

المركز العربي للأبحاث ودراسة السياسات
ARAB CENTER FOR RESEARCH & POLICY STUDIES



(معهد الدوحة)

www.dohainstitute.org

مراجعة كتاب

إسرائيل والحرب الالكترونية

قراءة في كتاب: حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل

د. محمود محارب

سلسلة (مراجعة كتب)

المحتوى

إسرائيل والحرب الالكترونية.....	
قراءة في كتاب: حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل	
إسرائيل والفضاء الالكتروني.....	٤
تدابير إسرائيل للدفاع عن فضاءها الالكتروني	٤
أولاً: البنية التحتية الحكومية لعصر الإنترنت.....	٥
ثانياً: السلطة الرسمية لحماية المعلومات.....	٥
ثالثاً: هيئة السايبر في الجيش الإسرائيلي.....	٥
رابعاً: وحدة إدارة أنظمة المعلومات.....	٦
خامساً: هيئة السايبر الوطنية.....	٦
استراتيجية للدفاع عن الفضاء الالكتروني الإسرائيلي.....	٧
الفضاء الالكتروني في استراتيجية الأمن الإسرائيلي.....	٨

مراجعة كتاب: حرب في الفضاء الإلكتروني:

اتجاهات وتأثيرات على إسرائيل

شمونيل ليفن ودافيد بن سيمان - طوفه

معهد دراسات الأمن القومي، تل أبيب، حزيران / يونيو ٢٠١١

الفضاء الإلكتروني (Cyberspace) ^(١) مصطلح حديث، ظهر في العقود الأخيرة نتيجة لثورة تكنولوجيا المعلومات. ويشمل الفضاء الإلكتروني، في ما يشمل، جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستخدمين ومنفصلة عن شبكة الإنترنت العامة.

وقد تعاضم في الفترة الأخيرة اهتمام مراكز الأبحاث والنخب في إسرائيل بموضوع الحرب في الفضاء الإلكتروني. ونظم معهد أبحاث الأمن القومي التابع لجامعة تل أبيب، في التاسع من حزيران/ يونيو ٢٠١١، يوماً دراسياً تناول هذا الموضوع، وتحت عنوان "حرب الفضاء الإلكتروني - تحديات على الصعيد العالمي والسياسي والتكنولوجي". وافتتح اليوم الدراسي رئيس الحكومة الإسرائيلية بنيامين نتنياهو، وتحدث فيه نخبة من الباحثين والمختصين الإسرائيليين، الذين أكدوا على أهمية الحرب في الفضاء الإلكتروني بالنسبة لأمن إسرائيل. وشدد بنيامين نتنياهو في مداخلته على أهمية وحيوية هذا الموضوع بالنسبة لإسرائيل، وأكد على ضرورة أن تصبح إسرائيل دولة عظمى في مجال حرب الفضاء الإلكتروني، وأن تكون فاعلاً هاماً على الصعيد العالمي في هذا المضمار ^(٢). كما ناقشت "لجنة العلم" التابعة للكنيست في الرابع من تموز/ يوليو ٢٠١١ موضوع الحرب في الفضاء الإلكتروني، واستمعت إلى الخبراء والمختصين في هذا المجال. وأشار الجنرال البروفيسور يتسحاق بن يسرائيل، رئيس "المجلس الوطني للبحث والتطوير" أمام "لجنة العلم"،

^١ - يعرف الاتحاد الدولي للاتصالات التابع للأمم المتحدة (ITU) الفضاء الإلكتروني كالتالي: Cyberspace: The physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users. Source: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>

^٢ - <http://news.walla.co.il/?w=/٩/١٨٣٠٦٩٣/@/@/item/printer>

إلى وجود فجوة في إسرائيل بين الاحتياطات الدفاعية عن البنى التحتية الأمنية وبين الدفاع عن بنى تحتية مدنية حساسة وهامة ضد هجمات في الفضاء الإلكتروني. وأضاف أن الهجمات في الفضاء الإلكتروني تحدث يومياً وأنها ليست جزءاً من الخيال العلمي بل هي حقيقة واقعة. واستطرد قائلاً: "جزء من هذه الهجمات يسبب ازعاجاً، بينما قد يلحق الجزء الآخر من هذه الهجمات أضراراً جسيمة. فهناك الكثير من البرامج والأنظمة المتطورة التي يمكن استعمالها في الفضاء الإلكتروني التي قد تشل وتعطل عمل مرافق الدولة الأساسية مثل: البورصة والبنوك والكهرباء والمواصلات والاتصالات، والناس لا يدركون عمق الخطر". وأشار يتسحاق بن إسرائيل إلى أن أحد أهداف إقامة "هيئة السايبر الوطنية" في إسرائيل، التي أعلن عن تأسيسها في أيار/ مايو ٢٠١١، هو إنشاء "الحاسوب المتطور" في إحدى الجامعات بإسرائيل، إذ لا تملك إسرائيل مثل هذا الحاسوب، ويحظر بيعه إليها، لعدم توقيعها على اتفاقية حظر انتشار الأسلحة النووية. أما رئيس "لجنة العلم" التابعة للكنيست، منير شطريت، فقال في سياق تشديده على موضوع تأمين الفضاء الإلكتروني، إنه بالإمكان التسبب في انهيار إسرائيل من دون دبابات وطائرات، وإنما بواسطة حرب الفضاء الإلكتروني^(٣).

وفي سياق هذا الاهتمام الإسرائيلي بحرب الفضاء الإلكتروني صدر باللغة العبرية، في حزيران/ يونيو ٢٠١١، عن معهد أبحاث الأمن القومي التابع لجامعة تل أبيب، كتاب "حرب الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل"، للباحثين شموئيل ايفن ودافيد بن سيمان- طوف، العاملين في معهد أبحاث الأمن القومي. ويضم الكتاب مقدمة وأربعة فصول وخاتمة وملحقين، بما مجموعه تسعين من الصفات. وأشار المؤلفان إلى أن الفضاء الإلكتروني بات مجال قتال جديد، وانضم بذلك إلى مجالات القتال الأخرى، في اليابسة والبحر والجو والفضاء. فالدول المتطورة وجيوشها تزيد من نشاطاتها وأبحاثها في الفضاء الإلكتروني الذي أصبح يشكل بالنسبة لها مصدر قوة عظيمة، ولكنه في الوقت نفسه يكشف خاصيتها الضعيفة، لأن البنى التحتية التي تقوم عليها الدول الحديثة مثل الكهرباء والمياه والمواصلات والاتصالات والبورصة والبنوك تعتمد في عملها على الفضاء الإلكتروني. وكذلك شبكات القيادة والسيطرة والتحكم العسكرية ومختلف أنواع التكنولوجيا المتطورة في ساحات القتال؛ مثل: أنظمة جمع المعلومات، واستعمال الأقمار الصناعية والطائرات من دون طيار في الحرب؛ كلها تعتمد على الفضاء الإلكتروني.

^٣ - <http://www.calcalist.co.il/Ext/Comp/ArticleLayout/CdaArticlePrintPreview/1,2006,L-3023149,00.html>

ونوه المؤلفان إلى ميزات الفضاء الإلكتروني كمجال قتال، وأبرزها التمكن من العمل بسرعة واحد من الألف من الثانية، ضد أعداء يبعدون آلاف الأميال من دون تعرض المهاجمين أو المقاتلين للأخطار.

والميزات التي يتمتع بها الفضاء الإلكتروني تجعله جذاباً للاستعمال في القتال خلال الحرب، إلى جانب الأسلحة التقليدية، مثلما فعلت روسيا، كما يقول المؤلفان، في حربها ضد جورجيا في سنة ٢٠٠٨. ويمكن أيضاً استخدامه أثناء الحرب ضد أهداف استراتيجية، مثل الهجوم الذي تعرض له المفاعل النووي الإيراني في سنة ٢٠٠٩، حيث اعتبر المؤلفان أن هذا الهجوم (الذي قامت به إسرائيل وفق العديد من المصادر الإعلامية) كان حدثاً تأسيسياً في مجال حرب الفضاء الإلكتروني، وشكل مرحلة جديدة في تطور استعمال الفضاء الإلكتروني في مجال القتال.

واعتبر المؤلفان أن استعمال الفضاء الإلكتروني في القتال وعمليات التطوير والاستعدادات التي قامت بها دول عديدة، يؤكد أن سباق التسلح في مجال الفضاء الإلكتروني قد بدأ. ويشيران إلى أن العديد من الدول أقامت في السنوات الأخيرة مؤسسات وهيئات مختلفة ومختصة باستعمال الفضاء الإلكتروني كمجال قتال، وطرقت استراتيجيات أمنية في الفضاء الإلكتروني.

وبدأ المؤلفان الفصل الأول الذي جاء تحت عنوان "الفضاء الإلكتروني والمجال الأمني - إطار مصطلحي"، بتعريف وشرح المصطلحات المتعلقة بموضوع الفضاء الإلكتروني. ثم عالجا في هذا الفصل المواضيع التالية: ميزات الفضاء الإلكتروني كمجال للحرب، الفضاء الإلكتروني - مصطلحات أمنية تقليدية مع مضمون جديد، البيئة الاستراتيجية للفضاء الإلكتروني، التجسس والحرب الإلكترونية الرخوة، وحرب الفضاء الإلكتروني.

وحمل الفصل الثاني عنوان "عمليات هجومية وعوامل كابحة في الفضاء الإلكتروني"، وشمل المواضيع التالية: عمليات هجومية بارزة في الفضاء الإلكتروني، العوامل التي قادت إلى زيادة المعرفة في الفضاء الإلكتروني، استعمال الفضاء الإلكتروني لأغراض الحرب - العوامل الكابحة، الإرهاب في الفضاء الإلكتروني، ميثاق دولي لتنظيم النشاط في الفضاء الإلكتروني، وتلخيص للعوامل المشجعة والعوامل الكابحة لاستعمال سلاح حرب الفضاء الإلكتروني في الصراعات بين الدول.

وعالج الفصل الثالث الذي جاء تحت عنوان "نظرة إلى ما وراء البحر - استعداد دول لتحدي الفضاء الإلكتروني"، استعدادات العديد من الدول الهامة واستراتيجياتها والمؤسسات التي أقامتها من أجل ضمان أمنها أمام المخاطر الكامنة في الفضاء الإلكتروني، وهذه الدول هي: الولايات المتحدة وفرنسا وألمانيا وبريطانيا والصين.

إسرائيل والفضاء الإلكتروني

عالج الباحثان في الفصل الرابع أهمية وحيوية الفضاء الإلكتروني لإسرائيل والتدابير المؤسسية التي اتخذتها إسرائيل لحماية فضاءها الإلكتروني. وقدما اقتراحا حول الاستراتيجية التي ينبغي على إسرائيل اتباعها للدفاع عن فضاءها الإلكتروني. كما عالجا كيفية دمج الفضاء الإلكتروني باستراتيجية الأمن الإسرائيلي.

وأشار المؤلفان إلى أن إسرائيل باتت دولة "محوسة" تعتمد مؤسساتها الحكومية ومختلف المرافق والشركات فيها على شبكة الإنترنت. كما تتم الكثير من معاملات المواطنين فيها مع مؤسسات الدولة والمرافق المختلفة في الدولة بوساطة شبكة الإنترنت. وأكد الباحثان أن تكنولوجيا المعلومات تساهم مساهمة مباشرة وغير مباشرة في نمو الاقتصاد الإسرائيلي، إذ تعتبر إسرائيل من ضمن مجموعة الدول العديدة المتقدمة في تطوير تكنولوجيا المعلومات. وقد بلغ حجم اقتصاد الإنترنت في إسرائيل في سنة ٢٠٠٩ خمسين مليار شيكل (الدولار يساوي ثلاثة شيكل ونصف)، وهو ما يعادل ٦,٥ في المئة من مجمل الانتاج المحلي الإسرائيلي. ومن المتوقع أن يبلغ اقتصاد الإنترنت في إسرائيل في سنة ٢٠١٥ خمسة وثمانين مليار شيكل، وهو ما سيعادل ٨,٥ في المئة من مجمل الانتاج المحلي الإسرائيلي.

تدابير إسرائيل للدفاع عن فضاءها الإلكتروني

ذكر المؤلفان أن إسرائيل اتخذت مجموعة من التدابير خلال العقد ونصف العقد الأخيرين من أجل حماية الفضاء الإلكتروني والدفاع عنه، وأهم هذه التدابير:

أولاً: البنية التحتية الحكومية لعصر الإنترنت

أقامت إسرائيل في سنة ١٩٩٧ مشروع "بنية الحكومة التحتية لعصر الإنترنت" في داخل وزارة المالية الإسرائيلية. وحدد هدف هذا المشروع في حماية وتأمين استعمال الإنترنت في الوزارات والمؤسسات الحكومية. وأقيم داخل هذا المشروع "مركز حماية المعلومات لحكومة إسرائيل" وأنيطت به مهام متابعة تطور وسائل حماية المعلومات في العالم والتنسيق بين الوزارات والمؤسسات الحكومية من أجل إيجاد حلول لمشاكل حماية المعلومات وكذلك إجراء أبحاث حول هذا الموضوع.

ثانياً: السلطة الرسمية لحماية المعلومات

أنشئت في سنة ٢٠٠٢ "السلطة الرسمية لحماية المعلومات"، في داخل جهاز المخابرات العامة (الشاباك). وأنيط بهذه السلطة مهام حماية البنى التحتية للحواسيب الهامة والحيوية في إسرائيل من مخاطر ما أطلق عليه "تهديدات إرهابية" و"عمليات تخريب" ونشاطات تجسسية. وأشار المؤلفان إلى وجود لجنة تابعة لمجلس الأمن القومي الإسرائيلي، والتي تقع من بين صلاحياتها السماح لـ"السلطة الرسمية لحماية المعلومات" التابعة لجهاز المخابرات العامة (الشاباك) بتوسيع قائمة المؤسسات التي تقوم بمراقبتها بغرض حماية المعلومات فيها. وذكر المؤلفان أن عمل "السلطة الرسمية لحماية المعلومات" تعثره العديد من النواقص، لكونه لا يشمل جميع المؤسسات والمنشآت في إسرائيل ولأن هذه السلطة تابعة لجهاز المخابرات العامة (الشاباك)، ما يردع الكثير من المؤسسات من التعامل والتفاعل معها بحرية وأريحية.

ثالثاً: هيئة السايبر في الجيش الإسرائيلي

في سنة ١٩٠٩، اعتبر غابي اشكنازي رئيس هيئة أركان الجيش الإسرائيلي الفضاء الإلكتروني كمجال قتال من الناحيتين الاستراتيجية والعملياتية. وبناء على ذلك أقام الجيش الإسرائيلي "هيئة السايبر" في الوحدة ٨٢٠٠ في جهاز المخابرات العسكرية الإسرائيلية (أمان)، بغرض توجيه وتنسيق نشاطات الجيش الإسرائيلي في الفضاء الإلكتروني. وفي كانون الأول/ ديسمبر ٢٠٠٩، أشار عاموس يادلين، رئيس جهاز المخابرات العسكرية الإسرائيلية حينئذ، في محاضرة له في معهد أبحاث الأمن القومي، إلى أن أحد أهم الأخطار التي تترصد بإسرائيل وقد تلحق بها الأذى، تكمن في احتمال اختراق الحواسيب الحيوية الإسرائيلية. وأوضح عاموس يادلين، أن هيئة السايبر في الجيش الإسرائيلي تهدف إلى توفير دفاع جيد لشبكات الأنترنت العاملة في إسرائيل، وكذلك القيام بهجمات في الفضاء الإلكتروني على أهداف خارجية.

رابعاً: وحدة إدارة أنظمة المعلومات

صادقت الحكومة الإسرائيلية في ٢٧ آذار/ مارس على إقامة "وحدة إدارة المعلومات"، وهي تتبع مدير عام وزارة المالية الإسرائيلية ومسؤولة مباشرة على جميع أنظمة الاتصالات المحوسبة الحكومية، بما في ذلك عن مشروع "بنية الحكومة التحتية لعصر الإنترنت".

خامساً: هيئة السايبر الوطنية

أعلن رئيس الحكومة الإسرائيلية بنيامين نتنياهو في ١٨ أيار/ مايو ٢٠١١ عن إنشاء "هيئة السايبر الوطنية" في إسرائيل. وذكر نتنياهو أن الهدف الأساس لهذه الهيئة هو تعزيز قدرات إسرائيل الدفاعية عن أنظمة البنى التحتية الحيوية، من "هجمات إرهابية" في الفضاء الإلكتروني، التي قد تقوم بها دول أجنبية أو "منظمات إرهابية". ووفق ما ذكره نتنياهو، فإن إسرائيل مكشوفة لهجمات في الفضاء الإلكتروني، فكل ما هو محوسب فإنه قد يتعرض للهجمات في الفضاء الإلكتروني، التي قد تشمل أنظمة مرافق ومؤسسات حيوية للغاية التي تشغل الدولة مثل: الكهرباء والمياه والاتصالات والمواصلات.

ويشير المؤلفان إلى أنه علاوة على مهامها الدفاعية عن الفضاء الإلكتروني الإسرائيلي، فإن من مهام "هيئة السايبر الوطنية" تشجيع وتطوير شركات إسرائيلية مختصة في الدفاع عن الفضاء الإلكتروني، بغرض الحصول على جزء من سوق الفضاء الإلكتروني الذي ينمو بسرعة كبيرة للغاية على الصعيد العالمي.

وأوضح الكاتبان أن ثلاثة عوامل هامة تدفع إسرائيل للإسراع في اتخاذ الاحتياطات والتدابير الأمنية في الفضاء الإلكتروني، وهي:

أولاً: كدولة متطورة ومرافقها ومؤسساتها محوسبة، يتعرض الفضاء الإلكتروني في إسرائيل إلى أخطار حدوث هجمات عليه، قد تؤدي إلى إلحاق الشلل بالبنى التحتية الإسرائيلية.

ثانياً: تواجه إسرائيل أعداء لهم دوافع لإلحاق الأذى بها كلما استطاعوا تحقيق ذلك، سواء من قبل دول أو منظمات أو أفراد.

ثالثاً: هناك فرصة أمام إسرائيل ليس فقط لتطوير دفاع متقدم في الفضاء الإلكتروني وإنما أيضا لاستعمال الفضاء الإلكتروني في الحرب.

استراتيجية للدفاع عن الفضاء الإلكتروني الإسرائيلي

اقترح المؤلفان أن تتبنى الحكومة الإسرائيلية استراتيجية وطنية للدفاع عن الفضاء الإلكتروني الإسرائيلي وفق الخطوات التالية:

١ - الاعتراف بالفضاء الإلكتروني كمجال وطني جديد، الذي ينبغي الدفاع عنه بشكل خاص (إلى جانب المجالات الأخرى: البر والبحر والجو)، من خلال رؤية شاملة وتعاون جميع الأطراف ذات الصلة.

٢ - تأسيس مؤسسة وقيادة مركزية للدفاع عن الفضاء الإلكتروني على المستوى الوطني.

٣ - وضع البنى التحتية الحيوية وأنظمة الأمن في قمة الأولويات، وفي الوقت نفسه القيام بالدفاع عن مركبات أخرى، مثل الدفاع عن المعلومات في الجامعات ومراكز الأبحاث والدفاع عن شركات لها تأثيرها على الاقتصاد الإسرائيلي ولكنها ليست مصنفة كجزء من البنى التحتية.

٤ - بناء نظام دفاعي دينامي وشامل في الفضاء الإلكتروني مثل النظام الذي أقامته وزارة الدفاع الأمريكية.

٥ - التعاون الدائم في مجال الفضاء الإلكتروني بين القطاع الحكومي والقطاع الأمني والقطاع الخاص.

٦ - التعاون مع دول أجنبية بشأن الفضاء الإلكتروني، وخاصة الدول الحليفة.

٧ - سن قوانين خاصة بالفضاء الإلكتروني والقيام بتطبيقها على أرض الواقع.

٨ - مساعدة الجمهور العام في زيادة الوعي بالفضاء الإلكتروني وتطوير قدراته في الدفاع في هذا المجال، ومنح محفزات للشركات والأفراد لشراء برامج دفاع، وزيادة الرقابة على شركات الحماية.

٩ - استعمال الوسائل والأجهزة التكنولوجية الأكثر تطورا المتعلقة بالفضاء الإلكتروني.

١٠ - بلورة وتطوير سياسة ردع إسرائيلية، بما في ذلك قدرة الرد المباشر ضد كل من يهاجم الفضاء الإلكتروني الإسرائيلي وإلحاق الأذى به، وهذا الأمر من مهام المؤسسة الأمنية الإسرائيلية.

الفضاء الإلكتروني في استراتيجية الأمن الإسرائيلي

يؤكد المؤلفان أن إضافة الفضاء الإلكتروني كساحة قتال جديد، إلى جانب ساحات القتال في البر والبحر والجو والفضاء، يستوجب دمج الحرب في الفضاء الإلكتروني في استراتيجية ومفهوم الأمن الإسرائيلي؛ وهو ما يستوجب استحداث تغييرات في مفاهيم المصطلحات الأساسية المتعلقة بنظرية الأمن الإسرائيلي. فمثلاً تختلف "البيئة الاستراتيجية" في الفضاء الإلكتروني عن المفهوم التقليدي لها في نظرية الأمن الإسرائيلي القائم على التهديدات الجيو-سياسية التقليدية. علاوة على ذلك، يختلف الزمان والمسافة والمساحة في الفضاء الإلكتروني عن المفاهيم التقليدية، لأن سرعة العملية الهجومية في الفضاء الإلكتروني، ضد هدف يبعد مئات أو آلاف الأميال، تبلغ واحد على الألف من الثانية. ويرى المؤلفان أنه من الصعب للغاية أن تقوم إسرائيل بتطبيق سياسة الردع، التي تعتبر حجر الزاوية في سياسة الردع الإسرائيلية، في حرب الفضاء الإلكتروني، لصعوبة تحديد هوية الطرف المهاجم في حرب الفضاء الإلكتروني.

ويقول صاحبها الكتاب أن الدفاع في حرب الفضاء الإلكتروني يشكل تحدياً من نوع جديد لإسرائيل، وذلك لأنه بمقدور العدو شن هجمات بسرعة البرق ومن الصعوبة بمكان تحديد من هو المهاجم. ويوصي المؤلفان أن تتعلم إسرائيل وتستفيد من مفهوم "الدفاع الفعال" في الفضاء الإلكتروني الذي تتبعه الولايات المتحدة الأمريكية. إذ يستند هذا "الدفاع الفعال" على قدرة مخبرية متطورة لتحديد النشاطات في الإنترنت وعلى أنظمة دفاع دينامية ذات رد تلقائي من دون تدخل الإنسان. ويستطرد المؤلفان، إن "الدفاع الفعال" لا يعتمد فقط على التكنولوجيا المتطورة، وإنما أيضاً على شبكة محكمة ذات قواعد وإجراءات صارمة وعلى ثقافة تفهم المخاطر وعلى انضباط شديد وعلى حماية المواقع وعلى رقابة بشرية قوية.

ويوصي المؤلفان، في ضوء اعتراف الجيش الإسرائيلي بالفضاء الإلكتروني كساحة قتال إلى جانب الساحات الأخرى، بإجراء تغييرات في قوات الجيش الإسرائيلي والعمل على إقامة جيش خاص بالفضاء الإلكتروني، أسوة بالقوات البرية والبحرية والجوية.