الحرب السيبرانيّة والأداء الإستراتيجيّ الفعال؛
دراسة حالة في الهجَمات السيبرانيّة بين إيران و"إسرائيل"

The Cyber War and the Effective Strategic Performance Study case in the cyber attacks between Iran and (Israel).

د. عبد العزيز محمود أبو عليان
باحث في التاريخ ودراسات الشرق الأوسط
اسطنبول – تركيا

YAFFA-1984@HOTMAIL.COM

تاريخ استلام البحث: 2023/03/17
تاريخ تحكيم البحث: 2023/05/14

ملخص:

لقد تصاعدت الهجَمات السيبرانيّة بين الولايات المتحدة، وبين الصين، وروسيا، في ظل ثورة المعلومات المتطورة في واقعنا المعاصر، وأصبحت الحروب السيبرانيّة ذات تأثير واضح في البيئات المختلفة، التي تؤثر على منظومة الأمن القوميّ للدول، فالصراع الخفي في الحرب السيبرانيّة بين (إسرائيل) وإيران هو صراعٌ خفي، تسعى كل دولة لإثبات قدراتها في إظهار نفسها على الساحة الإلكترونيّة؛ فإيران تريد أن تُظهر نفسها أنّ لديها القدرة على أنْ تنافس الولايات المتحدة بإيصال رسائل لها بشن هجَمات سيبرانيّة؛ لتؤكد لخصومها بأنها حاضرة في الميدان، ولا يمكن تجاوز قدرتها الإلكترونيّة الإيرانيّة في هذا المجال، كما تقوم (إسرائيل) بتوصيل رسائل غير معلنة من خلال تنفيذها هجَمات سيبرانيّة؛ لتحقق الردع والحسم في صد أي هجوم إلكترونيّ على مؤسساتها، وأنّ لديها القدرة على ضرب أعدائها في الوقت الذي تريد، وتعمل على إيقاع الخسائر في الأنظمة الإلكترونيّة الإيرانيّة.

الكلمات الدالة: الحرب السيبرانيّة – الأداء الإستراتيجيّ – إيران – (إسرائيل).

Abstract:

Cyber-attacks have escalated in major countries such as the United States of America, Russia, and China, in light of the advanced information revolution in our contemporary reality, and cyber wars have become clear in different environments, affecting the national security system of countries. Lightly, every country seeks to prove its capabilities to show itself in the electronic arena, as Iran wants to show itself that it has the ability to compete with the United States of America by sending its messages by through launching cyber-attacks to assure its opponents that it is present in the field and that Iran cannot be bypassed in this field, and in In the same framework, Israel delivers unannounced messages in carrying out its cyber-attacks to achieve deterrence and decisiveness in its ability to repel any attack on its institutions, and that it has the ability to strike its enemies at the time it wants and inflict losses on electronic systems .

Keywords: Cyber War - Strategic Performance - Iran – Israel.

مقدمة:

الحرب السيبرانيّة إحدى أدوات الجيل الخامس للحروب؛ فأصبحت أكثر تأثيرًا في الصراع القائم بين الدول؛ بسبب التكاليف القليلة للجهة المهاجمة بخلاف الجهة المستهدفة التي تكون منشآتها ومواقعها الإستراتيجيّة وبُناها التحتيّة الواقعة في مرمى الإنهاك والتدمير والإبطاء، وهذا ما وقع بين إيران و(إسرائيل) ؛ إذ تُعد الهجَمات السيبرانيّة بينهما الصفة الغالبة، مستخدمين البرمجيّات والفيروسات المدمرة كأسلحة إستراتيجيّة سيبرانيّة ناتجة عن توجهات الإستراتيجيّة (الإسرائيليّة)، كما تقوم ايران بإنشاء مؤسسات متخصصة في المجال نفسه، وتسعي (إسرائيل) لتدمير البُني التحية لإيران خاصة في مجالها النوويّ. حيث أصبح تبادل الهجَمات السيبرانيّة بين (إسرائيل) وإيران بديلًا عن المواجهة العسكريّة التقليديّة، وبين الطموح الإيرانيّ في الفضاء السيبرانيّ، والقدرات الإسرائيليّة المدعومة من الولايات المتحدة يشتعل الصراع في الحرب السيبرانيّة، لتصبح ساحة حرب غير مرئيّة، لنيل كل طرف من قدرات الآخر.

وفي ظل التصعيد المتبادل بين طرفي الصراع –مَحَلّ الدراسة –على مسرح العمليّات الإقليميّة في سوريا ولبنان، تتزايد حدة الصراع الإلكترونيّ، حيث يوفر ميزات مهمة للطرفين، من حيث عدم الدخول في مواجهة مباشرة، وسهولة التنصل من المسؤوليّة، وقلة التكاليف لهذه الهجَمات.

أهمية الدراسة:

تكمُن أهمية الدراسة في ظل تزايد الصراع السيبرانيّ بين الدول في وقتنا الحاضر، حيث أصبحت الهجَمات السيبرانيّة تشكل هاجسًا للدول العظمي، الأمر الذي استدعى إنشاء تحالفات دوليّة، وتوقيع اتفاقيات تعاون مشترك لصد أيّ هجوم سيبرانيّ محتمل مستقبلًا، وتأتي أهميّة الدراسة في ظل الصراع القائم بين إيران و(إسرائيل)، وتبادل الاتهامات بشن هجَمات سيبرانيّة بين الطرفين، دون

الإعلان الصريح عنها، إنّ هذه الدراسة تقف على معرفة الأداء الإستراتيجيّ للطرفين في هذه الحرب غير المعلنة، عبر فهم الحرب السيبرانيّة، ودراسة الهجَمات السيبرانيّة المتبادلة بين (إسرائيل) وإيران، ومعرفة الأثر الإستراتيجيّ على الطرفين.

مشكلة الدراسة:

تظهر بين الفينة والأخرى مجموعة من الاتهامات المتبادلة بين إيران و(إسرائيل)، حول الهجَمات السيبرانيّة ضد المواقع الإستراتيجيّة، والبنية التحتيّة لكل طرف من طرفي الصراع؛ ما يسبب دمارًا وإنهاكًا لتلك المؤسسات، وتحاول هذه الدراسة الوقوف على الأداء الإستراتيجيّ الفعال للحرب السيبرانيّة بين إيران و(إسرائيل) من خلال دراسة الهجَمات السيبرانيّة المتبادلة بين طرفي الصراع، وذلك عبر طرح عدد من التساؤلات الفرعيّة، هي:

1. ما هي الحرب السيبرانيّة؟ وما هو مفهومها؟ وماهي خصائصها؟ وما هي أهدافها؟
2. من هم الفواعل في الحرب السيبرانيّة؟ وما هي وسائل الحرب السيبرانيّة؟
3. ما هي الإستراتيجيّة الإيرانيّة في الحرب السيبرانيّة؟
4. ما هي الإستراتيجيّة (الإسرائيليّة) في الحرب السيبرانيّة؟
5. ما هي الهجَمات السيبرانيّة الإيرانيّة على (إسرائيل)، وأثرها الإستراتيجيّ؟
6. ما هي الهجَمات السيبرانيّة (الإسرائيليّة) على إيران، وأثرها الإستراتيجيّ؟

أهداف الدراسة:

تهدف الدراسة إلى عدد من الأهداف، هي:

1. التعرف على الحرب السيبرانيّة من حيث: نشأتها، ومفهومها، وخصائصها، وأساليبها.
2. معرفة الأطراف الفاعلة في الحرب السيبرانيّة وتأثيرهم الإستراتيجيّ في

مجريات الهجَمات السيبرانيّة في الصراع بين الدول.

3. فهم الإستراتيجيّة (الإسرائيليّة) والإيرانيّة للحرب السيبرانيّة.
4. دراسة الهجَمات السيبرانيّة المتبادلة بين إيران و(إسرائيل).
5. معرفة الأثر الإستراتيجيّ للهجَمات المتبادلة بين إيران و(إسرائيل).

منهج الدراسة:

استخدم الباحث المنهج التاريخيّ، والمنهج التحليليّ، لتفسير الأحداث التي تتعلق بمحتوى الدراسة.

هيكلية الدراسة:

شملت الدراسة ثلاثة مباحث، حيث جاء **المبحث الأول** بعنوان الحرب السيبرانيّة (المفهوم، والنشأة، والوسائل، والخصائص)، ودرس **المبحث الثاني** الإستراتيجيّة الإيرانيّة و(الإسرائيليّة) للحرب السيبرانيّة، ودرس **المبحث الثالث** الهجَمات السيبرانيّة التي تعرضت لها إيران و(إسرائيل)، ثم الخاتمة والمراجع.

المبحث الأول: الحرب السيبرانيّة (المفهوم والأهداف والوسائل):

يشهد العالم حربًا سيبرانيّة معلنة بين الولايات المتحدة من جانب، والصين، وروسيا، وإيران من جانب آخر، وكما توجد حربٌ خفيةٌ بين إيران و(إسرائيل) وبعض الدول الأخرى، فالجانب الخفي في الحرب السيبرانيّة أكبر من المعلن بين الدول، ولذلك فإنّ الحرب السيبرانيّة إحدى أدوات الجيل الخامس في ساحة الصراع في الفضاء السيبرانيّ، الذى بدأ في أثناء الحرب الباردة التي استعملت خلالها الأسلحة السيبرانيّة من فيروسات وبرمجيّات ذات نمط تدميريّ ضد الطرف المستهدف بأقلّ التكاليف للطرف المهاجم، التي تقوم به دول بعينها أو فواعل آخرون من ذوات غير الدول، الأمر الذي يجعلنا نتحدث في المبحث الأول عن نشأة ومفهوم الحرب السيبرانيّة والأهداف والوسائل والفواعل التي تؤثر

في الحرب السيبرانيّة بين الدول والكيانات التي يسعى كل طرف لإثبات قدراته السيبرانيّة؛ لتحقيق أهدافه بأقل التكاليف.

أولًا: نشأة ومفهوم الحرب السيبرانيّة:

أصل مصطلح السايبر (CYBER) الكلمة اللاتينيّة بمعني (افتراضي)، وتستخدم كلمة السايبر في الفضاء الذي يضم المعلومات، والشبكات العنكبوتيّة المحوسبة، ومنظومات الاتصال، وأنظمة التحكم عن بُعد. وتختلف استخدامات العالم الافتراضيّ وأشكاله من دولة إلى أخرى تبعًا لأولويّاتها؛ فمنها الأمنيّ، والسياسيّ، والاستخباراتيّ، والمدنيّ، والمهنيّ، والمعلوماتيّ البحت. ولمنظومة السايبر في الدول ثلاث ركائز أساسيّة، هي الأجهزة الصُلبة، والعامل البشريّ من مبرمجيّن ومستخدمين (Hardware)، وبرمجيّات رقميّة ناعمة (Software)[1].

ترجع نشأة الحرب السيبرانيّة إلى حقبة الحرب الباردة، فكانت أوّل حرب سيبرانيّة بين الولايات المتحدة، والاتحاد السوفييتي في عام 1982، من خلال قيام المخابرات السوفيتية (KGB) بتدريب عدد من العلماء على التسلل إلى الشركات والوكالات لسرقة المخططات والمعلومات السريّة للأبحاث والرسوم للمشروعات والإنشاءات الأمريكيّة ، ولقد وصلت معلومات إلى وكالة المخابرات الأمريكيّة (CIA) بهذا الشأن ، وقامت بعملية تجسس مضاد عبر نصب فخ بدلًا من القبض عليهم، وتركتهم يواصلون العمل، وإمدادهم بمعلومات مغلوطة، وقد تم وضع خطأ بسيط في الشيفرة بحيث لا يمكن كشفه بسهولة، فقام السوفييت بتوظيف المعلومات التي جمعها لبناء العمود الفقريّ لخطوط نقل الغاز الطبيعيّ والنفط القادم من سيبيريا، وبعد فترة قصيرة تسبب الخطأ المتعمد في الشيفرة بانفجار خطّ الأنابيب، وكان حجم الانفجار ثلث انفجار القنبلة النوويّة في

(1) علو، الحروب السيبرانيّة والعنف الرقمي واقع عالمي جديد.

هيروشيما[1].

اقترن مفهوم الحرب السيبرانيّة بالهجَمات الإلكترونية التي تقوم على اختراق الأنظمة الإلكترونيّة العالميّة، وكل ما يستند على التقنية؛ لتكون ضارة بالحواسيب والأجهزة التي تستخدم شبكة الإنترنت، وقد تؤدي لنتائج كارثيّة، مثل سرقة بيانات خاصة، وكوارث قد تكون عالميّة مثل الحروب النوويّة. وبعد التوسع الكبير والسريع لأجهزة الكمبيوتر والإنترنت في الولايات المتحدة الأمريكيّة، والدول المتقدمة، بدأت المخاوف تتزايد لدى الجميع بإمكانية تحقق الأمر. ففي عام 1997، أصدرت لجنة أمريكيّة متخصصة في تقريرٍ دعت فيه للنظر بشكل مغاير عن الصورة النمطيّة التي ينظر بها الجميع للأمن عمومًا والحرب السيبرانيّة خصوصًا وتداعياتها على الوضع العالميّ وآثارها في ظل التقدم الرقمي المتزايد. وفي ظل ذلك التقدم التكنولوجيّ وتخوف العالم من الحرب السيبرانيّة وأخطارها، شكلت الولايات المتحدة الأمريكيّة (الفريق الأحمر) المتخصص في الكشف عن الثغرات التي تتعرض لها الشبكة الرقميّة الأمريكيّة، وصار الفريق بمثابة الجيش السيبرانيّ الأمريكيّ، واكتشف الثغرات التي شكلت نقطة ضعف لهذا المجال.[2]

الحروب السيبرانيّة واحدة من العوامل الفعالة في الاقتصاد والسياسة على المستوى الدوليّ، نتيجة انتقال قسم كبير من الصراعات بين القوى العظمى في العالم، إلى شبكة الإنترنت والوسط الرقميّ، ورغم عدم إمكانية معرفة مصدر الهجَمات على الشبكة العنكبوتيّة، بصورة قاطعة، وما إذا كانت تدعمها حكومات أو جماعات، إلا أنّها باتت تثير جدلًا متبادلًا بين الدول، بينما تتهم دول غربيّة والولايات المتحدة، دولًامثل الصين وروسيا كوريا الشمالية وإيران ، بالوقوف خلف

(1) موقع الجندي، الحرب السيبرانيّة. نتائج ملموسة لمعارك غير مرئية.

(2) سايبر وان، ما هي الحرب السيبرانيّة؟ وما مدى خطورتها؟ .

الهجَمات، وتدعي الدول الأخيرة أنّها فريسة حقيقيّة لأعمال الهجَمات السيبرانيّة. وتحرص الدول على تعزيز بنيتها التحتيّة الأمنية، في الوسط الرقميّ، وتأهيل كوادرها المعنيّة، في مواجهة الهجَمات ذات المصدر الخارجي.[1]

وقد **تنوعت تعريفات حروب السايبر بين الدول،** ولم يتم الاتفاق على تعريف موحد لحروب السايبر ومن تلك التعريفات:

1. تعرّف الحرب السيبرانيّة بأنّها "التغلغل في شبكات الحواسيب في الدولة، عبر شبكات الإنترنت والحواسيب التابعة لدولةٍ أخرى أو منظمةٍ ما"، وتوصف الأنشطة الجارية في هذا الخصوص، بـ(الهجوم السيبرانيّ).[2]
2. عرف المفكر الصينيّ هاف كم جوانج، الحرب السيبرانيّة؛ بأنّها الغرف المغلقة أو حرب المنازل، كما أشار إلى المصطلح بمصطلح دبابات الفكر المكونة من خبراء حكوميّين تم اختيارهم من الصفوة العلميّة، يعملون على حواسيب شخصيّة، ويشاركون في صناعة القرار على المستوى القيادي في الدول.
3. عرف مكتب الأمم المتحدة الحرب السيبرانيّة؛ بأنّها وصف لمجموعة واسعة من الجرائم تتمثل في هجَمات سيبرانيّة ضد أنظمة الحواسيب مثل القرصنة والتزوير، والاحتيال، وجرائم المحتوى مثل المخالفات المتعلقة بحقوق النشر، وسرقة البيانات[3].
4. وتعرف اللجنة الدوليّة للصليب الأحمر، الحرب السيبرانيّة؛ بأنّها الأعمال التي ترتكز على أطراف نزاع ما؛ لتحقيق ميزة على خصومهم في الفضاء

(1) وكالة الأناضول، الحرب السيبرانيّة... تهديدات حقيقية من العالم الافتراضيّ.

(2) وكالة الأناضول، الحرب السيبرانيّة... تهديدات حقيقية من العالم الافتراضي.

(3) عبد العال، الحروب السيبرانيّة دراسة في المفهوم والنشأة ومعدلات النجاح، ص 290-291.

السيبرانيّ باستخدام أدوات تقنية متنوعة، كإتلاف المعلومات، أو القيام بعمليّات تجسس سيبرانيّ[1].

5. يعرف ريتشارد كلارك وربروت كناكي؛ حرب السايبر بأنّها مجموعة من الأعمال تنفذها الدول؛ بهدف التغلغل في حواسيب وشبكات الدولة المعادية؛ لتحقيق أضرار بالغة وتدميرها[2].
6. ويعرف بولو شاكرين الحرب السيبرانيّة أنّها استمرار للسياسة عبر التدابير المتخذة في الفضاء السيبرانيّ من دول وفاعلين دوليّين، إذ تُعد تهديدًا خطيرًا على الأمن القوميّ[3].

وجاء التعريف الاصطلاحيّ للحرب السيبرانيّة أنّها مجموعة الخطوات الإجرائيّة التي تنفذها الدول لمهاجمة على نظم معلومات الخصم، وتهدف للتأثير والإضرار به، وللدفاع عن منظومة المعلومات الخاصة بالدولة من أيّ هجوم محتمل على مؤسّسات الدولة العامّة والخاصّة[4].

ويظهر من التعريفات السابقة أنّه لا يوجد اتفاق على تعريف واحد لمفهوم الحرب السيبرانيّة، فكل دولة أو جهة تعرّفها من منطلق فهمها للمخاطر التي تواجها الدولة أو التنظيم، ويكمُن هذا في اختلاف إستراتيجيّات الدول وأهدافها والتنوع في مرتكزات التعريف، فالولايات المتحدة الأمريكيّة تستند في تعريفها على المقاربات الاقتصاديّة والماديّة، بينما دول أخرى تركز على أهداف الصراع مثل الهُويّة الثقافيّة، والسيادة الوطنيّة، ولذلك يبدو معَ ظل عدم وجود تعريف موحد

(1) عبد العال، الحروب السيبرانيّة دراسة في المفهوم والنشأة ومعدلات النجاح، ص 290-291.

(2) عباس، فرج، الحرب السيبرانيّة: دراسة في إستراتيجيّة الهجمات السيبرانيّة، ص200.

(3) زروقة، الفضاء السيبرانيّ والتحول في مفاهيم القوة والصراع، ص12.

(4) سعود، الحرب السيبرانيّة في ضوء القانون الدول الإنساني، ص84.

أنّها امتداد لحروب أجهزة الاستخبارات، وتمثل هذه الحروب ميدانًا جديدًا للنزاعات؛ فهي حرب سريّة غير معلنة، ومحاطة بالكثير من التضخيم والمغالطات؛ نتيجة لعدم وجود معلومات واضحة للهجَمات السيبرانيّة على الدول.

ثانيًا: أهداف الحرب السيبرانيّة:

إنّ لكل حرب أهدافًا متنوعة، وتميزت الحرب السيبرانيّة عن باقي الحروب؛ بأنّ لها أهدافًا بعيدة المدى، فلا تقف عند مدى خطورتها فحسب، بل إنّ أضرارها ليس لها نطاق محدد، ولهذا تنوعت أهدافها، ومن أبرز تلك الأهداف:[1]

1. تدعيم حماية أنظمة التقنيات التشغيليّة على كافة الأصعدة ومكوناتها من أجهزة وبرمجيّات، وما تقدمه من خدمات وما تحويه من بيانات.
2. مواجهة أيّ هجَمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكوميّة ومؤسسات القطاع العام والخاص.
3. تأمين بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
4. صمود البني التحتيّة الحساسة للهجَمات الإلكترونيّة.
5. توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونيّة التي تستهدف المستخدمين.
6. الخلاص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
7. سد الفجَوات في أنظمة أمن المعلومات.
8. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
9. تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة

(1) السمحان، متطلبات تحقيق الأمن السيبرانيّ لأنظمة المعلومات الإدارية بجامعة الملك سعود، ص12.

باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

ثالثًا: الفواعل في الحروب السيبرانيّة:

يُعد المجال السيبرانيّ أحد مجالات الحرب السيبرانيّة، فالحرب السيبرانيّة غير واضحة الأهداف، وتعمل من خلال منظومة المعلومات والاتصالات العابرة للحدود، وتستخدم أسلحة تقنية متطورة تتلاءم معَ طبيعة الصراع الإلكترونيّ، أو توجيهها ضد المنشآت الحيوية عن طريق عملاء يتبعون المخابرات[1].

ولهذا يمكن تقسيم الفواعل في الحرب السيبرانيّة ومن لديهم القدرة على شن هجَمات إلكترونيّة إلى:

1. **الدول:** تعد الدول من الفواعل الأساسيّة في الحروب السيبرانيّة، فلديها القدرة لشن هجَمات سيبرانيّة؛ ولهذا أنشأت جيوشًا سيبرانيّة داخل قواتها المسلحة من باب الاستعداد لصد أي هجَمات سيبرانيّة محتملة على الدولة، الأمر الذي دعا الدول لتوقيع اتفاقيات سياسيّة وعسكريّة لتقليل ومنع الهجَمات السيبرانيّة[2]، فقد وقعّت الصين والولايات المتحدة، اتفاقًا خاصًّا بالحرب السيبرانيّة عام 2015، بعدم شن أيّ هجَمات سيبرانيّة، وفي عام 2018، تمكنت أكثر من180، من امتلاك منظومة أسلحة إلكترونيّة هجوميّة دفاعيّة[3].
2. **الكيانات الافتراضية:** وهي مجموعة من الأفراد يتبادلون نفس الأفكار والنشاطات، ويسعون لتحقيق غاية وأهداف مشتركة مثل مجموعة (أنونيموس)، ويكون لهذه الكيانات الأثر الكبير في حال كان لها اتصال

(1) سعود، الحرب السيبرانيّة في ضوء القانون الدول الإنساني، ص84.

(2) خليفة، إيهاب، مجتمع ما بعد المعلومات، ص115.

(3) حسين، محمود، الحروب السيبرانيّة: المخاطر وإستراتيجيّات، ص181.

معَ الجماعات الإرهابية، ويكون لها تأثير على الأمن القوميّ عبر الفضاء السيبرانيّ[1].

3. **الأفراد:** لقد أصبح للأفراد دور في الحروب السيبرانيّة من خلال إحداث التغيير في مساراتها، فقد أظهرت دراسات بأن الأفراد لديهم القدرة على التحكم في تسيير الشبكات والمنظومات الإلكترونيّة فقد تفوق قدرات هيئات متخصصة بذاتها، ولقد كانت الوسائل التواصل الاجتماعي الأثر في إبداء الأفراد حرية الرأي بل المشاركة في تهديد سلامة وأمن المجتمعات[2].

رابعًا: خصائص الحرب السيبرانيّة:

لقد تميزت الحروب السيبرانيّة بعدد من الخصائص والصفات، هي[3]:

1. تعتبر حربًا رقمية متطورة؛ فلقد شكلت ثورة المعلومات المتطورة وسيلة محورية للحرب السيبرانيّة، وأصبحت الميدان الرئيس لها.
2. تُعد حربًا هلامية الملمح والشكل، حيث تتعدد في ميادينها، ومتنوعة ومتطورة بوسائلها وأدواتها المرتبطة بالأقسام التقنية تطورًا وتبدلًا في واقعنا المعاصر، وهي تطال بتدميرها أكثر المواقع الحساسّة والسياديّة ذات الحصانة العالية.
3. تتميز بأنّها قوة تدمير لا يوجد فيها دماء أو ضحايا.
4. تتميز بأنّها ذات مصاريف ماليّة منخفضة، بخلاف الحرب التقليديّة؛ فهي لا تحتاج لتكاليف ضخمة لتصنيع أسلحتها مقارنة بالأسلحة الفتاكة ذات التكاليف الباهظة.

---

(1) إبراهيم، الدسوقي، الأمن المعلوماتي، ص107.

(2) حسين، محمود، سمر، السيبرانيّة: المخاطر، ص181.

(3) العبودي، هاجس الحروب السيبرانيّة وتداعياتها، ص99-101.

5. تمنح المهاجم أفضليّة واضحة في حروب الإنترنت على المدافع، فالحروب السيبرانيّة تتميز بالسرعة والمراوغة والمرونة في بيئة مماثلة يظهر فيها المهاجم بأفضليّة من الصعب على عقليّة التحصن لوحدها أنْ تنجح.
6. تقوم بالتجسس ومن ثَمّ النسف دون وجود غبار ولا دخان، فتتم عمليّة التدمير بوابل من الفيروسات.
7. ساعد انتشار الفضاء الإلكترونيّ الحروب السيبرانيّة في توسيع دائرة استهداف المواقع بمختلف مستوياتها.

خامسًا: دوافع وطبيعة الحرب السيبرانيّة:

تختلف الحروب السيبرانيّة عن غيرها من خلال طبيعتها؛ لأن الصراع يكون داخل الفضاء السيبرانيّ، غير المضمون النتائج المتوقعة، فهي حرب تستهدف النظام والأمن بشكل خاص من خلال تعطيل الشبكة المعلوماتيّة في القضايا الأساسيّة في الدول المستهدفة، وتتميز بأنّها ديناميكيّة ودائمة؛ لأنّها خفية، وإما في حالة هجوم أو دفاع دائم، ولهذا تتسم الحرب السيبرانيّة من حيث طبيعتها العمليّاتية بالآتي[1]:

1. تعمل على جمع المعلومات الاستخباريّة المتعلقة بالبنية الإستراتيجيّة.
2. تستهدف تفكيك التركيبة النفسية والتفاهم داخل مجتمع العدو.
3. غياب التسلسل الهرمي للقيادة، ولا ترتكز لقيادة عليا.
4. الغموض في الخطوة الفاصلة بين الحرب والسياسة وبين المقاتلين والمدنيين.

وتكمُن دوافع الحرب السيبرانيّة في:

(1) حكيم، الإرهاب السيبرانيّ والأمن الدولي، ص113.

1. ظهور قواعد البيانات للاعتماد على نظم المعلومات في مجال صناعة القرار، وخاصة القرارات العسكريّة، أدى إلى توفير معلومات هائلة التي يتم استغلالها في المعارك وتطوير الكفاءات القتالية فيها، ما جعلها هدفًا للهجَمات الإلكترونيّة المختلفة من أجل السيطرة عليها.
2. سيطرة الطابع الهجوميّ على الدفاعي بحيث ترجح الكفة في ميدان الحرب السيبرانيّة للهجَمات الإلكترونيّة أكثر من الأحزمة الدفاعية؛ هو جعل الكل إما عنصرًا مهاجمًا أو مدافعًا بشكل إجباري، في ظل عدم وجود حدود مكانية أو زمانية للهجَمات الإلكترونيّة[1].

سادسًا: وسائل الحروب السيبرانيّة:

تتنوع وسائل الحرب السيبرانيّة على النحو الآتي[2]:

1. **فيروسات الحاسوب:** هي فيروسات خبيثة يتم إنشاؤها عمدًا؛ بهدف تغيير خصائص الملفات التي تصيبها؛ لتنفيذ بعض الأوامر لتعديلها أو إزالتها أو تخريبها، والغرض الرئيس منها هو التلف، سواء كان ضررًا ماديًّا متعلقًا بتدمير الأجهزة والأنظمة الإلكترونيّة، أو تلفًا رقميًّا متعلقًا بمعلومات البرامج الأخرى لأنظمة تشغيل المعلومات.
2. **الديدان:** إنّها برامج صغيرة لا تعتمد على برامج أخرى، ولكنها تتكاثر وتنسخ نفسها عبر الشبكات لتنفيذ هجَمات تخريبية، مثل قطع الاتصال بالشبكة أو سرقة بيانات بعض المستخدمين في أثناء تصفح الإنترنت، وتتميز بسرعة انتشارها، كما يصعب التخلص منها؛ نظرًا لقدرتها العالية على التناسخ والمراوغة.
3. **أحصنة طروادة:** هي برامج صغيرة مخبأة في برنامَج كبير من البرامج

(1) حسين، محمود، الحروب السيبرانيّة: المخاطر، ص117.

(2) خليفة، مجتمع ما بعد المعلومات، ص 117-119.

ذات الشعبية العالية، وتقوم ببعض المهام، مثل نشر دودة أو فيروس، وتتم برمجتها بمهارة عالية؛ لذلك لا يمكن الكشف عن وجودها، فهي تعمل دائمًا على محو آثارها التي لا تحمل طابعًا مدمرًا، وغالبًا ما تعمل على إضعاف قوات دفاع الضحية لتسهيل اختراق الجهاز الخاص بالضحية وسرقة بياناته. .

4. **القنابل المنطقية:** هي برمجيّات يتم زرعها داخل النظام أو البرنامج الذي يطوره، أي أنّ المستهلك يشتري البرنامج أو الجهاز مصابًا من البداية بالسلاح السيبرانيّ.
5. **البرمجيّات الخبيثة:** تميزت هذه البرمجيّات بأنّها تستهدف الكيانات الاقتصادية وليس الأفراد؛ وذلك لأنّ هذه المؤسسات هي الأقدر على دفع الفدية.
6. **الفيروسات الإلكترونيّة:** تتنوع الفيروسات ومنها فيروس "ستاكس نت Stux net"، وهو من أخطر الأسلحة السيبرانيّة التي تم اكتشافها في عام 2009، فمن خلالها انتقلت الحرب من تدمير بيانات وسرقتها، إلى تدمير المكونات الماديّة نفسها، ونظم تشغيل وليس فقط البيانات والمعلومات.

المبحث الثاني: الحروب السيبرانيّة بين إيران و(إسرائيل):

أولًا: الإستراتيجيّة الإيرانيّة في الحرب الإلكترونيّة:

تمكنت إيران من بناء منظومة القدرات الحربية الإلكترونيّة والاستطلاعية لتحييد القدرات التقنية العالية لخصومها من المعارضة السياسيّة داخل وخارج البلد، وكذلك أعدائها من الدول المعادية لها في المنطقة، وتوظيف الثورة التقنية منخفضة التكلفة التي يمكن توفيرها بسرعة، واستخدام هذه القدرات في التخريب

وعمليّات التجسس، واعتمدت إيران إستراتيجيّة تم إعدادها وتجهيزها منذ سنوات، وإعداد هيكلها في إطار مؤسسي، وَفْق رؤية أهداف وضعتها الجهات الحاكمة، وتقوم الإستراتيجيّة الإيرانيّة على الحرس الثوريّ، وقوات الباسيج، ومجموعات الميليشيات والفصائل الرقمية التابعة له مباشرة، وتدين بالولاء له، لتكون بمثابة كيان" افتراضي تأسس في عام 2005، ما يسمى بجيش الفضاء الإيرانيّ، الذي يعتبر أحد الأذرع الرقمية التي يستخدمها النظام الإيرانيّ لشن هجَمات إلكترونيّة على المعارضة ومناهضي النظام في العالم، أو الدول الكبرى التي تقف عائقًا أمام البرنامَج النوويّ الإيرانيّ، أو تطوير الصواريخ الباليستية، أو مجالات الاستخبارات، حيث وجدت إيران ميدانًا جديدًا وفاعلًا للمواجهة معَ أمريكيا وحلفائها، ومعارضي النظام في الداخل والخارج[1].

ولقد ساهم تعرض إيران للعديد من التهديدات السيبرانيّة الداخليّة والخارجيّة في تحولها نحو تطوير قدراتها السيبرانيّة الهجوميّة والدفاعيّة بقوة غير مسبوقة وعالية؛ للحفاظ على استقرار النظام الداخليّ، وتأمين البنية التحتيّة للدولة، ولهذا السبب أنشأت إيران عددًا من الهيئات الداخلية لتعزيز قدراتها السيبرانيّة الهجوميّة والدفاعيّة. ومن تلك الهيئات المجلس الأعلى للفضاء الإلكترونيّ، وهو أعلى سلطة في هذا المجال؛ لأنه يضم كبار المسؤولين من رئيس الدولة ووزراء الاتصالات، والثقافة، والعلوم، وغيرهم من أجهزة الأمن، والاستخبارات، والقضاء، والبرلمان. ويهتم المجلس بشكل أساس بتنسيق جهود الدفاع والهجوم السيبرانيّ، وإعداد السياسات العامة التي يتوجب على المؤسسات ذات العلاقة بالفضاء السيبرانيّ تنفيذها. كما تم إنشاء منظمة (قيادة الدفاع الإلكترونيّ) لحماية البنية التحتيّة لإيران من المخاطر السيبرانيّة، وتعزيز الدفاعات الإلكترونيّة، حماية

(1) الميموني، الجبهة النشطة تداعيات المواجهة السيبرانيّة بين إيران وإسرائيل، ص68-69.

أنظمة مؤسسات الدولة [1].

تأسس (الجيش الإلكترونيّ الإيرانيّ)، وهو موجه بشكل أساسيّ لتنفيذ الهجَمات الإلكترونيّة الخارجية، كونه كيانًا غير رسمي، ويضم مجموعة كبيرة من المتسللين المحترفين ، يقال: إن معظمهم من الروس لدعم المتسللين الإيرانيّين بالتعاون معَ الحرس الثوريّ، وقد شَنَّ الجيش الإلكترونيّ الإيرانيّ سلسلة من الهجَمات رفيعة المستوى على مواقع شهيرة لتكون في دائرة الضوء على عالميًّا، ويرسل رسائل ذات طبيعة سياسيّة أكثر من الحرب ذاتها، خاصة عندما هاجم ونجح في اختراق كل من موقع "توتير Twitter" في عام 2009، وموقع "بايدو Baidu"، وهو محرك البحث الأكثر شهرة في الصين في عام 2010، وكذلك وموقع "صوت أمريكيّاThe Voice of America "[2]. كما قامت إيران بتأسيس مقر الدفاع الإلكترونيّ في تشرين الأول (أكتوبر) 2011، وأصبحت من ضمن الدول ذات المنظومة الدفاعية المتكاملة في التصدي لتهديدات الحرب الإلكترونيّة، وظهر ذلك في نجاح إيران في احتواء فيروس "دوكوduku " في بداية عام 2012 بعد ساعة من إطلاقه[3].

ثانيًا: الهيكل السيبرانيّ الإيرانيّ:

يرى العديد من الخبراء أنّ الاختراق الإيرانيّ الإلكترونيّ كان سريعًا، ومكّنها من بناء قدرة إلكترونيّة تنافس الولايات المتحدة، والصين، وروسيا، بريطانيا، و(إسرائيل)، وهي أكثر الدول فاعلية وهيمنة في الفضاء الإلكترونيّ. ووَفْقًا لوثائق وكالة المخابرات الأمريكيّة التي نشرها إدوارد سنودن في عام 2013،

(1) راشد، نمو متصاعد للقدرات الإيرانيّة في مجال الحرب الإلكترونية.

(2) العتوم، الفضاء الإلكتروني الإيرانيّ.

(3) محمو، دور الحروب الالكترونية في الصراع الإيرانيّ الإسرائيلي http://www.acrseg.org/41764.

كثفت إيران من مراقبتها لحكومة الولايات المتحدة. ووصفت إحدى تلك الوثائق، التي كتبها الجنرال كيث ألكسندر، المدير السابق لوكالة الأمن القوميّ، التهديد بأنّه خطير بما يكفي لأنْ تطلب الولايات المتحدة المساعدة من بريطانيا لاحتواء الضرر الناجم عن (اكتشاف إيران لأدوات استغلال شبكات الكمبيوتر) –وهو مصطلح يعبر عن الأسلحة السيبرانيّة[1]، والسبب في التقدم السريع لقدرات إيران السيبرانيّة، هو فيروس Stuxnet الذي ضرب البرنامج النوويّ الإيرانيّ، وأوقع فيه ضررًا كبيرًا، ففي وثيقة أخرى نشرها سنودن، ذكرت وكالة الأمن القوميّ الأمريكيّة أنّ إيران " أظهرت قدرة واضحة على التعلم من قدرات الآخرين وتصرفاتهم"[2]، وقد تميزت إيران في بناء الشبكات الإلكترونيّة في جميع أنحاء العالم، وتستخدم طريقة غير مكلفة للتدريب والتعاون معَ الوكلاء، كما تدعم القدرات الإلكترونيّة لأذرعها العسكريّة في لبنان واليمن وسوريا والعراق. وخصصت في يوليو 2012، مليار دولار لتعزيز قوتها السيبرانيّة، والاستثمار في التِقْنِيّات الهجوميّة والدفاعيّة الجديدة، وتوظيف كادر من القراصنة وتدريبهم. كما شكلت مجموعة من الوكالات المحليّة المكلفة بإدارة شؤون الفضاء الإلكترونيّ[3]. ومن الجهات التي تصدر قرارات تنظيم الهجَمات السيبرانيّة في إيران، أو ممن تشرف على تنفيذه[4]:

1. **المرشد الأعلى علي خامنئي** – صانع القرار النهائي في جميع قضايا الأمن الداخليّ والوطنيّ؛ يمارس سيطرة مباشرة على الحرس الثوريّ الإيرانيّ والقوات المسلحة والأجهزة الأمنيّة.
2. **المجلس الأعلى للأمن القوميّ:** أعلى هيئة لصنع سياسات الأمن

(1)Brunn, Iran Has Built an Army of Cyber-Proxies, Link https://bit.ly/41ZOLLw.

(2) Ibid.

(3) Berman, Cyberwar And Iranian Strategy, Linkhttps://bit.ly/423Q5Nc.

(4) النعيمي، عزي، فريد، النشاط السيبرانيّ الإيرانيّ، https://bit.ly/3AtPnNL.

القوميّ. يتلقى توجيهات من المرشد الأعلى؛ ويضم في عضويته رئيس الجمهوريّة والبرلمان، ورئيس القضاء، والوزراء، وقادة الجيش.

3. **المجلس الأعلى للفضاء الإلكترونيّ:** يشرف على سياسة الإنترنت والفضاء الإلكترونيّ؛ ويقدم تقاريره إلى المرشد الأعلى علي خامنئي، ويضم في عضويته الرئيس والوزراء وقائد الحرس الثوريّ الإيرانيّ وغيرهم من كبار المسؤولين من أجهزة المخابرات والأمن ومَهَمَّته حفظ البلاد من المحتوى السلبي للفضاء السيبرانيّ.
4. **الحرس الثوريّ الإيرانيّ:** بالإضافة إلى وحدات الحرب الإلكترونيّة، يوظف الحرس الثوريّ الإيرانيّ مجموعات من المتسللين الإيرانيّين 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 الاجتماعيّة الغربيّة و(الإسرائيليّة)، والتسبب في أعطالهم، بالإضافة إلى الاحتيال الائتماني، والتسلل إلى قواعد البيانات والمؤسسات الماليّة.
5. **وحدات الباسيج:** تشارك وحدات الباسيج غير العسكريّة بنشر التعليقات على كثير من المواقع، وهم مشغلون غير محترفين، يقومون بعمليّات اختراق أو تسلل بسيطة ضد أعداء النظام في الداخل.
6. **الشرطة الإلكترونيّة (FETA):** تعمل على (التحكم) في مستخدمي الإنترنت، من خلال ممارسة الضغط على مزودي خدمة الإنترنت، وإجبارهم على تقديم معلومات عن مستخدمي الشبكة. وهي مسؤولة كذلك عن مكافحة ما يسمى بـِ(الجرائم السياسيّة والأمنية)، باستخدام مجموعة

من المتسللين لاختراق مواقع الويب وحسابات البريد الإلكترونيّ للمعارضين.

7. **لجنة تحديد المواقع غير المصرح بها:** شكّلها المجلس الأعلى للثورة الثقافية في يوليو 2009، الذي يخضع لسيطرة المرشد الأعلى، ويعمل على حصر المواقع التي لم يتم الموافقة على عمليّاتها من النظام لأسباب مختلفة، تتألف هذه اللجنة من أعضاء، مثل: النائب العام، والقائد العام للشرطة، ورئيس جهاز الإذاعة والتلفزيون الحكوميّ، ووزراء الثقافة، والاستخبارات، والاتصالات، والعلوم.

وفي ضوء ما تقدم تشير التطورات إلى ظهور حقبة جديدة من السيبرانيّة قد لا تصل تفاعلاتها إلى مستوى استخدام القوة أو الحرب، لكنّها تسعى إلى تحقيق تأثيرات إستراتيجيّة أو تكتيكيّة محددة تؤثر في سلوك الدول المعادية.

ثالثًا: الإستراتيجيّة (الإسرائيليّة) في الحرب الإلكترونيّة:

ترى الأجهزة الأمنيّة (الإسرائيليّة) أنّ الهجَمات السيبرانيّة مجهولة المصدر، وفي الوقت ذاته مدمِّرة، تشنّ (حرب ظلال سريّة) خلف لوحة المفاتيح، وتصنفها بأنّها أكثر الأسلحة المضادة للجيش (الإسرائيليّ)، وتستهدف بالعادة مرافق البنية التحتيّة في (إسرائيل)، وهي هجَمات كفيلة بتعطيلها، وانهيار أجهزتها الحاسوبيّة. وقد مضى على دخول (إسرائيل) في الحروب التكنولوجيّة قرابة 16 عامًا، ولا تتردد في الاعتراف بأنّ الهجَمات الإلكترونيّة هي معركة عقول استخباريّة شرسة معَ أعدائها من المنظمات والدول، ولهذا يجمع الجيش والأمن معلومات عن المهاجمين المحتملين الذين يخططون لاقتحام شبكات عمليّاتية

(إسرائيليّة).[1]

تمتلك (إسرائيل) قدرات متقدمة في مجال الحرب السيبرانيّة، وتتفوق على القدرات الإيرانيّة، إذ تعُّد (إسرائيل) من كبرى الدول في مجال السايبر عالميًّا، فلقد امتّدت الجهود (الإسرائيليّة) في السايبر منذ إنشاء وحدة الاستخبارات العسكريّة بالجيش (الإسرائيليّ) (الوحدة 8200)، التي تهتم بجمع المعلومات، وتقوم بعمليّات الاستهداف الإلكترونيّ، فقلد أسسها عام 1948، نخبة من مهندسي الكمبيوتر الخبراء، لتشمل جميع المجالات السيبرانيّة الهجوميّة والدفاعيّة، وكذلك لتنفيذ التجسس والتنصت، وجمع المعلومات، ومراقبة الأنشطة العدائيّة على الإنترنت ومواقع التواصل الاجتماعيّ[2]، وبعد سلسلة من الهجَمات التي تعرضت لها عدد من المنشآت في (إسرائيل)، أنشأت (إسرائيل) وحدة إلكترونيّة في عام 2015، متخصصة لتكون شبكة دفاع ضد الهجَمات الإلكترونيّة[3].

عملت (إسرائيل) على مسارين لمواجهة الهجَمات الإلكترونيّة (السايبر)، أولهما: المسار الدفاعي، حيث تعتقد أنّ جيشها هدف جذاب للهجَمات المعادية، ولا يمكنه تحمل الخسارة، وكجزء من الخطة المتعددة السنوات (جدعون) قرر رئيس الأركان السابق (غادي آيزنكوت) إنشاء نظام سيبرانيّ، لتشغيل وحدة إلكترونيّة للدفاع عن البنية التحتيّة العسكريّة والمدنيّة من أي هجوم خارجيّ. أما الثاني فهو: المسار الهجوميّ، قامت (إسرائيل) بتنفيذ عدد من الهجَمات الإلكترونيّة، أدت لتعطيل بعض مرافق بنى تحتيّة في دول بعينها، دون إعلان

(1) أبو عامر، هكذا تخوض إسرائيل جبهتها القتالية الجديدة عبر https://bit.ly/4493p4Y.

(2)عيتاني، الوحدة الإسرائيليّة 8200 ودورها، https://bit.ly/3V7XGZ5.

(3) الميموني، الجبهة النشطة تداعيات المواجهة السيبرانيّة، ص73.

مسؤوليتها عنها، لكنّ تبعاتها ونتائجها كانت خطيرة، وتمثل بعضها في انهيار أجهزتها الحاسوبيّة، وتعطيل حركة السفن لأيام طويلة، وهكذا ظهرت الحرب الإلكترونيّة (الإسرائيليّة) بشكل علني بعد أنْ كانت غير معلنة. [1]

رابعًا: الهيكل السيبرانيّ (الإسرائيليّ):

لقد تحدت التطورات المتعددة في قطاع الحرب الإلكترونيّة المفاهيم السائدة حول الأمن القوميّ، وصرح وزراء في (إسرائيل) بأنّ التصدي للتهديد المستجد نتاج تطور تكنولوجيّ للحرب السيبرانيّة، فيتلاءم معَ عقيدة الأمن القوميّ (الإسرائيليّ)، فما زالت الركائز التي تستند عليها عقيدة الأمن القوميّ الإسرائيليّ تصلح للتصدي للهجَمات السيبرانيّة، هي[2]:

1. **الردع:** تكمن القدرات السيبرانيّة في ردع أعدائها، فمثلًا: التغطية الإعلاميّة الواسعة التي اتبعت على خطى فيروس (ستاكنس نت)، الذي استخدم لتخريب أنظمة الكمبيوتر التي تتحكم في منشآت تخصيب اليورانيوم في إيران، المنسوبة إلى الولايات المتحدة، شكّل قفزة نوعية في القدرة الهجوميّة السيبرانيّة للدول وقوتها ونفوذها، ما ساهم في تعزيز الردع (الإسرائيليّ).
2. **الإنذار المبكر:** إنّ القدرات السيبرانيّة ستمكّن (إسرائيل) من جمع المعلومات عن أعدائها، في الوقت ذاته ستمنع أولئك من الوصول إلى قاعدة بياناتها، وهذا يُعد إنذارًا فعالًا بشأن نيّة أعدائها.
3. **الحسم:** تُعد (إسرائيل) من الدول المتقدمة في العالم من حيث القدرات السيبرانيّة؛ ما يمنحها التفوق في المعارك، من خلال الاستخدام القوي

(1) أبو عامر، هكذا تخوض إسرائيل جبهتها القتالية الجديدة، https://bit.ly/4493p4Y.
(2) برعام، تأثير تطور تكنولوجيا الحرب السيبرانيّة، ص5.

لأسلحة الحرب السيبرانيّة المتقدمة بهدف إنهاء المعركة.

وتتنوع هيكلية إدارة السايبر في داخل (إسرائيل) على النحو الآتي[1]:

1. **الهيئة الرسميّة 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.
2. **هيئة الأركان السايبر القوميّة:** أُنشِئت في تشرين ثانٍ (يناير) 2010، وصرح رئيسها (افتيار متانيا) بأنّه يجب العمل على خمسة، يجب أن تتدخل الدولة فيها بما يخدم مسار الحرب السيبرانيّة، وهي:

- تطوير رؤية شاملة لجميع أنظمة الكمبيوتر على مستوى الدولة، يتطلب الدفاع السيبرانيّ تقييمًا متعدد الأنظمة؛ نظرًا للعلاقة الوثيقة بين الأنظمة الخاصة، والقطاع العام، وقطاع الأعمال.
- جمع الموارد والأنشطة والمعلومات من مصادر متعددة؛ ليتم تجميعها في هيئة واحدة؛ تحقيق الاستجابة المثلى لأيّ تهديد محتمل.
- التعاون الدوليّ في التواصل والتعاون معَ الحلفاء حول العالم.
- إطلاق مبادرات الدولة لتحفيز التنمية الأكاديميّة والصناعيّة في مجال الحرب الإلكترونيّة.
- تنسيق وتوحيد الجهود والإجراءات في المجال السيبرانيّ.

(1) برعام، تأثير تطور تكنولوجيا الحرب السيبرانيّة، ص 8-9.

3. **الحكومة الإلكترونيّة:** تم إنشاء شبكة في قسم المحاسب العام بوزارة المالية عام 1997، لتكون سلطة مَهَمّتها تسهيل معاملات المواطنين وتمكينهم من تنفيذ مجموعة من العمليّات معَ الوزارات والدوائر والهيئات العامة عبر الإنترنت معَ الحفاظ على سريّة المعلومات المرسلة وخصوصيّة المستخدم.

4. **سلطة القضاء والتكنولوجيا:** تم تأسيسها في أيلول (سبتمبر) 2006، حيث تم تكليفها بمهامّ حماية المعلومات الشخصيّة داخل (إسرائيل)، وتعزيز حماية البيانات الشخصيّة، وتنظيم ومراقبة استخدام التوقيع الإلكترونيّ، وتعزيز إنفاذ انتهاكات الخصوصيّة، بما في ذلك انتهاكات تكنولوجيا المعلومات التي تتم في الفضاء الإلكترونيّ.

المبحث الثالث: الهجَمات السيبرانيّة بين إيران و(إسرائيل):

شهدت الفترة الأخيرة تصعيدًا غير مسبوق في الحرب السيبرانيّة ما بين إيران و(إسرائيل)، تنوعت هجَماتها السيبرانيّة ما بين مدنية وبُنى تحتيّة في كلا الطرفين، وتحولت الحرب السيبرانيّة إلى واحدة من الوسائل المُهِمة في حرب الظل بين إيران و(إسرائيل)، حيث تهدف كل منهما لإلحاق الضرر بالآخر من جهة، وردعه من جهة أخرى، ويُظهر كل طرف قدراته السيبرانيّة في مجال الدفاع والهجوم في هذه الحرب القائمة بينهما.

لعبت الهجَمات السيبرانيّة دورًا مُهِمًّا في الردع الإسرائيليّ اتجاه إيران، التي تكتشف شيئًا فشيئًا القدرات الهجوميّة (الإسرائيليّة). وبالاستناد إلى مصادر أمنيّة، تملك (إسرائيل) القدرة على القيام بهجَمات سيبرانيّة على منشآت نوويّة لإيران، وعلى أهداف عسكريّة ومدنيّة في وقت واحد. هذه الهجَمات تجري دون

أنْ تترك (توقيعًا)، وهي تُستخدم لممارسة ضغط على إيران بموازاة الضغط السياسيّ في موضوع الاتفاق النوويّ.

جرى في تموز (يوليو) 2010، تسريب فيروس (ستا كنسيت) إلى حواسيب منشآت نوويّة في بوشهر ونتانز، في الشهر ذاته من عام 2010، حدث انفجار كبير دمر منشأة أجهزة طرد مركزي متطورة في نتانز. اعتقد الإيرانيّون في بداية الأمر أنّ عَبْوة ناسفة كبيرة هي التي تسببت بالانفجار، لكنهم درسوا وتبين لهم أنّ الانفجار حدث إثر هجوم سيبرانيّ (إسرائيليّ)؛ ففي 2019، هوجمت مِئات المواقع (الإسرائيليّة) على الإنترنت على يد قراصنة إيرانيّين؛ من أجل إرباك شبكة الإنترنت وبلبلتها. حيث يملك الإيرانيّون قدرات سيبرانيّة متفوقة، فإيران دولة متقدمة جدًّا في مجال التكنولوجيا و(إسرائيل) قلقة جدًّا من هذه القدرات، حيث لدى (إسرائيل) قناعات بأنّ الإيرانيّين سيزيدون هجَماتهم السيبرانيّة على بنى مدنيّة وخدمات حيويّة فيها، مثل: المياه والكهرباء، وسيحاولون المس بالاقتصاد (الإسرائيليّ)، وفي وقت الحرب سيحاولون ضرب الجبهة الداخليّة في (إسرائيل) بواسطة الهجَمات السيبرانيّة وخلال شباط (فبراير) 2020، تعرضت شبكة الإنترنت في إيران لهجَمات سيبرانيّة كثيرة شلّت نحو 25% من نشاطها، وفي تقدير الإيرانيّين أنّ (إسرائيل) كانت وراء ذلك. غير أنّ الإيرانيّين لم يقفوا مكتوفي الأيدي؛ فقاموا بشن هجَمات سيبرانيّة مضادة على (إسرائيل).[1]

كما تعرضت عدة منشآت تابعة لسلطة المياه (الإسرائيليّة) لهجوم إلكترونيّ في نيسان (أبريل) 2020، على منشآت تابعة لسلطة المياه (الإسرائيليّة)، وذكرت مصادر (إسرائيليّة)، أنهم تعاملوا معَ الحادث من خلال الوحدة السيبرانيّة (الإسرائيليّة)، وورد في تقرير رئيس سلطة المياه (الإسرائيليّة)، أنّ سلطة المياه تعرضت لهجوم إلكترونيّ، ولم ينتج عنه أيّ ضرر، وقد تم توجيه العاملين في

(1) بن مناحيم، "الحرب السيبرانيّة بين إيران و(إسرائيل)"، https://bit.ly/3Awod8L.

مصلحة المياه بتغيير كلمات المرور للأنظمة الرئيسة، وفصل بعض الأنظمة من شبكة الإنترنت، وذكر الجانب (الإسرائيليّ) أنّ الهجوم كان يهدف إلى تعطيل أجهزة الكمبيوتر التي تتحكم في توزيع المياه المعالجة من مياه الصرف الصحي ومضخات كورين والمواد الكيميائية المستخدمة في عملية المعالجة[1].

اعتبرت (إسرائيل) الهجوم السيبرانيّ على مصلحة المياه تجاوزًا للخطوط الحمراء، وردّت عليه بصورة كبيرة؛ من أجل القيام بعملية ردع لإيران لمنعها القيام بمحاولة أخرى، حيث شمل الرد ضرب بُنى تحتيّة ومدنيّة إيرانيّة، كما تم استهداف منشآت عسكريّة عبر سلسلة من التفجيرات وإشعال النار فيها، وتم قطع الكهرباء عن مناطق مختلفة في إيران من خلال هجَمات سيبرانيّة، كما استغلت شن هجَمات سيبرانيّة بين الطرفين بشكل مكثف، ما جعل الهجَمات السيبرانيّة مركبًا مركزيًّا في حرب الظل بين البلدين، ففي عام 2021، سجلت (إسرائيل) نسبة 20% مقارنة بعام 2020، في الهجَمات السيبرانيّة بين إيران و(إسرائيل)[2].

ونفذت (إسرائيل) في 18 مايو (آيار) 2020، هجومًا إلكترونيًّا استهدف ميناء شهيد رجائي الإيرانيّ، الذي يطل على مضيق هرمز، ما تسبب في تعطيل الملاحة عبر الممرات والطرق المؤدية إلى الميناء، واعتبر ذلك انتقامًا لمحاولة الهجوم الإلكترونيّ الإيرانيّ على أنظمة سلطة المياه في داخل (إسرائيل)، وقد ذكرت بعض التقارير أنّ الهجوم كان له أضرار كانت أخطر مما ورد في التقارير الإيرانيّة، حيث أشارت التقارير (الإسرائيليّة) إلى أنّ نظام الحماية السيبرانيّ الإيرانيّ المسمى الحصن الرقمي الذي تعتبره إيران قادرًا على الحماية من أي هجَمات سيبرانيّة، لم يكن فعالًا، وتم اختراقه عدة مرات[3].

(1) هارئيل، موانئ إيران تتعرض لهجوم سيبرانيّ، https://bit.ly/3Lz9256.

(2) برعام، بن وايشيك، الحرب السرية بين (إسرائيل) وإيران، https://bit.ly/3Lbrv6u.

(3) الميموني، الجبهة النشطة تداعيات المواجهة السيبرانيّة، ص 74-75.

وذكر الجيش (الإسرائيليّ)، في أيلول (سبتمبر) 2022، أن هناك زيادة بنحو 70% في حجم الهجَمات الإلكترونيّة الإيرانيّة ضد أهداف داخل إسرائيل، وقال الجيش: إنّ معظم تلك الهجَمات تم إحباطها، واصفًا الزيادة بأنّها (مقلقة). وقد أحدثت إحدى الهجَمات، التي استهدفت مستشفى (هليل يافا) في الخضيرة، أضرارًا في الأداء الطبيعيّ للمؤسسة الطبيّة، ما استلزم تدخل الجيش؛ فأرسل جنودًا من قطاع تكنولوجيا المعلومات والاتصالات لمساعدة المستشفى على تجاوز الأزمة، والعودة إلى طبيعته[1]. كما أشارت التقديرات (الإسرائيليّة) بأنّ عام 2022، شهد تصعيدًا غير مسبوق في الهجَمات السيبرانيّة من طرف إيران وأذرعها على (إسرائيل)، فقد أشار رئيس مؤسسة السايبر (غابي بورطنوي)، أنّ (إسرائيل) رصدت (1500) هجوم سيبرانيّ خلال عام 2021، أغلبها مصدرها عناصر إيرانيّة، كما أظهرت وحدة (8200) الاستخبارية عبر قائدها السابق (أيهود شنيؤورسون)، أنّ عامي (2021–2022)، شهد تصاعدًا واضحًا في الحرب السيبرانيّة بين إيران و(إسرائيل)[2].

حذّر قادة كبار في المؤسسة الأمنية والعسكريّة (الإسرائيليّة) من الحرب السيبرانيّة على الجبهة القتالية الجديدة التي لم تكن مدرجة على قائمة التهديدات قبل سنوات، فقد أكد رئيس جهاز الموساد السابق (تامير باردو)، أنّ "حروب السايبر جعلت من التهديد بالفوضى السلاح الأكثر تحقيقًا لانتصارات مستقبليّة؛ فأعداء (إسرائيل) لن يكونوا بحاجة لطائرات أو صواريخ، فقط باستطاعتهم حيازة إمكانات تكنولوجيّة وقدرات سيبرانيّة لمهاجمتها؛ لإحداث شلل في كافة مجالات

(1) الجيش (الإسرائيلي) ازدياد الهجمات السيبرانيّة الإيرانيّة بـ 70%، https://bit.ly/3AuOswu.

(2) مصطفي، تصعيد الحرب السيبرانيّة، https://bit.ly/3LzZaYO.

العمل فيها[1].

كما حذّر مصدر أمني (إسرائيليّ) رفيع المستوى من "امتلاك القوى المعادية لـ(إسرائيل) لهذه القدرات التقنيّة؛ لأنّها تمنحها إمكانية أنْ تشيطن (إسرائيل)، وهذا هو الكابوس، لأنّ (إسرائيل) باتت تشعر بأنّ طائرات (F-16) ، وأرتال الدبابات لن تحدث أضرارًا كما يمكن أنْ تقوم به هجَمات سيبرانيّة سريّة معادية." وقال (مائير حيون) قائد جهاز منع الجريمة والعنف في (إسرائيل): إنّ "بعض التحديات التي تواجهنا أنّ العناصر المخترقة من الهاكرز والقراصنة تمتاز بذكاء متقدم، ولا تترك خلفها آثارًا لتعقبها؛ لذلك نبذل جهودًا حثيثة لجمع المعلومات عنهم، إنّنا نخوض حربًا في مجال السايبر لا تتوقف، ونواجه تحدّيات داخليّة وخارجيّة في مجال الاختراقات الواردة من جهات معادية"[2].

رغم من محاولات اختراق الهجَمات الإلكترونيّة التي يتعرض لها الطرفان بشكل مستمر وغير معلن عنها في كثير من الأحيان، إلّا أنّ إيران تقوم بمناورات، وتضغط بجميع الأوراق التي لديها في محاولة لإيصال رسالة إلى العالم أنّها قادرة على الوقوف في وجه الولايات المتحدة و(إسرائيل)، وأنّها قادرة على التصرف والرد كلما تعرضت لأيّ ضغط ، وهذا يأتي ضمن الأوراق للتحرك في الفضاء الإلكترونيّ؛ لاستهداف ما تسميه الأعداء، كلما استهدفت المنشآت النوويّة الإيرانيّة من الأمريكيّين و(الإسرائيليّين)، شنت إيران هجَمات ضد المنشآت المدنية والعسكريّة ضد الولايات المتحدة و(إسرائيل).

وعند دراسة الهجَمات السيبرانيّة (الإسرائيليّة) ضد إيران في السنوات الأخيرة، يتبين أنّ أهدافها، هي:

- **التجسس:** جمع معلومات استخباراتيّة عن إيران بشكل عام والمشروع

(1) أبو عامر، هكذا تخوض (إسرائيل) جبهتها القتالية الجديدة، https://bit.ly/4493p4Y.

(2) أبو عامر، هكذا تخوض (إسرائيل) جبهتها القتالية الجديدة.

النوويّ بشكل خاص، من خلال التسلل إلى الأجهزة الإلكترونيّة، وأنظمة الاتصالات الخاصة بالمؤسسات الإيرانيّة أو الأفراد لجمع معلومات عنها.

- **الهجوم:** إلحاق الضرر بتقدم المشروع النوويّ الإيرانيّ من خلال شن هجَمات إلكترونيّة تهدف إلى إتلاف الأجهزة الإلكترونيّة العاملة في المشروع بهدف إعاقة الإيرانيّين عن التقدم في المشروع.
- **الردع:** تهدف الهجَمات (الإسرائيليّة) عبر استهداف المواقع، والخدمات المدنيّة، والحكوميّة، والاقتصاديّة، إلى ردع إيران عن شن هجَمات إلكترونيّة على (إسرائيل) بشكل عام، وعلى المواقع المدنية بشكل خاص.

من ناحية أخرى، تواجه إيران صعوبات في مواجهة الهجَمات الإلكترونيّة التي تنفذها (إسرائيل) ضدها، فقدرات إيران صغيرة مقارنة بقدرات (إسرائيل) في مجال السايبر، ومعَ ذلك نجحت إيران في تنفيذ هجَمات عطلت المواقع الحكوميّة لفترة قصيرة، وتعتبر إيران الحرب النفسية هي أحد أهدافها في الحرب السيبرانيّة بينهما. يعود عدم نجاح الهجَمات السيبرانيّة الإيرانيّة ضد (إسرائيل) إلى عدة أمور، من أهمها:

1. **نظام الدفاع السيبرانيّ (الإسرائيليّ) المتقدم:** على المستويات المدنيّة والعسكريّة والأمنيّة، حيث تنفق (إسرائيل) الكثير من الموارد في تطوير نظامها الدفاعي السيبرانيّ، وتنسق الوكالة الوطنيّة السيبرانيّة بين هذه الهيئات، ومؤسسات النظام المدني لا تقل أهميّة عن أنظمة الدفاع العسكريّة والأمنيّة.
2. **وجود وعي داخل (إسرائيل)** بالهجَمات السيبرانيّة، وتحديدًا في المؤسسات والمصالح الاقتصاديّة التي تدرك أهمية وجود منظومة من الدفاع السيبرانيّ؛ لحماية معلوماتها وأمنها الاقتصاديّ، وتكثر الشركات الخاصة

التي تقدم خدماتها في مجال الدفاع من الهجَمات السيبرانيّة للمؤسسات الخاصة.

3. **إنّ امتناع إيران عن التصعيد معَ (إسرائيل)** في الحرب السيبرانيّة، جزء من الردع الذي تقوم به (إسرائيل) ضد إيران، وتدرك إيران أنّ إلحاق الضرر بالمنشآت (الإسرائيليّة)، وخاصة المنشآت المدنية، سيجعل ردًّا (إسرائيليًّا) قويًّا على المؤسسات والمنشآت الإيرانيّة[1]. كما تعلم (إسرائيل) أيضًا أنّ رد إيران على الهجَمات الإلكترونيّة (الإسرائيليّة)، عبر أربعة اتجاهات، هي[2]:

الاتجاه الأول: تسريع خطوات استكمال المشروع النوويّ بأجهزة تخصيب اليورانيوم.

الاتجاه الثاني: توطيد الوجود العسكريّ الإيرانيّ في العراق وسوريا ولبنان.

الاتجاه الثالث: استمرار إنتاج الصواريخ ونقل التكنولوجيا الصاروخيّة المتطورة إلى حلفائها، مثل حزب الله اللبناني وحركة المقاومة الإسلامية (حماس).

الاتجاه الرابع: شن هجَمات إلكترونيّة تستهدف منشآت مدنية في (إسرائيل).

يمكن القول: إنّ الصراع بين إيران و(إسرائيل) يدخل مرحلة جديدة من مواجهة غير تقليديّة تمنح إيران فرصًا جديدة للمناورة والتأثير على الجبهة (الإسرائيليّة). ورغم من التفوق (الإسرائيليّ) في منظومة السايبر، إلا أنّها معرضة للتهديد من الهجَمات الإيرانيّة، كما تعمل إيران على تطوير قدراتها السيبرانيّة، لتكون أكثر قدرة على توجيه هجَمات سيبرانيّة مؤثرة على المؤسسات المدنيّة (الإسرائيليّة)، ومن المتوقع أنْ تزداد الهجَمات بين الطرفين في هذه الحرب، في ظل عدم إنهاء الملف النوويّ الإيرانيّ، معَ (استيعاب) إسرائيل بأنّ الحرب السيبرانيّة بينهما لا يمكن أنْ تمنع إيران من تطوير مشروعها النوويّ.

---

(1) مصطفي، تصعيد الحرب السيبرانيّة بين (إسرائيل) وإيران، https://bit.ly/3LzZaYO.

(2) محسن، القوة السيبرانيّة بُعد جديد في المواجهة، https://bit.ly/3nfeYqF.

نتائج الدراسة:

بعد الانتهاء من هذه الدراسة، بالإمكان التوقف عند بعض نتائجها:

1. أصبحت الحرب السيبرانيّة في ظل البيئة الإلكترونيّة المتطورة واقعًا حربيًّا تتصارع فيه الدول للتأثير بالهجَمات السيبرانيّة على خصومها وأعدائها، دون خسائر ماديّة وبشرية، فالحرب السيبرانيّة يمكن التحكم بها بخلاف الحرب التقليديّة التي تؤدي إلى خسائر بشرية وماديّة كبيرة.
2. إنّ الناظر للواقع، يرى أنّ البيئة الإلكترونيّة أصبحت بيئة خصبة للتنافس، وأصبحت الحروب السيبرانيّة حاضرة في الصراعات المستقبلية بشكل فعال، وسيكون لها الأثر الكبير في التأثير على البيئة السياسيّة والعسكريّة والأمنية وكذلك على الأمن القوميّ للدول.
3. قامت (إسرائيل) في الآونة الأخيرة وفي إطار الحرب الإلكترونيّة المتبادلة معَ إيران بتطوير أنظمة تستطيع التشويش والتأثير على ترددات الطوارئ الإيرانيّة، كما قامت بزرع العديد من العملاء والجواسيس التابعين لجهاز الموساد (الإسرائيليّ) في إيران، لمتابعة ورصد تحركات العلماء الإيرانيّين المختصين بالتطورات النوويّة في إيران؛ ليتم اغتيال عددٍ منهم؛ وذلك في سياق الحرب المعلوماتيّة والسرية التي تشنها (إسرائيل) على إيران.
4. المُرجح أنْ تشهد السنوات القادمة مزيدًا من التطورات سواء على مستوى الهجَمات التي تشنها المجموعات الإيرانيّة، أو على مستوى القدرات الدفاعية على صدَّ الهجَمات الخارجية، خاصة في ظل استمرار الاتهامات بين الولايات المتحدة و(إسرائيل) لإيران بمسؤوليتها عن هذه الهجَمات.
5. يمكن الإشارة إلى أنّ النظام الإلكترونيّ العالمي –قيْد التشكُّل–لن يُقصي إيران منه، أو أنْ يقدر على تحييد، أو تقويض طموحها الإلكترونيّ، بل

إنّه سيضع قدراتها في الحسبان قبل اتخاذ أيّ قرارات، أو شنَّ أي هجَمات على بنيتها الأساسيّة لما يتوقعه من رد فعل؛ قد يكون أكبر من الفعل سواء في المقدار أو الاتجاه.

مراجع الدراسة

أولًا: المراجع العربية:

1. إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية على الأمن القوميّ، العربي للنشر والتوزيع، ط1، القاهرة، 2019.
2. برعام، جيل، تأثير تطور تكنولوجيا الحرب السيبرانيّة على بناء القوة في (إسرائيل)، ترجمة يولا البطل مؤسسة الدراسات الفلسطينية، معهد دراسات الأمن القوميّ، جامعة تل أبيب، م5، ع1، 2013.
3. حكيم، غريب حكيم، الإرهاب السيبرانيّ والأمن الدوليّ والتهديدات العالميّة الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات، م5، ع 02، الجزائر، 2018.
4. ربيعي، حسين، وسمر، محمود، الحروب السيبرانيّة: المخاطر وإستراتيجيّات تحقيق الأمن السيبرانيّ الدوليّ والداخلي، المجلة الجزائرية للأمن الإنساني، ع2، 2022.
5. زروقة، إسماعيل، الفضاء السيبرانيّ والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسيّة، جامعة الشهيد حمة لخضر بالوداي، م10، ع 1، الجزائر ،2009
6. سعود، يحيي ياسين، الحرب السيبرانيّة في ضوء القانون الدوليّ الإنساني، المجلة القانونية، ع 4، جامعة القاهرة، 2018.
7. السمحان، مني، متطلبات تحقيق الأمن السيبرانيّ لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، ع111، 2020.
8. طارق إبراهيم، عطية الدسوقي، الأمن المعلوماتيّ النظام الدوليّ للحماية المعلوماتيّة، دار الجامعة الجديدة للنشر، مصر، 2009.
9. عبد العال، جيهان أحمد، الحروب السيبرانيّة دراسة في المفهوم والنشأة ومعدلات النجاح، المجلة العلمية للدراسات التجارية والبيئية(JCES) ، م 13، ع 2، 2022.
10. العبودي، علي عبد الرحيم، هاجس الحروب السيبرانيّة وتداعياتها على الأمن والسلم الدوليّين، مجلة قضايا سياسيّة، ع57، جامعة النهرين، العراق، 2019.
11. فرج، كرار عباس متعب، الحرب السيبرانيّة: دراسة في إستراتيجيّة الهجَمات السيبرانيّة بين الولايات المتحدة الأمريكيّة وإيران، مجلة حمورابي للدراسات، ع40، جامعة كربلاء، كلية الإدارة والاقتصاد، العراق، 2021.
12. الميموني، أحمد بن علي، الجبهة النشطة تداعيات المواجهة السيبرانيّة بين إيران

و(إسرائيل)، المعهد الدوليّ للدراسات الإيرانيّة، مجلة الدراسات الإيرانيّة، ع 12، 2020.

ثانيًا: المواقع الإلكترونيّة:

1. أبو عامر، عدنان، هكذا تخوض إسرائيل جبهتها القتالية الجديدة عبر (السايبر)، الجزيرة، متاح على الرابطhttps://bit.ly/4493p4Y ، تم الاطلاع بتاريخ 2023/04/24.
2. برعام، غيل، بن أبرهام، وايتسيك بن أبرهام، الحرب السرية بين (إسرائيل) وإيران: حرب الظل تخرج للنور، متاح على الرابطhttps://bit.ly/3Lbrv6u ، تم الاطلاع بتاريخ 2023/04/22.
3. بن مناحيم، يوني، "الحرب السيبرانيّة بين إيران و(إسرائيل)، متاح على الرابط https://bit.ly/3Awod8L، تم الاطلاع بتاريخ 2023/04/25.
4. الجيش (الإسرائيليّ) ازدياد الهجَمات السيبرانيّة الإيرانيّة بـ 70% ضد (إسرائيل)، متاح على الرابطhttps://bit.ly/3AuOswu ، تم الاطلاع بتاريخ 2023/04/24.
5. راشد، باسم، نمو متصاعد للقدرات الإيرانيّة في مجال الحرب الإلكترونيّة، متاح على الرابط https://bit.ly/2O0vjli، تم الاطلاع بتاريخ 2023/04/24.
6. علو، أحمد، الحروب السيبرانيّة والعنف الرقمي واقع عالمي جديد، مجلة الجيش، ع 402، لبنان، 2018، متاح على الرابطhttps://bit.ly/41ItNRm ، تم الاطلاع في تاريخ 2023/04/20.
7. العتوم، نبيل، جيض الفضاء الإلكترونيّ الإيرانيّ، مركز التفكير الإستراتيجيّ، متاح على الرابط الإلكترونيّ https://bit.ly/41KOlZC، تم الاطلاع بتاريخ 2023/04/23.
8. عيتاني، فاطمة حسان، الوحدة (الإسرائيليّة) 8200 ودورها في التكنولوجيا التجسسية (الإسرائيليّة)، متاح على الرابط الإلكترونيّhttps://bit.ly/3V7XGZ5 ، تم الاطلاع بتاريخ 2023/04/23.
9. محسن، شادي، القوة السيبرانيّة بُعد جديد في المواجهة بين إيران و(إسرائيل)، المركز المصري للفكر والدراسات الإستراتيجيّة، متاح على الموقع الإلكترونيّ https://bit.ly/3nfeYqF، تم الاطلاع في تاريخ 2023/04/25.

10. محمود، آيه حسين، دور الحروب الإلكترونيّة في الصراع الإيرانيّ (الإسرائيليّ) (2006–2017)، المركز العربي للبحوث والدراسات، متاح على الرابط الإلكترونيّ http://www.acrseg.org/41764، تم الاطلاع بتاريخ 2023/04/21.
11. مصطفي، مهند، تصعيد الحرب السيبرانيّة بين إسرائيل وإيران، مركز الأمارات للسياسات، متاح على الرابط https://bit.ly/3LzZaYO، تم الاطلاع في تاريخ 2023/04/18.
12. موقع الجندي، الحرب السيبرانيّة. نتائج ملموسة لغير معارك مرئيّة، متاح على الرابط https://bit.ly/40GQzI4 ، تم الاطلاع في تاريخ 2023/04/20.
13. موقع سايبر وان، ما هي الحرب السيبرانيّة؟ وما مدى خطورتها؟، متاح على الرابط https://bit.ly/3HgLxLJ ، تم الاطلاع في تاريخ 2023/04/22.
14. النعيمي هدى، عزي، محمد فريد، مترف، عبد الله خليفة، النشاط السيبرانيّ الإيرانيّ: ما بين السرية والعلن، متاح على الرابط https://bit.ly/3AtPnNL، تم الاطلاع بتاريخ 2023/04/22.
15. هارئيل، عاموس، موانئ إيران تتعرض لهجوم سيبرانيّ، متاح على الرابط https://bit.ly/3Lz9256، تم الاطلاع في تاريخ 2023/04/19.
16. وكالة الأناضول، الحرب السيبرانيّة... تهديدات حقيقية من العالم الافتراضي، متاح على الرابط https://bit.ly/41HDEa2، تم الاطلاع في 2023/04/22.
17. Berman, Ilan Cyberwar And Iranian Strategy, Linkhttps://bit.ly/423Q5Nc, Accessed on 23/04/2023.
18. Brunn, Jordan, Iran Has Built an Army of Cyber-Proxies, Link https://bit.ly/41ZOLLw, Accessed on 23/04/2023.