القوة السيبرانية الإسرائيلية
وتأثيرها على استراتيجيات القوى الإقليمية

م.م محمد معن محسن
كلية العلوم السياسية/ جامعة النهرين
Muhammad.Maan@nahrainuniv.edu.iq

القوة السيبرانية الإسرائيلية
وتأثيرها على استراتيجيات القوى الإقليمية

م.م محمد معن محسن

كلية العلوم السياسية/ جامعة النهرين

Muhammad.Maan@nahrainuniv.edu.iq

تتناول هذه الدراسة مستقبل القوة السيبرانية كأحد العناصر الفاعلة في صياغة استراتيجيات القوى الإقليمية، مع التركيز على إسرائيل ** كنموذج بارز في هذا المجال ، اذ بات الفضاء السيبراني يشكّل ساحةً جديدة للتأثير والصراع، تستخدمها الدول لتعزيز قوتها، والحد من نفوذ خصومها، وتحقيق مكاسب سياسية وأمنية دون اللجوء إلى القوة التقليدية ، ويبرز هذا البحث كيف أن اسرائيل، في ظل التحديات المتعددة التي تواجهها، تتجه نحو تطوير قدراتها السيبرانية بوصفها أداة استراتيجية لتعويض مكامن الضعف في المجالات الأخرى، ولبناء ردع غير تقليدي يعزّز من مكانتها في محيطها الإقليمي ، ويركّز البحث على تحليل دوافع اسرائيل السيبرانية، وأهدافها، والتحديات التي تواجهها، فضلاً عن السيناريوهات المحتملة لمستقبل استخدامها لهذه القوة في إطار صراعات الشرق الأوسط.

الكلمات المفتاحية : إسرائيل، القوة السيبرانية، الفضاء السيبراني.

The Israeli cyber power and its impact on the strategies of regional forces

MOHAMMED MAAN MOHSIN

This study addresses the future of cyber power as one of the active elements in shaping the strategies of regional powers, focusing on Israel as a prominent model in this field. The cyber space has become a new arena for influence and conflict, used by countries to enhance their power, limit the influence of their adversaries, and achieve political and security gains without resorting to traditional power. This research highlights how Israel, in light of the multiple challenges it faces, is moving towards developing its cyber capabilities as a strategic tool to compensate for weaknesses in other areas and to build an unconventional deterrent that enhances its position in its regional environment. The research focuses on analyzing Iran's cyber motives, objectives, challenges it faces, as well as the potential scenarios for the future use of this power within the context of conflicts in the Middle East

Keywords: Cyber power - Cyberspace – Israel.

** تنويه : وردت إسرائيل بدون اقواس نظرا لكثرة استخدامها في البحث ، وهذا لايعني اعتراف من قبل الباحث بها .

المقدمة

تشهد البيئة الدولية تحوّلات متسارعة بفعل الثورة الرقمية والتطورات التكنولوجية، ما أسهم في بروز الفضاء السيبراني بوصفه ميداناً جديداً للتنافس والصراع بين الدول ، ولم تعد القوة السيبرانية مقتصرة على الجانب التقني أو الدفاعي، بل أصبحت أداة استراتيجية تعتمد عليها الدول لتحقيق مصالحها، وفرض تأثيرها في الإقليم والعالم ، وفي هذا السياق، برزت اسرائيل كإحدى القوى الإقليمية التي تولي أهمية متزايدة لتطوير قدراتها السيبرانية ضمن استراتيجياتها الشاملة، لاسيما في ظل التحديات الأمنية والسياسية التي تواجهها.

وتنبع أهمية الموضوع من تركيزه على بُعدٍ استراتيجي متنامٍ في بنية العلاقات الدولية المعاصرة، وهو القوة السيبرانية، مع تسليط الضوء على اسرائيل كنموذج إقليمي يسعى إلى توظيف هذه القوة في تعزيز مكانته ومصالحه ، كما يسهم في فهم آليات توظيف الفضاء السيبراني كأداة للردع، والتأثير، وإعادة تشكيل موازين القوة على المستويين الإقليمي والدولي.

وتثار إشكالية الموضوع من التساؤل الرئيس (كيف تسهم القوة السيبرانية في إعادة تشكيل المكانة الإقليمية لاسرائيل ضمن استراتيجياتها المستقبلية؟) لتنبع من هذا التساؤل فرضية مفادها (تعمل اسرائيل على دمج القوة السيبرانية في استراتيجياتها الإقليمية كوسيلة لتعزيز نفوذها، والتعامل مع التهديدات الأمنية، وموازنة تفوق خصومها في المجالات التقليدية) . لذا سيتم تقسيم هذا البحث الى المحاور الاتية :

المحور الأول : القوة السيبرانية الإسرائيلية

في ظل التحول الرقمي المتسارع الذي يشهده العصر الحديث، أصبح الفضاء السيبراني مجالًا جيوسياسيًّا حيويًّا، لا يقل أهمية عن البرّ والبحر والجوّ ، وتُشكّل القوة السيبرانية — كقدرة على استخدام التقنيات الرقمية للتأثير والتحكم في الأحداث — عمادًا استراتيجيًّا للدول والمؤسسات، سواء في تعزيز الأمن القومي أو تحقيق التفوق الاقتصادي أو فرض النفوذ السياسي ، فلم تعد الاستراتيجية السيبرانية مجرد خطة تقنية لمواجهة الهجمات الإلكترونية، بل تحولت إلى فلسفة شاملة تُحدِّد كيفية توظيف الأدوات الرقمية لخدمة أهداف كبرى، ترتكز على دوافع متشعبة ومرتكزات متعددة المستويات.

وتُعَد إسرائيل كيانًا جيوستراتيجيًّا فريدًا، نشأ في قلب منطقة تُعاني من صراعات تاريخية ودينية واقتصادية ، فمنذ إعلان قيامها عام 1948، سعت إلى تحقيق أمن وجودي عبر مزيج من الامتداد الجغرافي وتعزيز القوة العسكرية والتكنولوجية، مستفيدةً من دعم دولي وتحالفات إقليمية .

ويعد الامتداد الجيوستراتيجي عاملاً حاسماً في تحديد مكانة الدول على الصعيدين الإقليمي والدولي ، ففي حالة إسرائيل، يشكل موقعها الجغرافي ومواردها وتحالفاتها الاستراتيجية عوامل رئيسة في تعزيز قوتها الفعلية ، اذ يشير الامتداد الجيوستراتيجي إلى قدرة الدولة على التأثير في محيطها الجغرافي والسياسي عبّر عوامل كالموقع والتحالفات، والقوة العسكرية، والموارد الاقتصادية ، وتعتمد هذه الاستراتيجية على تحقيق التوسع أو النفوذ عبّر استخدام القوة الصلبة (العسكرية) أو الناعمة (السياسية والاقتصادية).[1] ويؤدي الموقع الجغرافي لإسرائيل تأثيرا استراتيجيا على المنطقة ، عبر الموقع الجغرافي أولا ، تقع إسرائيل في قلب الشرق الأوسط، مما يمنحها موقعًا استراتيجيًا يربط بين آسيا وإفريقيا وأوروبا ، وتحدها دول عربية من عدة جهات، مما يفرض تحديات أمنية ويجعلها تسعى لتعزيز قدراتها العسكرية ، فضلا عن الأهمية الجيوسياسية ثانيا ،اذ تنبع من قربها من الممرات البحرية المهمة كقناة السويس والبحر الأحمر ، ان وقوعها في منطقة غنية بالطاقة يعزز من أهمية تحالفاتها مع القوى العظمى ، إضافة الى استخدامها للسيطرة الجغرافية على الأراضي المحتلة لتعزيز أمنها ونفوذها. [2]

وتحاول إسرائيل باستخدام استراتيجيات متنوعة لتعزيز قوتها الفعلية لتحقيق الامتداد الجيوستراتيجي الخاص بها عبر الاتي :[3]

1. التفوق العسكري : تملك إسرائيل واحدة من أقوى الجيوش في المنطقة، مدعومة بتكنولوجيا عسكرية متقدمة وتقوم دائما بتعزيز قدراتها النووية والردع الاستراتيجي كعامل رئيسي في سياساتها الأمنية ، إضافة الى تطوير أنظمة دفاعية كـ "القبة الحديدية" و"مقلاع داوود".
2. التحالفات الدولية والإقليمية : عبر شراكة استراتيجية مع الولايات المتحدة، التي توفر لها دعمًا عسكريًا وماليًا واسعًا وتنامي التعاون مع بعض الدول العربية عبّر اتفاقيات التطبيع (اتفاقيات أبراهام) ، وتعزيز العلاقات مع قوى عالمية كالصين والهند لتعزيز نفوذها الاقتصادي والتكنولوجي.
3. التفوق التكنولوجي والاقتصادي : عبر الاستثمار في الصناعات العسكرية والتكنولوجية، مما يجعلها دولة رائدة في الابتكار ، إضافة الى استخدام القوة الناعمة عبّر التكنولوجيا، الشركات الناشئة، والاستثمارات في قطاع الذكاء الاصطناعي ، وتعزيز الاكتفاء الذاتي في الموارد مثل المياه والطاقة عبر مشاريع تحلية المياه والطاقة الشمسية.

4. السيطرة الجغرافية والتوسع الاستيطاني : عبر استمرار بناء المستوطنات في الضفة الغربية لتعزيز السيطرة على الأراضي المحتلة ، وفرض سياسة الأمر الواقع في القدس والجولان لضمها بشكل دائم واستخدام البعد الجغرافي كأداة لتعزيز الأمن والسيطرة على الموارد المائية في المنطقة.

اما عن التحديات التي تواجه الامتداد الجيوستراتيجي للقوة السيبرانية الإسرائيلية ، فيتمثل بالمقاومة الإقليمية عبر استمرار النزاع مع الفلسطينيين وتزايد قوة الفصائل المسلحة في غزة ولبنان ، و التهديدات الأمنية عبر تحديات أمنية متزايدة من إيران ومحور المقاومة، خاصة في ظل تنامي قدرات الطائرات المسيرة والصواريخ الباليستية ، فضلا عن التغيرات الجيوسياسية عبر تغير التحالفات الدولية وصعود قوى جديدة كالصين وروسيا، مما قد يؤثر على الدعم الأميركي لإسرائيل ، والتحديات الديموغرافية عبر ارتفاع عدد السكان العرب داخل إسرائيل مقارنة باليهود قد يؤثر على ميزان القوى الداخلي مستقبلاً. [4]

وهكذا ، تمكنت إسرائيل من تعزيز قوتها الفعلية عبر الجمع بين التفوق العسكري، والتوسع الجغرافي، والتحالفات الدولية، والتكنولوجيا المتقدمة ، ومع ذلك، لا تزال تواجه تحديات استراتيجية، أبرزها المقاومة الإقليمية والتحولات السياسية العالمية ، إن استمرارها في تعزيز نفوذها يعتمد على قدرتها على التكيف مع هذه المتغيرات والتعامل مع التهديدات المتزايدة ، وقد بدء التوسع الجيوستراتيجي الإسرائيلي في الأراضي المحتلة الفلسطينية والعربية عبر عدد من المراحل التاريخية، وهي باختصار كالاتي : [5]

1. المراحل التاريخية للامتداد وتتوزع الى ثلاث مراحل ، الأولى (1948–1967) وتميزت بالتوسع عبر حرب النكبة واحتلال 78% من فلسطين التاريخية ، اما المرحلة الثانية فكانت (1967–1993) وتمثلت باحتلال الضفة الغربية، غزة، الجولان، وسيناء، وتأسيس إسرائيل الكبرى ، اما المرحلة الثالثة عرفت بمرحلة ما بعد أوسلو (1993–الآن) وتشمل التوسع الاستيطاني تحت غطاء المفاوضات، وبناء الجدار العازل.

2. آليات السيطرة على الجغرافيا وتشمل الاستيطان كأداة جيوستراتيجية ، عبر وجود 700,000 مستوطن في الضفة الغربية والقدس الشرقية (2023) ، إضافة الى شبكة طرق عسكرية ومعازل لفصل التجمعات الفلسطينية ، فضلا عن السيطرة على الموارد عبر تحويل 85% من مياه نهر الأردن إلى إسرائيل ، واستغلال حقول الغاز في البحر المتوسط (حقل "تمار" و"ليفياثان").

3. الامتداد غير المادي ويشمل النفوذ السيبراني عبر تأسيس إسرائيل لشركات سيبرانية كـ"وادي السيليكون" للأمن الإلكتروني، مع تصدير تقنيات بقيمة 8 مليارات دولار سنويًا ، واستخدام برامج

مثل بيغاسوس لاختراق أنظمة دول معادية ، فضلا عن القوة الناعمة عبر تصدير السينما الإسرائيلية كـ(فيلم "فلسطيني أنا") لتشكيل الرواية التاريخية.

اما عن أدوات تعزيز القوة الفعلية للامتداد الجيواستراتيجي للقوة السيبرانية الاسرائيلية ، فتتلخص بالاتي :

1. التفوق العسكري: عبر امتلاكها لترسانة نووية تحوي على 90 رأسًا نوويًّا (وفق تقارير معهد ستوكهولم)، مع قدرة إطلاق عبر غواصات دولفين ،فضلا عن الجيش الذكي الذي يعتمد على الطائرات المسيرة (مثل هيرون تي بي 2) في عمليات الاستطلاع والاغتيالات، وتطوير أنظمة دفاع متطورة مثل القبة الحديدية (فاعلية 90% في اعتراض الصواريخ).[6]

2. القوة الاقتصادية والتكنولوجية : وتتمثل بالاقتصاد الابتكاري ، اذ ان 4.3% من الناتج المحلي يُنفق على البحث والتطوير (أعلى نسبة عالميًّا) ، وريادة في الزراعة الذكية (كالري بالتنقيط) وتصدير التقنيات إلى 150 دولة ، فضلا عن التحالف العسكري–الصناعي عبر تصدير أسلحة بقيمة 12 مليار دولار سنويًّا، مع عقود مع الهند (نظام صواريخ باراك 8) والإمارات. [7]

3. التحالفات الإقليمية والدولية : وتتمثل بالعلاقة مع الولايات المتحدة عبر دعم سنوي بقيمة 3.8 مليار دولار عسكريًّا، وتنسيق استخباراتي ضد إيران ، فضلا عن التطبيع العربي عبر توقيع اتفاقيات إبراهام (2020) لتحييد الخليج العربي، وفتح أسواق جديدة والشراكة مع الناتو عبر المشاركة في مناورات عسكرية، وتطوير تكنولوجيا الحرب الإلكترونية.[8]

وتواجه إسرائيل عدد من التحديات والتهديدات التي تهدد الامتداد الجيواستراتيجي للقوة السيبرانية الاسرائيلية ، أهمها :

1. التهديدات الخارجية التي تتوزع الى ، المحور الإيراني–المقاومة ، عبر 150 ألف صاروخ لدى حزب الله، وقدرات حماس الصاروخية المتطورة (صواريخ A–120) ، والبرنامج النووي الإيراني كتهديد وجودي و التحولات الجيوسياسية كصعود تركيا كمنافس في شرق المتوسط، وتنامي النفوذ الصيني في المنطقة. [9]

2. التحديات الداخلية : وتتوزع الى ، الانقسامات المجتمعية ، كتصاعد التوتر بين اليهود العلمانيين والمتدينين، وتمرد الشباب اليهود ضد الخدمة العسكرية ، واحتجاجات الفلسطينيين داخل الخط الأخضر (أحداث مايو 2021) و الأزمات السياسية كعدم الاستقرار الحكومي (5 انتخابات في 3 سنوات)، وتصاعد اليمين المتطرف . [10]

3. الضغوط الدولية: وتتوزع الى ، حركة المقاطعة (BDS) مما سبب خسائر اقتصادية تقدر بـ1.5 مليار دولار سنويًا و الاتهامات بجرائم حرب عبر تقارير الأمم المتحدة عن انتهاكات في حروب غزة (2008، 2014، 2021). [11]

وعلى الرغم من نجاح إسرائيل في ترسيخ نفسها كقوة إقليمية ، فإن استراتيجيتها تواجه مخاطر جسيمة عبر الامتداد الجيواستراتيجي للقوة السيبرانية الاسرائيلية ، أهمها الاستيطان ، اذ يعد الاستيطان كقنبلة موقوتة اذ ان توسيع المستوطنات يُعقِّد إمكانية حل الدولتين، ويزيد من عزلتها الدولية ، فضلا عن التوازن الهش مع إيران اذ ان أي تطور في البرنامج النووي الإيراني قد يُجبر إسرائيل على حرب مكلفة ، ناهيك عن التحدي الديمغرافي ارتفاع نسبة الفلسطينيين (23% داخل إسرائيل، 5 ملايين في الأراضي المحتلة) مما يهدد الهوية اليهودية للدولة. [12]

وفي المقابل، قد تُحافظ إسرائيل على تفوقها في الامتداد الجيواستراتيجي لقوتها السيبرانية ، عبر مجموعة من الحلول أهمها تعزيز التحالف مع دول الخليج ضد إيران والاستثمار في التكنولوجيا العسكرية والذكاء الاصطناعي وتوظيف الدبلوماسية الثقافية لتحسين صورتها العالمية.[13]

وفي العقدين الأخيرين، ركزت على بناء قدرات دفاعية وهجومية متقدمة لتعزيز أمنها القومي عبر المؤسسات السيبرانية الإسرائيلية والتي تضم :[14]

أ. الوحدات العسكرية المتخصصة كالوحدة 8200 التي تعد أهم وحدة استخبارات سيبرانية في الجيش الإسرائيلي، وهي مسؤولة عن جمع وتحليل المعلومات الإلكترونية، وتنفيذ عمليات هجومية ضد الخصوم والوحدة 81 المتخصصة في تطوير أدوات الهجوم السيبراني والذكاء الاصطناعي لأغراض عسكرية ، القيادة السيبرانية الإسرائيلية (Cyber Command) التي تأسست عام 2017 للإشراف على العمليات السيبرانية الدفاعية والهجومية.

ب. المؤسسات المدنية والحكومية كالهيئة الوطنية للأمن السيبراني (INCD) التي تعمل على حماية البنية التحتية المدنية من الهجمات السيبرانية وتعزيز التعاون بين القطاعين العام والخاص ، والمركز الوطني للسايبر (Cyber National Center) الذي يهدف إلى تطوير الأبحاث والابتكارات في مجال الأمن السيبراني.

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

وتعتمد القوة السيبرانية الإسرائيلية على استراتيجيات متعددة تطمح عبرها الى تحقيق الامتداد الجيواستراتيجي للقوة السيبرانية الاسرائيلية ، أهمها الاستراتيجية الدفاعية التي تعتمد على تطوير أنظمة حماية متقدمة لمنع الاختراقات والهجمات السيبرانية وتنفيذ تدريبات سنوية لمحاكاة الهجمات السيبرانية وتعزيز الجاهزية الإلكترونية وتعزيز التعاون الدولي في مجال الأمن السيبراني مع الولايات المتحدة ودول أوروبية ، كذلك الاستراتيجية الهجومية التي تشمل تنفيذ عمليات سيبرانية هجومية لتعطيل أنظمة الخصوم، كما حدث في الهجوم المشترك مع الولايات المتحدة باستخدام فيروس "ستوكسنت" (Stuxnet) لتعطيل البرنامج النووي الإيراني عام 2010 ، واستهداف البنية التحتية الإلكترونية لحركات المقاومة الفلسطينية وإيران لتعطيل أنظمتها المالية والعسكرية واستخدام البرمجيات الخبيثة وأدوات القرصنة لاستهداف شبكات الدول المعادية ، فضلا عن الاستراتيجية الاستخباراتية كتوظيف الذكاء الاصطناعي وتحليل البيانات لتعقب الجماعات المسلحة والشبكات الإرهابية وتنفيذ عمليات تجسس إلكتروني لجمع معلومات عن الجهات المعادية واستخدام تقنيات التعلم الآلي والبيانات الضخمة في تحليل المعلومات الأمنية. [15]

ويُظهر التطور التكنولوجي العسكري الإسرائيلي تحولًا نوعيًا في أنماط الحرب السيبرانية، مع التركيز على تنفيذ عمليات تكتيكية ذات تأثير استراتيجي، على سبيل المثال، في ايلول 2023، استهدفت إسرائيل أجهزة الاتصال اللاسلكي التابعة لحزب الله في بيروت، مما عكس قدرتها على تنفيذ هجمات سيبرانية متقدمة ، ومع ذلك، أثارت هذه العمليات قلقًا دوليًا بشأن الأضرار الإنسانية المحتملة الناتجة عن استخدام هذه التقنيات المتقدمة.

ان الدوافع وراء هذا التحول في العقيدة الأمنية الإسرائيلية نحو السيبرانية متعددة، منها تصاعد التهديدات السيبرانية من دول كإيران وتنظيمات لادولية كحزب الله والحوثيين ، والحاجة إلى تأمين شركات الاتصالات التي تُعد هدفًا رئيسا للهجمات السيبرانية ، بالإضافة إلى ذلك، تسعى إسرائيل إلى الحفاظ على تفوقها التكنولوجي في المنطقة عبر تبني استراتيجية دفاعية شاملة تشمل جميع الجبهات، بما فيها الجبهة السيبرانية.[16]

علاوة على ذلك، تستثمر إسرائيل بشكل مكثف في مجالات كالذكاء الاصطناعي، وتوظفه كمضاعف للقوة في المجالات الأمنية والعسكرية ، هذا الاستثمار يهدف إلى تعزيز قدراتها العملياتية وتحقيق مزايا استراتيجية في ساحة المعركة ، ومع ذلك، يواجه هذا الاستثمار تحديات، منها المخاوف من تحول هذه الأنظمة إلى وحدات مستقلة تمامًا في اتخاذ القرارات، مما قد يؤدي إلى تفاقم الأضرار الإنسانية ، بالإضافة إلى ذلك، هناك قلق من أن الاعتماد المتزايد على

التكنولوجيا السيبرانية قد يجعل إسرائيل أكثر عرضة للهجمات السيبرانية المضادة، خاصة في ظل التنافس مع دول كإيران.[17]

وبناءً على ما سبق، يمكن القول إن التطور التكنولوجي السيبراني في إسرائيل يُعد جزءًا أساسيًا من استراتيجيتها الأمنية والعسكرية، اذ تسعى عبره إلى تحقيق تفوق نوعي في المنطقة، مع مواجهة تحديات معقدة تتعلق بالأمن والأخلاق والشرعية الدولية.

وتشكل التكنولوجية السيبرانية في إسرائيل ظاهرةً استثنائيةً في المشهد العلمي والاستراتيجي العالمي، اذ تحولت الدولة ذات الموارد الطبيعية المحدودة إلى قوة عظمى في مجال الأمن السيبراني والابتكارات الرقمية ، ويعود هذا التحول إلى تفاعل معقد بين العوامل التاريخية، والاستثمارات الاستراتيجية في البحث والتطوير، والبيئة المؤسسية الداعمة، إلى جانب الخبرات العسكرية المتراكمة التي أعيد توظيفها في القطاع المدني. [18]

وقد نشأ الاهتمام الإسرائيلي بالتكنولوجيا المتقدمة في أعقاب تأسيس الدولة عام ١٩٤٨، اذ فرضت التحديات الجيوسياسية والأمنية ضرورةَ تطوير بنية تحتية تكنولوجية تعتمد على الابتكار لتعويض نقص الموادر البشرية والمادية ، ففي سبعينيات وثمانينيات القرن العشرين، بدأت ملامح النظام البيئي التكنولوجي (Ecosystem) بالتشكل عبر استثمارات مكثفة في التعليم التقني وإنشاء مراكز أبحاث مرتبطة بالقطاع العسكري ، ومع ظهور الإنترنت في التسعينيات من القرن العشرين ، تحول التركيز نحو الأمن السيبراني، خاصةً بعد تعرض البنية التحتية الإسرائيلية لهجمات إلكترونية مبكرة أظهرت نقاطَ ضعفٍ استراتيجية.[19]

وفي هذا الإطار، ادت وحدات النخبة العسكرية، كالوحدة 8200 ، دورًا محوريًا في صقل الكفاءات التقنية، اذ أصبحت بمثابة مدرسة غير رسمية لخريجيها الذين أسسوا لاحقًا شركاتٍ ناشئة (Startups) رائدة ، كما ساهم برنامج "يوزما" (Yozma) الحكومي في تسعينيات القرن العشرين في جذب الاستثمارات الأجنبية وإنشاء حاضنات تكنولوجية، مما عزز التعاون بين القطاعين العام والخاص. [20]

وتملك إسرائيل اليوم واحدةً من أكثر أنظمة الدفاع السيبراني تقدمًا في العالم، اذ تتبنى استراتيجيةً هجوميةً ودفاعيةً متكاملة ، كما تُطور الشركات الإسرائيلية تقنيات متقدمة في مجالات كالذكاء الاصطناعي التطبيقي في الكشف عن التهديدات، وأنظمة التشفير الديناميكي، وأدوات مراقبة الشبكات في الوقت الفعلي ، فعلى سبيل المثال، تعد تقنيات شركة "تشيك بوينت" (Check Point) و"سايبر آرك" (CyberArk) معاييرَ ذهبيةً في الحماية من الاختراقات. [21]

ولا يقتصر التفوق الإسرائيلي على الجانب الدفاعي ، ففي مجال الحرب السيبرانية الهجومية، تشير تقارير دولية إلى أن إسرائيل كانت من أوائل الدول التي استخدمت الهجمات الإلكترونية كأداة استخباراتية، كما في حالة برنامج "ستاكسنت" (Stuxnet) الذي استهدف المنشآت النووية الإيرانية عام ٢٠١٠ ، هذا التكامل بين القدرات الهجومية والدفاعية يعكس فلسفةً أمنيةً تقوم على الردع عبر التعقيد (Deterrence by Complexity)، اذ تُصعّب التقنيات المتشابكة على الخصوم التنبؤ بالثغرات أو الهجمات المحتملة[22]، ويمكن تفسير النجاح في التفوق الاسرائيلي عبر عدة محاور: [23]

1. رأس المال البشري اذ يستثمر النظام التعليمي بكثافة في العلوم التكنولوجية، مع التركيز على الرياضيات وعلوم الحاسوب منذ المراحل الثانوية ، كما أن الخدمة العسكرية الإلزامية توفر تدريبًا عمليًا مكثفًا لشريحة واسعة من الشباب في مجالات الأمن والاتصالات.
2. التكامل بين الجيش والصناعة اذ تؤدي المؤسسة العسكرية دورًا مزدوجًا كمستهلك للتقنيات وكممول لأبحاث التطوير، مما يخلق سوقًا ديناميكيًا للابتكار.
3. الدعم الحكومي عبر سياسات ضريبية مشجعة، وتمويل مباشر للمشاريع الناشئة، وإنشاء كيانات كالسلطة الوطنية السيبرانية (INCD) التي تنسق بين الجهات المختلفة.
4. العولمة التكنولوجية اذ تعتمد إسرائيل على شبكة تعاون دولية مع دول كالولايات المتحدة والهند، مما يتيح تبادل الخبرات واختبار التقنيات في أسواق متنوعة.

وفي سياق التطور التكنولوجي السيبراني الإسرائيلي، تبرز تحديات وأسئلة أخلاقية متعددة تتجاوز ما تم ذكره في أعلاه ، منها :[24]

1. استخدام الذكاء الاصطناعي في العمليات العسكرية وأثره على المدنيين ، اذ أظهرت التقارير استخدام إسرائيل لأنظمة ذكاء اصطناعي مثل "غوسبل" (The Gospel) و"لافندر" (Lavender) في تحديد الأهداف العسكرية، مما أدى إلى ضربات جوية تسببت في سقوط ضحايا مدنيين ، وهذا يطرح أسئلة حول دقة الخوارزميات ومدى توافقها مع القانون الدولي الإنساني، خاصةً في ظل غياب آليات رقابة فعالة لضمان التمييز بين الأهداف العسكرية والمدنية ، كما يتجلى هنا تناقض بين الابتكار التكنولوجي والمبادئ الأخلاقية المتعلقة بحماية الحياة البشرية.
2. تصدير تقنيات المراقبة إلى دول تنتهك حقوق الإنسان ، اذ برزت انتقادات لشركات إسرائيلية مثل NSO Group بسبب تصدير برامج مثل "بيجاسوس" إلى حكومات استخدمتها لمراقبة

الصحفيين والمعارضين، مما ينتهك حق الخصوصية ويُضعف الحريات الأساسية ، وهذا يثير تساؤلات حول المسؤولية الأخلاقية للدول المُصدرة، وضرورة وضع معايير دولية تحظر نقل التكنولوجيا إلى جهات تُساء استخدامها.

3. التحيز في الخوارزميات وانعكاساته على العدالة ، تعاني أنظمة الذكاء الاصطناعي من تحيزات مُضمنة في البيانات المُستخدمة لتدريبها، كما حدث في نظام توظيف أظهرت تفضيلًا للذكور على الإناث ، ففي السياق الإسرائيلي، قد يؤدي تطبيق هذه الأنظمة في مجالات كالأمن أو العدالة إلى تعميق التمييز ضد فئات معينة، مما يهدد مبدأ المساواة ويستدعي مراجعة شاملة لآليات تصميم الخوارزميات.

4. الغموض في تحديد المسؤولية القانونية عن أخطاء الأنظمة الذكية ، عند ارتكاب أنظمة الذكاء الاصطناعي أخطاءً جسيمة (كحوادث السيارات ذاتية القيادة)، يصعب تحديد الجهات المسؤولة(المطورين، المشغلين، أم النظام نفسه) ، وفي الحالة الإسرائيلية، يزداد هذا التعقيد مع استخدام أنظمة عسكرية ذاتية، مما يفتح باب النقاش حول إطار قانوني دولي يحدد معايير المساءلة.

5. التأثير على الهوية الوطنية والقيم الاجتماعية ، قد يؤدي الاعتماد المفرط على التكنولوجيا السيبرانية إلى تغيير في الهوية الوطنية الإسرائيلية، التي تُعرف بتركيزها على الابتكار الأمني ، وهذا يطرح أسئلة حول التوازن بين الأمن والقيم الإنسانية، وكيفية الحفاظ على البعد الأخلاقي في ظل سباق التسلح التكنولوجي .

6. أخلاقيات البيانات والخصوصية في البحث العلمي ، يعتمد التطور السيبراني الإسرائيلي على جمع كميات هائلة من البيانات، مما يهدد خصوصية الأفراد ، وهنا تبرز معضلات أخلاقية حول حدود الاستخدام المشروع للبيانات، خاصةً مع تقنيات كالتتبع الجغرافي أو تحليل السلوك ويتطلب هذا تعزيز الشفافية وضمان موافقة المستخدمين.

7.الأبعاد الثقافية والاستعمار الرقمي ، يؤدي تصدير النماذج التكنولوجية الإسرائيلية إلى دول أخرى إلى فرض قيم ثقافية معينة، مما يُعرف بالاستعمار الرقمي ، وهذا يثير تساؤلات حول احترام التنوع الثقافي وتجنب الهيمنة التكنولوجية .

وتتوزع القوة السيبرانية الإسرائيلية الى عدد من المكونات ، والتي يمكننا تقسيمها الى :[25]

1. البنية التحتية العسكرية والتكنولوجية: وتتوزع الى الوحدات العسكرية المتخصصة كالوحدة 8200 التي تُنتج كوادر سيبرانية تُؤسس شركات مثل NSO Group (مطورة برنامج بيغاسوس) ، وحدة كيليا 81: مسؤولة عن الهجمات السيبرانية الهجومية، كعملية ستوكسنت ضد إيران

(2010) ، فضلا عن القطاع الخاص إسرائيل هي ثالث أكبر مصدر للأمن السيبراني عالميًّا، بإيرادات سنوية تصل إلى 12 مليار دولار ، ولديها شركات كـ Check Point وCyberArk تُهيمن على سوق الحلول الأمنية العالمية.

2. التعاون بين المجالين العسكري والمدني عبر برنامج Talpiot لدمج نخبة الجامعات في المشاريع التكنولوجية العسكرية وشراكات بين الجيش وشركات الهايتك لتطوير تقنيات الذكاء الاصطناعي في الحرب الإلكترونية.

3. الإطار القانوني والسياسي كقانون الأمن السيبراني (2018): يُلزم المؤسسات الحكومية والخاصة باتباع معايير أمنية صارمة وتخصيص 20% من ميزانية وزارة الدفاع للتطوير السيبراني.

اما توظيف القوة السيبرانية في الاستراتيجية الإسرائيلية فتأتي أهميتها عبر ماتؤديه من دور فاعل وحاسم لتحقيق الامتداد الجيواستراتيجي للقوة السيبرانية الاسرائيلية ، عبر تعزيز الأمن القومي عبر القيام باولا تحقيق الدفاع السيبراني عبر حماية البنى التحتية الحيوية كمفاعل ديمونا النووي وشبكات الكهرباء ، إضافة الى صد الهجمات إلايرانية، كالهجوم على نظام المياه الإسرائيلي (2021) ، وثانيا زيادة فاعلية الهجوم السيبراني عبر تعطيل برامج تخصيب اليورانيوم الإيراني عبر فيروس ستوكسنت ، واختراق أنظمة حماس في غزة لتحديد مواقع القادة ، فضلا عن النفوذ الجيوسياسي عبر تصدير التكنولوجيا كأداة دبلوماسية، كتزويد الإمارات بأنظمة مراقبة بعد التطبيع واستخدام برامج التجسس (بيغاسوس) لمراقبة خصوم سياسيين، كما في فضائح التجسس على مسؤولين أوروبيين (2021) ، يضاف الى ذلك التفوق الاقتصادي عبر جذب استثمارات لشركات كبرى كجوجل ومايكروسوفت لإنشاء مراكز أبحاث في إسرائيل وتحويل البلاد إلى وادي السيليكون للأمن السيبراني، مع وجود 450 شركة ناشطة في المجال. [26]

ختاما ، قد تُعيد الحروب السيبرانية تشكيل مفهوم السيادة، لكن إسرائيل ستظلُّ لاعبًا مركزيًّا بفضل بنيتها التحتية الفريدة وثقافة الابتكار وتحالفاتها الدولية.

المحور الثاني مجالات استخدام القوة السيبرانية الاسرائيلية وانعكاساتها على الأمن الإقليمي

تُعد إسرائيل واحدة من أبرز القوى السيبرانية العالمية، اذ تستخدم تكنولوجياتها المتقدمة لتعزيز أمنها القومي وتوسيع نفوذها الإقليمي ، وتمتد تأثيرات هذه القوة من تعطيل البنى التحتية العسكرية للأعداء إلى شن حروب معلوماتية وتجسس على الحكومات .

اذ تُشكّل القوة السيبرانية أحد أبرز أدوات النفوذ الاستراتيجي في القرن الحادي والعشرين، وتحولت الفضاءات الرقمية إلى ساحة تنافسية تعكس صراعات جيوسياسية معقدة ، وفي هذا السياق، تبرز إسرائيل كواحدة من الدول الرائدة في تطوير قدراتها السيبرانية الهجومية والدفاعية، مدعومةً ببنية تحتية تكنولوجية متقدمة، وإطار تشريعي متكامل، وتعاون وثيق بين القطاعات العسكرية والمدنية والخاصة ، وفي هذا المطلب سنتطرق إلى تحليل مجالات استخدام القوة السيبرانية الإسرائيلية، وانعكاساتها على توازنات الأمن الإقليمي في الشرق الأوسط، مع التركيز على التفاعلات بين القدرات التكنولوجية والسياسات الأمنية والتداعيات الجيوسياسية.

وتعددت المجالات الاستراتيجية لاستخدام القوة السيبرانية الإسرائيلية ، وهي كالاتي :[27]

1. العمليات العسكرية والاستخباراتية:

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

2. حماية البنى التحتية الحيوية:

مع تزايد الاعتماد على الأنظمة الرقمية في إدارة الشبكات الكهربائية والمياه والاتصالات، تعمل إسرائيل على تعزيز الدفاعات السيبرانية لبنيتها التحتية الوطنية ، ومع ذلك، فإن امتلاكها قدرات هجومية متقدمة يسمح لها أيضاً بالتأثير على بنى تحتية لدول مجاورة في حالات الصراع، مما يخلق ردعاً افتراضياً يعزز أمنها القومي.

3. الحرب الاقتصادية والتجسس الصناعي:

تشير دراسات إلى أن إسرائيل تستخدم أدوات سيبرانية لاستهداف قطاعات اقتصادية في دول تعدها معادية، كإيران ولبنان، عبر اختراق أنظمة البنوك أو سرقة بيانات تكنولوجية ، في المقابل، تُوظف هذه القدرات في تعزيز التفوق التكنولوجي للإقتصاد الإسرائيلي عبر حماية شركاتها من الهجمات المنافسة.

4. التأثير في الرأي العام والعمليات النفسية:

يُلاحظ استخدام الحملات الإلكترونية للتأثير على الرأي العام في المنطقة، سواء عبر نشر معلومات مضللة أو اختراق منصات إعلامية تابعة لفصائل معادية ، على سبيل المثال، تم اتهام إسرائيل بتنفيذ عمليات اختراق لقنوات فضائية فلسطينية ولبنانية خلال فترات التوتر السياسي.

ويرتكز التفوق التكنولوجي الإسرائيلي على نظام تعليمي يُولي العلوم التكنولوجية أولوية قصوى ، فمنذ المرحلة الثانوية ، يتم تشجيع الطلاب على التخصص في مجالات كالرياضيات المتقدمة وعلوم الحاسوب، عبر برامج مثل مسار التميز التكنولوجي (MAGNET) ، ففي التعليم العالي، تُعد جامعات كالتخنيون في حيفا ومعهد وايزمان مراكزَ بحثيةً رائدةً تتعاون مع قطاع الصناعة لتطوير تقنيات ثورية، فعلى سبيل المثال، ساهم باحثون من جامعة تل أبيب في ابتكار خوارزميات الذكاء الاصطناعي المستخدمة في كشف الهجمات الإلكترونية ، يُضاف إلى ذلك برامج الجذب الدولية، كمنح التأشيرات الخاصة للخبراء الأجانب، مما يسد الفجوات في سوق العمل المحلي. [28]

وتُعد الثقافة المجتمعية الداعمة للابتكار عاملاً غير ملموسٍ لكنه بالغ الأهمية ، فخلافًا للمجتمعات ، تُشجع إسرائيل على المخاطرة التجارية، اذ يُنظر إلى الإفلاس كخطوة تعلم ضرورية ، هذا المناخ يدعمه وجود شبكةٍ واسعةٍ من حاضنات الأعمال ومسرعات النمو (Accelerators)، كـ واي فاند (OurCrowd)، التي توفر التمويل والإرشاد للشركات في مراحلها الأولى ، كما تُسهم الثقافة اللامركزية في المؤسسات الإسرائيلية في تعزيز الإبداع، اذ يُمنح الموظفون في الشركات الناشئة مساحةً كبيرةً لاتخاذ القرارات دون بيروقراطية مفرطة.[29]

وتواجه إسرائيل انتقاداتٍ مرتبطةً بالتداعيات الأخلاقية لتكنولوجياتها ، فتصدير برمجيات المراقبة إلى دول تُنتهك فيها حقوق الإنسان، كما في فضيحة بيجاسوس (Pegasus) التي شاركت فيها شركة NSO Group، يطرح تساؤلاتٍ حول المسؤولية الاجتماعية للشركات ، بالإضافة إلى ذلك، يُهدد التوسع السريع للذكاء الاصطناعي بخلق فجوات مهارية في سوق العمل، اذ تتطلب الوظائف الجديدة مهاراتٍ متقدمةً لا تتوفر لدى جميع الشرائح المجتمعية. [30]

ولضمان استمرارية الريادة، تعمل إسرائيل على تطوير استراتيجيات طويلة المدى تركز على تعميق التعاون بين القطاعين العام والخاص، واستقطاب الكفاءات العالمية، وزيادة الاستثمار في البحث الأساسي في مجالات كالحوسبة الكمومية والأمن السيبراني الفضائي ، وفي الوقت نفسه، تُعيد الدولة هيكلة سياساتها لمواجهة التهديدات الناشئة، كالهجمات المدعومة بالذكاء الاصطناعي، والتي تتطلب تطوير أنظمة دفاعية ذاتية التعلم. [31]

وهكذا ، تُقدم إسرائيل نموذجًا يقدم كيفية تحويل التحديات الأمنية في لدول الصغيرة إلى محركات للابتكار الاقتصادي ، ويعتمد هذا النجاح على تكامل غير مسبوق بين العسكرة والريادة المدنية، ودعم سياسي لا يتزعزع للبحث العلمي، وثقافة مجتمعية تُقدس المعرفة ، ومع ذلك، فإن استدامة هذا النموذج تتطلب موازنة دقيقة بين الابتكار والأخلاق، وبين النمو الاقتصادي والعدالة الاجتماعية، وهو ما سيكون التحدي الأكبر في العقود القادمة.[32]

ففي عالم تُهيمن عليه الحروب غير المتناظرة، أصبحت القوة السيبرانية أداةً مركزية في الاستراتيجية الإسرائيلية لمواجهة التهديدات الإقليمية ، بفضل تفوقها التكنولوجي والتعاون الوثيق بين قطاعاتها العسكرية والمدنية، وتملك إسرائيل قدرات سيبرانية هجومية ودفاعية تُؤثر بشكل مباشر على الأمن الإقليمي ، اما عن مجالات استخدام القوة السيبرانية الإسرائيلية ، فيمكننا ملاحظة الاتي :

أولا :المجالات العسكرية والأمنية : وتشمل تعطيل البنى التحتية العسكرية للأعداءكهجوم Stuxnet (2010) الناتج عبر تعاون إسرائيلي–أمريكي لإعاقة البرنامج النووي الإيراني عبر إتلاف أجهزة الطرد المركزي واستهداف أنظمة الدفاع الجوي السوري كالهجمات المتكررة منذ 2017 لشل قدرات الرادارات والأنظمة الإلكترونية ، فضلا عن التجسس الاستراتيجي عبر اختراق شبكات اتصالات إيران باستخدام أدوات مثل Duqu 2.0 لمراقبة المفاوضات النووية ، ومراقبة تحركات الجماعات المضادة لها عبر التجسس على اتصالات حزب الله في لبنان عبر برمجيات متخصصة ، والحرب الاستباقية والوقائية عب رضربات سيبرانية وقائية كتعطيل خوادم حماس قبل عمليات عسكرية برية. [33]

ثانيا : المجالات السياسية والدبلوماسية : وتشمل حروب المعلومات والتأثير على الرأي العام عبر حملات التضليل الإلكتروني بنشر أخبار مزيفة عبر حسابات وهمية لتشويه سمعة الخصوم (كإيران وسوريا) ، واختراق حسابات دبلوماسيين عبر سرقة وثائق حساسة من مسؤولين في دول الخليج وأوروبا ، والتأثير على الانتخابات الإقليمية كالتدخل في الانتخابات اللبنانية عام 2022 زاختراق منصات إعلامية لدعم مرشحين موالين ، فضلا عن تعزيز التحالفات الدولية كتدريب كوادر خليجية عبر شراكات مع الإمارات والسعودية لبناء أنظمة دفاع سيبراني. [34]

ثالثا: المجالات الاقتصادية والتكنولوجية : وتشمل حماية الاقتصاد الإسرائيلي عبر الدفاع عن البنية التحتية الرقمية كحماية شبكة الكهرباء الوطنية من هجمات إيرانية محتملة ، وتأمين الشركات الناشئة كدعم قطاع التكنولوجيا الذي يُشكل 15% من الناتج المحلي الإجمالي ، فضلا

عن الاستخبارات الاقتصادية عبر سرقة أسرار صناعية كاختراق شركات إيرانية لسرقة تصميمات طائرات مسيرة والتجسس على منافسين إقليميين كالتجسس على شركات النفط السعودية ، وتصدير التكنولوجيا الأمنية كبيع برمجيات تجسس مثل Pegasus إلى دول كالإمارات والمغرب لمراقبة المعارضين. [35]

رابعا: المجالات الاجتماعية والإعلامية : وتشمل السيطرة على السردية الإعلامية كاختراق منصات التواصل للتأثير على الرأي العام العربي (كالترويج لاتفاقيات التطبيع مع الخليج) ، إضافة الى تشويه سمعة الناشطين عبر تسريب بيانات شخصية أو تلفيق اتهامات ، و حماية المجتمع الإسرائيلي عبر مكافحة الجرائم الإلكترونية كهجمات الفدية التي تستهدف المستشفيات إضافة الى الرقابة على المحتوى كحجب مواقع تُنشر أخبارًا معادية لإسرائيل. [36]

خامسا: الانعكاسات على الأمن الإقليمي : وتشمل تصعيد التوترات مع إيران عبر حرب سيبرانية متبادلة كالهجمات الإسرائيلية على منشآت إيرانية مقابل هجمات إيرانية على البنية التحتية الإسرائيلية ، إضافة الى تأثيراتها على استقرار الخليج زيادة مخاطر تعطيل إمدادات النفط بسبب الهجمات ، وتغيير تحالفات إقليمية كالتقارب الخليجي–الإسرائيلي عبر تعاون أمني لمواجهة التهديد الإيراني (كاتفاقيات أبراهام) إضافة الى توتر العلاقات مع تركيا ، بسبب اختراقات إسرائيلية لشبكات اتصالات أنقرة ، فضلا عن تقويض سيادة الدول الضعيفة عبر الاختراقات المتكررة لبعض الدول العربية ، مما يُضعف قدرة حكوماتهما على السيطرة على الفضاء الإلكتروني. [37]

ومن امثلة الهجمات السيبرانية الإسرائيلية ، نستعرض الاتي : [38]

1. هجوم Stuxnet على إيران:

التكتيك: فيروس كمبيوتر دمَّر 20% من أجهزة الطرد المركزي الإيرانية.

الانعكاسات: تسريع البرنامج النووي الإيراني في منشآت سرية.

2. اختراق شبكة المياه الإسرائيلية (2020):

الهجوم : إيراني باختراق شبكة المياه الإسرائيلية .

الرد الإسرائيلي: شن هجمات انتقامية على موانئ إيرانية.

3. فضيحة Pegasus في العالم العربي: كتآكل الثقة في الحكومات الخليجية .

ختاما تمارس إسرائيل تأثيرًا جيوسياسيًا هائلًا عبر قوتها السيبرانية، مما يجعلها لاعبًا مركزيًا في صراعات الشرق الأوسط ، ومع ذلك، فإن الاعتماد المفرط على الأدوات الهجومية قد يُزيد من

عدم الاستقرار الإقليمي، ويُعمق الانقسامات بين الدول ، ويتطلب تحقيق التوازن تعاونًا دوليًا لتنظيم استخدام القوة السيبرانية، وحماية الفضاء الإلكتروني من التحول إلى ساحة حرب مفتوحة.

اما الانعكاسات التي تخص القوة السيبرانية الإسرائيلية على الأمن الإقليمي في الشرق الأوسط فقد أدّى تصاعد النشاط السيبراني الإسرائيلي إلى تغيير ديناميكيات الصراع الإقليمي، اذ لم تعد التهديدات تقتصر على المواجهات العسكرية التقليدية، بل امتدت إلى فضاء غير ملموس يتسم بالغموض والتعقيد ، ومن أبرز التأثيرات التي تخص القوة السيبرانية الإسرائيلية على الأمن الإقليمي في الشرق الأوسط ، مايأتي :[39]

1- تصعيد سباق التسلح السيبراني ، اذ دفع التفوق الإسرائيلي العديد من الدول، كإيران وتركيا، إلى استثمار موارد كبيرة في تطوير قدراتها السيبرانية الهجومية والدفاعية ، وأسهم ذلك في ظهور بيئة إقليمية أكثر تقلباً، حيث تزداد مخاطر الهجمات العابرة للحدود التي قد تُفجر أزمات سياسية حتى دون وجود نية مسبقة.

2- تآكُل الحدود بين الحرب والسلم ، تستخدم إسرائيل الهجمات السيبرانية كأداة للحرب تحت عتبة الصراع المسلح ، كتعطيل أنظمة الطاقة في لبنان أو استهداف المستشفيات في غزة عبر خوادم إلكترونية ، هذه الإجراءات تخلق حالة من عدم الاستقرار المزمن، اذ يصعب تحديد الجهة الفاعلة أو الرد وفقاً لقواعد القانون الدولي.

3- تقويض الثقة بين الدول ، يؤدي غياب إطار قانوني دولي واضح للتعامل مع الهجمات السيبرانية إلى تعميق الشكوك بين الحكومات ، فعلى سبيل المثال، اتهامات إيران المتكررة لإسرائيل باختراق منشآتها النووية تزيد من حدة العداء، وتحدّ من فرص الحوار الدبلوماسي.

4- تأثيرات إنسانية واجتماعية: لا تقتصر تداعيات الهجمات السيبرانية على الجوانب الأمنية، بل تمتد إلى تعطيل خدمات أساسية للمدنيين، كالصحة والكهرباء، مما يفاقم الأزمات الإنسانية في مناطق مثل غزة أو سوريا، ويخلق ضغوطاً ديموغرافية تزيد من عدم الاستقرار.

وكخلاصة لماتقدم ، يتبين ان مجالات استخدام القوة السيبرانية الإسرائيلية تبرز عبر الهجمات على البنية التحتية الحيوية كاستهداف منشآت الطاقة، المياه، والاتصالات في دول معادية والتجسس الإلكتروني عبر جمع المعلومات الاستخباراتية من الدول الإقليمية والجهات الفاعلة،

فضلا عن حملات التضليل والتأثير عبر نشر معلومات مضللة للتأثير على الرأي العام وزعزعة الاستقرار ، والقمع الداخلي عبر استخدام الأدوات السيبرانية لمراقبة وقمع المعارضة الداخلية. [40]

اما انعكاسات القوة السيبرانية الإسرائيلية على الأمن الإقليمي في المنطقة ، فيبرز عبر تصاعد التوترات الإقليمية ، اذ أدت الهجمات السيبرانية إلى زيادة التوتر بين إسرائيل ودول الجوار ، وجرّ المنطقة الى سباق التسلح السيبراني ، عبر دفع الدول الأخرى لتعزيز قدراتها السيبرانية كرد فعل على التهديدات الإسرائيلية ، فضلا عن تأثيرات اقتصادية متوقعه ، فالخسائر المالية الناتجة عن الهجمات السيبرانية وتأثيرها على اقتصادات الدول المستهدفة تكون كبيرة جدا ، والتعاون الإقليمي والدولي عبر تعزيز التعاون بين الدول لمواجهة التهديدات السيبرانية المشتركة. [41]

ختاما ، في ظل تنامي التهديدات السيبرانية، يبرز التساؤل حول إمكانية تطوير آليات تعاون إقليمية لإدارة الصراع في الفضاء الرقمي ، فبالرغم من أن إسرائيل تُعد لاعباً رئيسياً في هذا المجال، إلا أن غياب الثقة مع جيرانها يعيق أي مبادرات مشتركة ، ومع ذلك، قد تفرض الطبيعة العابرة للحدود للتهديدات السيبرانية حاجةً موضوعية إلى حوار متعدد الأطراف، يستند إلى معايير دولية تحدّ من الاستخدام التدميري للتكنولوجية ، ويكّون توازنٌ دقيقا مطلوباً بين تعزيز الأمن القومي وإدارة التداعيات الإقليمية، في سياق تُعيد فيه القوة السيبرانية تشكيل مفاهيم السيادة والصراع في الشرق الأوسط.

المحور الثالث مستقبل القوة السيبرانية الاسرائيلية في ظل استراتيجيات القوى الإقليمية في المنطقة

أصبحت القوة السيبرانية أحد أهم أبعاد الصراع الجيوسياسي في الشرق الأوسط، اذ تُعَد إسرائيل من أبرز الفاعلين في هذا المجال ، ففي الوقت الذي تستثمر فيه إسرائيل بشكل مكثف في تقنيات الأمن السيبراني لأغراض هجومية ودفاعية، ومع تزايد أهمية الأمن السيبراني في الحروب الحديثة، ويهدف هذا المحور إلى تحليل مستقبل القوة السيبرانية الاسرائيلية وتأثيرها على الاستراتيجيات الإقليمية في السنوات القادمة ، عبر الاتي :

اولا: الانكفاء على الذات (السيادة السيبرانية)

تتجه بعض القوى الفاعلة إلى تبني استراتيجيات جديدة تتسم بالانكفاء على الذات، وهو مفهوم يشير إلى الاعتماد المتزايد على الموارد المحلية وتعزيز الاستقلالية في المجالات التكنولوجية والسيبرانية ، وتسعى اسرائيل إلى تعزيز قدراتهما السيبرانية بعيدًا عن الاعتماد المفرط على الأطراف الخارجية، وذلك لأسباب تتراوح بين التهديدات الأمنية المستمرة، والرغبة في تحقيق التفوق الإقليمي، إلى جانب تداعيات البيئة الجيوسياسية المتوترة في الشرق الأوسط ، ويتجلى

مشهد الانكفاء على الذات كأحد أبرز السيناريوهات لمستقبل القوة السيبرانية الاسرائيلية، بما يحمله من تحديات وفرص تؤثر على توازن القوى في المنطقة والاستراتيجيات الإقليمية المرتبطة بالأمن السيبراني. [42]

تُشكِّل القوة السيبرانية اليوم محوراً رئيساً في الصراعات الإقليمية، لا سيما في الشرق الأوسط، اذ تتنافس إسرائيل وإيران على تعزيز نفوذهما عبر أدوات رقمية تُمكِّن من تحقيق أهداف استراتيجية دون التورط في مواجهات عسكرية تقليدية ، وفي ظلِّ تصاعد التوترات وتغيُّر التحالفات الإقليمية، يبرز الانكفاء على الذات كسيناريو محتمل للقوة الاسرائيلية ، ممايعكس توجهها نحو تعزيز الاعتماد على القدرات الداخلية وتقليل التبعية للخارج في مجال الأمن السيبراني ، ويطرح هذا المشهد تحديات وفرصاً متشابكة، تتطلب تحليلاً معمقاً لطبيعة التفاعلات التكنولوجية والسياسية التي تُشكِّل ملامح المستقبل.

وتواجه إسرائيل تحديات داخلية قد تُعيد توجيه استراتيجياتهما السيبرانية ، اذ يؤدي الاستقطاب السياسي والانتخابات المتكررة إلى تقلبات في أولويات الأمن القومي، بينما يهدد النمو السريع للقطاع التكنولوجي بخلق ثغرات أمنية بسبب الاعتماد المفرط على البنى التحتية الرقمية ، وسيتم التطرق في هذا المحور الى الاتي :

أولا : العوامل الدافعة نحو الانكفاء على الذات في المجال السيبراني

يعتمد مفهوم الانكفاء على الذات في المجال السيبراني على سعي الدول إلى تعزيز اكتفائها التكنولوجي، سواء عبر تطوير بنى تحتية محلية أو تقليل الاعتماد على الشركاء الخارجيين ، بالنسبة لإسرائيل، التي تُصنَّف كواحدة من الدول الرائدة في الأمن السيبراني عالمياً، يعد هذا التوجه امتداداً لاستراتيجيتها التاريخية القائمة على الابتكار العسكري ـ التكنولوجي ، بدعم من الشركات التكنولوجية الكبرى والعالمية مثل سيسكو ومايكروسوفت، التي ساهمت في تطوير أنظمة اتصالات عسكرية متقدمة .[43]

وتدفع مجموعة من العوامل إسرائيل إلى تبني نهج الانكفاء على الذات في مجال القوة السيبرانية ، اذ ينبع هذا التوجه من الحاجة إلى حماية بنيتها التحتية الرقمية من الهجمات المتزايدة ، فضلًا عن إدراكها لأهمية الحفاظ على تفوقها التكنولوجي في مواجهة خصومها الإقليميين ، وقد أدى تصاعد التهديدات السيبرانية ، خاصة القادمة من إيران والجماعات المرتبطة بها ، إلى دفع إسرائيل نحو تطوير منظومتها السيبرانية بشكل مستقل ، وتقليل الاعتماد على الشراكات الخارجية في بعض المجالات الحساسة، مع تعزيز صناعتها المحلية في قطاع الأمن السيبراني.[44]

ثانيا : التحديات التي يفرضها مشهد الانكفاء على الذات

رغم الفوائد التي قد تجنيها إسرائيل من تعزيز استقلاليتها السيبرانية ، إلا أن هذا التوجه لا يخلو من تحديات جوهرية ، اذ ان أحد أبرز هذه التحديات يكمن في صعوبة تحقيق الاكتفاء الذاتي التام في قطاع شديد التعقيد كالأمن السيبراني، اذ يعتمد هذا المجال على التطورات المستمرة في البرمجيات والعتاد الحاسوبي والذكاء الاصطناعي، والتي تتطلب موارد ضخمة وخبرات متراكمة قد لا تتوفر بالكامل ضمن الحدود الوطنية ، فاسرائيل ، رغم تقدمها التكنولوجي، الا ان تبني نهج الانكفاء على الذات قد يحد من قدرتها على الاستفادة من التعاون الدولي في مجال الأمن السيبراني، مما قد يؤثر سلبًا على ديناميكية الابتكار لديها ، كما أن التحول نحو المزيد من الاستقلالية السيبرانية قد يزيد من تكلفة تطوير تقنيات محلية، خاصة في ظل بيئة تتسم بالمنافسة العالمية الشرسة.[45]

ويمكن تحديد ابرز التحديات التي تواجها والمحصورة بين القيود الداخلية والضغوط الخارجية بالاتي :[46]

1. الاستقطاب السياسي وتقلبات الأولويات : في إسرائيل، يُهدِّد الاستقطاب السياسي الداخلي وتباين الرؤى بين الأحزاب اليمينية والمعتدلة بتباطؤ الاستثمار في البنية التحتية السيبرانية ، فالتغييرات المتكررة في الحكومات قد تؤدي إلى تفتيت الرؤية الاستراتيجية الموحدة، خاصةً في ظلِّ تنامي الاعتماد على القطاع الخاص، الذي يُشكِّل 31% من الاستثمارات العالمية في المجال السيبراني وفقاً لاحدث التقارير .

2. التهديدات العابرة للحدود وتعقيدات الإسناد: تُواجه اسرائيل صعوبات في إدارة التهديدات السيبرانية المتبادلة بسبب طبيعة الهجمات غير المنسوبة (plausible deniability)، مما يُعقِّد عملية الرد وفقاً للقانون الدولي ، فالهجمات الإلكترونية التي تستهدف أنظمة المراقبة الإسرائيلية، تخلق حالة من الحرب الرمادية التي تتفادى العتبات القانونية للرد العسكري المباشر .

ثالثا : الفرص التي يوفرها الانكفاء على الذات في المجال السيبراني

على الرغم من التحديات المرتبطة بمشهد الانكفاء على الذات، إلا أن هذا التوجه يحمل في طياته فرصًا استراتيجية ، ففي الحالة الإسرائيلية، يوفر التركيز على تطوير بنية سيبرانية محلية مزيدًا من الأمان والاستقلالية في إدارة البنية التحتية الحيوية، ويقلل من مخاطر التجسس والاختراقات التي قد تحدث عند الاعتماد على التكنولوجيا الأجنبية ، كما يعزز هذا التوجه من مكانة إسرائيل

كمركز عالمي للأمن السيبراني، اذ يمكنها من تسويق منتجاتها السيبرانية لدول أخرى، مما يمنحها ميزة اقتصادية وجيوسياسية إضافية.[47]

ويمكن تحديد ابرز الفرص التي تواجها والمحصورة بين الابتكار المحلي وإعادة تشكيل التحالفات بالاتي :[48]

1. تعزيز الاكتفاء التكنولوجي: قد يُسهم الانكفاء على الذات في تسريع وتيرة الابتكار المحلي ، فإسرائيل، التي تملك قاعدة صناعية سيبرانية متقدمة مدعومة بوحدات عسكرية كوحدة 8200 تُطور تقنيات كالذكاء الاصطناعي (AI) وأنظمة التجسس كـ (بيغاسوس) ، والتي تُستخدم لاستهداف خصوم إقليميين .

2. إعادة هيكلة التحالفات الإقليمية : في سياق الانكفاء، قد تعيد كل دولة تشكيل تحالفاتها لتعزيز الأمن السيبراني ، فإسرائيل تعتمد على شراكات مع دول كالإمارات والبحرين ضمن اتفاقات إبراهيم، والتي تشمل تبادل الخبرات في مجال الأمن الرقمي .

3. استغلال الفجوات القانونية: يُتيح الغموض في القانون الدولي بشأن الهجمات السيبرانية فرصةً للدول لاستخدام هذه الأدوات دون مواجهة عواقب مباشرة ، فإسرائيل، تستغل عدم وضوح المعايير القانونية لتبرير هجماتها على البنى التحتية الإيرانية.

رابعا : التأثيرات الإقليمية لمشهد الانكفاء السيبراني

يؤثر مشهد الانكفاء على الذات في المجال السيبراني بشكل مباشر على التوازنات الإقليمية، اذ يؤدي إلى تعزيز الاستقطاب بين القوى الفاعلة في المنطقة ، اذ تسعى إسرائيل إلى ترسيخ تحالفاتها السيبرانية مع دول الخليج، خاصة الإمارات والسعودية، عبر مشاركة تقنياتها الأمنية وتعزيز التعاون في مجال الدفاع السيبراني .

كما أن التحول نحو مزيد من الاستقلالية السيبرانية قد يؤدي إلى تصاعد حروب الظل (الحروب بالوكالة) بين إسرائيل وإيران، اذ يعتمد الطرفان بشكل متزايد على العمليات السيبرانية كبديل عن المواجهات العسكرية التقليدية ، وقد نشهد في المستقبل مزيدًا من الهجمات على البنى التحتية الحيوية، كشبكات الكهرباء والمواصلات والأنظمة المصرفية، مما يزيد من تعقيد المشهد الأمني في الشرق الأوسط.[49]

ويُهدِّد الانكفاء على الذات بتعزيز ديناميكيات الصراع غير المباشر، اذ تُصبح الهجمات السيبرانية أداةً رئيسة لزعزعة الاستقرار الإقليمي ، فإسرائيل، التي تعتمد على تفوقها التكنولوجي، قد تُواجه

تصعيداً في الهجمات الإلكترونية الإيرانية المدعومة من حلفاء إقليميين، مما يُزيد من مخاطر التصعيد غير المحسوب.[50]

من ناحية أخرى، يُثير هذا المشهد تساؤلات حول إمكانية تطوير أطر حوكمة إقليمية لإدارة الصراع السيبراني ، فغياب الثقة بين إسرائيل وإيران، بالإضافة إلى انقسامات أوسع في المنطقة، يُعيق إنشاء منصات تعاونية فعّالة، مما يُبقي المنطقة عُرضةً لسباق تسلح رقمي يزيد من هشاشة البنى التحتية الحيوية .[51]

وكخلاصة لما تقدم ، وفي هذا السياق، يشير الانكفاء على الذات إلى تعزيز القدرات السيبرانية الداخلية لاسرائيل بهدف حماية بنيتها التحتية الرقمية ومعلوماتها الحساسة ، اذ تُعَدُّ إسرائيل من الدول الرائدة في مجال الأمن السيبراني، اذ تمتلك وحدة 8200 والتي تُعد أكبر وحدة في الجيش الإسرائيلي والمسؤولة عن جمع المعلومات الاستخباراتية والعمليات السيبرانية الهجومية ، تُشَبَّه هذه الوحدة بوكالات كوكالة الأمن القومي الأمريكية (NSA) ومركز الاتصالات الحكومية البريطاني (GCHQ) ، وقد نُسبت إليها عمليات سيبرانية مهمة، بما في ذلك تطوير فيروس (ستكسنت) الذي استهدف البرنامج النووي الإيراني بين عامي 2005 و2010. [52] وهنا نلاحظ القوة السيبرانية الإسرائيلية عبر بناء الحصن الرقمي المغلق عبر الاتي :[53]

أ. الاستراتيجيات:

أولا : البنية التحتية السيبرانية وتجسدت بإنشاء القيادة الوطنية للأمن السيبراني (INCD) عام 2012، التي تُراقب الهجمات وتحمي البنى التحتية الحيوية كشبكات الكهرباء والمياه ، فضلا عن تطوير الدرع السيبراني الوطني ، وهو نظام دفاعي متكامل يعتمد على الذكاء الاصطناعي للكشف عن التهديدات في الوقت الفعلي.

ثانيا: التشريعات الصارمة عبر اصدار قانون أمن الشبكات الصادر في العام (2018) الذي يُلزم الشركات الحكومية والخاصة باتباع معايير أمنية عالية وفرض عقوبات على انتهاكات البيانات، كالغرامات التي تصل إلى 3.6 مليون دولار، فضلا عن التعاون العسكري–الأكاديمي كالشراكات بين وحدة 8200 الاستخباراتية وجامعات كالتخنيون لتطوير تقنيات مراقبة متقدمة.

ب. الآثار ، وتتوزع الى الاثار الإيجابية كتصنيف إسرائيل كثاني أكثر دولة متقدمة سيبرانياً عالمياً (حسب مؤشر ITU 2023) ، والتحديات عبر ارتفاع تكاليف الحماية ، وانتقادات دولية لاستخدام تقنيات مراقبة مثل Pegasus ضد المدنيين.

ختاما ، يمثل مشهد الانكفاء على الذات في مجال القوة السيبرانية تطورًا استراتيجيًا مهمًا لإسرائيل ، اذ تسعى إلى تعزيز استقلاليتها التكنولوجية والأمنية في ظل بيئة إقليمية متوترة ، ورغم التحديات التي يفرضها هذا التوجه ، إلا أنه يحمل فرصًا استراتيجية قد تسهم في إعادة تشكيل توازن القوى في المنطقة ، وفي ظل تسارع وتيرة التطورات التكنولوجية، ستظل القوة السيبرانية عنصرًا حاسمًا في تحديد معادلات النفوذ الإقليمي، مما يجعل من الضروري متابعة هذا المشهد عن كثب لفهم تداعياته المستقبلية على الأمن والاستقرار في الشرق الأوسط ، كما يُقدِّم مشهد الانكفاء على الذات فرصاً لتعزيز الابتكار المحلي وإعادة هيكلة الاستراتيجيات الإقليمية، لكنه يُنذر أيضاً بتصاعد التهديدات غير التقليدية التي تُعمق الانقسامات .

ثانيا: الانغماس المكثف (التوجه الى الخارج)

تُشكِّل القوة السيبرانية في العقد الثالث من القرن الحادي والعشرين محورًا جوهريًا في إعادة تشكيل ميزان القوى الإقليمي، لا سيما في الشرق الأوسط، اذ تتنافس إيران مع قوى المنطقة كالسعودية واسرائيل على تعزيز نفوذهما عبر أدوات رقمية تُمكِّن من تحقيق أهداف استراتيجية بعيدة المدى ، ويُقدِّم مشهد "الانغماس المكثف" في الفضاء السيبراني رؤيةً معقدةً تجمع بين التطور التكنولوجي السريع والصراعات الجيوسياسية التقليدية، مما يفرض تحولًا في استراتيجيات الأمن القومي الايراني.

وتعتمد إسرائيل على استراتيجية هجومية–دفاعية متكاملة، تجمع بين تعطيل البنى التحتية الحيوية للخصوم، كالهجوم على ميناء الشهيد رجائي الإيراني (2020)، الذي شلَّ حركة النقل لثلاثة أيام، وحماية شبكاتها الحيوية عبر السلطة الوطنية السيبرانية (INCD) ، كما تسعى إلى تحويل الفضاء السيبراني إلى ساحة لفرض الردع، عبر إظهار القدرة على اختراق الأنظمة الإيرانية، كالهجمات المتكررة على المنشآت النووية، والتي تهدف إلى إطالة أمد المفاوضات الدولية حول البرنامج النووي الإيراني. [54]

اذ أدَّى التصاعد في النشاط السيبراني إلى إعادة تشكيل ديناميكيات الصراع الإقليمي، اذ لم تعد المواجهات تقتصر على الجبهات العسكرية، بل امتدت إلى الفضاء الرقمي، الذي يتسم بالغموض وصعوبة الإسناد، فالهجمات السيبرانية، كتلك التي استهدفت محطات الوقود الإيرانية (2021)، أو أنظمة الاتصالات في إسرائيل، تُخلق حالة من الحرب تحت عتبة الصراع المسلح، وتُضعف الثقة بين الدول، وتزيد من مخاطر التصعيد غير المحسوب. [55]

كما يُسهم هذا السباق في تعميق الانقسامات الإقليمية؛ فإسرائيل تعزز تحالفاتها مع دول كالإمارات والبحرين في إطار اتفاقات إبراهام ، والتي تشمل التعاون في مجالات الأمن السيبراني، هذا التحول يخلق نظامًا إقليميًا متعدد الأقطاب، اذ تصبح القوة السيبرانية أداة لإعادة رسم التحالفات. [56] وسيتم التطرق هنا الى الاتي :

أولا : العوامل الدافعة نحو مشهد الانغماس المكثف

يُعرَّف الانغماس المكثف في السياق السيبراني بأنه التحول نحو الاعتماد الشامل على الأدوات الرقمية في تحقيق الأهداف العسكرية والاقتصادية والسياسية، مع تعزيز القدرات الهجومية والدفاعية لمواجهة التهديدات الناشئة ، فبالنسبة لإسرائيل، التي تحتل المرتبة الخامسة عالميًا في مؤشر القوة السيبرانية وفقًا لدراسة مركز بيلفر بجامعة هارفارد ، يمثل هذا الانغماس امتدادًا لاستراتيجيتها التاريخية القائمة على الابتكار التكنولوجي والتعاون الوثيق بين القطاعات العسكرية والمدنية ، فالوحدة 8200 التابعة للاستخبارات العسكرية الإسرائيلية، على سبيل المثال، تُعد حاضنةً للكفاءات والتي أسست شركات أمنية رائدة مثل NSO Group، والتي طورت برمجيات تجسس متقدمة مثل بيغاسوس .[57]

ويرجع تبني إسرائيل لاستراتيجية الانغماس المكثف في القوة السيبرانية إلى مجموعة من العوامل المرتبطة بالبيئة الأمنية والجيوسياسية المتغيرة في المنطقة ، فمن ناحية إسرائيل، يتمثل الدافع الأساسي في الحفاظ على تفوقها التكنولوجي والأمني في مواجهة خصومها الإقليميين، اذ تدرك اسرائيل أن امتلاك قدرات سيبرانية متقدمة يمنحها ميزة استراتيجية في ردع التهديدات التقليدية وغير التقليدية ، لذلك، كثفت استثماراتها في تطوير أدوات هجومية قادرة على اختراق الأنظمة المعادية، إلى جانب تعزيز قدراتها الدفاعية عبر شراكات مع قوى كبرى مثل الولايات المتحدة والاتحاد الأوروبي.[58]

ثانيا : تحديات مشهد الانغماس المكثف في القوة السيبرانية

على الرغم من المزايا التي يتيحها الانغماس المكثف في المجال السيبراني، إلا أن هذا التوجه يفرض تحديات معقدة عليها ، اذ إن التركيز المفرط على تعزيز القدرات الهجومية قد يجعل بنيتها التحتية عرضة لردود فعل انتقامية متزايدة من قبل خصومها، خاصة في ظل تعاظم القدرات السيبرانية الإيرانية ، كما أن توسيع نطاق العمليات السيبرانية الهجومية يزيد من احتمالات حدوث تصعيد غير متوقع، اذ يمكن أن تؤدي هجمات سيبرانية واسعة النطاق إلى مواجهات عسكرية مباشرة، وهو سيناريو قد لا يكون في مصلحة إسرائيل .[59]

ويمكن تحديد ابرز التحديات التي تواجها والمحصورة بين امن القيود التكنولوجية إلى تعقيدات الصراع بالاتي :[60]

1. الفجوة التكنولوجية : تواجه إسرائيل تحديات مرتبطة بالاستقطاب السياسي الداخلي، الذي قد يُبطئ الاستثمار في تحديث البنية التحتية الرقمية، خاصةً مع الاعتماد المتزايد على القطاع الخاص، الذي يُشكِّل 31% من الاستثمارات العالمية في الأمن السيبراني .

2. تعقيدات الإسناد وغياب الإطار القانوني: تتميز الهجمات السيبرانية بطابع غير منسوب (plausible deniability)، مما يُعقِّد عملية الرد وفقًا لقواعد القانون الدولي ، فعلى سبيل المثال، الهجمات المتبادلة على المنشآت النووية الإيرانية وأنظمة المراقبة الإسرائيلية تخلق حالة من الحرب الرمادية التي تتجنب العتبات القانونية للرد العسكري المباشر ، ويُفاقم هذا الغموض من حدة العداء بين الطرفين، ويحدُّ من فرص الحوار الدبلوماسي.

3. تصاعد سباق التسلح السيبراني : أدَّى التنافس بين إسرائيل وإيران إلى تحفيز دول إقليمية أخرى، كتركيا ودول الخليج، على استثمار موارد ضخمة في تطوير قدراتها السيبرانية ، هذا السباق يُشبه إلى حدٍّ ما سباق التسلح النووي في القرن العشرين، اذ تُصبح الهيمنة التكنولوجية عاملًا حاسمًا في إعادة رسم التحالفات الإقليمية .

ثالثا : الفرص التي يتيحها مشهد الانغماس المكثف

رغم التحديات المرتبطة بهذا المشهد، إلا أن الانغماس المكثف في المجال السيبراني يتيح فرصًا استراتيجية لاسرائيل ، اذ يمنحها هذا التوجه ميزة في مجال الردع الاستراتيجي، اذ يسمح لها بتنفيذ عمليات استباقية ضد التهديدات المحتملة، مما يعزز أمنها القومي ، كما أن التفوق السيبراني يعزز من قدرة إسرائيل على بناء تحالفات دولية، اذ أصبحت واحدة من الدول الرائدة في تصدير تقنيات الأمن السيبراني إلى مختلف أنحاء العالم، مما يمنحها نفوذًا اقتصاديًا وسياسيًا إضافيًا.[61]

ويمكن تحديد ابرز الفرص التي تواجه كلا الدولتين والمحصورة بين الابتكار وإعادة تشكيل التحالفات بالاتي :[62]

1. تعزيز الاكتفاء التكنولوجي: قد يُسرع الانغماس المكثف من وتيرة الابتكار المحلي ، فإسرائيل، التي تملك قاعدة صناعية سيبرانية متقدمة ، تُطور تقنيات كالذكاء الاصطناعي وأنظمة التحكم الذاتي، والتي تُستخدم لاستهداف الخصوم الإقليميين .

2. إعادة هيكلة التحالفات الإقليمية: في ظل التنافس السيبراني، تعيد إسرائيل تشكيل تحالفاتها مع دول كالإمارات والبحرين ضمن اتفاقات إبراهام ، والتي تشمل تبادل الخبرات في مجال الأمن الرقمي.

3. استغلال الفجوات في النظام الدولي: يُتيح الغموض في التشريعات الدولية المتعلقة بالفضاء السيبراني فرصًا للدول لاستخدام أدوات رقمية دون مواجهة عواقب مباشرة ، فإسرائيل، على سبيل المثال، تستغل هذه الفجوات لتبرير هجماتها على البنى التحتية الإيرانية .

رابعا : التأثيرات الإقليمية لمشهد الانغماس المكثف

يؤثر الانغماس المكثف في المجال السيبراني بشكل مباشر على الاستراتيجيات الإقليمية، اذ يؤدي إلى تصاعد المنافسة بين القوى الإقليمية والدولية ، فمن جهة، تسعى إسرائيل إلى توظيف قوتها السيبرانية كأداة للردع والضغط على خصومها، سواء عبر استهداف البنية التحتية الإيرانية أو عبر التعاون مع دول الخليج لتعزيز الأمن السيبراني المشترك ، وقد انعكس ذلك في توقيع اتفاقيات تعاون سيبراني مع دول كالإمارات والبحرين، مما يعكس تحولًا في موازين القوى السيبرانية في المنطقة.[63]

ويُهدِّد الانغماس السيبراني المكثف بتعزيز ديناميكيات الصراع غير المباشر، اذ تُصبح الهجمات الإلكترونية أداةً رئيسة لزعزعة الاستقرار ، فالهجمات على البنى التحتية الحيوية، كشبكات الطاقة والموانئ، قد تؤدي إلى اضطرابات اقتصادية واجتماعية واسعة النطاق، كما حدث في الهجمات على ميناء الشهيد رجائي الإيراني عام 2020، والتي شلت حركة النقل لثلاثة أيام ، في المقابل، قد تُعاني إيران من تراجع قدراتها بسبب العزلة الدولية، مما يدفعها إلى اعتماد استراتيجيات هجينة تجمع بين الحرب السيبرانية والحرب بالوكالة . [64]

وكخلاصة لما تقدم ، يشير الانغماس المكثف إلى الاستخدام النشط والعدواني للقدرات السيبرانية كجزء من الاستراتيجيات العسكرية والدبلوماسية ، ويمكن ملاحظة ذلك على إسرائيل ، اذ تُدمج العمليات السيبرانية بشكل وثيق في الاستراتيجيات العسكرية الإسرائيلية ، فعلى سبيل المثال، استخدمت الوحدة 8200 الذكاء الاصطناعي لتحديد أهداف تابعة لحركة حماس ، كما يُعتقد أن إسرائيل نفذت هجمات سيبرانية لتعطيل البنية التحتية لخصومها، كالهجوم على شركة الاتصالات اللبنانية (أوجيرو) في عام 2017. [65] وهنا على نلاحظ القوة السيبرانية الاسرائيلية عبر التحالف التكنولوجي مع القوى العظمى يكمن بالاتي : [66]

أ. الشراكات الدولية: وتتنوع الى :

أولا : الولايات المتحدة عبر التعاون في مبادرة الدفاع السيبراني الثنائي (2020)، والتي تشمل تبادل البيانات الاستخباراتية بين وكالة الأمن القومي الأمريكي (NSA) ووالحدة 8200 وتمويل مشاريع مشتركة كتطوير أنظمة Zero Trust Architecture.

ثانيا : دول الخليج ، فعقب اتفاقية التطبيع مع الإمارات (2020)، أُطلقت مشاريع عديدة كمركز الأمن السيبراني الإماراتي–الإسرائيلي في دبي ، فضلا عن تعاون مع السعودية في حماية أنظمة النفط من الهجمات الإيرانية.

ب. المبادرات الإقليمية: وتكمن بمنتدى الشرق الأوسط للذكاء الاصطناعي بمشاركة إسرائيلية لإقناع دول المنطقة بتبني تقنياتها الأمنية ، فضلا عن التدريبات العسكرية المشتركة كمناورة Blue Olive مع اليونان وقبرص لاختبار الدفاعات السيبرانية.

وهكذا ، يمثل مشهد الانغماس المكثف في القوة السيبرانية تحولًا استراتيجيًا بارزًا في لإسرائيل ، عبر تعزيز قدراتها في هذا المجال لتحقيق أهدافه الأمنية والجيوسياسية ، ورغم التحديات المرتبطة بهذا التوجه، إلا أنه يتيح فرصًا استراتيجية لها، اذ يمكنها من فرض نفوذهما بوسائل غير تقليدية ، ومع استمرار تصاعد الصراع السيبراني، من المرجح أن يشهد الشرق الأوسط مزيدًا من الهجمات المتبادلة، مما قد يؤدي إلى إعادة تشكيل معادلات القوة الإقليمية ، وفي ظل هذه التطورات، ستظل القوة السيبرانية عنصرًا حاسمًا في تحديد مسارات الصراع والتوازنات الأمنية في المنطقة، مما يجعل من الضروري دراسة تأثيراتها المستقبلية بعناية لفهم مآلات الصراع السيبراني بين القوى الإقليمية.

ختاما يُشكِّل الانغماس المكثف في القوة السيبرانية تحديًا وجوديًا للدول الإقليمية، اذ تجد نفسها في سباق ضد الزمن لتطوير أدوات دفاعية وهجومية قادرة على مواكبة التهديدات المتطورة ، اذ تملك إسرائيل التفوق التكنولوجي والشراكات الدولية، ومع استمرار غياب الإطار القانوني الدولي، يظل الشرق الأوسط ساحةً لصراع سيبراني معقد، تُعيد فيه القوة الرقمية تعريف مفاهيم السيادة والأمن في عصرٍ يُسيطر عليه الغموض الرقمي ، وقد تكون الفرصة الوحيدة لاحتواء هذا الصراع تكمن في تعزيز الحوار متعدد الأطراف، لكن تحقيق ذلك يظل رهينًا بتغيير جذري في الاستراتيجيات الإقليمية المتبناة.

ثالثا : احتمالية زيادة فاعلية القوة السيبرانية

تعد القوة السيبرانية اليوم واحدة من أبرز الأدوات التي تعتمد عليها الدول في تعزيز نفوذها الاستراتيجي وتحقيق أهدافها الأمنية والسياسية، خاصة في منطقة الشرق الأوسط التي تشهد صراعات وتنافسات معقدة ، وتبرز وإيران كفاعل رئيسي في هذا المجال، اذ عملت على تطوير قدراتها السيبرانية بشكل مكثف خلال العقود الأخيرة ، ومع تزايد أهمية الفضاء السيبراني كأحد مجالات الصراع الحديثة، فإن احتمالية زيادة فاعلية القوة السيبرانية لاسرائيل في المنطقة الإقليمية تمثل مشهدًا مستقبليًا قد يؤثر بشكل جذري على التوازنات الإقليمية والاستراتيجيات الأمنية للدول المجاورة .

وتستند احتمالية زيادة فاعلية القوة السيبرانية الاسرائيلة إلى مجموعة من العوامل التي تعزز هذا التوجه وتدفع بها إلى الاستثمار المستمر في تطوير تقنيات الهجوم والدفاع السيبراني ، وسنتناول هنا مجموعة من التحديات والفرص التي قد تواجهها اسرائيل في ظل السباق المتصاعد نحو تعزيز القدرات السيبرانية وكالاتي

أولا :الدوافع التي تعزز احتمالية زيادة فاعلية القوة السيبرانية الإسرائيلية والإيرانية

تستند احتمالية زيادة فاعلية القوة السيبرانية الاسرائيلية إلى مجموعة من العوامل التي تعزز هذا التوجه وتدفع الدولتين إلى الاستثمار المستمر في تطوير تقنيات الهجوم والدفاع السيبراني ، فمن جهة إسرائيل، تعتمد في استراتيجيتها السيبرانية على مبدأ التفوق التكنولوجي كأداة لضمان أمنها القومي وردع التهديدات المتزايدة التي تشكلها إيران والجماعات المسلحة المدعومة منها ، ولذلك، تستثمر اسرائيل بشكل كبير في تقنيات الذكاء الاصطناعي وتحليل البيانات لتطوير آليات هجومية متقدمة قادرة على تنفيذ عمليات اختراق سيبراني دقيقة ضد أهداف عسكرية ومدنية داخل إيران أو ضد حلفائها في المنطقة.[67]

ويمكن تحديد ابرز الدوافع التي تواجهها في سياق التنافس السيبراني بالاتي :[68]

1. التطور التكنولوجي والاستثمارات الضخمة ، تستثمر إسرائيل بشكل كبير في البنية التحتية السيبرانية ، اذ بلغت استثمارات شركات الأمن السيبراني الإسرائيلية 8.8 مليار دولار في عام 2022، مدفوعةً بزيادة الثغرات الأمنية عبر جائحة كورونا ، كما طورت إسرائيل القبة السيبرانية، وهي منظومة دفاعية تعتمد على الذكاء الاصطناعي والتعاون مع شركات كجوجل ومايكروسوفت لمراقبة التهديدات في الوقت الفعلي .

2- إعادة تشكيل التحالفات الإقليمية ، أدت اتفاقات إبراهام (2020) إلى تعزيز التعاون السيبراني بين إسرائيل ودول الخليج كالإمارات والسعودية، التي تسعى إلى حماية بنيتها من الهجمات الإيرانية ، فعلى سبيل المثال، تعاونت شركات إسرائيلية مع أرامكو السعودية للرد على هجمات سيبرانية في 2012 ، في المقابل .

3. الحرب غير المتماثلة وتجنب التصعيد العسكري ، تُفضل إسرائيل استخدام الأدوات السيبرانية لتحقيق أهداف عسكرية دون خسائر بشرية ، كما حدث في الهجوم على ميناء الشهيد رجائي الإيراني (2020)، الذي شل الحركة الاقتصادية لثلاثة أيام.

ثانيا :التحديات المرتبطة بزيادة فاعلية القوة السيبرانية الإسرائيلية والإيرانية

رغم الفرص التي قد توفرها زيادة الفاعلية السيبرانية لإسرائيل ، إلا أن هذا السيناريو لا يخلو من تحديات معقدة قد تؤثر على مدى نجاحها في تحقيق أهدافهما الاستراتيجية ، أحد أبرز هذه التحديات يتمثل في سباق التسلح السيبراني الذي قد يؤدي إلى تصعيد غير مسبوق في حجم ونوعية الهجمات الإلكترونية بين الطرفين، مما قد ينتج عنه تداعيات غير مقصودة تؤثر على الأمن الإقليمي ، فعلى سبيل المثال، قد تؤدي الهجمات السيبرانية واسعة النطاق إلى تعطيل منشآت حيوية، مما قد يدفع الأطراف المتضررة إلى الرد بوسائل عسكرية تقليدية، وهو ما قد يفتح المجال أمام مواجهات أوسع نطاقًا تتجاوز حدود الحرب السيبرانية.

بالإضافة إلى ذلك، يواجه كلا البلدين تحديات تتعلق بمدى قدرتهما على تطوير بنى تحتية سيبرانية قادرة على تحمل الهجمات المضادة ، ففي الحالة الإسرائيلية، ورغم تفوقها التكنولوجي، فإن ازدياد فاعلية الهجمات الإيرانية قد يؤدي إلى استهداف منشآت حساسة كشبكات الاتصالات والأنظمة المالية، مما قد يخلق نقاط ضعف غير متوقعة في الاقتصاد الإسرائيلي.[69]

ومن التحديات الأخرى التي قد تواجه زيادة فاعلية القوة السيبرانية الاسرائيلية هو التداخل المتزايد بين الفضاء السيبراني والجهات الفاعلة غير الحكومية ، فمع تطور التقنيات السيبرانية، أصبح بإمكان جهات فاعلة غير حكومية كالجماعات المسلحة أو الميليشيات السيبرانية تنفيذ عمليات معقدة تؤثر على الدول، مما قد يزيد من حالة عدم الاستقرار في المنطقة ، وقد تستفيد هذه الجهات من الفوضى السيبرانية الناتجة عن التصعيد بين إسرائيل وإيران لشن هجمات تستهدف بنى تحتية حساسة في دول أخرى، مما قد يعقد المشهد الأمني الإقليمي بشكل أكبر.[70]

ويمكن تحديد ابرز التحديات التي تواجهها بالاتي :[71]

1. الفجوة التكنولوجية والقيود الاقتصادية ، تواجه إسرائيل مخاطر مرتبطة بالاعتماد المفرط على البنية الرقمية، اذ تعرضت لـ3,400 هجوم سيبراني خلال الأشهر الأولى من حرب غزة 2023، وفقًا لتقارير أمنية.

2. تعقيدات الإسناد وغياب الإطار القانوني ، تتميز الهجمات السيبرانية بطابع غير منسوب، مما يُعقِّد الردود وفقًا لقواعد القانون الدولي .

3. سباق التسلح السيبراني وتصاعد المخاطر، أدَّى التنافس بين الطرفين إلى تحفيز دول إقليمية أخرى، كتركيا، لاستثمار موارد ضخمة في تطوير قدراتها، مما يزيد من هشاشة البنى التحتية الحيوية في المنطقة ، فالهجمات على محطات الوقود الإيرانية (2021) أظهرت كيف يمكن لأدوات سيبرانية واحدة شل اقتصاد دولة بأكملها.

ثالثا : الفرص التي يوفرها مشهد زيادة فاعلية القوة السيبرانية

رغم التحديات المرتبطة بزيادة فاعلية القوة السيبرانية الاسرائيلية ، إلا أن هذا السيناريو يوفر فرصًا استراتيجية قد تعزز من مكانتها على المستوى الإقليمي والدولي ، في الحالة الإسرائيلية، يمثل التفوق في المجال السيبراني فرصة لتوسيع نفوذها في الشرق الأوسط عبر تقديم نفسها كشريك رئيس للدول التي تسعى إلى تعزيز قدراتها السيبرانية ، وقد انعكس ذلك بالفعل في زيادة التعاون السيبراني بين إسرائيل ودول الخليج، اذ تسعى اسرائيل إلى تصدير تقنياتها الأمنية لحلفائها الإقليميين بهدف الحد من التهديدات السيبرانية القادمة من إيران. [72]

ويمكن تحديد ابرز الفرص التي تواجهها بالاتي :[73]

1. تعزيز الاكتفاء التكنولوجي عبر الابتكار ، قد يُسرع التنافس السيبراني وتيرة الابتكار المحلي ، فإسرائيل، التي تملك قاعدة صناعية متقدمة، تُطور تقنيات كالذكاء الاصطناعي وأنظمة المراقبة المتطورة كـ(بيغاسوس).

2. إعادة هيكلة الدبلوماسية الإقليمية ، يُشكل التعاون السيبراني مدخلاً لتعزيز العلاقات بين إسرائيل ودول الخليج ، اذ أصبحت التكنولوجيا ركيزةً اساسية للدبلوماسية ، كما ظهر في زيارة نتنياهو إلى عمان (2018) ، في المقابل، قد تدفع التهديدات المشتركة دولاً كالسعودية إلى تعميق التعاون مع إسرائيل رغم الخلافات السياسية.

3. استغلال الفجوات في النظام الدولي ، يسمح الغموض التشريعي الدولي باستخدام الأدوات السيبرانية دون عواقب مباشرة ، فإسرائيل تستغل هذه الثغرات لتبرير هجماتها.

رابعا : التأثيرات الإقليمية لمشهد زيادة فاعلية القوة السيبرانية

يُهدِّد تصاعد الفاعلية السيبرانية بتحويل المنطقة إلى ساحة لفوضى رقمية مُمنهجة ، اذ تُستهدف البنى التحتية الحيوية بشكل متكرر، كما حدث في هجمات إسرائيل على محطات الوقود الإيرانية، أو تعطيل الاتصالات في غزة ، ومع ذلك، قد تفرض الطبيعة العابرة للحدود لهذه التهديدات حاجةً موضوعية إلى حوار إقليمي، كإنشاء منصات لتبادل المعلومات أو تطوير أطر حوكمة مشتركة، وإن كان غياب الثقة بين إسرائيل وإيران يُعقّد هذا المسار.

فعلى المستوى الإقليمي، فإن ازدياد فاعلية القوة السيبرانية قد يدفع دول الشرق الأوسط إلى تبني استراتيجيات أكثر تطورًا في مجال الأمن السيبراني، اذ قد تجد العديد من الدول نفسها مضطرة لتعزيز بنيتها التحتية الدفاعية لمواجهة التهديدات المتزايدة ، وقد يخلق هذا الواقع فرصًا اقتصادية جديدة لشركات التكنولوجيا والأمن السيبراني، خاصة في ظل تزايد الطلب على حلول الحماية الإلكترونية المتقدمة.[74]

ختاما ، يمثل مشهد احتمالية زيادة فاعلية القوة السيبرانية الاسرائيلية في المنطقة الإقليمية تطورًا استراتيجيًا بارزًا قد يعيد تشكيل موازين القوى في الشرق الأوسط ، وعلى الرغم من أن هذا السيناريو يوفر فرصًا لتعزيز نفوذها وتحقيق أهدافها الأمنية والسياسية، إلا أنه يحمل في طياته تحديات كبيرة قد تؤدي إلى تصعيد الصراع السيبراني وتفاقم حالة عدم الاستقرار في المنطقة ، وفي ظل التقدم المستمر في مجال التقنيات السيبرانية، فإن هذا المشهد يظل مفتوحًا على عدة احتمالات تتراوح بين تعميق سباق التسلح السيبراني وبين إمكانية نشوء أنظمة جديدة للتعاون الدولي في مجال الأمن السيبراني ، وفي كلتا الحالتين، يبقى الفضاء السيبراني أحد أبرز ساحات التنافس في الشرق الأوسط، مما يجعل من الضروري متابعة تطوراته وتأثيراته على الأمن الإقليمي والدولي بشكل مستمر.

الخاتمة

وعليه ، يُشكّل التفوق التكنولوجي والمرونة الاستراتيجية عاملين حاسمين في تحديد ملامح الصراع السيبراني المستقبلي ، اذ تمتلك إسرائيل أدوات متطورة وشراكات دولية، ومع استمرار غياب إطار قانوني دولي، تظل المنطقة عُرضةً لتصعيد غير متوقع، قد يُعيد تعريف مفاهيم الأمن والسيادة في عصرٍ تُهيمن عليه القوة الرقمية ، وقد يكون السبيل الوحيد لاحتواء هذا الصراع هو تعزيز الشفافية وبناء آليات ثقة، لكن تحقيق ذلك يبقى رهينًا بإرادة سياسية غائبة في المدى المنظور.

وهكذا، يُتوقع أن يستمر الصراع السيبراني بين إسرائيل والقوى الإقليمية في المنطقة خاصة ايران في التصاعد، مع زيادة التركيز على تطوير القدرات الهجومية والدفاعية في هذا المجال. وسيكون

لهذا الصراع تأثيرات كبيرة على الأمن الإقليمي والدولي، مما يستدعي تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية المتزايدة.

المصادر:

[1] داليا رشدي، تأثير سوء الإدراك في الصراعات والأزمات "إطار تحليلي"، مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 203، مركز الاهرام ، القاهرة ، 2016 ، ص 76.

[2] المصدر نفسه ، ص 77

[3] سيد أحمد قوجيلي، فهم الأمننة: مقاربة نقدية للدراسات الأمنية، مجلة شؤون الأوسط ، مركز الوحدة العربية ، بيروت ، العدد 153، 2020 ، ص 176.

[4] داليا رشدي، تأثير سوء الإدراك في الصراعات والأزمات ، مصدر سبق ذكره ، ص 180

[5] المصدر نفسه ، ص 182

[6] مجدي كامل، حروب الجيل الرابع "الحرب بالوكالة" كيف يتم اذكاؤنا بالطائفية وإشعال الحروب الأهلية ودعم الجماعات الإرهاب واستخدام الطابور الخامس لإفشال الدولة وإخضاعها للإدارة الأمريكية؟، دار الكتاب العربي، دمشق، 2021 ، ص 78.

[7] انجي محمد مهدي، الجهاد الإلكتروني: دراسة لتنظيم داعش واستراتيجية الولايات المتحدة لمواجهته، مجلة دراسات ، سوريا، المجلد22، العدد 2، 2021 ، ص200.

[8] المصدر نفسه ، 202

[9] ريما موسي، إرهاب "الذئاب المنفردة"، مجلة قضايا التطرف والجماعات المسلحة، المركز الديمقراطي العربي ، العدد 5 ، بيروت ، 2021 ، ص 161.

[10] المصدر نفسه ، ص 162

[11] عزيز نوري وسميرة سليمان، التهديدات الهجينة بين إشكالية التعريف وأنماط المواجهة، المجلة الجزائرية للأمن والتنمية ، جامعة سيدي بوشناف، المجلد 10، العدد 1، 2021 ، ص 119.

[12] حكيم غريب، الإرهاب السيبراني والأمن الدولي، مصدر سبق ذكره، ص 221.

[13] عزيز نوري وسميرة سليمان، التهديدات الهجينة بين إشكالية التعريف وأنماط المواجهة ، مصدر سبق ذكره ، ص 121

[14] مارتي كوتشاك، متغيرات ساحة المعركة السيبرانية، الأمن والدفاع العربي، العدد 4، 2022 ، ص 54.

[15] المصدر نفسه ، ص 55

[16] رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مفاهيم استراتيجية، القاهرة، المركز العربي لأبحاث الفضاء الإلكتروني، 2025، ص 35 .

[17] المصدر نفسه ، ص 36

[18] باسل رزق، إسرائيل على الجبهة الإلكترونية، موقع متراس، 2023، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://metras.co/

[19] علاء عبد العزيز عبد العازي، توازن إدراك التهديد وآفاق الحوار المتوسطي لحلف الناتو، 2024، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://emirate.wiki/wiki/Balance_of_threat

[20] المصدر نفسه .

[21] أحمد بن علي الميموني، الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل، مجلة الدراسات الإيرانية ، العدد12، الرياض، 2020، ص75-79.

[22] المصدر نفسه ، ص 81 .

[23] كمال الاسطل، نظرية الحرب السيبرانية والجيوش السيبرانية: جيوش السوشيال ميديا والأمن السيبراني، مطبعة وهران ، الجزائر ، 2022 ، ص 118 -119 .

[24] هيبت الغربي ، دور القوة الناعمة في السياسة الخارجية الايرانية ومستقبلها في الشرق الأوسط ، مصدر سبق ذكره ، ص ص24 - 28.

[25] فاطمة عبد الفتاح، تطور توظيف جماعات العنف للإرهاب السيبراني، مجلة السياسة الدولية، مركز الأهرام ، القاهرة، العدد 208، 2017 ، ص 109.

[26] المصدر نفسه ، ص 111 .

[27] محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها ، مصدر سبق ذكره ، ص120 .

[28] فاتح حارك ورياض حمدوش، الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني، المجلة الجزائرية للأمن الانساني، العدد 9 ، الجزائر ، 2024 ، ص 212 .

[29] المصدر نفسه ، ص 214 .

[30] صباح عبدالصبور عبدالحي، استخدام القوة الإلكترونية في التفاعلات الدولية ، مصدر سبق ذكره ، ص 127.

[31] فاتح حارك ورياض حمدوش، الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني ، مصدر سبق ذكره ، ص 218.
[32] المصدر نفسه ، ص 220
[33] جمال رضوان، الأمن السيبراني: أولوية في استراتيجيات الدفاع، مجلة الجيش، سوريا ، العدد 630، 2022 ، ص 176.
[34] مصطفى يوسف كافي وآخرون، الإعلام والإرهاب الإلكتروني ، مصدر سبق ذكره ، ص 185
[35] أماني عصام محمد، استخدام اسرائيل للقوة السيبرانية ، مصدر سبق ذكره ، ص 116 .
[36] سيد أحمد قوجيلي، فهم الأمننة: مقاربة نقدية للدراسات الأمنية، مجلة شؤون الأوسط ، بيروت، العدد 183، 2024 ، ص 176.
[37] المصدر نفسه ، ص 180
[38] انجي محمد مهدي، الجهاد الإلكتروني: دراسة لتنظيم داعش واستراتيجية الولايات المتحدة لمواجهته، مجلة دراسات، بغداد، العدد 22، 2025 ، ص200.
[39] فاطمة حسان عيتاني، الوحدة الإسرائيلية 8200 ودورها في خدمة التكنولوجيا التجسسية الإسرائيلية، مركز الزيتونة للدراسات والاستشارات، بيروت، 2023، ص 118 .
[40] المصدر نفسه ، ص ص 120 -121 .
[41] خالد المعيني، الصراع الدولي بعد جائحة كورونا ، مصدر سبق ذكره ، ص 152.
[42] محمد مؤنس محب الدين، تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها ، مصدر سبق ذكره ، ص 133 .
[43] مرعى على الرمحي، الحرب السيبرانية ومتطلبات الأمن القومي الجديدة ، مصدر سبق ذكره ، ص 115 .
[44] عزيز نوري وسميرة سليمان، التهديدات الهجينة بين إشكالية التعريف وأنماط المواجهة، المجلة الجزائرية للأمن والتنمية، الجزائر، العدد 11، 2025 ، ص 119.
[45] المصدر نفسه ، ص 225 .
[46] فاطمة بيرم، مصدر سبق ذكره ، ص 229
[47] محمد زهير عبد الكريم، الإرهاب السيبراني: أزمة عالمية جديدة، مجلة قضايا سياسية ، العدد 64 ، كلية العلوم السياسية جامعة النهرين ، 2021 ، ص 271
[48] استراتيجية اسرائيلية شرسة للأمن الإلكتروني تستهدف ايران، عربية sky news، أبو ظبي، 2024، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://www.skynewsarabia.com/world/1184165
[49] علاء عبدالعزيز عبد العازي، توازن إدراك التهديد وآفاق الحوار المتوسطي لحلف الناتو، 2024، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://emirate.wiki/wiki/Balance_of_threat
[50] المصدر نفسه .
[51] كمال الاسطل، نظرية الحرب السيبرانية والجيوش السيبرانية ، مصدر سبق ذكره ، ص 176.
[52] ريما موسي، إرهاب "الذئاب المنفردة"، مجلة قضايا التطرف والجماعات المسلحة، المركز الديمقراطي العربي، برلين، العدد 15، 2025 ، ص 161.
[53] المصدر نفسه ، ص ص 162- 263
[54] هيبت الغربي ، دور القوة الناعمة في السياسة الخارجية الايرانية ومستقبلها في الشرق الأوسط ، مصدر سبق ذكره ، ص 122 .
[55] ميثاق بيات ألضيفي، ايران والاستراتيجية السيبرانية، مقال منشور على شبكة النبأ المعلوماتية، 2024، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://annabaa.org/arabic/informatics/17712
[56] المصدر نفسه .
[57] فراس إلياس، عقيدة الأمن السيبراني في إيران ومعادلات المواجهة مع أمريكا، مصدر سبق ذكره .
[58] أحمد سالم المنتصر، تجليات جديدة في مفهوم الأمن الإلكتروني "السيبراني" (دراسة مقارنة)، مصدر سبق ذكره ، ص 210 .
[59] هارتس، قراصنة موالون لإيران يهاجمون شركة طبية أمريكية ، مصدر سبق ذكره .
[60] مصطفى شلش ، الحرب السيبرانية في الشرق : ايران واسرائيل نموذجا ، مصدر سبق ذكره .
[61] سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي- رؤية مستقبلية، مصدر سبق ذكره ، ص 100 .
[62] مليندا كوهون ، عمليات ضبط المعلومات في الفضاء السيبراني الإيراني ، مصدر سبق ذكره ، ص 207
[63] محمد فريد عزي ، النشاط السيبراني الايراني مابين السر والعلن ، مصدر سبق ذكره .
[64] إدريس عطية، الحاجة العالمية لتطبيق الهندسة الأمنية المستدامة ، مصدر سبق ذكره ، ص210 .
[65] المصدر نفسه ، 212 .
[66] استراتيجية اسرائيلية شرسة للأمن الإلكتروني تستهدف ايوان، عربية sky news، أبو ظبي، 2022، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://www.skynewsarabia.com/world/1184165
[67] فاتح حارك ورياض حمدوش، الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني ، مصدر سبق ذكره ، 239.

[68] خالد عبد العظيم، التحولات الكبرى في الاستراتيجية العالمية، مصدر سبق ذكره ، ص 187 .
[69] أمينة فلاح، مكانة القوة الذكية في المدرك الاستراتيجي ، مصدر سبق ذكره ، ص 231 .
[70] رغدة البهي، الردع السيبراني ، مصدر سبق ذكره
[71] أمينة فلاح، مكانة القوة الذكية في المدرك الاستراتيجي ، مصدر سبق ذكره ،ص ص 233 -235
[72] فايروس ضرب برنامج إيران النووي، عربي bbc news، 2025، الانترنيت ، تاريخ الولوج 2024/6/5 ، الموقع: https://www.bbc.com/arabic/middleeast/2010/11
[73] المصدر نفسه ، ص 203
[74] مارتي كوتشاك، متغيرات ساحة المعركة السيبرانية، ترجمة مجلة الأمن والدفاع السعودية ، المملكة العربية السعودية ، 2024 ، ص 76 .