الأمن السيبراني، من خلال تبادل المعلومات الاستخباراتية، وتنسيق الدفاع الإلكتروني المشترك، لمواجهة التهديدات العابرة للحدود.

3. الاستثمار في التقنيات المتقدمة، خاصة أدوات الذكاء الاصطناعي، لتحسين قدرات الرصد والردع المبكر ضد الهجمات السيبرانية المعقدة.

4. الدفع نحو تبني إطار قانوني دولي، ينظم قواعد الاشتباك في الفضاء الرقمي، ويُحمّل الجهات المهاجمة، سواء كانت رسمية أو غير رسمية، المسؤولية القانونية والسياسية.

5. مراقبة نشاط الجماعات السيبرانية غير الرسمية، والحد من استخدامها كأدوات إنكار سياسي، لما تسببه من تعقيد في آليات الردع والمحاسبة الدولية.

6. تنفيذ برامج توعية شاملة، تستهدف الأفراد والمؤسسات، لتعزيز الثقافة الأمنية الرقمية، وتمكين المجتمعات من التصدي لمحاولات الاختراق والتضليل السيبراني.