: https://doi.org/10.25130/tjfps.v4i30.99

TJFPS

ISSUE 30

IRAQI Academic Scientific Journals

العراقية المجلات الاكاديمية العلمية

ISSN: 2663-9203 (Electronic)
ISSN: 2312-6639 (print)

Contents lists available at:
http://tjfps.tu.edu.iq/index.php/poiltic

Tikrit Journal For Political Science

Tikrit Journal For Political Science SINCE 2014

مؤسسات الفضاء السيبراني في منطقة الشرق الاوسط : ايران وإسرائيل انموذجاً

" Cyberspace Institutions in the Middle East: Iran and Israel as a model "

Hiba a. khattab Alnasiry [a]
Muthanna Faeq Merei [a]
[a] Tikrit University / College of Political Science

الباحثة هبه عبد السلام خطاب الناصري [a] *
أ.د مثنى فائق مرعي [a]
[a] جامعة تكريت/ كلية العلوم السياسية

Article info.

Article history:
- Received: 20\08\2022
- Accepted: 22\10\2022
- Available online :31\12\2022

Keywords:
- Iran
- Israel
- cyber
- institutions
- strategy

Abstract: The trend towards enhancing cyber capabilities is one of the priorities of the Iranian and Israeli governments, especially in recent years, which witnessed great competition between them in the context of preserving vital interests and expanding influence, as Iran sought through developing cyber capabilities not only for defensive or offensive purposes, but also to limit the freedom of information flow To the citizens, which caused the outbreak of revolutions, most notably those that occurred in 2009, in contrast to Israel, which supported the development of national cyber capabilities with the aim of maintaining superiority in the electronic field over other neighboring countries, as well as providing another factor to deter others in the event of entering into a cyber confrontation, especially by Iran.

*Corresponding Author: Researcher Hiba a. khattab Alnasiry & Prof. Dr. Muthanna Faeq Merei, hiba.a@st.tu.edu.iq , muthannaf@tu.edu.iq, Affiliation: Tikrit University/ College of Political Science

معلومات البحث:

تواريخ البحث:
الاستلام: 20\08\2022
القبول:22\10\2022
النشر :31\12\2022

الكلمات المفتاحية:
- **ايران**
- **اسرائيل**
- **السيبرانية**
- **المؤسسات**
- **الاستراتيجية**

الخلاصة: يعد التوجه نحو تعزيز القدرات السيبرانية من أولويات الحكومة الإيرانية و(الإسرائيلية) لاسيما في السنوات الأخيرة التي شهدت تنافساً كبيراً بينهما في سياق المحافظة على المصالح الحيوية وتوسيع النفوذ، اذ ان أيران سعت من خلال تطوير الإمكانيات السيبرانية ليس فقط لأغراض دفاعية أو هجومية بل للحد من حرية تدفق المعلومات الى المواطنين والتي تسببت في اندلاع ثورات كان ابرزها تلك التي حدثت عام 2009، بعكس من (إسرائيل) التي دعمت تطوير الإمكانيات الوطنية السيبرانية بهدف المحافظة على التفوق في المجال الإلكتروني على غيرها من دول الجوار؛ فضلاً عن توفير عامل اخر لردع الأخرين في حال الدخول في مواجهة سيبرانية لاسيما من قبل ايران.

المقدمة:

تعد ايران و(إسرائيل) من أوائل الدول في الشرق الأوسط التي أخذت على عاتقها الاهتمام بالفضاء والامن السيبراني منذ تسعينيات القرن العشرين، بالتوازي مع التطور العلمي التكنولوجي الذي اجتاح العالم نتيجة العولمة، اضف الى ذلك استطاع كلا البلدين الوصول الى شبكة الانترنيت والتكنولوجيا الحديثة في المجال الالكتروني قبل غيرهم من الدول الاخرى، فضلاً عن قيام حكومات كلا البلدين بدعم العديد من المؤسسات من اجل تعزيز القدرات السيبرانية بشقيها الهجومية والدفاعية من اجل حماية البنى التحتية الوطنية والمؤسسات الحكومية، لذا ان هذا البحث جاء لبيان ابرز المؤسسات السيبرانية والكشف عن ملامح الاستراتيجيات السيبرانية الايرانية والاسرائيلية.

اولاً. أهمية البحث: تكمن اهمية البحث من خلال الاتي:

- تسليط الضوء على المؤسسات السيبرانية الايرانية والاسرائيلية كونها الاكثر تطوراً في منطقة الشرق الاوسط في هذا المجال ، علاوةً على ان ايران و(اسرائيل) اكثر الدول اهتماماً بالمجال السيبراني.
- افتقار المكتبة العراقية لهذا النوع من الدراسات السياسية لاسيما في المجال والمؤسسات السيبرانية التي قلما تم تناولها من قبل الباحثين العراقيين.
- الكشف عن طبيعة الاستراتيجية السيبرانية الايرانية والإسرائيلية.

ثانياً. إشكالية البحث: تقوم اشكالية الدراسة على ان كل من ايران و(اسرائيل) تبحث عن عناصر جديدة للقوة لتعزيز استراتيجيتها في المجال الاقليمي والدولي بهدف تحقيق اهدافهما في ظل تزايد التحديات الداخلية والخارجية، ومن هذه الاشكالية الرئيسية تتفرع عدة تساؤلات فرعية اهمها:

- ما هي المؤسسات السيبرانية الايرانية والاسرائيلية؟
- ما طبيعة الاستراتيجية السيبرانية الايرانية والاسرائيلية؟.

ثالثاً. فرضية البحث: ينطلق هذا البحث من فرضية تتضمن أن لكل من ايران و(اسرائيل) العديد من المؤسسات الفاعلة في المجال السيبراني واستراتيجية تسعى من خلالها للوصول الى اهم اهدافها؛ الا وهي حماية فضائها السيبراني من الهجمات التي تتعرض لها سواء كانت هذه الهجمات داخلية او خارجية، فضلاً عن محاولة القضاء على الخصوم من خلال شن هجمات سيبرانية.

رابعاً. مناهج البحث: بهدف اثبات فرضية البحث سيتم استعمال المنهج الوصفي والتحليلي في دراسة وتتبع مضامين هذا البحث.

خامساً. حدود البحث: تتقسم حدود البحث الى:

- الحدود الزمانية: يركز البحث على القوة السيبرانية الايرانية والاسرائيلية منذ مطلع القرن الحادي والعشرين.
- الحدود المكانية: يتحدد النطاق المكاني للبحث في الفضاء السيبراني الايراني والاسرائيلي.
- الحدود الموضوعية: تتمحور الحدود الموضوعية للبحث حول المؤسسات السيبرانية الايرانية والاسرائيلية، فضلاً عن الاستراتيجية السيبرانية الايرانية والاسرائيلية.

سادساً. هيكلية البحث: يقسم البحث الى مقدمة ومبحثين، تناول المبحث الاول: القوة السيبرانية الايرانية، كما تضمن هذا المبحث مطلبين، المطلب الاول ركز على المؤسسات السيبرانية الايرانية، بينما عالج المطلب الثاني الاستراتيجية السيبرانية الايرانية، اما المبحث الثاني فقد تضمن: القوة السيبرانية الاسرائيلية، وتضمن هذا المبحث مطلبين، ركز المطلب الاول على المؤسسات السيبرانية الاسرائيلية، بينما تناول المطلب الثاني الاستراتيجية السيبرانية الاسرائيلية، كما تضمن البحث خاتمة كخلاصة لأهم ما تم التوصل اليه من استنتاجات علمية .

المبحث الأول: القوة السيبرانية الإيرانية

تمتلك ايران العديد من المؤسسات التي تعزز امنها السيبراني ومؤسساتها من الهجمات الإلكترونية التي تتعرض لها سواء كانت من قوى دولية أو إقليمية، اضف الى ذلك امتلاكها استراتيجية سيبرانية لها ابعاد هجومية ودفاعية تسعى من خلالها تحقيق اهدافها، سيتم تقسيم هذا المبحث الى مايلي:

المطلب الاول: المؤسسات السيبرانية الايرانية: تشمل هذه المؤسسات العديد من الجهات وهي:

1. **المجلس الأعلى للفضاء السيبراني (SCC)** : كما يعرف هذا المجلس بأسم (المجلس الأعلى للفضاء الإلكتروني) ومهمة المجلس هي تنسيق الفضاء السيبراني الايراني كما تقوم بتنسيق العمليات السيبرانية الهجومية والدفاعية.[1]

أسس هذا المجلس في عام 2012 برئاسة رئيس الجمهورية الإسلامية، والوزراء الرئيسيين، والقائد العام لقوات حرس الثورة الإسلامية، وقائد الشرطة، ورئيس منظمة الدعوة الإسلامية، ورئيس الإذاعة التي تديرها الدولة، وشبكات التلفزيون (IRIB)، ورئيس اللجنة الثقافية في مجلس النواب وسبعة آخرين وقد عينوا بشكل مباشر من قبل (علي خامنئي).[2]

2. **كتائب الباسيج السيبراني (Basij Cyber Council)**: كتائب الباسيج تابعة للحرس الثوري الإيراني وهـدفها هو حمـــاية مسؤولي الدولة ودعم النظام الايراني ضد المعارضين من خلال شبكات التواصل [3]

تتكون كتائب الباسيج من عناصر غير محترفين، يعملون تحت إشراف متخصص في الحرس الثوري, يطلق عليهم أسم (كوماندوز الحرب السيبرانية)، وأهم الأنشطة التي تقوم بها هي شبه العسكرية وتقوم هذه الكتائب بنشر منشورات تدعم النظام ورئيس الجمهورية الإسلامية على المدونات الخاصة بهم وكتابة تعليقات على المنشورات التي تنتقد الحكومة .[4]

---

1. Congressional Research Service Informing the legislative debate since 1914, Iranian Offensive Cyber Attack Capabilities, 13/1/2020, P1.

2. Radio Farda, Iran Cyberspace Supreme Council Among 20 Worst Digital Predators in 2020, 12/3/2020, in: https://bit.ly/3G4HBfe, (18/5/2022).

3. ايهاب خليفة، قدرات إيران الإلكترونية بين التهوين والتهويل، مركز المستقبل للأبحاث والدراسات المتقدمة، 2014/8/20، في : (2022/5/18) https://bit.ly/3sLic4O.

4. مصطفى كمال، مُختصر التعريف بالقدرات السيبرانية الإيرانية، مركز الانذار المبكر، 2020/8/20، في: https://bit.ly/3wpMU5x,(18/5/2022).

3. **المركز الوطني للفضاء السيبراني (National Cyberspace Center)**: ان المركز الوطني قام بإنشائه المجلس الأعلى للفضاء السيبراني وان مهمته هي متابعة الاحداث والتطورات التكنولوجية والسياسية من خلال الفضاء السيبرانية واصدر المركز الوطني للفضاء السيبراني الايراني قانون في 13 ايلول 2013 يتضمن مايلي :[1]

أ- تقليل اعتمادهم على انترنيت الدول الاخرى من خلال تطوير مواقع الويب الايرانية والقدرات السيبرانية الايرانية.

ب-قيامها في عملية توعية المواطنين لحماية مواقعهم الشخصية.

ت-دعم المنتوجات المحلية من خلال الانترنيت.

ث-تطوير محتوى الانترنيت لغرض دعم الايدلوجية الدينية ومساندة الدولة.

ج-الاستعداد للحرب الثقافية التي تشنها ايران ضد اعدائها.

ح-اعادة تنظيم تبادل المعلومات مع الشبكة الدولية.

خ-القيام بحماية الدولة من الهجمات السيبرانية التي تُشن ضد ايران.

4. **الجيش السيبراني الإيراني (The Iranian Cyber Army)** :ان الجيش السيبراني الإيراني يتكون من مجموعة متخصصين ذوي مهارات عالية في تكنولوجيا المعلومات ومتسللين محترفين غير معروفة هويتهم، واحدى القدرات التقنية للجيش السيبراني الإيراني هي اختراق الكثير من وسائل الإعلام الأجنبية وكذلك Twitter وبعض المواقع الحكومية الاجنبية.[2]

5. **مركز التحقيق في الجريمة المنظمة(Center to Investigate Organized Crime)**:تم أنشاء المركز في عام 2007 ويسمى بـ (مكتب الجرائم الإلكترونية) وهو تابع للحرس الثوري الإيراني، مهمته ضمان أمن الفضاء السيبراني لإيران.[3])

1. 'Iranian Internet Infrastructure and Policy Report', smallmedia.org.uk, February/ 2014, p 4.
2. Sommaire, Structure of Iran's Cyber Warfare, Institute Francais D'analyes Strategique, in: https://bit.ly/3GjumaC, (26/5/2022) .
3. Gerdab: A Dictated Scenario; Systematic Torture to Obtain Televised Confessions, Justice for Iran, 1/6/2012, in: https://justice4iran.org/8815/, (29/5/2022).

6. **وزارة المخـــابرات والأمـــن (MOIS) (Ministry of Intelligence and Security)**: تستخدم وزارة الاستخبارات والأمن كافة الوسائل المتاحة لها لحماية الثورة الإسلامية الإيرانية، باستخدام أساليب مثل اختراق المعارضة الداخلية ومراقبة التهديدات المحلية والمعارضين المغتربين واعتقال الجواسيس والمنشقين وفضح المؤامرات التي تعتبر تهديداً لأمنها والحفاظ على الاتصال مع الآخرين مثل وكالات الاستخبارات الأجنبية وكذلك مع المنظمات التي تحمي مصالح ايران حول العالم، وان جميع المنظمات تشارك كافة المعلومات مع الوزارة وتشرف على جميع العمليات السرية، وعادة تقوم الوزارة بتنفيذ بعض العلميات داخل ايران.[1]

7. منظمة الحرب الإلكترونية والدفاع السيبراني (**Electronic Warfare and Cyber Defense Organization**): ان هذه المنظمة تابعة لقوات الحرس الثوري الايراني، وتقوم هذه المنظمة بدورات تدريبية في الدفاعات السيبرانية, وحماية البنية التحتية للدولة من التهديدات السيبرانية.[2]

8. المنظمة الوطنية للدفاع السلبي **(National Passive Defense Organization)**: انشئت من قبل الحرس الثوري الإيراني في عام 2003 كوسيلة للدفاع عن الجبهة الداخلية من التحديات الأيديولوجية، مهمتها هي ابقاء السيطرة على المدن خلال الاضطرابات الداخلية كما تتولى السيطرة على العديد من أنشطة الحرب السيبرانية للحرس الثوري الإيراني.[3]

تقوم هذه المنظمة باستغلال كافة الموارد الإلكترونية وغير الإلكترونية الوطنية لردع ومنع وتحديد والتصدي بفعالية لأي هجوم إلكتروني على البنى التحتية لإيران ضد القوى الخارجية او الداخلية وبسبب طبيعة النظم الاستبدادية أصبحت مهمة هذه المنظمة هي مواجهة أي استياء داخلي أو مطالبة علنية بالحريات المدنية، بما في ذلك عبر شبكة الإنترنت، واهتمت منظمة الدفاع السلبي بشكل خاص بمواجهة "قوة الإجبار"، وهو مفهوم قامت باقتراحه منظمة "راند" في دراسة أجرتها عام 2016 والتي تشمل استخدام الوسائل غير المميتة لإرغام الخصم على الإذعان .[4]

1.The Library of Congress, **Iran's Ministry of Intelligence and Security: A profile** (**Washington,** December 2012), P1.

2. Congressional Research Service Informing the legislative debate since 1914, Op.cit, P1.

3. Gholam Reza Jalali, Iran: Passive Defense Organization and Basij Sign Memorandum of Understanding, Middle East, North Africa, 9/2020, P47.

4. Farzin Nadimi, Iran's Passive Defense Organization: Another Target for Sanctions The Washington institute for near east policy internship, Washington,16/8/2018, in:

9. فيلق الحرس الثوري الإسلامي **(Islamic Revolutionary Guard Corps) (IRGC)**: هو فرع من القوات المسلحة الإيرانية، تقوم هذه القوة العسكرية بالاشراف على الأنشطة السيبرانية الهجومية.[1]

10. قيادة الدفاع السيبراني. تسمى هذه المجموعة بإسم المقر السيبراني في الجيش الإيراني وتقوم بعمليات هجومية عبر الإنترنت الى جانب كتائب الباسيج الإلكترونية.[2]

11. هيليكس كيتن **(HELIX KITTEN)** : وهي مجموعة من القراصنة تتعاون مع الحكومة الايرانية وخاصة مع وزارة المخابرات الايرانية وبدأت نشاطاتها عام 2015 .[3]

يعتقد خبراء الأمن السيبراني ان هيليكس كيتن واحدة من أكثر أجهزة APT الإيرانية نشاطاً في السنوات الأخيرة، وان المجموعة متخصصة في حملات التجسس السيبراني التي تتوافق مع مصالح الحكومة الإيرانية وانها عكس المجموعات الإيرانية الأخرى لا تقوم بتجسس إلكتروني على أهداف محلية إيرانية، انما تقع الأهداف الأساسية للمجموعة في الشرق الأوسطكما شنت هجمات على كيانات في إفريقيا والولايات المتحدة الامريكية .[4]

12. القطة الساحرة **(Charming Kitten)**: هي مجموعة تجسس إلكترونية إيرانية مارست نشاطاتها منذ عام 2014، وان أهدافها الأساسية هي نشطاء حقوق الإنسان والعاملين في وسائل الإعلام، كما ان معظم ضحاياها في الشرق الأوسط والولايات المتحدة والمملكة المتحدة.[5]

انها تقوم بانتحال صفة مواقع التواصل الاجتماعي واستخدام هذه المنصات لتوزيع روابط خبيثة وإرسال رسائل نصية مباشرة إلى الجهاز الخلوي للضحية.[6]

---

https://bit.ly/3PMjzdl ,(29/5/2022).

1. Michael N. Schmitt, Noteworthy Releases of International Cyber Law Positions/ PART II: Iran, Lieber Institute, 27/8/2020, in: https://bit.ly/3aaMBTK, (29/5/2022).

2. Congressional Research Service Informing the legislative debate since 1914, Op.cit, P1.

3. Matthew Armelli, Stuart Caudill and others, The Impact of Information Disclosures on APT Operation,2020. P42.

4. Marie Baezner, *Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions* (Zürich: Center for Security Studies, 2019), P6-10.

5. The Kittens Are Back in Town: Charming Kitten Campaign Against Academic Researchers, Clear Sky Security, September 2019, P3.

6. Emiel Haeghebaer, Iran's decade of credential harvesting and surveillance operations, Virus Bulletin Conference, 7-8/10/2021 ,P2.

13. القط الطائر **(Flying Kitten)**: بدأت أنشطتها خلال السنوات 2009–2010 كمجموعة قرصنة وطنية بأسم AjaxTM، و تخصصت المجموعة في البداية في تشويه موقع الويب لإثبات مهارات القرصنة لديهم، ان المهارات التقنية لـ Flying Kitten ليست معقدة للغاية، ولكنها تستخدم برمجياتها الخبيثة المصممة خصيصاً لها .[1]

14. مجموعة شمعون **(Shamoon Group)**: تعرف بأسم (Dist Track) وهي مجموعة تمتلك برامج ضارة شديدة التدمير تُستخدم في الحرب السيبرانية، منذ عام 2012 شنت هجوم ضد أهداف في الشرق الأوسط واهمها على المملكة العربية السعودية وكانت الأهداف الرئيسية تستهدف قطاع الطاقة وخاصة النفط والغاز ، ولكن في الآونة الأخيرة قامت بهجمات ضد نطاق أوسع من الصناعات، وبحلول عام 2012 استهدفت مجموعة شمعون الأولى شركة أرامكو السعودية ويقال انه أكبر اختراق في التاريخ في ذلك الوقت، ادت الى مسح أكثر من 30.000 محطة عمل و 2000 خادم وإجبار الشركة على قطع إنتاج النفط، وأنهم اضطروا إلى وقف إنتاج النفط لأكثر من شهر .[2]

15. مجموعة القطة الصاروخية **(Rocket Kitten)** أو **(Rocket Kitten Group)**: تختص هذه المجموعة بالقرصنة الالكترونية التي تتميز بالجدارة التقنية غير المتطورة نسبياً ضد المنظمات والأفراد في الشرق الأوسط ولا سيما (إسرائيل) والسعودية فضلاً عن جميع أنحاء أوروبا والولايات المتحدة الامريكية وكذلك الأهداف داخل إيران نفسها واخترقت العديد من هذه الأهداف بنجاح بواسطة البرامج الضارة المتنوعة وعلى الرغم من تحديد البنية التحتية الخاصة بهم والإبلاغ عنها، الا انهم قاموا بالضرب مراراً وتكراراً من خلال إجراء تغييرات طفيفة على أدواتهم أو مجالات التصيد .[3]

16. معهد مبنا **(Mabna Institute)**: تقوم هذه مجموعة بعمليات تهكير الكمبيوتر والاحتيال الإلكتروني وسرقة البيانات بطلب من الحكومة الايرانية والحرس الثوري الإيراني ويقومون باختراق أنظمة مئات الجامعات والشركات، لسرقة البحوث والبيانات الأكاديمية والملكية الفكرية، اذ سرقوا أكثر من 31

1. Marie Baezner,Op.cit, P10.
2. The link between Kwampirs (Orangeworm) and Shamoon APTs, Cylera, January, 2022, P5.
3. Rocket Kitten: A campaign with 9 Lives, Check Point Software Technologies, 2015, P3.

تيرابايت من الوثائق والبيانات من أكثر من 140 جامعة أمريكية و30 شركة أمريكية، وخمس وكالات حكومية أمريكية، وأكثر من 176 جامعة في 21 دولة أجنبية .[1]

المطلب الثاني: الاستراتيجية السيبرانية الإيرانية: عملت ايران على تبني استراتيجية سيبرانية، لذا سيتم التطرق في سطور قليلة حول اهم مميزات استراتيجية ايران التي تميزها عن استراتيجية خصومها، ومن خلالها تسعى الى تحقيق أهدافها المنشودة.

منذ الثورة الإيرانية وتأسيس الجمهورية الإسلامية الحاليةفي عام 1979 كانت القيادة الإيرانية في صراع شبه دائم مع الغرب والعديد من جيرانها في الشرق الأوسطونتيجة لافتقارها إلى القوة العسكرية والاقتصادية التي تحتاجها لمواجهة خصومها الغربيين، نظرت الحكومة الإيرانية إلى (الإنترنت) كأداة غير متكافئة لإلحاق الضرر بأعدائها وجمع المعلومات بشكل فعال عن الحكومات والشركات والمؤسسات الأكاديمية والمنظمات غير الحكومية الأجنبية خارج بلدها، فضلاً عن مواطنيها، اذ كان يُنظر إلى أجهزة الاستخبارات الإيرانية ذات مرة على أنها (هواة للفضاء السيبراني)، وقد عملت بشكل مستمر وواضح لكي تقوم بتنمية خبرتها الإلكترونية المحلية وقدراتها في القرصنة الإيرانية، وبالرغم من انه لا يُنظر إلى المشغلين السيبرانيين الإيرانيين على أنهم من الدرجة الأولى من حيث تطورهم التقني، وبعكس النظام الايراني الذي ابدى استعداده لإجراء عمليات سيبرانية عدوانية ومدمرة يزيد بشكل كبير من التهديد المحتمل الذي تتعرض له تلك الشركات التي تجد نفسها في مرمى هذه النيران، وأن خطة النظام الايراني قد اكتملت وأن الإنترنت أصبح مكوناً أساسياً كاملاً في استراتيجية إيران لكي تضايق وتنافس وتعاقب خصومها في جميع أنحاء الشرق الأوسط والعالم.[2]

ان الأنشطة السيبرانية الإيرانية لها أبعاد هجومية ودفاعية، أذ وفرت القدرات السيبرانية الهجومية الإيرانية خياراً منخفض التكلفة لقادة إيران لرد ع التهديدات الخارجية وإدارتها، ويعترف المسؤولون الأمريكيون والباحثون

1. Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps, Department of Justice, 23/3/2018, in: https://bit.ly/3xi3lRW,(4/6/2022).
2. Adam Hlavek, Strategic goals behind Iranian cyber attacks , Security Bloggers Network, 26/10/2020, in: https://bit.ly/3xIOT5P, (11/6/2022).

المختصون بأن إيران من بين أكثر الدول تقدماً من ناحية الامكانيات السيبرانية ولا توجد استراتيجية سيبرانية شاملة ومعلنة للفضاء السيبراني الايراني.[1]

تسعى إيران إلى أعادت تشكيل نفسها بعدها قوة إقليمية من خلال تدخلها بهدوء في الصراعات المحيطة، وتستفيد من مجالها السيبراني لكي تشن حرب ناعمة ضد الخصوم، وانخرطت ايران في الكثير من العمليات السيبرانية المدمرة والعمليات التي تستخدمها للتجسس .[2]

ان برنامج الدفاع السيبراني الإيراني له هدفين يتمثل الاول بمنع الهجمات التي تستهدف البنى التحتية الايرانية لاسيما المؤسسات الحيوية (النووية) بواسطة الفايروسات مثل فايروس "ستاكنست" وثانياً السعي لمراقبة وحجب تدفق المعلومات خاصة التي ينظر اليها النظام الايراني كخطر مهدد لوجوده.[3]

ان ايران لديها عدة أهداف أساسية في مجال الحرب السيبرانية وهي: الدفاع عن بنيتها التحتية الحيوية وبياناتها الحساسة من الهجمات السيبرانية، فضلاً عن مراقبة الأنشطة عبر الإنترنت والرد عليها داخل بلدها، وتنفيذ عمليات هجومية إلكترونية، و في عام 2011 خصص النظام الايراني مبلغ مليار دولار لتعزيز القدرات السيبرانية للبلاد وبهدف الاستثمار في التقنيات الحديثة وتوظيف وتدريب كادر من الخبراء السيبرانيين [4]

تجدر الاشارة الى ان ايران لجئت الى تطوير قدراتها السيبرانية لتقليل الخسائر المالية بعد ان كانت ذات تكلفة، علاوة على ذلك احداث اضرار جسيمة بمواقع الخصوم.[5]

فرضت عقيدة الأمن السيبراني الايراني نفسها في اطار استراتيجية الأمن القومي الايراني واستندت على ركيزتين؛ الاولى تمثلت بحماية الأمن الوطني الايراني عبر بناء بنية تحتية علمية تقنية واستخباراتية تقوم على استراتيجية وقائية في الدفاع واستراتيجية استباقية في الهجوم في المجال السيبراني، والثانية تمثلت

---

1. Paul Bucala and Caitlin Shayda Pendleton, Iranian Cyber Strategy: A View from the Iranian Military, 24/11/2015, in: https://bit.ly/3xrJq3d ,(7/6/2022).
2. Jason G. Spataro," Iranian Cyber Espionage", Master of Science in Cyber security , Utica University, New York, 2019,P4.
3. Gabi Siboni and Sami Kronenfeld," Iran and Cyberspace Warfare", **Military and Strategic Affairs**, The number 3 (Israel: 2012), P77.
4 . The Iranian Cyber Threat, United Against Nuclear Iran, December 2020, P4.
5. القدرات السيبرانية الإيرانية (الحرب الأخرى بين إيران وخصومها)، مجلة اتحاد الديمقراطيين السوريين، 2021/2/2، في : https://bit.ly/3mLUYbf, (14/6/2022).

بتطوير مجموعة من المفاهيم والتقاليد القتالية السيبرانية من خلال تشكيل شبكة معقدة من الجيوش الالكترونية التي تقوم بشن هجمات سيبرانية متنوعة على اهداف محددة في وقت واحد, وكذلك تقوم بتفعيل قدراتها الاستخبارية في نشر المعلومات المضللة للقضاء على الحركات المناهضة لإيران، وفي عام 2009 ادخل اسم ايران من قبل شركة "American security" بين الدول التي تمتلك أقوى قدرات انترنت في العالم.[1]

خلاصة القول مما تقدم:

ان الادوات السيبرانية هي إحدى الأدوات المهمة لحكومة إيران، كونها وفرت فرصاً أقل خطورة وأدنى تكلفة بالنسبة لإيران لجمع المعلومات وتوجيه ضربات لأعدائها داخل البلاد وخارجها وخاصة ان ايران تعاني اقتصادياً بسبب العقوبات المفروضة عليها، كما تبين لنا ان للاستراتيجية السيبرانية الايرانية لها ابعاد دفاعية وهجومية، وان الابعاد الدفاعية تمثلت بحماية مؤسساتها و البنى التحتية من الهجمات السيبرانية التي تتعرض لها وخاصة عندما تعرضت الى هجمات اصيبت المفاعلات النووية الايرانية، اما الابعاد الهجومية لايران كانت لغرض قيامها بهجمات سيبرانية خارج ايران وداخلها، اذ سعت من خلالها في تحقيق اهدافها وفي نشر رسالتها الثورية ومواجهة المعارضون لها.

المبحث الثاني: القوة السيبرانية (الاسرائيلية)

سعت (اسرائيل) في السنوات الاخيرة لتعزيز امكانياتها السيبراني؛ اذ اتجهت الى تطوير هذه الامكانيات وذلك من خلال رسم استراتيجية سيبرانية شاملة وانشاء مؤسسات سيبرانية لحماية البنى التحتية وتحقيق اهدافها الداخلية والخارجية والحفاظ على مكانتها، وسنقسم هذا المبحث الى ما يلي:

المطلب الاول: المؤسسات السيبرانية الاسرائيلية: لدى (اسرائيل) العديد من المؤسسات ومهمتها دعم وتعزيز فضائها السيبراني وحماية امنها السيبراني والبنى التحتية من الهجمات التي تتعرض لها سواء كانت دولية او اقليمية، فيمكننا تقسيم هذه المؤسسات الى مايلي:

[1]. كرار عباس متعب فرج، "الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وإيران"، مجلة حمورابي للدراسات، العدد40 (بغداد: 2021)، ص213.

1. الوحدة (8200) الإسرائيلية: هي اكبر وحدة في الجيش الإسرائيلي وتوزاي وكالة الامن الوطني الامريكية وهي جهاز تجسس الكتروني عالي التقنية ويعدها المحللون الاستخباراتيون انها اقوى اجهزة التجسس عالمياً .[1]

ان مهام هذه الوحدة هي جمع المعلومات من خلال الادوات الاستخبارات التقليدية والحديثة وتركز على الاساليب التقنية التكنولوجية لجمع المعلومات وكما تقوم بفك رموز المعلومات التي جمعت في مجموعة متنوعة من اللغات الأجنبية، ويشترط للتقديم اليها التكلم باللغة العربية والفارسية، كما انها تقوم باختراقات للدول الأعداء مثل إيران وعدد من الدول العربية وخاصة دولة لبنان/ المنطقة الجنوبية كونها مصدر قلق للجبهة الشمالية في (إسرائيل) بسبب وجود تنظيم حزب الله، فضلاً عن الحدود التي تربطها مع سوريا اذ يوجد التنظيم.[2]

2. الوحدة (131): هي واحدة من الوحدات المعلوماتية التقنية تابعة للاستخبارات العسكرية الإسرائيلية, وعملها خارج حدود (اسرائيل) في الدول المحيطة بها, فهي تقوم بأعمال التجسس والتخريب وخاصة في الدول العربية المحيطة بها, وان هدفها هو زعزعة أمن البلدان العربية, فتقوم بتخريب علاقات الدول العربية فيما بينها من خلال ضربها احد الدول داخل الدولة المستهدفة.[3]

منذ بدء الثورات العربية في عدد من البلدان العربية قامت (اسرائيل) إلى إعادة تدريب ونشر هذه الوحدة, لكي تواكب التطورات الحاصلة في بلدان العالم العربي, وجمع المعلومات عن المستجدات الحديثة لهذه الثورات الشعبية .[4]

3. هيئة السايبر التابعة للجيش الاسرائيلي: تم انشائها من قبل الجيش الاسرائيلي ضمن وحدة8200 لتقوم بتوجيه وتنسيق الجيش في فضائها السيبراني، وأن هيئة السايبر هدفها هو حماية شبكات الإنترنت العاملة

---

1. جون ريد، "الوحدة 8200 : تعرف على ذراع اسرائيل في إدارة عمليات الامن السيبراني"، الايام (رام الله)، السبت 2021/2/13.

2. محمد الليثي، الوحدة 8200: تعرف على ذراع الاستخبارات الإسرائيلية للاختراق عن بُعد، مركز الانذار المبكر، 2021/03/16، في: (2022/6/22) https://bit.ly/3yceO60.

3. يوسف حسن يوسف، دماء على ابواب الموساد: دماء على أبواب الموساد: اغتيالات علماء العرب (القاهرة: سما للنشر والتوزيع، 2016)، ص14.

4. وليد غسان سعيد جلعود, "دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية, فلسطين, نابلس، 2013, ص155-156.

في (إسرائيل) التي قد تتعرض الى هجمات، وكذلك القيام بهجمات في الفضاء السيبراني على أهداف خارجية.[1]

4. البنية التحتية الحكومية لعصر الإنترنت: في عام 1977 أنشئت (اسرائيل) مشروع (بنية الحكومة التحتية لعصر الإنترنت) في داخل وزارتها المالية، وهدف المشروع هو حماية وتأمين استعمال الإنترنت في الوزارات والمؤسسات الحكومية، ولقد أقيم داخل هذا المشروع (مركز حماية المعلومات لحكومة إسرائيل) واعطيت له مهام متابعة تطور وسائل حماية المعلومات في العالم والتنسيق بين الوزارات والمؤسسات الحكومية لكي تجد حلول لمشاكل حماية المعلومات والقيام بأبحاث حول هذا الموضوع .[2]
5. السلطة الرسمية لحماية المعلومات: أنشئت في عام 2002 في داخل جهاز المخابرات العامة (الشاباك)، كما تسمى "الهيئة الحكومية لحماية المعلومات" ومن مهامها هي حماية البنى التحتية لاجهزة الحاسوب المهمة والحيوية وحماية الشبكات في (إسرائيل) من خطر التهديدات الإرهابية والانشطة التجسسية، وأن عمل السلطة الرسمية لحماية المعلومات يحتوي الكثير من النواقص كونه لا يشمل جميع المؤسسات والمنشآت في (إسرائيل) وهذه السلطة تابعة لجهاز المخابرات العامة (الشاباك)، مما يمنع الكثير من المؤسسات من التعامل والتفاعل معها بحرية.[3]
6. هيئة الأركان السيبرانية القومية: كلف رئيس حكومة (اسرائيل) رئيس المجلس القومي للبحث والتطوير في عام 2010، الجنرال (في الاحتياط) "اسحاق بن اسرائيل" بإعداد خطة عمل لإطلاق مبادرة وطنية لمواجهة التهديد السيبراني وجاء ضمن توصيات فريق المبادرة هو تشكيل "هيئة الأركان السيبرانية القومية" ومهمتها تشجيع حماية الفضاء السيبراني في (إسرائيل) وتعزيز القدرات وتحسين فرص مواجهة التحديات الحالية والمستقبلية في فضائها السيبراني، ولابد هنا من التأكيد هنا الى ان هيئة الأركان السيبرانية القومية وضعت خطة عمل شاملة في مجال الدفاع السيبراني وهدف هذه الخطة هو تعزيز إجراءات الحماية في المؤسسات بواسطة أداة منظمة شاملة تتلائم مع جميع المجالات، وصممت خصيصاً لحماية قواعد البيانات فضلاً

---

[1]. فيصل محمد عبد الغفار، الحرب الالكترونية (عمان: الجنادرية للنشر والتوزيع،2016), ص172- 173.

[2]. محمود محارب, حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل (الدوحة: المركز العربي للأبحاث و دراسة السياسات،2011)، ص5.

[3]. فيصل محمد عبد الغفار، مصدر سبق ذكره، ص171-172.

عن أهداف أخرى تشمل وضع برامج وطنية، والتعاون وتبادل المعلومات وخاصة بين المؤسستين الأمنية والمدنية، اذ تقوم بتصميم برامج شاملة وتعمل على تأسيس آليات لتطوير رأس المال البشري في المجال السيبراني، كما تعمل على تطوير البنى التحتية التكنولوجية والبحثية في الجامعات وفي قطاع الصناعة، و زيادة التعاون بين القطاع الحكومي والخاص، والصناعة والجامعات، والمؤسسات الأمنية والعسكرية، كما تقوم بتوعية الرأي العام حول التهديدات السيبرانية.[1]

7. فرق قرصنة الكمبيوتر: تتكون من نُخبة عناصر الجيش المختصة بالمجال المعلوماتي، ومهمتها مواجهة الحرب السيبرانية وعمليات القرصنة ضد الساحة الإسرائيلية, وتم اختيار ما يقارب (300) خبير تكنولوجي من عناصر الجيش للعمل ضمن فرق للقرصنة والحوسبة لحماية الشركات الوطنية الإسرائيلية من خطر الاختراق السيبراني مثل شركات الكهرباء والمياه والهاتف, فضلاً عن تعزيز قدرات قوات الجيش الإسرائيلي في الحروب السيبرانية وكما تقوم بتدريب عناصر جهازي الشاباك والموساد لفك رموز الشفرات المعلوماتية .[2]

8. وحدة الملك داود: وهي وحدة خاصة تابعة لقوات الجيش الاسرائيلي ومهمتها الحرب الإلكترونية وتقوم باختراق البث الإذاعي والتلفزيوني، كما أنها تخترق أجهزة الاتصالات والمراقبة للعدو والهدف الرئيسي من هذه الوحدة هو إزعاج العدو وتعطيل اتصالاته والعمل على إيصال رسائل لاسيما في أي عمليات اسرائيلية، وتقوم بالسيطرة على أي جهاز يستخدم ترددات الكترونية وان عمل هذه الوحدة ليس فقط داخل الغرف ولكنه يتم عبر البر والبحر والجو وحتى في الطائرات والسفن الحربية .[3]

9. وحدة الحرب الإلكترونية الاسرائيلية مع إيران: انشئها الجيش الإسرائيلي نتيجة تصاعد التوتر مع إيران وذلك للاستعداد لحرب المعلومات والتكنولوجيا من الناحية الدفاعية والهجومية، واختراق أجهزة الحاسوب في إيران, ان الوحدة (8200) تشرف على عمل وتدريب هذه الوحدة، وتخضع مباشرة إلى قيادة رئيس الحكومة,

---

[1]. جيل برعام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل، مؤسسة الدراسات الفلسطينية، في: https://bit.ly/3BaAWPd.

[2]. وليد غسان سعيد جلعود، مصدر سبق ذكره، ص160-161.

[3]. الترسانة النووية الصهيونية تاريخ ومكونات، الجيش العربي، 2014/4/11، في:(28/6/2022), https://bit.ly/3R47r8e .

وهدفها: اختراق منظومة الحواسيب الإيرانية في البرنامج النووي، وكذلك الجيش الإيراني، والقيام بتوجيه هجمات سيبرانية على البنية التحتية المدنية.[1]

10. وحدة إدارة أنظمة المعلومات: انشأت في عام في 2011 تحت إشراف مدير عام في وزارة المالية الإسرائيلية ومسؤولة بصورة مباشرة على جميع أنظمة الاتصالات المحوسبة الحكومية، بما في ذلك مشروع بنية الحكومة التحتية لعصر الإنترنت.[2]

المطلب الثاني: الاستراتيجية السيبرانية الاسرائيلية: سنتعرف على استراتيجية (اسرائيل) التي وضعتها لتكون في مصاف الدول الرائدة في مجال الفضاء السيبراني للوصول الى ما تبغى اليه.

تبنت (اسرائيل) استراتيجية سيبرانية وطنية وفقاً لقرار الحكومة المرقم 3611 لتعزيز القدرات الوطنية في الفضاء السيبراني و تهدف هذه الاستراتيجية إلى زيادة قوتها السيبرانية وتطوير التكنولوجيا السيبرانية كمحرك اساسي للنمو الاقتصادي والاستفادة من الأمن السيبراني لتعزيز التعاون الدولي وإنشاء مكتب السيبرانية الوطني الإسرائيلي والمعروف اختصاراً بـ (INCB) لتطوير وتنفيذ الاستراتيجية .[3]

ان استراتيجية الأمن السيبراني الإسرائيلية هي قبل كل شيء وسيلة للحفاظ على أمن الفضاء السيبراني وكذلك مواجهة التهديدات السيبرانية المختلفة، التي تهدد مصالحها الوطنية، فضلاً عن ان هذه الاستراتيجية تهدف إلى ضمان استمرار دور (إسرائيل) في الساحة الدولية كرائدة في الابتكار التكنولوجي وكشريك نشط في مواجهة العمليات السيبرانية.[4]

وتجدر الاشارة الى ان (اسرائيل) تبنت رؤية المديرية السيبرانية الوطنية كأساس لاستراتيجيتها التي تضمنت عدة خصائص ابرزها:[5]

---

[1] .الكيان الصهيوني ينشأ وحدة للحرب الإلكترونية مع إيران، المجد الأمني، في:
https://bit.ly/3uvlfxR, (28/6/2022) .

[2] . فيصل محمد عبد الغفار، مصدر سبق ذكره، ص 173.

[3]. The National Cyber-Strategy of Israel and the INCB, Springer Link, in:
https://bit.ly/3QYTeJD, (30/6/2022).

[4]. Israel National Cyber Security Strategy in Brief, National Cyber Directorate, Israel, September, 2017, P5.

[5] . فادي ميده، رضا النحاس، أحمد عرنوس، "دراسة حول القدرات الإسرائيلية في مجال الحروب السيبرانية"، **دراسات سياسية** (دمشق: مركز توازن للأبحاث والدراسات، 2020)، ص11.

1. متانة البنى التحتية: وهي الطبقة الأولى والأساسية التي تقوم عليها التقنيات التكنولوجية في العمليات الأمنية السيبرانية، والاستثمار فيها هو أرخص وأقل تكلفة من الطبقات الاخرى.
2. المرونة: تعتمد على افتراض تلقي الهجمات وفق سيناريوهات متعددة ونوعية، بغرض التعافي منها بأسرع وقت ممكن، وتحقيق أقل قدر من الأضرار.
3. الدفاع: تتكون هذه الطبقة من الجيش والمؤسسات والهيئات الأخرى التي تقوم بالمشاركة بالدفاع ضد الهجمات السيبرانية.

في عام 2015 طالبت وثيقة (استراتيجية الجيش الإسرائيلي) بتوفير دفاع متوازن في كافة الظروف وفي جميع مجالات المعارك وحتى في مجال السيبرانية و كما طالبت بتوفير معدات للدفاع في مجال السايبر وتقديم إمكانيات ومعدات لتواجه بها أي هجمات ممكن ان تتلقاها، واستخدمت السيبرانية للتأثير على الرأي العام ولحصولها الشرعية الدولية والدعم القانوني والمحافظة على التفوق الإعلامي بعد الحرب، اما في الجانب الهجومي وفرت القدرات السيبرانية امكانيات استخباراتية قوية وساهمت في الدعم اللوجيستي في حالة وجود هجمات سيبرانية، وأن تكون قادرة على القيام بحملات أمنية لمنع الهجمات السيبرانية.[1] استخدمت (اسرائيل) السيبرانية كسلاح في السلم والحرب على حد سواء، فالسيبرانية مهمة لجمع المعلومات وتحقق بعض الأهداف عبر العمليات العسكرية وان مجال السايبر تجانس مع مرتكزات العقيدة الأمنية والردع والحسم والإنذار والدفاع لإسرائيل.[2]

كما أنشئت (اسرائيل) القبة السيبرانية لردع الهجمات السيبرانية وهي نظام استباقي جديد للتنبؤ وصد الهجمات السيبرانية وتحديد التهديدات السيبرانية وحماية فضائها من مختلف المخاطر السيبرانية التي تتعرض لها الشبكات الإسرائيلية سواء كانت على الأنظمة التي يديرها الأفراد أو المؤسسات الحكومية أو الجيش أو القطاع الخاص، وان "القبة السيبرانية" لن تقوم بشن هجمات سيبرانية بل عملها هو تزويد جيش

1. باسل رزق الله، إسرائيل على الجبهة الإلكترونية، موقع متراس، 2019/7/23، في: https://bit.ly/3QUZaDk (1/7/2022).

2. المصدر نفسه.

الدفاع الإسرائيلي بمعلومات دقيقة حول طبيعة المهاجم ومكان تواجده لإفشال هجومه أو لتوجيه هجمات سيبرانية ضده.[1]

الخاتمة:

يتضح مما تقدم، لقد ادرك صناع القرار في ايران و(إسرائيل) ان إمكانية الدخول في صدام مباشر بينهما في الوقت الحالي ينطوي على مخاطر كبيرة على الصعيدين الاقتصادي والبشري؛ لذلك نجد بأن كلتاهما فضلتا اللجوء الى الصراع السيبراني بهدف الاضرار بمصالح الاخر، فايران فتوجهت لتطوير المجال السيبراني لغرض حماية البنى التحتية والمؤسسات الحكومية الحساسة والبرنامج النووي، علاوةً على ايجاد نوع من التوازن الاستراتيجي السيبراني، اما(اسرائيل) فقد سعت من خلال استراتيجيتها السيبرانية لردع ايران واعدائها الاقليمين، فضلاً عن ادخال المزيد من التقنيات الحديثة لمؤسساتها السيبرانية بهدف تعزيز الردع السيبراني وزيادة تفوقها في هذا المجال.

كما توصل البحث الى استنتاجات وهي :

- اظهرت دراسة وتحليل الاستراتيجية السيبرانية الايرانية والاسرائيلية ان كل منهما يسعى من خلال تطوير القوة السيبرانية لتحقيق اهدافه بحسب الاولويات وطبيعة البيئة الداخلية والخارجية.
- إن ايران اعطت الاولوية في استراتيجيتها السيبرانية الى الداخل لمنع وصول المعلومات لأنه سيشكل تهديد حقيقي على النظام السياسي الحاكم للبلاد.
- اما (اسرائيل) على العكس من ايران اعطت الاولوية للخارج، وبالتالي توجهت لتعزيز وتطوير قدراتها السيبرانية الهجومية بهدف الأضرار بمصالح خصومها الاقليميين وعلى رأسهم ايران.

1. القبة السيبرانية الإسرائيلية.. السمات والدوافع، الشروق،2022/8/4، في: (29/8/2022), http://bit.ly/3tqhJoy .

Conclusion:

As evident from the preceding discussion, decision-makers in Iran and Israel have recognized the significant risks, both economic and human, associated with engaging in direct confrontation at present. Consequently, both parties have opted to resort to cyber conflict with the aim of damaging each other's interests. Iran has focused on developing its cyber domain to protect critical infrastructure, sensitive governmental institutions, and its nuclear program. Additionally, it seeks to establish a form of cyber strategic equilibrium. On the other hand, Israel has pursued a cyber strategy aimed at deterring Iran and its regional adversaries. It has also introduced advanced technologies into its cyber institutions to enhance cyber deterrence and gain a competitive edge in this field.

The research findings have led to the following conclusions:

- The study and analysis of Iranian and Israeli cyber strategies demonstrate that each party seeks to achieve its objectives through the development of cyber power based on internal and external priorities and the nature of the environment.
- Iran prioritizes its domestic concerns in its cyber strategy, aiming to prevent the leakage of information that could pose a real threat to the country's political system.
- In contrast, Israel prioritizes external factors and, therefore, focuses on enhancing and developing its offensive cyber capabilities to damage the interests of its regional adversaries, particularly Iran.

Therefore, it is clear that both Iran and Israel are strategically pursuing cyber power to fulfill their respective goals.

المصادر

الكتب:

1. عبد الغفار، فيصل محمد. الحرب الالكترونية (عمان: الجنادرية للنشر والتوزيع،2015).

2. محارب, محمود. حرب في الفضاء الالكتروني: اتجاهات و تأثيرات على إسرائيل (الدوحة: المركز العربي للأبحاث و دراسة السياسات،2011).

3. يوسف، يوسف حسن. دماء على ابواب الموساد: دماء على أبواب الموساد: اغتيالات علماء العرب (القاهرة: سما للنشر والتوزيع، 2016).

البحوث والدراسات :

1. فرج، كرار عباس متعب. "الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وإيران"، مجلة حمورابي للدراسات، العدد40 (بغداد: 2021).

2. ميده، فادي، واخرون. "دراسة حول القدرات الإسرائيلية في مجال الحروب السيبرانية"، دراسات سياسية (دمشق: مركز توازن للأبحاث والدراسات، 2020).

الصحف:

1. ريد، جون. "الوحدة 8200 : تعرف على ذراع اسرائيل في إدارة عمليات الامن السيبراني"، الايام (رام الله)، السبت 2021/2/13.

الرسائل الجامعية:

1. جلعود, وليد غسان سعيد. "دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"، رسالة ماجستير غير منشورة، جامعة النجاح الوطنية, فلسطين, نابلس، 2013.

الأنترنيت:

1. برعام، جيل. تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل، مؤسسة الدراسات الفلسطينية، في: (2022/7/4) https://bit.ly/3BaAWPd .

2. الترسانة النووية الصهيونية تاريخ ومكونات، الجيش العربي، 2014/4/11، في: https://bit.ly/3R47r8e, (28/6/2022) .

3. خليفة، ايهاب. قدرات إيران الإلكترونية بين التهوين والتهويل، مركز المستقبل للابحاث والدراسات المتقدمة، 2014/8/20، في: (2022/5/18) https://bit.ly/3sLic4O .

4. رزق الله، باسل. إسرائيل على الجبهة الإلكترونية، موقع متراس، 2019/7/23، في: https://bit.ly/3QUZaDk, (1/7/2022).

5. القبة السيبرانية الإسرائيلية.. السمات والدوافع، الشروق،2022/8/4، في:
http://bit.ly/3tqhJoy, (29/8/2022) .

6. القدرات السيبرانية الإيرانية (الحرب الأخرى بين إيران وخصومها)، مجلة اتحاد الديمقراطيين السوريين، 2021/2/2، في : (2022/6/14) https://bit.ly/3mLUYbf .

7. كمال، مصطفى. مُختصر التعريف بالقدرات السيبرانية الإيرانية، مركز الانذار المبكر، 2020/8/20، في: (2022/8/15) https://bit.ly/3wpMU5x.

8. الكيان الصهيوني ينشأ وحدة للحرب الإلكترونية مع إيران، المجد الأمني، في:
https://bit.ly/3uvIfxR, (28/6/2022).

9. الليثي، محمد. الوحدة 8200: تعرف على ذراع الاستخبارات الإسرائيلية للاختراق عن بُعد، مركز الانذار المبكر، 2021/03/16، في: (2022/6/22) https://bit.ly/3yceO60 .

المصادر الإنكليزية :

1. Armelli, Matthew. Stuart Caudill and others, The Impact of Information Disclosures on APT Operation,2020.
2. Baezner, Marie. Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions (Zürich: Center for Security Studies, 2019).
3. Bucala, Paul and Pendleton, Caitlin Shayda. Iranian Cybe r Strategy: A View from the Iranian Military, 24/11/2015, in: https://bit.ly/3xrJq3d ,(7/6/2022).
4. Congressional Research Service Informing the legislative debate since 1914, Iranian Offensive Cyber Attack Capabilities, 13/1/2020.
5. Gerdab: A Dictated Scenario; Systematic Torture to Obtain Televised Confessions, Justice for Iran, 1/6/2012, in: https://justice4iran.org/8815/, (29/5/2022).
6. Haeghebaer, Emiel. Iran's decade of credential harvesting and surveillance operations, Virus Bulletin Conference, 7-8/10/2021.
7. Hlavek,Adam. Strategic goals behind Iranian cyber attacks , Security Bloggers Network, 26/10/2020, in: https://bit.ly/3xIOT5P, (11/6/2022).
8. 'Iranian Internet Infrastructure and Policy Report', smallmedia.org.uk, February/ 2014.

9. Israel National Cyber Security Strategy in Brief, National Cyber Directorate, Israel, September, 2017.

10. Jalali, Gholam Reza. Iran: Passive Defense Organization and Basij Sign Memorandum of Understanding, Middle East, North Africa, 9/2020.

11. Nadimi, Farzin. Iran's Passive Defense Organization: Another Target for Sanctions.

12. Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps, Department of Justice, 23/3/2018, in: https://bit.ly/3xi3lRW, (4/6/2022).

13. Radio Farda, Iran Cyberspace Supreme Council Among 20 Worst Digital Predators in 2020, 12/3/2020, in: https://bit.ly/3G4HBfe, (18/5/2022).

14. Rocket Kitten: A campaign with 9 Lives, Check Point Software Technologies, 2015.

15. Schmitt, Michael N. Noteworthy Releases of International Cyber Law Positions/ PART II: Iran, Lieber Institute, 27/8/2020, in: https://bit.ly/3aaMBTK, (29/5/2022).

16. Siboni, Gabi and Kronenfeld, Sami." Iran and Cyberspace Warfare", **Military and Strategic Affairs**, The number 3 (Israel: 2012).

17. Sommaire, Structure of Iran's Cyber Warfare, Institute Francais D'analyes Strategique, in: https://bit.ly/3GjumaC, (26/5/2022)

18. Spataro, Jason G. " Iranian Cyber Espionage", Master of Science in Cyber security , Utica University, New York, 2019.

19. The Iranian Cyber Threat, United Against Nuclear Iran, December 2020.

20. The Kittens Are Back in Town: Charming Kitten Campaign Against Academic Researchers, Clear Sky Security, September 2019.

21. The Library of Congress, **Iran's Ministry of Intelligence and Security: A profile (Washington,** December 2012).

22. The link between Kwampirs (Orangeworm) and Shamoon APTs, Cylera, January, 2022.

23. The National Cyber-Strategy of Israel and the INCB, Springer Link, in: https://bit.ly/3QYTeJD, (30/6/2022).

24. The Washington institute for near east policy internship, Washington,16/8/2018, in: https://bit.ly/3PMjzdl ,(29/5/2022).

References

Books:

1. Abdul Ghaffar, Faisal Muhammad. Electronic War (Amman: Al-Janadriyah for Publishing and Distribution, 2015).

2. Muhareb, Mahmoud. War in Cyberspace: Trends and Impacts on Israel (Doha: Arab Center for Research and Policy Studies, 2011).

3. Youssef, Youssef Hassan. Blood at the Gates of the Mossad: Blood at the Gates of the Mossad: The Assassinations of Arab Scholars (Cairo: Sama for Publishing and Distribution, 2016).

Research and studies:

1. Faraj, Karrar Abbas Meteb. "Cyber War: A Study in the Strategy of Cyber Attacks between the United States of America and Iran," Hammurabi Journal of Studies, Issue 40 (Baghdad: 2021).

2. Meedeh, Fadi, et al. A Study on Israeli Capabilities in the Field of Cyberwarfare, Political Studies (Damascus: Tawazun Center for Research and Studies, 2020).

Newspapers:

1. Reid, John. "Unit 8200: Learn about Israel's arm in managing cybersecurity operations," Al-Ayyam (Ramallah), Saturday 2/13/2021.

University theses:

1. Jaloud, Walid Ghassan Saeed. "The Role of Electronic Warfare in the Arab-Israeli Conflict", an unpublished master's thesis, An-Najah National University, Palestine, Nablus, 2013.

the internet:

1. Baram, Gil. The impact of the development of cyber warfare technology on building strength in Israel, Institute for Palestine Studies, in: (4/7/2022) https://bit.ly/3BaAWPd.

2. The Zionist nuclear arsenal, history and components, Arab Army, 4/11/2014, at: https://bit.ly/3R47r8e, (28/6/2022).

3. Khalifa, Ehab. Iran's electronic capabilities between underestimation and intimidation, The Future Center for Research and Advanced Studies, 20/8/2014, at: (18/5/2022) https://bit.ly/3sLic4O.

4. Rizkallah, Bassel. Israel on the Electronic Front, Mitras website, 7/23/2019, at:

https://bit.ly/3QUZaDk, (1/7/2022).

5. The Israeli Cyber Dome.. Features and Motives, Al-Shorouk, 4/8/2022, in: http://bit.ly/3tqhJoy, (29/8/2022).

6. Iranian cyber capabilities (the other war between Iran and its opponents), Journal of the Union of Syrian Democrats, 2/2/2021, at: (6/14/2022) https://bit.ly/3mLUYbf.

7. Kamal, Mustafa. Brief definition of Iranian cyber capabilities, Early Warning Center, 8/20/2020, at: (8/15/2022) https://bit.ly/3wpMU5x.

8. The Zionist entity establishes a unit for electronic warfare with Iran, al-Majd al-Amni, in: https://bit.ly/3uvIfxR, (6/28/2022).

9. Al-Laithi, Muhammad. Unit 8200: Learn about the Israeli intelligence arm for remote penetration, Early Warning Center, 03/16/2021, at: (6/22/2022) https://bit.ly/3yceO60.