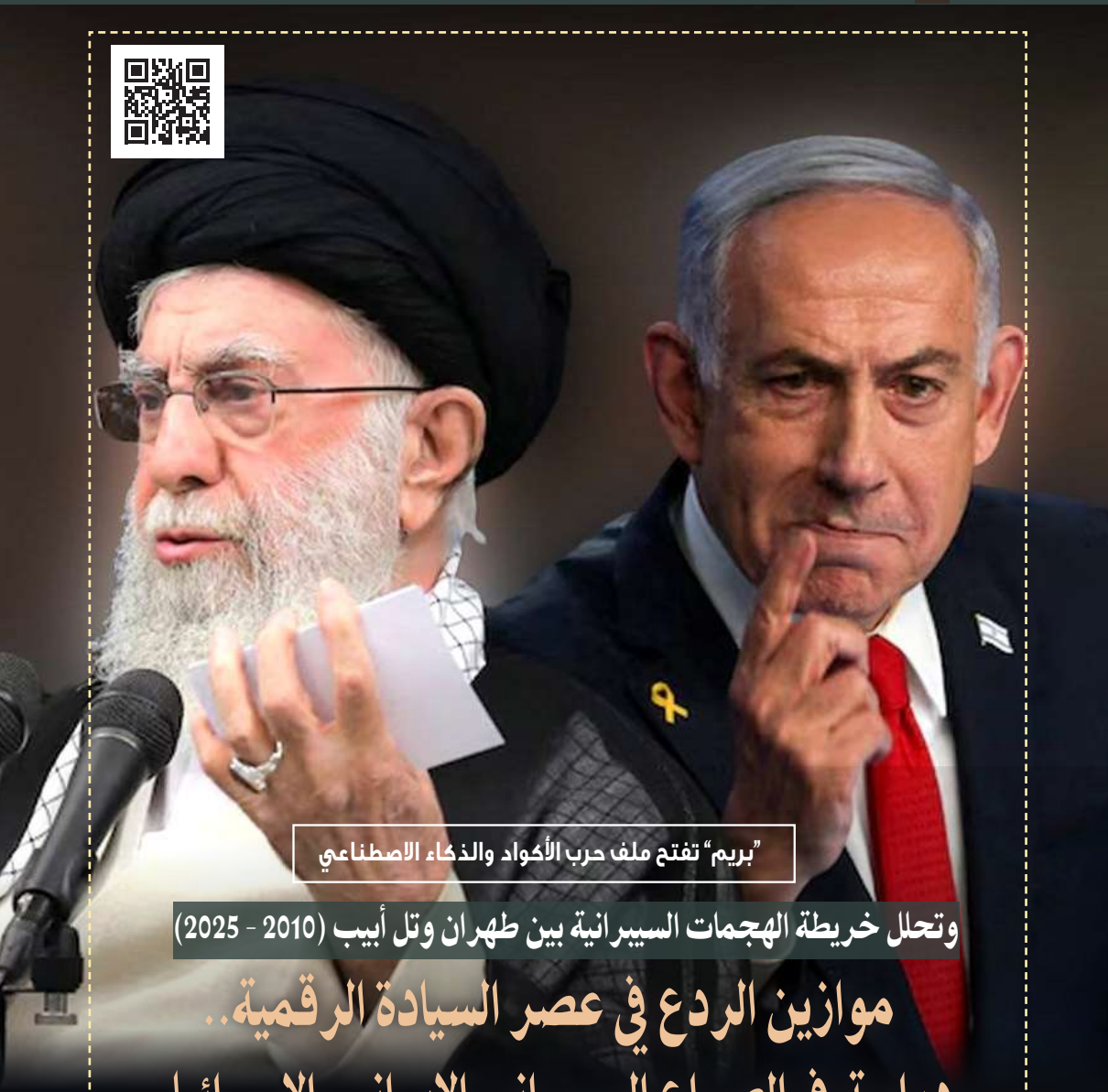
بريم
Perim
مجلة شهرية تحليلية تصدر كل شهر
تهتم بقضايا الدول المشاطئة على البحر الأحمر وخليج عدن
العدد: (16) - يونيو/ شباط 2025



"بريم" تفتح ملف حرب الأكواد والذكاء الاصطناعي

وتحلل خريطة الهجمات السيبرانية بين طهران وتل أبيب (2010 - 2025)

موازين الردع في عصر السيادة الرقمية..
دراسة في الصراع السيبراني الإيراني-الإسرائيلي

تهتم بقضايا الدول المشاطئة على البحر الأحمر وخليج عدن
تصدر عن مؤسسة اليوم الثامن للإعلام والدراسات

Political and Economic Magazine Concerned with the Issues of the Red Sea and Gulf of Aden Countries - Published by the alyoum8th Foundation for Media and Studies

العدد: (16) - يونيو/ شباط 2025

مجلة سياسية اقتصادية تهتم بقضايا الدول المشاطئة على البحر الأحمر وخليج عدن، صادرة عن مؤسسة اليوم الثامن للإعلام والدراسات، وتحمل ترخيص رقم (0693).
تأسست في مدينة عدن جنوب اليمن في فبراير/ شباط العام 2024م
العنوان - جنوب اليمن - عدن - البريقة
للتواصل
واتساب: 00967777491124
ايميل: perimjournal@gmail.com
الموقع الإلكتروني:
perimjournal.com - perimjournal.net

للإعلان في مجلة بريم

كن حيث يُصنع التأثير

تسرّ مجلة بريم، المجلة الفصلية المتخصصة في قضايا البحر الأحمر والأمن الإقليمي، أن تفتح أبوابها أمام المؤسسات والشركات والجهات الفاعلة للإعلان ضمن صفحاتها المرموقة

إن إعلانك في "بريم" ليس مجرد مساحة دعائية، بل هو حضور استراتيجي في منصة نخبوية تُقرأ من قبل صانعي القرار، الباحثين، الصحفيين، والمهتمين بالشأن السياسي والاقتصادي والأمني في المنطقة

لماذا تعلن في "بريم"؟

- توزيع إقليمي ودولي يضمن وصول إعلانك للفئات المؤثرة.
- محتوى تحليلي متخصص يعزز من مصداقية الإعلان.
- تصميم احترافي يُبرز علامتك التجارية بأفضل صورة.
- حضور ضمن عدد يُناقش قضايا الساعة: "التهريب، النفوذ الإقليمي، الأمن البحري"

كن شريكًا في المعرفة والتأثير. واحجز مساحتك الآن.

للتواصل والاستفسار:

perimjournal@gmail.com

00967777491124

تابعنا: perimjournal.com – perimjournal.net

شروط وضوابط النشر

1. أصالة البحث:
يجب أن يكون البحث جديدًا وأصيلًا، ولم يسبق نشره في أي وسيلة من وسائل النشر، سواء الورقية أو الإلكترونية

2. القيمة العلمية:
يشترط أن يُمثّل البحث إضافة علمية واضحة، سواء كانت نظرية أو تطبيقية

3. حجم البحث وإعداد الصفحات:
- ألا يتجاوز البحث (20) صفحة بقياس (B5)
- يجب ترك هامش لا يقل عن (3 سم) من جميع جوانب الصفحة

4. تحكيم البحوث:
- تخضع جميع البحوث المقدمة للتحكيم العلمي
- يُقبل البحث للنشر في حال اتفق اثنان من المحكّمين على صلاحيته، بعد إجراء التعديلات المطلوبة

5. محتوى الصفحة الأولى:
- تتضمن الصفحة الأولى: عنوان البحث، اسم الباحث/الباحثين، وملخصًا لا يتجاوز (100) كلمة

6. طريقة التقديم:
- يُقدّم البحث بنسخة إلكترونية بصيغة (Word)
- تُرسل النسخة إلى بريد المجلة الإلكتروني: perimjournal@gmail.com
- يجب أن تتضمن الرسالة البيانات التالية:
- عنوان البحث
- اسم الباحث/الباحثين
- الرتبة العلمية والوظيفة الحالية
- رقم الهاتف والبريد الإلكتروني

7. الملخص والمستخلص:
- يُرفق بالبحث ملخصان (بالعربية) لا يزيد كلّ منهما عن (100) كلمة، ويتضمّنان
- موضوع البحث
- الأهداف
- المنهج
- أبرز النتائج والتوصيات
- كلمات مفتاحية (لا تزيد عن خمس كلمات)

8. توثيق المراجع:
- يجب ترتيب المراجع حسب تسلسل ورودها في متن البحث

9. مسؤولية المحتوى:
- الآراء الواردة في البحوث المنشورة تعبّر عن أصحابها فقط، ولا تعكس بالضرورة رأي المجلة

10. لغة النشر:
- تقبل المجلة البحوث باللغتين: العربية أو الإنجليزية

محتويات العدد

بريم Perim الافتتاحية

منـذ أن ضرب فيروس "سـتاكس نـت" منشـآت نطنـز النوويـة الإيرانيـة عـام 2010، والعـالم يشـهد انتقـالًا حـاسمًا في مشـهد الصراع الـدولي، حيـث لم تعـد الحـروب تـدار في ميادين مكشـوفة، بـل باتـت تُخـاض في فضـاءات خفيـة، بلا جنـود ولا دبابـات، ولكـن بأكـواد مدمـرة، وذكاء اصطناعـي لا يرحـم

لقـد دخلنـا عصرًا جديـدًا مـن الحـروب غير التقليديـة، تتـكسر فيـه الحـدود الجغرافيـة، وتُعـاد فيـه صياغـة مفاهيـم السـيادة، والـردع، والأمـن القومـي. وفي قلـب هـذا التحـول، تتصـدر الحـرب السـيبرانية بين إيـران وإسرائيـل واجهـة المواجهـات الجيوسياسـية المعـاصرة، بوصفهـا نموذجًـا مثاليًـا لحـروب غير متناظـرة، تتداخـل فيهـا أدوات التقنية مـع استراتيجيات الدولـة، ويُعـاد فيهـا تعريـف مفهـوم القـوة

في هـذا العـدد الخـاص، تفتـح مجلـة "بريـم" ملـف الصراع السـيبراني الإيراني-الإسرائـيلي بين عامـي 2010 و2025، في دراسـة معمّقـة توثـق أبـرز الهـجمات، وتشرح بنيتهـا التقنيـة، وتفـكك دلالاتهـا السياسـية والعسـكرية. كما تناقـش الدراسـة كيـف تحولـت الفضـاءات الرقميـة إلى مسـارح مركزيـة لـلصراع، وميادين ردع بديلـة في ظـل اخـتلال موازيـن القـوة التقليديـة

إننـا أمـام لحظـة مفصليـة، تتطلـب فـهمًا جديـدًا لطبيعـة التهديـدات العابـرة للحـدود، وتفـكيرًا نقديًـا في مسـتقبل الأمـن والاسـتقرار في الشرق الأوسـط والعـالم. فهـل نملـك مـا يكفـي مـن أدوات التشـخيص والاسـتشراف؟ وهـل تسـتطيع القـوانين الدوليـة مواكبـة سرعـة الاختراقـات والتصعيـدات الرقميـة؟

بين أسطر هذا العدد، نحاول الإجابة... أو على الأقل فتح النقاش.

رئيس التحرير

ملف العدد

الحروب السيبرانية المتبادلة بين إسرائيل وإيران (2010 - 2025)

دراسة تحليلية

☐ د. صبري عفيف العلوي

مدير تحرير مجلة بريم الصادرة عن مؤسسة اليوم الثامن للإعلام والدراسات

الملخص:

تتناول هذه الدراسة موضوع الحرب السيبرانية وتحوّلات القوة والصراع في النظام الدولي، من خلال تحليل الإطار المفاهيمي والنظري لهذه الظاهرة، واستعراض تطبيقاتها المعاصرة، مع التركيز على الحالة الإسرائيلية – الإيرانية خلال الفترة من ٢٠١٠ إلى ٢٠٢٥. وقد سعت الدراسة إلى فهم كيف أعادت الفضاءات الرقمية صياغة مفاهيم القوة، والردع، والسيادة، وأثّرت في هيكل الصراع الجيوسياسي، من خلال توظيف تقنيات متقدمة كالهجمات السيبرانية، والذكاء الاصطناعي، والأنظمة النووية

انطلقت الدراسة من فرضية أساسية مفادها أن الحرب السيبرانية لم تعد مجرد نشاط تقني أو استخباراتي، بل أصبحت بُعدًا استراتيجيًا في معادلات الردع والصراع الدولي، وخصوصًا في حالات التنافس بين خصوم يمتلكون قدرات غير متماثلة، كما هو الحال في الصراع بين إسرائيل وإيران

اعتمدت الدراسة على منهج تحليلي-تركيبي متعدد المستويات، حيث تم تقسيمها إلى خمسة مباحث رئيسية

المبحث الأول تناول الإطار النظري والمفاهيمي للحرب السيبرانية، واستعرض خصائصها، وأنماطها، والجهات الفاعلة فيها، وحدودها القانونية

المبحث الثاني تناول العلاقة بين الفضاء السيبراني والتحولات في مفاهيم القوة والردع العسكري، ومقارنة استراتيجيات الدول الكبرى في بناء قدراتها الرقمية

المبحث الثالث ركّز على التداخل المتصاعد بين الذكاء الاصطناعي والمجال النووي، ودورهما في تعقيد الصراعات، مع التركيز على الاستخدامات الثنائية من قبل إيران وإسرائيل

المبحث الرابع حلّل تطوّر البنية السيبرانية لكل من إسرائيل وإيران، وبيّن كيف تحوّلت إلى أدوات مركزية في العقيدة الأمنية والسياسات الهجومية والدفاعية

المبحث الخامس قدّم تحليلًا زمنيًا وتطبيقيًا للهجمات السيبرانية المتبادلة بين البلدين، وأثرها على الأمن الإقليمي والدولي

وتوصّلت الدراسة إلى أن الفضاء السيبراني أصبح ميدانًا جديدًا للصراع بين الدول، يعيد تشكيل معادلات الأمن والاستقرار، ويطرح تحديات قانونية وأخلاقية غير مسبوقة. كما أكدت على ضرورة صياغة أطر قانونية دولية ملزمة لحوكمة هذا الفضاء، وتنظيم سلوك الدول فيه، تفاديًا للتصعيد والانفلات

الكلمات المفتاحية: الحروب السبرانية - الذكاء الاصطناعي- الردع العسكري

Summary

This study addresses the topic of cyber warfare and the transformations of power and conflict in the international system, through an analytical approach to the conceptual and theoretical framework of this phenomenon and a review of its contemporary applications—particularly focusing on the Israeli–Iranian case between 2010 and 2025. The study seeks to understand how digital domains have reshaped core concepts such as power, deterrence, and sovereignty, and how they have influenced the structure of geopolitical conflict by employing advanced .technologies including cyberattacks, artificial intelligence, and nuclear systems

The study is based on the fundamental premise that cyber warfare is no longer merely a technical or intelligence activity, but has become a strategic dimension in international deterrence and conflict equations—especially in asymmetric rivalries, as exemplified by the .conflict between Israel and Iran

A multi-level analytical and synthetic methodology was adopted, and the study was struc-:tured into five main chapters

Chapter One: Examined the theoretical and conceptual foundations of cyber warfare, its .characteristics, typologies, active actors, and legal limitations

Chapter Two: Explored the relationship between cyberspace and the evolving notions of power and military deterrence, comparing how major global powers build and employ their .cyber capabilities

Chapter Three: Focused on the growing convergence between artificial intelligence and the nuclear field, highlighting their dual-use roles in intensifying conflicts, especially in the Is-.raeli–Iranian context

Chapter Four: Analyzed the development of cyber infrastructures in both Israel and Iran, and how they became central tools within their respective security doctrines and strategic .policies

Chapter Five: Provided a chronological and applied analysis of the cyberattacks exchanged between the two countries and assessed their implications for regional and international .security

The study concludes that cyberspace has emerged as a new battlefield for inter-state conflict, reshaping the dynamics of security and stability, while raising unprecedented legal and ethical challenges. It underscores the urgent need for binding international legal frameworks .to govern cyberspace and regulate state conduct to prevent escalation and digital disorder

Keywords: Cyber Warfare – Artificial Intelligence – Military Deterrence

- **المقدمة:**

شهدت الفترة من 2010 إلى 2025م، تحولات جذرية في طبيعة الحروب ومجالات الصراع بين الدول، حيث لم تعدّ المعارك تدار فقط في ميادين القتال التقليدية أو عبر الأسلحة المتطورة والبيولوجية، بل برزت ساحة جديدة للصراع تعرف بـ»الفضاء السيبراني». لقد غيّرت التكنولوجيا الرقمية من أدوات قوة الردع العسكري، وأعادت تشكيل مفاهيم الأمن القومي، ليصبح الأمن السيبراني مكوِّنًا استراتيجيًا لا غنى عنه في موازنات الردع والحرب لدى الدول الحديثة

وفي هذا الإطار، تشكل الحرب السيبرانية المتبادلة بين إسرائيل وإيران نموذجًا مركزيًا في فهم طبيعة التهديدات الرقمية العابرة للحدود، والتي لا تخضع بالضرورة لمفاهيم الحرب التقليدية. فمنذ هجوم فيروس Stux-net عام 2010، الذي أصاب منشآت إيران النووية في نطنز، بدأت مرحلة جديدة من التوتر تتسم بالتصعيد غير المعلن، والضربات الخفية، والهجمات المعقدة التي تستهدف بنى تحتية حيوية كشبكات الكهرباء والمياه والمواصلات، فضلًا عن المؤسسات الحكومية والأمنية

وقد سعت كل من إيران وإسرائيل إلى تطوير قدراتها السيبرانية كمكمل بل بديل في بعض الأحيان للعمليات العسكرية التقليدية، حيث أنشأت إسرائيل وحدات متخصصة ضمن جيشها أبرزها «وحدة 8200»، في حين أنشأت إيران وحدات هجومية سيبرانية ضمن «الحرس الثوري» وأذرعه الإلكترونية، مثل مجموعة "APT33" و"APT34". ومع تصاعد حدة المواجهات في ساحات إقليمية كاليمن وسوريا ولبنان والعراق وفلسطين، وزادت أهمية أدوات الحرب السيبرانية، وأصبحت إحدى وسائل إدارة الصراع وتكتيكات الردع غير المباشر

إن هذا النوع من الحروب لا يقتصر على إحداث أضرار تقنية فقط، بل يمتد تأثيره ليشمل الاقتصاد، والمجتمع، والثقة في مؤسسات الدولة، بل ويُعدُّ أحد أخطر التهديدات للأمن الإقليمي والدولي في ظل غياب أطر قانونية دولية واضحة تنظم الفضاء الرقمي أو تحد من استخدامه في الأعمال العدائية

وعليه، تسعى هذه الدراسة إلى تحليل الحروب السيبرانية المتبادلة بين إسرائيل وإيران خلال الفترة من 2010 إلى 2025، من خلال تتبع أهم الهجمات، وفهم أدوات وأساليب التنفيذ، وتحليل أهداف ودوافع الطرفين، فضلًا عن مناقشة تداعيات هذه الحرب على الأمن الإقليمي في الشرق الأوسط وعلى توازنات القوى الدولية. كما تهدف الدراسة إلى بناء تصور نظري ومعرفي يمكن من خلاله فهم هذا النمط المتجدد من الصراع في ضوء متغيرات السياسة الدولية والثورة الرقمية المتسارعة

- **<u>إشكالية الدراسة:</u>**

في ظلّ التحول الاستراتيجي للصراعات الدولية من الحروب التقليدية إلى الحروب السيبرانية، تبرز العلاقة العدائية بين إسرائيل وإيران كنموذج شديد التوتر في هذا السياق، حيث باتت الهجمات الإلكترونية

المتبادلة بين الطرفين تمثل أحد أبرز مظاهر النزاع

وتتمثل الإشكالية في:

ما طبيعة الحروب السيبرانية المتبادلة بين إسرائيل وإيران خلال الفترة (2010–2025)، وما أبرز أدواتها وأبعادها وتأثيراتها على الأمن الإقليمي والدولي؟

- **تساؤلات الدراسة**

1. ما الإطار النظري لمفهوم الحرب السيبرانية؟
2. كيف تطورت القدرات السيبرانية لكل من إيران وإسرائيل؟
3. ما أبرز الهجمات السيبرانية المتبادلة بين الطرفين خلال الفترة (2010–2025)؟
4. ما أهداف ومجالات هذه الهجمات (عسكرية، اقتصادية، مدنية)؟
5. كيف تُوظّف الحرب السيبرانية كأداة ردع في العلاقة بين الطرفين؟
6. ما السيناريوهات المستقبلية المتوقعة لهذه الحرب الرقمية بين الطرفين؟

- **أهداف الدراسة**

- تحليل مفهوم وأدوات الحرب السيبرانية.
- توثيق وتحليل أبرز الهجمات السيبرانية المتبادلة بين إسرائيل وإيران.
- دراسة التطورات المؤسسية والتقنية في القدرات السيبرانية للطرفين.
- الكشف عن تأثير هذه الحرب على موازين الردع الإقليمي.
- استشراف مستقبل الحرب السيبرانية في الشرق الأوسط.

- **أهمية الدراسة**

- علميًا: تسد فجوة في الأدبيات المتعلقة بالحروب السيبرانية في الشرق الأوسط.
- عمليًا: توفر مادة تحليلية تفيد صانعي القرار والباحثين في الأمن السيبراني والدراسات الاستراتيجية.
- زمنيًا: تغطي مرحلة تمتد 15 عامًا، شهدت تطورات نوعية في الفضاء السيبراني.

- **المنهجية وأدوات البحث**

اعتمد هذا البحث على المنهج الوصفي التحليلي، لما له من قدرة على وصف وتحديد طبيعة الهجمات والحروب السيبرانية، وتحليل أبرز التهديدات والفرص المرتبطة بها، بما يسهم في توضيح الظاهرة وتفسير أبعادها. كما يُتيح هذا المنهج تقديم قراءة موضوعية للعوامل المؤثرة في تطور الحروب السيبرانية، ويساعد في رسم صورة شاملة للبيئة الرقمية كأحد ميادين الصراع الدولي في العصر الحديث

وإلى جانب ذلك، تم توظيف المنهج التحليلي في تتبّع مسار الهجمات وأهدافها، والمنهج المقارن لإبراز أوجه التشابه والاختلاف بين القدرات السيبرانية لكل من إسرائيل وإيران. كما تم الاعتماد على تحليل المحتوى في دراسة وثائق وتقارير أمنية وتغطيات صحفية متخصصة، لفهم السياق السيبراني الإقليمي بشكل معمّق

- **مجتمع الدراسة ومصادرها**

استند البحث في جمع معلوماته وتحليل

بياناتـه إلى مجموعـة مـن المصـادر المتنوعـة والموثوقـة، شـملت الوثائـق والتقاريـر الأمنيـة الدوليـة الصـادرة عـن مؤسسـات متخصصـة في الأمـن السـيبراني مثـل *Kaspersky*، و*FireEye*، ومراكـز الأمـن السـيبراني العالميـة، بالإضافـة إلى التقاريـر الصحفيـة المعتمـدة مـن وسـائل إعلام موثوقـة مثـل *BBC*، و*The Times of Israel*، و*Al-Monitor*، و*Iran International*. كما تـم الرجـوع إلى الدراسـات الأكاديميـة والمقـالات العلميـة المحكمـة ذات الصلـة بموضـوع الصراع السـيبراني، إلى جانـب الاسـتفادة مـن قواعـد البيانـات العسـكرية والأمنيـة مثـل *Global Conflict Tracker* و*CyberPeace Institute*، وذلـك لتـأمين تغطيـة شـاملة ومتوازنـة لمختلـف أبعـاد الظاهـرة قيـد الدراسـة

- **هيكل الدراسة:**

اشـتملت هـذه الدراسـة على الإطـار الإجـرائي للدراسـة، وخمسـة محـاور رئيسـة عالجـت مختلـف أبعـاد الحـرب السـيبرانية في سـياق الصراع الإيراني–الإسرائـيلي، وذلـك على النحـو الآتي

- المحـور الأول: الإطـار النظـري والمفاهيمـي للحـرب السـيبرانية، ويتنـاول تعريـف الحـرب السـيبرانية، وخصائـص وأشـكال الحـرب الإلكترونيـة، بالإضافـة إلى عـرض لأبـرز الدراسـات السـابقة ذات الصلـة وتحليلهـا النقـدي.
- المحـور الثـاني: الفضـاء السـيبراني والتحـول في مفاهيـم القـوة والردع، ويسـتعرض الاسـتراتيجيات السـيبرانية للـدول الكـبرى، بمـا في ذلـك الاتحـاد الأوروبي، والصـين، والولايـات المتحـدة، وروسـيا، وتحليـل كيفيـة توظيـف الفضـاء السـيبراني كأداة جديـدة في إعـادة تشـكيل موازيـن القـوة العالميـة.
- المحـور الثالـث: البنيـة السـيبرانية الإسرائيليـة والإيرانيـة، ويحلـل تطـور القـدرات السـيبرانية لـدى كل مـن إسرائيـل (مـع التركيـز عـلى وحـدة 8200 وغيرهـا مـن الأجهـزة)، وإيـران، مثـل (مجموعـة APT33 والحـرس الثـوري)، مـع عـرض للعقيـدة السـيبرانية العسـكرية لـدى الطرفـين.
- المحـور الرابـع: أبـرز الهجـمات السـيبرانية المتبادلـة خـلال الفـترة (2010–2025)، ويتنـاول تحليـلًا تفصيليًـا لأهـم الهجـمات السـيبرانية بـين الطرفـين، مثـل هجـوم Stuxnet عـلى منشـآت نطنـز النوويـة، والهجـمات الإيرانيـة عـلى البنيـة التحتيـة الإسرائيليـة (مثـل الميـاه والنقـل)، وكذلـك الهجـمات الإسرائيليـة عـلى منشـآت الاتصـالات والمطـارات الإيرانيـة، مـع تقديـم تحليـل فنـي للهجـمات مـن حيـث الأدوات المسـتخدمة، والأهـداف، والنتائـج العمليـة.
- المحـور الخامـس: الاسـتنتاجات والتوصيـات، ويتضمـن عرضًـا لأهـم النتائـج التـي توصلـت إليهـا الدراسـة، وتقديـم توصيـات متعلقـة بتعزيـز الأمـن السـيبراني في المنطقـة، إضافـة إلى اسـتشراف عـدد مـن السـيناريوهات المسـتقبلية المحتملـة في ظـل تصاعـد الحـرب السـيبرانية، وتُختتـم الدراسـة بقائمـة موثقـة للمصـادر والمراجـع المعتمـدة.

المبحث الأوّل:
الإطار النظري والمفاهيمي للحرب السيبرانية

شـهدت الـفترة مـن 2010 إلى 2025

تحـوّلًا نوعيًـا في طبيعـة الصراعـات الدوليـة، حيـث بـرزت الحـروب السـيبرانية كواحـدة مـن أخطـر التهديـدات التـي تواجـه الأمـن القومـي للـدول. فقـد أصبحـت الفضـاءات الرقميـة ميدانًـا فعّـالًا للمواجهـة والتجسـس والتخريـب، مـن خلال أدوات غير تقليديـة. وتطـرح هـذه التحـولات إشـكاليات متعـددة، سـواء على مسـتوى القانـون الـدولي، أو مـن حيـث تحديـد هويـة الفاعـلين وطـرق الـردع، مما يفـرض ضرورة دراسـة هـذه الظاهـرة مـن منظـور شـمولي يجمـع بين البعـد التقنـي، والسـياسي، والقانـوني

أولاً: مفاهيم الحرب السيبرانية

الحـرب هـي ظاهـرة إنسـانية موغلـة في القـدم ارتبطـت بالوجـود الإنسـاني على الأرض، وهـي ظاهـرة متـغيرة ومتطـورة مـن ناحيـة الميـدان الخطـط والأدوات والآثـار بفعـل التطـور الإنسـاني فالحـرب، عمليـة صـدام وحشي يقاتـل فيهـا البـشر أمـا للبقـاء أو الحفـاظ على مصالحهـم، أو يمكـن أن توصـف بأنهـا عمليـة قتـل جماعـي؛ لتحقيـق أهـداف مشتركـة

- **السبرانية لغة:**

وتعـد لفظـة السـيبرانية في اللغـة كلمـة (Cy-ber) يونانيـة الأصـل، وترجـع إلى مصطلـح " kybernetes" ويعنـي القيـادة أو التحكـم عـن بعـد[1] وورد اللفـظ في قامـوس المـورد حيـث عرفهـا بأنّها(عـلم الضَبـط- cyberrnetics) أيّ ضبـط الأشـياء عـن بعـد والسـيطرة عليهـا[2]، والسـيبرانية في القامـوس تعنـي علـم الضبـط، ومصدرهـا "Cybernetics "، أيّ ضبـط الأشـياء عـن بعـد والسـيطرة عليهـا، وأوّل مـن اسـتخدم مصطلـح السـيبرانية هـو عـالم الرياضيـات " نوربـرت وينر " وذلـك في عـام 1948، أثنـاء دراسـته موضـوع القيـادة والسـيطرة في عـالم الحيـوان، فـضلاً عـن حقـل الهندسـة الميكانيكيـة، وعـرف قامـوس مصطلحـات الأمـن المعلومـاتي مفهـوم السـيبرانية بأنّهـا" هجـوم عبر الفضـاء الإلـكتروني يهـدف إلى السـيطرة على مواقـع إلكترونيـة، لتعطيلهـا أو تدميرهـا أو الإضرار بهـا"

ولتعريـف المفهـوم اصطلاحيـاً نجـد أن هنـاك عـدّة مصطلحـات حولـه، مثـل تبنـي البعـض مصطلـح الفضـاء السـيبراني، الهـجمات السـيبرانية، الحـرب السـيبرانية، ولكننـا سـوف نتبنـى مصطلـح الحـرب السـيبرانية:

فقـد انـتشر مصطلـح الحرب السـيبرانية بسـبب الجرائـم السـيبرانية والهـجمات والخـطيرة التـي اعتمـدت على تقنيـات متقدمـة كالـذكاء الاصطناعي وأجهـزة مراقبـة على الشـبكات السـلكية واللاسـلكية وبرمجيـات لفـك واختراق أنظمـة الشـبكات والحاسـبات وتسـتخدمها الـدول؛ لأغـراض استراتيجيـة وحربيـة. ويعرّفهـا مجلـس الأمـن الـدولي، بأنّهـا اسـتعمال الوسـائل الرقميـة أو أجهـزة الحاسـوب مـن قبـل الـحكومة أو بمعرفـة أو موافقـة مـن تلـك الحكومـة ضـد دولـة أخـرى أو ملكيـة خاصـة داخـل الـدول الأخـرى، والوصـول المتعمـد أو اعتراض الأجهـزة التـي يمكـن اسـتخدامها في

(1) - الهجـرات السـيبرانية، مفهومهـا والمسـؤولية الدوليـة الناشـئة عنـهما في ضـوء التنظيـم الـدولي المعـاصر، أحمـد عبيس نعمـه، (بابل، مجلـة المحقـق المـحلي العلـوم القانونيـة والسياسـية، العـدد (4)، 2016)، ص 614

(2) - قاموس المَورد عربي أنكليزي، منُير البَعلبكي، (بيروت، دار الملايين، 2004)، ص 244.

تـخريب النشـاطات المحليـة.[(3)]

وتُعـرّف الحـرب السـيبرانيّة تبعًا لقامـوس أوكسـفورد بأنّها: «اسـتخدام تكنولوجيـا الكمبيوتـر لمهاجمـة أنظمـة المعلومـات التابعـة لدولـة أو منظمـة، ومنعهـا مـن القيـام بأنشـطة هامّـة.» بالإضافـة إلى ذلـك إنّ قاموس كامبردج يُعـرّف كالتـالي: «نشـاط اسـتخدام الإنترنـت للهجـوم على أجهـزة الكمبيوتـر الخاصـة بالدولـة مـن أجـل الإضرار بأشـياء، مثـل أنظمـة الاتصـالات والنقـل أو إمـدادات الميـاه والكهربـاء. وكذلـك يُـشير القامـوس نفسـه إلى أنّ الحـرب السـيبرانيّة غيّرت مفهـوم الأمـن القومـي التقليـدي؛ ليُصبـح أوسـع مـن ذلـك؛ إذ هنـاك إمكانيّـة أن تـأتي هـجمات الشـبكات السـيبرانيّة مـن أي مـكان

كما أنّ يُعرّف قامـوس الأمـن الدولي الحـرب السـيبرانيّة على أنّهـا: «حـرب يتـم شـنّها مـن خلال أجهـزة الحاسـوب وشـبكة الإنترنـت. وهـي تشـمل- على حـد سـواء- إجـراءات هجوميّـة لإلحـاق الضرر بنظـم معلومـات الخصـوم، وأخـرى دفاعيّـة لحمايـة النظـم الخاصـة بالمهاجـمين، حمايـة لنظمهـم مـن أن تُهاجـم.[(4)]»

ويُعـدُّ كل من جـون أركـولا- John Arquilla وديفيـد رونفلـدت- David Ronfeldt مـن أوائـل الباحـثين الذيـن تحدّثـوا عـن الحـرب السـيبرانيّة، وذلـك مـن خلال مقالـهما في العـام 1997 بعنـوان "Cyberwar is Coming"- الحـرب السـيبرانيّة قادمـة، وعمـدوا إلى تعريفها كالتـالي: «تـشير الحـرب السـيبرانية إلى إجـراء عمليـات عسـكرية والاسـتعداد لتنفيذهـا وفقًـا للمبـادئ المعلوماتيّـة. إنّهـا تعنـي تعطيـل، إن لم يكـن تـدمير أنظمـة المعلومـات والاتصـالات، التـي تُعـرّف على نطـاق واسـع لتشـمل حتـى الثقافـة العسـكرية.» أي أنّ هـذا التعريـف يُركّـز على الربـط بين الحـرب والمعلوماتيّـة وذلـك لتحقيـق أهـداف عسـكريّة وذلـك مـن خلال معرفـة معلومـات حـول العـدو والتهديـدات التـي يُـفترض مواجهتهـا تبعًـا لأسـاليب حديثـة عـن بُعـد

كما يُعرّفها جوزيـف نـاي- Joseph Ny، على أنّهـا «الأعمال العدائيّـة في الفضـاء السـيبراني التـي لهـا آثـار تُعـادل أو تفـوق العنـف الحـركي التقليـدي.» بذلـك يكـون قـد حـدّد مـدى قـوّة تـأثير الحـرب السـيبرانيّة وتفوّقهـا على كافـة الحـروب التقليديّـة. وتُشـن الحـروب السـيبرانيّة مـن قبـل دول وجيـوش نظاميـة أو منـظمات دوليـة أو ميليشـيات عسـكرية لمهاجمـة أجهـزة الكمبيوتـر أو شـبكات المعلومـات في دولـة أخـرى ومحاولـة الإضرار بهـا. وبذلـك يكـون قـد حـدّد بتعريفـه أنّهـا تُقـام مـن خلال أطـراف متنوّعـة سـواء رسـميّة أو غير رسـميّة.[(5)]

وعرّفهـا «جوزيـف نـاي» بأنّهـا "مجموعـة المـوارد المتعلقـة بالتحكـم والسـيطرة على أجهـزة الحاسـبات، والمعلومـات، والشـبكات الإلكترونيـة، والبنيـة التحتيـة والمعلوماتيـة، والمهـارات البشريـة المدربـة للتعامـل مـع

(3) السيبرانية وتحولات القوة في النظام الدولي، فراس شاكر، (عمان، دار امجد للـنشر والتـوزيع ، 2022) ، ص250.

(4) الأمن السـيبراني المـفهوم وتحـديدات الـعصر، فارس محمد العمارات، (عمان، دار الخليج للنشر والتوزيع، ط 1، 2024)، ص123

(5) - الحـرب السـيبرانية، مواجهـة العقيـدة العسـكرية اسـتعدادا للمعركـة القادمـة، أيهـاب خليفـة، (القاهـرة، مجلـة السياسـة الدوليـة ، العـدد 11 ، المجلـد 53 ، 2018) ، ص 64

هـذه الوسـائل»[(6)]. ففـي الوقـت الـذي كان فيـه النقـاش يـدور حـول الجريمـة الإلكترونيـة والاحتيـال عبر الإنترنـت، توسـع نطـاق التهديـدات ليشـمل مـا بـات يُعـرف بـ»حـرب المعلومـات» و»الأمـن المعلومـاتي» و»الحـرب السـيبرانية»، وهـي مفاهيـم أصبحـت تشـكل اليـوم ركائـز رئيسـة في السياسـات الأمنيـة الوطنيـة لغالبيـة دول العـالم (الموسـوعة السياسـية، 2019)

ويُـشير مصطلـح الحـرب السـيبرانية إلى اسـتخدام الحواسـيب وشـبكات الإنترنـت كوسـائل هجوميـة في النزاعـات، وتُعـدُّ هـذه الأفعـال – التـي تُنفـذ مـن قبـل جهـات متخصصـة تُعـرف باسـم "الهاكـرز" (Hack-ers) – جـزءًا مـن الاستراتيجيـات الحربيـة الحديثـة، سـواء مـن قبـل الـدول أم الفاعـلين غير الحكوميين. وتُعـدُّ هـذه الحرب أحـد أبـرز مظاهـر التهديـد غير التقليـدي للأمـن القومـي والـدولي، لمّا لهـا مـن قـدرة على تجـاوز الحـدود الجغرافيـة دون اسـتخدام الجيـوش أو الأسـلحة التقليديـة، مما يجعلهـا مـن التحديـات المعقدة في تطبيـق قواعـد القانـون الـدولي الإنسـاني.[(7)]

- **المفاهيـم المُقاربـة للحـرب السـيبرانية**

عـرّف مصطلـح «الفضـاء الإلـكتروني» ظاهـرةً ظهـرت مـع اختراع التلغـراف عـام ١٨٤٤، والتـي تنطـوي على الاسـتفادة مـن المجـال الكهرومغناطـيسي لتلبيـة احتياجـات الإنسـان عبر التكنولوجيـا. وكان اختراع الحاسـوب الرقمـي عـام ١٩٤٩ نقطـة تحـول جوهريـة في تطـور الفضـاء الإلـكتروني. ومـن المعـالم البـارزة الأخـرى: ربـط شـبكات الاتصـالات بالحواسـيب والآلات، والـذي بـدأ في سـبعينيات القـرن الماضي؛ والاسـتخدام الواسـع للإنترنـت والحواسـيب الشـخصية منـذ منتصـف التسـعينيات؛ وفي العقـد الماضي، التكامـل الشـامل بين أنظمـة الحاسـوب ومختلـف أنظمـة الاتصـالات والآلات (كما هـو الحـال في الصناعـة والنقـل...)[(8)].

- **الابتزاز السيبراني:**

هـو كلُ سـلوك غير قانـوني يتـم باسـتعمال التقنيـات والأجهـزة الإلـكترونية، ينتـج عنهـا حصـول المجـرم على فوائـد ماديـة ومعنويـة مـع تحميـل الضحيـة خسـارة مقابلـة وغالبًـا مـا يكـون هدفهـا سرقـة أو اتلاف للمعلومـات غالبًـا مـا تكـون البيانـات شـخصية

- **الجريمة السيبرانية:**

هـي نشـاط إجرامـي يتـم بتوظيـف الشـبكات الإلـكترونية للحصـول على المعلومـات أو تدميرهـا أو إيـذاء الأفـراد أو المؤسسـات أو الإضرار بالنظـام السـيبراني وهـذا يجعلـه مـن الصعـب التحقيـق فيـه ومحاسـبة المسـببين لـه. وهـو كل فعـل أو امتنـاع عـن فعـل باسـتعمال

(7) - الحـرب السـيبرانية مـن منظـور القانـون الـدولي الإنسـاني، نسـيب نجيـب، المجلـة النقديـة للقانـون والعلـوم السياسـية، كليـة الحقـوق والعلـوم السياسـية، جامعـة تيـزي وزو، المجلـد 19، العـدد 4، 2021، ص 22

(8) - الحـرب السـيبرانية: المفاهيـم والاتجاهـات الاستراتيجيـة، شـموئيل إيفـن ديفيـد سـيمان تـوف، تاريـخ حقـوق النـشر: 1 مايـو 2012 نُشر بواسـطة: معهد دراسـات الأمـن القومـي، الصفحـات: 95 https://www.jstor.org/stable/resrep0894

نظام معلوماتي معين للأضرار بمصلحة أو حق يحميه القانون من خلال جزاء.

- **الأمن السيبراني :**

هو وسيلة لحفظ البرامج وأجهزة الكومبيوتر والشبكات، وهو سلسلة الإجراءات المتخذة لمواجهة الهجمات والاختراقات السيبرانية وما ينتج عنها من أخطار. ظهر مع بداية الحرب الباردة وتطور مع ثورة الإنترنت وأنظمة الحاسوب، وصار وسيلة أمنية وحربية دولية أساسية

- **الإرهاب السيبراني:**

هي التهديدات على أنظمة المعلومات بدوافع سياسية أو دينية بعد أن أصبح الانترنيت أكثر الأسلحة تدميرًا وفتكًا؛ نتيجة تدخل وتغلغل الِكتروني الذي يكون جزء من عمل الإرهابين السيبرانيين والاستخبارات الأجنبية[(9)]

- **الحرب الإلكترونية:**

هي استعمال الطيف الكُهرومغناطيسي لتشويش وتعطيل الاتصالات وأنظمة التحكم والتوجيه الخاصة بالعدو، ويعدُّ هذا النوع من الحروب أداة مهمة في العملية العسكرية الحديثة، حيث يستخدم لتعطيل اتصالات العدو، وإرباك أنظمة الرادار، وحتى حماية القوات العسكرية من الهجمات. وتختلف الحرب السيبرانية في جوهرها عن الحرب الإلكترونية. إذ تركز على الهجمات التي تستهدف الشبكات الحاسوبية والأنظمة الرقمية. هذه الهجمات يمكن أن تتراوح بين سرقة البيانات الحساسة وتعطيل البُنية الرقمية مثل محطة الطاقة أو شبكة الاتصال

- **الفضاء السيبراني:**

وهو البيئة التفاعلية الالكترونية يحتوي عناصر مادية وغير مادية مكون من العديد من الأجهزة الرقمية والأنظمة والبرمجيات، الشبكة المتصلة في البنى الأساسية لتقنية المعلومات، والتي تشمل شبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها

- **حروب الجيل الخامس**

طوّر المحللون مفاهيم جديدة للتعبير عن التحوّلات في شكل الحروب، فبرز مفهوم حروب الجيل الخامس للتدليل على الأعمال العسكريّة غير الحركيّة، إذ يُستخدم فيها أساليب جديدة تجعل من الصعوبة التمييز بين السلم والحرب. حيث تتداخل مجالات متنوّعة من الحرب بما فيها العسكريّة والاقتصاديّة والتكنولوجيّة والمعلوماتيّة والإلكترونيّة والسيبرانيّة. فيقول فاليري جيراسيموف- Valery Gerasimov: "لقد شهدنا في القرن الحادي والعشرين ميلاً نحو طمس الخطوط الفاصلة بين حالتي الحرب والسلام.. لم تعد الحروب معلنة وفي حالة اندلاعها، فإنها تتطور وفقًا لنمط غير مألوف». وذلك في ظل القدرة على توظيف أدوات الحرب حتّى في وقت السلم من خلال التركيز على أنواع جديدة من الحروب كالحرب المعلوماتيّة والحرب

(9) - الاستراتيجية والتكتيك في فن علم الحرب، منير شفيق، (بيروت، الدار العربية للعلوم ناشرون، ط 1، 2008).

السـيبرانيّة وغيرهـا... فقـد تميّـزت حـروب الجيـل الخامـس بتعـدّد الفواعـل القـادرة على القيـام بهـا فلـم تعـد مقـتصرة على الـدول. فـإنّ الحـرب السـيبرانيّة هـي واحـدة مـن حـروب الجيـل الخامـس، «ولعـل أخطـر مـا يميـز هـذه الحـرب هـو صعوبـة الـردع، ففـي الحـروب التقليديـة، يُعـد الهجـوم المضـاد هـو الـرادع الحقيقـي أمـام التفـكير في شـن الحـرب، وهـو الأمـر الـذي يصعـب القيـام بـه في حالـة الحـروب السـيبرانية. ويرجـع ذلـك إلى عـدّة عوامـل منهـا صعوبـة اكتشـاف الهجـوم السـيبراني في وقتـه الحقيقـي، فـضلا عـن صعوبـة تقييـم الأضرار الناتجـة عـن شـن هـذه النوعيـة مـن الحـروب، وصعوبـة التحكـم في مـدى الهجـوم السـيبراني المضاد، وأخيرًا صعوبـة تحديـد هويـة الطـرف القائـم بالهـجمات السـيبرانية على وجـه اليـقين.»[10]

هنـاك تداخـل لعـدة أجيـال واستراتيجيـات في الحـروب الحاليـة سـواء كانـت حـروب معنيـة بأفشـال الدولـة وتـدمير قوتهـا ومؤسسـاتها فحـروب الجيـل الخامـس تعنـى بالتعامـل مـع كيانـات صـغيرة متعـددة وتشـكيلات (عصابـات وتنظـيمات) إرهابيـة اذ تسـتخدم الشـعوب كلاعـب أسـاسي وليـس عـن طريـق الجيـوش مـع تفعيـل المجـال السـايبري في كلاهما وحتـى في حـروب الـجيل السـادس التـي تعنـى بـكل مـا يتـم التحكـم والسـيطرة عليه، أي إدارة الحرب عـن بعـد إلا إن حروب الجيـل السـادس لا تسـتخدم الأسـلحة والجنـود وإنمـا تهـدف إلى خلـق تناقضـات بين الدولـة والمجتمـع باسـتغلال وسـائل نشر المعلومـات الزائفـة التـي تقـوم على استراتيجيـة احـتلال العقـول أولاً ثـم الأرض.»[11]

ثانيا: خصائص الحرب السيبرانية.

تتسـم الحـرب السـيبرانية بخصائـص فريـدة، أبرزهـا أنهـا غير مرتبطـة بميـدان جغـرافي محـدد، كما أن أهدافها قـد تكـون غير واضحـة أو متـغيرة باسـتمرار. إضافـة إلى ذلـك، فهـي تتحـرك بسرعـة فائقـة عبر شـبكات عابـرة للحـدود، مما يجعلهـا تتطلـب منظومـات دفاعيـة متقدمـة واستراتيجيـات مرنـة ومسـتمرة للتأقلـم مـع التهديـدات[12] للحـرب السـيبرانيّة مجموعـة مـن السـمات التـي تميّزها عـن غيرهـا. فإنّها بحاجـة إلى أجهـزة كمبيوتـر لشـن هجماتهـا إلى جانـب مبرمـجين قادريـن مهاجمـة الأنظمـة التـي يريـدون إلحـاق الضرر بهـا. كما أنّهـا تتسـم بأفضليّـة الهجـوم أي أنّ التفـوّق فيهـا يكـون للـذي يمتلـك القـدرة على الهجـوم بسرعـة ومرونـة لاسـتغلال الثغـرات. بالإضافـة إلى ذلـك إنّهـا تتميّـز بالتداخـل بين الجوانـب العسـكريّة والمدنيّـة وتراجـع الفصـل فـيما بينـهما. وذلـك لأن حمايـة المؤسّسـات المدنيّـة مـن الهـجمات السـيبرانيّة يُصبـح مـن مسـؤوليّة المؤسّسـات العسـكريّة لما تشـكّله مـن خطـر وتهديـد على الأمـن القومـي. كما أنّ الأمـر نفسـه بالنسـبة إلى التداخـل بين الحـرب

(10) حـروب الجيـل الخامـس- أسـاليب «التفـجير مـن الداخـل» على السـاحة الدوليّـة، شـادي عبدالوهـاب منصـور، العـربي للـنشر والتوزيـع، مصر، 2019.

(11) الحـروب المتقدمـة، الحـروب التكنلوجيـة البـاردة بين الـدول العظمـى نموذجـاً عمـرو حسـن فتـوح، (القاهـرة ، مجلـة السياسـة الدوليـة، 2022) ، www.siyassa.org.eg

(12) - الموسوعة السياسية، 2019/08/28؛ رابط المرجع: http://political-encyclopedia.org/dectionary

السيبرانيّة والجوانب السياسيّة والاقتصاديّة، إذ تستطيع الدولة استخدام السيبرانيّة في خلافاتها وصراعاتها السياسيّة والاقتصاديّة. علاوةً على ذلك إنّها تتسم أيضًا بتهديداتها للبنى التحتيّة للخصم. إلى جانب ذلك إنّها تتميّز بصعوبة تحديد هويّة الطرف المهاجم. إذ «يعود ذلك إلى ما يطلق عليه ‹مشكلة الإسناد› (Problem of Retribution)، أي صعوبة ربط العمل العدائي في الفضاء السيبراني بدولة معينة. فكما أشار نائب وزير الدفاع الأمريكي السابق، ‹ويليام لين› في عام 2010، ‹في حين أن الصاروخ يتم إرساله مع ‹عنوان المرسل›، فإن فيروس الكمبيوتر من الصعب ربطه بدولة محددة، إذ إن العمليات اللازمة لتحليل هوية المهاجم قد تأخذ أشهراً، وربما تفشل في النهاية في التوصل إلى هويته.» فضلاً على ذلك، إنّ الحرب السيبرانيّة تتسم بأنّه من الاستحالة أن تنأى أي دولة بنفسها عن هذه الحروب، فهي عرضة دائمًا لهذه الهجمات ولا يُمكن لها تحقيق الأمن الكامل

هي حروب اللاتناظرية : أي لا تحتاج الدولة قدرات ضخمة لتشكيل تهديد خطير، فالتكاليف قليلة نسبيا، إذ أن نشوئها في الفضاء يرتبط بالحاسبات وشيكات الاتصال وأن هذا الهجوم يخلق الاضطراب ويعطل الأنظمة والأجهزة أي لا يتطلب شراء الأسلحة والمعدات، إذ يقتصر على أجهزة الكومبيوتر والمهارات الفنية ولا يحتاج إلى عناصر بشرية[13] عدم التواجد بالمكان لا يحتاج المهاجمون التواجد في المكان الذي يحدث فيه الهجوم أو حتى في المكان الذي يظهر فيه ويستطيع المهاجمون أثناء القيام بالهجوم استخدام تكنلوجيا الاتصال مجهول الهوية وتشفير وإخفاء الهوية مثل الضرر بنظم المعلومات والمواد الحيوية للأجهزة الهامة مثل تعطيل الأنظمة (السياسية والاقتصادية والاجتماعية).[14]

سرعة وسهولة الاتصال يمكنها أن تصل إلى أي مكان في العالم بسرعة خيالية عن طريق سرعة تبادل المعلومة وسرعة تنفيذ الهجمات التي قد لا تتجاوز الدقائق فمن الممكن إطلاق برامج ضارة (فيروسات للكومبيوتر)، فضلًا عن سهولة شن الهجرات السيبرانية لاعتمادها على الحواسيب وتدريب المحترفين التي تكون أثارها سريعة[15].

تجاوز الحدود الوطنية (انعدام السيادة) إذ تؤثر هذه الحروب على عمليات نقل البيانات على أكثر من بلد في نفس الوقت وقد تسبب للجهات المعرضة للهجوم أضرارًا مالية ضخمة ولا يوجد حدود واضحة للدول حيث تتداخل الدول في نفس الشبكات سواء كانت دولة صغيرة أم كبيرة

إخلاء المسؤولية تستخدم الأسلحة السيبرانية للهجوم على عكس الاسلحة التقليدية تستخدم للهجوم والدفاع فالأسلحة

(13) الصراع والأمن الجيوسيبراني في السياسة الدولية دراسة في استراتيجية الاشتباك الرقمي، علي زياد العلي، (عمان، دار امجد للنشر والتوزيع، ط1 ، 2019)

(14) الخصخصة الأمريكية للحروب الجيل الخامس من وسائل التدخل والاستخبارات، علي زياد العلي، (مركز دراسات كاتبغون، http://katehon.com (27/7/2017

(15) الحروب المتقدمة، الحروب التكنلوجية الباردة بين الدول العظمى نموذجاً عمرو حسن فتوح، (القاهرة ، مجلة السياسة الدولية،2022) www.siyassa.org.eg

السيبرانية هي غير مرئية وغير ملموسة[(16)] . إذ تتميز يفعل الردع كونها لا تترك أثر أو دليل على حصولها، وإمكانية التلاعب والتمويه العالية فيما يتعلق بمصدر ومكان توجيه وشن الهجوم الالكتروني[(17)].

ويكمن تلخيص أبرزها بالآتي[(18)]:

1- الافتراضية: (Virtuality) ففي الفضاء السيبراني، الأنشطة والمكونات لا تتطلب وجوداً مادياً. البيانات تنتقل عبر الشبكات الرقمية ويمكن تخزينها في سحابات إلكترونية. **مثل** الاجتماعات عبر الإنترنت، البريد الإلكتروني، والتطبيقات السحابية مثل Google Drive وDropbox.

2- العالمية:(Globality) لا توجد قيود جغرافية على الفضاء السيبراني. يمكن للمستخدمين في أي جزء من العالم الوصول إلى نفس المعلومات والتفاعل مع نفس الأنظمة. **مثل** شبكات التواصل الاجتماعي مثل Facebook وTwitter، والتجارة الإلكترونية التي تتيح البيع والشراء عبر الحدود.

3- الاتصال الفوري: (Instantaneous Connectivity) يتم تبادل المعلومات في الوقت الحقيقي، مما يتيح الاتصالات والتفاعلات الفورية. **مثل** الدردشة الفورية عبر التطبيقات مثل WhatsApp وMessenger، والبث المباشر عبر منصات مثل YouTube وTwitch.

4- اللامركزية (Decentralization): لا يوجد مركز تحكم واحد في الفضاء السيبراني، مما يزيد من مرونة الأنظمة وصعوبة السيطرة الكاملة عليها. **مثل** تقنيات البلوك شين والعملات الرقمية مثل Bitcoin، والتي تعتمد على شبكة موزعة بدون نقطة مركزية.

5- قابلية التوسع (Scalability) يمكن للفضاء السيبراني التوسع بسهولة ليتناسب مع نمو البيانات وعدد المستخدمين. **مثل** خدمات الاستضافة السحابية التي يمكنها التكيف مع زيادة حجم البيانات وحركة المرور مثل AWS و Azure.

6- التفاعلية (Interactivity):حيث يسمح الفضاء السيبراني بتفاعلات مباشرة بين المستخدمين والأنظمة. **مثل** ألعاب الفيديو عبر الإنترنت مثل Fortnite وWorld of Warcraft، ومنصات التعليم الإلكتروني التي تتيح التفاعل بين الطلاب والمعلمين.

7- التشابك والتداخل (Interconnectivity and Interdependency):الأنظمة والشبكات مترابطة بشكل كبير، مما يعني أن خللاً في جزء يمكن أن يؤثر على أجزاء أخرى. **مثل** انقطاع خدمات الإنترنت أو الخدمات السحابية التي تؤدي إلى تعطيل العديد من التطبيقات والخدمات الأخرى.

الديناميكية (Dynamism):الفضاء

(16) أيكلوجيا الارتقاء الصين وتجليات المستقبل دراسة في الامكانيات والتحديات محمد كاظم المعيني، (بيروت، دار السنهوري، 2018) ، ص 312.

(17) الحروب السيبرانيه وتداعياتها على الامن والسلم الدوليين، علي عبد الرحيم العبودي (بغداد، المجلة الأكاديمية العلمية ، المجلد 57 ، 2019) ، ص96

(18) - التهديدات السيبرانية والعلاقات الامريكية الروسية- #https://democraticac.de/?p=99583

السـيبراني يتطـور ويتـغير باسـتمرار مـع التقـدم التكنولوجـي وتـغير احتياجـات المسـتخدمين. مثل الابتكارات التكنولوجيـة مثـل إنترنـت الأشـياء (IoT)، والـذكاء الاصطناعـي (AI) التـي تـغير كيفيـة تفاعلنـا مـع الفضـاء السـيبراني

9 - عـدم التحقـق مـن الهويـة بشـكل مبـاشر (Anonymity and Pseudonymity) يمكـن للمسـتخدمين التفاعـل بـدون الكشـف عـن هويتهـم الحقيقيـة، مما يوفـر بعـض الخصوصيـة ولكنـه يفتـح البـاب أيضـاً لسـوء الاسـتخدام. مثـل المنتديـات والمواقـع التـي تسـمح باسـتخدام أسماء مسـتعارة مثـل Red-dit، والشـبكات المظلمـة (Dark Web) التـي تسـهل الأنشـطة غير القانونيـة

10 - التنـوع الكـبير (Diversity): يشـمل الفضـاء السـيبراني مجموعـة واسـعة مـن الأجهـزة والأنظمـة والتطبيقـات والخدمـات، مما يوفـر فرصـاً متعـددة للأعمال والترفيـه والتعليم. مثل الأجهـزة المتنوعـة مثـل الهواتـف الذكيـة، الحواسـيب اللوحيـة، وأجهزة الكمبيوتـر المكتبيـة، والتطبيقـات التـي تتراوح مـن التطبيقـات الاجتماعيـة إلى تطبيقـات الأعمال والتعليـم.

هـذه الخصائـص تجعـل الفضـاء السـيبراني بيئة غنيـة بالإمكانيـات، لكنهـا تتطلـب أيضـاً وعيـاً وتخطيطـاً دقيقـاً لإدارة المخاطـر والتحديـات المرتبطـة بـه

ثالثـا: الحـرب السبرانية،العمليـات والأنمـاط والجهـات الفاعلـة والوسـائل

يقول أنـدرو كريبينفيتـش- Andrew F. Krepinevich: "يمكـن أن تتضمـن الحـرب السـيبرانيّة الانخـراط في أعمال التجسـس والأنشـطة الإجراميّـة والحـرب الاقتصاديّـة. ويمكـن أن تشـمل أيضًـا إجـراءات مصمّمـة لدعـم العمليـات العسـكريّة على المسـتويين التكتـيكي والتشـغيلي للحـرب. فـضلاً عـن العمليـات المسـتقلة المصمّمـة لتحقيـق تـأثيرات استراتيجيّـة." لـذا إنّهـا تعمـل على القيـام بمجموعـة مـن الأعمال التـي تـؤدّي إلى إلحـاق الضرر بأجهـزة العـدو ويكـون ذلـك عبر مـا يلي

- مهاجمة الشبكات:

تُقـام الهـجمات هـذه عبر الشـبكات الالكترونيّـة والأجهـزة الرقميّـة، ويكـون ذلك من خلال محاول الوصول إلى الأنظمة التـي تحتـوي على بيانـات خاصّـة دون إذن. وكذلـك قـد تُقـام المهاجمـة عبر اختراق مواقـع الخصـم ونشر معلومـات مضلّلة وفيروسـات لتعطيل أنظمته وذلك بغية إتلاف كل م تحتويـه مـن بيانات هامّة. فلهذه الهجمات أنـواع عدّة تبعً لما يختـاره مُعـد الهجمات فقد تكون إمّا عن طريق الاختراق كما ذُكِـر آنفًا أو التجسّـس للحصـول على معلومـات سريّـة والقرصنـة أو وقف المعدّات وتخريبها لتعطيل البنى التحتيّة الأساسيّة. فتعطي دليلـة العوفي نمـاذج عمّا يُسـتخدم ضمن هـذه الحـرب فتقول: "تتميز الحرب السـيبرانية عن الحرب التقليديـة في اعتمادهـا على أسـلحة إلكترونيـة تلائـم طبيعة الصراع القائم بين مختلف الأطراف في الفضاء الرقمي، حيث تسـتخدم عـدة أسـلحة تتمثـل أساسًـا في مختلـف البرامـج الضـارة التـي تحملهـا الحواسـب كالفيروسـات (Virus-es) والديـدان (Worms) والبرامـج الخبيثـة (Malware) والقنابـل المنطقيـة (Logic Bombs)، وهـي برامـج تسـتهدف أساسـا أنظمـة المعلومـات بهـدف إلحـاق الضرر بهـا وتخريبهـا». فتسـتطيع مـن خلال ذلـك التحكّـم في أنظمـة العـدو والسـيطرة على أقماره الاصطناعيّـة للتمكّـن مـن تشويشـها

- الدفاع عن الشبكات:

وذلـك مـن خلال اتخـاذ التـدابير كافّـة التي

تحمي الشبكات والبيانات والحفاظ على أمنها وحمايتها من التهديدات السيبرانيّة الأخرى التي قد تشنّها الأطراف المقابلة. وهذا ما يتطلّب اتخاذ إجراءات الحماية والكشف السريع عن أي مشكلة بغية القيام برد فعل مناسب لحل أي مشكلة مفاجئة

- استطلاع الشبكات:

وذلك من خلال القيام بشكل مستمر بالتجسّس والاستخبارات، وتُستخدم هذه الطريقة أيضًا من أجل نشر المعلومات التي تُشعر العدو بالخطر وذلك لإضعافه نفسيًّا ضمن سياق الحرب النفسيّة

أنماط الحرب السيبرانيّة من حيث التأثير والشدّة

يمكن تصنيف الحروب السيبرانية إلى ثلاثة أنماط رئيسية، بحسب شدّة تأثيرها وطبيعة ساحات الصراع، وذلك على النحو الآتي

الحرب السيبرانية منخفضة الشدة (الباردة): تتميز هذه الحرب بأنّها تدور بشكل رئيسي في الفضاء الإلكتروني دون اللجوء إلى مواجهات عسكرية تقليدية. وتستمر هذه الحرب لفترات طويلة بين أطراف متنازعة، وتتركز أدواتها في الاختراقات السيبرانية، وسرقة المعلومات، والتجسس الإلكتروني، والتأثير النفسي والفكري عبر وسائل الإعلام الرقمي. وتشمل ساحات التأثير الجوانب الاقتصادية، والثقافية، والاجتماعية. من أبرز الأمثلة على هذا النوع من الحروب الصراع الإلكتروني المستمر بين كوريا الشمالية وكوريا الجنوبية

الحرب السيبرانية متوسطة الشدة: يشهد هذا النمط توازياً بين الفضاء الإلكتروني وأعمال عسكرية تقليدية على الأرض، حيث تُستخدم الهجمات السيبرانية كجزء مكمل للحرب الكلاسيكية أو لتسريع نتائجها. وتُعد الحرب بين روسيا وجورجيا عام 2008 مثالًا بارزًا على هذا النوع، إذ صاحبت الهجمات السيبرانية العمليات العسكرية على الأرض، واستُهدفت خلالها البُنى التحتية الرقمية وشبكات الاتصالات الحكومية

الحرب السيبرانية مرتفعة الشدة (الساخنة): يمثل هذا النمط أعلى درجات الحرب السيبرانية من حيث التأثير والتدمير. وتتمثل بوقوع حرب إلكترونية شاملة غير متزامنة بالضرورة مع عمليات عسكرية تقليدية، وتركّز بشكل كبير على تعطيل وشلّ قدرات العدو الحيوية من خلال استهداف المرافق الاستراتيجية، مثل أنظمة الطاقة، والبنية التحتية الرقمية، والدفاعات الإلكترونية. لم يشهد العالم بعد هذا النوع من الحروب بشكل كامل، إلا أنّه مرجّح الحدوث مستقبلًا مع تزايد اعتماد الدول على التكنولوجيا، وتنامي دور الجهات غير الحكومية في الفضاء السيبراني. وتشمل أدوات هذا النمط استخدام الأسلحة السيبرانية،

والطائـرات المـسيّرة، والروبوتـات القتاليـة، بهـدف فـرض السـيطرة الكاملـة وتحقيـق التفـوق الإلـكتروني السريـع

- **الفاعلون السيبرانيون.**

إنّ الفضـاء السـيبراني تحـوّل إلى ميـدانٍ تـدور فيـه الحـروب الحديثـة، وإنّ أطرافهـا قـد تكـون فواعـل حكوميّـة دوليّـة أو فواعـل مـن غير الـدول. فليسـت الـدول هـي الجهـة الوحيـدة التـي يُمكنهـا القيـام بالهـجمات الإرهابيّـة، وهـي كالتـالي

- **الدول :** "

إذ تُعـد الدولـة فاعـل محـوري في تسـيير الفضـاء السـيبراني انطلاقًـا مـن إمكاناتهـا الماديـة والبنيويـة والبشريـة والقانونيـة». فقـد تسـتخدم الـدول الحـرب السـيبرانيّة كي لا تلجـأ إلى الحـرب العسـكريّة المبـاشرة، وبذلـك تسـتخدمها ضمـن صراعاتهـا وعمليّاتهـا. لـذا إنّهـا تعمـد إلى توظيـف شـبكة الاتصـالات والمعلومـات الحديثـة لتحقيـق مكاسـب وإضعـاف الخصـوم. فـعلى سـبيل المثـال إنّ الدولـة قد تشـن حرب سـيبرانيّة لإلحـاق الضرر بالمصالـح الاقتصاديّـة والأمنيّـة للخصـم أو حتّى التلاعـب بمعطيـات هامّـة كالانتخابـات ونشر معلومـات كاذبـة. فـإنّ السـيبرانيّة تحوّلـت إلى قـوّة غيرّت مفهـوم القـوّة التقليديّـة وأضحـت الـدول تتنافـس في إطارهـا. فـإنّ الـدول الـكبرى التـي تمتلـك بنـى تحتيّـة سـيبرانيّة قويّـة قـادرة أن تشـن هجومـات تُسـبب خسـائر للخصـم

- **المنظمات والشركات :**

وهـي كالشركات المتعـدّدة الجنسـيّات القـادرة أن تـخترق أنظمـة معلومـات أفـراد وجماعـات.

فـعلى سـبيل المثـال إنّ مواقـع التواصـل الاجتماعـي كفيسـبوك وتـويتر في ظـل البيانـات التـي تجمعهـا، إنّهـا قـادرة أن تـخترق العديـد مـن الحسـابات وتسـتخدمها لصالـح أهـداف مرتبطـة بهـا أو بيعهـا لجهـات معيّنـة. وبذلـك تسـتطيع ضرب اقتصاديـات دول معيّنـة وتتلاعـب في بياناتهـا. ومـن الـنماذج على تـأثير هـذه الشركات في العلاقـات الدوليّـة هـو «الصراع بين شركـة جوجـل والحكومـة الصينيـة؛ حيـث قامـت الأخيرة بـاختراق حسـابات البريـد الإلـكتروني Gmail الخاصـة بالناشـطين السياسـيين في الـصين. وهـو مـا دفـع الشركـة إلى التهديـد بالخـروج مـن السـوق الصينيـة إن لم تتوقـف الحكومـة الصينيـة عـن أفعالهـا، وقامـت بتطويـر محـرك بحـث Baidu الصينـي حتـى تسـتطيع الـصين الاسـتغناء عـن جوجـل."

- **الجماعات :**

وهـي كالجماعـات الإرهابيّـة التـي تقـوم بالحـرب السـيبرانيّة مـن أجـل اختراق المواقـع التابعـة للدولـة ونشر مـا يـتلاءم مـع أجندتهـا، وذلـك للترويـج لأفكارهـا وأيديولوجيتهـا ونشر الأخبـار التـي تبـث الخـوف.

- **الأفراد:**

يمتلـك الأفـراد القـدرة على تهديـد أمـن الـدول مـن خلال السـيبرانيّة وذلـك في ظـل الإمكانـات التـي تؤهلهـم للقيـام بذلـك مثـل «المال- الإعلام- الأفـكار- المعلومـات وتوظيفهـا ضمـن أهـداف خاصـة، بهـدف التـأثير في سـلوك الوحـدات الفاعلـة على المسـتوى الـدولي، بمـا يخـدم ويحقـق مصالحـه، فـعلى سـبيل المثـال اسـتطاع ‹روبـرت مـردوخ› Rupert Mur-doch)) تحقيـق نفـوذ وتـأثير في السياسـة

الدوليـة بمـا يمتلكـه مـن مؤسسـات إعلاميـة وإخباريـة فاقـت 800 مؤسسـة في أكثر مـن 55 بلـد((19)).

وسائل القوة السيبرانية :

فـكما ذكرنـا أن الفضـاء السـيبراني مـا يميـزه أنـه صراع مجهـول الأطـراف في كـثير مـن الأحيـان، ويسـعى كل طـرف فيـه لتحقيـق أكبر قـدر من المكاسـب، وإلحـاق أكبر قـدر مـن الخسـائر بالخصـم، فلابـد أن تمتلـك الـدول أدوات القـوة السـيبرانية، وكيفيـة توظيفهـا ضمـن نمطيهـا الصلـب والناعـم، وهـذه التهديـدات يمكـن أن تتنـوع في طبيعتهـا وأهدافهـا ووسـائلها، وتشـمل عـدة أنـواع شـائعة منهـا((20))

- بنيـة تحتيـة تكنولوجيـة : وهـي البنيـة الأساسـية لتكنولوجيـا المعلومـات، وتتضمـن هـذه البنيـة مراكـز البيانـات، وأجهـزة وشـبكات الكمبيوتـر، وأجهـزة إدارة قواعـد البيانـات، وأي نظـام للوائـح التنظيميـة، وتشـمل وسـائل النقـل عـبر الكابـلات، والأقـمار الصناعيـة.
- الفيروسـات : وهـي برامـج تـم تصميمهـا لإلحـاق الـضرر بقواعـد البيانـات، أو سرقتهـا وتخريبهـا أو قطـع الاتصـال بالشـبكة، وهـي برامـج صُنعـت عمـداً لتغيـير خصائـص الملفـات، والغـرض منهـا هـو إلحـاق الـضرر بالحاسـوب أو الهاتـف والسـيطرة عليـه، وكتابتها تكـون بطريقـة معينـة، وقد تسـتخدم الفيروسـات لتعطيـل شـبكات الخدمـات والبنيـة التحتيـة للطـرف المسـتهدف، كإحـداث فشـل في شـبكة الاتصـالات لدولـة مـا .
- الديـدان : وهـي برامـج صغـيرة تتكـون مـن الشـبكات، وغايتهـا قطـع الاتصـال عـن الشـبكة أو سرقـة البيانـات، وذلـك أثنـاء تصفـح المسـتخدمين للإنترنـت.
- دودة ميليسـا (Melissa Worm) : أدت إلى خسـائر تُقـدر بالملايـين الـدولارات، ثـم نـشر الفـيروس بواسـطة البريـد الإلكـتروني، وذلـك مـن خـلال رسـالة بريـد إلكـتروني مزيفة تقـوم بإرسـالها نفسـها إلى 50 بريـد إلكـتروني آخـر عنـد فتحهـا ، وانتـشرت عـام1999.
- دودة ستكسـنت (Stuxnet worm): انتـشرت عـام 2010 عبر أجهـزة USB (drivers)، عنـد وصلهـا بجهـاز الحاسـوب، وهـي لا تتطلـب وجـود اتصـال بشـبكة الإنترنـت لـكي تتمكـن مـن الانتشـار، وقـد أصـاب الفـيروس محطـات توليـد الطاقـة النوويـة بالإضافـة لمحطـات تخصيـب اليورانيـوم في إيـران.
- أحصنـة طـراودة (Trojan Horse): هـي شـفرة صغـيرة يتـم تحميلهـا مـع برنامـج رئيسي مـن البرنامـج ذات الشـعبية العاليـة، ويقـوم ببعـض المهـام الخفيـة، ويركـز غالبـاً عـلى إضعـاف قـوى الدفـاع أو اخـتراق الأجهـزة وسرق البيانـات، فهـو نـوع مـن البرميجيـات الخبيثـة، ويعتمـد عـلى الثغـرات الأمنيـة التـي تتيـح الوصـول غـير المـصرح بـه إلى جهـاز المسـتهدف.
- القنابـل المنطقيـة (logic Bombs) هـي أحـد أنـواع أحصنـة طـروادة،

(19) https://political-

(20) Heinl, Caitríona H. "NATIONAL SECURITY IMPLICATIONS OF INCREASINGLY AUTONOMOUS TECHNOLOGIES: DEFINING AUTONOMY, AND MILITARY AND CYBER-RELATED IMPLICATIONS." S. Rajaratnam School of International Studies, 2015. http://www.jstor.org/stable/resrep05847.

وتصمم تحت ظروف معينة أو لتنفيذ أمر معين، وتؤدي إلى تخريب أو مسح البيانات أو تعطيل النظام.

- الماكينات والميكروبات فائقة الصغر : وهي عبارة عن (robots) فائقة الصغر، قد تنتشر في مبني نظام معلوماتي لدولة معادية أو منافسة، حيث تتفشي في المكاتب حتي تجد حاسباً آلياً، وتدخل إليه من خلال الفتحات الموجودة به، لتبدأ بإتلاف الدوائر الإلكترونية، أما الميكروبات فتقوم بتدمير الدوائر الإلكترونية فيأى معمل به حسابات آلية .
- الأبواب الخلفية (backdoors): وهي ثغرة تترك عن عمد، من قبل مصمم النظام لكي يستطيع الدخول إلى النظام عند حاجته إليه، ولذلك كل البرامج والنظم التي تنتجها الدول الكبرى (إسرائيل) تحتوى على أبواب خلفية ، وهو ما يمكن هيئات وأركان حرب المعلومات من التجوال الحر داخل أي نظام لأى دولة أجنبية.
- مدافع (HERF): وهي التي تعمل على إطلاق موجات راديو مركزة وعالية الطاقة والتردد، تستطيع تعطيل وإتلاف أي هدف إلكتروني، أما مستويات الضرر التي قد تحدثها فهي تختلف من ضرر متوسط ، كغلق شبكة حاسب مثلاً أو إعادة تشغيله بشكل دوري فلا يمكن استغلاله، ويمكن أن تؤدى إلى إحداث ضرر بالغ، كإتلاف الشبكة بشكل لا يمكن بعده إصلاح الحاسب أو الشبكة.
- الرقائق (Shippings): من الممكن أن تحتوي بعض الرقائق على وظائف غير متوقعة أو معروفة كما في البرامج والنظم، حيث يمكن للدوائر المجمعة التي تشكل هذه الرقائق أن تحتوي على وظائف إضافية أثناء تصنيعها لا تعمل في الظروف العادية، إلا أنها قد تعلن العصيان في توقيت معين، أو بالاتصال بها عن بعد، حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو فتشل الحياة في دولة ما.
- الفيروسات والبرمجيات الخبيثة (Malware):) هي برمجيات مصممة لإحداث أضرار بالأجهزة أو الشبكات. تشمل الفيروسات، الديدان، وبرامج الفدية (Ran-somware).
- الهجمات من خلال الفدية (Ransomware): هي نوع من البرمجيات الخبيثة التي تقوم بتشفير بيانات الضحية وتطالب بفدية لإعادة الوصول إليها.
- الهجمات الموجهة (Targeted Attacks) تشمل الهجمات التي تستهدف شخصاً أو مؤسسة معينة بغرض السرقة أو التجسس أو إحداث ضرر.
- الهجمات الاحتيالية (Phish-ing) تتضمن خداع الأفراد للكشف عن معلومات حساسة مثل كلمات المرور أو بيانات البطاقة الائتمانية عن طريق رسائل بريد إلكتروني أو مواقع مزيفة.
- الهجمات على الشبكات ((Net-work Attacks: تشمل محاولات اختراق أو تعطيل شبكات الكمبيوتر، مثل الهجمات الحجبية (DDoS).

- القرصنة (Hacking) تتضمن محاولات غير مشروعة للوصول إلى الأنظمة والشبكات من خلال استغلال نقاط الضعف فيها.
- التجسس السيبراني (Cyber Espionage) هي عمليات سرية تستهدف الحصول على معلومات حساسة أو سرية بدون إذن.
- الهجمات الداخلية (Insider Threats) تحدث عندما يقوم شخص داخل المؤسسة بإلحاق ضرر بالمعلومات أو الأنظمة، سواء بقصد أو بدون قصد.

1- مطالبات بتشريعات ضابطة

لقد طُرحت انتقادات حول الحرب السيبرانيّة، فهناك من يعتبر أنّها لم تحدث ولن تحدث؛ وحتّى ضد تسمية الحرب السيبرانيّة. فيرى توماس ريد- Thomas Rid "أنّ الأمر لا يتعدّى كونه ‹هجمات سيبرانية Cyber Attacks' وليس حربًا سيبرانية، وأنّ الهجمة السيبرانية تسعى بالأساس لتحقيق ثلاث وظائف رئيسية أقدم من فكرة الحرب نفسها، وهي «التخريب والتجسس والتدمير.» بالإضافة إلى ذلك، يشير بيتر بي سيل- Peter B. Seel أنّ لا بدَّ من العمل على وضع بروتوكولات لفرض ضوابط على استخدام الأسلحة السيبرانيّة للإنترنت مثل تلك التي فُرضت للحد من انتشار الأسلحة النوويّة.

إذ يقول بيتر: «وسيتحقَّق أفضلُ ما في صالح مواطني الكوكب إنْ تمكَّنَتْ حكوماتهم من الاتفاق على بروتوكولات تمنع استخدام الأسلحة السيبرانية. لقد أصاب أجهزةَ الكمبيوتر والشبكات العالمية في العقدَيْن المنصرِمَيْن ما يكفي من الضرر بسبب الفيروسات والديدان وأحصنة طروادة الرقمية التي صمَّمَها متسلِّلون ومجرمون سيبرانيون، وهذا دون احتساب التهديد الجديد المتمثِّل في الإرهاب السيبراني برعاية الدول.» إلّا أنّ في السياق نفسه، قد اعتبرت جهات أخرى أنّه لا يُمكن وضع حد للحروب السيبرانيّة وإساءة استخدامها كون هناك غياب في معرفة الجهة التي تشنّها وبالتالي لا يمكن تنظيمها وتجنّب تداعياتها. ويرى شيرود دي غريبو- Sherrod DeGrippo: " أنه لا شيء يحفز على التعاون في مجال عدم انتشار الأسلحة دولياً. من الصعب معرفة الجهة المسؤولة عنها، بالتالي قد لا تتمكن حكومات العالم من التعاون في مجال الحروب السيبرانية بالطريقة التي تتعاون فيها على عدم انتشار الأسلحة النووية

رابعا: أدبيات الدراسة

شهدت الدراسات التي تناولت الحرب السيبرانية بين إسرائيل وإيران تطورًا معرفيًا ومنهجيًا ملحوظًا خلال العقد الماضي، عكست تنوعًا في المقاربات التحليلية، واتساعًا في فهم أبعاد الفضاء السيبراني كأداة صراع. وتبرز خمس دراسات أساسية تسير وفق تسلسل زمني يمكن من خلاله تتبع مسار هذا التحول

جاءت أولى هذه الدراسات في عام 2016، وهي دراسة نسرين الشحات الصباحي بعنوان "الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول"، والتي اتخذت من إسرائيل نموذجًا لتوضيح التأثيرات

العسكرية للقدرات السيبرانية. ركزت الدراسة على الهجوم السيبراني المعروف باسم «ستاكسنت»، الذي استُخدم لتعطيل أجهزة الطرد المركزي الإيرانية، مبيّنةً كيف استطاعت إسرائيل، بالتعاون مع الولايات المتحدة، استخدام أدوات سيبرانية هجومية لإبطاء البرنامج النووي الإيراني. كما أشارت إلى تصاعد الهجمات السيبرانية المتبادلة بين إسرائيل وخصومها الإقليميين، مؤكدة أن الردع في الفضاء الرقمي يختلف عن الردع التقليدي نظرًا لغموض الفضاء السيبراني وصعوبة تتبع مصدر الهجوم، مما يعزز من مخاطر ما أسمته بـ«الإرهاب السيبراني» على الأمن القومي الإسرائيلي

أما دراسة جهاد أبو سعدة (2018)، التي حملت عنوان "إسرائيل واستراتيجية مواجهة البرنامج النووي الإيراني"، فقد انتقلت بالتحليل من التركيز على الأبعاد العسكرية إلى الاهتمام بالبُعد الاستراتيجي والإعلامي للصراع السيبراني. اعتمدت الدراسة على المنهج الوصفي لتحليل التحركات الإسرائيلية في الفضاء السيبراني خلال العقد الأخير، مع التركيز على كيفية استثمار إسرائيل لتفوقها الرقمي في إعداد الرأي العام الداخلي والدولي لتقبل فكرة الحرب السيبرانية كخيار مشروع. وأبرزت الدراسة المخاوف الإسرائيلية من تمكن إيران من تطوير قدرات تمكنها من شن هجمات رقمية على أهداف حيوية، أو من خلال حلفائها غير الحكوميين مثل حزب الله، مستشهدة بحادثة عام 2006. وقد خلصت الدراسة إلى أن إسرائيل تسعى لتنفيذ عمليات رقمية يصعب تتبعها، ما يوفر لها ميزة الردع دون تكاليف سياسية

وفي عام 2020، قدّمت مريم محمد سيد حسن دراسة بعنوان "القوة السيبرانية في السياسة الخارجية الإسرائيلية تجاه إيران *(2010-2020)*"، والتي شكلت نقلة نوعية في تحليل الدور المتصاعد للفضاء السيبراني في العلاقات الدولية. أكدت الباحثة أن إسرائيل لم تعد تستخدم الحرب السيبرانية فقط في الأطر الأمنية، بل أصبحت توظفها بفعالية في سياستها الخارجية، خصوصًا تجاه إيران. وبيّنت الدراسة أن الصراع السيبراني يعكس تحولًا استراتيجيًا في أدوات القوة والتأثير، معتبرة أن ساحة المعركة في المستقبل لن تكون مادية بقدر ما ستكون رقمية. وقد أوصت الدراسة بضرورة بناء بنية تقنية عربية مستقلة، وتحديث الإطار التشريعي المرتبط بالأمن السيبراني

ومن منظور غربي، جاءت دراسة ريتشارد هاركنيت المنشورة أيضًا في عام 2020 عبر مركز سكوكروفت بعنوان "رؤية مضطربة: فهم الهجمات السيبرانية المتبادلة بين إسرائيل وإيران". ركزت الدراسة على تحليل طبيعة التصعيد المتبادل في الهجمات السيبرانية بين الطرفين، خاصة تلك التي وقعت عام 2020، مثل استهداف منشآت تصنيع الصواريخ الإيرانية. وخلصت الدراسة إلى أن كلًا من إسرائيل وإيران فشلتا في بناء نموذج ردع فعّال في الفضاء السيبراني، مما أدى إلى استمرار التصعيد وغياب الاستقرار. واعتبرت الدراسة أن السلوك الاستراتيجي للطرفين يعكس سعيًا محمومًا لتحقيق

تفـوق نسـبي في بيئـة رقميـة تتسـم بعـدم الوضـوح والتـوازن

أخيرًا، جـاءت دراسـة د. تقـى إيـاد خليـل القـيسي المنشـورة في عـام 2025 تحـت عنـوان "حـروب الجيـل السـادس واستراتيجية المواجهـة السـيبرانية: إنموذجًـا"، لتقـدّم رؤيـة شـمولية متقدمـة لمفهـوم الحـرب السـيبرانية ضمـن إطـار أوسـع يتصـل بأجيـال الحـروب الحديثـة. تناولـت الدراسـة الحـرب السـيبرانية مـن زاويـة تطورهـا المفاهيمـي، وأكـدت أنهـا لم تعـد تقـتصر على الجوانـب العسـكرية فقط، بـل امتـدت لتشـمل اسـتهداف البنـى التحتيـة الحيويـة مثـل الكهربـاء والميـاه والاتصـالات، بـل وحتـى الجوانـب الاجتماعيـة والسياسـية في محاولـة لزعزعـة الاسـتقرار الـداخلي للـدول. وقـد أبـرزت الدراسـة أهميـة الفضـاء السـيبراني كأحـد أعمـدة الصراع الـدولي في القـرن الحـادي والعشريـن، معـتبرة أن السـيطرة عليـه لا تحقق الـنصر بمفردهـا، ولكـن لا يمكـن الانتصـار مـن دونـه، كما خلصـت إلى ضرورة إعـادة تشـكيل الاستراتيجيـات الدفاعيـة والهجوميـة للـدول بمـا يتوافـق مـع التحـولات الجاريـة في هـذا المجـال

يتضـح مـن خلال هـذا التسلسـل الزمنـي أن الدراسـات تطـورت مـن التركيـز على الـردع السـيبراني بوصفـه أداة عسـكرية (2016)، إلى تحليـل الاستراتيجيـة السياسـية والإعلاميـة (2018)، مـرورًا بتوسـيع الأفـق ليشـمل السياسـة الخارجيـة والدبلوماسـية الرقميـة (2020)، ووصـولًا إلى نقـد فعاليـة الـردع وقـراءة التصعيـد السـيبراني كسـلوك استراتيجـي مسـتمر (2020)، وانتهـاءً بتحليـل شـامل ضمن إطـار نظـري متقـدم لحـروب الجيـل السـادس (2025). هـذا يعكـس نضوجًـا تدريجيًـا في تنـاول موضـوع الحـرب السـيبرانية كمجـال متكامـل تتداخـل فيـه التقنيـة بالسياسـة، والعسـكر بالاقتصـاد، والأمـن بالهويـة.

الفجوة البحثية

رغـم تعـدد الدراسـات السـابقة التـي تناولـت الحـرب السـيبرانية بين إسرائيـل وإيـران مـن زوايـا مختلفـة (عسـكرية، أمنيـة، سياسـية، واستراتيجيـة)، إلا أنهـا لم تقـدم تحليـلًا متـكاملًا ومواكبًـا يغطـي الـفترة الزمنيـة مـن 2010 حتـى 2025، ولم تربـط بين تطـور أدوات الصراع السـيبراني، وتحـولات العلاقـات الجيوسياسـية في الإقليـم، ضمـن رؤيـة تحليليـة تتجـاوز الوصف الجـزئي للهـجمات إلى فهـم شـامل لاستراتيجيـة الصراع المتبـادل في بعديـه الهجومـي والدفاعي يمكـن تلخيـص الفجـوات الرئيسـية في النقـاط التاليـة

1. القصـور الزمنـي والميـداني: معظـم الدراسـات ركـزت عـلى مراحـل زمنيـة محدودة (مثـل 2010–2020)، وأغفلـت تطـورات السـنوات الخمـس الأخـيرة (2021–2025) التـي شـهدت تصعيـدًا ملحوظًـا في الهجـمات السـيبرانية المتبادلـة، واسـتهداف البنيـة التحتيـة الحيويـة بشـكل مبـاشر.
2. غيـاب منظـور التحليـل المتبـادل (Two-Way Dynamics): أغلـب الدراسـات تناولـت إسرائيـل كفاعـل رئيـسي، بينـما أهملـت تحليـل الاسـتراتيجية الإيرانيـة السـيبرانية بشـكل معمّـق، بمـا في ذلـك تطـور وحداتهـا، أدواتهـا، وتحولاتهـا بعـد اغتيـال قاسـم سـليماني وتطـور الحـرب بالوكالـة.

3. الافتقار إلى تحليل استراتيجي مشترك للردع والفشل: لم تُخصص الدراسات السابقة مساحة كافية لمناقشة فشل نماذج الردع السيبراني، واستمرار التصعيد رغم توازن الكفاءة التقنية، وهو ما يفتح بابًا لتحليل جديد حول أزمة الردع في الفضاء السيبراني.

4. ضعف الربط بين الفضاء السيبراني والأمن الإقليمي والدولي: لم توظف معظم الدراسات الحرب السيبرانية كعامل مؤثر في إعادة تشكيل موازين القوى الإقليمية، أو التأثير على المسارات الدبلوماسية، مثل الاتفاق النووي أو التحالفات الإقليمية الجديدة.

5. الافتقار إلى مقاربة متعددة الأبعاد (Multi-dimensional Approach): اقتصرت الدراسات السابقة على بُعد واحد (عسكري/سياسي/نظري)، ولم تقدم قراءة شاملة تدمج بين البعد التكنولوجي، الأمني، السياسي، والمجتمعي، داخل إطار مفاهيمي متكامل لحرب الجيل السادس أو الحروب الهجينة

أهمية دراستنا في سد الفجوة

بناءً على ما سبق، تسعى دراستك إلى سد هذه الفجوة البحثية من خلال

- تقديم رؤية تحليلية شاملة تغطي الفترة الممتدة من 2010 حتى 2025.
- دراسة الهجمات السيبرانية المتبادلة بين إسرائيل وإيران باعتبارها نموذجًا لصراعات الجيل السادس.
- تحليل التحول في أدوات الردع السيبراني، وفهم أسباب فشله أو هشاشته في البيئة الرقمية.
- ربط الحرب السيبرانية بـ الأمن الإقليمي والتحالفات الدولية.

نتائج المبحث

في ضوء ما سبق من عرض وتحليل للإطار النظري والمفاهيمي للحرب السيبرانية، وما تضمّنه من استعراض شامل لتعريفاتها، وخصائصها، وأنماطها، ووسائلها، والجهات الفاعلة فيها، يمكن استخلاص النتائج التالية

1. مثّلت الحرب السيبرانية تحوّلًا نوعيًّا في مفهوم الحروب المعاصرة، حيث انتقلت من حروب مادية تقليدية قائمة على الحدود الجغرافية إلى حروب رقمية غير متماثلة، تدار في الفضاء السيبراني، مما يفرض إعادة صياغة لمفاهيم السيادة، والردع، والتوازن الاستراتيجي.

2. تُعدُّ مشكلة تحديد هوية الجهة المهاجمة (Attribution Problem) إحدى أبرز سمات الحرب السيبرانية، ما يجعل من الصعب تحميل المسؤولية أو اتخاذ ردود فعل قانونية أو عسكرية مضمونة، ويقلّص فعالية مبدأ الردع الكلاسيكي.

3. لم تعد الدول وحدها الطرف المحتكر للعمل العسكري أو الأمني، بل أصبحت الشركات، والجماعات الإرهابية، والمنظمات العابرة للحدود، والأفراد المحترفون (Hackers)، أطرافًا فاعلة قادرة على شنّ هجمات سيبرانية فعالة.

4. لم تعد الحرب السيبرانية تقتصر على المجالات العسكرية، بل امتدت إلى البنى التحتية المدنية، والنظم المالية، والاتصالات، والصحة، والطاقة، والتعليم،

بـل وحتـى العمليـات السياسـية كالتأثـير في الانتخابـات وخلـق حمـلات تضليـل.

5. باتـت الهجـمات السـيبرانية تُسـتخدم كأداة مركزيـة ضمـن اسـتراتيجيات الحـرب الهجينـة، سـواء في تمهيـد العمليـات العسـكرية، أو مرافقتهـا، أو تعزيـز تأثيرهـا عـبر اختراقـات معلوماتيـة، وهجـمات إعلاميـة، وتعطيـل البنـى التحتيـة الرقميـة.

6. لم تواكـب القوانـين الدوليـة تطـورات الحـرب السـيبرانية، فالمواثيـق القائمـة لا توفّـر نصوصًـا صريحـة تنظـم هـذا النـوع مـن النـزاع، ولا تحـدد بوضـوح مسـؤولية الفاعلـين الرقميـين، رغـم بعـض الجهـود التفسـيرية كـ«دليـل تالـين» غـير الملـزم.

7. تحـوّل الأمـن السـيبراني مـن مسـألة فنيـة إلى ركيـزة جوهريـة في مفاهيـم الأمـن القومـي، الأمـر الـذي دفـع الـدول إلى تأسـيس وحـدات رقميـة دفاعيـة وهجوميـة متخصصـة، وتطويـر اسـتراتيجيات وطنيـة للـردع الرقمـي.

8. تكـرّس الحـروب السـيبرانية الفجـوة بـين الـدول الغنيـة بالتكنولوجيـا وتلـك التـي تعـاني مـن ضعـف البنيـة التحتيـة الرقميـة، مـما يجعـل الـدول الأقـل نمـوًا أكـثر عرضـة للاخـتراق، وأقـل قـدرة عـلى الـرد أو الاحتـواء أو حتـى الاكتشـاف.

9. يتيـح الطابـع الافـتراضي واللامركـزي للفضـاء السـيبراني إخفـاء الهويـة والمنـاورة خـارج نطـاق المسـاءلة، مـما يعقّـد التتبـع والـردع، ويُـبرز الطابـع اللاتماثـلي للحـرب السـيبرانية، حيـث يمكـن لجهـات صغـيرة أن تُحـدث تأثـيرات كبـيرة بتكاليـف منخفضـة.

المبحث الثاني:

الفضاء السيبراني والتحول في مفاهيم القوة والردع العسكري

أضحـت القـدرات السـيبرانية العسـكرية التـي تمتلكهـا الجيـوش على مسـتوى العـالم مـؤشرًا هامًـا في تقييـم القـوة الوطنيـة لأي دولـة، وهو مـا ركـز عليـه تقريـر «التـوازن العسـكري لعـام 2020» الـذي يصـدره المعهـد الـدولي للدراسـات الاستراتيجيـة سـنوياً، إذ وجـد أن عـددًا قليـلًا مـن الـدول قـد تحـوّل بشـكل شـامل نحـو دمـج عمليـات الفضـاء الإلـكتروني في هيـاكل القـوة المختلفـة.

- **القـوة السـيبرانية (Cyber Power)**: قدرتهـا عـلى التأثـير أو التدمـير أو الـردع عـبر الفضـاء الرقمـي.
- **الـردع السـيبراني (Cyber Deterrence)**: اسـتخدام التهديـد بالانتقـام أو الإجـراءات الدفاعيـة المتقدمـة لمنـع الهجـمات السـيبرانية.

ونظـرًا لنـدرة البيانـات الأساسـية المتعلقـة بالقـدرات العسـكرية السـيبرانية، قـام المعهـد بجمـع بيانـات استرشـادية في أربعـة مجـالات: مجـال الاستراتيجيـة والعقيـدة، ومجـال الوحـدات الرئيسـية للدفـاع السـيبراني، ومجـال الأقمار الصناعيـة العسـكرية، والمجـال المتعلـق بتدريبـات الدفـاع السـيبراني، لتقديـم أدلـة على نشر المفاهيـم والقـدرات العملياتيـة لعمليـات الفضـاء السـيبراني مـن خلال التدريبـات الإلكترونيـة العسـكرية الوطنيـة، وإبـراز القـدرات السـيبرانية للـدول الـكبرى في النظـام الـدولي، وذلـك على النحـو التـالي

أولا: القـدرات السـيبرانية الأوروبيـة (فرنسـا، بريطانيـا) والـصين

شـهد العـالم خلال العقديـن الأخيريـن تحـوّلًا جذريًـا في طبيعـة التهديـدات الأمنيـة، حيـث لم تعـد الحـروب التقليديـة وحدهـا تشـكّل الخطـر الأكبر على اسـتقرار الـدول، بـل ظهـرت الفضـاءات الرقميـة كسـاحات جديـدة للمواجهـة والصراع. وقـد أصبـح الفضـاء السـيبراني اليـوم ميدانًـا استراتيجيًـا بالـغ الحساسـية، تُوظـف فيـه أدوات الهجـوم والدفـاع والمراقبـة والتجسـس، ضمـن مـا يُعرف بـ»القـوة السـيبرانية». وفي هـذا السـياق، برزت كل مـن الـصين ودول الاتحـاد الأوروبي كفاعـلين رئيسـيين في بنـاء وتعزيـز قدراتهـم السـيبرانية، لكـن مـن منطلقـات وخلفيـات مختلفـة

ففـي حين تعتمـد الـصين مقاربـة مركزيـة هجوميـة تسـتند إلى الدمـج الكامـل بين الدولـة والتكنولوجيـا، مسـتغلة أدوات الرقابـة والتحكـم المعلومـاتي كجـزء مـن أمنهـا القومـي واستراتيجيتهـا الجيوسياسـية، تتجـه دول الاتحـاد الأوروبي إلى تطويـر بنيـة سـيبرانية متعـددة الأطـراف، تـوازن بين احترام الخصوصيـة الفرديـة وتعزيـز الأمـن الرقمـي، مـع تركيـز خـاص على الدفـاع والحمايـة

تسـعى هـذه الورقـة إلى تحليـل طبيعـة ومجـالات القـوة السـيبرانية لـدى الطـرفين، مـن خلال تفكيـك السياسـات، والمؤسسـات، والأدوات المسـتخدمة، واسـتعراض أبـرز التحديـات التـي تواجـه كل طـرف في عـالم يتّسـم بالتداخـل الشـديد بين الأمـن القومـي والسـيادة الرقميـة.

1- القدرات السيبرانية البريطانية

تتركـز القـوة السـيبرانية للمملكـة المتحـدة -بشـكل أسـاسي- في المركـز القومـي للأمـن السـيبراني، إلى جانـب القـدرات التـي يمتلكهـا مكتـب الاتصـالات الحكوميـة (جهـاز المخابـرات البريطـاني) في مجـال الاسـتخبارات السـيبرانية. وتقـود التشـكيلات العسـكرية السـيبرانية في بريطانيـا القيـادة الاستراتيجيـة التـي تأسسـت في عـام 2020، لعـدم وجـود قيـادة عسـكرية سـيبرانية موحـدة. فالقـوات المسـلحة البريطانيـة تمتلـك بعـض التشـكيلات الخاصـة بالفضـاء الإلـكتروني.

كما قامـت الدولـة بتطويـر استراتيجيـة أساسـية في مجـال الأمـن السـيبراني في إطـار الاستراتيجيـة العامـة في كل القطاعـات. فقـد عرضـت الاستراتيجيـة التـي ترتكـز عليهـا العقيـدة العسـكرية البريطانيـة بالتفصيـل للهجـوم السـيبراني، وكيفيـة اسـتخدامه لخلـق حريـة المنـاورة، وزيـادة القـوة وتحقيـق عمليـة الـردع

حرصـت المملكـة المتحـدة على تعزيـز قدراتهـا الهجوميـة في الفضـاء السـيبراني عبر مشروع مـشترك بين مكتـب الاتصـالات الحكوميـة (GCHQ) ووزارة الدفـاع. وفي هـذا السـياق، أطلقـت وزارة الدفـاع عـام 2014 برنامجًـا وطنيًـا لتطويـر القـدرات الهجوميـة السـيبرانية، والـذي جـرى اسـتبداله ببرنامـج جديـد في عـام 2020. ورغـم هـذا التطـور، لا يـزال البرنامـج يفتقـر إلى وجـود قيـادة عسـكرية سـيبرانية متخصصـة تتـولى إدارة ملـف الأمـن السـيبراني بشـكل مبـاشر، حيـث مـا تـزال هـذه المسـؤولية موكلـة إلى القيـادة الاستراتيجيـة العامـة في بريطانيـ

2- القدرات السيبرانية الفرنسية.

تأسست قيادة الدفاع السيبراني الفرنسي في عام 2017، تحت إشراف وزارة الدفاع. وتخضع جميع العمليات الهجومية العسكرية الإلكترونية لهذه القيادة، ولكنها موزعة على المستوى التكتيكي.

كما يوجد فصل بين العمليات السيبرانية الهجومية والدفاعية، فالوكالة الفرنسية للأمن السيبراني تضطلع بصورة حصرية بعمليات الدفاع، كما أن كل فرع من فروع القوات المسلحة الفرنسية مسؤول عن القيام بعملياته الإلكترونية الدفاعية من خلال مركز خاص لإدارة هذه العمليات. ويعتبر مركز تحليل الدفاع السيبراني هو مركز عمليات الأمن التابع لوزارة الدفاع. ويقوم بمهمة تقييم المخاطر السيبرانية العالمية حتى تتمكن القيادة السيبرانية من التصرف وتقديم المشورة للسلطات السياسية. كما يقوم مركز مراجعة أمن نظم المعلومات بإجراء اختبارات الاختراق والتدقيق الأمني على الأنظمة العسكرية. ولقيادة الدفاع السيبراني الفرنسي شركة تسمى «شركة الإشارات 807»، يقع مقرها في رين، وهي مسؤولة عن تأمين الاتصالات وأنظمة الأسلحة

3- القدرات السيبرانية الصينية

أنشأت الصين في عام 2015 قوة الدعم الاستراتيجي كجزء من الإصلاحات التنظيمية لجيش التحرير الشعبي، وتجمع هذه القوة بين قدرات الحرب الفضائية والسيبرانية والنفسية. وتتبع اللجنة العسكرية المركزية، ولها فرعان: إدارة أنظمة الشبكة التي تسيطر على القوة الإلكترونية المسؤولة عن عمليات المعلومات، وإدارة النظم للعمليات الفضائية.

وتتمثل المهام الرئيسة لقوة الدعم الاستراتيجي في الصين في جمع المعلومات الاستخباراتية الفنية، وتزويد القوات المسلحة ببيانات استراتيجية تُمكنها من تنفيذ عمليات تخريبية وهجومية ضد أنظمة العدو، بما يشمل شل شبكاته العسكرية وقيادته المركزية

والحقيقة أن إنشاء الصين لهذه القوة ستكون له تداعياته الإيجابية على القدرة السيبرانية العسكرية الصينية من شقين: أولهما ستكون هذه القوة قادرة على تتبع نوع العمليات المعلوماتية المعقدة والمتعددة الأبعاد، والتي يتوقعها جيش التحرير الشعبي في النزاعات المستقبلية. وثانيهما ستعمل هذه القوة على تحسين الاستعداد العسكري لبكين ومساعدة جيش التحرير الشعبي على التحول السلس من حالة السلم إلى الحرب.

فمن خلال الجمع بين وظائف التجسس والهجوم عبر الوحدات الإلكترونية ووحدات الحرب الفضائية، ومن خلال وضعها تحت قيادة واحدة، يهدف جيش التحرير الشعبي إلى مسح ساحة المعركة، وإعداد عمليات متعددة التخصصات، وتطوير قدرات معينة يمكن تكييفها باستمرار لتلائم متطلبات المواقف سريعة الحركة

البند	الصين	الاتحاد الأوروبي

الهيكل المؤسسي	مركزي وموجه من الدولة	لامركزي (دول متعددة + ENISA)
القدرات الدفاعية	قوية ومتكاملة	عالية تقنيًا ولكن متباينة
القدرات الهجومية	متقدمة ومعلنة في إطار سري	موجودة في بعض الدول (فرنسا، ألمانيا)
السيطرة على الإنترنت	رقابة شديدة وتحكم صارم	حرية نسبية وتعدد منصات
استخدام القوة السيبرانية	هجومي وتجسسي واستراتيجي	دفاعي إلى حد كبير
العلاقات الدولية السيبرانية	المواجهة والغموض	التعاون والشفافية

ثانيا: التطور في القدرات السيبرانية الأمريكية والروسية

تحتفظ كل من روسيا والولايات المتحدة بقدرات متقدمة في مجال تطوير واستخدام «الأسلحة السيبرانية»، وقد بات هذا المجال يدخل ضمن مخصصات الهيئات المعنية بالدفاع والأمن. وتُعدّان من بين الدول الخمس الكبرى في مجال «القوة السيبرانية». وقد تطوّر هذا الصراع إلى بُعد أكثر سخونة، مع قيام روسيا بشنّ هجمات سيبرانية ضد حلفاء الولايات المتحدة، مثل بريطانيا عام 2018، وأوكرانيا عام 2015، وجورجيا بالتزامن مع العمليات الحربية عام 2008، وكذلك ضد إستونيا عام 2007. وعلى إثر هذه الهجمات، أنشأ حلف الناتو مركزًا للدفاع الإلكتروني في إستونيا، وبدأ في دراسة موقفه القانوني من الهجوم السيبراني باعتباره «هجومًا مسلحًا» وفقًا للقانون الدولي، مع بحث إمكانية تطبيق المادة (5) من ميثاق حلف الناتو، والتي تنص على أن أي هجوم مسلح ضد دولة أو أكثر من الدول الأعضاء في أوروبا أو أمريكا الشمالية هجومًا على جميع الدول الأعضاء، ويحق لكل منها، استنادًا إلى حق الدفاع الفردي أو الجماعي المنصوص عليه في المادة 51 من ميثاق الأمم المتحدة، أن تتخذ الإجراءات التي تراها ضرورية، بما في ذلك استخدام القوة المسلحة، لاستعادة الأمن وإعادته في منطقة شمال الأطلسي.على أن أي هجوم أو عدوان مسلح على أي دولة عضو يُعد اعتداءً على جميع الدول الأعضاء، مما يستوجب تفعيل نظام الدفاع المشترك، وهو ما يُنذر بتصاعد التوتر العسكري"[21].

وفي المقابل، اتهمت الدول الغربية، وعلى رأسها الولايات المتحدة، روسيا بشنّ هجمات سيبرانية استهدفت منشآتها الحيوية، في محاولة لبسط سيطرتها المعلوماتية واختراق أنظمة الحماية للبنية التحتية الرقمية. كما وُجّهت إلى روسيا اتهامات باختراق الحزب الديمقراطي الأمريكي عام 2016، والتدخل في الانتخابات الرئاسية لدعم «دونالد ترامب» على حساب

(21) المصدر الرسمي: Charter of the United Nations – Article 51. UN Charter – un.org
https://www.un.org/en/about-us/un-charter/full-text

«هـيلاري كلينتـون»، إضافـة إلى اتهامهـا بعسـكرة الفضـاء الإلـكتروني، واسـتخدام الشـبكات الاجتماعيـة للتـأثير على الـرأي العـام.[22]

وعلى الرغـم مـن أن هـذه الأحـداث تعكـس نقاط مواجهـة سـاخنة بين الولايات المتحـدة وحلفائها مـن جهـة، وروسـيا مـن جهة أخـرى، إلا أن نمـط الصراع اتّخـذ منحى «الحـروب البـاردة» الجديدة، مـن خلال الاتهامـات المتبادلـة بالقرصنـة الإلكترونيـة، وسرقـة الأسرار الصناعيـة، والتجسـس، فـضلاً عـن دعـم روسـيا لحلفائهـا بالتكنولوجيـا السـيبرانية في مجـالات الدفـاع والأمن."

شـمل الصراع بين القـوتين العظمـيين، الولايـات المتحـدة وروسـيا، نمـطين رئيسـيين في توظيـف الفضـاء السـيبراني ضمـن أدوات التدخـل الخارجـي

النمـط الأول: توظيـف القـوة «الناعمـة"، ويتمثـل في اسـتخدام الفضـاء السـيبراني لشـن حـروب نفسـية، ونشر المعلومـات المضللـة، والتـأثير على الـرأي العـام، بالإضافـة إلى دعـم المعارضـة الداخليـة عبر الإنترنـت، سـواء مـن خلال حـملات إعلاميـة موجهـة أو اختراق المنصـات الرقميـة المؤثـرة

النمـط الثـاني: توظيـف القـوة «الصلبـة"، ويتجسّـد في تهديـد أمـن البنيـة التحتيـة المعلوماتيـة للـدول المسـتهدفة، مـن خلال شـنّ هـجمات سـيبرانية، ونشر فيروسـات تخريبيـة، وتطويـر مـا يُعـرف بـ»الأسـلحة السـيبرانية» التـي تُسـتخدم لتعطيـل الأنظمـة الحيويـة كالكهربـاء، والمصـارف، وشـبكات الاتصـالات.

ويعكـس هـذان النمطـان تـداخلاً عميقًـا بين أدوات الحـرب التقليديـة وغير التقليديـة، مما يجعـل الفضـاء السـيبراني سـاحة مرنـة ومعقّـدة لصراعـات النفـوذ في القـرن الحـادي والعشريـن."

جدول رقم(1) يوضح

الفروقات والتقاطعات بين القدرات السيبرانية الأمريكية والروسية

المحور	روسيا الاتحادية	الولايات المتحدة الأمريكية
الجهـات السـيبرانية الرئيسـية	جهـاز الاسـتخبارات العسـكرية - (GRU) جهـاز الأمـن الفيـدرالي - (FSB) مجموعـات هاكـرز - (APT) مدعومـة	(USCY-BERCOM) القيـادة السـيبرانية - وكالـة الأمـن - (NSA) وزارة الأمـن القومـي (DHS) الـداخلي
القدرات الدفاعية	متقدمـة لكـن تركـز أكثر على الدفـاع عـن البنيـة الداخليـة ووسـائل السـيطرة	قويـة، تعتمـد على أنظمـة الـذكاء الاصطناعـي والرصـد المبكـر

(22) تقاريـر الكونغـرس الأمـريكي عـن تدخـل روسـيا عبر وسـائل التواصـل الاجتماعـي: تقريـر لجنـة الاسـتخبارات في مجلـس النـواب الأمريكيـة (2018) https://intelligence.house.gov/uploadedfiles/final_report.pdf

القدرات الهجومية	هجومية وواسعة الانتشار، تشمل اختراقات إعلامية وسياسية وتجارية	متطورة وتُستخدم في إطار ضيق (رسمي أو عسكري فقط)
الهجمات البارزة	إستونيا (2007) - جورجيا - (2008) - أوكرانيا (2015–2022) (- الانتخابات الأمريكية (2016	اغتيالات رقمية مستهدفة - (مع إسرائيل Stuxnet (مثل
التأثير على السياسة الدولية	تدفع نحو مبدأ "السيادة الرقمية" ورفض التدخل الدولي	تدعو لنظام عالمي مفتوح للفضاء السيبراني ومنظم بالقانون الدولي
الدور في الناتو	مصدر تهديد رئيسي للناتو، دفعه لإنشاء مركز الدفاع (Estonia) السيبراني	عضو مؤسس ومحوري في تحديث عقيدة الناتو الإلكترونية
استخدام الشبكات الاجتماعية	أداة استراتيجية للتأثير على الرأي العام وزعزعة المجتمعات	لمواجهة حملات التضليل وتحسين الصورة الدولية
الابتكار والتقنيات	تعتمد على أدوات متقدمة في التشويش والتلاعب المعلوماتي	رائدة في الذكاء الاصطناعي وتحليل البيانات الضخمة
الطابع العام للصراع	صراع غير متماثل يتداخل فيه الحروب النفسية مع التجسس والهجمات	صراع معلوماتي – استخباراتي في إطار منضبط

يُظهر هذا الجدول بوضوح أن الصراع السيبراني بين الولايات المتحدة وروسيا لم يعد مجرد منافسة تقنية على اختراق الأنظمة والشبكات، بل أصبح أحد أبرز تجليات التحوّل في طبيعة الصراع الجيوسياسي في القرن الحادي والعشرين. فقد تحوّل الفضاء السيبراني إلى ميدان غير تقليدي لإعادة رسم توازنات القوى ومفاهيم السيادة، بحيث بات يُستخدم كسلاح ناعم وفعّال لتحقيق أهداف سياسية واستراتيجية دون الحاجة إلى اللجوء للحرب التقليدية. فالولايات المتحدة تسعى إلى تأطير الفضاء السيبراني ضمن منظومة القانون الدولي وضمان حرية الوصول والمساءلة، بينما تروج روسيا لمفهوم «السيادة الرقمية» كوسيلة لحماية فضائها المعلوماتي من التأثيرات الغربية، وكمبرر للهجمات الوقائية التي تشنها ضد خصومها

يتداخل في هذا الصراع البُعد العسكري مع البُعد المعلوماتي والنفسي، حيث أصبحت الهجمات السيبرانية أداة لإرباك المجتمعات، والتأثير على الرأي العام، والتلاعب بنتائج الانتخابات، بل وتشكيل سرديات جديدة تخدم مصالح الدولة المهاجِمة. وبذلك، فإن هذا

الصراع لا يعكس فقط سباقًا على التفوق التكنولوجي، بل يرمز إلى مواجهة أوسع بين نمطين متباينين في الحكم والسيطرة والتأثير، مما يطرح تساؤلات جوهرية حول مستقبل النظام الدولي وحدود الشرعية الرقمية

1- القدرات السيبرانية الأمريكية

تُعتبر الولايات المتحدة الأمريكية الدولة الأكثر تفوقًا في مجال امتلاك القدرات العسكرية السيبرانية، فقد تم تشكيل قيادة سيبرانية موحدة في وقت مبكر من عام 2018، من أجل التماشي مع التطور الكبير والواسع في القدرات السيبرانية الأمريكية، وقد كان هذا أحد أهداف الاستراتيجية السيبرانية الوطنية لوزارة الدفاع الأمريكية. ويشغل منصب قائد هذه القيادة الموحدة مدير وكالة الأمن القومي، وتشرف السلطات الحكومية الأمريكية على تنظيم قدراتها المختلفة.

تعتمد القيادة السيبرانية الأمريكية على خمسة مكونات أساسية: القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة الإلكترونية للقوات الجوية، والقيادة الإلكترونية لقوات مشاة البحرية وخفر السواحل، بالإضافة إلى وحدات الحرس الوطني. ويبلغ عدد الفرق السيبرانية في هذه القيادة نحو 133 فريقًا يضطلع بمهام مختلفة في مجال حماية الأمن السيبراني الأمريكي

وترتكز استراتيجية الفضاء الإلكتروني الأمريكي على مبدأ «الدفاع المتقدم»، لذا ينظر البعض إلى القوة السيبرانية الأمريكية على أنها قوة هجومية في المقام الأول. فالولايات المتحدة الأمريكية أصبحت تركز بشكل متزايد على دمج القدرات التكنولوجية في جميع مراحل العمليات التي تقوم بها قواتها المسلحة، وفي كل مستوى من مستويات القيادة كذلك

جدول: بأهم الهجمات السيبرانية التي تعرضت لها الولايات المتحدة من 2021:2023.[23]

الشهر والسنة	طبيعة الهجوم/ الاعتداءات	حادثة	هدف
يوليو ٢٠٢٣	شراء وبيع البيانات الشخصية الهامة لمسؤولي الحكومة الأمريكية	قام قراصنة صينيون بجمع رسائل البريد الإلكتروني من مختلف المسؤولين الحكوميين الأمريكيين من خلال ثغرة أمنية في نظام البريد الإلكتروني لشركة Microsoft.	وزارة الخارجية ووزارة التجارة

(23) Home Research Long-Form Issue Briefs

Decoding the Biden Administration's Cyber Security Policy

Authors : Vivek Mishra | Sameer Patilhttps://www.orfonline.org/research/decoding-the-biden-administration-s-cy-

يونيو ٢٠٢٣	تركت منشآت الطاقة الحيوية عرضة للهجمات الفضائية والإغلاق.	شن قراصنة مرتبطون بروسيا هجومًا إلكترونيًا عالميًا من خلال استغلال ثغرة أمنية في البرامج التي تستخدمها الوكالات الفيدرالية الأمريكية بشكل شائع.	وكالتان (وزارة الطاقة وأخرى لم يتم تقديم تفاصيلها)
يونيو ٢٠٢٣	تسبب الهجوم الإلكتروني في أضرار لا يمكن إصلاحها لأموال المستشفى، مما أدى إلى إغلاقه.	أصبح المستشفى أول منشأة صحية تشير إلى هجوم الفدية باعتباره السبب الرئيسي لإغلاق أبوابها.	مستشفى في إلينوي
مايو ٢٠٢٣	إن وصول المتسللين إلى أوراق الاعتماد المشروعة للأفراد العسكريين الأمريكيين جعل اكتشافهم أكثر صعوبة.	تمكن قراصنة صينيون من الوصول إلى شبكات الاتصالات في موقع عسكري أمريكي في جزيرة غوام.	القاعدة الأمريكية في غوام
أبريل ٢٠٢٣	ويُشتبه في أن المجموعة، التي يُعتقد أنها نشطة منذ عام ٢٠١٤، قامت بتركيب أبواب خلفية في مختلف قطاعات الصناعة. التفاصيل لا تزال غير معروفة.	أطلق المتسللون الإيرانيون المرتبطون بالدولة سلسلة من الهجمات التي استهدفت البنية التحتية الحيوية في الولايات المتحدة ودول أخرى باستخدام برامج ضارة غير مسبوقة. تم تعديلها لهذا الغرض المحدد.	البنية التحتية الأمريكية

ber-security-policy#_edn7:~:text=Home,SAMEER%20PATIL

مارس ٢٠٢٣	اكتشف المتسلل ثغرة أمنية في خادم خدمات Mi-معلومات الإنترنت التابع للوكالة crosoft وقام بتثبيت برامج ضارة، مما أدى إلى سرقة معلومات حساب المستهدفين.	هجمات متعددة على الوكالات الفيدرالية الأمريكية كجزء من حملة تجسس إلكتروني بين نوفمبر ٢٠٢٢ ويناير ٢٠٢٣، بما في ذلك من قبل مجموعة تجسس فيتنامية.	وكالات فيدرالية
مارس ٢٠٢٣	تهدف الحملة إلى تقديم برامج ضارة للتجسس عبر الإنترنت من خلال تنزيلات الخلفية Whatsapp المزروعة، والحصول على المعلومات الشخصية لآلاف المستخدمين.	صمم قراصنة كوريا الشمالية حملة تصيد احتيالي ضد شركات أبحاث الأمن السيبراني التي يوجد مقرها في الولايات المتحدة.	شركات أبحاث الأمن السيبراني ومقرها الولايات المتحدة
فبراير ٢٠٢٣	وأعاق الهجوم الاتصالات بين مقر حلف شمال الأطلسي والطائرات التي تقدم المساعدات بعد الزلزال الذي ضرب تركيا.	شنت مجموعة قرصنة موالية لروسيا على أنظمة الناتو DDoS هجمات التي تتعامل مع البيانات الحساسة وتنقلها. كما تمت إزالة موقع الناتو مؤقتًا.	شبكات منظمة حلف شمال الأطلسي (الناتو).
ديسمبر ٢٠٢٢	تم عرض المعلومات المسروقة للبيع على الإنترنت مقابل ٥٠ ألف دولار أمريكي.	استولى المتسللون على تفاصيل الاتصال لأكثر من ٨٠ ألف عضو في برنامج تبادل معلومات التهديدات التابع لمكتب التحقيقات الفيدرالي، InfraGard.	مكتب التحقيقات الفدرالي

ديسمبر ٢٠٢٢	تمت سرقة الأموال من قروض إدارة الأعمال الصغيرة وأموال التأمين ضد البطالة، ولم يمكن استرداد سوى نصفها. وقد أثر هذا بشكل غير متناسب على أولئك الذين ينتمون إلى الطبقات الاجتماعية والاقتصادية الدنيا، وزاد من المشاكل الاقتصادية للحكومة.	سرق قراصنة مدعومون من الحكومة الصينية ما يقدر بنحو ٢٠ مليون دولار أمريكي من أموال الإغاثة الخاصة بكوفيد-١٩ من الحكومة الأمريكية.	الحكومة الأمريكية
نوفمبر ٢٠٢٢	قام المتسللون بتثبيت برامج تعدين العملات المشفرة والبرامج الضارة للتنقل عبر أنظمة الوكالات الفيدرالية والحصول على معلومات حساسة.	هاجم قراصنة مدعومون من الحكومة الإيرانية مجلس حماية أنظمة الجدارة الأمريكي، مستغلين log4، وهي نوع من الثغرة واجهة الأمنية في تنفيذ التعليمات البرمجية عن بعد والتي تمكن الجهات الفاعلة الضارة من استهداف الخوادم.	مجلس حماية أنظمة الجدارة الأمريكية
نوفمبر ٢٠٢٢	أثر ناقل العدوى على مجموعة من كيانات القطاعين العام والخاص، في المقام الأول في جنوب شرق آسيا وامتد إلى الولايات المتحدة وأوروبا.	لقد دبر قراصنة يشتبه في صلاتهم بالصين حملة تجسس على المنظمات العامة والخاصة في الفلبين وأوروبا والولايات المتحدة، بدءًا من عام ٢٠٢١.	المنظمات العامة والخاصة في الولايات المتحدة
أكتوبر ٢٠٢٢	وأعلنت مجموعة قرصنة موالية لروسيا عن الهجوم قبل أن يؤثر على المواقع. لقد جعل الوصول إلى المواقع الإلكترونية لـ ١٤ مطارًا عامًا غير ممكن.	استهدف قراصنة مستقلون العديد من المطارات الرئيسية في الولايات المتحدة، مما أثر على DDoS بهجمات المتحدة، مواقعهم الإلكترونية.	المطارات في الولايات المتحدة

أكتوبر ٢٠٢٢	أصبح الوصول إلى المواقع الرسمية لحكومات الولايات غير ممكن بشكل متقطع. وكشف الهجوم عن قدرة المتسللين المدعومين من الحكومة الروسية على تشويه مواقع الويب والتلاعب بالمعلومات، مما قد يؤثر على النتائج السياسية.	تفاخر المتسللون المؤيدون لروسيا بدورهم في الهجوم الذي أدى إلى تعطل المواقع الإلكترونية الحكومية في ولايات كولورادو وكنتاكي والمسيسيبي.	موقع حكومة الولايات الأمريكية
أكتوبر ٢٠٢٢	وقد تسربت معلومات تتعلق بالأمن القومي لفترة طويلة دون علم السلطات.	وقيل إن العديد من المتسللين الذين ترعاهم الدولة لديهم إمكانية الوصول على المدى الطويل إلى شركات الدفاع، وبالتالي المعلومات الحساسة.	شركات الدفاع الأمريكية
يونيو ٢٠٢٢	أتاحت اختراقات شركات الاتصالات للقراصنة إمكانية الوصول إلى البيانات الشخصية للمواطنين العاديين، وتم استخدامها لاستغلال مجموعة واسعة من الأهداف في جميع أنحاء العالم، بما في ذلك مؤسسات القطاعين العام والخاص.	وهاجم قراصنة مدعومون من الصين شركات الاتصالات الكبرى وخدمات الشبكات منذ عام ٢٠٢٠ على الأقل.	شركات الاتصالات الأمريكية ومقدمو خدمات الشبكات

يونيو ٢٠٢٢	سرقت الحملة بيانات اعتماد Microsoft Office 365 وOutlook من هذه الشركات.	استهدفت حملة التصيد الاحتيالي الشركات الأمريكية في قطاعات الدفاع والبرمجيات وسلسلة التوريد والرعاية الصحية والأدوية.	شركات أمريكية مختلفة
مايو ٢٠٢٢	وقد أدى هذا الاختراق إلى تعريض جهود البحث والتطوير الأمريكية للخطر وتقويض موقف الأمن السيبراني لهذه القطاعات.	سرقت مجموعات القرصنة الصينية الملكية الفكرية من الشركات الأمريكية والأوروبية في عام ٢٠١٩.	الشركات الامريكية
أبريل ٢٠٢٢	قام المتسللون بتحويل الأموال إلى خلاط العملات المشفرة لإخفاء مصدر الأموال.	اخترق قراصنة من كوريا الشمالية Ronin Network منصة التمويل اللامركزي وسرقوا ما قيمته ٥٤٠ مليون دولار أمريكي من عملة الإيثيريوم والعملة المستقرة المرتبطة بالدولار الأمريكي USDC.	دولار أمريكي
أبريل ٢٠٢٢	واستهدفت الحملة الناشطين والأكاديميين والشركات الخاصة، مثل قطاعات الطاقة وأشباه الموصلات والاتصالات في الولايات المتحدة، إلى جانب العديد من البلدان التي تستخدم تقنيات التصيد والهندسة الاجتماعية، والتي صورت قدرات إيران المستمرة على التصيد للحصول على بيانات الاعتماد وعمليات المراقبة.	استهدفت مجموعتا تجسس إلكتروني مرتبطتان بإيران أكاديميين وناشطين وصحفيين وغيرهم من الضحايا.	الأعمال في قطاعات الطاقة وأشباه الموصلات والاتصالات

مارس ٢٠٢٢	أدى الهجوم إلى تعطيل خدمات الإنترنت في جميع أنحاء أوروبا وكذلك الاتصالات العسكرية الأوكرانية في المراحل الأولى من الغزو الروسي.	الأمريكية Viasat هاجم قراصنة شركة واستهدفوا أجهزة مودم الأقمار الصناعية لآلاف الأوروبيين.	خدمة النطاق العريض عبر الأقمار الصناعية التابعة لشركة Viasat الأمريكية
فبراير ٢٠٢٢	زودت البيانات المسروقة المهاجمين بمعرفة كبيرة حول جداول تطوير ونشر منصات الأسلحة الأمريكية، وخطط البنية التحتية للاتصالات، والتقنيات المحددة التي تستخدمها الحكومة والجيش الأمريكي.	اخترق قراصنة روسيون ترعاهم الدولة العديد من مقاولي الدفاع الأمريكيين بين يناير/كانون الثاني ٢٠٢٠ وفبراير/شباط ٢٠٢٢. وقاموا بالتنقيب في رسائل البريد الإلكتروني والبيانات الحساسة المتعلقة بمنتجات الشركات الخاضعة لرقابة التصدير، ومعلومات الملكية، والتفاعلات مع الحكومات الأجنبية.	مقاولو الدفاع الأمريكيون
ديسمبر ٢٠٢١	حاول المتسللون الوصول على المدى الطويل إلى أنظمة الكمبيوتر لسرقة البيانات الحساسة من الشركات الأمريكية.	هاجم قراصنة صينيون أربع شركات دفاع وتكنولوجيا أمريكية.	شركات الدفاع والتكنولوجيا الأمريكية
نوفمبر ٢٠٢١	وقد عرّضت البيانات المسروقة هوية الأفراد للخطر وأتاحت المجال لارتكاب جرائم سرقة الهوية.	اخترق قراصنة الضمان الاجتماعي للموظفين وأرقام رخص القيادة عن طريق اختراق مقاول دفاع أمريكي.	مقاول الدفاع الأمريكي

نوفمبر ٢٠٢١	ولا يزال مدى خرق البيانات غير واضح.	اخترق المتسللون بوابة مؤسسة إنفاذ القانون التابعة لمكتب التحقيقات الفيدرالي، وهو نظام يستخدم للتواصل مع المسؤولين الحكوميين والمحليين.	بوابة مؤسسة إنفاذ القانون التابعة لمكتب التحقيقات الفيدرالي
أكتوبر ٢٠٢١	وكانت الحسابات المستهدفة إما تابعة لشركات تكنولوجيا الدفاع الأمريكية أو الإسرائيلية التي ركزت على موانئ الدخول في الخليج العربي أو شركات النقل البحري التي لها وجود في المنطقة.	حاولت مجموعة قرصنة تابعة لإيران اختراق أكثر من ٢٥٠ حسابًا على Office 365.	شركات تكنولوجيا الدفاع الأمريكية
أكتوبر ٢٠٢١	أثر الهجوم على سلاسل توريد تكنولوجيا المعلومات، بما في ذلك الموزعين ومقدمي خدمات التكنولوجيا الآخرين الذين يقومون بتخصيص ونشر وإدارة الخدمات السحابية والتقنيات الأخرى نيابة عن عملائهم في الولايات المتحدة.	كشفت شركة أمريكية أن جهاز المخابرات الخارجية الروسي أطلق حملة تستهدف الموزعين ومقدمي خدمات التكنولوجيا الآخرين.	شركة أمريكية
يوليو ٢٠٢١	من المحتمل أن يكون خرق البيانات الحساسة قد أدى إلى طلب فدية من المتسللين.	أنشأ قراصنة إيرانيون حسابات مزيفة على فيسبوك للتظاهر بأنهم مجندون وصحفيون ومنظمات غير حكومية لمهاجمة أفراد الجيش الأمريكي.	أفراد الجيش الأمريكي

يونيو ٢٠٢١	ولم يكن حجم الأضرار الناجمة عن خرق البيانات واضحا.	قام قراصنة مرتبطون بالمخابرات الروسية بتثبيت برامج ضارة على أجهزة الكمبيوتر، مما فتح بابًا خلفيًا للقراصنة للوصول إلى الحسابات ومعلومات الاتصال.	عملاء Microsoft المقيمون في الولايات المتحدة، والذين يعملون في شركات تكنولوجيا المعلومات والحكومة
يونيو ٢٠٢١	كشف الاختراق عن معلومات حساسة حول الأسلحة النووية.	هاجمت مجموعة القرصنة REvil المرتبطة بروسيا مقاولًا حكوميًا يعمل لصالح وزارة الطاقة في مجال تكنولوجيا الأسلحة النووية.	سول أورينس
مايو ٢٠٢١	سرق المهاجمون ٧٠ غيغابايت من الملفات الداخلية ووضعوها على الشبكة المظلمة.	تم استهداف شركة خطوط الأنابيب Colonial بهجوم فدية إلى جانب Pipeline.	خدمات النزاهة Lin-eStar
مايو ٢٠٢١	أدت حملة برامج الفدية إلى تعطيل خدمات العديد من الشركات.	أطلق مكتب التحقيقات الفيدرالي ومركز الأمن السيبراني الأسترالي (FBI) ناقوس الخطر بشأن حملة برامج التي تستهدف (Avaddon) الفدية قطاعات مختلفة في بلدان متعددة.	الأوساط الأكاديمية وشركات الطيران والبناء وشركات الطاقة
مايو ٢٠٢١	واجهت الشركة اضطرابات في عملياتها ودفعت في النهاية فدية قدرها ٥ ملايين دولار أمريكي.	تم استهداف خط الأنابيب في هجوم Darkside، وهي، يُنسب إلى جماعة إجرامية مقرها روسيا.	خط الأنابيب الاستعماري

أبريل ٢٠٢١	وتتهم الولايات المتحدة الصين بشكل منتظم بالتجسس التجاري عبر الإنترنت الذي يستهدف مقاوليها الدفاعيين. ربما كان هذا الهجوم جزءًا من هذه الحملة.	استخدم قراصنة مدعومون من الدولة، وبعضهم تابع للصين، ثغرة لمهاجمة VPN أمنية في خدمة المؤسسات في جميع أنحاء الولايات المتحدة وأوروبا، وخاصة شركات الدفاع الأمريكية.	مقاولو الدفاع الأمريكيون
أبريل ٢٠٢١	ولو نجح المتسللون، لكان من الممكن أن يتسببوا في اضطرابات واسعة النطاق.	هاجم قراصنة مدعومون من الصين ومع ذلك، لم ينجح MTA. شركة	هيئة النقل الحضرية في مدينة نيويورك (MTA)
مارس ٢٠٢١	تمت سرقة التفاصيل الشخصية والطبية للأفراد المرتبطين بالأمن القومي.	استهدف قراصنة إيرانيون مشتبه بهم باحثين طبيين في إسرائيل والولايات المتحدة للوصول إلى أوراق اعتماد علماء الوراثة، وأطباء الأعصاب، وأطباء الأورام.	الباحثين الطبيين
مارس ٢٠٢١	ومن خلال الاختراق، تمكن المتسللون من الوصول إلى عدة أجزاء من المعلومات السرية.	حصل قراصنة روس مزعومون على آلاف رسائل البريد الإلكتروني بعد هجوم على خادم البريد الإلكتروني التابع لوزارة الخارجية الأمريكية.	وزارة الخارجية الأمريكية
فبراير ٢٠٢١	وسعى المتسللون إلى الحصول على معلومات حول اللقاحات والعلاجات لـ COVID-19.	حاول قراصنة كوريون شماليون اختراق أنظمة الكمبيوتر الخاصة بشركة فايزر، وهي شركة أدوية.	فايزر

يناير ٢٠٢١	وكان الغرض من الهجمات جمع المعلومات الاستخبارية وسرقة البيانات.	استهدف قراصنة مرتبطون بحزب الله شركات الاتصالات ومقدمي خدمات الإنترنت ومقدمي الاستضافة في الولايات المتحدة والمملكة المتحدة ومصر وإسرائيل ولبنان والأردن والمملكة العربية السعودية والإمارات العربية المتحدة وفلسطين.	شركات الاتصالات ومقدمو خدمات الإنترنت ومقدمو خدمات الاستضافة في الولايات المتحدة

تبنّت الولايات المتحدة في عام 2017 قانون «كاتسا" (CAATSA) الخاص بمواجهة خصومها من خلال العقوبات، والذي شمل 33 شخصية ومؤسسة روسية على صلة بالصناعات العسكرية والأمنية والاستخباراتية. كما فرضت واشنطن قيودًا على وسائل الإعلام الروسية، إضافة إلى طرد عدد من الدبلوماسيين الروس

وعلى الرغم من تصاعد التوتر بين البلدين، فقد تم تدشين «خط ساخن» بين الولايات المتحدة وروسيا في عام 2013 بهدف تجنّب الحوادث السيبرانية الكارثية، إلا أن هذا الخط توقّف عن العمل عقب الغزو الروسي لأوكرانيا في عام 2014. كما شهد التعاون الدولي في هذا المجال انتكاسة كبيرة، مع انهيار مجموعة الخبراء الحكوميين حول أمن المعلومات، التي كانت تُدار برعاية الأمم المتحدة، وذلك نتيجة الفشل في التوصل إلى توافق حول آليات تعزيز الأمن السيبراني العالمي[24]

في أغسطس 2018، أقرّت الولايات المتحدة استراتيجية جديدة للأمن السيبراني، اتسمت باتخاذ موقف أكثر شراسة في مواجهة التهديدات الإلكترونية المتزايدة من دول مثل الصين وروسيا وغيرها. وقد دخلت هذه الاستراتيجية حيّز التنفيذ في أعقاب قرار الرئيس دونالد ترامب إلغاء القيود التي كان قد فرضها سلفه باراك أوباما على العمليات السيبرانية، مما أتاح للولايات المتحدة هامشًا أوسع للتحرّك الهجومي في الفضاء الإلكتروني

وتقوم هذه الاستراتيجية على عدة محاور رئيسية، أبرزها: بناء قوة أكثر فتكًا واستعدادًا للحرب، وتوسيع التحالفات والشراكات السيبرانية، والتأكيد على أن أي نشاط سيبراني عدائي ضد الولايات المتحدة أو حلفائها سيُواجَه بردّ هجومي ودفاعي، وقد لا يقتصر هذا الرد على الفضاء السيبراني، بل قد يشمل المجال العسكري التقليدي. كما تنصّ الاستراتيجية على أن فشل الردع في مواجهة الأنشطة السيبرانية التي تُعدّ استخدامًا للقوة، قد يدفع الولايات

(24) صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، https://accronline.com/article_detail.aspx?id=32528#~:

المتحدة إلى استخدام القوة المشتركة، بما في ذلك الوسائل العسكرية المادية

ومن أبرز التحولات في هذه الاستراتيجية تبنّي مفهوم «الهجوم الدفاعي»، والذي يقوم على التحرك الاستباقي خارج الحدود، واختراق شبكات الخصم، وتعزيز القدرات على جمع المعلومات الاستخباراتية، والاستعداد لصراعات مستقبلية محتملة

وترى الولايات المتحدة أن الفضاء السيبراني يجب أن يكون رافدًا لتكريس تفوّقها العسكري، ومجالًا لممارسة الأنشطة الاستخباراتية، وحماية الأمن القومي، وردع القوى الدولية المنافسة، بالإضافة إلى مواجهة سرقة الأسرار الصناعية، وصدّ تهديدات البنية التحتية المعلوماتية، والدفاع عن النظام الديمقراطي الأمريكي."

2- القدرات السيبرانية الروسية

اعتبرت الاستراتيجية والعقيدة العسكرية الروسية تاريخيًا أن الأمن السيبراني والعمليات الإلكترونية يشكلان جزءًا من عمليات المعلومات بمفهومها الواسع، مما قد يُطمس التمييز بين القدرات العسكرية والمدنية. لكن العقيدة العسكرية الروسية لعام 2015 أوضحت أن الفضاء الإلكتروني يُعد جزءًا من الأراضي الروسية، وبناءً عليه كُلفت القوات المسلحة بحمايته

وفي عام 2011، صدرت وثيقة بعنوان «آراء مفاهيمية حول نشاط القوات المسلحة للاتحاد الروسي في فضاء المعلومات»، قدّمت فيها القوات المسلحة رؤيتها لدورها في الفضاء الإلكتروني، مع التركيز على الوعي بالتهديدات وحماية القوة

وفي عام 2017، شكّلت السلطات الروسية «قوات عمليات المعلومات»، وقد اعتقد البعض أن مهام هذه القوات تقتصر على المسؤوليات السيبرانية، إلا أن معظم المؤشرات تشير إلى تركيزها الأساسي على الأنشطة التقليدية للمعلومات والعمليات النفسية

وبحسب السلطات الأمريكية، تُعد المديرية الرئيسية لهيئة الأركان العامة الروسية، والتشكيلات التابعة لها، بما في ذلك مركز الخدمة الخاصة الرئيسي الخامس والثمانين (الوحدة 26165) ومركز الخدمة الخاصة رقم 72 (الوحدة 54777)، الجهات الفاعلة الرئيسة في مجال العمليات السيبرانية الهجومية

لم تُنشئ روسيا قيادة عسكرية منفصلة للفضاء السيبراني كما فعلت الولايات المتحدة، لكنها تعتمد على استراتيجيات حديثة لتعزيز قدراتها في مجال القوة السيبرانية. ترتكز الرؤية الروسية على استخدام مصطلح «أمن المعلومات» كتعريف أوسع يشمل «الأمن السيبراني» باعتباره جزءًا من هذا المفهوم الشامل. وتعتبر روسيا أن ممارسة الرقابة والتنظيم الكامل للأمن السيبراني من قبل الدولة أمرٌ صعب التحقيق، لذا تسعى لبناء معايير دولية عبر التعاون في الفضاء السيبراني، سواء لتعزيز مواجهة التهديدات الداخلية المتعلقة بأمن المعلومات أو التصدي للتهديدات الخارجية

وتُعدّ أبرز سمات الأمن السيبراني الروسي

تطبيق مبدأ «السيادة السيبرانية" (Cyber Sovereignty)، حيث تركز على سيطرة الدولة على الفضاء السيبراني داخل حدودها الوطنية، مع التأكيد على الدور المحوري للدولة في مجال المعلومات والتنظيم والسيطرة. وتُشكّل هذه الرؤية الوطنية للأمن السيبراني أساسًا استراتيجيًا للسياسة الروسية في هذا المجال، وهو ما يُعد عائقًا أمام جهود بناء معايير دولية مشتركة للأمن السيبراني، وفقًا لوجهة نظر الدول الغربية.[25]

يُذكر هذا المنظور الروسي في العديد من الوثائق الرسمية المتعلقة بعقيدة الاتحاد الروسي بشأن «ضمان أمن المعلومات»، حيث تظهر نية الحكومة الروسية لقيادة الجهود الدولية لتحقيق مستويات عالية من الأمن من خلال عدة وسائل قانونية ومؤسسية وتقنية وغيرها لكن هذا النهج يواجه انتقادات حادة من القوى الغربية، وعلى رأسها الولايات المتحدة، التي ترى في سياسات روسيا ممارسات استبدادية تهدف إلى قمع الحريات وتضييق نطاق المعارضة الداخلية، معتبرةً أن ذلك يعكس «تحكمًا» مفرطًا في الفضاء السيبراني. على الرغم من ذلك، تتضمن الاستراتيجية الروسية للأمن السيبراني مبدأً ينص على احترام حرية المواطنين وحقوقهم الدستورية، مما يعني أن السيادة الروسية على الفضاء السيبراني لا تصل إلى درجة «السيطرة الكاملة»، بل هي أقرب إلى مستوى «الرقابة"

تحافظ روسيا على علاقات تعاونية مع الصين في مجال الفضاء السيبراني، من خلال اتفاقية عام 2015 وانضمامها إلى منظمة شنغهاي للتعاون، بينما لا توجد علاقات متقاربة مع الولايات المتحدة فيما يخص التفاوض حول قضايا الفضاء السيبراني

ورغم ذلك، تصر روسيا على سعيها لإرساء قواعد دولية تستند إلى توافق جماعي، إلا أن هناك تناقضات مع القوى الغربية حول وضع معايير الإنترنت الدولية، خاصة فيما يتعلق بالاختلاف في تناول ومعالجة مفهومي «الفضاء السيبراني» و«السيادة السيبرانية». كما توجد خلافات بشأن استخدام السلطة السيادية في الفضاء السيبراني وتعريف «التهديدات السيبرانية»، التي تصنفها روسيا تحت مصطلح أوسع هو «التهديدات الأمنية المعلوماتية»، مفرقةً بين التهديدات الخارجية والداخلية، مع تركيز خاص وحساسية عالية تجاه التهديدات الموجهة إلى الداخل الروسي

جدول رقم(2) يوضح أبرز الضربات السيبرانية التي تعرّضت لها روسيا

الهدف / تفاصيل الهجوم	الجهة المشتبه بها/ المنفذة	اسم أو نوع العملية	التاريخ
تعرّضت بعض الخوادم الحكومية لانقطاعات بسبب اختبارات في سياق تدريبات سيبرانية	غير معروف (قد تكون اختبارات داخلية)	هجوم على مواقع حكومية روسية	أبريل ٢٠٠٧

(25) صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، https://accronline.com/article_detail.aspx?id=32528#

شل بعض المواقع الإعلامية والحكومية الروسية كردّ على التدخل في أوكرانيا	نشطاء أوكرانيون/ جهات غير حكومية	عقب DDoS هجمات غزو القرم	مارس ٢٠١٤
تسلّل الفيروس عبر شركات روسية وأصاب أنظمة عديدة، منها شركات نفط ومطارات وبنوك	يُعتقد أنها من مجموعة أوكرانية أو غربية	**NotPetya**	يونيو ٢٠١٧
تعطيل مواقع حكومية وإعلامية كبرى مثل RT، الكرملين، وزارة الدفاع الروسية	جماعة «أنونيموس" (Anonymous)	قبل وبعد غزو أوكرانيا	فبراير ٢٠٢٢
تم تغيير محتوى البث المباشر الروسي ليعرض مشاهد من الحرب في أوكرانيا ومقاطع مناوئة للغزو	Anonymous	اختراق بث قنوات حكومية	24 فبراير ٢٠٢٢
تسريب بيانات وزارات ومؤسسات مثل Roskomnadzor ووزارة الدفاع، ونشرها على الإنترنت	جماعات غربية / هاكرز مستقلون	سلسلة اختراقات قواعد بيانات	مارس-يونيو ٢٠٢٢
تعطيل أنظمة النقل العسكرية الروسية لإعاقة إمدادات القوات في أوكرانيا	قراصنة أوكرانيون (تقديريًا)	اختراق نظام السكك الحديدية	يوليو ٢٠٢٢
استهداف النظام المالي الروسي عبر رسائل وهمية وبرمجيات خبيثة	جماعات مرتبطة بالغرب (تقديريًا)	عمليات تصيد إلكتروني ضد البنوك	2023
إيقاف مؤقت لمواقع وزارات ومؤسسات سيادية، منها وزارة الطاقة والاتصالات	Ukraine IT Army / Anonymous	تعطيل مواقع حكومية روسية كبرى	يناير ٢٠٢٤
محاولة لتعطيل بديل روسيا لنظام Visa/Mastercard ضمن العقوبات الغربية.	جهة غير معلومة – يُرجح دعم استخباراتي	هجوم على نظام "مير" للدفع البنكي	(مطلع) 2025
			المصدر: متابعات إخبارية الباحث.

الخطوات الروسية لمواجهة الاستراتيجية الامريكية

1- أنشأ جهاز الأمن الفيدرالي الروسي عام 2018 تزامنا مع اعتماد الاستراتيجية الأمريكية في الفضاء السيبراني، مركزا وطنيا لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية في روسيا، يتولى مهام الكشف والوقاية والقضاء على تداعيات الهجمات الإلكترونية، وتبادل المعلومات بين الهيئات المتخصصة في الداخل والخارج وتحليل الهجمات السيبرانية الماضية وتطوير أساليب مكافحتها.

2- وافق البرلمان الروسي في2018 على قانون عزل البلاد عن شبكة الإنترنت العالمية، لجعل روسيا في موقع أفضل لصد أي هجمات إلكترونية محتملة من الخارج، خاصة من قبل الولايات المتحدة الأمريكية. فالهجمات الإلكترونية وفق استراتيجية الأمن الروسي تأتي الأولى ضمن قائمة أكثر المخاطر التي تهدد البنية التحتية الروسية، بينما تأتي في المرتبة الثانية عملية تطوير القدرات التكنولوجية للقوات المسلحة حتى يتحقق الردع الإلكتروني.

3- أنشأت روسيا الاتحادية وكالة أبحاث الانترنت، أو ما يعرف باسم "جيش المتصيدين" تابع لوكالة الأمن الاتحادي الروسي يضم الاف الموظفين ويخصص له سنويا 300مليون دولار من ميزانية الدفاع الروسية، إذ يعد الجيش الالكتروني الروسي خامس أقوى جيوش العالم الالكترونية بعد كل من: الولايات المتحدة والصين وبريطانيا وكوريا الشمالية على التوالي.

ويمكن أن نحدد الاستراتيجية الدفاعية السيبرانية الروسية في الآتي:

1- حماية البنى التحتية تعزز روسيا أمن أنظمة الاتصالات والشبكات المستخدمة في العديد من القطاعات مثل الطاقة والنقل والدفاع، حيث ترى هذه البنى كجزء من سيادتها الرقمية التي يجب حمايتها من الهجمات.

2- الردع السيبراني تمزج روسيا بين الهجوم السيبراني الوقائي والدفاعي بهدف ردع أي محاولة اختراق أو هجوم محتمل، وتطوير القدرة على الهجوم والدفاع مما يمكنها من مواجهة التهديدات السيبرانية .

3- الحرب المعلوماتية وفق العقيدة الروسية لا يوجد خط واضح بين السلم والحرب في السيبرانية اذ تعمل روسيا على مراقبة الأنظمة والتدخل في الاعِتداءات المعلوماتيه للتفوق في مواجهة التهديدات السيبرانية .

4- تطوير القدرات تعتمد روسيا بشكل كبير على التعلم من الحوادث السابقة لتحسين دفاعاتها، وتمثل الهجمات التي تعرضت لها مصدر لتحليل نقاط الضعف وتقوية الدفاعات.

***

ومن خلال تحليل الاستراتيجية السيبرانية للولايات المتحدة الأمريكية وروسيا، يتبين أن كلا الدولتين قد طوّرتا سياسات واستراتيجيات معقّدة لمواجهة أي تهديد سيبراني. فقد ركّزت الولايات المتحدة على تعزيز الدفاعات السيبرانية وتطوير تقنيات متقدمة لرصد ومنع الهجمات، في حين أولت روسيا اهتمامًا أكبر بدعم القدرات الهجومية المتقدمة، واستخدام الفضاء السيبراني كوسيلة لتحقيق أهدافها الجيوسياسية، من خلال توظيف استراتيجية شاملة تجمع بين القوة الصلبة والناعمة لتعزيز أمنها القومي وضمان مكانتها في منظومة الهيمنة العالمية

وتُظهر المعطيات أن التهديدات السيبرانية تُحدث تأثيرات بعيدة المدى على العلاقات

الدولية، ما يستوجب تعاونًا دوليًا فعّالًا وإطارًا قانونيًا واضحًا لضمان أمن واستقرار الفضاء السيبراني. ومن الضروري أن يعمل المجتمع الدولي على التصدي لهذه التهديدات، وتعزيز الثقة المتبادلة بين الدول، والتأكيد على أهمية التفاهم والحوار لتجنّب النزاعات المستقبلية

***

نتائج المبحث الثاني:

توصلت البحث الى نتيجة عامة مفادها أن تصاعد التهديدات في الفضاء السيبراني أدّى إلى إعادة تعريف مفاهيم كلاسيكية في نظريات العلاقات الدولية، مثل القوة والردع والسيادة. ففي هذا المجال غير المتناظر وغير المحدود جغرافيًا، أصبحت القدرات الرقمية والمعلوماتية بديلاً فعّالًا عن القوة الصلبة التقليدية، بل ومكمّلًا لها في إدارة الصراع والتأثير الجيوسياسي. وهذا يفرض على الدول تبني نماذج جديدة من الردع السيبراني تتجاوز مفهوم الدفاع السلبي، نحو تبني استراتيجيات مرنة تتضمن الردع بالتكلفة، والردع بالحرمان، والردع بالإبهام، بما يعزز مناعة الدولة الرقمية، ويحافظ على استقرار النظام الدولي في وجه هذا التهديد المتنامي

نتائج البحث التفصيلية

1. أصبحت القدرات السيبرانية مكونًا رئيسيًا في تقييم القوة الوطنية والردع الاستراتيجي للدول، إلى جانب القوة العسكرية التقليدية.
2. يشهد مفهوم الردع تحولًا نوعيًا، من الردع النووي أو العسكري إلى الردع السيبراني القائم على القدرة على تنفيذ أو إحباط هجمات إلكترونية.
3. يختلف نموذج بناء القوة السيبرانية من دولة لأخرى؛ حيث تعتمد الصين نموذجًا مركزيًا هجوميًا، بينما يتبنى الاتحاد الأوروبي نموذجًا دفاعيًا لا مركزيًا.
4. المملكة المتحدة وفرنسا طوّرتا قدرات هجومية ودفاعية سيبرانية محدودة، مع استمرار التحديات الهيكلية في توحيد القيادة والفاعلية العملياتية.
5. الصين دمجت بين قدرات الحرب السيبرانية والفضائية والنفسية تحت قيادة موحدة ضمن «قوة الدعم الاستراتيجي»، ما عزز قدرتها على تنفيذ عمليات معقدة.
6. تعتمد القدرات السيبرانية الصينية على فلسفة الدولة–الأمن، مع تركيز على الرقابة والسيطرة المعلوماتية الداخلية والخارجية.
7. تميزت القدرات السيبرانية الأوروبية بالتركيز على الحماية والشفافية، مع احترام القيم الديمقراطية وحقوق الخصوصية، مما حدّ من فاعلية القدرات الهجومية.
8. تحتفظ الولايات المتحدة وروسيا بأكبر وأخطر منظومات السيادة السيبرانية، مما جعلهما فاعلين رئيسيين في تشكيل بيئة الصراع الرقمي العالمي.
9. طورت الولايات المتحدة قيادة سيبرانية مركزية (USCYBERCOM) وأنظمة رصد مبكر تعتمد على الذكاء الاصطناعي وتحليل البيانات الضخمة.

10. تركز الاستراتيجية السيبرانية الروسية على الهجوم غير المتماثل والتخريب والاختراق النفسي، باستخدام مجموعات قرصنة مدعومة حكوميًا.
11. شهدت الفترة 2021–2025 أكثر من 30 هجومًا إلكترونيًا عالي التأثير على الولايات المتحدة، طالت وزارات، مؤسسات دفاعية، بنى تحتية، ومراكز أبحاث.
12. تتداخل في الهجمات السيبرانية أدوات الحرب النفسية، التضليل الإعلامي، والتجسس الصناعي، مما يجعلها سلاحًا هجوميًا شاملًا ومتعدد الوظائف.
13. استخدمت روسيا والصين وإيران الفضاء السيبراني كأداة لتوسيع النفوذ الجيوسياسي، سواء عبر استهداف الانتخابات، أو البنية التحتية، أو الاقتصاد الرقمي.
14. تحول الفضاء السيبراني إلى ساحة مواجهة غير تقليدية ضمن صراع النفوذ بين القوى الكبرى، دون التورط المباشر في الحروب العسكرية التقليدية.
15. تعاني المنظومة الدولية من فراغ قانوني دولي واضح ينظم الصراعات السيبرانية، مع غياب معايير حاكمة لمسؤولية الدولة وحدود الرد المشروع.
16. تُوظّف مفاهيم مثل «السيادة الرقمية» من قبل دول مثل روسيا والصين لتبرير الهجمات السيبرانية الوقائية ورفض التنظيم الدولي المشترك.
17. ازداد دور الفاعلين من غير الدول (مثل جماعة Anonymous وREvil) في شن هجمات عابرة للحدود، مما زاد من تعقيد مشهد التهديدات السيبرانية.
18. تداعيات الهجمات السيبرانية تجاوزت الأضرار التقنية لتشمل الأمن القومي، الاقتصاد، الثقة المؤسسية، واستقرار المجتمعات.
19. يسير الصراع السيبراني نحو طابع «الحرب الباردة الرقمية» بين معسكرات كبرى، وسط تصاعد في الاتهامات، وسباق التسلّح التكنولوجي.
20. تبرز الحاجة الملحّة إلى وضع إطار قانوني دولي ملزم لحوكمة الفضاء السيبراني، وتنظيم سلوك الدول، ومنع التصعيد الذي قد يتحوّل إلى مواجهة شاملة.

المبحث الثالث:

الصراع الإسرائيلي-الإيراني وتوظيف تقنيات الذكاء الاصطناعي[(26)]

يظهر التداخل المتزايد بين الذكاء الاصطناعي والصراعات النووية، كما يتجلى في الحالة الإسرائيلية - الإيرانية، كيف يمكن للتقنيات الذكية أن تعزز القدرات الهجومية والدفاعية في الفضاء السيبراني، مما قد يؤدي إلى تصعيد النزاعات، وتعقيد مسألة تحديد المسئوليات، وتوليد عواقب غير متوقعة. فهم هذه الجوانب المعقدة ضروري لتجاوز مخاوف الانتشار النووي، وإدراك المخاطر الجديدة الناتجة عن دمج التكنولوجيا المتقدمة بالصراعات الخطيرة.

(26) الحرب الإسرائيلية-الإيرانية..الذكاء الاصطناعي كبعد جديد في الصراع السيبراني النووي https://www.siyassa.org.eg/News/22

إلى جانب تعزيز الجهود الرامية إلى وضع أطر تنظيمية دولية تضمن الاستخدام الآمن والمسئول لهذه التكنولوجيا

تتطلب مراكز البيانات المستخدمة لتدريب نماذج الذكاء الاصطناعي كميات كبرى من الطاقة الكهربائية، ومع تزايد ضغط هذه النماذج على الطاقة الكهربائية المنتجة من الوقود الأحفوري، اضطرت الشركات العالمية إلى البحث عن بدائل لاستهلاك الطاقة لتدريب نماذج الذكاء الاصطناعي، فعلى سبيل المثال نموذج (GPT_3) الذي يحتوي على 175 مليار معلومة يستخدم 1287 ميجا واط في الساعة الواحدة، وهذا يعادل نحو 100 ضعف متوسط الطاقة التي تستخدمها أسرة أمريكية في عام كامل، وغير ذلك لا يمكن الاعتماد على الطاقة المتجددة لأن الشمس غير متوفرة على مدار اليوم، كما تتأثر الرياح بالتقلبات الجوية لذلك يصعب تخزين كمية كبيرة من الطاقة الكهربائية اللازمة لتشغيل نماذج الذكاء الاصطناعي، لذلك يتم استخدام الطاقة النووية لأنها تستطيع توليد كمية ضخمة من الطاقة الكهربائية في وقت اقصر نسبيا، مما يجعلها مثالية لتلبية احتياجات مراكز البيانات الضخمة. لذلك قامت العديد من الشركات العالمية، مثل جوجل وميكروسوفت وأمازون وميتا بالاعتماد على المفاعلات النووية الصغيرة لإنتاج الطاقة الكهربائية لتلبية احتياجات مراكز البيانات الخاصة بتدريب نماذج الذكاء الاصطناعي[(27)].

كما يساعد الذكاء الاصطناعي المفاعل النووي من خلال تقديم مجموعة من الأدوات والقدرات التي يمكن أن تحسن بشكل كبير من أداء المفاعلات النووية. يعمل الذكاء الاصطناعي على زيادة السلامة والأمان وذلك عن طريق المراقبة المستمرة لكميات هائلة من البيانات، وتحديد أي انحرافات طفيفة قد لا يلاحظها البشر، وأيضا يمكنه اكتشاف أي ارتفاع بسيط في درجات الحرارة في أحد أجزاء المفاعل أو أي اهتزاز غير عادي في المضخة وبالتالي يقوم بتنبيه المشغلين لإجراء الصيانة الفورية للمفاعل، كما يمكن أن يساعده في تحسين كفاءة التشغيل مما يؤدي إلى تحسين استخراج الطاقة الكهربائية وتحسين جداول الصيانة لتقليل فترات التوقف عن العمل المكلفة. يساعد الذكاء الاصطناعي في دعم اتخاذ القرار من خلال مساعدة الوكالة الدولية للطاقة الذرية في مراقبة المفاعلات النووية حول العالم والتحقق من التزام الدول بالمعاهدات، عن طريق البيانات المدخلة عن كل مفاعل مما يؤدي إلى الكشف عن أي أنشطة غير معلنة لذا، تقوم العلاقة التبادلية أساسًا على اعتبار الذكاء الاصطناعي أداة داعمة تسهم في تعزيز أداء المفاعل النووي ورفع مستوى سلامته. أما المفاعل النووي فيوفر الساحة المعقدة والتحديات والبيانات التي تدفع عجلة تطوير الذكاء الاصطناعي

(27) - Paper: "Energy and Policy Considerations for Deep Learning in NLP"
المؤلفون: Emma Strubell, Ananya Ganesh, Andrew McCallum
المجلة: https://aclanthology.org/P19-1355.pdf ACL 2019

يهدف تخصيب اليورانيوم إلى زيادة نسبة النظير القابل للانشطار، اليورانيوم-235، مقارنة باليورانيوم-238 الأكثر وفرة. وهذه العملية معقدة للغاية وتستخدم فيها تقنيات مختلفة، مثل الطرد المركزي بالغاز. لذلك يمكن للذكاء الاصطناعي أن يلعب دورا كبيرا في تحسين كفاءة عمليات التخصيب وخاصة أجهزة الطرد المركزي التي يستخدمها الذكاء الاصطناعي (مثل الشبكات العصبية) لربط كميات هائلة من البيانات التشغيلية من أجهزة الطرد كدرجة حرارة المولد والضغط وسرعة الدوران، وتدفق الغاز، من خلال تحليل الكميات الكبيرة من المعلومات المترابطة بين المفاعلات النووية، ويمكن للذكاء الاصطناعي أيضا محاكاة المفاعل النووي من خلال تحسين وتصميم أجهزة الطرد المركزي والتي تساعده في محاكاة سلوك غاز سادس فلوريد اليورانيوم (UF6) داخل الجهاز الطارد المركزي في ظروف مختلفة، مما يساعد المهندسين على تصميم أجهزة أكثر كفاءة وفعالية.ويمكن للذكاء الاصطناعي إدارة المواد النووية والنفايات من خلال تتبع مخزون إنتاج الوقود النووي. مما يزيد من إنتاج الطاقة وتقليل عمليات السرقة والعمليات غير المشروعة (التحول إلى سلاح نووي أو قنبلة نووية). بالإضافة إلى تتبع النفايات، وذلك من خلال تحليل تلك النفايات الناتجة عن عملية التخصيب لتحديد مكوناتها بدقة وفعالية أكبر

مع ذلك فإن استخدام الذكاء الاصطناعي في العمليات الحساسة للغاية مثل تخصيب اليورانيوم سوف يتجاوز مجرد كفاءة التشغيل التي تمس الأمن العالمي والاستقرار، فتلك المميزات السابقة سوف تزيد من الانتشار النووي ويمكن للذكاء الاصطناعي تقليل العوائق أمام الدول لامتلاك أسلحة نووية أو حتى القنابل النووية. وذلك سوف يزيد من مخاطر الانتشار النووي عن طريق تحسين الإعدادات وتقليل الأخطاء أو إطالة عمر المعدات، يؤدي ذلك إلى إنتاج كميات أكبر من اليورانيوم عالي التخصيب (HEU) في وقت أقل. هذا يجعل مسار الحصول على المواد الانشطارية أسهل وأقل تكلفة. ويمكن للذكاء الاصطناعي أن يحل المشكلات التقنية المعقدة أو يقلل من الحاجة إلى الخبرة البشرية الكبيرة في عمليات التخصيب الصعبة، مما يسهل على الدول الأقل خبرة تحقيق أهدافها النووية. يجب الأخذ في الاعتبار أن الاعتماد المتزايد على الذكاء الاصطناعي قد يؤدي إلي فقدان السيطرة البشرية عليه، كما يمكن للأخطاء في تصميم خوارزميات الذكاء الاصطناعي أو التحيزات في البيانات التي تدربت عليها أن تؤدي إلى قرارات خاطئة أو غير متوقعة في عمليات حرجة، قد لا يكتشفها المشغلون البشريون إلا بعد فوات الأوان، قد تكون بعض نماذج الذكاء الاصطناعي معقدة لدرجة يصعب على البشر فهم كيفية اتخاذها لقرارات معينة والتي تعود إلى مشكلة «الصندوق الأسود» في بيئة نووية -الصندوق الأسود في الذكاء الاصطناعي: يعني أن البشر يمكنهم رؤية المدخلات والمخرجات، ولكن من الصعب جدًا فهم المنطق الداخلي الدقيق

الـذي تسـتخدمه الخوارزميـة لاتخـاذ قراراتهـا- التـي تقلـل مـن قـدرة المشـغلين على التدخـل أو تصحيـح الأخطـاء إذا شـعروا بـأن النظـام يـسير في اتجـاه خاطـئ. على الرغـم مـن أن الـذكاء الاصطناعـي يمكنـه أن يسـاعد في تصنيـع السـلاح النـووي، إلا أنـه يمكنـه تحسين أنظمـة توجيـه الصواريـخ الباليسـتية القـادرة على حمـل رءوس نوويـة. وهـذا يشـمل أنظمـة الملاحـة، وتصحيـح المسـار، والقـدرة على التغلـب على الدفاعـات الجويـة للعـدو. ويمكنـه تصميـم مسـارات طيران معقـدة للصواريـخ لجعلهـا أقـل قابليـة للاعتراض، أو تطويـر قـدرات المنـاورة التـي تزيـد مـن فـرص وصولهـا إلى الهـدف

وتمثـل الحـرب بين إسرائيـل وإيـران التـي تـدور -في ظاهرهـا- حـول امـتلاك إيـران للبرنامـج النـووي، أحـد أخطـر التوتـرات الجيوسياسـية في العـالم. مـع التطـور السريـع للـذكاء الاصطناعـي، أصبحـت هـذه التقنيـة عـاملًا جديـدًا ومـهمًا في هـذا الصراع، حيـث تُسـتخدم مـن كلا الجانـبين لتعزيـز القـدرات الاسـتخباراتية والعسـكرية، مما يزيـد مـن تعقيـد المشـهد الأمنـي والمخاطـر المحتملـة تسـتخدم إسرائيـل الـذكاء الاصطناعـي كأداة حيويـة في استراتيجياتها لعرقلـة البرامج النووية الإيرانيـة، حيـث تعتمـد وكالات الاسـتخبارات الإسرائيليـة على الـذكاء الاصطناعـي لتحليـل كميـات هائلـة مـن البيانـات والمعلومـات الاسـتخباراتية المجمعـة مـن مصـادر مختلفـة مـن الأقمار الصناعيـة واعتراض الاتصـالات وتقاريـر العمليـات الاسـتخباراتية، لتحديـد مواقـع المنشـآت النوويـة الإيرانيـة، والمنشـآت العسـكرية، وكبـار المسـئولين والعـلماء المرتبـطين بالبرنامـج النـووي مـن خلال مسـاعدة الـذكاء الاصطناعـي في تمييـز الأنمـاط المختلفـة، وتخطيـط وتنسـيق عملياتها السرية داخـل إيـران والكشـف عـن الأنشـطة السرية، كما يسـاعد في تقييـم التهديـد الـذي يمثلـه كل هـدف، وتحديـد الأولويـات للعمليـات الهجوميـة أو التخريبيـة، وقـد تضمنـت هـذه العمليـات اسـتخدام طائـرات مـسيرة صـغيرة تهـدف إلى إربـاك الدفاعـات الإيرانيـة، وسـاعد الـذكاء الاصطناعـي في التحكـم في المفـاعلات النوويـة مـن خلال أنظمـة التعلـم الآلي لتصميـم أنظمـة التحكـم الصناعيـة (ICS) المسـتخدمة في المنشـآت النوويـة الإيرانيـة، والتـي كان الهـدف منهـا اكتشـاف نقـاط الضعـف غير المعروفـة في جهـاز الطـرد المركـزي في المفـاعلات النوويـة في أنظمـة الكشـف التقليديـة(Zero- day exploits)، مـن خلال الهجـوم على ثغـرات المفاعـل النـووي والتـي يمكـن اسـتغلالها، أشـهر مثـال على ذلـك هـو هجـوم ستوكسـنت (Stuxnet) في عـام 2010، هـذا الـفيروس الـذي اسـتهدف أجهـزة الطـرد المركـزي الإيرانيـة في منشـأة نطنـز لتخصيـب اليورانيـوم، مما تسـبب في أضرار ماديـة كـبيرة عـن طريـق التلاعـب بأنظمـة التحكـم الصناعيـة (SCADA). بالإضافـة إلى اسـتخدام الجيـش الإسرائـيلي نمـاذج الـذكاء الاصطناعـي لتحديـد الأهـداف العسـكرية بدقـة، بمـا في ذلـك أنظمـة الصواريـخ الإيرانيـة وهـذا يمنـح إسرائيـل القـدرة على شـن ضربـات جويـة

فعالـة[(28)].

بيـنما إيـران تسـتخدم الـذكاء الاصطناعـي في سـياق برنامجهـا النـووي حيـث إنهـا تسـتمر في تطويـر نمـاذج مـن الـذكاء الاصطناعـي لتعزيـز قدراتهـا العسـكرية والدفـاع عـن برنامجهـا النـووي وذلـك مـن خلال تطويـر القـدرات النوويـة على تخصيـب اليورانيـوم، على الرغـم مـن عـدم وجـود تأكيـد معلـن مـن جانـب إيـران على زيـادة نسـبة تخصيـب اليورانيـوم، إلا أن هنـاك بعـض التقاريـر مـن الوكالـة الدوليـة للطاقـة الذريـة تصرح بـأن عنـد فحصهـا عـن كثـب للبرنامـج النـووي الإيـراني وجـدت مسـتويات أعلى بكـثير مـن المسـتويات المصرح بهـا بموجـب القانـون الـدولي لعـام 2015 فالمسـتويات المسـموح بهـا في تخصيـب اليورانيـوم تتراوح بين 3% إلى 5%، بينـما وصلـت مسـتويات التخصيـب في إيـران عـام 2021 بعـد انفجـار المولـد إلي 60% وهـذه المسـتويات مـن التخصيـب تسـتخدم لإنتـاج الأسـلحة النوويـة، وهـذا التزايـد السريـع في نسـب التخصيـب يجعـل هنـاك مخـاوف الوصـول السريـع إلى مسـتويات 90% لأن هـذه النسـبة سـوف تسـاعد إيـران في الحصـول على قنبلـة نوويـة في وقـت قـصير[(29)].

ختامًـا، فالعلاقـة المعقـدة والمتطـورة بين الـذكاء الاصطناعـي والمجـال النـووي، خاصـة في سـياق الصراع الإسرائـيلي - الإيـراني بـات واضحًـا، الـذكاء الاصطناعـي لم يعـد مجـرد أداة مسـاعدة، بـل أصبـح عـنصرًا فـاعلاً يُشـكل ملامـح هـذا التوتـر المحتـدم فالطريقـة التـي يمكـن أن يسـهم بهـا الـذكاء الاصطناعـي في تحـسين كفـاءة تخصيـب اليورانيـوم، قـد يقلـل مـن العوائـق أمـام الدول السـاعية لامـتلاك القـدرات النوويـة، بينـما يُمثـل في الوقـت ذاتـه أداة حاسـمة في المراقبـة وتحقيـق الالتـزام بالقانـون الـدولي، وتتـجلى خطـورة هـذه العلاقـة بشـكل أكبر في الحـرب السـيبرانية النوويـة، حيـث تُوظّـف التقنيـات الذكيـة في الهـجمات الدفاعيـة والهجوميـة على حـد سـواء، مما يُزيـد مـن تعقيـد وتحديـد المسـئولية وتفاقـم المخاطـر والتصعيـد غير المقصـود، وصـولا إلى احتماليـة وقـوع آثـار جانبيـة غير متوقعـة أو غير قابلـة للسـيطرة في بيئـة شـديدة الحساسـية كالمفـاعلات النوويـة إن التحديـات التـي يفرضهـا هـذا التقاطـع بين الـذكاء الاصطناعـي والبرامـج النوويـة هائلـة، وتدعـو إلى ضرورة حاسـمة لوضـع أطـر أخلاقيـة وقانونيـة دوليـة واضحـة، إلى جانـب تعزيـز التحكـم الـبشري والشـفافية في تصميـم وتطبيـق هـذه الأنظمـة. ففـي عـالم تتزايـد فيـه التوتـرات، وتتسـارع فيـه وتيرة التطـور التكنولوجـي، يظـل ضمان الاسـتخدام المسـئول للـذكاء الاصطناعـي في أخطـر المجـالات هـو مفتـاح الحفـاظ على الأمـن والاسـتقرار العالمي

قـدّر مصـادر أمنيـة رفيعـة المسـتوى في إسرائيل أن الحـرب السـيبرانية سـتزداد في السـنة المقبلـة في مـوازاة الصراع السـياسي الإسرائـيلي ضـد الاتفـاق النـووي، ومحـاولات إسرائيـل منـع التمركـز العسـكري لإيـران وحـزب اللـه في سـورية

(28) https://openai.com/research/ai-and-compute -

(29) https://www.jstor.org/stable/48662042?searchText=&searchUr

لقد تحولت الحرب السيبرانية إلى جزء لا يتجزأ مما يسمى في الجيش الإسرائيلي «المعركة بين الحروب». رئيس الحكومة قال مؤخراً إن «الهجمات السيبرانية الإيرانية هي أمر يومي»، وفي كانون الأول/ديسمبر الماضي تطرق رئيس الأركان أفيف كوخافي إلى موضوع الحرب السيبرانية الهجومية للجيش الإسرائيلي في جبهات متعددة، وهذه مسألة اختار الجيش حتى الآن عدم التطرق إليها بصورة علنية. وذكر رئيس الأركان بواسطة الناطق بلسان الجيش الإسرائيلي أن «مجال القتال الأهم الذي تغير هذه السنة هو المجال السيبراني – حيث نفذنا فيه عمليات هجومية كثيرة."

توصل المبحث إلى نتيجة عامة مفادها أن الذكاء الاصطناعي أصبح عنصرًا محوريًا في تعقيد التفاعل بين المجالين السيبراني والنووي، ويمثل أداة استراتيجية مزدوجة الاستخدام تُوظَّف في الصراع الإسرائيلي-الإيراني لتحقيق التفوق المعلوماتي والتقني، والتأثير في التوازنات الإقليمية. فقد أدى هذا التداخل إلى تغيير قواعد الاشتباك التقليدية، حيث تم توظيف الذكاء الاصطناعي في تطوير قدرات التخصيب، وتعزيز أمن المفاعلات، وتوجيه الهجمات السيبرانية، والتخطيط الاستراتيجي العسكري. وتشير الحالة الإسرائيلية-الإيرانية إلى أن الذكاء الاصطناعي قد تحول من مجرد أداة مساعدة إلى فاعل رئيسي في النزاع الجيوسياسي المعقّد، ما يهدد بتوسيع رقعة الصراع وتغيير طبيعة الردع والاستهداف في المنطق

نتائج البحث التفصيلية

1. العلاقة بين الذكاء الاصطناعي والمجال النووي باتت علاقة متبادلة ومعقدة، حيث يخدم كل منهما الآخر في التطوير وتعزيز الأداء.
2. يُستخدم الذكاء الاصطناعي لتعزيز السلامة والكفاءة التشغيلية في المفاعلات النووية، من خلال المراقبة الدقيقة وتحليل البيانات واستباق الأعطال.
3. الذكاء الاصطناعي يُمكّن أنظمة التحكم في المفاعلات من اكتشاف الانحرافات الطفيفة، مثل ارتفاع درجة الحرارة أو اهتزازات المضخات، وتنبيه المشغلين بشكل فوري.
4. تعتمد الوكالة الدولية للطاقة الذرية بشكل متزايد على الذكاء الاصطناعي في مراقبة الالتزام الدولي باستخدام البيانات المدخلة من المفاعلات حول العالم.
5. يتطلب تدريب نماذج الذكاء الاصطناعي كميات هائلة من الطاقة الكهربائية، مما دفع الشركات الكبرى للاعتماد على الطاقة النووية، خاصة من خلال المفاعلات النووية الصغيرة.
6. الذكاء الاصطناعي يحسن كفاءة عمليات تخصيب اليورانيوم، من خلال تحليل البيانات التشغيلية لأجهزة الطرد المركزي ومحاكاة سلوك غاز سادس فلوريد اليورانيوم.
7. يساعد الذكاء الاصطناعي في تصميم أجهزة طرد أكثر كفاءة، مما يسهم في رفع مستوى التخصيب وزيادة الإنتاجية.
8. يُستخدم الذكاء الاصطناعي لتتبع

المـواد النوويـة والنفايـات، مـا يسـهم في منـع التحويـل غـير المـشروع إلى الاسـتخدام العسـكري.

9. إدمـاج الـذكاء الاصطناعـي في عمليـات التخصيـب قـد يقلـل مـن الحاجـة إلى خـبرات بشريـة عاليـة، مـا يخفـض العوائـق التقنيـة أمـام الـدول السـاعية لامتـلاك قـدرات نوويـة.

10. يُسـهّل الـذكاء الاصطناعـي إنتـاج اليورانيـوم عـالي التخصيـب (HEU) بكميـات أكـبر وفي وقـت أقـصر، مـا يزيـد مـن مخاطـر الانتشـار النـووي.

11. هنـاك خطـر مـن أن تتحـول خوارزميـات الـذكاء الاصطناعـي إلى «صنـدوق أسـود»، مـما يجعـل مـن الصعـب عـلى البـشر تفسـير أو التدخـل في قراراتهـا داخـل بيئـات نوويـة عاليـة الحساسـية.

12. يمكـن للـذكاء الاصطناعـي تعزيـز قـدرات أنظمـة توجيـه الصواريـخ النوويـة، عـبر تطويـر أنظمـة الملاحـة، المناورة، والتغلـب عـلى الدفاعـات الجويـة.

13. في الحالـة الإسرائيليـة – الإيرانيـة، أصبـح الـذكاء الاصطناعـي عنـصرًا حاسـمًا في الـصراع السـيبراني-النووي، خاصـة في مهـام التجسـس، التنبـؤ، وتحديـد الأهـداف الاسـتراتيجية.

14. تسـتخدم إسرائيـل الـذكاء الاصطناعـي لتحليـل البيانـات الاسـتخباراتية الضخمـة وتحديـد مواقـع المنشـآت النوويـة والعسـكرية الإيرانيـة.

15. سـاهم الـذكاء الاصطناعـي في هجـمات إلكترونيـة اسـتهدفت المفاعـلات الإيرانيـة، أبرزهـا **هجـوم Stuxnet (2010)** الـذي عطّـل أجهـزة الطـرد المركـزي في منشـأة نطنـز.

16. تسـتخدم إيـران الـذكاء الاصطناعـي في تعزيـز قدراتهـا عـلى تخصيـب اليورانيـوم، وتحسـين تشـغيل المفاعـلات رغـم القيـود الدوليـة.

17. تقاريـر الوكالـة الدوليـة للطاقـة الذريـة تشـير إلى وصـول تخصيـب اليورانيـوم في إيـران إلى 60% عـام 2021، مـا يثـير مخـاوف مـن قـرب امتـلاك قنبلـة نوويـة.

18. الـذكاء الاصطناعـي يجعـل الهجـمات السـيبرانية النوويـة أكـثر تعقيـدًا، ويصعـب تحديـد مصدرهـا أو المسـؤولية عنهـا، مـما يرفـع احتـمالات التصعيـد غـير المقصـود.

19. توظيـف الـذكاء الاصطناعـي في المجـال النـووي يحمـل في طياتـه مخاطـر **فقـدان السـيطرة البشريـة**، ووقـوع **عواقـب غـير متوقعـة** في بيئـات حساسـة.

20. تتزايـد دعـوات الخـبراء والمؤسسـات الدوليـة إلى وضـع **أطـر قانونيـة وأخلاقيـة عالميـة** لتنظيـم اسـتخدام الـذكاء الاصطناعـي في المجـالات النوويـة والعسـكرية.

21. تُوظـف إسرائيـل الـذكاء الاصطناعـي كجـزء مـن «المعركـة بـين الحـروب»، وصرّح مسـؤولوها بـأن العمليـات السـيبرانية ضـد إيـران أصبحـت «يوميـة ومتعـددة الجبهـات".

22. يتجـه الـصراع بـين إسرائيـل وإيـران نحـو تصاعـد في الجبهـة السـيبرانية – النوويـة، مـما يهـدد الاسـتقرار الإقليمـي والـدولي، ويعكـس حجـم الخطـورة الناتجـة عـن هـذا التداخـل التكنولوجـي

المبحث الرابع:
تطور البنية السيبرانية الإسرائيلية والإيرانية (2010 – 2025))

تخوض إيران وإسرائيل حربًا سيبرانية متصاعدة في سياق الصراع القائم بينهما بشأن البرنامج النووي الإيراني. وقد شهدت الآونة الأخيرة تصاعدًا ملحوظًا في الهجمات السيبرانية المتبادلة، لاسيما على المنشآت الحيوية والحساسة في كلا البلدين

فقد أقدمت إيران على الانخراط بفاعلية في ساحة السجال السيبراني، مستفيدة مما تمتلكه من معرفة تقنية متقدمة في هذا المجال، وساعية إلى حماية منشآتها من الاختراقات السيبرانية، إضافة إلى استخدام هذه القدرات في تهديد خصومها على الصعيدين الداخلي والخارجي. في المقابل، تُعدّ إسرائيل دولة نووية، وقد مكّنها الدعم الأمريكي المستمر من امتلاك قدرات سيبرانية متقدمة، تُوظَّف في تقويض الطموحات الإيرانية في الفضاء الرقمي، وفي تعزيز الردع ضد أي تهديد سيبراني محتمل

يتناول هذا المحور مدى فعالية الحرب السيبرانية بين إيران وإسرائيل من خلال تحليل القدرات السيبرانية لكل دولة على حدة، واستعراض الهجمات السيبرانية المتبادلة، وبيان تأثير هذا الصراع على الأمن القومي لكلا البلدين. وذلك عبر ثلاثة مطالب رئيسية

أولا: الاستراتيجية السيبرانية الإسرائيلية:

أضحى المجال السيبراني ميدانًا جديدًا لتنافس الدول، ومحورًا رئيسيًا للاستثمار في مجالات تدرُّ فوائد اقتصادية ملموسة وتعزز من مداخيل ميزانيات الدول. كما تحوّل هذا المجال إلى سلاح فعّال، لا يقلّ أهمية عن الأسلحة التقليدية، وبات يشكّل تهديدًا حقيقيًا للأمن القومي للدول

وعلى الرغم من سعي إسرائيل للتميّز في هذا المجال عبر تطوير وتعزيز قدراتها السيبرانية، إلا أن ذلك لم يمنعها من التعرّض لهجمات سيبرانية متكررة من قِبل إيران. ورغم احتلال الشركات الإسرائيلية مراكز متقدمة عالميًا في صناعة التكنولوجيا السيبرانية، إلا أن القلق الإسرائيلي من تنامي القدرات السيبرانية الإيرانية لا يزال قائمًا

وتُعلن إسرائيل بين الحين والآخر عن تقدّمها التقني في المجال السيبراني، من خلال تطوير وحدات متخصصة في التجسّس المعلوماتي والرقمي الموجّه نحو أعدائها، واستخدام أجهزة آلية وإلكترونية لجمع المعلومات، إلى جانب برامج مُخصصة لأغراض الحرب الإلكترونية والهجمات السيبرانية الدفاعية والهجومية على حد سواء

سعت إسرائيل إلى توظيف الهجمات الإلكترونية كأداة استراتيجية لتعزيز مكانتها الدولية وترسيخ نفوذها في النظام العالمي الرقمي. ووفقًا لدراسة صادرة عن شركة الاستشارات الدولية «ماكينزي" (McK-insey & Company)، فإن اقتصاد الإنترنت في إسرائيل ينقسم إلى مجالين رئيسيين: الأول، وهو الأكبر، يتمثل في صناعة تقنيات المعلومات والاتصالات، ويتضمن إنتاج المعدات والبرمجيات وتطوير الحلول السيبرانية؛ أما الثاني، فيُعنى بالتجارة الإلكترونية، ويشكل نسبة أقل. وقد بلغت

المساهمة المباشرة لاقتصاد الإنترنت في الناتج القومي لإسرائيل نحو **50 مليار شيكل** في عام **2009**، ما يضعها في مصاف الدول الرائدة عالميًا في مجال الاقتصاد الرقمي. ويدل ذلك على الأهمية الكبرى التي توليها إسرائيل للفضاء السيبراني ضمن استراتيجيتها الأمنية الشاملة، بهدف كسر عزلتها الجغرافية في الشرق الأوسط، وتعزيز علاقاتها مع دول ومؤسسات دولية عبر أدوات القوة الناعمة والتكنولوجية.[30]

منذ مطلع الألفية، بدأ الكيان الصهيوني بإصدار سلسلة من القرارات والتدابير الاستراتيجية والسياسية لحماية فضائه السيبراني وتعزيز أمنه الرقمي. وتتمثل أبرز هذه الخطوات، وفق تسلسلها الزمني، في الآتي

1. **السلطة الرسمية لحماية المعلومات (2002):** تم إنشاء هذه السلطة ضمن جهاز المخابرات العامة، وكُلّفت بمهمة حماية الحواسيب الحيوية والهامة من التهديدات الإرهابية وعمليات التخريب والتجسّس، وذلك في إطار إدراك متزايد لأهمية البنية التحتية الرقمية في الأمن القومي.

2. **هيئة السايبر في الجيش الإسرائيلي (2009):** وهي هيئة تابعة لجهاز الاستخبارات العسكرية الإسرائيلية (أمان)، أُنشئت بهدف توجيه وتنسيق عمليات الجيش في الفضاء السيبراني، ودمج القدرات الدفاعية والهجومية ضمن الاستراتيجية العسكرية الشاملة.

3. **وحدة إدارة أنظمة المعلومات (2009):** تتبع مباشرة لوزارة المالية، وتُعنى بإدارة وتأمين جميع أنظمة الاتصالات الحكومية، بما يضمن حمايتها من الاختراقات ويُسهّل توحيد الإجراءات التقنية بين مؤسسات الدولة.

4. **هيئة السايبر الوطنية (2011):** أعلن رئيس الوزراء بنيامين نتنياهو عن إنشاء هذه الهيئة بهدف تعزيز الدفاعات السيبرانية للمنشآت الحيوية والبنية التحتية في مواجهة الهجمات التي قد تنفذها منظمات إرهابية أو دول معادية. كما أُنيط بها مسؤولية شراء المنظومات الدفاعية، سعيًا لاستحواذ إسرائيل على حصة من السوق السيبراني العالمي.

5. **السلطة الوطنية للدفاع في مجال السايبر (2016):** شُكّلت هذه السلطة لتتولى تنسيق الدفاع السيبراني الشامل، ورسم صورة استخبارية متكاملة حول التهديدات، إلى جانب الردع الفوري عند وقوع هجمات سيبرانية. وقد وُضعت هذه السلطة تحت إشراف مباشر من رئيس هيئة السايبر القومية، بهدف تحقيق تكامل مؤسسي في إدارة الأمن السيبراني للدولة.[31]

6. عملت إسرائيل، منذ الطفرة التقنية العالمية، على تحويل الكيان الصهيوني إلى مركز جذب عالمي للشركات

(30) ماكينزي آند كومباني. (2011). Innovation and Israel's High-Tech Economy. تقرير داخلي حول اقتصاد الإنترنت في إسرائيل. McKinsey Global Institute.
رقم المرجع في الهو

(31) المركز الفلسطيني للدراسات الإسرائيلية – مدار. (2017). الاستراتيجية الإسرائيلية في الفضاء السيبراني: الأمن والهيمنة.

الناشئة، لا سيما تلك المتخصصة في تكنولوجيا المعلومات والبرمجيات المتطورة، بما في ذلك برامج التجسس الإلكترونية. ويُقدّر عدد الشركات الإسرائيلية العاملة في مجال الأمن السيبراني الدفاعي والهجومي بنحو 500 شركة، يعمل فيها أكثر من 17 ألف خبير في تكنولوجيا المعلومات.

7. نجحت إسرائيل في تحويل نفسها إلى سوق ضخم لتصدير المنتجات السيبرانية، خصوصًا تلك ذات الطابع الاستخباراتي والتجسسي، وتبيعها بأسعار مرتفعة للأنظمة والدول تحت شعار «مكافحة الإرهاب». وتشكل هذه القدرة على العمل في ميدان الحرب السيبرانية أحد الركائز الرئيسية في حضور إسرائيل المهيمن على الساحة الدولية.[(32)]

القوات السيبرانية الإسرائيلية لحماية أمنها وهي:

1- الوحدة8200

تتكوّن الوحدة من مجموعة من المجندين والضباط يعملون ضمن مديرية الاستخبارات العسكرية (أمان - AMAN) التابعة لجيش الدفاع الإسرائيلي، وتضطلع بدور الخدمة المركزية في جمع المعلومات الاستخباراتية، لاسيما في المجالات السيبرانية واعتراض الإشارات وفك الشفرات

وتُعد هذه الوحدة العمود الفقري للحرب السيبرانية في إسرائيل، إذ لا تكاد تخلو أي عملية نوعية للموساد أو لأي جهاز استخبارات إسرائيلي آخر من مشاركة فاعلة لوحدة 8200، سواء في التخطيط أو الدعم الفني أو الاختراق المعلوماتي.[(33)]

2- **جهاز الأمن الدَّاخلي (شن-بيت):**

تُعرف هذه الوحدة بقدرتها على جذب أفضل العقول التكنولوجية في إسرائيل، كما اعتُبرت سادس أكبر وأخطر وحدة من حيث عدد الهجمات السيبرانية المنفذة على مستوى العالم. ويُقدّر عدد خبراء الحاسوب الشباب المنخرطين ضمن صفوف الجيش الإسرائيلي بحوالي 300 متخصص، يعملون بشكل مكثف في مجالات الدفاع والهجوم السيبراني، لا سيما على الشبكة العنكبوتية العالمية

3- **جهاز C4I :**

تولى هذا الجهاز مسؤولية تنسيق الاتصالات وتنظيم القدرات السيبرانية الإسرائيلية، وقد تم تعيين ضابط رفيع المستوى من جهاز الاستخبارات في مركز الشيفرة والأمن المعلوماتي، ليتولى مهمة جمع المعلومات المتعلقة بقدرات خصوم إسرائيل في مجال القرصنة الإلكترونية

يُشرف هذا الضابط على عمليات فك شفرات الاتصالات المنقولة عبر شبكات «الشاباك» (الشين بيت)، والموساد، والجيش الإسرائيلي، كما يشرف على فِرَق تقنية متخصصة تعمل داخل الجهاز ذاته، مهمتها فحص الشيفرات

رام الله: مدار – المركز الفلسطيني للدراسات الإسرائيلية. رقم الصفحة المحتمل: صـ 24–27

(32) المركز الفلسطيني للدراسات الإسرائيلية – مدار. (2017). الاستراتيجية الإسرائيلية في الفضاء السيبراني: الأمن والهيمنة. رام الله: مدار، صـ 29–30.

(33) منظمة التحرير الفلسطينية، الحرب العربية الإسرائيلية الرابعة، وقائع وتفاعلات، مركز الأبحاث، بيروت، 1974، ص 394.

والأنظمة الأمنية لضمان تحصين الفضاء السيبراني الإسرائيلي وتعزيز قدراته الدفاعية في البيئة الافتراضية.

4- وحدة " منمار" (مديرية منظومات المعلومات الحكومية):

تُناط بهذه الهيئة مسؤولية تركيز وتنسيق مجال الاتصالات الإلكترونية على مستوى الحكومة الإسرائيلية، حيث تتولى الإشراف المباشر على توجيه وحدات الاتصال الإلكتروني في مختلف الوزارات والمؤسسات الحكومية

كما تتحمل هذه الجهة المسؤولية الكاملة عن جميع مشاريع الحوسبة الحكومية، بما يشمل تصميمها، تنفيذها، وتأمينها، بما يضمن التكامل والتحديث المستمر للبنية الرقمية للدولة

5- وحدة إدارة المعلومات :

أجازت الحكومة الإسرائيلية إنشائها عام 2011 ، وهي تتولى مسئولية مباشرة عن جميع أنظمة الاتصالات الحكومية ، ومنها مشروع بنية الحكومة التحتية لعصر الإنترنت ، واستحدثت الدولة الإسرائيلية الفريق القومي المخصص للمجال الافتراضي ، حيث يقوم هذا الفريق بتحصين الشبكات المفصلية للدولة الإسرائيلية ضد القرصنة، وحماية القطاع الخاص في هذا المجال، ويتكون الفريق من 80 شخصاً يقومون بمهمات دفاعية ، وسيقوم الفريق بتخصيص موارد لتحسين البحث الجامعيً المتعلق بالدفاع عن المجال الافتراضي[34].

6- قبة حديدية رقمية

في عام 2009، أطلقت إسرائيل برنامجًا تحت اسم «القبة الحديدية الرقمية»، وهو مشروع تابع لمكتب الحرب الافتراضية الإسرائيلي، يهدف إلى تعزيز القدرات التكنولوجية والأمن السيبراني للدولة. يركز هذا البرنامج على تطوير منظومة دفاع إلكتروني متقدمة للتصدي للهجمات السيبرانية التي تستهدف البنية التحتية الإسرائيلية الحيوية، سواء من قبل دول معادية أو منظمات إرهابية

ومن المميزات الأساسية لهذا المشروع هي استقطاب الطلاب المتميزين الذين تتراوح أعمارهم بين 16 و18 عامًا، والذين يُكلفون بمهمة الاعتراض والمواجهة الفورية للهجمات الإلكترونية الموجهة ضد إسرائيل. من خلال هذا البرنامج، تم بناء جيل جديد من الكوادر الأمنية السيبرانية القادرة على التصدي للتحديات الرقمية المعقدة بسرعة وفعالية. ويعكس هذا البرنامج استراتيجية إسرائيلية شاملة في مجال الأمن السيبراني والهجمات المضادة الرقمية، حيث أصبحت إسرائيل من الدول الرائدة عالميًا في مجال الدفاع السيبراني، وقد ساهم هذا المشروع في بناء منظومة دفاعية إلكترونية قوية[35].

مشروع البنية التحتية الحكومية لعصر الإنترنت "تهيلاه " عام1997

الهدف من المشروع هو تزويد خدمات تصفح محمًية لوزارات الحكومة ومؤسساتها،

(34) إيران والخليج، عبدالله النفيسي، مجلة السياسة الدولية، (العدد ١٣٧، حزيران ١٩٩٩)، ص٦٣

(35) - مقال من مجلة Foreign Policy عن جهود إسرائيل في الأمن السيبراني وتدريب الشباب .https://foreignpolicy /com/2014/11/10/the-kids-who-fight-israels-cyber-wars

ويتم استخدام وسائل وتدابير خاصة لحماية أمن شبكة الإنترنت الحكومية، ابتداء من طاقم خبراء حماية المعلومات والاتصالات، وانتهاء بمنتجات وتقينات لشركات عالمية رائدة، كما تشمل مهمته متابعة ورصد الحوادث المتعلقة بحماية المعلومات على مستوى العالم، مع الاهتمام المتزايد لحدوث أي هجمات داخل الشبكة الإسرائيلية

7- وحدة الحرب الإلكترونية الإسرائيلية مع إيران:

استجابة للدواعي الأمنية وتصاعد وتيرة التوتر بين إيران وإسرائيل؛ قام الجيش الإسرائيلي بإنشاء هذه الوحدة في صفوفه؛ وذلك بهدف الاستعداد لحرب المعلومات والتكنولوجيا من الناحية الدفاعية، والهجومية، وتنفيذ بعض المهام التكنولوجية باختراق أجهزة الحاسوب في إسرائيل، حيث يشرف علي عمل هذه الوحدة،الوحدة8200، وتخضع مباشرة إلي قيادة رئيس الحكومة الإسرائيلية، وتختص باختراق منظومة الحواسيب الإلكترونية في المشروع النووي، وكذلك الجيش الإيراني، وضمان استمرارية الهجوم علي البنية التحتية المدنية في إيران، خاصة أنظمة الحاسوب العاملة في إيران بهدف شلها، ووقف عملها وتكبدها مخاسر مادية ومعنوية

8- صخور التجسس:

هي عبارة عن صخور صناعية تشبه تماما الصخور الطبيعية، حيث يتم وضع أدوات التصنت والمراقبة والاختراق والتصوير بداخلها، ومن ثم التحكم بها بشكل آلي، وآحيانا تكون صخور طبيعية بشكل كامل، وقامت إسرائيل باستخدام هذا الأسلوب في إيران بالقرب من محطة "فردو" والتي هي من أهم محطات تخصيب اليورانيوم في إيران

9- فرق قرصنة الكمبيوتر الإسرائيلية:

هي عبارة عن فرق مكونة من نخب من عناصر الجيش الإسرائيلي المتخصصين بالشأن المعلوماتي، ومخصصة لمواجهة الحرب الإلكترونية، وعمليات القرصنة المحسوبة ضد الساحة الإسرائيلية، حيث قامت قيادة أركان الجيش الإسرائيلي بتجميع ما يقارب عن 300 خبير تكنولوجي من عناصر الجيش الإسرائيلي، ووضعتهم ضمن فرق للقرصنة؛ وذلك لحماية الشركات الوطنية الإسرائيلية من خطر الاختراق الإلكتروني، إضافة إلي تعزيز قدرات قوات الجيش الإسرائيلي في مجال الحرب الإلكترونية، وتدريب عناصر جهازي الشباك والموساد علي فك رموز الشيفرات المعلوماتية

10- حزمة القرارات الاستراتيجية المعلوماتية الإسرائيلية:

قامت إسرائيل بالعديد من التدابير الاستراتيجية الحكومية السياسية والإلكترونية لحماية فضائها الإلكتروني، كان أهمها إطلاق المشروع المعروف بالبنية التحتية الإلكترونية لعصر الإنترنت عام 1977 والذي خصصته إسرائيل لوزارة المالية، وحددت أهدافها بحماية المعلومات في الوزرات الإسرائيلية بشكل عام

كما يتم إصدار إنذارات حماية المعلومات

للمنظمات العاملة في مجال تكنولوجيا المعلومات

ومن أشهر البرمجيات السيبرانية التجسّسية والهجوميّة[36] هي

- Flame (2007-2012) : استهدف المنشآت النفطية في إيران، والأراضي الفلسطينية، وكان الغرض منه توفير معلومات استخباراتية عن الهجوم الإلكتروني Stuxnet .
- Gauss 2011-2012)): وهي برامج ضارة تهدف إلى سرقة معلومات النظام، وبيانات الاعتماد البنكي.
- Miniflame (2012) : وهي مخصصة للتجسس الإلكتروني، تستهدف على الأقل 100جهاز في دول مختلفة مثل لبنان وإيران وقطر والأراضي الفلسطينية.
- Duqu 2.0 (2014-2015) : وهو عبارة عن برمجيات خبيثة متطورة للتجسس الإلكتروني استهدفت المنظمات والأماكن المرتبطة بمفاوضات الاتفاق النووي الإيراني.

ثانيًا: أبعاد القدرات السيبرانية الإسرائيلية:

تُعد إسرائيل من الدول الرائدة عالميًا في تطوير القدرات السيبرانية، حيث نجحت خلال العقدين الأخيرين في تحويل الفضاء السيبراني إلى مكوّن مركزي في عقيدتها الأمنية والعسكرية والاقتصادية. وقد ساهم الدعم الأمريكي المباشر، والتكامل بين الأذرع الأمنية والمدنية، والاستثمار الاستراتيجي في البحث والتطوير، في بناء منظومة سيبرانية متقدمة تتضمن وحدات استخباراتية متخصصة، وبنية تحتية رقمية محصّنة، وشركات تكنولوجيا أمنية تُعد من الأكثر تطورًا في العالم

تتجاوز القدرات السيبرانية الإسرائيلية حدود الدفاع الرقمي إلى تبنّي عقيدة هجومية مرنة تشمل الاستباق والتخريب الرقمي والتجسس والاستهداف الدقيق. وقد أصبحت هذه القدرات أداة حيوية في "المعركة بين الحروب" التي تنتهجها إسرائيل، بهدف إحباط التهديدات دون الانزلاق إلى مواجهات عسكرية شاملة. كما أسهمت هذه القدرات في تعزيز نفوذ إسرائيل الإقليمي والدولي، وتحقيق مكاسب استراتيجية من خلال التأثير على سلوك الخصوم، لا سيما إيران

يناقش هذا المحور الأبعاد المختلفة لهذه القدرات، من حيث: البنية المؤسساتية، والمرتكزات التقنية، والاستراتيجية العملياتية، والتوظيف السياسي والعسكري، وصولًا إلى تداعياتها على الأمن الإقليمي والدولي

1. البعد الأمني والمعلوماتي السيبراني:

يُشار إلى أن إسرائيل تمتلك، في منطقة النقب الغربي، واحدة من أكبر قواعد التنصّت التابعة للوحدة 8200 في جهاز الاستخبارات العسكرية الإسرائيلية. وتُعد هذه القاعدة من البنى التحتية الأساسية لأنشطة التجسّس السيبراني، إذ تقوم باعتراض المكالمات الهاتفية، والتسلل إلى عناوين البريد الإلكتروني للحكومات، والمنظمات الدولية، والشركات الأجنبية. وتغطي القاعدة نطاقًا جغرافيًا واسعًا يمتد عبر الشرق

(36) - السياسة الأمريكية وإيران، سيد حسن الموسوي، فصلية إيران والعرب، (عدد٥، ٢٠٠٢)، ص٤

الأوسط، وآسيا، وأفريقيا، ما يجعلها نقطة ارتكاز استراتيجية في شبكة جمع المعلومات الاستخباراتية الإسرائيلية. وقد صرّح قائد الوحدة السابق يائير كوهين أن ما يقارب 90% من المعلومات الاستخباراتية الإسرائيلية يتم الحصول عليها عبر الوحدة 8200، مؤكدًا أنه لا توجد عملية استخباراتية كبرى لا تشارك فيها هذه الوحدة بشكل مباشر أو غير مباشر

0. البعد العسكري السيبراني:

قامت هيئة الأركان العامة في الجيش الإسرائيلي عام 2003، بتأسيس شعبة تحمل اسم "شعبة المعالجة عن بعد"، بهدف توفير استجابة فورية لحالات التعرض لهجمات سيبرانية معادية، وبهدف الربط بين نظم الحواسيب العسكرية بالجيش الإسرائيلي، كما أعلنت هذه الشعبة عن برنامج مستقبلي يحمل اسم " كود المستقبل"؛ وذلك بهدف تحسين مدي جاهزية الجيش الإسرائيلي للعمل غي كجال الفضاء السيبراني، كما قام الجيش الإسرائيلي بتأسيس غرفة "الحرب الرقمية" عام 2013، بهدف تمكين الجيش من العمل بشكل سلس في الفضاء الإلكتروني، ويعتبر الجيش الإسرائيلي هذه الغرفة مركز أعصاب الدولة في عمليات الحماية والاعتراض.

0. البعد الإستراتيجي السيبراني:

تدعي إسرائيل أن مجال الفضاء السيبراني يكشفها أمام مخاطر أساسية بارزة، ومن بينها مخاطر تعرض البنية الحيوية والمؤسسات الأمنية لاعتداءات تتعلق بأدائها لوظائفها، بالإضافة إلى إمكانية تضرر الاقتصاد، كما تزعم إسرائيل انها تقف أمام أعداء لديهم دوافع واضحة لمواجهتها في كافة المجالات الممكنة، وبالتالي تعمل إسرائيل على بلورة استراتيجية قوية لحماية الفضاء السيبراني، من شأنها أن تحقق الأهداف الاستراتيجية بالحد الأدنى من الموارد

تأسست سلطة الدفاع السيبراني القومي الإسرائيلي عام 2016، تحت مسؤولية رئاسة الحكومة مباشرة، ووظيفتها الرئيسية هي إدارة جميع الجهود الدفاعية والعملانية في الفضاء السيبراني وتشغيلها وتنفيذها، الأمر الذي يتيح الرد الدفاعي الكامل والدائم على الهجمات السيبرانية، بما في ذلك التعامل مع تهديدات الفضاء السيبراني والحوادث السيبرانية في وقت حقيقي، وصياغة تقدير للوضع الحالي

كما أن المقاربات التي تتخذها إسرائيل تندمج في المتطلبات الثلاثة الأصلية الخاصة بمفهوم إسرائيل التقليدي بشأن الأمن القومي

اولًا: الردع:

يمكن للقدرات السيبرانية المتقدمة أن تكون وسيلة فعالة لردع أعداء إسرائيل. وكان أحد الأمثلة لذلك عملية Stuxnet التي تنسب إلى الولايات المتحدة وإسرائيل، والتي تم فيها تعطيل أداء أجهزة الطرد المركزي الإيرانية

ثانيًا: الإنذار المبكر:

الاعتماد على التقنيات السيبرانية المتقدمة لجمع المعلومات الدقيقة بشأن نيات الخصم وخططه المستقبلية. وأن تمنع من الوصول إلى قواعد البيانات الخاصة بها

في الوقت نفسه. وهكذا، يمكن لأجهزة إسرائيل الأمنية أن تقدم للمؤسسة الدفاعية إنذارات فعالة بشأن نيات الخصم بغية اتخاذ التدابير الضرورية ضده في اللحظة الصحيحة

ثالثًا: الانتصار العملاني الحاسم:

يمكن للجيش الإسرائيلي، باستعمال أدواته السيبرانية المتقدمة، أن يكسب أفضلية في القتال تمكّنه من قلب الميزان لمصلحته. وعلى سبيل المثال، جرى تعطيل أجهزة الرادار السورية خلال الهجوم على المفاعل النووي السوري عام 2007، والذي نُسب على نطاق واسع إلى إسرائيل، وذلك بواسطة رمز معادٍ يبدو أنه كان يبث إشارات عادية، وهذا ما مكّن سلاح الجو الإسرائيلي من اختراق المجال الجوي السوري من دون أن يُكتشف، واستهداف المجمّع النووي وتدميره بالكامل، ومن احتمالات من الممكن ان تتلاشى الحرب التقليدية بفعل التقدم الهائل في التكنولوجيا العسكرية

ثانيا: القدرات السيبرانية الإيرانية (2010-2025)

في ظلّ المشهد المتطور للحرب السيبرانية العالمية، برزت إيران بسرعة كلاعبٍ قوي، مُظهرةً قدراتٍ هجومية سيبرانية متطورة تُشكّل تحديًا كبيرًا لخصومها. ويُعدّ نموّ الترسانة السيبرانية الإيرانية دليلًا على استثمارها الاستراتيجي في الحرب السيبرانية كأداةٍ للدفاع الوطني واستعراض القوة. وتتناول هذه المقالة هيكلَ عمليات الهجوم السيبراني الإيرانية واستراتيجيتها وتداعياتها.[37]

لقد عملت إيران على بناء قدرات الحرب الإلكترونية والاستطلاعية لتحييد القدرات التقنية العالمية لمنافسيها في المنطقة ولمعارضي النظام في الداخل والخارج، واستعمال تلك القدرات في التجسس والتخريب، وقد تبنت إيران استراتيجية من خلالها تقود مؤسسة الحرس الثوري وقوات الباسيج التابعة لها، مجاميع من الميليشيات والفصائل الرقمية التي اما انها تنتمي إليها بشكل مباشر او تدين لها بالولاء، ليشكلوا كيانا افتراضيا تأسس منذ عام 2005 م، واطلق عليه "جيش فضاء إيران الالكتروني" الذي يعد احد الاذرع الرقمية التي يستخدمها النظام؛ لشن هجمات إلكترونية على المعارضة ومناهضي النظام في العالم والدول التي تقف عائقا امام البرنامج النووي الإيراني.[38]

تزايد اهتمام إيران بتطوير قدراتها السيبرانية خلال العقد الاول من القرن الحادي والعشرين، حيث في عام 2005 م، فكر الحرس الثوري الإيراني في انشاء قياده سيبرانية إيرانية

ولكن كان هناك متغيران اساسيان لعبوا دورا هاما في تزايد الاهتمام بتطوير القدرات السيبرانية الإيرانية: -

اولهما: إدراك إيران بأن امريكا تستهدف تغيير النظام الإيراني ودعم المعارضة

(37) الحرب السيبرانية الإيرانية: الاستراتيجيات والدفاع العالمي ماثيو د. فيرانتي، عميل خاص سابق في جهاز الخدمة السرية الأمريكي https://citanex.com/resources/irans-cyber-offensive-

(38) https://citanex.com/resources/irans-cyber-offensive-capabilities-structure-strategy-countermeasures/?utm_source=chatgpt.com

الداخلية وتأكد هذا عقب اندلاع " الثورة الخضراء " في إيران عام 2009 م، وذلك عقب فوز الرئيس الاسبق احمدي نجاد بولاية رئاسية ثانية.[39]

مارس المشرّعون الإيرانيون ضغوطًا كبيرة على الإدارة القانونية في مجلس الشورى لتمرير «مشروع قانون حماية مستخدمي الفضاء السيبراني» بدءًا من عام 2021. وبموجب المادة 11، تملك السلطات والمؤسسات الحكومية إمكانية الوصول إلى المعلومات الخصوصية، عبر مراقبة مستخدمي شبكة الإنترنت، في حين تصنّف المادة 15 المستخدمين بناءً على توصيفهم الوظيفي، وتحدّد لهم مقدار الوصول إلى الإنترنت بناءً على مهاراتهم وعلاوة على ذلك، من شأن مشروع القانون تنظيم المعلومات الواردة على شبكة الإنترنت، ومنع الوصول إليها بحسب مستوى الإذن الصادر عن الحكومة بحسب كل مواطن. صحيحٌ أنه من المفترض أن يكون الوصول إلى الخدمات والمواقع العالمية الشهيرة مثل يوتيوب YouTube وتويتر غير ممكن، وبالنتيجة مقيّدًا بشدّة، إلا أنّ الشبكات الخصوصية الافتراضية كانت بمنزلة إجراء مضادّ فعّال ضد الحكومة الإيرانية

ليست شبكة المعلومات الوطنية الهيئة الحكومية الوحيدة في إيران التي تدعم المنافسة الاستراتيجية، وتساعد على التأثير الإقليمي في عملية المراقبة والرقابة على شبكة الإنترنت؛ للإبقاء على السيطرة الجيوسياسية، وتعزيز النزعة الإقليمية للفضاء السيبراني الإيراني من خلال الحرب الناعمة. وتتّخذ العديد من الهيئات الحكومية الأخرى تدابير فعّالة، بما في ذلك الشرطة السيبرانية الإيرانية، والمجلس الأعلى للفضاء السيبراني الإيراني، وقيادة الدفاع السيبراني الإيراني، والمنظمة الوطنية للدفاع السلبي الإيراني، والمركز الوطني للفضاء السيبراني الإيراني، وفيلق حرس الثورة الإسلامية (سپاه) ومنظمة الحرب الإلكترونية والدفاع السيبراني التابعة للحرس الثوري الإيراني، ومجلس الباسيج السيبراني، إضافة إلى تعيين مجموعات بالوكالة لشنّ عمليّات سيبرانية فعلى سبيل المثال، تراقب الشرطة السيبرانية الإيرانية، المعروفة بـ «فتا» (وهو المختصر باللغة الفارسية لمصطلح پليس فضای توليد وتبادل اطلاعات ايران، أو پليس فتا)، نشاطات الإيرانيين على الشبكة الإلكترونية؛ ما يؤدي إلى الملاحقة القضائية للمعارضين المزعومين الناشطين على الشبكة الإلكترونية، وإغلاق المواقع الإلكترونية التي تراها الشرطة الإلكترونية غير إسلامية ومبتذلة

أصدر المرشد الأعلى، آية الله علي خامنئي، أمرًا بإنشاء مركز بيروقراطي للشبكة الداخلية (إنترانت Intranet) الوطنية عُرف باسم شبكة المعلومات الوطنية National Information Network بهدف تطوير شبكة إنترانت إيرانية وطنية تنعم ببنية تحتية تقدّم خدمات للقطاعَين العام والخاص في عام 2006. وتمنع شبكة المعلومات الوطنية

(39) https://citanex.com/resources/irans-cyber-offensive-capabilities-structure-strategy-countermeasures/?utm_source=chatgpt.com

أساسًا الأجانب من الوصول إلى الفضاء السيبراني الإيراني، وذلك من خلال مفاتيح التحويل وأجهزة التوجيه ومراكز البيانات، وهي تحثّ في الوقت نفسه الجمهور الإيراني على استخدام المواقع الإلكترونية ومواقع التواصل الاجتماعي المحلية. ويحافظ برنامج شبكة المعلومات الوطنية التابع للحكومة الإيرانية، الذي بلغت تكلفته مليارات الدولارات، على سير عمل الإنترنت من خلال محرّكات البحث والبريد الإلكتروني ووسائل الإعلام، أو بالأحرى شبكة محلية لتصفية محتوى الإنترنت، والتضييق في الوقت نفسه على الحركة الدولية لمرور البيانات عبر شبكة الإنترنت، بخاصةٍ أثناء الاحتجاجات[40]

وفي الوقت الذي تستخدم فيه جمهورية إيران الإسلامية الفضاء السيبراني لممارسة الرقابة على مواطنيها ومراقبتهم، بما في ذلك الحرب الإلكترونية لإلحاق الضرر بنُظم المعلومات خارج البلاد، فإنها تسعى باستراتيجية القمع الإلكتروني للحرب الناعمة التي تتّبعها إلى الحدّ من تداول المعلومات عبر شبكة الإنترنت لمنع «نشر الأفكار والثقافة والتأثيرات الأجنبية باعتماد تكنولوجيا المعلومات والاتصالات» داخل البلاد

إن الحرب الناعمة هي استراتيجية لضبط المعلومات التي تحظر صراحةً على الأجانب، مثل الغرب والولايات المتحدة الأميركية تحديدًا، الوصول إلى المعلومات، وفي الوقت نفسه، منع انتشار المعلومات الصادرة عن الغرب بين المواطنين الإيرانيين. وإضافة إلى نشر المعلومات المضلّلة، تسعى استراتيجية الحكومة لضبط المعلومات الخاصة بالقوة الناعمة، لتقديم سردية الدولة من خلال حملتها الأيديولوجية المرتبطة ارتباطًا وثيقًا بإرثها الإمبريالي الفارسي وأساطيرها وتاريخها، أو بعبارة أخرى، السيطرة على الثقافة.

لقد برز إلى الواجهة أجندة إيران المحافظة والمتعلّقة بضبط المعلومات، في محاولتها الأخيرة لعزل البلاد عن الفضاء السيبراني من خلال «قانون حماية حقوق مستخدمي الفضاء السيبراني». وتحول العقوبات الأميركية دون وصول الإيرانيين إلى أدوات التكنولوجيا الرئيسة ومواقع إلكترونية أساسية مثل أمازونAmazon ، وغوغل Google، وآبل Apple، والألعاب الإلكترونية المتعدّدة اللاعبين على الإنترنت مثل لعبة World of Warcraft ؛ ما يؤدي فعليًّا إلى فصل الإيرانيين عن الفضاء السيبراني.

وما فاقم الأمور سوءًا، هو أنّ الإيرانيين يعيشون أصلًا استراتيجية الحرب الناعمة والقوة الناعمة التي أطلقتها الحكومة لعزلهم أكثر فأكثر عن الفضاء السيبراني العالمي. وتسهّل العقوبات الأميركية من جهتها عملية المراقبة والرقابة في إيران؛ إذ إنها تحجب عن المواطنين إمكانية الوصول إلى مختلف المنصّات والبرمجيات والأدوات على الإنترنت. ولا تزال حرية المواطنين الإيرانيين باستخدام الإنترنت مهدّدة بسبب الدعم المتزايد لـ «قانون حماية حقوق

(40) Loqman Salamatian et al., "The Geopolitics behind the Routes Data Travel: A Case Study of Iran," Journal of Cybersecurity, vol. 7, no. 1 (2021), p. 8, accessed on 23/5/2022, at: https://bit.ly/3Kby0DN

مستخدمي الفضاء السيبراني»، والذي من شأنه أن ينشئ شبكة إنترنت محلية حقيقية معزولة عن الفضاء السيبراني العالمي

ثانيهما: إدراك قادة إيران بأن الفضاء السيبراني أصبح أداه مهمة تستخدم من قبل الخصوم في استهداف وتعطيل البرنامج النووي الايراني، وتأكد هذا عقب هجوم " ستاكسنت "الشهير على منشأه نطنز النووية عام 2010م

أدّى هذان المتغيران إلى رسم وتحديد أهداف إيران من تطوير قدراتها السيبرانية، حيث تهدف من جانب صون استقرار نظامها السياسي واستخدام الفضاء للتجسس على المعارضين، ومن جانب آخر تستهدف استخدام الفضاء السيبراني لأغراض الهجوم والدفاع من أجل إدارة صراعاتها الدولية مع خصومها لاسيما امريكا والسعودية وإسرائيل.

؛ لتحقيق الهدفين السابقين تصاعد الانفاق الإيراني على تحسين قدراتها السيبرانية منذ عام 2011 بدرجه ملحوظة حيث أسست عام 2012 جهاز " هاكتفست " بهدف التجسس على المعارضة الإيرانية وفي ذات العام أسست المجلس الاعلى للفضاء السيبراني بهدف رسم الإستراتيجية السيبرانية الإيرانية في مجالي الدفاع والهجوم وفي عام 2013م أسست الانترنت الوطني والبريد الإلكتروني الوطني

وعندما ازدادت الهجمات السيبرانية التي تتعرض لها إيران ومنشآتها سواء مدنية كانت أم نووية، طوّرت إيران ما يعرف بـ " القلعة الرقمية " التي بدأت تشغيلها عام 2019م، وذلك بهدف صد أي هجوم سيبراني يهدف لإنكار وقطع الخدمات واهتمت إيران في مجال تطوير قدراتها السيبرانية بالاعتماد على الذات مثلما فعلت إسرائيل، حيث انتشرت في إيران مؤسسات دراسية، ومراكز بحوث علمية متخصصة في مجالات تكنولوجيا المعلومات وبرمجة الحاسوب، وصد الهجمات الإلكترونية.

1- مكونات المنظومة السيبرانية الإيرانية:

تتمركز قدرات إيران الهجومية السيبرانية تحت مؤسستين أساسيتين: فيلق الحرس الثوري الإسلامي ("3 IRGC") ووزارة الاستخبارات والأمن الإيرانية 4 («MOIS") () باللغة الفارسية: وزارت اطّلات جمهورى اسلامى ايران). وداخل هذه الهيئات، تقوم وحدات متخصصة بإجراء عمليات إلكترونية تهدف إلى التجسس والتعطيل والتأثير

قيادة الدفاع السيبراني التابعة للحرس الثوري الإيراني، والمعروفة أيضًا باسم القيادة السيبرانية الإلكترونية للحرس الثوري الإيراني (IRGC-CEC") : تتخصص هذه الوحدة في العمليات السيبرانية الهجومية، بما في ذلك تخريب البنى التحتية الحيوية والتجسس. وتشتهر بمرونتها واستخدامها لأدوات سيبرانية متطورة. وقد صنفت الولايات المتحدة الحرس الثوري الإيراني منظمة إرهابية أجنبية عام ٢٠١٩.

وزارة الاستخبارات والأمن الإيرانية: بينما تُركّز الوزارة بشكل أساسي على جمع المعلومات

الاستخبارية، فإنها تُمارس أيضًا التجسس الإلكتروني لخدمة المصالح الوطنية الإيرانية. وتستهدف الحكومات الأجنبية والبنى التحتية الحيوية وجماعات المعارضة[41].

تتضمن منظومه القدرات السيبرانية الإيرانية قدرات بشرية مدربة في مجالات تقنية المعلومات والاختراق الإلكتروني، وفق تنظيم إداري يصل الى المستويات العليا من الدولة، للتنظيم والإشراف على الجهات المعنية بالحرب السيبرانية وذلك على النحو التالي: -

1. المجلس الأعلى للسايبر

تم تشكيله بقرار من المرشد الإيراني علي خامنئي وذلك في عام 2012م، ويضم في عضويته المسؤولين في الجهات الحكومية الرئيسية، برئاسة رئيس الجمهورية، ويتولى المجلس الإشراف على جميع الجهات التي لها علاقة بالسايبر ويحدد السياسات ومجالات العمل.

2. قيادة دفاع السايبر :

ومهمتها دفاعية، حيث تهدف إلى حماية المنشآت الوطنية ضد أي هجوم إلكتروني

3. الجيش الإلكتروني الإيراني

يهتم بالجانب الهجومي من السايبر ويتبع لقيادة الحرس الثوري/ القوات الإلكترونية، ويضم خبرات عالية في مجال تقنية المعلومات والهاكرز المحترفين (لمهاجمة وسائل الاعلام، ومصالح الدول الغربية والمعادية، والمعارضين، وجمع المعلومات)

4. دعم منتديات القرصنة المعلوماتية :

وتعمل الكثير من المجموعات الإلكترونية تحت مظلة النظام الإيراني، الذي ضم جميع القراصنة الموجودين في الفضاء الرقمي الإيراني، وجند آخرين من خارجها، وعمد إلى تشكيل كيانات رقمية لتحقيق غاياته السياسية في المنطقة، وذلك عن طريق ممارسة التهديدات والهجمات والتجسس الإلكتروني والاحتيال الرقمي لبسط نفوذه في المنطقة

5- الوحدات والتكتيكات التشغيلية الرئيسية

يتم تنفيذ العمليات الهجومية السيبرانية الإيرانية من قبل وحدات متخصصة، ولكل منها تركيزها وتكتيكاتها الفريدة[42].

1- يُشير مصطلح APT إلى مجموعة أو حملة تستخدم تقنيات اختراق متطورة للوصول غير المصرح به إلى نظام ما والبقاء فيه لفترات طويلة، وغالبًا ما تستهدف جهات محددة لأغراض التجسس أو سرقة البيانات. تتميز هذه الهجمات بسرّيتها واستمراريتها ومواردها الهائلة واستراتيجياتها المعقدة للتسلل إلى شبكات مستهدفة والحفاظ على الوصول إليها،

2- APT33 . وبرنامج Shamoon غالبًا ما يُربط اسم APT33 ببرنامج

(41) - الحرب السيبرانية الإيرانية: الاستراتيجيات والدفاع العالمي ماثيو د. فيرانتي، عميل خاص سابق في جهاز الخدمة السرية الأمريكي https://citanex.com/resources/irans-cyber-offensive-

(42) - الحرب السيبرانية الإيرانية: الاستراتيجيات والدفاع العالمي ماثيو د. فيرانتي، عميل خاص سابق في جهاز الخدمة السرية الأمريكي https://citanex.com/resources/irans-cyber-offensive-

Shamoon الخبيث، وهو أداة إلكترونية مدمرة تُستخدم في تنفيذ هجمات سيبرانية موجهة، تستهدف بشكل رئيسي مؤسسات قطاع الطاقة. يُعرف Shamoon بقدرته على محو البيانات من أجهزة الحاسوب المصابة، مما يجعلها غير قابلة للاستخدام تمامًا. ورغم أن APT33 تُجري عمليات متنوعة تشمل التجسس والتخريب الإلكتروني، فإن ارتباطها الوثيق بـ Shamoon يشير إلى تركيزها على ضرب البنية التحتية الحيوية وإحداث أضرار واسعة النطاق، بما يخدم أهدافًا استراتيجية أو انتقامية للنظام الإيراني

3- APT34 (OilRig) تُعرف APT34، التي تُطلق عليها أيضًا تسمية OilRig، بأنها واحدة من أبرز مجموعات التجسس السيبراني الإيرانية. وقد اشتهرت بهجماتها الإلكترونية المتقدمة التي تتركّز في منطقة الشرق الأوسط، مع تركيز خاص على القطاعات الحكومية وقطاعي الطاقة والاتصالات. وتعتمد المجموعة على مجموعة متنوعة من الأدوات والتقنيات، من أبرزها:

- رسائل البريد الإلكتروني التصيدية المستهدفة (Spear-phishing)
- استغلال تطبيقات الويب
- نشر برامج خبيثة مخصصة،

وتهدف هذه الهجمات إلى اختراق المؤسسات الحساسة، وسرقة البيانات، والحفاظ على موطئ قدم طويل الأمد داخل الأنظمة المخترقة.

4- APT35 القط الساحر – Charming Kitten تُعرف APT35، والتي تُلقب أيضًا بـ "القط الساحر" (Charming Kitten)، بأنها مجموعة سيبرانية إيرانية متخصصة في التصيد الاحتيالي والهندسة الاجتماعية. تستهدف هذه المجموعة أفرادًا وجهات ذات أهمية استراتيجية لإيران، بمن فيهم:

- المسؤولون الحكوميون
- الصحفيون
- النشطاء، خصوصًا أولئك المنخرطين في المعارضة السياسية الإيرانية، تُستخدم تقنيات متطورة لجمع المعلومات، منها رسائل البريد الاحتيالي الموجهة بعناية، وإنشاء صفحات وهمية، واستغلال الثقة الاجتماعية، بهدف سرقة بيانات حساسة أو اختراق حسابات وشبكات مستهدفة، وغالبًا ما ترعاها أو تديرها دول أو منظمات إجرامية كبيرة.
- إيران خصصت جزءًا كبيرًا من ميزانيتها من أجل تطوير قدراتها السيبرانية، حيث ارتفعت ميزانية الأمن السيبراني الإيراني خلال الاعوام من عام 2013 الى عام 2017 بنسبة 1200٪، وتحدث عن ذلك مدير أمن السايبر ونائب رئيس جامعة جورج واشنطن فرانك تشيلوبو في عام ٢٠١٧م، " أن إيران خصصت خلال السنوات الأخيرة الكثير من الأموال لبناء قدرات هجومية، ولمهاجمة الشبكات واختراق الحواسيب، واثناء حكم الرئيس حسن روحاني، تضاعفت ميزانية السايبر 12 مرة، وجعل إيران واحدة من القوى السيبرانية

الكبرى الخمسة، وكذلك دمجت إيران عمليات السايبر في استراتيجيتها وعقيدتها العسكرية.

***

توصل المبحث إلى نتيجة عامة مفادها أن الصراع السيبراني بين إيران وإسرائيل (2010–2025) أصبح ساحة مواجهة مركزية، تُستخدم فيها القدرات الرقمية كأداة للردع والهجوم، وأسهم في تشكيل توازن ردع سيبراني متبادل دون استبعاد خطر التصعيد المستقبلي.

ومن النتائج التفصيلية الآتي:

1- أقامت إسرائيل بنية تحتية سيبرانية متقدمة بدعم أمريكي مباشر، وتضمنت مؤسسات مثل وحدة 8200 وهيئة السايبر الوطنية، مع استراتيجية تركز على الردع والإنذار المبكر والانتصار العملياتي. وتوجّهت إسرائيل لتحويل الفضاء السيبراني إلى أداة قوة ناعمة واقتصادية، مكّنتها من تعزيز موقعها عالميًا.

2- طورت إسرائيل شبكة واسعة من الوحدات العسكرية والمدنية السيبرانية، من أبرزها: القبة الحديدية الرقمية، مشروع «تهيلاه»، جهاز C4I، ووحدات التجسس المتقدمة مثل صخور التجسس، وأنتجت برمجيات هجومية مثل Flame وDuqu و Gauss، مما أتاح لها تنفيذ عمليات معقدة ضد خصومها.

3- استثمرت إيران بشكل كبير في القدرات السيبرانية، ونجحت في بناء منظومة دفاعية وهجومية متكاملة بقيادة الحرس الثوري وفيلق الباسيج، من خلال تأسيس شبكة مؤسسات مثل المجلس الأعلى للفضاء السيبراني وقيادة الدفاع السيبراني، وتنفيذ عمليات إلكترونية ضد الخصوم الإقليميين والدوليين.

4- اعتمدت إيران على مجموعات APT المتخصصة مثل APT33 وAPT34 و APT35 (القط الساحر) في تنفيذ هجمات مستهدفة على منشآت الطاقة، والقطاعات الحكومية، والأفراد ذوي الأهمية، مما مكّنها من إخفاء مصدر الهجوم وتوسيع أثره الجغرافي.

5- أقرت إسرائيل وإيران سياسات وتشريعات خاصة بالفضاء السيبراني لتعزيز الأمن الرقمي، فأسست إسرائيل البنية التحتية لعصر الإنترنت وأطلقت تحذيرات استراتيجية للمؤسسات، في حين مررت إيران قانون «حماية مستخدمي الفضاء السيبراني» الذي منح الحكومة سلطة واسعة على الإنترنت المحلي.

6- كشفت الحرب السيبرانية بين البلدين عن تحوّل الفضاء الرقمي إلى جبهة حرب مستقلة وفعّالة، يمكن من خلالها إحداث خسائر ماديّة ومعنويّة دون الدخول في مواجهة عسكرية تقليدية، كما باتت جزءًا مركزيًا من العقيدة الأمنية والعسكرية لدى الطرفين.

7- أكدّت التجربة الإيرانية والإسرائيلية أن الأمن القومي لم يعد مقتصرًا

على الحدود المادية، بل أصبح مرتبطًا بالسيادة الرقمية والقدرة على حماية المعلومات، وتأمين البنية التحتية، والتحكم في الفضاء الافتراضي الوطني.

8- رغم التقدم الإسرائيلي التقني الواضح، أظهرت إيران قدرة على المبادرة والمباغتة في عدة هجمات سيبرانية، ما يعكس نوعًا من «توازن الرعب السيبراني» الذي يمنع أحد الطرفين من فرض تفوق حاسم أو مطلق في هذا المجال.

9- أصبحت الهجمات السيبرانية جزءًا من أدوات الضغط والردع في النزاعات الإقليمية والدبلوماسية، واستخدمها الطرفان كوسيلة للتأثير على المفاوضات بشأن البرنامج النووي، ولإرسال رسائل سياسية وأمنية دون التصعيد المباشر.

المبحث: الخامس
الهجمات السيبرانية الإسرائيلية والإيرانية (2010-2025)

الحرب بين إسرائيل وإيران ربما انتهت حاليا من الناحية العسكرية ولكنها بدأت سيبرانيا منذ الفترة الممتدة من عام 2010 حتى عام 2025 تصاعدًا ملحوظًا، وتبادل الطرفان الهجمات سيبرانية التي طالت قطاعات عسكرية وحكومية وخدمية، وقد كثرت أسماء الهجمات وتنوعت أغراضها ولكن هدفها واحد وهو التجسس وجمع المعلومات الاستخباراتية وأحيانا التخريب والاغتيال والتهديد

وتلك الهجمات السيبرانية بين إسرائيل شكلت واحدة من أبرز ساحات الصراع غير التقليدي في الشرق الأوسط، بل وفي النظام الدولي بأسره.

لقد انتقل الصراع بين الطرفين من نطاقه العسكري والأمني التقليدي إلى الفضاء الرقمي، حيث باتت الحروب السيبرانية أداة استراتيجية تستخدمها الدول لفرض الإرادة السياسية، وتحقيق أهداف استخباراتية، والتأثير على الخصم دون الحاجة إلى خوض مواجهات ميدانية مباشرة

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

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

مـن هـذا المنطلـق، يسـعى هـذا المحـور إلى تحليـل مسـار الهـجمات السـيبرانية المتبادلـة بين إيـران وإسرائيـل خلال الـفترة (2010–2025)، مـن حيـث تطورهـا الزمنـي، وأهدافهـا الاستراتيجية، ونتائجهـا العمليـة، ودلالاتهـا السياسـية، وذلـك لفهـم مـدى تـأثير هـذا الصراع الرقمـي على الأمـن الإقليمـي والاسـتقرار الاستراتيجـي في الشرق الأوسـط

أولا: الأهداف الاستراتيجية للطرفين

في سـياق التنافـس الإقليمـي والـدولي بين إسرائيـل وإيـران، لم تعـد الحـرب السـيبرانية مجـرّد أدوات تكميليـة ضمـن منظومـة الـردع، بـل غـدت وسـيلة مركزيـة تسـعى مـن خلالهـا كل دولـة إلى تحقيـق أهـداف استراتيجيـة محـددة، تُترجـم في الغالـب ضمـن رؤيتهـا للأمـن القومـي، وطبيعـة تموضعهـا في المعـادلات الإقليميـة والدوليـة. فقـد وظّفـت إسرائيـل قدراتهـا التكنولوجيـة المتقدمـة لتكريـس سياسـة «الضربـات الاسـتباقية» تجـاه البنـى التحتيـة الإيرانيـة، خاصـة مـا يتعلـق ببرنامجهـا النـووي وشـبكاتها اللوجسـتية، في حين وظّفـت إيـران الهـجمات السـيبرانية كأداة ردع غير متماثلـة لتعويـض ضعفهـا التقليـدي في مواجهـة التفـوق الإسرائـيلي

وتكشـف طبيعـة الأهـداف التـي اختارهـا كل طـرف عـن منطـق مغايـر في اسـتخدام الفضـاء السـيبراني: حيـث تميـل إسرائيـل إلى اسـتهداف المنشـآت ذات الطابـع الاستراتيجـي – الأمنـي والعسـكري – بهـدف تقويـض قـدرات إيـران وتعطيـل مشـاريعها بعيـدة المـدى، بينـما تميـل إيـران إلى اسـتهداف المنشـآت المدنيـة والمؤسسـات الخدميـة داخـل إسرائيـل، في محاولـة لزعزعـة الثقـة الشـعبية بالمنظومـة الحكوميـة، وإثبـات حضورهـا الإلـكتروني كمصـدر تهديـد فعّـال

وبالتـالي، فـإن تحليـل الأهـداف الاستراتيجيـة للطـرفين يُعـد مـدخلًا حـاسمًا لفهـم طبيعـة هـذا الصراع، وحـدود تـأثيره، وإمكانيـة تصعيـده أو احتوائـه في المسـتقبل

جدول رقم (1) يوضح الأهداف الاستراتيجية لطرفي الصراع

أطراف الصراع	إسرائيل	ايران
الأهداف الاستراتيجية	- شـلّ البنيـة التحتيـة الإيرانيـة النوويـة واللوجسـتية - جمـع المعلومـات الاسـتخباراتية - ردع القـدرات الإيرانيـة ومنـع تصعيدهـا الإقليمـي - الحفاظ على تفوقها التقني	- التـأثير على الداخـل الإسرائـيلي نفسـيًا وسياسـيً - إرباك المؤسسات الحيوية والمدنية - تقويـض ثقـة الجمهـور بالحكومـة الإسرائيليـة - خلـق أدوات ردع غير متماثلـة في مواجهـة التفـوق الإسرائيلي

ثانيا: الهجمات السيبرانية الإسرائيلية ضد إيران (2010–2025):

منـذ عـام 2010، أصبحـت الهـجمات السـيبرانية أحـد أبـرز أدوات إسرائيـل في تنفيـذ استراتيجيتهـا لاحتـواء المشروع النـووي الإيـراني وعرقلـة توسّـع نفـوذ طهـران الإقليمـي. وقـد مثّلـت هـذه الهـجمات جـزءًا مما يُعـرف بـ»حـرب الظـل» بين الجانـبين، وهـي حـرب غير تقليديـة، تـدور خارج

أطـر الصـدام العسـكري المبـاشر، وتُسـتخدم فيهـا أدوات رقميـة عاليـة الدقـة، وتُنفّـذ غالبًـا مـن خلال أجهـزة اسـتخبارات متخصصـة، في مقدمتهـا الموسـاد ووحـدة 8200 التابعـة للاسـتخبارات العسـكرية الإسرائيليـة

تميّـزت الهـجمات الإسرائيليـة على إيـران بطابعهـا الاسـتباقي والانتقـائي، إذ ركـزت على أهـداف نوعيـة وحساسـة تمـسّ البنيـة التحتيـة النوويـة والصناعيـة واللوجسـتية، كما طالـت منظومـات القيـادة والسـيطرة، والموانـئ، وحتـى وسـائل الإعلام الرسـمية. وقـد تراوحـت هـذه العمليـات مـا بين تـدمير مـادي مبـاشر (عبر فيروسـات مثـل «سـتاكس نـت») إلى شـلل تقنـي شـامل في شـبكات اتصـالات أو أنظمـة ملاحـة، إضافـة إلى عمليـات تجسـس رقميـة واختراق قواعـد بيانـات إستراتيجيـة

وعلى مـدار الـفترة (2010–2025)، تكشـف الهـجمات الإسرائيليـة ضـد إيـران عـن تطـوّر مسـتمر في الأدوات السـيبرانية المسـتخدمة، وتكاملهـا مـع العمـل الاسـتخباراتي التقليـدي والعمليـات الميدانيـة، في إطـار استراتيجيـة ردع مرنـة ومتصاعـدة تهـدف إلى إبقـاء إيـران تحـت الضغـط الدائـم، ومنعهـا مـن بلـوغ العتبـة النوويـة أو توسـيع قدراتهـا الهجوميـة في المنطقـة

وفي هـذا المحـور، سـيتم اسـتعراض أبـرز الهـجمات السـيبرانية الإسرائيليـة التـي اسـتهدفت إيـران، مرتبـة زمنيًـا، مـع توضيـح نـوع كل عمليـة، موقـع تنفيذهـا، والجهـة المنفـذة أو المسـؤولة عنهـا، مـا يوفّـر رؤيـة تحليليـة شـاملة لهـذا الجانـب الحاسـم مـن الصراع الإسرائيلي–الإيـراني في الفضـاء الرقمي

جـدول رقـم(2) يوضـح الـفترة الزمنيـة للعمليـات الإسرائيليـة داخـل إيـران وخارجـه (2010–2025)

الوصف	النوع	الموقع	العملية	التاريخ
فيروس سيبراني دمّر آلاف أجهزة الطرد المركزي لتخصيب اليورانيوم.	هجوم سيبراني/ تخريبي	نطنز، إيران	Stuxnet	2010
حجز سفينة تنقل أسلحة إيرانية لفصائل في غزة.	اعتراض عسكري/ مخابراتي	البحر الأحمر	حجز سفينة إيرانية	2014
اختراق شركة الاتصالات الرسمية للتجسس على مكالمات اللبنانيين.	هجوم سيبراني/ تجسس	لبنان	عملية أوجيرو	2017

الموساد استولى على وثائق نووية سرية عبر ٢٠ عميلًا داخل إيران.	تجسس ميداني/ اختراق	طهران، إيران	سرقة الأرشيف النووي الإيراني	٢٠١٨
تفجير أدى إلى دمار كبير في المنشأة النووية.	تخريب داخلي/ سيبراني	نطنز، إيران	تفجير أول في منشأة نطنز	٢٠٢٠
استخدام رشاش مثبت على شاحنة ويتحكم به عن بعد.	اغتيال ذكي عبر الذكاء الصناعي	طهران، إيران	اغتيال محسن فخري زاده	٢٠٢٠
عملية خفية عطلت أجهزة الطرد المركزي	تخريب داخلي/ سيبراني	نطنز، إيران	تفجير ثانٍ في نطنز	٢٠٢١
كشف أن مسؤول مكافحة الموساد كان عميلًا له.	اختراق استخباراتي	إيران	تصريحات أحمدي نجاد	2021
أكد أن الموساد تسلل إلى مفاصل الدولة الإيرانية.	تقدير استخباراتي	إيران	تصريحات علي يونسي	2022
استهداف مصنع ذخيرة.	هجوم مسير/ عمليات خاصة	أصفهان، إيران	هجوم بطائرات مسيرة على أصفهان	٢٠٢٣
استُهدف داخل دار ضيافة تابعة للحرس الثوري بعد حفل تنصيب الرئيس بزشكيان.	اغتيال سياسي خارجي	طهران، إيران	اغتيال إسماعيل هنية	٢٠٢٤
سبق عملية تصعيد كبرى؛ توقيت يثير الشكوك حول اختراق أمني.	حادث غامض/تحرك استخباراتي	إيران	حادث وفاة الرئيس إبراهيم رئيسي	٢٠٢٤
الأجهزة المستوردة تم تفخيخها مسبقًا وتحولت لعبوات ناسفة في توقيت واحد.	تفجير عبر أجهزة مخترقة	إيران + لبنان	تفجير أجهزة نداء لـ ٣٠٠٠ عنصر من حزب الله	٢٠٢٥
اغتيال سامي عبد الله، فؤاد شكر، نصر الله وآخرين بضربات دقيقة.	اغتيالات استخباراتية متسلسلة	لبنان	سلسلة اغتيالات لقيادات حزب الله	٢٠٢٥

هجوم جوي وصاروخي واسع استهدف منشآت نووية وقيادات عسكرية.	حرب سيبرانية + عسكرية	إيران	بدء الحرب الإسرائيلية–الإيرانية	٢٠٢٥
اغتيال٢٠ من كبار القادة العسكريين بصواريخ ومسيرات.	اغتيال ميداني بالتوازي مع القصف	إيران	اغتيال كبار القادة العسكريين	٢٠٢٥
سرقة بيانات ٤٢ مليون عميل (١٢ تيرابايت) وتسريبها لاحقًا.	هجوم سيبراني/ ابتزاز مالي	إيران	اختراق بنك "سباه" الإيراني	٢٠٢٥
تدمير ٩٠ مليون دولار من الأصول الرقمية ونقلها لمحافظ خارجية.	هجوم سيبراني مالي	إيران	اختراق بورصة Nobitex للعملات الرقمية	٢٠٢٥
شلل شبه تام للبنية الرقمية والاتصالات الداخلية والعسكرية.	شلل سيبراني/ هجوم شامل	إيران	انهيار الإنترنت بنسبة ٩٧%	٢٠٢٥
				المصدر: متابعات إخبارية: الباحث

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

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

التقييم العام والتوجهات المستقبلية

- يظهر من التحليل أن إسرائيل نجحت في تطوير تكامل عالٍ بين القدرات السيبرانية،

الاستخباراتية، والعسكرية الميدانية، مما جعلها قوة فاعلة في فرض قواعد الاشتباك في منطقة الشرق الأوسط

- العمليات اتسمت بالتدرج الزمني في التعقيد والجرأة، حيث انتقلت من عمليات تجسس واختراق إلكتروني إلى هجمات مسلحة معقدة واغتيالات ذكية
- استغلال التكنولوجيا الحديثة مثل الطائرات المسيرة، الذكاء الصناعي، والاختراقات السيبرانية المالية يعكس اتجاه إسرائيل نحو حرب هجينة شاملة متعددة الأبعاد.
- استمرار هذا النمط من العمليات يُنذر بتصعيد مستمر في المواجهة، ويطرح تحديات كبيرة لإيران وحلفائها، خصوصًا في مجال حماية البنية التحتية الحيوية والمعلوماتية.

2- الهجمات السيبرانية الإيرانية ضد إسرائيل (2010-2025)

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

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

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

وفي هذا السياق، سيتم عرض أبرز الهجمات السيبرانية الإيرانية ضد إسرائيل خلال الفترة (2010-2025)، مرتبة زمنيًا، مع تحليل نوع الهجوم، والجهة المنفذة، وطبيعة الأهداف، والنتائج المترتبة، لفهم أعمق للوظيفة السياسية والأمنية التي تؤديها الحرب السيبرانية في الاستراتيجية الإيرانية تجاه إسرائيل وامريكا[(43)]

جدول رقم(3) يعرض الهجمات السيبرانية

(43) - الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، أحمد بن علي الميموني، مجلة الدراسات الإيرانية، تصدر عن المعهد الدولي للدراسات الإيرانية، السنة الرابعة، العدد الثاني عشر، أكتوبر 2020، ص77.

الإيرانيــة ضــد إسرائيــل خلال الـفترة (2010–2025)

م	التاريخ	الدولة المستهدفة	الهدف	الجهة المنفذة	نوع الهجوم	أبرز النتائج
1	2011–2013	أمريكا	بنكًا 47 ومؤسسة مالية	قراصنة إيرانيون	DDoS	تعطيل وصول العملاء للحسابات، خسائر مادية
2	2013	أمريكا	سد مياه قرب نيويورك	خلايا إلكترونية إيرانية	اختراق نظام التحكم	فشل الهجوم بسبب فصل النظام للصيانة
3	2013–2017	أمريكا ودول أخرى	جامعات ومؤسسات علمية (١٧٦ جامعة)	مجموعة إيرانية	تسلل وسرقة بيانات	سرقة ٣١ تيرابايت من الوثائق
	أغسطس ٢٠١٢:		**هجوم أرامكو السعودية**	باسم ديست تراك ١٧،		هجوم فيروس شمعون
4	2014	إسرائيل	مواقع عسكرية ومدنية أثناء «الجرف الصامد”	غير محددة	اختراق وتشويش	اختراق حساب وزير الدفاع – ضرر محدود
5	2014	أمريكا	شركة Sands Las Vegas	قراصنة إيرانيون	تعطيل أنظمة	خسائر كبيرة وتعطيل الخدمات
6	أبريل ٢٠٢٠	إسرائيل	شبكة المياه	غير محددة (نسبت لإيران)	اختراق أنظمة تحكم	محاولة تسميم المياه – أضرار محدودة[44]
7	مايو ٢٠٢٠	إسرائيل	مراكز أبحاث كورونا	قراصنة إيرانيون	هجوم تخريبي	بدون سرقة بيانات – أضرار محدودة

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

تسريب آلاف الوثائق – طلب فدية مليون دولار	فدية وتسريب	Black Shadow	شركة "شيربيت" للتأمين	إسرائيل	ديسمبر ٢٠٢٠	8
شلل بمستشفى، سرقة بيانات، ١٠ مليون $ فدية	اختراق وتسريب وفدية	عصا موسى / بلاك شادو	شركات دفاع ومستشفيات	إسرائيل	2021	9
محاولة اختراق – تم إحباطها[45]	استغلال ثغرة Log4j	APT35 (Charming Kitten)	7 أهداف حكومية	إسرائيل	ديسمبر ٢٠٢١	10
خروج المواقع عن الخدمة – لا تسريبات مؤكدة	DDoS	غير محددة (نسبت لإيران)	مواقع حكومية (.gov.il)	إسرائيل	مارس 14 ٢٠٢٢	11
نشر صور سليماني، رسائل تهديد	اختراق دعائي	بلاك شادو أو جهات موالية	منصات إعلامية	إسرائيل	يناير ٢٠٢٣	12

المصدر:[(46)]

أولاً: التحول في الأهداف

1. من الأهداف الاستراتيجية إلى الأهداف الحيوية والمدنية:

- الهجمات في بداية العقد (2011–2014) ركزت على مؤسسات مالية أمريكية أو بنى تحتية محدودة.
- بدءًا من 2020، توسعت إيران لاستهداف منشآت حيوية مدنية (مثل شبكات المياه في إسرائيل، والمستشفيات، وشركات التأمين)، ما يعكس تصعيدًا في محاولة الضغط على السكان المدنيين وإرباك الدولة.

2. استهداف البيانات والمعلومات الحساسة بدلًا من التدمير المادي فقط: هجمات مثل تلك التي نفذتها مجموعتا «بلاك شادو» و«عصا موسى» ركزت على اختراق وسرقة وتسريب بيانات حساسة، ما يدل على تطور في طبيعة الحرب السيبرانية نحو «الحرب

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

(46) - الحرب السيبرانية الإيرانية: الاستراتيجيات والدفاع العالمي- ماثيو د. فيرانتي، عميل خاص سابق في جهاز الخدمة السرية الأمريكي https://citanex.com/resources/irans-cyber-offensive-

النفسية والمعلوماتية".

ثانيًا: تطور الوسائل والتكتيك

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

- يمثل الانتقال من هجمات تعطيل الخدمة إلى هجمات باستخدام ثغرات «يوم الصفر» مؤشرًا على احترافية متزايدة وتقنيات متقدمة

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

2. اللجوء المتزايد إلى هجمات الفدية (Ransomware):كما حدث في الهجوم على مستشفى «هيليل يافه»، ما يكشف عن تشابك الأهداف المالية والسياسية في عمليات إيران ووكلائها.

ثالثًا: النتائج والتأثيرات

1. فعالية محدودة من حيث التدمير المباشر، لكن عالية من حيث التأثير الرمزي والسياسي: معظم الهجمات لم تؤدِ إلى تدمير مادي كبير (باستثناء بعض التعطيلات المؤقتة)، لكنها نجحت في إثارة الذعر، وكشف ثغرات إسرائيلية وأمريكية.

2. نجاح تكتيكي لإيران في اختراق العمق المدني الإسرائيلي والأمريكي: استهداف منشآت طبية، وشبكات مياه، وشركات خاصة، يظهر قدرة إيران على اختراق شبكات محمية نسبيًا.

3. تصعيد في «الردع السيبراني المتبادل» بين إيران وإسرائيل: الهجوم على شبكة المياه الإسرائيلية (أبريل 2020) جاء بعد سلسلة هجمات منسوبة لإسرائيل على أهداف داخل إيران (مثل الموانئ والمنشآت النووية)، ما يدل على دخول الطرفين في حرب سيبرانية غير معلنة ولكن مستمرة.

4. ضعف واضح في جاهزية بعض القطاعات الإسرائيلية أمام الهجمات المعقدة: الهجوم على مستشفى «هيليل يافه» كشف عن هشاشة في البنية التحتية السيبرانية الصحية، وأدى إلى اعتراف رسمي بعدم الجاهزية التامة.

5. استخدام الهجمات كأداة دعائية واستعراضية: مثل اختراق «جيروزالم بوست» ونشر صور قاسم سليماني، ما يعكس استخدام الحرب السيبرانية كوسيلة رمزية للرد السياسي والمعنوي.

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

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

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

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

تـشير هـذه النتائـج إلى أن إيـران نجحـت في تثبيـت نفسـها كقـوة سـيبرانية هجوميـة مـن الدرجـة الثانيـة عالميًـا، قـادرة على إربـاك الخصـوم، وتهديـد البنيـة التحتيـة، والتـأثير على الـرأي العـام. وفي المقابـل، تواجـه إسرائيـل والولايـات المتحـدة تحديـات متزايـدة في تـأمين جبهاتـهما الداخليـة، وسـط تصاعـد نوعـي في الحـروب غير المتناظـرة

جـدول رقـم (4) يوضـح الإطـار التحلـيلي المقـارن للهـجمات السـيبرانية الإسرائيليـة والإيرانيـة (2010–2025)

محور المقارنة	إيران	إسرائيل
الطبيعة العامة للعمليات	هجومية انتقامية أو ردعية، تهدف إلى إرباك المؤسسات الإسرائيلية، وزعزعة الجبهة الداخلية، وتسجيل حضور سيبراني.	هجومية استباقية، دقيقة، تركز على إضعاف البنية التحتية الحساسة وعرقلة البرنامج النووي الإيراني.
الجهة المنفذة	مزيج من جهات حكومية (الحرس الثوري ووكلاء إلكترونيين (APT34)، بلاك شادو، عصا موسى	وحدات رسمية ضمن هيكل الدولة (الوحدة ٨٢٠٠ – الموساد السيبراني)
طبيعة الأهداف	شبكات المياه، المستشفيات، شركات التأمين، مواقع حكومية، مراكز بحث، أهداف مدنية.	منشآت نووية، موانئ، أنظمة طاقة، شبكات لوجستية، قواعد بيانات حساسة.
أدوات التنفيذ	برمجيات فدية، هجمات تعطيل الخدمة (DDoS)، تسريب البيانات، التصيد الإلكتروني، استغلال ثغرات عامة مثل Log4j.	برامج اختراق متقدمة، أدوات زراعة برمجيات تجسسية، استغلال ثغرات معروفة وغير معروفة (Zero-Day).
أهداف الهجوم	التأثير على الرأي العام الإسرائيلي، تعطيل الحياة اليومية، الضغط النفسي، الاستعراض الرمزي، أحيانًا الفدية المالية.	إضعاف القدرات النووية والعسكرية الإيرانية، خلق فوضى تنظيمية، جمع معلومات استخباراتية.
أثر الهجمات	أثر رمزي أو نفسي، وأحيانًا تعطيل جزئي (مثال: مستشفى هيليل يافه، تسريب بيانات شركة شيربيت).	أثر مباشر عالي التأثير (مثل تعطيل أجهزة الطرد المركزي في نطنز).

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

يُظهر هذا الإطار التحليلي أن الصراع السيبراني بين إسرائيل وإيران لم يعد مجرد مواجهات تكتيكية متفرقة، بل بات يُشكل ميدانًا استراتيجيًا موازٍ للمواجهات العسكرية والأمنية التقليدية فبينما تميل إسرائيل إلى تبني استراتيجية الضربات الاستباقية النوعية بدقة استخباراتية عالية، فإن إيران تستخدم الحرب السيبرانية كأداة ردع غير متماثلة لتعويض ضعفها التقليدي، مركّزة على الاستهداف الرمزي والضغط النفسي والمعلوماتي[47].

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

- فعالية نسبية للطرفين: نجحت إسرائيل في إحداث أضرار حقيقية في المنشآت الإيرانية (مثل نطنز وبندر رجائي)، بينما تمكنت إيران من اختراق مؤسسات إسرائيلية مدنية وتسريب معلومات حساسة.

- تحول الأهداف من عسكرية إلى مدنية: يدل على رغبة الطرفين في توسيع ساحة الصراع لتشمل المجتمع، بما يعزز «الردع الشعبي".

- تصاعد الهجمات الانتقامية : أصبحت الهجمات السيبرانية ردودًا مباشرة على عمليات ميدانية (مثل اغتيال سليماني أو استهداف علماء نوويين).

- توظيف الهجمات للفدية والإرباك الاقتصادي: كما حدث في الهجمات الإيرانية على مستشفيات وشركات تأمين إسرائيلية.

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

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

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

رابعًا: الدلالات السياسية والاستراتيجية

1. تآكل الخط الفاصل بين الحرب والسلام: فقد أصبحت الدول تستخدم الهجمات السيبرانية في أوقات «اللا حرب» لتحقيق مكاسب استراتيجية دون تكلفة دبلوماسية علنية.

2. الحرب السيبرانية كأداة ردع بديلة: خصوصًا لإيران، التي توظفها لتعويض ضعفها التقليدي أمام التفوق الإسرائيلي التقني والعسكري.

3. انعدام الإطار القانوني الدولي: ما يمنح الأطراف منفذًا للإنكار السياسي، ويصعّب تحميل المسؤوليات.

4. إعادة تعريف الأمن القومي: أصبح يشمل حماية نظم المعلومات والبيانات والمؤسسات الرقمية لا الجغرافيا فقط.

5. احتمالية التصعيد الخطر : في حال أفضت هجمات سيبرانية إلى أضرار بشرية أو بيئية جسيمة، قد يُستخدم ذلك كمبرر لرد عسكري، ما يعني تحول الصراع الرقمي إلى حرب شاملة.

خامسًا: مدى تأثير الصراع السيبراني على الأمن الإقليمي والاستقرار الاستراتيجي

• أدى الصراع السيبراني إلى توسيع رقعة الصراع بين إسرائيل وإيران إلى خارج حدود الدولتين، مع إدخال أطراف إقليمية ودولية ثالثة في دائرة التأثر والتورط.

• أحدثت الهجمات اضطرابًا في مفهوم الردع الإقليمي، حيث أصبحت الدول تعتمد على «الرد غير المباشر» عبر أدوات إلكترونية بدلًا من المواجهة العسكرية.

• خلقت هذه الحرب بيئة هشة للأمن المعلوماتي في المنطقة، حيث باتت أي أزمة سياسية مرشحة للتطور إلى هجمات إلكترونية واسعة، مما يهدد البنية التحتية الحيوية للدول.

• كما أنها تعمّق الانقسام في الشرق

الأوسط بين محورين تقنيين: محور متقدم (إسرائيل وداعموها الغربيون)، ومحور يسعى للحاق والاختراق (إيران وحلفاؤها)، مما يكرس عدم الاستقرار طويل الأمد.

***

نتائج المبحث:

توصّل المبحث إلى نتيجة عامة مفادها أن الفضاء السيبراني تحوّل خلال الفترة من 2010 إلى 2025 إلى ميدان صراع رئيسي بين إسرائيل وإيران، تجسّد في حرب هجينة استخدمت فيها الأدوات الرقمية كسلاح استراتيجي بديل عن المواجهة العسكرية التقليدية. فقد سخّرت إسرائيل تفوقها التكنولوجي لتعطيل المنشآت الحيوية الإيرانية، بينما اعتمدت إيران على الهجمات غير المتماثلة لاستهداف البنى التحتية المدنية الإسرائيلية. هذا التصعيد السيبراني أعاد رسم حدود الأمن القومي، وأدى إلى تفاقم التهديدات الإقليمية في ظل غياب أطر قانونية دولية ناظمة لهذا النوع من الحروب

النتائج التفصيلية:

1- أن الفترة من 2010 إلى 2025 تصاعدًا غير مسبوق في وتيرة الهجمات السيبرانية بين إسرائيل وإيران، مما جعل الفضاء الرقمي ساحة مركزية للصراع بينهما. ففي حين استخدمت إسرائيل قدراتها التكنولوجية لشن هجمات سيبرانية استباقية تستهدف البرنامج النووي الإيراني والمنشآت اللوجستية الحساسة، ركزت إيران على توظيف الفضاء السيبراني كأداة ردع غير متماثلة لتعويض تفوق إسرائيل التقليدي، واستهدفت به المؤسسات المدنية الإسرائيلية بهدف إرباك الجبهة الداخلية وزعزعة الثقة الشعبية.

2- تباينت أهداف الطرفين بوضوح، حيث سعت إسرائيل إلى تقويض القدرات النووية والعسكرية الإيرانية، بينما ركزت إيران على التأثير النفسي والإعلامي، واستهداف القطاعات المدنية والخدمية داخل إسرائيل. فالهجمات الإسرائيلية اتسمت بالدقة والسرية والتنفيذ النوعي، مثل استخدام «ستاكس نت» لتعطيل منشأة نطنز النووية، أو اغتيال قادة إيرانيين باستخدام الذكاء الصناعي. أما الهجمات الإيرانية، فقد شملت اختراق شبكات المياه والمستشفيات وشركات التأمين الإسرائيلية، باستخدام أدوات مثل برامج الفدية، وهجمات تعطيل الخدمة، والتصيد الإلكتروني.

3- التطور الزمني للهجمات يعكس انتقال الصراع من عمليات استكشاف واختراق محدودة إلى حرب هجينة متعددة الأبعاد، تشمل التجسس، والتخريب، والاغتيالات، والابتزاز المالي، ففي السنوات الأوّلى (2010–2014)، تميزت العمليات بالاستكشاف والهجمات التخريبية المحدودة. ثم تطورت في (2015–2021) إلى هجمات مركزة على البنية التحتية، بينما اتخذت في الفترة (2022–2025) طابعًا شاملاً، جمع بين الضربات السيبرانية، والاغتيالات الذكية، والهجمات الاقتصادية الرقمية.

4- أظهرت إسرائيل قدرة عالية

على دمج أدواتها السيبرانية مع عمل استخباراتي وميداني، مما مكنها من إحداث أضرار كبيرة داخل إيران وشل منظومات حيوية. في المقابل، نجحت إيران في تجاوز العزلة التقنية بإنشاء شبكة من المجموعات السيبرانية شبه الرسمية مثل «عصا موسى» و«بلاك شادو»، مما مكّنها من تنفيذ هجمات رمزية فعالة على أهداف مدنية إسرائيلية، معتمدة في كثير من الأحيان على هامش «الإنكار السياسي» الذي توفره هذه المجموعات.

5- أما على مستوى التأثير العملي، فقد أحرزت إسرائيل تفوقًا في تعطيل البنية التحتية الإيرانية، بما في ذلك شبكات الطاقة والموانئ والمنشآت النووية، كما أدت هجماتها إلى تقليص قدرات التنسيق الإيراني مع وكلائها في الإقليم، وعلى الجانب الآخر، أظهرت إيران قدرة متزايدة على استغلال الثغرات الأمنية داخل إسرائيل، حيث تمكنت من تنفيذ هجمات أربكت بعض القطاعات الحيوية، وكشفت عن هشاشة البنية الرقمية في مؤسسات الصحة والإعلام والتأمين.

6- سياسيًا واستراتيجيًا، أدى الصراع السيبراني إلى تآكل الفاصل بين الحرب والسلم، حيث أصبحت الهجمات الإلكترونية وسيلة لتحقيق مكاسب دون اللجوء إلى صدامات عسكرية تقليدية.

7- غاب الإطار القانوني الدولي المنظم لهذا النوع من الصراع، مما منح الطرفين مساحة للمناورة، والإنكار، وتصعيد الهجمات دون تبعات قانونية واضحة. وفي هذا السياق، برز الفضاء السيبراني كعنصر مركزي في إعادة تعريف الأمن القومي، الذي لم يعد يقتصر على الجغرافيا بل بات يشمل البيانات والشبكات الرقمية.

8- أثر هذا الصراع على الأمن الإقليمي كان بالغًا، إذ أدى إلى توسيع رقعة المواجهة لتشمل أطرافًا دولية (كالولايات المتحدة) وأخرى إقليمية (كسوريا ولبنان واليمن)، وخلق مناخًا من التهديد المستمر للمنشآت الحيوية المدنية في المنطقة. كما أسهم في تكريس انقسام تقني بين محور متقدم (إسرائيل وحلفاؤها الغربيون)، ومحور يسعى للاختراق (إيران وحلفاؤها)، وهو ما يهدد الاستقرار طويل الأمد في الشرق الأوسط.

النتائج العامة للدراسة

توصلت الدراسة – من خلال تحليل الإطار النظري وتطبيقاته على الحالة الإسرائيلية–الإيرانية – إلى جملة من النتائج العامة التي تعكس طبيعة التحول في بنية الصراعات الدولية في العصر الرقمي، وتبيّن كيف أعادت الحرب السيبرانية تشكيل مفاهيم القوة، والردع، والسيادة، وحدود الأمن القومي. وقد أمكن تلخيص أبرز النتائج العامة فيما يلي

1. **تشكل الحرب السيبرانية تحولًا بنيويًا في مفهوم الحروب والصراعات الحديثة**، إذ لم تعد المعارك تدور في الميادين التقليدية، بل انتقلت إلى فضاءات رقمية

غير متماثلة، تتيح لمجموعة صغيرة إحداث أثر كبير خارج القواعد الكلاسيكية للاشتباك.

2. **أصبحت القدرات السيبرانية مكونًا استراتيجيًا محوريًا في بناء القوة الوطنية**، جنبًا إلى جنب مع القدرات العسكرية التقليدية، ما يستدعي إعادة تعريف موازين الردع، واعتبار «الردع السيبراني» آلية فعّالة ضمن أدوات السياسة الخارجية والأمن القومي.

3. **يتّسم الصراع السيبراني بالغموض في الهوية والفاعلين والمسؤولية**، مما يجعل من الصعب تحميل جهة بعينها المسؤولية القانونية أو السياسية عن الهجمات، وهو ما يضعف قدرة المجتمع الدولي على الردع أو التنظيم.

4. **أدى تداخل الذكاء الاصطناعي مع الأنظمة النووية والسيبرانية إلى تعقيد بيئة التهديدات**، حيث باتت تقنيات الذكاء الاصطناعي أداة مزدوجة الاستخدام، قادرة على دعم السلامة التشغيلية، وفي الوقت ذاته تسريع وتيرة التسلّح أو الهجمات الخفية.

5. **مثّل الصراع السيبراني-النووي بين إسرائيل وإيران نموذجًا لحروب الجيل الخامس**، التي تجمع بين التجسس والتخريب والاغتيال والابتزاز والردع، وتُدار بأدوات تقنية عالية التجريد، مع قدرات مزدوجة التأثير (مدنية-عسكرية).

6. **تُظهر حالة إسرائيل وإيران تبلور نمط من «توازن الرعب السيبراني"**، حيث يتمتع كل طرف بقدرات كفيلة بإلحاق أضرار جسيمة بالآخر، دون الحاجة لخوض مواجهة عسكرية تقليدية مباشرة، مما يحوّل الفضاء السيبراني إلى أداة استراتيجية للتأثير المتبادل.

7. **يفتقر النظام الدولي إلى أطر قانونية وتنظيمية فاعلة لحوكمة الفضاء السيبراني**، الأمر الذي يسمح للدول والجهات الفاعلة من غير الدول بالمناورة خارج إطار المساءلة الدولية، ويعزز احتمالات التصعيد غير المقصود في بيئة شديدة الحساسية.

8. **أدى تصاعد الحرب السيبرانية إلى توسيع نطاق مفهوم الأمن القومي ليشمل الفضاء الرقمي والسيادة المعلوماتية**، وفرض على الدول تطوير استراتيجيات وطنية للأمن السيبراني تجمع بين الدفاع، والهجوم، والرصد المبكر، والشراكة مع القطاع الخاص.

9. **انعكس الصراع السيبراني بين إسرائيل وإيران على الأمن الإقليمي والدولي**، من خلال توسيع رقعة التهديدات لتشمل دولًا حليفة أو خصومًا إقليميين، مما أسهم في عسكرة الفضاء السيبراني، ورفع مستوى التوتر الجيوسياسي في الشرق الأوسط.

10. **تبرز الحاجة الملحّة إلى صياغة نظام قانوني وأخلاقي دولي ملزم ينظم الاستخدام العسكري والتقني للفضاء السيبراني والذكاء الاصطناعي**، وذلك للحد من الانفلات الرقمي، ومنع تحوّل النزاعات الرقمية إلى مواجهات عسكرية شاملة.

التوصيات

في ضوء النتائج التي توصلت إليها الدراسة، وفي ظل التهديدات المتصاعدة الناتجة عن الحرب السيبرانية وتداخلها مع الذكاء الاصطناعي والقدرات النووية، خاصة في السياق الإسرائيلي-الإيراني، توصي الدراسة بما يلي

أولًا: على المستوى الدولي

1. **إقرار اتفاقية دولية ملزمة لتنظيم الحروب السيبرانية**، تتضمن تعريفًا واضحًا للهجمات السيبرانية، وتحدد قواعد الاشتباك، ومبدأ المسؤولية، وآليات الرد المشروعة.
2. **إنشاء هيئة دولية متخصصة في أمن الفضاء السيبراني**، تتبع الأمم المتحدة، تتولى المراقبة، والتحقيق، وتقديم تقارير دورية عن التهديدات والانتهاكات.
3. **وضع معايير أخلاقية وقانونية لاستخدام الذكاء الاصطناعي في المجالات العسكرية والنووية**، بما يضمن الشفافية، والرقابة البشرية، ويمنع الاستخدامات غير المسؤولة أو المجهولة المصدر.

ثانيًا: على مستوى الدول النامية

4. **تعزيز بناء القدرات الدفاعية السيبرانية لدى الدول ذات البنية التحتية الضعيفة**، من خلال التدريب، ونقل التكنولوجيا، والتعاون مع المنظمات الدولية المختصة.
5. **تبني استراتيجيات وطنية للأمن السيبراني**، تشمل تشريعات واضحة، وآليات استجابة سريعة للهجمات، وتكامل بين القطاعات الحكومية والخاصة.
6. **دعم البحث العلمي في مجالات الأمن الرقمي والذكاء الاصطناعي**، وتوجيه التمويل نحو تطوير حلول محلية للتحديات الرقمية والتهديدات السيبرانية.

ثالثًا: على مستوى الإقليم (الشرق الأوسط)

7. **تفعيل التعاون الإقليمي في مجالات تبادل المعلومات الاستخباراتية السيبرانية**، وتنسيق إجراءات الحماية من الهجمات العابرة للحدود.
8. **إنشاء مراكز إقليمية مشتركة لرصد التهديدات السيبرانية والنووية**، وتطوير آليات للإنذار المبكر والاستجابة الجماعية.
9. **احتواء التصعيد السيبراني بين الخصوم الإقليميين** من خلال الحوار غير المباشر والوساطات التقنية، وتحديد «خطوط حمراء رقمية» تُمنع اختراقها.

رابعًا: على مستوى البحث الأكاديمي

10. **تشجيع الدراسات البينية التي تجمع بين القانون الدولي، والأمن السيبراني، والذكاء الاصطناعي، والاستراتيجية النووية**، لفهم الظاهرة بشكل متكامل.
11. **إنشاء قواعد بيانات أكاديمية توثّق الهجمات السيبرانية الكبرى**، وتُستخدم في تحليل الاتجاهات وصياغة السيناريوهات المستقبلية.
12. **تحفيز الحوار الأكاديمي والسياسي حول حوكمة الفضاء السيبراني**، من خلال المؤتمرات، والمنتديات، والمبادرات البحثية المشتركة.

المصادر والمراجع:

أولا: الكتب والمجلات العلمية

1- الاستراتيجية الإسرائيلية في الفضاء السيبراني: الأمن والهيمنة، المركز الفلسطيني للدراسات الإسرائيلية – مدار، رام الله: مدار، 2017، الاستراتيجية والتكتيك في فن علم الحرب، منير شفيق، بيروت: الدار العربية للعلوم ناشرون، ط1، 2008.

2- الأمن السيبراني: المفهوم وتحديات العصر، فارس محمد العمارات، عمان: دار الخليج للنشر والتوزيع، ط1، 2024.

3- إيران والخليج، عبد الله النفيسي، مجلة السياسة الدولية، العدد 137، حزيران 1999،

4- أيكلوجيا الارتقاء: الصين وتجليات المستقبل دراسة في الإمكانيات والتحديات، محمد كاظم المعيني، بيروت: دار السنهوري.

5- الحرب السيبرانية: المفاهيم والاتجاهات الاستراتيجية، شموئيل إيفن، ديفيد سيمان توف، معهد دراسات الأمن القومي، 2012.

6- الحرب السيبرانية: مواجهة العقيدة العسكرية استعدادًا للمعركة القادمة، إيهاب خليفة، القاهرة: مجلة السياسة الدولية، العدد 11، 2018.

7- الحرب السيبرانية من منظور القانون الدولي الإنساني، نسيب نجيب، المجلة النقدية للقانون والعلوم السياسية، جامعة تيزي وزو، المجلد 19، العدد 4، 2021>

8- الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، علي عبد الرحيم العبودي، بغداد: المجلة الأكاديمية العلمية، المجلد 57، 2019.

9- الحروب المتقدمة: الحروب التكنولوجية الباردة بين الدول العظمى نموذجاً، عمرو حسن فتوح، القاهرة: مجلة السياسة الدولية، 2022.

10- حروب الجيل الخامس: أساليب «التفجير من الداخل» على الساحة الدولية، شادي عبد الوهاب منصور، العربي للنشر والتوزيع، مصر، 2019.

11- الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، أحمد بن علي الميموني، مجلة الدراسات الإيرانية، العدد 12، أكتوبر 2020.

12- الخصخصة الأمريكية لحروب الجيل الخامس من وسائل التدخل والاستخبارات، علي زياد العلي، مركز دراسات كاتبغون، 27/7/2017. http://katehon.com

13- السياسة الأمريكية وإيران، فصيلة إيران والعرب، سيد حسن الموسوي، عدد 5، 2002.

14- السيبرانية وتحولات القوة في النظام الدولي، فراس شاكر، عمان: دار أمجد للنشر والتوزيع، 2022

15- الصراع والأمن الجيوسيبراني في السياسة الدولية: دراسة في استراتيجية الاشتباك الرقمي، علي زياد العلي، عمان: دار أمجد للنشر والتوزيع، ط1، 2019.

16- الفضاء السيبراني كساحة لإدارة التنافس الإيراني-الإسرائيلي حول النفوذ في الشرق الأوسط، أميرة صديق، مجلة قضايا آسيوية، المركز الديمقراطي العربي، العدد 9، يوليو 2021.

17- قاموس المورد عربي-إنكليزي، منير البعلبكي، بيروت: دار الملايين، 2004.

18- الموسوعة السياسية، المركز الديمقراطي العربي، 28/08/2019. http://political-encyclopedia.org/dectionar

19- الهجرات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، أحمد عبيس نعمه، مجلة المحقق المحلي، العدد 4، 2016.

20- منظمة التحرير الفلسطينية: الحرب العربية الإسرائيلية الرابعة، وقائع وتفاعلات، مركز الأبحاث، بيروت، 1974.

ثانيا: المواقع الاكترونية

1- الأبعاد العسكرية للقوة السيبرانية على

الأمن القومي للدول "دراسة حالة إسرائيل، نسرين الشحات، المركز الديمقراطي العربي، متاح على الرابط: https://www.democraticac.de/?p=30962

2- الحرب الإسرائيلية-الإيرانية.. الذكاء الاصطناعي كبعد جديد في الصراع السيبراني النووي، مجلة السياسة الدولية – الأهرام، https://www.si-yassa.org.eg/News/2

3- التهديدات السيبرانية والعلاقات الأمريكية الروسية، المركز الديمقراطي العربي، https://democraticac.de/?p=99583

4- تداعيات التأثير السيبراني على قدرات إيران في المواجهة مع إسرائيل، قناة القاهرة الإخبارية، https://alqaheranews.net/news/132

5- الردع السيبراني: المفهوم والإشكاليات والمتطلبات، د. رغدة البهي، المركز الديمقراطي العربي، 21 فبراير 2017.متاح على الرابط: https://www.democraticac.de/?p=43837

6- صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، المركز العربي للبحوث والدراسات، https://accronline.com/article_detail.aspx?id=32528

المراجع الأجنبية

1. Cyber Warfare: A "Nuclear Option"? Andrew F. Krepinevich, Center for Strategic and Budgetary Assessments (CSBA), USA, 2012.

2. Cyber-attack Targeted Israel's Water Supply, Internal Report Claims Ahiya Raved, *Ynet News*, 24 April 2020. https://bit.ly/324oLlU

3. Decoding the Biden Administration's Cyber Security Policy Vivek Mishra & Sameer Patil, *Observer Research Foundation (ORF)*, India. https://www.orfonline.org/research/decoding-the-biden-administration-s-cyber-security-policy

4. Innovation and Israel's High-Tech Economy McKinsey & Company, *McKinsey Global Institute*, 2011. تقرير داخلي حول اقتصاد الإنترنت في إسرائيل).

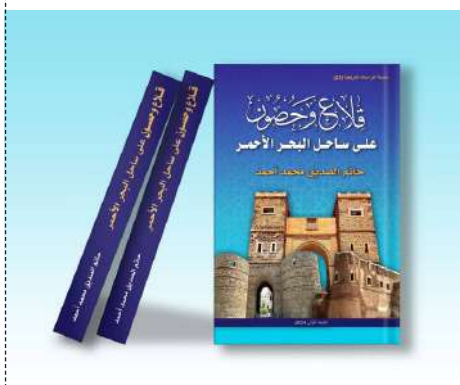
5. National Security Implications of Increasingly Autonomous Technologies: Defining Autonomy, and Military and Cyber-Related Implications Caitríona H. Heinl, *S. Rajaratnam School of International Studies*, 2015. http://www.jstor.org/stable/resrep05847

6. The Geopolitics behind the Routes Data Travel: A Case Study of Iran Loqman Salamatian et al., *Journal of Cybersecurity*, vol. 7, no. 1 (2021), p. 8. Accessed 23 May 2022. https://bit.ly/3Kby0DN

عرض كتاب «قلاع وحصون على ساحل البحر الأحمر» للمؤلف حاتم الصديق..

القلاع والحصون على ساحل البحر الأحمر: قراءة في معمار الذاكرة الدفاعية للمنطقة

تقديم/ رئيس التحرير



قلاع وحصون على ساحل البحر الأحمر، حاتم الصديق محمد أحمد، سلسلة الدراسات التاريخية(٣١)، دار آريثيريا للنشر والتوزيع، الخرطوم _ السودان، ط١، ٢٠٢٤م.

كتاب يشتمل على تسعة فصول في ٧٥٢ صفحة، بدأه المؤلف، بعد الآية القرآنية، بإهداء يكشف عمَّا يعيش فيه كثير من أبناء الأمة العربية من غربة واغتراب قسري، وأحلام في العيش بأوطان تسودها المحبة والعدل والأمن والاستقرار، يليه شكر وتقدير لكل من كان عونًا في تأليف هذا الكتاب، من أسرته، وأساتذة راجعوا مسودة الكتاب وآخرين وقدموا له، وأتت قائمة محتويات الكتاب بعده، ويليها تقديم الأستاذ الدكتور عز الدين عمر موسى، ثم تقديم الأستاذ الدكتور سمير محمد علي حسن الرديسي، اللذين أشارا في تقديمهما لهذا الكتاب إلى أهمية المنطقة ميدان الدراسة وما اختاره المؤلف من موضوع لم يُتطرَق له، وتقسيمه المنهجي الجغرافي لتناول ذلك الموضوع، وتزويده الدراسة بالصورة التي لا تقل أهمية عن الكلمة المكتوبة إن لم تفقها في بعض المواطن، فضلًا عمَّا عاد إليه من مصادر تاريخية عالية الموثوقية في دراسته، ويلي التقديمان مقدمة المؤلف لكتابه التي تكلم فيها بشكل عام عن بناء تلك القلاع والحصون على ساحل البحر الأحمر وتطورها عبر التاريخ وما تميزت به من نمط معماري وأهمتها

وجاء بعد تلك المقدمة فصول الكتاب التسعة، فجعل الفصل الأول تمهيدًا تكلم فيه بصورة عامة عن القلاع والحصون والبوابات والأسوار...، وعرف كل عنصر من تلك العناصر، وخصص الفصل الثاني لما جاء من تلك البنايات في الساحل اليمني وجنوب العرب، والفصل الثالث في الساحل السعودي، والفصل الرابع في الساحل الأردني والفلسطيني، والفصل الخامس في الساحل المصري، والفصل السادس في الساحل السوداني، والفصل السابع في الساحل الأريتري، والفصل الثامن في الساحل الصومالي، وأفرد الفصل التاسع لتناول المتشابهات المعمارية فيما تناوله في الفصول السابقة في تلك السواحل في شرق البحر الأحمر وغربه

ويمكن عرض محتوى تلك الفصول بصورة موجزة شاملة على النحو الآتي

الفصل الأول

القلاع والأبراج والحصون والبوابات

لقد عرف الإنسان القلاع والحصون والأبراج والبوابات منذ قديم الزمان؛ لحاجته لها إلى حماية نفسه وممتلكاته من أي هجوم محتمل، واستعمالها في أوجه الحياة المختلفة، وشهد ساحل البحر الأحمر عبر تاريخه الطويل إنشاء العديد من التحصينات الحربية بغرض حماية المدن الساحلية الاستراتيجية من هجمات الأعداء المتواصلة، ومن أنواع التحصينات الحربية

_ القلاع: وهي مباني شديدة التحصين، تشيد على جبل أو على أرض منبسطة أو تطل على البحر، ولها العديد من المهام الحربية والمدنية، وقد تم استخدامها لأغراض متعددة، فاستخدمت مساكن وسجون ومستودعات وبيوت للمال وإدارة المنطقة التي توجد القلعة ضمنها، ومخازن للذخيرة والمؤن والعتاد والجند، وقد ظهرت القلاع منذ العهد الآشوري في العراق، وتطورت في العصور الإسلامية، وضمت بعض القلاع في المشرق العربي مكان للمصارعة، وهي خاصية إضافية ظهرت في تلك القلاع التي يرجح أنها أخذت من الحضارة الرومانية

_ الحصن: يستخدم في توفير الحماية الضرورية للمدن في مراحل الحروب، وبتلك الخصوصية يتميز الحصن عن القلعة التي تستخدم لأغراض مدنية أو حربية

_ السور: هو بناء يرتفع من سطح الأرض يحيط بالمدينة كليًا، لاسيما تلك المدن التي تنشأ في الوديان والسهول والسواحل، ويكون طوله وارتفاعه مناسبًا للمدينة وحجمها؛ لكي يعمل على حمايتها، ويختلف حجمه وارتفاعه من مدينة إلى أخرى، بحسب قدرتها المالية وتوفر المادة الخام اللازمة لتشييد تلك المرافق الدفاعية، وقد شكلت أسوار المدن أهم الاستحكامات الحربية التي اهتم بها الحكام بغرض التحصين، وتم تدعيم أسوار القلاع في مستواها السفلي بسطح أملس مائل مغطى بأحجار ملساء لكي يصعب تسلقها، ويستفاد من هذه الدعامات في تمتين السور تحسبًا لأي انهيار محتمل

_ البوابات: جمع بوابة، وهي الفتحة القائمة في سور المدينة، وتغلق بمصراع أو مصراعين، وتُعدُّ الأبواب في أسوار المدن من

أهم الأشكال المعمارية بالمباني الحربية، ومن أضعفها حيث تكون من أوائل النقاط التي يتم استهدافها من العدو عند مهاجمته لأي مدينة محصنة ذات أبواب، وقد تم إنشاء هذه البوابات لتسهيل عملية دخول الناس وخروجهم، وهناك أبواب عادية وأبواب أخرى سرية يتم تصميمها للنجدة أو لخروج الحاكم وحاشيته عند الحاجة لها. وقد ابتكر الإنسان منذ فجر التاريخ القديم بناء الأسوار والبوابات؛ لتحصين المدن بغرض توفير الحماية لها ضد الهجمات التي تشن بغرض الاستيلاء عليها أو تدميرها، ومعظم البوابات في المدن التاريخية يتم فتحها عند أذان الفجر ويتم إغلاقها عقب صلاة العشاء مباشرة؛ حيث نجد هذا الأمر في بوابة جدة، وسواكن، ومدينة أم درمان، وهذا التشدد في عملية الإغلاق والفتح لهذه الأبواب وفي مواعيد محددة الغرض منها تأمين هذه المدن، وتسهيل عملية مراقبتها ليلًا، ولمنع أي نشاط يعرض المدينة وسكناها للخطر، وقد تم تعيين حراسة خاصة لهذه البوابات تقوم بمراقبتها والإشراف عليها، ومراقبة الداخلين والخارجين عبرها

_ الخنادق: جمع خندق، وهو أخدود يحفر بالأرض بحيث يكون محاطًا بالمدينة؛ ليمنع تجاوز الأعداء وغير المرغوب بهم في الوصول إلى المدينة، والعلاقة واضحة بين السور والخندق، فهما يحيطان بالمدينة أحدهما فوق الأرض والآخر محفورًا فيها، ولا ينشأ سور فوق خندق، ولا خندق تحت سور، لكن قد يجتمعان سور وخندق حول مدينة واحدة، فيوجد سور يليه خندق مثلًا، والأسوار والخنادق وسائل دفاعية استخدمها الإنسان لتحصين المدن، إلى جانب المصاطب الترابية والموانع الطبيعية

_ الأبراج: وهي عبارة عن بناء مرتفع في سور المدينة أو المباني العسكرية المحيطة بها مثل القلاع والحصون، ويكون بها عدد من الجنود بغرض المراقبة والحماية والدفاع، وتميزت الأبراج بارتفاعها عن السور ويتم تزويدها بعدد من الغرف الدفاعية العلوية لقذف النار وإطلاق السهام، ويمكن من خلالها صب السوائل الحارقة مثل الزيوت والشحوم وغيرها على المهاجمين، وقد تطورت عمارة الأبراج بصورة كبيرة عبر التاريخ، وقد حرص المسلمون على جعل محيط الأبراج الحائطية المدمجة في أسوار المباني الدفاعية من الأسفل أكبر من محيطها من الأعلى حيث تتناقص مساحة البرج كلما اتجه إلى أعلى، وذلك بغرض تدعيمها، واعتمد المسلمون على الأبراج في تدعيم المعمار الحربي، من خلال وضعها في أطراف البناء أو توزيعها على امتداد السور المحدد لحماية المدينة، بحيث تكون المسافة بين كل برج وآخر ما مقداره رمي سهم أي ٢٥ مترًا، وقد تعددت أشكال الأبراج في العمارة الإسلامية فنجد الأبراج المربعة الشكل والمستطيلة، التي ورثتها العمارة الإسلامية من الحضارة الرومانية والبيزنطية في العصور الوسطى ولتفادي العيوب والمشاكل في الأبراج المربعة والمستطيلة ابتكر المسلمون أنماطًا جديدة من الأبراج التي تسهل حركة المدافعين عن المدينة وتساعد على وضوح الرؤية لمسافات بعيدة وتغطية الزوايا المنفرجة

أسفل الأسوار؛ لذلك اعتمدوا على الأبراج المضلعة والأسطوانية الشكل وقد ظهرت الأبراج الأسطوانية في البلاد الإسلامية منذ الدولة الأموية والعباسية. والعمارة الحربية في أبراج المدن الساحلية على البحر الأحمر تتوزع بين المربع والدائري، فالأبراج المربعة توجد في قلعة باب الغفل في مدينة اللحية في اليمن، وقلعة صلاح الدين بجزيرة فرعون بجمهورية مصر العربية، وبوابات سواكن وطوابي مدينة محمد قول في السودان، وأما الأبراج الدائرية فتوجد في قلعة صيرة في مدينة عدن، وقلعة باب النخيل في مدينة الحديدة، وقلعة باب مشرف، وقلعة الفقيه في اليمن، وفي بوابة مدينة جدة القديمة والحديثة، والقلعة العثمانية القديمة في مدينة ينبع بالمملكة العربية السعودية

_ الممشى: هو المساحة المكشوفة بين أجزاء السور في المدن المحصنة، فهو جزء من السور وعرضه يتوقف على مدى اتساع عرض السور أو نقصانه، واتساع الممشى من الأعمال المحببة؛ لأنها تتيح فرصة تجميع القوات المدافعة في أسرع وقت ممكن، ويساعد في مراقبة المدينة من خلال تغطية المساحات المحصورة بين نقاط الدفاع الثابتة من السور خلال عمليات المراقبة. وقد أُطلِق على الممشى العديد من الأسماء مثل مطاف الحراس، وممر الحراس، ودرب السعة، ويتم الوصول إليه عبر سلالم مدرجة للراجلين أو منحدرة بغرض إيصال الأسلحة الثقيلة إلى أماكنها المحددة أعلى السور مثل المدافع. ومن الأجزاء المهمة في الممشى حائط الممشى الذي يعلو الأبراج والأبواب ويكون به عدد من الشرفات، وقد تفتح بها عدد من فتحات المراقبة ومهمة هذا الجدار حماية مستعملي الممشى خلال تنقلاتهم بين أجزاء السور أو كساتر يحتمون به عندما يتعرضون لهجوم

_ الشرفات: هي تلك المباني التي تزين أعلى المباني في الأسوار، وقد تم استخدامها من قبل المسلمين في المنشآت العسكرية والمدنية مثل: المساجد، والأضرحة، والقصور، والحمامات، والعيون، بأشكالها المختلفة، ومنها الشكل المسنن والمتدرج، أو على شكل ورقة ثلاثية البتلات، فتختلف أشكالها في العمارة الدفاعية، إلا أنها تقوم بوظيفة توفير مساحة لعمل المزاغل التي تمكن الجنود من رؤية أهدافهم ورميها بالسهام أو الأسلحة النارية، وفي الوقت نفسه توفر لهم الحماية من ضربات أعدائهم.

_ المزاغل: وهي عبارة عن فتحة للرماية على شكل مثلث مبتور الرأس ضيق من الخارج وعريض من الداخل لتسهيل حركة المدافعين عند تصويب أسلحتهم نحو العدو، وفي بعض الأحيان تكون الفتحة إلى الأسفل لمراقبة جوانب السور، وتصميم المزاغل بهذا الشكل يوفر عدد من الأشياء، مثل: إصابة الهدف بسهولة، وحماية المدافعين خلفه من المهاجمين، وتقليل تسرب مياه الأمطار إلى داخل المبنى. وتعرف المزاغل باسم (صوبت)، ويعتقد أنها من صوب السلاح، وقد استخدمت المزاغل منذ وقت مبكر في العمارة الإسلامية

_ الساقطة: وهي عبارة عن شرفة بارزة في أبواب المدن والبنيات الحربية، وقد

زودت أرضيتها بفتحات بغرض رمي الحجارة والسهام والمواد الحارقة كالزيت المغلي وغيره على المهاجمين، ويرجح سبب استخدامها لضعف يطرأ على النظام الدفاعي في قلاع وبوابات المدن

وقد ظهرت المدن المحصنة بصورة واضحة في أوروبا في العصور الوسطى مثل آبلة في إسبانيا، وقلعة (لاسيتي) في قرقشونة بفرنسا وغيرها من المناطق، وكانت هناك عدة مدن محصنة في البلاد العربية مثل: القدس، وبغداد، وسواكن، وجدة، وأم درمان، وغيرها من المدن التي عرفت التحصينات الدفاعية من أسوار وقلاع وحصون وبوابات واهتمت بها وأصبحت جزءًا من تاريخها ومعالمها الأثرية، وعندما بسط الصليبيون سيطرتهم على عدد من المدن في فلسطين والعراق وبلاد الشام ومصر عملوا على إنشاء عدة قلاع وحصون، بغرض حمايتهم من هجمات المسلمين التي كانت تهدف لاستعادة أراضيهم المسلوبة وطرد الوجود الصليبي منها، وقد نجح الصليبيون في وضع معظم المناطق التي سيطروا عليها تحت المراقبة المستمرة، وعملوا على إنشاء عدد من القلاع والحصون تحرس بعضها بعضًا من نهر الفرات شرقًا إلى ساحل حوض البحر الأحمر غربًا، وقد كانت هذه التحصينات بأنواعها المختلفة في مدن البحر الأحمر وحواضره تهدف إلى تحقيق عدد من المهام، منها: تأمين المدن من الهجمات، وحماية الحجاج، وفرض السلطة وهيبة الدولة، ومقر للجند والحكام والاجتماعات

الفصل الثاني
قلاع وحصون وبوابات الساحل اليمني

شهدت اليمن عمومًا وجنوب الجزيرة العربية خصوصًا ومدنها التي تطل على ساحل البحر الأحمر وخليج عدن منذ فجر التاريخ قيام العديد من الحضارات والممالك والسلطنات، التي تميزت ببناء العديد من القلاع والحصون والبوابات؛ لغرض حماية المدن من أي هجوم خارجي، وشهد القرن العاشر الهجري/ السادس عشر الميلادي اهتمامًا ملحوظًا بالقلاع والحصون الحربية، بسبب الأطماع الأجنبية في المنطقة والتدخلات الخارجية، وبمرور الوقت أصبحت تلك القلاع والحصون مصدرًا من مصادر الحكم فلم تقم دولة إلا وكان لها قلعة تتخذها مقرًا لحكمها وقاعدة لملكها، الأمر الذي أسهم في تنوع العمارة الدفاعية. وتميزت تلك العمارة بجمالها ونقوشها الفريدة وضخامتها الواضحة للعيان، ومن تلك المدن التي تميزت بوجود القلاع والحصون والبوابات فيها

_ مدينة عدن

تُعدُّ هذه المدينة من أهم المدن المطلة على البحر الأحمر وبوابته الجنوبية، وتتميز بموقعها الاستراتيجي ودورها التجاري والحضاري عبر العصور، وأمن الحرمين الشريفين وجدة وكل ساحل البحر الأحمر يرتبط بهذه المدينة الاستراتيجية، فمن يسيطر عليها يمكنه منع الملاحة في جنوب البحر الأحمر، وتعرضت مدينة عدن، عبر تاريخها الطويل، إلى العديد من الغزوات، فسعت القوات البرتغالية في العام ١٥١٣م

إلى السيطرة عليها؛ كي تسيطر على المدخل الجنوبي للبحر الأحمر وإغلاقه أمام السفن الإسلامية، لكن وجدت مشقة في ذلك لتحصين المدينة. ويمثل ميناء عدن أهم موانئ مدخل البحر الأحمر من جهته الجنوبية، وكان قبلة للسفن بمختلف أنواعها من موانئ البحر الأحمر والخليج العربي وشرق آسيا، وتحديدًا الهند

_ أبواب عدن

تميزت مدينة عدن بوجود عدد كبير من البوابات، أشهرها باب عدن أو عقبة عدن الذي يُعدُّ واحدًا من المنافذ البرية التي تربط مدينة عدن بمدينة المعلا من ناحية الغرب، ويقع باب عدن أسفل جبل(التعكر) ويسمى باب البر، وباب اليمن، وباب السقايين، والباب، وتشير بعض المصادر التاريخية إلى أن تاريخ بنائه يعود إلى شداد بن عاد الذي قام بثقب باب في الجبل، وبذلك أصبحت عدن سجنًا لكل من يغضب عليه

_ قلعة صيرة في عدن

تقع في الجزيرة التي تحمل اسمها، شرق مدينة (كريتر)، فوق جبل يبلغ ارتفاعه ٤٣٠ قدمًا فوق سطح البحر. بنيت في سنة ١١٧٣م من قبل الحاكم التركي في عهد الأمير عثمان الزنغابيلي التكريتي، وقد شكلت نقطة حماية مهمة للمدينة، وتم تصميمها للقيام بهذا الدور، ويوجد في جدرانها فتحات عديدة يتم استخدامها في حالة الهجوم على المدينة، وقد ساعدت عبر تاريخها الطويل في صد الكثير من الهجمات، ويوجد فيها مدخلان الأول بين البرجين ويقع في الجهة الغربية والآخر يوجد في الجهة الشمالية، ويتم الصعود إلى المدخل الرئيس عبر درجات دائرية الشكل تؤدي إلى فتحة باب مستطيل بطول ٤٧,٢ سم وعرض ٩٦,١ سم، كان يغلق عليها باب خشبي سميك، وهناك باب آخر بطول ٧٢,٢ سم وعرض ٩٦,١ سم، ويفتح على الصالة الرئيسة

_ قلعة تعز(القاهرة).

تقع قلعة تعز التي يطلق عليها اسم (القاهرة) _ ويطلق هذا الاسم(القاهرة) على عدة قلاع في أماكن مختلفة داخل اليمن _ على سفح جبل صبر فوق مرتفع صخري يطل على المدينة، وقد عُرِفَت بعدد من الأسماء، منها القلعة الحمراء، ودار الأدب، وحصن تعز، ويرجح أن تاريخها يعود إلى العصر الحميري، وتمت عملية إعادة بنائها في عصر الدولة الصليحية (٤٣٦-٥٣٢هـ/ ١٠٤٥-١١٣٨م) على يد السلطان عبدالله بن محمد الصليحي شقيق الملك علي بن محمد الصليحي مؤسس الدولة، وخلال الحكم العثماني في اليمن (٩٤٦-٩٦٢هـ / ١٥٣٩-١٥٥٥م) تم تجديد هذه القلعة، الأمر الذي أدَّى إلى تغيير معالمها القديمة، وأصبحت تتناسب مع المهام الدفاعية التي وضعها لها العثمانيون في ذلك الوقت، وتُعدُّ من أهم القلاع الدفاعية في المنطقة التي أسهمت في الدفاع عن المدينة في فترات تاريخية مختلفة، ونجحت في تأمين الطريق التجاري الواصل للبحر الأحمر. يحيط بالقلعة سور دائري يبلغ طوله ٣٥٥م تتوسطه أبراج مربعة الشكل، وللقلعة مدخلان المدخل الرئيس من الجهة الشمالية والمدخل الآخر

مـن الجهـة الجنوبيـة، وقـد تمـت إضافـة قصر في وسـطها بواسـطة الإمـام يحيـى وابنـه أحمـد في نهايـة الثلاثينـات وبدايـة الأربعينـات مـن القـرن الماضي، ويوجـد فيهـا سـت بـرك للميـاه كما ظلـت تقـوم بدورهـا حتـى نهايـة القـرن العشريـن حيـث تـم تحويلهـا إلى سـجن

مدينة المخا

تطـل على سـاحل البحـر الأحمـر، وهـي مـن المـدن اليمنيـة التاريخيـة والتجاريـة المهمـة، قبلـة التجـار مـن مختلـف بقـاع العـالم، ويطلـق عليهـا عاصمـة (البُن)، وتُعـدُّ حـاضرة القهـوة اليمنيـة التـي عرفـت في جميـع أنحـاء العـالم، ومينـاء المخـا أول مينـاء يصـدر البُن للعـالم، توجـد العديـد مـن قلاع المدينـة في جبـال الثوبـاني ومنطقـة يختـل ووادي الملـك بالإضافـة للشريـط السـاحلي، ومـن أشـهرها: قلعـة السـاحل، والطيـار، وقلعـة المـواصلات، وقلعـة الحـالي، وقلعـة العمـودي، وكلهـا بنيـت للدفـاع عـن المدينـة التـي تعرضـت لعـدة غـزوات عبر تاريخهـا الطويـل مـن قبـل الأحبـاش والبرتغاليين والعثمانيين والبريطانيين

مدينة الحديدة

تُعـدُّ مـن أهـم الموانـئ اليمنيـة، وقـد تميـزت بـكثرة الـقلاع والحصـون

بوابات مدينة الحديدة

تمـت إحاطـة المدينـة بسـور مـن كل الجهـات، ومـن الأبـواب التـي اشـتهرت فيهـا: بـاب النخـل، وبـاب مشرف، وبـاب السـاحل، وبـاب الفرحـة، وبـاب الـنصر

قلعة الكورنيش

أُنشـئت عـام ٩٤٦هـ/ ١٥٣٨م خلال الحكـم العـثماني، وبقيـت قائمـة لخمسـة قـرون. بُنيـت مـن الطـوب المحـروق وتضـم متحفًـا، وتتكـون مـن طابـقين على شـكل سـور مربـع تلتصـق بأركانـه أربـع بوابـات بـارزة

قلعة باب مشرف

أسسـها الشريـف حـسين آل خيرات، وقـام ببنـاء هـذا البـاب الشريـف حمـود آل خيرات الملقـب بـ (أبـو مـسمار) سـنة ١٢١٥هـ وقـد اهتمـت الدولـة العثمانيـة بترميـم سـور المدينـة والأبـواب التـي شـكلت معـالم المدينـة في ذلـك الوقـت

قلعة بيت الفقيه

تـم بنـاء هـذه القلعـة في العهـد العـثماني على يـد الـوالي مصطفـى باشـا، وتقـع على تـل مرتفـع على الجانـب الشرقـي مـن مدينـة بيـت الفقيـه، وتـم بناؤهـا مـن الأجـر وزينـت جدرانهـا وأسـطح سـقوفها بزخـارف بديعـة، وسُـقِفت غرفهـا بجـذوع الأشـجار، تـم تجديـد بنائهـا في العـام ١٣٤٩هـ، **وتضـم** مسـجدًا وبعـض الملحقـات وفنـاء داخلي

مدينة اللحية

تقـع شمال مدينـة الحديـدة على بعـد ١١٠ كلـم، تحيـط بهـا المياه مـن ثلاث جهـات، وتُعدُّ مـن الموانـئ والمـدن اليمنيـة الاستراتيجيـة، تـم تأسيسـها في القـرن السـابع الهجـري، وكان فيهـا العديـد مـن القصـور كـقصر عبدالـودود، وهـو مـا يـدل على ثرائهـا وغناهـا الكـبير، وضمـت العديـد مـن الـقلاع والحصـون الحربيـة ومـن أشـهرها قلعـة المسـيلة، والحمـراء، وقـد تعـرض معظـم هـذه الـقلاع للإهمال مما أدى إلى تهدمهـا بمـرور الوقـت، ويبلـغ عددهـا أكثر مـن ١٤ قلعـةً وحصنًـا، ومـن أهـم وأكبر هـذه الـقلاع قلعـة الزيلعـي

قلعة الزيلعي

تقـع على تـل مرتفـع يشرف على المدينـة

ويتحكم في مدخلها الرئيس من جهة البر، تتكون من طابقين على مساحة تقدر بـ ٣٠٠٠م²، حجراتها من الكلس البحري وجدرانها من الطوب المحروق، وتضم عددًا من المرافق مثل: صهريج للمياه مزود بنظام محكم لتجميع مياه الأمطار، ولها سراديب سرية تحت الأرض بطول ٥٠٠م تمتد إلى الشاطئ

قلاع جبل الملح:

تتكون من ثلاث قلاع تتوزع على جبل الملح الذي يبعد مسافة ١٥م عن مدينة اللحية، تم بناؤها في فترة الوجود العثماني الأول، وهي: قلعة الدريهمي، وتستخدم حاليًا مقرًا إداريًا للمديرية، وقلعة الطائف وعرفت باسم قلعة أحمد فتيني، وتتميز بضخامة مبانيها ومرافقها وقربها من الشاطئ، فضلًا عن ذلك فهناك قلاع أخرى، مثل قلعة قضبة، وقلعة الولاج، وقلعة الضحي، وهي من القلاع الأثرية تم تجديدها على يد الشريف الحسين بن حيدر الخيراتي، يصل ارتفاعها إلى ١٥م وأبعادها ٣٠×٦٠ تميزت أساساتها بالقوة والصلابة؛ لأنها بنيت من الحجر وجدرانها من الطوب، وقلعة المغلاف، وقام بتجديدها الشريف الحسين بن علي حيدر الخيراتي أمير المخلاف السليماني عام ١٢٥٤هـ وتتكون من طابقين على مساحة ١٥٠م²، وقلعة الفناوص كانت عبارة عن غرفة واحدة، أضاف إليها أمير المخلاف السليماني طابقين وقام شخص يدعى غالب المداني بترميم الجزء الشمالي منها في العام ١٩٧٠م تم استخدامها سجنًا في بعض الأوقات، وتعرضت هذه القلعة وغيرها من القلاع للإهمال

قلعة الضحى

تم بناؤها خلال العصر العثماني الأول ١٥٣٨-١٦٣٥م، وتم تجديد بنائها خلال العصر العثماني الثاني ١٩١٨-١٨٤٩م، مستطيلة الشكل تبلغ مساحتها ٣٠م × ٦٠م، ويرتفع سورها المبني من الطوب ١٥م، وتتميز بأساسها المتين الذي بني من الأحجار الصلبة، تم بناء أساسات السور حولها من أحجار البازلت الضخمة، وتم رفعها عن الأرض لبعض الأمتار قبل بناء الطوب (الياجور الأحمر) الذي تمت ليآسته من الخارج بطبقة سميكة من القضاض ملساء مدهونة بشحم الحيوانات وذلك لزيادة تحصيناتها الحربية للجزء الأسفل من الجدران، نوب الحراسة لها قواعد ضخمة، والسور مزود بزوائد بارزة للخارج تشبه المشربيات فيها فتحات إلى الأسفل ومن الجوانب وذلك ليتم استخدامها في رمي الحجارة الثقيلة والزيوت والسهام فوق رؤوس الأعداء الذين يرغبون في تسلق الجدار، وتُعدُّ من القلاع المميزة التي شيدت على أرض سهلية منبسطة وتعتمد على سورها بوصفه خط دفاع أول في حالة تعرضها لأي هجوم خارجي، وتطل على سوق الضحى، وهو سوق أسبوعي بالمدينة، ويطلق عليه اسم سوق الاثنين

قلعة القفل في اللحية:

تم تشييدها على الجبل الذي أخذت اسمه، وتطل على الميناء ومسجد الزيلعي، وهي مبنى مكون من طابقين، والأحجار التي تم البناء بها من شعب البحر التي تساعد على امتصاص الرطوبة، ويتكون السقف من الأخشاب التي تصنع منها السفن وذلك لقوتها، ويحيط بها سور، ويقع مدخل القلعة الرئيس في الجهة الجنوبية

الغربيـة باتجـاه السـاحل ويوجـد فيهـا أيضًـا بابـان آخـران، ويقـع جنوبهـا صهريـج لتخزيـن الميـاه وسرداب

قلعة كمران

تتكـون مـن عـدد مـن الغـرف تحيـط بهـا مجموعـة المتاريـس، ويوجـد بهـا مخـزن للـغلال وبئر للميـاه ونفـق طويـل للطـوارئ، وتُعـدُّ جزيـرة كمـران أو لؤلـؤة البحـر الأحمـر، كما أطلـق عليهـا حصـن ملـوك تهامـة، مـن أكبر وأهـم جـزر حـوض البحـر الأحمـر، تقـع بالقرب مـن ميناء الصليف، وتبلـغ مسـاحتها ١٠٧ كم^2، وتوجـد عـدد مـن الجـزر القريبـة منهـا تسـمى بأرخبيـل كمـران، وهـي كمـران الـكبرى، وكمران الصغـرى، وعقبـان الصـغير، والجريـد، وشـيب وفنجـان، وعقبـان، والبـوزي، وربشـة، والقطيـع. وقـد تعرضـت هـذه الجزيـرة للاحـتلال مـن قبـل الفـرس الذيـن بنـوا القلعـة في العـام ٦٢٠م، ثـم الرومـان، واحتلهـا البرتغاليـون في العـام ١٥١٣م، والمماليـك في العـام ١٥١٥م، وعاد البرتغاليـون إلى احتلالهـا في العـام ١٥١٧م وتـم تجديـد بنائهـا في هـذه المـدة، وتعرضـت بعـد ذلـك للاحـتلال البريطـاني

الفصل الثالث

قلاع وحصون وبوابات الساحل السعودي

لقـد اشـتمل هـذا السـاحل على عـدة قلاع وحصـون وبوابـات وأسـوار، تبنـى مـن الحجـر الجيري، والرملي، والصخـور البركانيـة، والجـص، وجـذوع الأشـجار، والنخيـل، ويصـل ارتفـاع أسـوارها مـن بين ٤ إلى ١٠م، وتكـون مسـتطيلة أو مربعـة الشـكل، ومعظـم الـقلاع احتـوت على ٤ أبـراج في الزوايـا، بعضهـا مسـتدير وبعضهـا نصـف أسـطواني، وتضـم مزاغيـل للمدافـع والبنـادق، وممـرات داخليـة، ومواقـع مرتفعـة تسـهل الرؤيـة والمراقبـة، لتحصين تلـك المواقـع والدفـاع عنهـا ومـا تشرف عليـه، وتكون وظائـف تلـك التحصينـات حمايـة المـدن، والحجـاج، وتـأمين السـاحل، وتـوفير ميـاه الشرب، وغالبًـا مـا تحـوي مسـجدًا وبئرًا وسـكنًا للحـكام والجنـود

مدينة جدة

عُرِفَـت جـدة بأنهـا عـروس البحـر الأحمـر والبوابـة التجاريـة للمملكـة، تميـزت عبر التاريـخ بسـورها الحـصين وبواباتهـا المتعـددة، تبلـغ مسـاحتها الإجماليـة ٧٤٨ كـم^2، ويُعـدُّ ميناؤهـا مـن أهـم موانـئ البحـر الأحمـر وأقدمهـا، وتعـود نشـأته إلى مـا يقـارب ٣٠٠٠ سـنة

سور المدينة وبواباتها

شُـيّد سـور جـدة بأمـر مـن السـلطان قنصـوه الغـوري سـنة ٩١٧هـ/ ١٥٠٩م، بطـول ٢,٥ كلـم وارتفـاع ٤م، محصـن بالـقلاع والأبـراج والمدافـع. أُزيـل في ١٣٦٦هـ/ ١٩٤٧م، واحتـوى على ٨ بوابـات، منهـا بـاب مكـة، وبـاب شريـف، وبـاب النافعـة، وبـاب المغاربـة، وغيرهـا، وتفتـح هـذه البوابـات مـع أذان الفجـر وتُغلَـق بعـد صلاة العشـاء

بوابة مكة

تُعـدُّ مـن أبـرز بوابـات مدينـة جدة، أُنشـئت عـام ١٥٠٩م، تحيـط بهـا أسـواق تاريخيـة مثـل سـوق البـدو وسـوق قابـل

بوابة بيت نصيف

بنـي بيـت نصيـف في عـام ١٨٧٢م، وتتميـز بوابتـه الحجريـة بالأقـواس القويـة والمتينـة

بوابة متحف بيت المتبولي

شُـيد عـام ١٠٢٢هـ ويتكـون مـن عـدة طوابـق ومدخـلين، وتتميـز بوابتـه الخشـبية بمتانتهـا

بوابة بيت سلوم

شُيد عام ١٣٠١هـ في حارة المظلوم، ببوابة بنية ذات نقوش خشبية تقليدية

قلعة الليث

كانـت تضـم أبراجًـا دائريـة مطلـة على البحـر، بُنيـت لحمايـة الميناء الـذي اسـتخدم منـذ العهـد الفرعـوني

مدينة ينبع

تنقسـم إلى قسـمين: ينبـع البحـر، وينبـع النخيـل. وسـميت بهـذا الاسـم لـكثرة الينابيـع فيهـا، وينبـع البحـر هـي الجـزء الـذي يقـع على سـاحل البحـر الأحمـر، وينبـع النخيـل يقـع إلى الداخـل وإلى الشرق قلـيلًا مـن ينبـع البحـر، وسـميت بينبـع النخيـل لـكثرة النخيـل فيهـا، وقديمًـا عندمـا يقـال ينبـع يقصـد بهـا ينبـع النخيـل لشـهرتها ووقوعهـا على طريـق الحـج والقوافـل التجاريـة بين الحجاز والشـام ومصر، أمـا الآن فيقصـد بهـا ينبـع البحـر أو الميناء. ولحمايـة المدينـة مـن أي هجـوم خارجـي أمـر السـلطان قنصـوه الغـوري في العـام ٩١٥هـ/ ١٥٠٩م ببنـاء سـور حـول ينبـع النخيـل وتـم تدعيمـه بعـدد مـن الـقلاع، وتوجـد في مدينـة ينبـع قلعـة داخليـة تُعـدُّ مـن أهـم المبـاني الدفاعيـة بالمدينـة، عُرِفَـت باسـم قلعـة (المدينـة المنـورة)، أمـر السـلطان سـليمان القانـوني بتجديـد سـورها في العـام ١٥٣٢م، وتـم تدعيـم السـور بعـدد مـن الأبـراج والبوابـات

قلعة ينبع

تقـع داخـل سـور المدينـة، مثمنـة الشـكل، بُنيـت على جبـل متوسـط الارتفـاع بعلـو ٥م، بهـا ٨ أبـراج نصـف أسـطوانية، وتتكـون مـن طابـقين، وضـم حصـن القلعـة بئرًا للميـاه وحمامـات وفـرن، ولتدعيـم قـدرة ينبـع الدفاعيـة قـام وزيـر الشريـف غالـب بـن مسـاعد ببنـاء سـور جديـد حـول المدينـة سـنة ١٢١٨هـ/ ١٨٠٣م، وإضافـة أبـراج بغـرض المراقبـة وحمايـة المدينـة

القلعة العثمانية

تجمـع بين الطـراز الإسلامـي والأنـدلسي، وتتكـون مـن مجموعـة مـن الأبـراج والأسـوار تحيـط بسـاحة كـبيرة، وضمـت مجموعـة مـن الغـرف والمخـازن وبئر للميـاه

قلعة أملج (قصر الإمارة)

شُـيدت على هضبـة شمال الميناء، مـن صخور بركانيـة سـوداء، بطـول ٣٠م×٢٥م، بهـا بـرج مراقبـة وروشـان ودرج حلـزوني، ويوجـد بهـا عـدد مـن الغـرف _ يفتـح أغلبهـا على القلعـة مـن الداخـل بنوافـذ عديـدة _ المخصصـة لسـكن الحاكـم واسـتقبال الوفـود وأخـرى كسـجن، في العـام ١٣٣٦هـ تـم تدميرهـا مـن قبـل القـوات الإيطاليـة، وأُعيـد بناؤهـا على الطـراز المعماري الحديـث، فأصبحـت شـبيهة بالـقصر، ورُمِّمـت عـام ١٣٧٥هـ مـع زيـادة عـدد الغـرف بداخلهـا وإضافـة طابـق ثـانٍ، واسـتخدموا جـذوع الأشـجار وجريـد النخـل في سـقفها، وتـم اسـتخدامها مقـرًا للإمـارة لـفترة طويلـة

قلعة الملك عبد العزيز في حقل

بنيـت عـام ١٣٥٩هـ بالحجـر الـجيري على الطـراز العـثماني، بطـول أسـوار ٥م وأبـراج مسـتديرة، تحتـوي على فنـاء داخلي وفي كل

برج منها أربعة مزاغل مستطيلة الشكل، وحجرات ذات نوافذ متعددة، وسقف بجذوع النخل، ويوجد فيها بئر للمياه

قلعة ذات الحاج

بنيت عام ٩٧١هـ/ ١٥٦٣م، في عصر السلطان العثماني سليمان القانوني، مساحتها ٢٣,٦م×٢٣,٨م، جدرانها بسمك ١,٨م، تتكون من ٣ طوابق، وفيها عين ماء، و٥ حجرات أرضية وغرف علوية ومسجد في الطابق الأوسط، وأسوار بممر دفاعي داخلي

قلعة تبوك

أُنشئت بأمر من السلطان سليمان القانوني سنة ٩٦٧هـ استخدمت لحماية مورد الماء وركب الحج، تم تجديدها في عهد السلطان محمد الرابع ١٠٦٤هـ/ ١٦٥٣م، وترميمها في ١٢٦٠هـ بأمر من السلطان عبدالحميد خان بن محمود، وتجديدها مرة أخرى سنة ١٣٧٠هـ/ ١٩٥٠م، وتحولت لاحقًا إلى مركز شرطة

قلعة المويلح

بنيت عام ٩٦٨هـ على ربوة، لتأمين الحجاج، وتوفير المياه لهم وخدمتهم، وحفظ أمتعتهم ومقتنياتهم، وحماية الساحل من البرتغاليين، وهي قلاعة حصينة طولها ١٠٠م×٨٠م، وبها عدد من الأبراج في أركانها بقطر ١٠م، وطول حوشها ٨٣م×٦٢م، وبها بئر ماء بعمق ١١م، وتتكون من ٧غرف ومسجد وبئر ومخازن للسلاح، ويوجد بها مخازن لتجار الفحم والحطب، والسمن والعسل، تم ترميمها عدة مرات

أسوار القلعة وأبراجها

يصل بين أسوار القلعة وأبراجها ممر داخلي علوي يسمح بتحرك الجنود بين الأبراج، وله جدار ساتر تنتشر به المزاغيل والمشرفات، وتم تزويدها بأبراج ضخمة في أركانها الأربعة، وصمم البرج على أن يكون بمستوى علوي وآخر سفلي للدفاع، وصممت ثلاث فتحات في الجزء السفلي وأربعة في العلوي، وتزويد كل برج بسبعة مدافع والسور تم تزويده بمزاغيل للبنادق على طول البرج

قلعة رابغ

تعود لبدايات القرن ١٠هـ تحتوي على برج شمالي غربي، ومخازن غلال، وخمس آبار، كانت محطة لحجاج الشام ومصر ومنها إحرامهم

قلعة الأزنم

بُنيت عام ٩١٦هـ بأمر من السلطان المملوكي قنصوة الغوري على يد المعماري خشقدم الخازن، مربعة الشكل، وفيها أبراج مضلعة، و٤ أسوار متعامدة، وحول فنائها حجرات أسقفها مغطاة بالقبوات، وممرات دفاعية ومزاغيل

قلعة الملك عبد العزيز - ضباء

شُيدت عام ١٣٥٢هـ على ربوة مشرفة على البحر، من الحجر الجيري، بها ٤ أبراج شبه دائرية، ومسجد داخلي، ومرافق إدارية وسكنية، تميزت بأسلوب معماري عثماني

مدينة الوجه

تقع على الساحل، وبها قلعة أخذت اسم المدينة وتقع إلى الشرق منها بحوالي ٨ كلم في وادي (الزريب)، وهو واد فسيح تتوزع في جنباته أشجار الأراك والطلح، وقد بنيت القلعة في سفح أحد جبال الوادي، تم استخدام الحجر الرملي المجلوب من

المحاجر لبنائها، وتم سقفها بأشجار الدوم والأثل، وجلبوا المياه للبناء من الآبار العديدة التي حفرت في الوادي، وقد تم تشييدها لتكون محطة لحجاج بيت الله الحرام، وحفظ الأمتعة والودائع، وحفظ الأمن بوادي الوجه، وتضم بالإضافة لسورها والمباني الداخلية مسجدًا وبئرًا لمياه الشرب، و٣ برك للمياه ملاصقة للسور الشمالي من الخارج، واحدة لشرب الحجاج، والثانية لسقي البهائم، والثالثة لغسيل الملابس والاستخدامات الأخرى

مبنى محافظة الوجه

من أقدم مباني المدينة، استخدمته البحرية العثمانية، وبه أول معمل لتحلية مياه البحر

قلعة السوق

بُنيت عام ١٢٧٦هـ على جرف صخري، مستطيلة الشكل، بها برج واحد مربع بفتحتين للمدافع، وحجرات تستخدم للإدارة، وسلمان داخليان.

قلعة فرسان

بنيت عام ١٢٥٠م في جزيرة فرسان، مساحتها ٥٠٠م² وارتفاعها ١٠م. مستطيلة الشكل، جدرانها بسمك ٦٥ سم، بها غرف، وساحة، وخزان مياه، ودكة للمراقبة، وبوابة محصنة، استخدم في بنائها الجص، والحديد، وسيقان الأشجار

الفصل الرابع

قلاع وحصون الساحل الأردني والفلسطيني

مدينة آيلة العقبة

يقع ميناء آيلة - العقبة على الطرف الشرقي من خليج العقبة، وهي من المدن القديمة يرجع تاريخها إلى ١٢ ألف سنة ق.م، وكلمة أيلة اشتقت من (أيل)، التي جاءت في نص جلجامش بمعنى(الله)، وكان(أيل) إله الأكاديين والكنعانيين والعبرانيين، وفي القرن الثامن ق.م استولى الآراميون على أيلة

قلعة أيلة - العقبة

هي قلعة أثرية تقع في وسط العقبة جنوب الأردن، يعود تاريخها إلى العصر المملوكي، وتم اختيار موقعها بالقرب من شاطئ البحر الأحمر؛ لأهمية هذا الموقع من الناحية الجغرافية والاستراتيجية. وتتكون القلعة من فناء مربع مسور طول ضلعه ٥٨م، وكان يبرز عن الجدران المحيطة أبراج مضلعة استبدلت بأخرى دائرية في منتصف القرن الثالث عشر والتاسع عشر الميلاديين، زار القلعة في العام ١٨٢٨م الرحالة (ليون دي لابورد) ومن خلال رسمه لها يبدو أن الأبراج المضلعة ما تزال قائمة في ذلك الوقت، كانت مهمتها تيسير مهمة الحجاج المصريين القادمين إلى مكة المكرمة والمدينة المنورة، وفي العام ١٨٤١م ونتيجة لاتفاقية لندن أصبحت مصر تتولى إدارة العقبة بغرض حماية طريق الحج المصري، وبذلك أخذت طابعًا عسكريًا أدى إلى إعادة أبراجها فضلًا عن مجموعات الغرف المقامة في الجهتين الشمالية والغربية. يقع مدخل القلعة في الجدار الشمالي ويحيط به برجان دائريان قطراهما غير متساويين، ويظهر على كل برج قرص بداخله اسم السلطان العثماني مراد بن سليم خان، وموضح داخل القلعة بأن من قام ببنائها خاير بك العلائي، وقد أرخت القلعة لفترات تاريخية مهمة من

خلال النقوش التي وجدت بداخلها، وتم تدمير الجدار الغربي خلال الحرب العالمية

أشار محمد صادق باشا صاحب كتاب (مشعل المحمل) إلى قلعة تقع في منطقة العقبة، وقد وصفها عند زيارته لها، وهو أمين لصرة الحج المصري في سنة ١٢٩٧هـ/ ١٨٨٠م بأنها من القلاع المتينة وأكبرها في طريق الحج المصري، مبنية من الحجر المقطوع مساحتها ٣٠٠م² تطل على شاطئ البحر الأحمر، أنشأها السلطان مراد بن السلطان سليم الأول، ويبلغ طولها ٦٣م وعرضها ٦٣م أيضًا، ويوجد في أركانها ٤ أبراج اثنان منهما آيلان للسقوط، وتبلغ مساحتها الداخلية ٤٥×٤٥م، وتحتوى على بئر للمياه صالحة للشرب يبلغ عمقه ٢٠م، وتضم مسجدًا للصلاة، ومكانًا للذخيرة، وعليها يوزباشي من الجهادية الطوبجية، ومزودة بأربعة مدافع أحدهما نحاس عيار ٣٥ والثلاثة المدافع الأخرى من الحديد، وبها ٣٣ من العساكر بيادة المشاة و٧ طوبجية؛ أي ضاربي المدافع ويوجد بجوارها عدد من البيوت الصغيرة والعشش. وتأتي إلى القلعة القبائل العربية القريبة بغرض التجارة، حيث كانوا يتاجرون بالفواكه مثل: الخوخ، والرمان، والعنب، من بلدة معان في حدود الشام، وتتم زراعة البامية والخضروات المختلفة في المنطقة، ويوجد بها بالإضافة للخضروات أشجار النخيل ومياه عذبة للشرب، وقد تم حفر عدد من الحفائر بالقرب من البحر الأحمر فتنبع منها مياه أعذب من مياه البئر الموجودة بالقلعة، ويوجد بالمنطقة العديد من أنواع الأسماك مختلفة الألوان والأشكال

قلعة أم رشراش

تقع أم الرشراش أقصى جنوب فلسطين المحتلة كان يطلق عليها اسم قرية الحجاج؛ إذ كان الحجاج المصريون يستريحون بها في طريقهم إلى الحجاز، ويرجع اسم أم الرشراش إلى إحدى القبائل التي كانت تقطن في المنطقة، وكان ميناء أم الرشراش ميناء رئيس للحجاج تحت الإدارة المصرية، ووقعت تحت سيطرة الصليبيين، وتمكن القائد صلاح الدين الأيوبي من طردهم منها وتحصين الميناء في العام ١١٧٠م ضد الهجمات الصليبية التي تعرضت لها المنطقة، وعمل على بناء عدد من الحصون والقلاع على خليج العقبة. ثم عادوا إليها مرة أخرى، وتمكن السلطان الظاهر بيبرس من طردهم منها نهائيًا في العام ١٢٦٧م، وفي عهد السلطان قنصوه الغوري تم بناء قلعة في أم الرشراش بغرض حمايتها. وتأتي أهمية ميناء أم الرشراش وقلعته التاريخية، من الاهتمام الكبير بها من قبل القائد صلاح الدين الأيوبي وقنصوه الغوري اللذين عملا على بناء قلعتين في فترات تاريخية مختلفة بغرض حماية الميناء والمدينة، وما يدل على أهمية الميناء والمنطقة التي تبلغ مساحتها ١٥٠٠م٢، وقعت تحت سيطرة الاحتلال الإسرائيلي في ١٠/ ٣/ ١٩٤٩م

الفصل الخامس

قلاع وحصون وبوابات الساحل المصري

قلعة صلاح الدين الأيوبي

تقع في جزيرة فرعون عند رأس خليج العقبة على بعد ٨ كلم من مدينة العقبة، وأم رشراش، مساحتها ٣٢٥م من الشمال إلى

الجنوب و٦٠م من الشرق للغرب، وقد دلت الكشوف الأثرية التي نقبت في الجزيرة إلى أنها ميناء قديم، وجزيرة فرعون ذات طبيعة صخرية تتكون من تلّين كبيرين أحداهما شمالي، وهو الأكبر والأعلى، والآخر جنوبي أصغر، بينهما سهل أوسط، ويرجح أن أصل تسميتها بجزيرة فرعون يعود إلى (فارا)، الذي أطلقه الرومان عليها، وتعني المنارة ثم تحولت إلى فرعون، تم بناء القلعة لتكون نقطة حصينة لحماية الطرق البرية والبحرية بين مصر والشام والحجاز، وقاعدة بحرية لتأمين خليج العقبة والبحر الأحمر من الهجمات الصليبية، استخدمت الجزيرة في العصور الإسلامية للعديد من الأغراض، وتمت السيطرة عليها من قبل الصليبيين في سنة ١١١٦م أثناء هجماتهم المتعاقبة على سيناء حتى تم تحريرها على يد صلاح الدين الأيوبي سنة ١١٧٠م، الذي شرع في بناء العديد من التحصينات لتأمين البحر الأحمر من الهجمات الصليبية وحماية طريق الحج المار بوسط سيناء بداية من السويس مارًا بنخل ثم منطقة (التمد) حتى رأس خليج العقبة لينتهي في الحجاز

شكل القلعة

تتكون القلعة من مجموعة تحصينات شمالية جنوبية، وكل منهما عبارة عن قلعة مستقلة تستطيع أن تستقل بمفردها إذا تمت محاصرة إحداهما، والحصن الشمالي أكبر من الجنوبي ومازال يحتفظ بكثير من عناصره المعمارية، أما المساحة الوسطى بين القلعتين فقد أقيمت فيها المخازن والغرف، وهي عبارة عن بقايا حجرات صغيرة لا يوجد منها إلا الجزء السفلي من الجدران ويوجد بها فرن لتصنيع الأسلحة وحظائر للماشية، ومخازن للأسلحة، ومعدات للصيد، وبقايا كنيسة على الطراز البازيلكي والبحرية الداخلية تم استخدامها ميناء لرسو القوارب التي تقوم بنقل المياه والطعام والجنود إلى الجزيرة، أما القلعة الجنوبية فهي مجرد أطلال ترجع إلى العصر البيزنطي. ويتكون الحصن الشمالي من عدد من الأسوار يصل ارتفاعها إلى ٦م يتخللها مجموعة أبراج مربعة ذات طابقين، وأحيانًا ذات ثلاثة طوابق بغرض زيادة قدرتها الدفاعية، كما توجد بها مزاغل لرمي السهام في ثلاثة اتجاهات بحيث يمكن التحكم في كل اتجاه، وخاصة في المناطق التي يمكن الصعود منها إلى أعلى، وعدد هذه الأبراج ٩ أبراج، ويبلغ سمك السور الغربي ١,٦م، ويحتوى على طرقات وشرفات كانت تستخدم ليقف الجنود خلفها لرمي السهام، أما السور الشرقي فهو متهدم تمامًا ولم يتبق منه سوى الآثار الدالة على خط سيره، وهناك برج آخر يطل على الجهة الشرقية وملحق به برج للحمام الزاجل الذي كان يستخدم في نقل الرسائل بين القلعة والقاهرة والقلعة والشام

ويضم الحصن الشمالي عددًا من المباني، هي: غرف للمبيت، ومخازن، ومطبخ وفرن، ووجد فيه صهريج للمياه محفور في الصخر بالقرب من المدخل الشمالي شيّد من الحجر الجيري مكسو من الداخل بطبقة من الملاط، وصهريج آخر بالقرب من المدخل الثاني في الجنوب، ويقع الحمام بالقرب من صهريج الماء، ويتكون من ٣ غرف مشيدة من الحجر الجيري ومغطاة بأقبية من الحجر الجيري أيضًا، ويوجد فيه مسجد، وهو مستطيل

الشـكل، وكان يحيـط بالجزيـرة سـور يبلـغ طولـه ٩٥٠م تهـدم معظمـه، وكان بـه ٩ أبـراج دفاعيـة لم يبـق منهـا إلا بـرج واحـد بالجهـة الغربيـة

قلعة القلزم

تقـع قلعـة القلـزم أو الطابيـة في بلـدة القلـزم (السـويس) وهـي مـن القلاع القديمـة التـي تتميـز بتحصيناتهـا القويـة، تـم بناؤهـا على تلّـة عاليـة تطـل على البحـر الأحمـر بارتفـاع ٥٠م فـوق سـطح البحـر، وذلـك للقيـام بعـدد مـن المهـام، منهـا: الدفـاع عـن المدينـة، ومقـر دائـم للقـوات، ومدرسـة عليـا للعلـوم العسـكرية وتعليـم الجنـود كيفيـة خـوض المعـارك في البر والبحـر، وكانـت مركـزًا لصناعـة وصيانـة السـفن بأنواعهـا المختلفـة وترميمهـا. وشـهدت القلعـة العديـد مـن الأحـداث والـفترات التاريخيـة منهـا حكـم المماليـك والعثمانـيين، وتـم إحاطتهـا بسـورين مزوديـن بعـدد مـن الاسـتحكامات العسـكرية المزدوجـة مـن الداخـل والخـارج، وقـد بلـغ عـرض السـور الخارجـي مترين وارتفاعـه ٨م بـه عـدد مـن الأبـراج، أمـا السـور الـداخلي فقـد كان سـمكه أصغـر مـن السـور الخارجـي بـه عـدد مـن الأبـراج مسـتديرة ومسـقوفة بفتحـات ضيقـة. وتضـم مجموعـة مـن الحجـرات المتجـاورة تـم إعدادهـا ثكنـات للجنـد، تميـزت بأبوابهـا الضخمـة مـزودة بفتحـات (مزاغـل) للتهويـة، تبلـغ مسـاحة القلعـة (الطابيـة) ٣٣٠م× ١٥٠م، وقـد دلَّ الكشـف الأثـري فيهـا على وجـود حصـون قديمـة مما يـدل على الأدوار الدفاعيـة التـي كانـت تقـوم بهـا في حـدود مصر الشرقيـة ومنهـا تحركـت الحملـة المصريـة ضـد البرتغالـيين في جنـوب البحـر الأحمـر، وتمكنـت مـن إجبـار الأسـطول البرتغـالي بقيـادة (اسـتفاو داجامـا) حاكـم الهنـد على الانسـحاب نحـو قاعدتـه في (أرقيفـو) في مينـاء مصـوع على السـاحل الأريتري، تعرضـت القلعـة للهـدم والإزالـة في العـام ١٩٦٢م بحجـة بنـاء عـدد مـن المسـاكن الجديـدة

قلعة عجرود

تـم إنشـاؤها في إبـان الحكـم المملـوكي لمصر؛ بغـرض خدمـة ضيـوف الرحمـن، وقـد اشـتملت على العديـد مـن المنشـآت المعماريـة المختلفـة، منهـا: خـان حـصين للمسـافرين، ومسـجد، وملحقـات خدميـة تشـتمل على بئر للميـاه، وجبانـة لدفـن المتـوفين مـن الحجـاج. فكانـت محطـة مهمـة في السـويس للحجـاج والتجـار العابريـن بين مصر والشـام، وكذلـك للتجـار العابريـن بقنـاة السـويس وموانـئ البحـر الأحمـر، تراجـع دورهـا بعـد تطـور وسـائل النقـل والمـواصلات وبعـد أن حلـت القطـارات محـل الـدواب، وتـم هجرهـا بشـكل كامـل في عهـد الخديـوي إسماعيـل في العـام ١٨٨٣م

مدينة القصير

يقـع ميناء القصير على سـاحل البحـر الأحمر، وهـو مـن أقـدم الموانـئ، ولحمايـة المدينـة تـم تشـييد (قلعـة) القـصير التـي يطلـق عليهـا أهـل المنطقـة اسـم الطابيـة في عهـد السـلطان العـثماني سـليم الأول بـاقتراح مـن والي مصر في ذلـك الوقـت سـنان باشـا، واكتمـل بناؤهـا في العـام ١٥١٧م وقـد بنيـت بالحجـر الـجيري للقيـام بالمهـام التاليـة: حمايـة الميناء البحـري، ومطـاردة اللصـوص وقطـاع الطـرق، وتـأمين قوافـل الحجـاج. وقـد تـم تزويدهـا بعـدد مـن المدافـع التـي تـم وضعهـا على أبراجهـا الأربعـة للقيـام بالمهـام الدفاعيـة والمراقبـة. وتُعـدُّ مـن

مباني الحماية التي انتشرت على طول ساحل البحر الأحمر في العصر العثماني وقبله، ولأن اللصوص وقطاع الطرق ضيقوا على أهل المدينة ودفعوهم لتركها، كان لابد من بناء هذه القلعة(الطابية) التي تميزت بوجود أعداد كبيرة من المدافع، وقد شيدت فوق هضبة مرتفعة، وتُعدُّ من أشهر معالم مدينة القصير وتميزت جدرانها بالمتانة، ويوجد بها خزان للمياه بغرض توفير المياه للمقيمين بالقلعة. وتُعدُّ طابية القصير من أكثر المباني الدفاعية على امتداد الساحل امتلاكًا للمدافع الأمر الذي يوضح الأهمية الكبيرة لهذا الميناء التاريخي. ويلاحظ أن فكرة الطوابي وبنائها ظهرت في وادي النيل السودان ومصر وغيرها من المناطق حيث تم استخدامها لأغراض دفاعية وهي موجودة، حتى يومنا هذا، في شمال السودان ووسطه

الفصل السادس

قلاع وحصون وبوابات الساحل السوداني

حصن برنيس

ميناء برنيس من الموانئ السودانية القديمة تم تأسيسه في العهد البطلمي في منطقة حلايب، وأُطلِق عليه ميناء برنيق Berenike وميناء الحبش، وميناء الساباي، ولشحة المياه فيه تم جلبها من(شنشيف) التي تبعد ٣٥ كم جنوب برنيق، ويرجح أن الميناء كان يستخدم لنقل الأفيال من مناطق السودان للمشاركة بها في العديد من الأنشطة الحربية لدى البطالمة، وقد عُرِفَت مروي بأنها من المناطق التي استخدمت الأفيال في الحروبات. ويرجع تاريخ الحصن إلى عام ٢٣٠٠ ق.م، وتم تشييده بغرض حماية ميناء برنيس، وضم ساحات كبيرة ومجموعة من الورش والمخازن والتحصينات الدفاعية، مع بئر لتجميع مياه الأمطار

سواكن

تُعدُّ مدينة سواكن من أهم الموانئ السودانية على ساحل البحر الأحمر وأقدمها، نالت سواكن شهرة كبيرة على مستوى العالم القديم والمعاصر، وكانت قبلة للتجار والبحارة والرحالة من مختلف البلدان، وكانت الميناء الرئيس للصادرات والواردات السودانية، بحكم موقعها الاستراتيجي الرابط بين الموانئ الأوربية عبر البحر الأحمر والمحيط الهندي والخليج العربي، وسعت جميع القوى وعبر فترات تاريخية مختلفة للسيطرة عليها؛ لتكون قاعدة للأساطيل والقوات، فتعرضت لهجمات البطالمة والرومان والمرويين، وخضعت للسيطرة البرتغالية والعثمانية ومملكة الفونج وتوسعات الخديوية المصرية وتمكنت بريطانيا من وضع يدها عليها، وحاولت المهدية عبر قوات الأمير عثمان دقنة السيطرة على المدينة الساحلية، لكن لتحصيناتها القوية لم يتمكنوا من ذلك رغم من محاولاتهم المستمرة حتى سقوط دولتهم في العام ١٨٩٨م، وتدلُّ كل الشواهد التاريخية والحضارية والاقتصادية على مكانة سواكن بوصفها ميناءً ومدينةً لها أهميتها التي اكتسبتها عبر التاريخ، وتميزت من جهة البحر بتحصينها الذي وفر لها التواصل مع العالم الخارجي لذلك يصعب إسقاطها عبر الحصار؛ لأن كل متطلباتها تأتيها عبر البحر الممتد من الحجاز ومصر والهند وغيرها من المناطق

صيانة بعض المرافق في سواكن من قبل الدولة العثمانية

شـهدت الـفترة بين (١٥١٧-١٨٨٢م) التـي بسـط العثمانيـون سـيطرتهم على سـواكن العديـد مـن أعمال الصيانـة بحسـب مـا تضمنتـه وثائقهـم، فبحلـول العـام ١٨٥٤م شـهدت المدينـة بعـض أعمال الترميـم التـي شـملت مقـر قائمقاميـة سـواكن وبعـض الأحيـاء الداخليـة فيهـا، وقـد طلـب القائمقـام في سـواكن مـن الصـدر الأعظـم بضرورة تجديـد مبنـى الـجمارك وإنشـاء مينـاء جديـد على أن يتـم دفـع تكاليفـه مـن قبـل إدارة الـجمارك في جـدة بولايـة الحجـاز العثمانيـة، الأمـر الـذي يوضـح بُعـد نظـر الإدارة العثمانيـة في ذلـك الوقـت وأن مينـاء سـواكن لا يغطـي حركـة الصـادر والـوارد مـن السـلع والمنتجـات بالصورة المطلوبـة، وقـام الاحـتلال البريطاني بعد سـطرته على السـودان بإنشـاء مينـاء بورتسـودان الـذي يقـع إلى الـشمال مـن سـواكن، وبذلـك تلاقـت مشروعـات الدولـة العثمانيـة مـع الطمـوح والرغبـة البريطانيـة الراميـة إلى تأسـيس مينـاء حديـث على السـاحل السـوداني بـدلًا عـن سـواكن

وفي العـام ١٨٦٤م حصلـت شركـة العزيزيـة المصريـة على امتيـاز بنـاء خـط سـكة حديـد سـواكن الخرطـوم، وقـد قـام العثمانيـون ببنـاء قلعـة في سـواكن بغـرض حمايتهـا مـن الخطـر البرتغـالي الـذي تمـدد في المنطقـة، وقـد اتاحـت سـواكن مـن خلال موقعهـا الاستراتيجـي للإدارة العثمانيـة ضمان سلامـة التجـارة في البحـر الأحمـر، ووقـف التقـدم البرتغـالي فيـه، وضمان أمـن البحـر الأحمـر والبحـر الأبيـض المتوسـط. وأصبحـت سـواكن ميناءً مـهمًا يسـتقبل التجـار القـادمين مـن الهنـد والداخـل الأفريقـي والباشـوات المسـافرين على اليمـن والحبشـة ومجموعـات الحجـاج القـادمين مـن داخـل السـودان وغـرب أفريقيـا إلى الأراضي المقدسـة في الحجـاز. وانتعـش الطريـق البحـري عبر البحـر الأحمـر الـذي ازدحـم بحركـة السـفن التجاريـة مما أدى إلى إعـادة الحيوية إلى الموانئ المطلـة عليـه ومـن بينهـا سـواكن. وقـد سـعى الخديـوي إسماعيـل إلى تطويـر المدينـة مـن خلال بنـاء منـازل جديـدة ومصانـع ومسـاجد ومستشـفيات وكنيسـة للأقبـاط. فعـادت إليهـا السـفن الأوربيـة، وجـرت عمليـات نقـل وتبادل السـلع السـودانية المختلفـة، مثـل: الذهـب، والتمـور، والجلـود والقطـن والصمـغ العـربي، وسـن الفيـل، وريـش النعـام، وشـمع العسـل، والسـمن بمنتجـات الشرق والغـرب، ومـن بينهـا التوابـل والزجـاج، والـورق، والمنسـوجات وازداد عـدد سـكان المدينـة مـن البجـا والعـرب وغيرهـم مـن التجـار القـادمين مـن مختلـف بقـاع العـالم، مثـل: الدولـة العثمانيـة، ومصر واليونـان واليمـن، وأرمينيـا والهنـد وأوروبـا

سور سواكن

قامـت بريطانيـا بعـد سـيطرتها على مصر في العـام ١٨٨٢م بإنشـاء قنصليـة لهـا في سـواكن، وكلفـت المهنـدس الملازم غـردون، الجنرال فـيما بعـد، ببنـاء سـور حـول المدينـة ليمنـع هجمات القبائـل القاطنـة حولهـا، فبنـاه وبنيـت حولـه مـن الداخـل السـكنات الحربيـة، الأمـر الـذي أدَّى إلى زيـادة اسـتحكامات المدينـة وأصبحـت مـن المـدن المحصنـة بعـد اسـتكمال السـور، وصـل ارتفـاع السـور إلى ٤م وسـمكه ٣م، وبحلـول العـام ١٨٨٦م تـم فتـح ٥ بوابـات على السـور بغـرض مراقبـة الداخـلين والخـارجين للمدينـة، كما تـم وضـع قـوة عسـكرية لحمايـة تلـك الأبـواب

قلاع سواكن وبواباتها

توجد في سواكن ١٧ قلعة، تعرَّض معظمها للإهمال وتهدمت مع مرور الوقت، منها قلعة الحاكم البريطاني - المصري التي تم بناؤها في مدخل الجزيرة بواسطة الضابط البريطاني في ذلك الوقت شرلس جورج غردون، وتم تجهيز القلاع الحربية التي تبعد مسافة ميلين بالأسلحة والقوات والمساكن للقوات المرابطة هناك، وتم وضع ثلاثة وابورات حربية راسية بالميناء لتضيء المناطق المحيطة بالمدينة ليلًا. وكانت في سواكن ٥ بوابات، هي: بوابة الأنصاري، وبوابة أندارا، وبوابة المحلج، وقد عرفت سواكن محالج القطن منذ وقت مبكر، وبوابة أسفنكس، وبوابة كتشنر التي تم بناؤها بواسطة الضابط البريطاني كتشنر في العام ١٨٨٦م، وهي أشهر البوابات في السودان وقد تم تضمينها في إحدى إصدارات العملة السودانية، وتمت إعادة ترميمها بواسطة الشيخ محمد نور هداب على نفقته، بعد أن سقط أحد برجيها، وكانت القوافل التجارية تدخل إلى المدينة عبر هذه البوابة التي تُعدُّ أهم بواباتها، وفضلًا عن بواباتها ففيها عدد من الحصون، وهي: حصن مهاجر، وحصن أبو الهول، وحصن طوكر، وحصن السوداني، وحصن الأنصاري، وحصن اليمني. وتضم المدينة أيضًا متحف هداب الذي يحتفظ بالكثير من المقتنيات الأثرية لفترات تاريخية مختلفة من سواكن والسودان

الخيول في سواكن

عرف السودان الخيول منذ قديم الزمان، وأشارت العديد من المصادر التاريخية والشواهد الأثرية إلى حب الملك بعانخي للخيول، وقد تم العثور على رفات فرس يعود تاريخها إلى العصر المروي وتحديدًا إلى ٣٠٠٠ ألف عام ق.م. وقد تم دفنها بعناية كبيرة، وقد كانت ذات لون كستنائي وقد تم تكفينها مما يعني أن الخيول كانت محل تقدير في ذلك الوقت من قبل حكام ذلك العصر في السودان، وقد أكدت البعثة الأثرية التي نجحت في الكشف عن هذه المهرة أنها كانت تجر عربة، وقد أطلق على هذه الفرس اسم(تومبوس) وهو اسم المكان الذي اكتشفت فيه، وقد ذكر الباحثون من جامعة بوردو ومن خلال استخدام الكربون أن الفرس يعود تاريخها إلى ٩٥٠ ق.م تقريبًا

بوابة غردون في سواكن

تم تعيين غردون باشا في العام ١٨٧٧م حاكمًا عامًا على السودان وجاء للمرة الثانية لهذا البلد عبر سواكن إلى الخرطوم، فأمر ببناء طريق معبد يربط بين جزيرة سواكن والبر، وبالفعل تم الشروع بواسطة سجناء المدينة في بناء الطريق في ستة أشهر، وتم تشييد بوابة غردون في سواكن في العام ١٨٧٩م لتصبح واجهة المدينة الحضارية من جهة البحر، وقد استخدمت البوابة لعبور الحجاج والمشاة والإبل التي كانت تحمل البضائع من السفن التي ترسو في الميناء لتحملها إلى مناطق السودان المختلفة، ونجح غردون في بناء بوابته والممر الموصول بها، ومدينة مثل سواكن تستحق مثل هذه البوابات التي تدل على مكانتها التاريخية والحضارية بين مدن ساحل البحر الأحمر. ويتمُّ إغلاق بوابة الجزيرة بعد صلاة العشاء مباشرة وذلك بغرض تأمين المدينة، وعليها حراسة مشددة ويتم فتحها في صباح اليوم التالي

القصور في سواكن

ضمت مدينة سواكن عدد من القصور، منها: قصر كتشنر باشا، وقصر ممتاز باشا، وقصر الشناوي، وقصر محمد علي شاويش، وهي من القصور التاريخية المهمة في المدينة التي ارتبط أسمها باسم المدينة

قصر ممتاز باشا

تم بناؤه في عهد ممتاز باشا الذي عين حاكمًا على المدينة في بدايات العام ١٨٦٦م، وقد قام بتوسيع ميناء سواكن، وببناء عدد من المنازل الجديدة

قصر محمد علي شاويش

كان محمد علي شاويش أحد أهم أثرياء المدينة، ويُعدُّ قصره الذي يقع بالقرب من بوابة غردون، من أهم معالم المدينة التاريخية، ويعود تأسيسه إلى العهد العثماني

قصر الشناوي

الشناوي بك هو أحد شيوخ تجار سواكن، وتم إنشاء قصره في العام ١٨٧٩م على النمط المصري، ويُعدُّ من أهم معالم المدينة، يتكون من ٣ طوابق و٣٦٥ غرفة، وهناك غرفة للضيوف من الرجال و(حرملك) للنساء، استغل الشناوي الطابق الأول لبضائع التجار والطابق الثاني للسكن، والثالث للنوم في فصل الصيف، والقصر به ساحة فسيحة للبيع والشراء والمزاد والبورصة، وكان يطلق عليه اسم وكالة الشناوي أو بورصة سواكن، ويتم فيها عرض السلع المختلفة المحلية والمستوردة

قصر الأمير عثمان دقنة (أمير الشرق)

يقع القصر على ساحل البحر الأحمر مباشرة، لدرجة أن بعض الأعمدة والطابق الأرضي مغمور بمياه البحر، وأرضية ذلك الطابق مصنوعة من الخشب القوي المشبع بالرطوبة، وبه (بالكونة) مطلة تمامًا على البحر، وغرفه واسعة وجدرانه سميكة صامدة، ولا يوجد أي مبنى ملاصق له ولا أسوار

مدينة محمد قول

تقع على ساحل البحر الأحمر، اشتهرت بمينائها القديم وصيد الأسماك وتصديرها للأسواق الخارجية كالسعودية

طابية محمد قول:

مبنى يشبه الحصن أكثر من الطابية، له طابقان وسقف خشبي ونوافذ للمراقبة، بُني بالحجر بمتانة عالية، وتميّز عن طوابي الخديوية والمهدية، ويشكل شاهدًا على العمارة الدفاعية في شرق السودان

الفصل السابع

قلاع وحصون الساحل الإريتري

مدينة مصوع

أُطلِقَ على مصوع، لؤلؤة البحر الأحمر، ويقال إن اسم مصوع جاء من القاضي الشرعي للمدينة والمعروف باسم محمد مسؤ، ولد في العام ١٢٠٠هـ، وكان يحضر إليه الناس، ويقول الواحد منهم (إني ذاهب إلى القاضي مسؤ)، وحرفت بعد ذلك كلمة مسؤ إلى مصوع، وكانت أحد المراكز الإسلامية في شرق القارة الأفريقية بعد مكة

ومدينة مصوع من أهم المدن الإريترية على ساحل البحر الأحمر، كانت عاصمة لإريتريا حتى مجيء الاستعمار الإيطالي الذي حول العاصمة إلى مدينة أسمرة، ومصوع شديدة الشبه بكل من سواكن وجدة، وهذه المدن الثلاث لعبت أدوارًا مهمة في

التاريخ الاقتصادي والاجتماعي والحضاري للبحر الأحمر عبر عصوره المختلفة وحتى اليوم، وتتميز بأهميتها الاستراتيجية ودورها في التجارة المحلية والدولية، وشكلت هذه المدن عنصر جذب للكثير من المجموعات البشرية لتأتي وتستقر فيها

ولأهمية مصوع وموقعها الاستراتيجي في الجزء الجنوبي الغربي من البحر الأحمر تعرضت للاحتلال من قبل القوى الإقليمية والدولية، كمصر والدولة العثمانية، وإيطاليا، وبريطانيا وأثيوبيا التي كانت أريتريا جزءًا منها، وقد تم إنشاء ميناء مصوع في عصر الفراعنة ٢٦٢٥ _ ٢٤٧٥ ق.م، وعبر الميناء استطاعوا أن يتحصلوا على البخور، والذهب، والعاج، وغيره من المنتجات من داخل العمق الأفريقي

قام إسماعيل حقي حاكم مصوع بحرق قرية (دخنو) وبنى قلعة فيها وذلك لتثبيت دعائم الوجود العثماني هناك ولقمع أي حركة معارضة جديدة. وفي العام ١٨٧٢م، وفي عهد سيطرة الخديوية المصرية قرر الخديوي إسماعيل تعيين المستشرق السويسري (متزنجر) باشا حاكمًا عامًا على مصوع، وقام بربط سواكن بميناء مصوع من خلال خدمة البريد والتلغراف، ووصل عدد السفن بين الميناءين إلى ١٧٢ سفينة في إحدى السنوات لتقوم بنقل البن، والسمسم، والذرة، والسنامكي، والحيوانات المختلفة، مثل: الأسود، والنور والأنعام والأبقار، وريش النعام، وسن الفيل، وفي الفترة ما بين ١٨٧٠-١٨٧١م وصل عدد السفن إلى ٩٢ سفينة، منها سفن البريد والسفن التجارية، وقد تم ربط سواكن ومصوع بميناء السويس ومدن الساحل الشرقي من البحر الأحمر

قلعة مصوع

عرفت مصوع القلاع منذ أن هاجر إليها بني أمية، بعد زوال دولتهم في ١٣٢هـ على يد العباسيين، وعندما بسطت الدولة العثمانية سيطرتها عليها قامت ببناء طابية في منطقة(مشتاق) على قمة جبل(حطملو)، وقلعة في(حفيفو)، ووصلوا الماء إليها من(أم كلو) إلى جزيرة طوالات، ويطلق أهالي مصوع على هذه القلعة اسم (فورتو مشناق)، وتشرف القلعة على المدينة وعلى واد وسهول(أم كلو)، والقوات التي كانت تتمركز في هذه القلعة من البوسناك أو البوشناق، وهي مجموعات من البوسنة، يرجح أنها تكونت على يد القائد سنان باشا، وعندما حصل الخديوي إسماعيل خديوي مصر على فرمان عثماني في ٢٧ مايو ١٨٦٠م مكنه من ضم مينائي سواكن ومصوع لحكمه، أصبحت بعد ذلك كل من سواكن ومصوع محافظتين جديدتين تتبعان للخديوي على ساحل البحر الأحمر حيث تبدأ حدود محافظة سواكن من جبال علبة في مثلث حلايب شمالًا وحتى رأس قصار، ومحافظة مصوع من رأس قصار إلى حلة رهيجة عند باب المندب، وقام الخديوي إسماعيل بإنشاء جسر وقلعة في مصوع ومباني للحكومة وموظفيها

بعد أن تعرضت قلعة (مشتاق) للتدمير وهي القلعة التي تم بناؤها على يد العثمانيين تم نقل حجارتها لعمل جسر بين البر والطوالون وعرف هذا الجسر، فيما بعد باسم جسر الرفيع أو سقالة قطان، وفي العام ١٨٧٢م قام السويسري(متزنجر) باشا حاكم مصوع بتوجيه من الخديوي إسماعيل بأخذ

بعض الحجارة من القلعة القديمة؛ ليبني جسرًا يربط بين طوالون ومصوع، ويقال إن من الأسباب التي دفعت حاكم مصوع لبناء هذا الجسر الهجمات المتكررة من قبل أسماك القرش التي كان يتعرض لها الأهالي عند عبورهم من الجزء المقابل لمصوع من جزيرة(قرار) سباحة(بالقربة) وهي عبارة عن جلد من الماعز أو الضأن ينفخ فيه الهواء ويقومون بربط ملابسهم على رؤوسهم وقد كان مكان عبورهم بالقرب من مقر المحافظة الأمر الذي شجعه على إتمام الجسر

التجارة في مصوع

اشتهرت المدينة بأهميتها التجارية في منطقة جنوب البحر الأحمر، وهناك عدد من السلع التي تميزت بها عبر تاريخها الطويل، ومنها اللؤلؤ ويُعدُّ الصدف الموجود في أرخبيل(دهلك) من أجود الأنواع التي يوجد بداخلها اللؤلؤ في منطقة جنوب البحر الأحمر، وقد كانت مجموعات الصيادين التي تبحر على ظهور السنابيك من المملكة العربية السعودية والكويت والبحرين تتوجه إلى مصوع؛ لبيع ما تحصلت عليه من لؤلؤ في موسم الصيد، وكانت مصوع قبلة للتجار القادمين من الهند والخليج العربي وأوروبا لشراء اللؤلؤ من هناك؛ وذلك لجودته العالية

مدينة عصب

عصب مدينة إريترية تقع على ساحل البحر الأحمر ذات أهمية استراتيجية، كانت الميناء الرئيس لأثيوبيا قبل استقلال أريتيريا، وكانت جزءًا من سلطنة (أوسا) العفرية وبعد أن تم الاتفاق بين السلطان محمد حنفري العفري والإيطاليين لإنشاء شركة ملاحة إيطالية في عصب زاد النفوذ الإيطالي في الساحل الأريتري والبحر الأحمر عمومًا، ويطل ميناء عصب على باب المندب المدخل الرئيس للبحر الأحمر، والمسافة بين عصب والمخا على الساحل الشرقي للبحر الأحمر ٤٠ ميل بحري فقط

قلعة البحر الأحمر في عصب:

تحتوي مدينة عصب على العديد من المواقع الأثرية والتاريخية ومنها قلعة البحر الأحمر التي تتميز بجمالها وروعتها

الفصل الثامن

قلاع وحصون الساحل الصومالي

تأثرت العمارة الصومالية في العصور الوسطى بالعمارة الإسلامية التي وفدت إليها من شبه الجزيرة العربية وبلاد فارس، وتم استخدام العديد من المواد المحلية مثل الحجر المرجاني، والطوب المجفف(اللبن)، والحجر الجيري، في بناء القلاع والحصون فيها، وقد ظهرت فيها العديد من المدن التجارية التي بنيت بالحجر الجيري مثل مقديشو وغيرها من المدن الصومالية

القلاع والحصون الصومالية

بنيت القلاع والحصون الصومالية التي كانت تعرف باسم(كالكادس) من قبل السلاطين الصوماليين؛ لحماية المدن من الهجمات الخارجية، ومن الممالك التي نجحت في إنشاء العديد من القلاع والحصون سلطنة(أجوران) وعندما استولى حاجي شارماركي علي صالح على مدينة بربر على الساحل شمال غربي الصومال في عام ١٨٤٥م عمل على تشييد ٤ حصون، ووضع

جيشًا مكونًا من ٣٠ رجلًا في كل حصن

ويرجع الفضل لدولة الدراويش في الصومال في بناء العديد من الحصون في شبه الجزيرة الصومالية، وبعد انسحاب القوات البريطانية من العمق الصومالي إلى الساحل في العام ١٩١٣م بنيت العاصمة الدائمة التي أصبحت مقر الدراويش في منطقة (تلاح)، وهي بلدة كبيرة مسورة تحتوي على ١٤ حصنًا، وقد اشتمل الحصن الرئيس على حديقة مسورة وبيت وحراسة، وأصبح هذا البيت مقرًا لسكن الشيخ محمد عبدالله حسن قائد الدراويش في الصومال، وضم زوجاته وعائلته وبعض قادته العسكريين الصوماليين، واستضاف العديد من الشخصيات البارزة والمهندسين والمعماريين وعمال البناء ومصنعي الأسلحة الأتراك واليمنيين والألمان، وبنيت عشرات القلاع الأخرى في مناطق(إيليج) و(شمبيرس) ومناطق أخرى من القرن الأفريقي

وظهرت العديد من الأسوار حول المدن الساحلية في الصومال مثل مدن(ميركا) و(باراوا) ومقديشو؛ لحمايتها من الهجمات البرتغالية وغيرها من المجموعات المحلية التي عملت على مهاجمة هذه المدن

قلعة دوبار: هي عبارة عن حصن دفاعي تم بناؤه في القرن الثامن عشر الميلادي في العصر العثماني ويقع في شمال الصومال

مقديشو

تُعدُّ مدينة مقديشو من أهم المراكز التجارية في الساحل الشرقي من أفريقيا، وكانت معروفة لدى الإغريق والرومان منذ أكثر من ألفي عام، وقد سميت عند الإغريق باسم (سيرابيون)، واشتهرت بوصفها مدينة تجارية تأتي إليها السفن محملة بالسلع والبضائع من مختلف البلدان، ولتحصين المدينة المطلة على المحيط الهندي تم إنشاء سور يحيط بها من جميع الجهات مبني من الحجر مما زاد من تحصيناتها الدفاعية

الحصون في الجزء الشمالي الشرقي من الصومال

كان الساحل الشمالي الشرقي من الصومال من أكثر المناطق التجارية ازدهارًا وقد نجحت سلطنة ماجيرتين في القرن الثامن عشر الميلادي في بسط سيطرتها على هذه المنطقة المهمة، وأصبحت حلقة الوصل بين البر الصومالي والمحيط الهندي، ومن خلال مدنهم المحصنة تمكنوا من السيطرة على تجارة التوابل في المنطقة مع شبه الجزيرة العربية والهند

الفصل التاسع

المتشابهات المعمارية في حوض البحر الأحمر

هناك شبه كبير بين موانئ **سواكن وجدة ومصوع** وهي من الموانئ المهمة والاستراتيجية على ساحل البحر الأحمر وتتمثل أوجه الشبه بين هذه الموانئ الثلاثة في أنها تطل على البحر الأحمر في دائرة، وهي من أقدم وأعرق الموانئ على ساحل البحر الأحمر، وتتميز مدنها بشكلها البيضاوي، ويتشابه طرازها المعماري بصورة كبيرة، وتعرضت في فترات عديدة للاحتلال من قبل البطالمة والمماليك والبرتغاليين والعثمانيين والبريطانيين وغيرهم، وكانت هذه الموانئ الثلاثة في فترة الحكم العثماني تحت إدارة واحدة، وهناك علاقة كبيرة بين المجموعات السكانية فيها

مقارنة بين مينائي جدة وسواكن

يوجد تشابه كبير بين مدينتي ومينائي جدة وسواكن عبر التاريخ، من حيث شكل المعمار وطريقة البناء والأبواب والمشربيات، والحجارة والأخشاب التي بنيت بها المنازل والمرافق الخدمية في المدينتين، والشبه كبير في طريقة البناء وشكله داخل المدينة وأيضًا المساجد والمرافق العامة، وكذلك الإطلالة على ساحل البحر الأحمر، وشكلهما شبه بيضاوي أو دائري، وكذلك في السور الذي تم تشييده حول المدينتين لغرض الحماية، وأيضًا البوابات في السور، فمدينة جدة بها ثمانية أبواب ولمدينة سواكن ستة أبواب، ووجه الشبه الآخر أن ميناء جدة أقدم موانئ المملكة العربية السعودية وميناء سواكن من أقدم الموانئ السودانية. ويمكن القول إن مدينتي جدة وسواكن مدينتين توءمتين على ضفتين مختلفتين من البحر الأحمر، لكنهما يشابهان بعضهما بعضًا في الجغرافية والتاريخ والتطور الحضاري

المتشابهات بين قلعة الصيرة في عدن وباب مكة في مدينة جدة

الشبه كبير جدًّا في شكل العمارة وطريقة البناء وشكل الطوب بين قلعة صيرة في عدن وبوابة جدة التاريخية، وهذه القلعة من القلاع الدفاعية، ويتضح ذلك من شكل البناء وسمكه وتزويدها بالمدفعية كل ذلك يؤكد على أنها من القلاع الدفاعية

المتشابهات المعمارية بطابية محمد قول في السودان وقلعة أملج في السعودية

هناك شبه بين طابية محمد قول بشرق السودان وقلعة أملج بالسعودية، فبنائهما من الحجارة، المتميز بالمتانة، وبوابتيهما من الحديد، وتوجد فيهما نوافذ، وتتكونان من طابقين أو دورين، وتوجد في الطابق الأرضي في كل منهما فتحات صغيرة

المتشابهات في البوابات

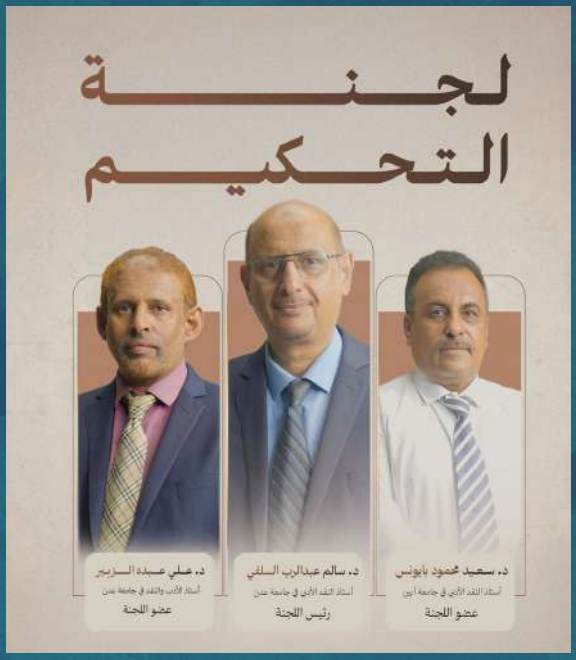
تتميز مدن ساحل البحر الأحمر بكثرة بواباتها التي أصبحت من السمات الحضارية والمعمارية لهذه المدن، فيوجد شبه كبير بين بواباتها إلى حد يثير الدهشة والإعجاب، ومن هذه البوابات بوابة ينبع البحر بالمملكة العربية السعودية وبوابة السلطان علي دينار بمدينة الفاشر غرب السودان ومن أوجه الشبه بين البوابتين: الشكل المستطيل للمدخل واتساعه، والبوابتان تمتازان بالمتانة والقوة، والسور الملحق بهما يمتاز بالمتانة والسماكة والقوة، ويوجد في أعلى بوابة ينبع غرفة للمراقبة ذات نافذتين وبوابة صغيرة، وفي أعلى بوابة قصر السلطان علي دينار مظلة مزينة بمجموعة من الأعواد ربما الغرض منها إضفاء ناحية جمالية على البوابة

وهناك شبه كبير بين بوابة عبد القيوم بمدينة أم درمان في السودان وبوابة مدينة الوجه في المملكة العربية السعودية، ويتمثل وجه الشبه بينهما في البوابتين والسورين المرتفعين، والارتفاع واحدة من مواصفات بوابات الحماية في المدن قديمًا، ويوجد في البوابتين شكل قوس، والبناء في السورين والبوابتين يتكون من الطوب والحجارة

ويتشابه برج ميناء الوجه في المملكة العربية السعودية وبوابة كتشنر بمدينة سواكن في السودان في الشكل والنوافذ والفتحات والمهام

برعاية إماراتية..

عدن تكتب بيتها الأول.. "أمير الشعراء"



في مدينة تتنفس الشعر وتكتب بالحبر والملح، عادت عدن لتفتح دفاترها البيضاء لمسابقة "أمير الشعراء"، برعاية وزارة الثقافة الإماراتية، وبمشاركة لجنة تحكيم أكاديمية، لتكون الكلمة هذه المرة هي الحدث، والمجاز هو المرسى

المسابقة، التي تُقام لأول مرة في عدن (العاصمة)، تمنح جوائز تصل إلى 150,000 ريال سعودي للفائزين الخمسة الأوائل، لكنها - في الحقيقة - تمنح ما هو أثمن: فرصة لأن يُسمَع الشعر، وأن يُصدّق، وأن يعود لمكانه الطبيعي فوق المنابر وبين الناس

لجنة التحكيم يترأسها أ. د. سالم عبدالرب السلفي، أستاذ النقد الأدبي بجامعة عدن، وعضوية كل من أ. د. سعيد محمود بايونس، أستاذ النقد الأدبي بجامعة أبين، أ. د. علي عبده الزبير، أستاذ الأدب والنقد بجامعة عدن، وأشراف الشاعر المعروف فهد بن جعموم

وقد بدأت اللجنة عملها في فرز النصوص المتقدمة لاختيار الشعراء المتأهلين، ضمن مراحل تنافسية تبدأ بـ64 شاعرًا وتنتهي بتتويج واحدٍ فقط "أمير الشعر"

لكن عدن، التي استقبلت الشعراء ببحرها الحالم، لا تبحث عن أمير واحد. هي تبحث عن زمن شعري جديد، عن جملة تُكتَب فلا تُمحى، عن بيت شعر يسند ذاكرة مدينة ويوقظ قلب قارئ