Cyber warfare: its concept, tools, and implications for military power (The Iranian-Israeli cyber war as a case study)

Ola Marouf Yassmen *

(Received 7 / 6 / 2026. Accepted 9 / 9 / 2026)

□ ABSTRACT □

This research aims to clarify the concept of cyberwarfare, its tools, and its impact on military power. The research adopts a descriptive-analytical approach to describe concepts and interpret information related to cyberwarfare and cyber power, using Iran and Israel as a case study to understand this impact—by identifying the cyber power structure of both parties, military cyberattacks, and the reflection of modern technologies on military power and their uses by both sides. The research stems from the following question: How have technological developments, including cyber ones, influenced the course of the Iran-Israel war? The research aims to clarify the concept of cyberwarfare and its tools, elucidate the cyber power of both Iran and Israel and its reflection on their military power, and identify the implications of technological developments on the course of the Iran-Israel war. The descriptive-analytical approach was employed in this research. The research reached several conclusions, the most important of which are: cyberwarfare is characterized by the absence of geographical boundaries and low material cost; the use of technological developments in cyberwarfare is not limited to states but can also be employed by companies, organizations, and individuals; the objectives of such uses vary between data theft and destruction; Iran and Israel have established a technological base and entered a technological arms race aimed at protecting their political and security systems and attacking and destroying adversaries; modern technological developments have also reflected on conventional warfare and military power, as the Iran-Israel war has demonstrated qualitative developments in military and defensive warfare methods.

Keywords: Cyberwarfare, cyber tools, military power, the Iran-Israel conflict, cyberattacks.

Copyright **:**Latakia University journal (formerly tishreen) -Syria, The authors retain the copyright under a CC BY-NC-SA 04

* **Researcher - Master's degree in International Relations – Syria.** olayassmen@gmail.com

الحرب السيبرانية مفهومها أدواتها انعكاساتها على القوة العسكرية (الحرب السيبرانية الإيرانية_ الإسرائيلية نموذجاً)

علا معروف ياسمين*

(تاريخ الإيداع 7 / 6 / 2026. قُبِل للنشر في 9 / 9 / 2026)

□ ملخّص □

يهدف هذا البحث على توضيح مفهوم الحرب السيبرانية وأدواتها وتأثيرها على القوة العسكرية، ويتخذ هذا البحث المنهج الوصفي التحليلي لوصف المفاهيم وتفسير المعلومات المتعلقة بالحرب السيبرانية والقوة السيبرانية الإيرانية والاسرائيلية نموذجاً لفهم هذا التأثير، من خلال تحديد هيكل القوة السيبرانية لكلا الطرفين والهجمات العسكرية السيبرانية وانعكاس التقنيات الحديثة على القوة العسكرية واستخداماتها لكلا الطرفين. ينطلق البحث من التساؤل التالي كيف انعكست التطورات التكنولوجية بما فيها السيبرانية على مسار الحرب الإيرانية–الإسرائيلية؟ ويهدف البحث إلى توضيح مفهوم الحرب السيبرانية وأدواتها، وإيضاح القوة السيبرانية لدى كل من إيران وإسرائيل وانعكاسها على القوة العسكرية للطرفين، ومعرفة تداعيات التطورات التكنولوجية على مسار الحرب الإيرانية–الإسرائيلية. تم استخدام المنهج الوصفي التحليلي في هذا البحث. كما توصل البحث إلى نتائج أهمها ان الحرب السيبرانية تتصف بغياب الحدود الجغرافية وانخفاض التكلفة المادية، وان استخدام التطورات التكنولوجية للحرب السيبرانية لا تقتصر على الدول بل يمكن للشركات والمنظمات والأفراد استخدامها، وتتنوع أهداف هذه الاستخدامات ما بين سرقة البيانات أو تدميرها، أيضاً قيام إيران وإسرائيل بتشكيل قاعدة تقنية ودخول سباق التسلح التقني، تهدف إلى حماية النظام السياسي والأمني ومهاجمة الخصوم وتدميرهم، كما انعكست التطورات التكنولوجية الحديثة على الحرب التقليدية والقوة العسكرية، فالحرب الإيرانية الإسرائيلية أظهرت تطورات نوعية في الأساليب العسكرية الحربية والدفاعية.

الكلمات المفتاحية: الحرب السيبرانية، الأدوات السيبرانية، القوة العسكرية، الصراع الإيراني الإسرائيلي، الهجمات السيبرانية.

حقوق النشر : مجلة جامعة اللاذقية (تشرين سابقاً)– سورية، يحتفظ المؤلفون بحقوق النشر بموجب الترخيص CC BY–NC–SA 04

* باحث– ماجستير باختصاص العلاقات الدولية – سورية.olayassmen@gmail.com

مقدمة:

تُعد الحرب السيبرانية بعداً جديداً في مفهوم الحروب بين الدول فقد أفرزت التطورات التقنية تطورات كبيرة وهامة في كافة المجالات الاقتصادية والثقافية والسياسية والعسكرية، وانعكست على مسار الحروب التقليدية وخاصة في مجال التسلح والهجوم والدفاع، وبرز نوع من القوة عُرف بالقوة السيبرانية لدى الدول وظهر سباق التسلح التقني، وأثر على مقدرات الدولة العسكرية. كما أصبحت القوة والأدوات السيبرانية جزءاً من الحروب العسكرية وقوة الدولة وقدراتها. وظهر ذلك في العديد من الحروب بين الدول ومنها الحرب الإيرانية–الإسرائيلية التي استخدم فيها الطرفين الأدوات التكنولوجية في الحرب بينهما، مما غير مسار الحرب العسكرية التقليدية وانعكست على قوة الطرفين، ومن هنا تكمن أهمية البحث العلمية والعملية وأهدافه في معرفة مدى انعكاس القوة السيبرانية على مسار الحرب الإيرانية–الإسرائيلية.

الدراسات السابقة:

1- نبيلة قشطى، 2024، [1] بعنوان: الحرب السيبرانية وسبل مواجهتها. مجلة شؤون استراتيجية، العدد 17.

تناول البحث تحديد ماهية الحرب السيبرانية وأنماط هذه الحرب، بالإضافة لتحديد سمات الحرب السيبرانية وسبل مواجهتها.

استخدام البحث المنهج الوصفي التحليلي.

خلص البحث إلى نتائج أهمها ان الهجمات الإلكترونية أصبحت أهم الوسائل والتكتيكات المعتمدة بين الأطراف المتصارعة حول العالم، نظراً لتدني تكلفتها وزيادة الخسائر الناجمة عنها. وعززت الحرب السيبرانية من فرص الحرب اللا متماثلة؛ وذلك بتمكين دول متماثلة القوة شن هجمات ضد الدول ذات القوة العسكرية والاقتصادية الأكبر.

2- فتحي التريكي، 2025، [2] بعنوان: الحرب السيبرانية والأمن القومي تهديدات وتحديات مستقبلية. المجلة الأفروآسيوية للبحث العلمي، المجلد 3، العدد 3.

تناول هذا البحث الحرب السيبرانية من حيث المفهوم والأبعاد والتأثيرات، بالإضافة لمفهوم الأمن السيبراني ومفهوم الأمن من حيث العلاقة والتأثير. كما تتطرق لرؤية مستقبلية تحدد السيناريوهات المستقبلية للحرب السيبرانية.

تم استخدام المنهج الوصفي التحليلي في هذه البحث.

هدف البحث إلى تقديم صورة واضحة للحرب السيبرانية ومدى خطورتها على أمن الدول، وتحديد واقع الأمن في ظل التطور التكنولوجي واستخدام تقنية المعلومات في الحروب الحديثة، بالإضافة إلى وضع السيناريوهات المستقبلية للحرب السيبرانية.

خلص البحث إلى نتائج أهمها وجود علاقة وثيقة بين الأمن وأمن المعلومات "الأمن السيبراني" حيث أصبح من الضروري إدراج تقنية المعلومات في قواعد التدريب والدراسة للمجتمعات. كما إن الحرب السيبرانية تشكل تهديد للمستقبل في كل النواحي الحيوية، وعملية مواجهتها لا تقل أهمية عن مواجهة اي تهديد تقليدي.

3- هشام حمودي، 2025، [3] بعنوان: توظيف تقنيات الذكاء الاصطناعي في الحرب الإسرائيلية على قطاع غزة. المجلة العلمية لجهاز مكافحة الإرهاب، المجلد 5، العدد 9.

تناول هذا البحث التحول النوعي الذي شهده نمط القتال خلال الحرب الإسرائيلية على قطاع غزة عام 2023 بالاستخدام المكثف لتقنيات الذكاء الاصطناعي في العمليات العسكرية، والتركيز على الأبعاد العملياتية والاستخبارية لهذه التقنيات، وانعكاسها على طبيعة الاشتباك في البيئة الحضرية الكثيفة بالسكان، مثل قطاع غزة.

استخدام هذا البحث المنهج الوصفي التحليلي.

هدف البحث إلى توضيح تطبيقات الأسلحة الذكية في التخطيط الاستراتيجي العسكري للكيان الصهيوني، وانعكاس توظيف هذه الأسلحة على العمليات العسكرية.

توصل البحث إلى نتائج أهمها ان الكيان الصهيوني لديه قدرة متقدمة في دمج الذكاء الاصطناعي مع منظوماته العسكرية، مما عزز فعالية الضربات الجوية وخفف من الاعتماد على العمليات البرية. كما أدى الاعتماد على الأنظمة الذاتية إلى تقليص زمن القرار العسكري، لكنه أوجد تحديات فيما يخص دقة الاستهداف والمسؤولية الأخلاقية.

الدراسات الاجنبية

1-Chen Yao (2024).[22] "Iran-Israel Cyberspace Conflict: Evolution, Motivations and Impacts." *Journal of National Philosophy and Social Sciences*

دراسة صينية ، ترصد تطور الصراع منذ هجمة "ستوكسنت" عام 2010 وتصفه بأنه دخل "مرحلة احتدام". تحلل كيف حوّل الطرفان الفضاء السيبراني إلى ساحة جديدة للصراع الاستراتيجي، وتشير إلى أن هذا النزاع ساهم في تعزيز مستوى "الميكنة المعلوماتية" للقوات العسكرية لدى كلا البلدين، وبروز اتجاه "الحرب الهجينة" التي تدمج بين الهجمات السيبرانية والمواجهات العسكرية التقليدية.

2- Haroon, A. (2024). [23] "AI and Cyber Drove Warfare in the Israeli-Iran Conflict and its Impact on Gulf States' Security." *Journal of Politics and International Studies*

تتناول هذه الدراسة الدور المحوري الذي لعبته تقنيات الذكاء الاصطناعي والحرب السيبرانية في تشكيل مسار النزاع الإيراني–الإسرائيلي، مع تحليل لتداعيات هذا الصراع على أمن دول الخليج العربي.

أوجه الشبه والاختلاف بين الدراسات السابقة والدراسة الحالية

تتشارك الدراسات السابقة مع الدراسة الحالية في اعتماد **المنهج الوصفي التحليلي** كأداة رئيسية لفهم ظاهرة الحرب السيبرانية وتداعياتها، كما تتفق جميعها على أن الحرب السيبرانية تمثل تحولاً نوعياً في الصراعات المعاصرة، حيث تؤكد دراسات قشطى (2024) والتريكي (2025) على انخفاض تكلفتها وارتفاع خسائرها، وهو ما يتوافق مع ما تذهب إليه الدراسة الحالية من أن الحرب السيبرانية تتصف بغياب الحدود الجغرافية وتدني التكلفة المادية. غير أن الاختلاف الجوهري يكمن في أن الدراسات السابقة تناولت الموضوع **بشكل عام ونظري**، فركزت قشطى على سبل المواجهة، وركز التريكي على السيناريوهات المستقبلية والأمن القومي، بينما تتسم الدراسة الحالية بالتركيز **التطبيقي والموضوعاتي** من خلال دراستها لحالة محددة وهي الصراع الإيراني–الإسرائيلي، مما يمنحها عمقاً تحليلياً في فهم تأثير التطورات التكنولوجية على مسار حرب فعلية، وهذا الجدول يوضح تحليل SWOT و TOWS لتنظيم نقاط القوة والضعف والفرص والتهديدات بشكل مقارن بين الدراسة الحالية والدراسات السابقة:

المحور	الدراسة الحالية (الحرب السيبرانية الإيرانية–الإسرائيلية 2010–2024)	الدراسات السابقة (قشطى 2024، التريكي 2025، حمودي 2025)
نقاط القوة الداخلية (Strengths)	•تركيز تطبيقي على صراع حقيقي بين دولتين. •مقارنة منهجية بين قوتين سيبرانيتين (إيران وإسرائيل). •إطار زمني ممتد (2010–2024) يسمح برصد التطور. •ربط البعد السيبراني بالقوة العسكرية التقليدية. •تغطية أدوات سيبرانية متنوعة (ستوكسنت، دويل، فيروس شمعون، هجمات البنية التحتية).	•اعتماد المنهج الوصفي التحليلي. •تغطية أبعاد مستقبلية وأمنية شاملة (التريكي). •تطبيق عملي على حرب غزة (حمودي). •تقديم سبل مواجهة عملية (قشطى).

المحور	الدراسة الحالية (الحرب السيبرانية الإيرانية–الإسرائيلية 2010–2024)	الدراسات السابقة (قشطى 2024، التريكي 2025، حمودي 2025)
نقاط الضعف الداخلية (Weaknesses)	•تركيز محدود على طرفين فقط قد لا يعمم على صراعات أخرى. •صعوبة الحصول على بيانات دقيقة عن الهجمات السرية. •تغير التقنيات بسرعة قد يجعل بعض النتائج قابلة للتقادم. •تعقيد الفصل بين الهجمات السيبرانية والعمليات الاستخباراتية التقليدية.	•عمومية الطرح وعدم التخصص في حالة محددة. •قصر الإطار الزمني (حمودي اقتصر على 2023). •غياب المقارنة بين طرفين متخاصمين. •عدم ربط الحرب السيبرانية بشكل مباشر بتطور القوة العسكرية التقليدية.
الفرص الخارجية (Opportunities)	•إمكانية تعميم النموذج التحليلي على صراعات أخرى (الولايات المتحدة–الصين، روسيا–أوكرانيا). •الاستفادة من التقارير الدولية المفتوحةMandiant) ، .(CrowdStrike •إمكانية توسيع البحث ليشمل الردع السيبراني والدبلوماسية الدولية. •دراسة تأثير الحرب السيبرانية على الرأي العام والسياسات الدولية.	•وجود وعي متزايد بأهمية الأمن السيبراني عالمياً. •تزايد الاستثمارات في تقنيات الذكاء الاصطناعي والحرب السيبرانية. •إمكانية تطوير سياسات وطنية ودولية لمواجهة التهديدات. •توفر أدوات بحثية حديثة لتحليل الهجمات.
التهديدات الخارجية (Threats)	•صعوبة التحقق من صحة المعلومات الإيرانية والإسرائيلية حول الهجمات. •تصعيد الحرب السيبرانية إلى حرب شاملة قد يغير ملامح البحث أثناء إعداده. •تدخل أطراف ثالثة (الولايات المتحدة، روسيا) في المشهد السيبراني. •احتمالية تغيير استراتيجيات الطرفين بشكل مفاجئ.	•سرية المعلومات المتعلقة بالهجمات السيبرانية. •التطور السريع للتقنيات مما يصعب مواكبته. •غياب تشريعات دولية موحدة لتنظيم الحرب السيبرانية. •احتمالية تحيز المصادر لحساب أحد الأطراف.

أهمية البحث وأهدافه:

أهمية البحث:

تكمن أهمية البحث العلمية في دراسة قدرة التطورات التكنولوجية في تغير مسار الحرب العسكرية التقليدية وانعكاسها على قوة الدولة العسكرية، أم من الناحية العملية تكمن في إدخال التطورات التكنولوجية كأدوات جديدة في الحرب بين الدول، وبرز ذلك في الحرب الإيرانية–الإسرائيلية التي استُخدمت فيها التقنية العسكرية مما أفرز تطور كبير في مسار الحرب بينهما.

إشكالية البحث:

تبرز إشكالية البحث من خلال التساؤل الرئيسي التالي:

كيف أثرت التطورات التكنولوجية على مسار الحرب التقليدية بين الدول؟

يتفرع عن هذا التساؤل عدة تساؤلات فرعية:

1- ما هو مفهوم وطبيعة الحرب السيبرانية؟

2- ما هي الأدوات والقوة السيبرانية لدى كل من إيران وإسرائيل؟

3- كيف انعكست التطورات التكنولوجية بما فيها السيبرانية على مسار الحرب الإيرانية–الإسرائيلية؟

فرضيات البحث:

1- أثرت التطورات التكنولوجية على مسار الحرب العسكرية.

2- أفرزت الحرب السيبرانية بين إيران وإسرائيل تداعيات كبيرة في مفهوم القوة العسكرية.

3- ان الحرب السيبرانية أبرزت أدوات تقنية جديدة في الحرب الإيرانية–الإسرائيلية.

أهداف البحث:

1- التعرف على مفهوم الحرب السيبرانية

2- إيضاح القوة السيبرانية لدى كل من إيران وإسرائيل.

3- معرفة مدى انعكاس القوة السيبرانية على مسار الحرب الإيرانية-الإسرائيلية.

منهجية البحث:

تم استخدام المنهج الوصفي التحليلي، حيث اعتمد البحث على المنهج الوصفي في جمع وتصنيف المعلومات المتعلقة بالحرب السيبرانية والقوة السيبرانية والإسرائيلية، وتحليل تلك المعلومات وربطها بانعكاساتها على القوة العسكرية من خلال مقارنة الهجمات وأهدافها وفعالياتها.

الحدود الزمانية والمكانية:

يتناول هذا البحث الصراع السيبراني بين إيران وإسرائيل خلال الفترة الممتدة من عام **2010 إلى عام 2024**، حيث شهدت هذه الحقبة تحولاً نوعياً في استخدام الأدوات السيبرانية كسلاح استراتيجي في المواجهات غير المباشرة بين الطرفين. ويمتد الإطار المكاني للدراسة ليشمل كل من **الفضاء السيبراني الإيراني والإسرائيلي**، مع التركيز على البنية التحتية الرقمية للمؤسسات العسكرية والنووية والحيوية لكلا البلدين، بالإضافة إلى تحليل انعكاس هذه الهجمات على القوة العسكرية التقليدية في منطقة الشرق الأوسط، خاصة في ضوء التصعيد الذي شهدته المنطقة خلال هذه الفترة الزمنية.

المبحث الأول: مفهوم الحرب السيبرانية وأدواتها

ان التطورات التقنية أفرزت العديد من المفاهيم التكنولوجية والعديد من الوسائل التقنية الحديثة التي تستخدم في الفضاء السيبراني، وهنا برز مفهوم الحرب السيبرانية التي تتضمن العديد من الأدوات التقنية.

المطلب الأول: تعريف الحرب السيبرانية

لا شك ان الحرب السيبرانية أصبحت من المفاهيم الهامة التي برزت حديثاً بفعل التطورات التكنولوجية، مما استدعى تعريف هذه الحرب وتحديد مضمونها.

عُرفت الحرب السيبرانية بأنها امتداد للسياسة من خلال إجراءات وأفعال ترتكب في فضاء السايبر بواسطة الدولة أو الأطراف الفاعلة من غير الدولة والتي تشكل تهديداً خطيراً لأمن البلد أو تجري في استجابة لتهديد محتمل ضد أمن الدولة، أو هي تلك الإجراءات التي تتخذها الأطراف في النزاع لكسب الميزة على خصومهم في فضاء السايبر باستخدام مختلف الأدوات التكنولوجية والأشخاص التقنيين وتحصل المزايا من خلال إتلاف أو تدمير أو تعطيل أنظمة الحاسوب للعدو السيبرانية، أو من خلال الحصول على معلومات يرغب العدو في أن تبقى سرية. وفي تعريف أخر عرفت بأنها الاستعمال الدفاعي والهجومي للمعلومات وأنظمتها بقصد تعريض عناصر المعلومات والعمليات القائمة على المعلومات، والأنظمة المعلوماتية لشبكات الإنترنت التابعة للعدو في الفضاء السيبراني للخطر [16].

كما تُعرف بأنها عمليات في الفضاء الالكتروني، حيث تستخدم وسائل وأساليب قتال ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه. أيضاً أنها أحد أنماط الحروب الإلكترونية، وهي إجراء عسكري يتضمن استخدام الطاقة

الكهرومغناطيسية للتحكم في المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لاستخدام البيانات[10].

أيضاً أنها أعمال تقوم بها دولة ما تحاول من خلالها اختراق أجهزة الكمبيوتر لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها. أما منظمة التعاون الاقتصادية والتنمية فقد عرفتها كل فعل أو الامتناع من شأنه الاعتداء على الأصول المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن التدخل في التقنية المعلوماتية[8]. كما تُعرف بأنها استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية مدروسة داخل الفضاء الالكتروني بهدف التعطيل الفوري أو السيطرة علي موارد العدو [4] .

كما عرفت اللجنة الدولية للصليب الأحمر الحرب السيبرانية بأنها الأفعال التي يتخذها أطراف النزاع لتحقيق ميزة على خصومهم في الفضاء الالكتروني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على الطاقة البشرية من الناحية النظرية، ويمكن تحقيق المزايا عن طريق اتلاف أو تدمير أو اعطاب أو نهب أنظمة الحاسوب لدى الخصم "الهجوم السيبراني" أو بالحصول علي معلومات يفضل الخصم أن تبقي سرية "التجسس السيبراني" أو من خلال الاستغلال السيبراني [20] إذاً يتضح ان الحرب السيبرانية هي استخدام أطراف النزاع سواء دول أو أشخاص أو منظمات ومؤسسات لأحدث التقنيات التكنولوجية ضد خصومها بهدف سرقة البيانات أو تدميرها أو التجسس عليها، بشكل يهدد أمن المعلومات والبيانات.

المطلب الثاني: أدوات الحروب السيبرانية

ان الحرب السيبرانية تعتمد على استخدام العديد من البرامج والتطبيقات التقنية والفيروسات، كما تتنوع استخدامات هذه الأدوات ما بين سرقة البيانات أو تعطيلها، وتدمير الأجهزة أو توجيهها.

أولاً: القنابل المنطقية

هي نوع من الهجمات السيبرانية التيُ تُدخل سراً مجموعة من التعليمات في نظام حاسوبي أو تطبيق لإحداث ضرر، وتبدأ نشاطها باستيفاء شروط معينة، وما أنُ تُفعل تستطيع البرمجيات الخبيثة التي تحملها القنابل المنطقية أن تسبب مجموعة من العواقب، وهي تراوح من عواقب طفيفة نسبياً، مثل تباطؤ الكمبيوتر أو عدم إمكان الوصول إلى الملفات أو تلفها، إلى فقدان بيانات أو تعطل النظام. ولها القدرة على تعطيل البنية التحتية لتكنولوجيا المعلومات في المؤسسة بالكامل [9].

ثانياً: فيروسات الحاسب

هي فيروسات خبيثة يتم إنشاؤها عمداً؛ بهدف تغيير خصائص الملفات التي تصيبها؛ لتنفيذ بعض الأوامر لتعديلها أو إزالتها أو تخريبها، والغرض الرئيس منها هو التلف، سواء كان ضرراً مادياً متعلقاً بتدمير الأجهزة والأنظمة الإلكترونية، أو تلفاً رقمياً متعلقاً بمعلومات البرامج الأخرى لأنظمة تشغيل المعلومات [15].

مثال فيروس شمعون Shamoon وهو فايروس خبيث شديد التدمير يهدف إلى محو البيانات من الأنظمة المصابة، واستبدالها ببيانات جديدة. اكُتشف لأول مرة في إثر هجوم إيراني على شركة أرامكو السعودية الأمريكية في سنة 2012 ما أدى إلى تعطيل أكثر من30.000 جهاز كمبيوتر.

ثالثاً: الديدان

إنها برامج صغيرة لا تعتمد على برامج أخرى، ولكنها تتكاثر وتنسخ نفسها عبر الشبكات لتنفيذ هَجمات تخريبية، مثل قطع الاتصال بالشبكة أو سرقة بيانات بعض المستخدمين في أثناء تصفح الإنترنت، وتتميز بسرعة انتشارها، كما يصعب التخلص منها؛ نظراً لقدرتها العالية على التناسخ والمراوغة.

مثال **ستاكسنت Stuxnet** وهي دودة حاسوبية متطورة للغاية تستغل ثغرات أمنية غير معروفة سابقاً في نظام ويندوز، لإصابة أنظمة مستهدفة والانتشار في أنظمة أخرى.

رابعاً: أحصنة طروادة

هي برامج صغيرة مخبأة في برنامَج كبير من البرامج ذات الشعبية العالية، وتقوم ببعض المهام، مثل نشر دودة أو فيروس، وتتم برمجتها بمهارة عالية؛ لذلك لا يمكن الكشف عن وجودها، فهي تعمل دائماً على محو آثارها التي لا تحمل طابعاً مدمراً، وغالباً ما تعمل على إضعاف قوات دفاع الضحية لتسهيل اختراق الجهاز الخاص بالضحية وسرقة بياناته.

خامساً: دوكو Duqu

هو سلاح تحضيري يُجري عمليات استطلاع وتجسس وزرع معلومات في أنظمة العدو، ماُ يُسهل الاختراق والسرقة والتخريب والتدمير. اكتشف سنة 2011 في ثماني دول دفعة واحدة، وهي الهند وإيران وفيتنام والسودان وأوكرانيا وهولندا وفرنسا والسويد [9].

سادساً: التزييف العميق

هي عبارة عن إنشاء محتوى فيديو وصوت يتم من خلال انتحال شخصيات أخرى وتقديم معلومات مزيفة عن سلوكهم وأنشطتهم والبيئة المحيطة بهم، ومن خلال التزييف العميق يتم توليد صور أو مقاطع فيديو أو صوت أو نصوص مزيفة باستخدام أدوات التعلم الآلي المتقدمة، مما يؤدي إلى انتشار المعلومات المضللة على نطاقات ضخمة عبر الإنترنت، وهذا يمكن أن يقوض سلامة المعلومات ويقوض الثقة في مصادر الأخبار وقد يؤدي إلى قيام صناع القرار في مجال الأمن القومي إلى اتخاذ إجراءات فعلية بناء على معلومات خاطئة، مما قد يؤدي إلى أزمة كبيرة، أو أسوأ من ذلك الحرب [11].

يمكن القول من خلال ما تقدم أن أدوات الحرب السيبرانية وظفت كأسلحة غير تقليدية لتحقيق مكاسب استراتيجية دقيقة، حيث تُستخدم **هجمات التصيد والبرمجيات الخبيثة** لاختراق أنظمة الخصوم وسرقة أسرارهم الدفاعية والاقتصادية، بينما تُوظَّف **هجمات الحرمان من الخدمة (DDoS)** لشلّ البنى التحتية الحيوية كشبكات الكهرباء والمياه، مما يُضعف تماسك الدول من الداخل دون إطلاق رصاصة واحدة. كما تُستغل **منصات التواصل الاجتماعي وبوتات الذكاء الاصطناعي** في شنّ حروب نفسية وتضليل إعلامي، تعمل على زعزعة الثقة بالحكومات وإشعال الفتن الداخلية، بينما تُستخدم **أدوات التجسس الرقمي** لرصد تحركات القادة وكشف نقاط الضعف قبل أي مواجهة. وفي المقابل، تُوظَّف **أنظمة الحماية السيبرانية والذكاء الاصطناعي الدفاعي** لتحصين الشبكات وكشف الاختراقات، مما يحوّل الفضاء الإلكتروني إلى ساحة معركة موازية، حيث تُقاس الكفاءة بقدرة الدولة على توظيف هذه الأدوات هجومياً ودفاعياً في آنٍ واحد، لتحقيق تفوق استراتيجي يعيد تشكيل ميزان القوة لصالحها.

المبحث الثاني: أهداف الحرب السيبرانية وخصائصها

تتعدد أهداف الحرب السيبرانية التي تقوم بين الفواعل سواء دول أو غير دول، حيث تتراوح هذه الأهداف ما بين أمنية أو سياسية وعسكرية. كما تتميز الحرب السيبرانية بالعديد من السمات التي تجعلها ذات فاعلية في الاستخدام سواء من حيث التكلفة أو اختفاء الحدود الجغرافية وتقليل الخسائر البشرية.

المطلب الأول: أهداف الحروب السيبرانية

ان أهم أهداف الحرب السيبرانية هي البنية التحتية للمعلوماتية للقطاعات العسكرية والحكومية والاقتصادية، كما أن استهداف البيئة الثقافية والفكرية للحكومات والأفراد للخصوم وتغييرها يعتبر سلاح استراتيجي، وأداة هامة في الحروب الحديثة بين الدول المتحاربة. وقد تهدف هذه العمليات إلى القيام بأمور مختلفة، مثل التسلل إلى نظام حاسوب وجمع بيانات أو تصديرها أو إتلافها أو تغييرها أو تشفيرها، مثل إطلاق عمليات يسيطر عليها النظام المُتَسلل إليه أو تبديلها أو التلاعب بها، وفي بعض الظروف لا يقتصر أثرها على بيانات نظام الحاسوب أو الحاسوب المستهدف بل ترمي في الواقع عادةً إلى إحداث أثر في العالم الحقيقي.

كما يمكن للفاعل السيبراني تحقيق مكاسب عسكرية أو سياسية ضد عدو ما. ومن ثم يمكن تشبيه الحرب السيبرانية بأنها نوع من أنواع الإرهاب، ولكنه إرهاب إلكتروني والذي يقصد به استخدام شبكة الإنترنت والشبكة المعلوماتية من أجل استهداف أمن الدول وبناها التحتية، وحتى الأشخاص، من أجل تحقيق أهداف سياسية أو اقتصادية. أيضاً تدمير واسع النطاق للبنى التحتية والاقتصادية بما فيها البنى الإلكترونية للدولة المستهدفة.

المطلب الثاني: خصائص الحروب السيبرانية

تعتبر الحرب السيبرانية حرباً رقمية متطورة؛ فقد شكلت ثورة المعلومات المتطورة وسيلة محورية للحرب السيبرانّية، وأصبحت الميدان الرئيسي لها، وتتميز بأّنها ذات مصاريف مالّية منخفضة، بخلاف الحرب التقليدّية؛ فهي لا تحتاج لتكاليف ضخمة لتصنيع أسلحتها مقارنة بالأسلحة الفتاكة ذات التكاليف الباهظة. كما تمنح المهاجم أفضلّية واضحة في حروب الإنترنت على المدافع، فالحروب السيبرانّية تتميز بالسرعة والمراوغة والمرونة في بيئة مماثلة يظهر فيها المهاجم بأفضلّية من الصعب على عقلّية التحصن لوحدها ان تنجح.

ان الحروب السيبرانية، تدور معاركها في الفضاء السيبراني وبين خصوم مجهولين غالباً في الفضاء السيبراني، ولا تكون الدول المتحاربة بالضرورة على قدم المساواة اقتصادياً وعسكرياً، وقد تتفوق الدول الأضعف عسكرياً على الدول الأقوى في الفضاء السيبراني من ناحية كثافة الهجمات. كما تفتقر هذه الحروب أيضاً إلى نموذج الردع الشائع في الحروب التقليدية، إذ يعتمد الردع في الأخيرة على العقاب والانتقام من المهاجم، فيسعى الطرف المهاجم لتدمير مواقع إطلاق الصواريخ، بوصف ذلك صورة من صور العقاب أو الردع. أما في الحروب السيبرانية، فيصعب تحديد مواقع إطلاق الهجمات، وحتى لو كان ذلك ممكناً، فإنه قد يستغرق شهوراً أو سنوات في بعض الحالات.

بالإضافة لذلك تتميز الحرب السيبرانية، من منظور استراتيجي بغياب التسلسل الهرمي التقليدي للقيادة، إذ لا تعتمد على الصورة التقليدية للقيادة العسكرية أو الإدارة الحكومية، ويصعب التمييز بين العملين العسكري والسياسي، ولا توجد خطوط فاصلة واضحة بين المدنيين والعسكريين [13].

أما على مستوى الفاعلين فقد تركت حروب الفضاء الإلكتروني تأثيرات هامة في طبيعة المواجهات، حيث بات بالإمكان أن يكون هناك أطراف فاعلة من غير الدول، إذ أن الأسلحة المستخدمة في هذه الحروب ليست حكراً بيد الدولة، وبحيث بات يتردد الوصف لحروب الفضاء الإلكتروني بأنها حروب غير تناظرية.

بالإضافة لذلك تميز حروب الفضاء الإلكتروني عن الحروب التقليدية، بأنه لا توجد حدود جغرافية واضحة في هذه الحروب. كما لا يتواجد مفهوم" السيادة "بمعناه السائد في العالم الواقعي، بحيث يتم منع الأطراف الأخرى من الدخول إلى المناطق الخاضعة لسيادة دولة ما مثلاً. بل إنه بالإمكان وصف الحدود في الفضاء الإلكتروني بأنها حدود مائعة. فإنه لا توجد حدود في العالم الافتراضي، إذ أن الحدود تتداخل مع بعضها، حيث أن كل الدول صغيرة وكبيرة، تشترك في نفس الشبكات، التي يمكن اعتبارها بمثابة سحابة واحدة.

يتضح مما سبق ان الحرب السيبرانية لها العديد من الأهداف ما بين اقتصادية ومالية وسياسية وعسكرية تشمل سرقة البيانات أو إتلافها أو تعطيل الأنظمة والحواسيب. كما تتميز هذه الحرب بسمات مثل تلاشي الحدود الجغرافية وانخفاض التكلفة المادية وعدم اقتصار الفاعليين على الدول بل تشمل الأفراد والمؤسسات.

إذاً أصبح الحرب السيبرانية من أهم وأخطر الحروب كونها تعتمد على تقنيات وبرمجيات أصبح بإمكان العدد من الدول والمؤسسات امتلاكها واستخدامها، مما يهدد البنية التحتية للبيانات والأنظمة، ويشكل خطراً على أمن الدول والمؤسسات والأفراد.

المبحث الثالث: أهداف وهيكلية الحرب السيبرانية بين إيران وإسرائيل

شكل الفضاء السيبراني بيئة مناسبة يمكن من خلالها استهداف الخصوم وتهديد أمنهم، مما وسع من نطاق الحروب العسكرية التقليدية وتم ادخال التقنيات الحديثة في الحرب العسكرية بين الدول. وهذا ما حدث في الحرب الإيرانية الإسرائيلية حيث تم استخدام الأدوات والتقنيات التكنولوجية الحديثة في الحرب العسكرية بينهما.

المطلب الأول: أهداف الحرب السيبرانية الإيرانية الإسرائيلية

شملت أهداف إسرائيل من الحرب السيبرانية على إيران شّل البنية التحتية الإيرانية النووية واللوجستية وجمع المعلومات الاستخباراتية، بالإضافة لردع القدرات الإيرانية ومنع تصعيدها الإقليمي، والحفاظ على تفوق إسرائيل التقني [12].

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 جزءاً مما يُعرف بـ "حرب الظل" بين الجانبين، وهي حرب غير تقليدية، تدور خارج أطر الصدام العسكري المباشر، وتُستخدم فيها أدوات رقمية عالية الدقة، وتُنفّذ غالباً من خلال أجهزة استخبارات متخصصة، في مقدمتها الموساد ووحدة 8200 التابعة للاستخبارات العسكرية الإسرائيلية.

أما أهداف إيران من الحرب السيبرانية على إسرائيل تمثلت في التأثير على الداخل الإسرائيلي نفسياً وسياسياً، بالإضافة لإرباك المؤسسات الحيوية والمدنية، وتقويض ثقة الجمهور بالحكومة الإسرائيلية وأيضاً خلق أدوات ردع غير متماثلة في مواجهة التفوق الإسرائيلي.

كما تسعى إيران إلى التشويش واختراق أنظمة القيادة والسيطرة الإسرائيلية، والحصول على معلومات أمنية حساسة [14].

إذاً تنوعت أهداف إيران وإسرائيل من الحرب السيبرانية ما بين سرقة البيانات الحكومية الرسمية وتدمير أنظمة التشغيل وتدمير البنية التحتية التقنية وامتلاك أدوات التفوق التقني ومنع الخصم من امتلاكها والتفوق فيها.

المطلب الثاني: القوة السيبرانية الإيرانية– الإسرائيلية

ان الحرب السيبرانية تعتمد وجود بنية تحتية تقنية ومعلوماتية ووجود هيكلية قيادية تقود هذه الحرب وتتحكم بها، لذلك تتطلب هذه الحرب وجود مؤسسات وشركات متخصصة تمتلك هذه التقنيات وقادرة على إدارة هذه الحرب.

أولاً: القوة السيبرانية الإيرانية

عملت إيران على بناء مؤسسات تكنولوجية بهدف امتلاك أدوات وتطبيقات تقنية حديثة تمهد لدخولها لسباق التسلح التكنولوجي بين الدول، وقد استطاعت إيران من الحصول على هذه التقنيات وتطويرها، وأصبحت من الدول الهامة في مجال تطوير التكنولوجية وتطبيقاتها.

1. مركز التحقيق في الجريمة المنظمة

يعرف أيضاً باسم مكتب مكافحة الجرائم السيبرانية، وقد أسسه الحرس الثوري في سنة 2007، ليتبع له مباشرة. مهمته ضمان أمن الفضاء السيبراني وحماية الحكومة الإلكترونية في إيران. لقد ساعد المركزُ الحكومةَ، في أثناء الانتخابات الرئاسية الإيرانية في سنة 2009، عبر حجب المواقع الإلكترونية للمعارضة وتحديد هوية نشطائها.

2. المجلس الأعلى للفضاء السيبراني

لقد تم أنشأ هذا المجلس في سنة 2011 بأمر من علي خامنئي بهدف تنسيق الجهود في مجال الدفاع والهجوم السيبرانيين، ويضم في عضويته كبار المسؤولين في الأجهزة الأمنية والاستخباراتية ووزراء الثقافة والاتصالات[7].

3. المركز الوطني للفضاء السيبراني

أنشئ المركز بقرار من المجلس الأعلى للفضاء السيبراني بهدف تطوير القدرات السيبرانية لإيران، وتقليل اعتمادها على الإنترنت من الدول الأخرى، وتطوير محتوى يدعم الفكر الديني الرسمي للبلاد، وشن حرب ثقافية إلكترونية ضد الدول المعادية. كما يُطلق المركز حملات توعية للمواطنين لتشجيعهم على حماية مواقعهم الشخصية، وكذلك المواقع الحكومية والرسمية، من الهجمات السيبرانية.

4. قوة الباسيج السيبرانية

أسست قوة الباسيج منذ مطلع العقد الثاني من الألفية الجارية وحدات خاصة تعنى بمواجهة القوى المعادية لإيران. وفي عام 2019 أعلنت عن تعزيز قدرات قوة الباسيج السيبرانية عبر استحداث كتائب سيبرانية تماشياً مع التحديات التي تواجه بلاده في الفضاء السيبراني.

5. الحرس الثوري الإيراني

بالإضافة إلى وحدات الحرب الإلكترونيّة، يوظف الحرس الثوريّ الإيرانيّ مجموعات من المتسللين الإيرانيين النشطين في الداخل والخارج، لإخفاء أنشطته الإلكترونيّة، ودحض أيّ مزاعم بتورط إيران في حرب الفضاء والجرائم الإلكترونيّة، ويتعاون معَ الحرس الثوريّ فريق Ashiyane Digital Security لتدريب المتسللين إلى العمل في مجالات السياسة والدعاية الموالية لإيران على مواقع ومنتديات الشبكات الاجتماعية الغربية و(الإسرائيليّة)، والتسبب في أعطالهم، بالإضافة إلى الاحتيال الائتماني، والتسلل إلى قواعد البيانات والمؤسسات المالية.

الجيش السايبيري الإيراني

يقدر عدد أفراده بـ 2500 فرد، وتخصص له ميزانية سنوية تقدر قيمتها بنحو 80 مليون دولار أمريكي، ويقوم هذا الجيش بمهام داخلية تهدف أساساً إلى حماية النظام السياسي القائم، وأخرى خارجية تتمثل أساس في القيام بهجمات سيبرانية ضد أهداف حيوية للدول المعادية لإيران.

يمكن القول ان إيران قامت بتهيئة بيئية تحتية معلوماتية وتقنية ليس فقط بهدف امتلاك أدوات التكنولوجيا وتطويرها ودخول سباق التسلح الإلكتروني، بل أيضاً بهدف حماية نظامها السياسي والاقتصادي والأمني ومهاجمة خصومها وتدميرهم.

ثانياً: القوة السيبرانية الإسرائيلية

تمتلك إسرائيل العديد من الأدوات التكنولوجية التي تستخدمها في محاربة خصومها، ولديها العديد من المؤسسات والوحدات السيبرانية التي تتبع للجيش الإسرائيلي وتستخدم في العمليات العسكرية.

1. الوحدات العسكرية المتخصصة

تضم الهيئة الرسمية لحماية المعلومات تم إنشاء الهيئة في عام 2002، لتعمل في إطار قانون الشاباك، وتقوم بتوجيه المنشآت التي تعد أساسيّة في مجال أمن الحواسيب وحماية الشبكات، وتشرف على تطبيق حماية المعلومات، كما أنّها مخولة باتخاذ إجراءات عقابيّة ضد المؤسسات التي تخترق تعليماتها.

أيضاً **الوحدة 8200** التي تعد أهم وحدة استخبارات سيبرانية في الجيش الإسرائيلي، وهي مسؤولة عن جمع وتحليل المعلومات الإلكترونية، وتنفيذ عمليات هجومية ضد الخصوم التي تُنتج كوادر سيبرانية تُؤسس شركات مثل NSO Grou مطورة برنامج بيغاسوس، **والوحدة 81** المتخصصة في تطوير أدوات الهجوم السيبراني والذكاء الاصطناعي لأغراض عسكرية، مسؤولة عن الهجمات السيبرانية الهجومية. بالإضافة إلى **القيادة السيبرانية الإسرائيلية** التي تأسست عام 2017 للإشراف على العمليات السيبرانية الدفاعية والهجومية [19].

2. المؤسسات المدنية والحكومية

مثل **المديرية الوطنية للأمن السيبراني** التي تتولى مسؤولية حماية الفضاء السيبراني كله، وبناء القوة السيبرانية الإسرائيلية وتطويرها، وتعمل على التحسين المستمر لمستوى حماية المؤسسات والأفراد، ومنع الهجمات السيبرانية ومواجهتها، وتعزيز قدرات الاستجابة للطوارئ. تصدر تقيماً سنوياً لحالة الأمن السيبراني في إسرائيل، وأهم المخاطر التي قد تواجهها، وكيفية التصدي لها. أيضاً **المركز الوطني للسايبر** الذي يهدف إلى تطوير الأبحاث والابتكارات في مجال الأمن السيبراني.

3. فيلق الأمن السيبراني الموحد

أسسه في سنة 2015 قائد سابق في الجيش، وهو غادي آيزنكوت، بهدف توحيد خبرات الجيش السيبرانية تحت مظلة واحدة. جاء ذلك بعد تزايد التهديدات السيبرانية للجيش الإسرائيلي، خاصةً من إيران. وأن هذا الفيلق سيواجه التهديدات السيبرانية المحتملة وخاصة الهجمات الإيرانية وتشمل مهمته أيضاً إدارة العمليات السيبرانية الدفاعية والهجومية في الفضاء السيبراني العسكري، بما يتماشى مع احتياجات الأمن القومي.

4. الوحدة 433

تابعة للشرطة الإسرائيلية وتضم أقساماً مختلفة، بما في ذلك قسم الأمن السيبراني الذي يتخصص في التجسس لدعم الملاحقات الأمنية.

القبة السيبرانية الإسرائيلية

تعمل إسرائيل على تطوير نظام دفاع إلكتروني تطلق عليه اسم "القبة السيبرانية"، تشبه القبة السيبرانية درعاً رقمياً يواجه الهجمات السيبرانية، باستخدام الذكاء الاصطناعي والتعاون الدولي للكشف عن التهديدات الآنية. يحلل الذكاء الصناعي

بيانات متنوعة لتحديد التهديدات السيبرانية المحتملة وتوقيت حدوثها. تشارك هذه المعلومات جهات مختصة من قطاعات مختلفة ذات فهم عميق للأمن السيبراني، فما أن يحدد التهديد يُصدر فريق الاستجابة السيبرانية الأمر باتخاذ الإجراءات الملائمة. كما تسعى إسرائيل لتوسيع شبكتها السيبرانية الدولية، من خلال تبادل المعلومات مع الدول، بهدف بناء شبكة دفاع سيبراني إقليمية.

5. **التعاون مع القطاع الخاص**

تعتمد إسرائيل على التعاون الوثيق مع الشركات التكنولوجية الكبرى مثل Check Point و NSO Group، التي تطور أدوات سيبرانية متقدمة تُستخدم في الأمن والدفاع والاستخبارات.

يمكن القول من خلال ما سبق ان إسرائيل عملت على بناء قوة سيبرانية اعتماداً على أدوات تكنولوجية متطورة، تهدف إلى حماية الأمن الإسرائيلي وقواعد البيانات وأيضاً استخدامها عسكرياً في محاربة خصومها وتحقيق ميزة عسكرية متطورة.

المبحث الرابع: طبيعة الحرب السيبرانية الإيرانية الإسرائيلية وانعكاساتها

ان التطورات التقنية الحديثة أفرزت استخدامات جديدة في كافة المجالات ومنها العسكرية والأمنية، وهو ما تم استخدامه في الحرب السيبرانية الإيرانية الإسرائيلية التي تم فيها دمج الحرب التقليدية بالتطورات التكنولوجية، حيث استخدم فيها شتى أنواع البرمجيات والتطبيقات العسكرية الحديثة سواء من حيث التخطيط أو التوجيه والاستهداف العسكري في هذه الحرب.

المطلب الأول: الهجمات السيبرانية الإيرانية الإسرائيلية

لا شك ان الهجمات التي شنها كل من الطرفين إيران وإسرائيل ضد بعضهما، تمت بأحدث التقنيات والأساليب العسكرية المتطورة، وهذا يدل على وجود تطورات تقنية بشكل عام وعسكرية بكل خاص لدى الطرفين.

أولاً: الهجمات الإسرائيلية

تُستخدم القدرات السيبرانية الإسرائيلية بشكل مكثف في العمليات الاستخباراتية والهجمات الإلكترونية ضد الأعداء الإقليميين، فعلى سبيل المثال، تُعد الهجمات على المنشآت النووية الإيرانية، كهجوم "ستوكسنت" 2010 نموذجاً لاستخدام الفضاء السيبراني لإعاقة البرامج العسكرية للخصوم، كما تشير تقارير إلى تورط وحدات إسرائيلية في اختراق شبكات مراقبة تابعة لمنظمات كحماس وحزب الله، بهدف تعطيل عملياتهما أو جمع معلومات استخباراتية حساسة.

في سنة 2011، استُهدفت مؤسسات حكومية إيرانية بفيروس دوك، ثم في سنة 2012 استُهدفت وزارة النفط الإيرانية بفيروس فليم الذي كان يهدف إلى سرقة المعلومات ومحوها، وقد أدى هذا الهجوم إلى تعطيل خوادم الوزارة وخوادم أربع شركات تابعة لها.

في سنة 2013، تعرض موقع الباسيج الإيراني لهجوم، بهدف تعطيله بالكامل، ويُعتقد أن إسرائيل كانت وراء الهجوم في سنة 2015، هاجم قراصنة إسرائيليون أجهزة كمبيوتر في ثلاثة فنادق أوروبية يقيم فيها أعضاء الوفود المكلفة بالتفاوض بشأن الملف النووي الإيراني، وكان الهدف جمع معلومات عن الفعالية والمشاركين فيها.

كما استولى الموساد على وثائق نووية سرية عبر 20 عميلاً داخل إيران. وهي عملية تجسس ميداني واختراق استخباراتي داخل طهران، بهدف سرقة الأرشيف النووي الإيراني عام 2018. أيضاً أحدث تفجير في المنشأة النووية أدى إلى دمار كبير، وهو ما يعد تخريب داخلي سيبراني في منشأة نطنز النووية عام 2020. وتم باستخدام رشاش

مثبت على شاحنة ويتحكم به عن بعد. بالإضافة لعملية اغتيال ذكي عبر الذكاء الاصطناعي في طهران، حيث تم اغتيال محسن فخري زاده عام 2020.

كما تعرضت إيران لهجوم إلكتروني كبير استهدف 4300 محطة وقود في مختلف المدن الإيرانية في تشرين الأول 2021، ما تسبب في حدوث خلل كبير في توزيع الوقود لعدة أيام.

أيضاً الهجوم على ميناء رجائي الإيراني الذي شلَّ حركة النقل لثلاثة أيام استهدفت محطات الوقود الإيرانية 2021.

في 13 حزيران 2025 نفذت إسرائيل عملية عسكرية واسعة النطاق حملت عنوان "الأسد الناهض" هدفت إلى تحطيم البنية الاستراتيجية الإيرانية سواء العسكرية أو السياسية، فقد استهدفت الغارات مواقع تصنيع الصواريخ والمسيرات كما استهدفت مراكز نووية الحساسة في نطنز وفوردو وآراك، تم اغتيال قيادات هامة في الحرس الثوري الإيراني وعلماء نوويين [21].

بالإضافة لهجوم جوي وصاروخي واسع استهدف منشآت نووية وقيادات عسكرية، حيث تم اغتيال 6 من كبار القادة العسكريين بصواريخ ومسيرات، بالتوازي إلى سرقة بيانات 42 مليون عميل في هجوم سيبراني وابتزاز مالي حيث تم اختراق بنك "سباه "الإيراني 2025، وتدمير 90 مليون دولار من الأصول في هجوم سيبراني مالي استهدف البنية الرقمية ونقلها لمحافظ خارجية واختراق بورصة Nobitex للعملات الرقمية.

إذاً يتضح ان الهجمات السيبرانية الإسرائيلية على إيران استهدفت بنك واسع من الأهداف شمل الوزارات والمنشآت النووية، وتم دمج القدرات العسكرية بالتطورات التقنية من خلال استخدام الطائرات المسيرة والصواريخ الموجهة، وهدفت إلى تدمير البنية التحتية للمنشآت النفطية وأيضاً النووية وتعطيلها، بالإضافة لهجمات استهدفت سرقة البيانات الرسمية وابتزاز مالي.

ثانياً: الهجمات الإيرانية

لا شك ان الهجمات الإسرائيلية على إيران استدعى رداً إيرانياً مماثلاً، تمثل في استخدام التكنولوجية في الحرب العسكرية، وأيضاً عمليات التجسس والاختراق وسرقة البيانات.

فالرد الإيراني على الهجمات الإلكترونية الإسرائيلية، كان أوله هجوم إلكتروني ضد أهداف إسرائيلية حتى سنة 2009، عندما شنت إيران سلسلة من الهجمات الإلكترونية استهدفت القطاع المصرفي الإسرائيلي بصورة خاصة وتزامنت هذه الهجمات مع حرب غزة. وفي سنة 2012، نُسبت إلى إيران مسؤولية هجوم سيبراني استهدف 54 مسؤولاً إسرائيلياً، بمن فيهم موظفو سفارات، وكان الهجوم يهدف إلى سرقة وثائق ومعلومات. وفي نيسان 2020 تعرضت منشآت تابعة لسلطة المياه الإسرائيلية لهجوم، وفي 16 آذار من العام نفسه، تمكنت المخابرات الإيرانية من اختراق هاتف السياسي الإسرائيلي بيني غانتس، وهو زعيم حزب أزرق أبيض الذي كان في ذلك الوقت أقوى منافس لرئيس الوزراء الإسرائيلي بنيامين نتنياهو.

بالإضافة لمحاولة تسميم المياه واختراق أنظمة تحكم شبكة المياه في إسرائيل عام 2020، بدون سرقة بيانات أيضاً هجوم تخريبي تسبب بأضرار محدودة في مراكز أبحاث كورونا إسرائيل في نفس العام. بالإضافة لتسريب آلاف الوثائق وطلب فدية مليون دولار لشركة شيربيت للتأمين عام 2020. أيضاً هجوم هدف إلى اختراق وتسريب بيانات وفدية 10 مليون دولار لشركات دفاع ومستشفيات إسرائيل عام 2021. وهجوك أدى إلى خروج مواقع حكومية إسرائيل عن الخدمة عام 2022.

كما أنه في أعقاب اندلاع الحرب في غزة في تشرين الأول عام 2023، زادت حدة الهجمات الإلكترونية بين إيران وإسرائيل، ووفقاً لتقرير صادر عن مايكروسوفت، كثفت إيران عملياتها السيبرانية ضد إسرائيل، منذ بدء الحرب الإسرائيلية على غزة، وكانت العمليات التي تمكنت مايكروسوفت من رصدها تستهدف في جزء كبير منها شركات إسرائيلية.

يُلاحظ ان إيران قامت بشن حرب سيبرانية ضد إسرائيل استخدمت فيها أبرز الأدوات والتطبيقات التقنية استهدفت من خلالها القطاع المصرفي وسرقة البيانات والحسابات، وسرقة البيانات الحكومية الإسرائيلية بالإضافة للبنية التحتية للمنشآت الإسرائيلية وإخراج المواقع الرسمية عن الخدمة وتعطيل شبكات الإنترنت والاتصالات.

المطلب الثاني: انعكاسات الحرب السيبرانية على القوة العسكرية الإيرانية – الإسرائيلية

تعد العلاقة بين القوة السيبرانية والقوة التقليدية علاقة تكاملية وتنافسية في آن معاً. فالقوة السيبرانية رغم طابعها الافتراضي، إلا إنها عنصر أساسي في دعم أدوات القوة التقليدية وخاصة بعدما أصبحت معظم الأدوات التقليدية ذات وجه رقمي يمكن التحكم بها عن بعد ولاسيما القدرات العسكرية، فأصبحت القوة السيبرانية تعزز القوة العسكرية لا سيما في الحرب الهجينة أو الذكية لجمع المعلومات الاستخباراتية، والتحكم بالأسلحة الذكية، والطائرات المسيرة، وخاصة بعدما أصبحت العمليات السيبرانية جزءاً من الاستراتيجية العسكرية الشاملة [18].

فأصبح هناك نمط آخر من الحروب السيبرانية يتمثل في تحويل الصراع عبر الفضاء الالكتروني كساحة موازية أو مرافقة أو مرتبطة لحرب تقليدية دائرة على الأرض، نوع من الحروب وفقاً لأثارها المدمرة من خلال اختراق العمليات العسكرية عالية التقنية أو استهداف الحياة المدنية أو البنية التحتية بالشكل الذي يمكن تصوره إلا ان هناك نماذج لتلك الحروب تتمثل على شكل رسائل تهديد مصحوبة بآثار محدودة جراء تلك الهجمات[6].

كما يظهر أن إسرائيل نجحت في تطوير تكامل عالي بين القدرات السيبرانية الاستخباراتية والعسكرية الميدانية، مما جعلها قوة فاعلة في فرض قواعد الاشتباك في منطقة الشرق الأوسط. حيث انتقلت من عمليات تجسس واختراق إلكتروني إلى هجمات مسلحة معقدة واغتيالات ذكية، واستغلال التكنولوجيا الحديثة مثل الطائرات المسيرة، الذكاء الصناعي، والاختراقات السيبرانية المالية يعكس اتجاه إسرائيل نحو حرب هجينة شاملة متعددة الأبعاد.

فمنذ بداية العقد الثاني من القرن الحادي والعشرين، اتخذت العقيدة الدفاعية الإسرائيلية منحى جديد تمثّل في إعادة بناء شبكة دفاع جوي متكاملة، قائمة على التكنولوجيا المتقدمة، والردع الوقائي، والاستجابة السريعة للتهديدات الجوية المتعددة، وأصبح تطوير تكنولوجيا الدفاع الجوي أولوية قصوى في بنية الأمن القومي الإسرائيلي، فشهدت هذه التكنولوجيا قفزة نوعية عبّرت عنها ثلاث منظومات رئيسية القبة الحديدية، مقلاع داوود، ومنظومة حيتس [5].

وتعد أحد أبرز تطبيقات الذكاء الاصطناعي في الجيش الإسرائيلي يتمثل في استخدامها لتحليل كميات هائلة من البيانات الاستخبارتية، وتعمل حالياً على دمج الذكاء الاصطناعي بالطائرات بدون طيار ذاتية التشغيل لجعلها أكثر استقلالية في تنفيذ المهام، بما يشمل التعرّف على الأهداف، تتبعها، وحتى اتخاذ القرار بضربها دون تدخل بشري مباشر [17].

كما جرى تصميم القبة الحديدية خصيصاً للتعامل مع التهديدات القريبة المدى، مثل الصواريخ التي تُطلق من غزة أو جنوب لبنان، وقذائف الهاون. وتعتمد هذه المنظومة على تكنولوجيا الرصد الراداري عالي الحساسية، إلى جانب نظام اعتراض ذكي يُطلق صواريخ اعتراضية دقيقة تجاه الأهداف التي تكتشفها الرادارات. أما منظومة" مقلاع داوود هذه المنظومة مخصّصة لاعتراض الصواريخ التي يتراوح مداها بين 40 إلى 300 كيلومتر، وكذلك الصواريخ المجنّحة

والطائرات المسيّرة التي تحلق على ارتفاعات متوسطة أما منظومة حيتس فهي تمثل الذراع الطويلة لمنظومة الدفاع الجوي الإسرائيلية، وهي مخصصة لاعتراض الصواريخ الباليستية على ارتفاعات عالية جداً، وفي طبقات الغلاف الجوي العليا، وقد تم تصميم هذه المنظومة تحديداً لمواجهة تهديدات صواريخ بعيدة المدى مثل تلك التي قد تُطلق من إيران، أو من مناطق أبعد كاليمن أو العراق، وتحمل رؤوساً تقليدية أو غير تقليدية، وتعتمد حيتس3 على اعتراض الأهداف خارج الغلاف الجوي، وتعمل بتقنية "القتل الصامت"، أي أنها لا تستخدم تفجيراً تقليدياً، بل تصطدم بالرأس الحربي مباشرة لتفجيره، وهو ما يُقلل من خطر تساقط الحطام فوق الأراضي الداخليّة.

أيضاً حققت إيران تقدماً ملحوظاً في مجال التكنولوجيا العسكرية، وكان لهذا التطور دوراً كبيراً في تعزيز قدراتها الدفاعية، حيث سعت إيران إلى تحسين قوتها العسكرية عبر الابتكار المحلي، مع التركيز على تطوير أنظمة الدفاع الجوي الصواريخ الباليستية، الطائرات المسيرة والسفن الحربية. فقد شهدت المنظومة الصاروخية الإيرانية تطوراً تقنياً، ركزت إيرانمن خلاله على تعزيز قدراتها الدفاعية والهجومية فشمل ذلك تطوير صواريخ باليستية متقدمة مثل "فتّاح" الفرط صوتي 2023، و"قاسم بصير" 2025، بمدى يتجاوز 1200 كم، وقادر على اختراق أنظمة الدفاع الجوي، كما أدخلت تقنيات الذكاء الاصطناعي في التوجيه والمناورة، وطورت منظومات دفاع جوي محلية. وأصبحت الطائرات المسيرة الإيرانية (الطائرات بدون طيار) عنصراً بارزاً في القدرات العسكرية والتكنولوجية لإيران، في تصميم وتصنيع طائرات مسيرة متعددة الأغراض، تتراوح بين النماذج التكتيكية قصيرة المدى والاستطلاعية إلى الطائرات الهجومية بعيدة المدى.

كما توسعت إيران في استهداف منشآت حيوية مدنية (مثل شبكات المياه في إسرائيل، والمستشفيات، وشركات التأمين)، ما يعكس تصعيداً في محاولة الضغط على السكان المدنيين وإرباك الدولة، واستخدام تقنيات تجسسية دقيقة تدل على وجود دعم مباشر من أجهزة استخباراتية إيرانية.

يمكن القول أن الحرب السيبرانية أحدثت تحولاً جذرياً في موازين القوى العالمية، إذ لم تعد القوة العسكرية التقليدية أو التفوق الاقتصادي وحدَهما العاملين الحاسمين في ترتيب النفوذ الدولي، بل أصبحت القدرة على اختراق الأنظمة، وحماية البنى التحتية، والتلاعب بالمعلومات، وشلّ حركة الخصوم عبر الفضاء الإلكتروني أدواتِ قوةٍ استراتيجيةً تُعيد رسم خريطة التنافس بين الدول. ففي هذا العصر، تستطيع دولةٌ صغيرةٌ أو جهةٌ غير حكومية أن تُحدث أضراراً تعادل تأثيرات حرب تقليدية، وذلك عبر استهداف شبكات الطاقة، أو المؤسسات المالية، أو أنظمة الاتصالات، مما يُخلخل الاستقرار الداخلي للدول الكبرى ويُقلب المعادلات الأمنية. كما أن غياب القواعد الدولية الملزمة في هذا المجال، وسرعة وتيرة التطور التكنولوجي، يمنحان الدول المتقدمة سيبرانياً هامشاً واسعاً للتفوق، بينما تزيد الفجوة الرقمية من عزلة الدول الأقل تطوراً وتُضعف قدرتها على الصمود في وجه الهجمات، مما يُعمق الهيمنة التقنية للقوى العظمى ويُنتج نوعاً جديداً من التبعية الاستراتيجية. وفي المحصلة، لم تعد الحرب السيبرانية مجرد بُعد تكتيكي في الصراعات، بل أصبحت ميداناً رئيسياً لتغيير توازن القوى، حيث يُقاس النفوذ اليوم بقدرة الدول على السيطرة على الفضاء الرقمي وحماية سيادتها الافتراضية، وهو ما يُعيد تعريف مفاهيم الأمن والسيادة والتفوق في النظام الدولي المعاصر.

الخاتمة:

ان ما شهده العالم من ثورة تكنولوجية متطورة أثر على كافة مجالات الحياة سواء الاقتصادية أو السياسية أو الثقافية والصحية وحتى الأمنية والعسكرية، وانعكس هذا التأثير على طبيعة الحروب بين الدول فلم تعد تقتصر تلك الحروب التقليدية بالجيوش والدبابات والجنود المشاة، بل أدخلت التطورات التقنية الجديدة استخدامات متطورة سواء من حيث التخطيط للمعارك ووضع الاستراتيجيات والخطط العسكرية والمحاكاة الافتراضية لأرض المعارك إلى توجيه الأسلحة العسكرية من غرف القيادة أو إرسال فيروسات تدمر أجهزة الحواسيب وأنظمة التشغيل لدى الخصم، وأيضاً سرقة البيانات والمعلومات الأمنية والعسكرية الحساسة.

نتيجة لهذه التطورات التكنولوجية الحديثة بدء سباق تسلح تقني سعت العديد من الدول إلى دخوله والتفوق فيه وامتلاك أدوات وأساليب التكنولوجية وأيضاً محاولة منع الخصم من امتلاكها. ومن بين الأطراف التي دخلت هذا السباق وعملت على امتلاك التكنولوجية الحديثة إيران وإسرائيل حيث سعى الطرفان إلى تطوير الأدوات التقنية والتفوق فيها واستخدامها في كافة المجالات. وبرز الاستخدام الأمثل في الحرب بينهما حيث انتقلت من حرب تقنية تعتمد على سرقة المعلومات والبيانات الحكومية وأرصدة المصارف وتعطيل أنظمة التشغيل والحواسيب، إلى حرب عسكرية تقنية استخدمت فيها أساليب التخطيط المتطورة والهجمات المركزة عن بُعد بواسطة الطائرات المسيرة وأحدث أنظمة الدفاع الجوي.

الاستنتاجات والتوصيات:

الاستنتاجات:

1_ ان استخدام التطورات التكنولوجية للحرب السيبرانية لا تقتصر على الدول بل يمكن للشركات والمنظمات والأفراد استخدامها، وتتنوع أهداف هذه الاستخدامات ما بين سرقة البيانات أو تدميرها أو التجسس عليها، وتدمير الأجهزة أو توجيهها أو التحكم في الأجهزة المخترقة.

2_ تتميز الحرب السيبرانية بالعديد من السمات مثل تلاشي الحدود الجغرافية وانخفاض التكلفة المادية.

3_ عملت إيران على بناء بنية تحتية معلوماتية وتقنية ودخول سباق التسلح التقني، هدفت إلى حماية نظامها السياسي والاقتصادي والأمني ومهاجمة خصومها وتدميرهم. كما قامت إسرائيل بتأسيس قوة سيبرانية اعتماداً على أدوات تكنولوجية متطورة. هدفت من خلالها إلى حماية الأمن الإسرائيلي وقواعد البيانات وأيضاً استخدامها عسكرياً في محاربة خصومها.

4_ اثرت الهجمات السيبرانية الإسرائيلية على إيران حيث هدفت إلى تدمير البنية التحتية للمنشآت النفطية وأيضاً النووية وتعطيلها، بالإضافة لهجمات استهدفت سرقة البيانات الرسمية وابتزاز مالي. كما ان الهجمات الإيرانية ضد إسرائيل هدفت إلى سرقة البيانات الحكومية الإسرائيلية وتدمير البنية التحتية للمنشآت الإسرائيلية وإخراج المواقع الرسمية عن الخدمة وتعطيل شبكات الإنترنت والاتصالات.

5_ اثرت التطورات التكنولوجية الحديثة على الحرب التقليدية والقوة العسكرية، فالحرب الإيرانية الإسرائيلية أظهرت تطورات نوعية في الأساليب العسكرية الحربية والدفاعية، فقد شكل استخدام التكنولوجيا في الحرب تطور في القوة العسكرية لإيران وإسرائيل حمل تهديداً حقيقياً لكلا الطرفين.

التوصيات:

1. إعادة تعريف مفهوم الأمن القومي: في ضوء أن الحرب السيبرانية لا تقتصر على الدول بل تشمل الشركات والمنظمات والأفراد، وتتميز بغياب الحدود الجغرافية وانخفاض التكلفة، توصي الدراسة بإعادة تعريف مفهوم الأمن القومي ليشمل البعد السيبراني كعنصر أساسي إلى جانب الأبعاد العسكرية والاقتصادية والسياسية التقليدية.

2. وضع استراتيجيات وطنية شاملة للحرب السيبرانية: نظراً لتنوع أهداف الهجمات السيبرانية (سرقة، تدمير، تجسس، تحكم، ابتزاز)، توصي الدراسة بوضع استراتيجيات وطنية متكاملة تغطي الجوانب الهجومية والدفاعية والوقائية، مع تحديد آليات واضحة للاستجابة السريعة لأي طارئ سيبراني.

3. تعزيز التعاون الدولي لوضع أعراف وقواعد ملزمة :انطلاقاً من أن الحرب السيبرانية تتجاوز الحدود الجغرافية، توصي الدراسة بالعمل على المستوى الدولي لوضع أطر قانونية وأخلاقية تنظم استخدام الأدوات السيبرانية في النزاعات، وتحدد مسؤوليات الدول والجهات غير الحكومية، وتجرم الهجمات التي تستهدف البنية التحتية الحيوية.

4. الاستثمار في البنية التحتية السيبرانية: كما فعلت إيران وإسرائيل في بناء بنية تحتية معلوماتية وتقنية، توصي الدراسة جميع الدول بالاستثمار في تطوير أنظمة أمن سيبراني متطورة، وتحديث البنية التحتية الرقمية باستمرار لمواكبة التهديدات المتجددة.

5. تأسيس وحدات عسكرية سيبرانية متخصصة: توصي الدراسة بتأسيس وحدات عسكرية مستقلة متخصصة في الحرب السيبرانية، أسوة بما تملكه إسرائيل (وحدة 8200) وإيران (قوات الفضاء السيبراني التابعة للحرس الثوري)، على أن تكون هذه الوحدات قادرة على تنفيذ عمليات هجومية ودفاعية واستخباراتية بشكل متزامن.

Reference:

[1] N. Qashti, "Cyberwarfare and Ways to Confront It," Journal of Strategic Affairs, (In Arabic) vol. 0, no. 17, 2024.
[2] F. Al-Tariki, "Cyberwarfare and National Security: Threats and Future Challenges," Afro-Asian Journal of Scientific Research, (In Arabic), vol. 3, no. 3, 2025.
[3] H. Hamoudi, "Utilizing Artificial Intelligence Technologies in the Israeli War on the Gaza Strip," Scientific Journal of the Counter-Terrorism Agency, (In Arabic) vol. 5, no. 9, 2025.
[4] I. Ramadan, "Countering Cyber Attacks in Light of International Law Provisions," Journal of Legal and Economic Sciences, vol. 67, no. 1, 2025.
[5] A. Alaaeddine, "The Technological Military Evolution of Israel 2006–2024: An Analytical Study of Field Transformations and Security Doctrines," Al-Khaneedein: Science and News, 2025.
[6] A. al-Akabi, "Employing Cyber Conflicts in Developing the Concept of State Power among Major Powers," Journal of Political Issues, vol. 73, 2023.
[7] A. bin Ahsan, "Iranian Cyberpower and Its Impact on Regional Stability," Global Politics Journal, vol. 6, no. 2, 2022.
[8] G. Abdel Aal, "Cyberwarfare: A Study in Concept, Origins, and Success Rates," Journal of Business and Environmental Studies, vol. 13, no. 2, 2022.
[9] H. Al-Khatib, "Geopolitical Implications of Iranian-Israeli Cyberwarfare on the Syrian Revolution Path," Journal of Geopolitics, vol. 9, no. 33, 2025.
[10] D. Wali, "Cyberterrorism: Electronic Terrorism—Cyber Warfare, Tactics, Tools, and Strategies," Journal of Radio and Television Research Studies, part 2, no. 31, 2025.
[11] S. Al-Shawsh, "Cyberwarfare and Its Impact on International Relations: The Zionist Entity's War on Hezbollah as a Case Study," Journal of Political Issues, no. 80, 2025.
[12] S. Al-Alawi, "Cyberwarfare between Iran and Israel 2010–2025: An Analytical Reading of Objectives, Tools, and Regional Reflections," Prim Journal, 2025.

[13] S. Abdel-Wahid, “Cyber Warfare: A Study in its Concept, Characteristics, and Ways to Confront It,” MS thesis, College of Arts and Sciences, Al-Sharq University, Jordan, 2021.
[14] A. Abu Haeneh, “Iranian–Israeli Cyberwarfare,” Institute for Palestinian Studies on National Security, 2025.
[15] A. Abu Aliyan, “Cyberwarfare and Effective Strategic Performance: A Case Study of Cyber Attacks between Iran and Israel,” Initiative Journal, vol. 2, 2023.
[16] G. Qasimi, “The Concept of Cyber Attacks and its Legal Nature,” Iraqi University Journal, vol. 73, no. 4, 2025.
[17] O. Laqouni, “The Impact of Modern Technology on the Iranian–Israeli Conflict Trajectory,” MS thesis, College of Law and Political Science, Zian Ashour University, Algeria, 2025.
[18] M. Zeytoun, “The Threshold of Cyber Power and Its Effect on Contemporary International Relations,” Gulf of Arabs Journal of Humanities and Social Studies, vol. 2, 2025.
[19] M. Mohsen, “Israeli Cyber Power and Its Influence on the Strategies of Regional Powers,” Counter-Terrorism Agency Scientific Journal, vol. 5, no. 9, 2025.
[20] M. Abū Anūr et al., “Countering Cyberwarfare During Armed Conflicts in Light of International Humanitarian Law,” Journal of the College of Sharia and Law, part 3, no. 29, 2024.
[21] N. Jamil, “Iranian Deterrence Shifts in Facing Israel: Strategic Analysis of the Role of Rocket and Drone Capabilities in Managing Low-Intensity Conflict,” Policy Assessment, Hammurabi Center for Research and Strategic Studies, 2025.
[22] Y. Chen "Iran-Israel Cyberspace Conflict: Evolution, Motivations and Impacts." *Journal of National Philosophy and Social Sciences*, Issue 3, pp. 125-150, 2024.
[23] A. Haroon, "AI and Cyber Drove Warfare in the Israeli-Iran Conflict and its Impact on Gulf States' Security." *Journal of Politics and International Studies*, Vol. 10, No. 2, pp. 145–163, 2024.