ترجمة وإعداد: سعيد عيّاش

الحرب في الحيّز الافتراضي

تعريف

ننقل هنا ملخصا لـ«مذكرة» تحمل رقم (١٠٩) صدرت في حزيران ٢٠١١ عن «معهد دراسات الأمن القومي» في جامعة تل أبيب باللغة العبرية تحت العنوان «الحرب في الحيز الافتراضي- مصطلحات واتجاهات، ومعانٍ ودلالات بالنسبة لإسرائيل».

وتتناول هذه «المذكرة»، التي شارك في إعدادها الباحثان الخبيران في المعهد شموئيل إيفن ودافيد سيمنطوف، بصورة مفصلة، المميزات والسمات الخاصة لما تصفه بـ«الحيز القتالي الجديد»، مقترحة مقاربات جديدة لمصطلحات ومفاهيم تقليدية في هذا الصدد (حرب الحيز الافتراضي).

ويحث معدا الوثيقة إسرائيل على مواكبة التطورات العالمية في هذا المجال وتسريع وتيرة «استعدادها في مواجهة هذا التحدي الجديد» وذلك «بغية تحسين سبل ووسائل الدفاع عن حيزها الافتراضي» كما جاء في تقديم «المذكرة» التي أتت في ٩٠ صفحة، واحتوت على أربعة فصول وملاحق إضافية، وقد اخترنا ترجمة الأجزاء المهمة منها، ذات الصلة بالسياق الإسرائيلي.

*****

توطئة

إن الحيز الافتراضي Cyberspace هو حيز قتالي جديد، وينضم إلى مجالات البر والبحر والجو والفضاء، في ساحة المعركة العصرية. وتتناول هذه "المذكرة" بشكل مفصل المميزات والسمات الخاصة للحيز القتالي الجديد، مقترحة تفسيرات جديدة لمصطلحات ومفاهيم تقليدية، فيما يقترح معداها على إسرائيل العمل على حث وتسريع استعدادها في مواجهة هذا التحدي الجديد، وذلك بغية

تحسين سبل ووسائل الدفاع عن حيزها الافتراضي.

وقد شرعت دول عصرية وجيوش متقدمة في العالم بزيادة وتكثيف نشاطها وجهودها في الحيز الافتراضي الذي يشكل بالنسبة لها مصدر قوة لكنه يكشف في الوقت ذاته أيضا عن مواطن ضعف. وعلى سبيل المثال، فإن البنى التحتية الحيوية لعمل الدولة (كالكهرباء والمياه والمواصلات) وشبكات القيادة والسيطرة والتحكم العسكرية، وكذلك التقنيات المتطورة لساحة القتال العصرية، كلها تعتمد على هذا الحيز الافتراضي.

وللحيز الافتراضي، كحيز قتالي، خصائص خاصة تمكن من العمل بسرعة قصوى ضد أعداء يتواجدون على مسافة بعيدة جداً عن الدولة، من دون أن تعرض مقاتليها وجنودها للخطر، وهو ما يجعل هذا الحيز مغريا للقتال في الفترات الفاصلة أيضا بين حروب تقليدية. ويمكن التمييز بين مواجهات تقع في الحيز الافتراضي (كالهجوم المنسوب إلى روسيا على أستونيا في العام ٢٠٠٧) وبين حروب يشكل فيها الهجوم في الحيز الافتراضي عنصرا أو مكونا في الحرب إلى جانب قوات وعناصر أخرى (مثل الهجوم الذي شنته روسيا على جورجيا في العام ٢٠٠٨). كذلك يمكن التمييز بين هجمات تتم داخل الحيز الافتراضي (ضرب شبكات الاتصال الالكترونية) وبين استخدام الحيز كوسيلة بغية تعطيل عمل وأداء أجهزة وآلات تعمل في الحيزات المادية. مثال: الهجوم الافتراضي الذي تعرض له المشروع النووي الإيراني في العام ٢٠٠٩، وقد جسد هذا الحدث الطاقة الكامنة الهائلة للسلاح الافتراضي، واعتبر حدثا مؤسسا في تطور الحيز الافتراضي كمجال قتالي. وفي هذا السياق، فإن عدداً من حوادث الهجمات الافتراضية، واستعداد بعض الدول في الحيز الافتراضي، تدل على أن سباق التسلح الافتراضي قد انطلق! حيث أقيمت في السنوات الأخيرة في دول مختلفة هيئات ودوائر تتناول الحيز الافتراضي كحيز قتالي، كما جرى بلورة استراتيجيات أمنية للعمل في هذا الحيز (في الولايات المتحدة وبريطانيا وفرنسا وألمانيا والصين وغيرها).

في الوقت ذاته، هناك وعي آخذ في التطور والتنامي في الساحة الدولية بشأن وجوب حماية الحيز الافتراضي وتنظيم النشاط فيه بما يخدم الصالح العام، على غرار تنظيم النشاط في المجالات الأخرى، وذلك عن طريق إقامة تعاون بين الدول ومواءمة قواعد القانون الدولي وبلورة معاهدة دولية ملزمة في هذا الصدد. غير أن تقدم هذه الجهود ما زال بطيئا ولا يواكب وتيرة التطورات في الحيز الافتراضي.

في السياق الإسرائيلي لهذا الموضوع، يمكن القول إن إسرائيل تمتلك قدرة على أن تغدو بين الدول الرائدة في العالم في مجال الأمن الافتراضي وذلك في ضوء ما لديها من ثروة بشرية ومعرفة تكنولوجية عالية. وعليه فإن استنفاد هذه القدرة يمكن أن يخدم ويفيد الدولة في مجالي الأمن والاقتصاد.

الحيز الافتراضي والحقل الأمني
تعريفات، مفاهيم ومصطلحات

يصف مصطلح «حيز افتراضي» ظاهرة تعود بدايتها إلى اختراع التلغراف في العام ١٨٤٤، وجوهرها استغلال الإنسانية الحقل الالكترو- مغناطيسي بواسطة التكنولوجيا. وقد كانت نقطة التحول الجوهرية في تطور الحيز الافتراضي اختراع الحاسوب الرقمي في العام ١٩٤٩، ثم تبعت ذلك، في وقت لاحق، محطات مهمة أخرى منها على سبيل المثال: ربط شبكات الاتصال بالحواسيب والآلات في السبعينيات؛ الاستخدام الجماهيري لشبكة الانترنت والحواسيب الشخصية في أواسط التسعينيات؛ الدمج الشامل بين منظومات وأجهزة الحاسوب والاتصالات والآلات على اختلاف أنواعها (في الصناعة والمواصلات.. إلخ.)؛ ازدهار الشبكات الاجتماعية في الانترنت خلال العقد الأخير. وكل هذه الأمور غيرت وجه المجتمع والاقتصاد.

كذلك فإن تكنولوجيا المعلومات والحيز الافتراضي يغيران بسرعة وجه ساحة القتال العصرية، ويدخل في ذلك استخدام التقنيات المتطورة مثل الأجهزة الذكية والتشارك في المعلومات واستغلال الأقمار الصناعية واستخدام الأجهزة الأوتوماتيكية وغيرها. وقد أدى تطور الحيز الافتراضي بدوره إلى تغطية مدنية واسعة لساحة المعركة، بما في ذلك بواسطة أجهزة الهواتف النقالة، الأمر الذي حول ساحات القتال إلى مجال أضحى فيه الجمهور لاعبا مركزيا يمارس- أكثر من الماضي- تأثيره على مواقف سياسية لحكومات ومؤسسات دولية، أحيانا على أساس معلومات هادفة أو منحازة. هذه الظاهرة لها أبعاد واسعة في كل ما يتعلق باستخدام القوة العسكرية. فهي تحد من القدرة على استخدام القوة، لكن يمكن لها أيضا أن تساهم في تجنيد الرأي العام من أجل استخدام القوة.

تعريفات

هناك عدة تعريفات للحيز الافتراضي الذي يطلق عليه أيضا حيز «السايبر» (Cyberspace). وكالة الأمم المتحدة- ITU (International Telecommunication Union) تعرف الحيز الافتراضي على النحو الآتي: الحيز المادي وغير المادي الذي ينشأ أو يتكون من جزء أو من كل العناصر التالية: حواسيب، أجهزة ممكننة، شبكات، معلومات محوسبة، برامج ومضامين، معطيات مرور ورقابة، والذين يستخدمون كل ذلك. ويستدل من هذا التعريف أن الحيز الافتراضي يحتوي على ثلاث شرائح مرتبطة بعضها ببعض:

١. شريحة إنسانية- المستخدمون للاتصالات والحواسيب.
٢. شريحة عقلية- وهي شريحة البرامجيات وأنظمة المعلومات، وتتحرك هذه بسرعة الضوء وتعرض معلومات وأوامر وعقارات افتراضية وغيرها.
٣. شريحة مادية: المكونات المادية للشبكة، الثابتة والمنقولة.

ثمة تعريفات أخرى للحيز الافتراضي، ومع أنها كلها تعترف بالشرائح الثلاث المذكورة، إلا أن كل واحد منها يميز تعريف المصطلح ذاته (الحيز الافتراضي) بواسطة جزء من هذه الشرائح فقط.

وخلافا للتعريفات التي تنظر إلى الحيز الافتراضي كبعد أو مجال خامس، هناك توجه يرى فيه واحداً من سبعة مجالات (حيزات)، إلى جانب الجو والفضاء والبحر والبر والحيزين الالكترو- مغناطيسي والإنساني. كذلك فإن هذا التوجه، يميز بين الحيز الافتراضي وبين الحيز الالكترو- مغناطيسي ويعتبر الشريحة الإنسانية حيزا أو مجالا قائما بذاته.

إن القاسم المشترك الواضح بين سائر التعريفات هو الشريحة العقلية، أما الاختلاف والتباين فيما بينها، فيعكس على ما يبدو الاهتمام الذي توليه كل دولة أو منظمة في سياق مواجهتها للتحديات في الحيز الافتراضي، ولكن يبدو أن الفوارق في التعريفات لا تعكس فهما مختلفا للمجال الافتراضي، وذلك لأن جميع أصحاب هذه التعريفات يقرون، كما أسلفنا، بوجود الشرائح الثلاث التي يتضمنها تعريف الأمم المتحدة.

سمات الحيز الافتراضي كمجال قتالي

تتضمن كل شريحة من الشرائح الثلاث (الإنساني، العقلي والمادي) الواردة في تعريف الأمم المتحدة، أنواعا من النشاطات الأمنية المتعلقة بالحيز الافتراضي، ومنها على سبيل المثال:

- نشاطات في الحيز الافتراضي موجهة للشريحة الإنسانية، وهدفها تغيير سلوك الإنسان المستخدم، ومن هذه النشاطات نقل رسائل معلوماتية (علنية أو سرية) للخصم بواسطة الحيز الافتراضي.
- عمليات تسلل عقلية لأغراض التجسس ومهاجمة حواسيب الخصم لمنع الفائدة التي يجنيها في الحيز الافتراضي، وكذلك مهاجمة أجهزة وآلات ومنشآت في الحيزات المادية المسيطر عليها بواسطة الحيز الافتراضي.
- في الشريحة المادية- ضرب المكونات/ المعدات المعدنية (hard ware) للحاسوب (أو الحواسيب) التي ترتكز عليها الشريحة العقلية، إضافة إلى نشاطات وعمليات خارج الحيز الافتراضي، ضد شبكات وبنى تحتية يرتكز عليها الحيز.
- وتدخل في هذه النشاطات على سبيل المثال عمليات نارية وحرب الكترونية هدفها ضرب أو تعطيل مكونات اتصال ومنظومات طاقة يرتبط بها الحيز الافتراضي.
- ومن السمات التي يتميز بها هذا الحيز القتالي الجديد:
- قدرة عمل بسرعة قريبة من سرعة الضوء، وذلك من دون أي قيود أو معيقات جغرافية تقليدية، وهو ما يمكن المهاجمين من شن هجمات على مسافات بعيدة وبسرعة خاطفة من دون احتكاك مع الخصم في الحيزات المادية.
- قدرة عمل بصورة سرية. فالدروس المستخلصة من الهجمات التي جرت حتى الآن في الحيز الافتراضي، والمعلومات المتوفرة حول استراتيجيات العمل في هذا الحيز، تدل على أن المهاجم

السلاح الافتراضي قابل للاستخدام أيضا كسلاح غير فتاك أو قاتل. فالقدرة على إلحاق ضرر شديد بأداء الدولة من دون التسبب بتخريب بنى تحتية مادية أو إيقاع خسائر في الأرواح، يعتبر أفضلية للسلاح الافتراضي على هجمات حركية (بالنار) إستراتيجية. مع ذلك فإن الهجمات الافتراضية يمكن أن تتسبب أيضا بدمار كبير وخسائر بشرية وذلك عن طريق ضرب المنظومات والأجهزة المرتبطة بالحيز الافتراضي، والموجودة في الحيزات المادية.

يمتلك قدرة على العمل في الحيز الافتراضي بسرية ومن دون ترك أية بصمات أو آثار، والاختباء خلف جهات أخرى من قبيل قراصنة يعملون لحسابهم الخاص، وعناصر جنائية ومنظمات ودول أجنبية. هذه الميزة تتيح إذن تقليص إمكانية الانكشاف والإدانة وخطر التعرض لرد (هجوم) مضاد.

- السلاح الافتراضي قابل للاستخدام أيضا كسلاح غير فتاك أو قاتل. فالقدرة على إلحاق ضرر شديد بأداء الدولة من دون التسبب بتخريب بنى تحتية مادية أو إيقاع خسائر في الأرواح، يعتبر أفضلية للسلاح الافتراضي على هجمات حركية (بالنار) إستراتيجية. مع ذلك فإن الهجمات الافتراضية يمكن أن تتسبب أيضا بدمار كبير وخسائر بشرية وذلك عن طريق ضرب المنظومات والأجهزة المرتبطة بالحيز الافتراضي، والموجودة في الحيزات المادية.

يتيح الحيز الافتراضي الوصول إلى أهداف يصعب ضربها بواسطة هجوم حركي (ناري)، مثل :

منشآت ومنظومات (اتصالات، سيطرة وتحكم . . إلخ) موجودة في مناطق يصعب مهاجمتها بالنار لأسباب مختلفة كالبعد ووجود وسائل دفاع قوية أو لوجودها على مقربة من تجمعات سكانية . . .

الفروع المصرفية والمالية، والتي تعتبر حاليا بنية قومية حاسمة مكشوفة للهجوم في الحيز الافتراضي، وعلى سبيل المثال فإن ضرب الجهاز المالي يمكن أن يمنع دفع الأجور وأن يعطل التجارة الخارجية واقتصاد البلد بأكمله.

الشبكات اللوجستية والمواصلات، والتي بات الحاسوب واحداً من مكونات عملها، وكذلك قواعد معطيات ومعلومات الدولة، كالوزارات والجامعات وجهاز القضاء وغيرها.

الفيروسية، وتتعلق هذه الميزة بميل "الفيروسات" إلى إعادة نسخ نفسها من دون توقف، وبقدرتها على الانتقال داخل الشبكة إلى أماكن مختلفة. وتشكل هذه الخاصية تحديا صعبا للطرف المدافع، الذي يتعين عليه منع انتشار الفيروس وانتقاله إلى مناطق مختلفة.

وحدة معايير الحيز الافتراضي. يعتمد الحيز في جوهره على بنى شركات عالمية (مثل مايكروسوفت، سيسكو، تشيك بوينت وغيرها) مرتبطة بعضها ببعض وموجودة في جميع الدول. وفي الواقع فإن الطابع العالمي للحيز واستخدام المعدات نفسها، يخدمان بناة الحيز الافتراضي، لكن ذلك ينطوي على خطورة شديدة من ناحية الطرف المدافع. وعلى سبيل المثال فإن اختراق برمجة حماية معلومات أو مستودع معلومات تكنولوجي معين تابع لشركة افتراضية عالمية، من الممكن أن يعرض للخطر جميع الأماكن التي تستخدم فيها هذه البرامجيات. هذه الحوادث تقلل من جدوى منتجات الحماية الرائجة لدى الشركات والحكومات.

قدرة إنسانية عالية على السيطرة في الحيز الافتراضي. فنظرا لكون الحيز الافتراضي حيزا مصطنعا، من صنع الإنسان، فمن الطبيعي أن يتمكن المدافع من السيطرة في الحيز الذي بناه بنفسه. فهو يستطيع توقع الظروف في الحيز، خلافا لصعوبة التنبؤ بالظروف في المجالات الأخرى، مثل حالة الطقس. كذلك باستطاعته تعطيل الحيز أو الحد من استخدامه. ومن الأمثلة على محاولة الحد من استخدام الحيز الافتراضي ما تقوم به الصين وإيران والعديد من الدول العربية. إضافة إلى ذلك فإن من السهل أكثر على المدافع أن يعيد بسرعة إصلاح وترميم شبكة منظمة من أن يصلح شبكة ليست بهذه الكيفية. على الرغم مما ذكر فإن الحيز الافتراضي لا يخلو من حوادث مفاجئة، لم يتكهن بها بناة الحيز مسبقا، وهي ناتجة عن تفاعلات بين الحواسيب، أو عن تفاقم أخطاء بشرية (مثلا أخطاء في إصدار الأوامر في سوق المال).

إن في استطاعة الدول إقامة قوات افتراضية ذات قدرات هجومية متقدمة بأسعار وتكاليف منخفضة مقارنة مع التكاليف اللازمة لبناء قوات متحركة (نارية) متقدمة، كذلك باستطاعة المنظمات والمجموعات أيضا أن تتزود وأن تستخدم السلاح الافتراضي. مع ذلك يجب التمييز بين قدرات هجومية يمكن أن تتسبب بأضرار محلية أو مؤقتة، مهما كانت جسيمة، وبين قدرات على تنفيذ هجوم افتراضي واسع ومتواصل على أهداف إستراتيجية لعدو يمتلك قدرات دفاعية متقدمة. وعلى ما يبدو فإن هجوما من النوع الثاني يتطلب قدرة لا تتوفر حتى الآن سوى لدول ذات قدرة تكنولوجية عالية.

يتسم الحيز الافتراضي أيضا بكونه حيزا يدمج المجالين المدني والعسكري. ففي الكثير من الحالات تكون الاتصالات العسكرية مرتبطة بشبكات مدنية. من هنا تغدو حماية البنى والشبكات المدنية حيوية للأغراض العسكرية أيضا. في الوقت ذاته، تمتلك الجيوش قدرات افتراضية يمكن أن تساعد في حماية الشبكات المدنية. ويشكل هذا الدمج في الدول الديمقراطية تحديا قانونيا للمدافع في ضوء التشريعات المتقدمة في مجال حقوق الفرد، والتي تخلق، من ضمن جملة أشياء أخرى، صعوبة في جمع المعلومات وتفعيل وحدات عسكرية في الحيز الافتراضي المدني.

استغلال موارد اتصالات الكترونية تابعة لجهات أخرى. فشبكات الاتصال العالمية تتيح للمهاجم عبور الحدود والتحرك بسرعة نحو الأهداف المرتبطة بها، وحتى استخدام موارد اتصالات الخصم من أجل مهاجمة أجهزته وشبكاته. مع ذلك فإن الارتباطات تمكن المدافع من الاستعانة بدول صديقة من أجل رصد هجمات وإحباطها قبل وصولها للدولة.

إجمالا يمكن القول: إن في استطاعة الدول إقامة قوات افتراضية ذات قدرات هجومية متقدمة بأسعار وتكاليف منخفضة مقارنة مع التكاليف اللازمة لبناء قوات متحركة (نارية) متقدمة، كذلك باستطاعة المنظمات والمجموعات أيضا أن تتزود وأن تستخدم السلاح الافتراضي. مع ذلك يجب التمييز بين قدرات هجومية يمكن أن تتسبب بأضرار محلية أو مؤقتة، مهما كانت جسيمة، وبين قدرات على تنفيذ هجوم افتراضي واسع ومتواصل على أهداف إستراتيجية لعدو يمتلك قدرات دفاعية متقدمة. وعلى ما يبدو فإن هجوما من النوع الثاني يتطلب قدرة لا تتوفر حتى الآن سوى لدول ذات قدرة تكنولوجية عالية.

من ناحية المدافع في الحيز، فإن وسائل الدفاع الافتراضية متوفرة في السوق الحرة، لكن الدفاع أو الحماية الافتراضية الشاملة تتطلب الاستجابة لتشكيلة واسعة من أنواع التهديدات، وهو ما تترتب عليه تكاليف باهظة.

الحيز الافتراضي – مصطلحات أمنية تقليدية مع مضمون جديد

يختلف الحيز الافتراضي بمعان كثيرة عن الحيزات المادية، بما في ذلك في السياق الأمني. هذا الاختلاف الكبير يستوجب إعادة النظر في صلاحية المفاهيم والمصطلحات الإستراتيجية التقليدية وصب مضامين جديدة داخلها.

وتحتوي وثائق الجيش الأميركي على مصطلحات تنفيذية جديدة تتعلق بالقتال في الحيز الافتراضي. مع ذلك يبدو أن المصطلحات الرئيسة المستخدمة في سياق ساحة الحرب التقليدية، ما زالت تستخدم أيضا في ساحة الحرب الافتراضية، مثل: الردع، الدفاع، الهجوم، سباق التسلح.. إلخ. وعلى ما يبدو فإن استخدام هذه المصطلحات سيستمر لسنوات كثيرة أخرى وسط ملاءمتها للحيز الجديد، وقد تكون هذه فترة انتقالية لحين بلورة مصطلحات ومفاهيم جديدة من قبل المؤسسات الأمنية والعسكرية.

البيئة الإستراتيجية

تختلف البيئة الإستراتيجية الافتراضية عن البيئة الإستراتيجية التقليدية، التي يحددون بموجبها في إسرائيل دوائر التهديد الجغرافية. وتتناول العلاقة بين الحيز الافتراضي والحيز الجغرافي التوزيع الجغرافي لبنى الحواسيب والشبكات، وبالتالي ثمة لمصطلح الجغرافيا معنى مختلف في الحيز الافتراضي. كذلك يختلف التناول

ويخلق الحيز الافتراضي، بالطريقة نفسها، فرصا أمنية جديدة ويتيح الاستعانة بحلفاء بشكل مختلف، تبعا لقدراتهم وموقعهم في هذا الحيز. لهذا السبب، ونتيجة للأولوية التي تعطيها الدول المختلفة لتطوير قدرات افتراضية، من المحتمل أن تنشأ موازين قوى جديدة بين الدول أو بين دول ومنظمات غير دولانية، وعليه فإن الحيز الافتراضي يخلق بيئة استراتيجية خاصة ويوسع البيئة الإستراتيجية بمجملها.

المطلوب لبعد الزمن في الحيز الافتراضي، في ضوء السرعة التي تتحرك فيها الأبعاد في الحيز الالكترو- مغناطيسي . نتيجة لذلك فإن الحيز الافتراضي يمكن أن يعاظم قدرات أعداء قدماء، كما ويمكن أن ينضم إليهم أعداء ولاعبون جدد ومختلفون، واجهوا صعوبة في المشاركة في حروب ومعارك سابقة.

ويخلق الحيز الافتراضي، بالطريقة نفسها، فرصا أمنية جديدة ويتيح الاستعانة بحلفاء بشكل مختلف، تبعا لقدراتهم وموقعهم في هذا الحيز. لهذا السبب، ونتيجة للأولوية التي تعطيها الدول المختلفة لتطوير قدرات افتراضية، من المحتمل أن تنشأ موازين قوى جديدة بين الدول أو بين دول ومنظمات غير دولانية، وعليه فإن الحيز الافتراضي يخلق بيئة استراتيجية خاصة ويوسع البيئة الإستراتيجية بمجملها.

وتشخص في سياق النشاطات الأمنية ضد خصوم في البيئة الإستراتيجية الافتراضية، ثلاثة مجالات عمل:

أ- التسلل إلى شبكات الاتصال الالكترونية للعدو لأغراض التجسس. ولا يعتبر هذا النشاط بمثابة حرب افتراضية.

ب- حرب افتراضية ناعمة Soft Cyber Warfare ، وهي نشاطات في الحيز الافتراضي هدفها تشويش أداء العدو (من قبيل الحرب النفسية) من دون التسبب مباشرة بدمار أو خراب.

ج- حرب افتراضية (Cyber War)، نشاطات في الحيز الافتراضي تشمل هجمات تهدف التسبب، بشكل مباشر، بأضرار أو دمار للعدو، ومن ضمن ذلك إلحاق أضرار بشبكات الاتصالات الالكترونية أو بأهداف في الحيزات المادية، عن طريق ضرب الآلات والأجهزة المسيطر عليها من الحيز الافتراضي.

أما المسؤولية عن أنواع النشاطات المذكورة، فتتولاها عادة جهات أمنية في الدول، كالجيوش وأجهزة الاستخبارات، في حين تشارك في حماية الحيز الافتراضي جهات كثيرة من القطاع المدني ومن ضمنها وزارات حكومية (مثل وزارة أمن الوطن في الولايات المتحدة) وشركات خاصة (شركات تعمل في مجالات الحراسة والتكنولوجيا والاتصالات)، مما يتطلب إيجاد هيئة مشتركة للتنسيق بين سائر هذه الجهات، وخلق توازن بين المدافعين وبين المهاجمين، وهو ما يشكل تحديا مركزيا أمام مهندسي الإستراتيجيا الافتراضية على المستوى القومي.

تجسس وحرب افتراضية ناعمة

التجسس:

يعتبر التجسس نوعا من النشاطات (غير الهجومية) الشائعة في إطار مهام المؤسسات الأمنية في الحيز الافتراضي، ولا يهدف هذا النشاط إلى ضرب وتشويش أجهزة وشبكات العدو، أو حتى التأثير عليه بشكل مباشر. إن استخدام الحيز الافتراضي لأغراض جمع المعلومات له تاريخ طويل، منذ الشروع باستخدام الحواسيب والبرامجيات في أجهزة الاتصالات على اختلاف أنواعها. ويمكن في هذا المجال ملاحظة ثلاثة أنواع من النشاطات:

أ- جمع المعلومات الاستخباراتية عن قدرات الخصم ونواياه، وذلك لأغراض تقويم الوضع وبلورة الاستراتيجيات واتخاذ القرارات اللازمة.

ب- التجسس الصناعي، ومن ضمن ذلك سرقة أسرار تكنولوجية وتجارية.

ج- سرقة ثروات افتراضية يمتلكها الخصم مثل البرامجيات وقواعد البيانات والمعلومات، وذلك بهدف الاستفادة منها واستخدامها من دون إذن أو تصريح.

تجدر الإشارة إلى أنه وفي عالم اليوم، الذي توجد فيه لمصادر

ومنذ انتقال وسائل الإعلام الجماهيري إلى الانترنت في التسعينيات، طرأت زيادة مستمرة على استخدام الحيز الافتراضي في حرب رسائل المعلومات والدعاية. والاختلاف الرئيس بين حرب رسائل المعلومات في الحيز الافتراضي وبين الحرب الافتراضية يتمثل في الشريحة المتعرضة للهجوم مباشرة. أحد الدلائل الملموسة على التأثير الشديد لحرب رسائل المعلومات يمكن رؤيته في الثورات الجارية في الشرق الأوسط، بمساعدة الحيز الافتراضي. فقد نجح الشبان الذين يستخدمون رسائل المعلومات والأدوات الافتراضية في إحداث تغييرات سلطوية، كما حصل في مصر وتونس.

القوة الاقتصادية والتكنولوجية انعكاسات بعيدة الأثر على موازين القوى الإستراتيجية، يمكن أن يكون لجمع المعلومات والثروات الافتراضية التكنولوجية والاقتصادية وسرقتها تأثير وانعكاسات ملموسة على الأمن القومي للطرفين. فهذه المعلومات يمكن أن تحسن قدرة المنافسة لدى الدولة، التي تقوم بالجمع، في الاقتصاد العالمي وكذلك قدرتها على تقليص الفجوات في مجال البحث والتطوير الأمني. كذلك من الممكن أن تفقد الدولة، التي يتعرض حيزها الافتراضي للاختراق والقرصنة، ميزاتها ونقاط تفوقها الاستراتيجية. ويدور الحديث هنا على مجال تخرج فيه أنشطة الجمع عن نطاق الحاجة التقليدية لجمع معلومات من أجل معرفة الخصم والوقوف على قدراته ونواياه.

حرب رسائل معلوماتية:

حرب رسائل المعلومات هي نوع من الحرب الناعمة تعتمد على استغلال المعلومات والتلاعب بها، ما يشكل مكونا مركزيا في مجالات الحرب النفسية، والخدعة والدعاية وكشف معلومات يحرص الخصم على إخفائها. وتهدف هذه الحرب إلى التأثير على تفكير الخصم وسلوكه ومن يؤيده بشكل يتلاءم مع أهداف الطرف المبادر ومن دون اللجوء للقوة الحركية (النارية). الجانب الآخر في هذه النشاطات، أو «الحرب» هو الدعاية، وغايتها ضخ معلومات وعرض منطق العمل للجمهور المحلي والأصدقاء، وهو ما يعتبر أمراً حيويا لشرعية استخدام القوة.

ومنذ انتقال وسائل الإعلام الجماهيري إلى الانترنت في التسعينيات، طرأت زيادة مستمرة على استخدام الحيز الافتراضي في حرب رسائل المعلومات والدعاية. والاختلاف الرئيس بين حرب رسائل المعلومات في الحيز الافتراضي وبين الحرب الافتراضية يتمثل في الشريحة المتعرضة للهجوم مباشرة. أحد الدلائل الملموسة على التأثير الشديد لحرب رسائل المعلومات يمكن رؤيته في الثورات الجارية في الشرق الأوسط، بمساعدة الحيز الافتراضي. فقد نجح الشبان الذين يستخدمون رسائل المعلومات والأدوات الافتراضية في إحداث تغييرات سلطوية، كما حصل في مصر وتونس.

ففي هذه الحرب يشكل الحيز الافتراضي وسطا مساعداً ومؤثراً، غير أن أعداء أنظمة الحكم الشمولية هنا هم مواطنو الدولة وليسوا أعداء خارجيين.

هناك مجال آخر في حرب رسائل المعلومات، وهو كشف أسرار الخصم بهدف المس به. ويتناول الحديث هنا كشف نوايا وأعمال محظورة وتصريحات محرجة للزعماء وما شابه، وتبرز في هذا المجال نشاطات يقوم بها أفراد ومنظمات سياسية ضد مؤسسات دولانية.

عقوبات افتراضية:

العقوبات هي حرب ناعمة، غير سرية، هدفها معاقبة من يخل بالقواعد لإجباره على تغيير سلوكه وردعه عن تكرار عمله مرة أخرى، أو إضعافه تمهيدا لاستخدام وسائل قوة أخرى. هناك تشكيلة واسعة من العقوبات ابتداء من حرمان الدولة «المارقة» من التعاون وحقوق أخرى، مرورا بنبذها ومقاطعتها، وانتهاء بفرض حصار على حدودها (مثل الحصار الذي فرضه الائتلاف بقيادة الولايات المتحدة على العراق في عهد صدام حسين). ويعتبر الحيز الافتراضي مغريا للعقوبات، ذلك لأن الحديث يدور من ناحية فنية على نشاطات وأعمال سهلة التنفيذ نسبيا، من قبيل منع الاتصال مع الخارج، وهي عقوبة لها تأثير ملموس. مع ذلك فإن فرض عقوبات افتراضية ناجعة يتطلب ائتلافا يضم دولا ذات صلة.

حرب افتراضية:

هجوم افتراضي: الهجوم الافتراضي هو عمل حربي في الحيز الافتراضي ضد عدو بهدف إلحاق الضرر به وتشويش أدائه وجعله يرضخ لإرادة المهاجم. ولا يمكن للهجوم الافتراضي في حد ذاته تحقيق حسم أو إنجازات استراتيجية من قبيل احتلال مناطق على يد جيش بري، غير أنه قادر على إلحاق الضرر بأهداف وقدرات حيوية للعدو. في شهادته أمام الكونغرس في نيسان ٢٠١٠ تطرق قائد هيئة الـ«Cyber» الأميركية، إلى أنواع الأهداف القابلة للاستهداف بواسطة هجوم في الحيز الافتراضي، ومنها شبكات الدفاع الجوي ووسائل قتالية ومنظومات سيطرة وتحكم عسكرية، إضافة إلى بنى تحتية مدنية مثل شبكات الكهرباء والمواصلات والاتصالات والجهاز المالي. يجب الافتراض إذن أن الهجوم الافتراضي يمكن أن يصبح عنصرا في أي حرب عصرية في المستقبل، إلى جانب عناصر ومكونات قوة أخرى. وفي هذا السياق يمكن للهجمات الافتراضية أن تستخدم للغايات التالية:

- وسيلة لممارسة ضغوط من أجل تغيير سياسة الخصم (مثل الهجوم المنسوب لروسيا في أستونيا) في الفترات بين حروب تقليدية.
- إحباط تهديدات أمنية في طور التكون (على غرار هجوم Stuxnet في إيران).
- بناء قدرة هجومية كجزء من ميزان ردع.
- هجوم افتراضي مضاد كرد على مهاجمين أو دول تنطلق منها هجمات افتراضية.

وعلى الرغم من أن موضوع الهجوم في الحيز الافتراضي غير منظم من ناحية القانون الدولي، إلا أن هجوما من هذا النوع قد يعتبر عملا حربيا، خلافا لأعمال التجسس الافتراضي التي لا ينجم عنها ضرر مباشر ملموس، وبالتالي لا ينظر لها كعمل حربي.

ويمكن ملاحظة نوعين من الهجمات في هذا السياق: الأول هجوم في الحيز الافتراضي هدفه تشويش أو إلحاق ضرر بالحيز الافتراضي للخصم (حواسيب، شبكات، قواعد معلومات إلخ) بشكل يمنعه من استغلال الحيز الافتراضي لفائدته؛ والثاني استخدام الحيز الافتراضي لمهاجمة أجهزة مرتبطة بهذا الحيز (منشآت بنى تحتية، وسائل قتالية وغير ذلك).

الردع:

هناك إقرار بضعف هذا المصطلح التقليدي في سياق الحيز الافتراضي ذلك لأن هوية المهاجم لا تكون معروفة في جميع الحالات، خاصة في ضوء إمكانية قيامه باستخدام بنى وشبكات طرف ثالث. إضافة إلى ذلك فإن امتلاك الردع يتطلب عرض قدرات سرية يؤدي كشفها إلى فقدان قيمتها.

على الرغم من ذلك، فإن من الممكن القيام بأنشطة وعمليات ردع في الحيز الافتراضي، كتوجيه تحذير لدول عدوانية، وشن عمليات هجومية محدودة ضد أعداء بغية تأكيد القدرة، ولو بثمن كشف قدرات معينة. وعلى الرغم من صعوبة ممارسة الردع إجمالا، إلا أنه من الممكن أن تنشأ موازين ردع بين الدول في الحيز الافتراضي.

الدفاع في الحيز الافتراضي:

أدى تطور الحيز الافتراضي كحيز حيوي لأداء الدول إلى إثارة مسألة ضرورة حماية هذا الحيز والحيلولة دون المس بأهداف تقع خارج الحيز الافتراضي بواسطته. وبمقدار ما تستغل الدولة الحيز الافتراضي لفائدتها، فإنها تكون عرضة أكثر للمس به، وبالبنى التحتية والشبكات المرتبطة به. هذا الأمر ينسحب أيضا على المؤسسات الأمنية والعسكرية. فبمقدار ما تعتمد الجيوش والمؤسسات الأمنية على الحيز الافتراضي، تزداد أيضا تبعيتها له من حيث الأداء، وكذلك انكشافها.

وتنبع هشاشة الحيز الافتراضي من اعتماده أيضا على الحيز الالكترو- مغناطيسي. وتتطلب حماية الحيز الافتراضي مواجهة طائفة واسعة من عمليات الاختراق، ابتداء من عمليات اختراق لغرض جمع المعلومات وانتهاء بهجمات افتراضية. أما قائمة الأعداء الذين يتعين على منظومة الحماية مواجهتهم، فتشمل دولا معادية ومنظمات إرهابية وأشخاصا من الداخل يقومون بأعمال عامدة أو عابثة، ومجموعات قرصنة تعمل بدوافع أيديولوجية وغيرها، بالإضافة إلى حوادث الخلل.

على الرغم من المقولة الشائعة بأن الحيز الافتراضي هو «حيز بلا حدود»، إلا أنه يجب التمييز بين الحيز الافتراضي الكوني وبين الحيز الافتراضي الدولاني. فهذا الأخير يعني حواسيب وأجهزة ممكننة وشبكات وبرامجيات ومعلومات محسوبة وأوامر مرور ورقابة، والتي تستخدم كلها من جانب الدولة وسكانها.

على الرغم من المقولة الشائعة بأن الحيز الافتراضي هو «حيز بلا حدود»، إلا أنه يجب التمييز بين الحيز الافتراضي الكوني وبين الحيز الافتراضي الدولاني. فهذا الأخير يعني حواسيب وأجهزة ممكننة وشبكات وبرامجيات ومعلومات محسوبة وأوامر مرور ورقابة، والتي تستخدم كلها من جانب الدولة وسكانها.

إن الدفاع في الحيز الافتراضي هو تحد من نوع جديد، خاصة في ضوء قدرة العدو على شن هجوم بسرعة البرق والصعوبة في معرفة هوية المهاجم. كذلك فإن التمييز بين عمل تجسسي وبين عمل هجومي، أمر مهم بالنسبة للرد المضاد، إذ إن الدول تخرج للحرب بعد تعرضها لعدوان، لكنها لا تفعل ذلك في أعقاب تعرضها لعمل تجسسي، والذي لا يعتبر عملا حربيا. إلى ذلك، فإن ثغرة بسيطة أو حلقة ضعيفة واحدة- إنسانية أو تكنولوجية- من شأنها أن تؤدي إلى فشل الدفاع أو الحماية. ولا بد من الإشارة في هذا السياق أيضا، إلى أن الحيز الافتراضي يعزز من قدرة الجهة المعادية على استغلال ثغرات في منظومة الدفاع لصالحه، خاصة وأن منظومات الحماية تقف أحيانا عاجزة في مواجهة أعمال عامدة من جانب أفراد «من الداخل».

في العام ٢٠١٠ صدرت عن الجيش الأميركي وثيقة تحدد وتشرح مصطلح الدفاع الافتراضي على المستوى العملي (التنفيذي). ووفقا للوثيقة فإن الدفاع الافتراضي يتضمن جملة من النشاطات التي تدمج حماية شبكات حاسوب وحماية منشآت حساسة في منظومة واسعة، يمكن الرد منها أيضا بهجوم مضاد أو هجوم وقائي. ويمكن في إطار الدفاع في الحيز الافتراضي القيام بسلسلة واسعة ومنوعة من الخطوات والإجراءات الهادفة إلى منع ضرب، والحد من الخطر والضرر الذي يمكن أن تتعرض له بنى وشبكات اتصال الحواسيب الحيوية. كما ويتضمن ذلك خطوات من قبيل عزل شبكات معلومات معينة، الفصل بين شبكات، نشر شبكة حماية معلومات تقليدية مكونة من عدة مستويات أو شرائح، إتباع إجراءات حماية معلومات صارمة ومتغيرة، وغيرها.

هناك استجابة (جزئية) لتحدي سرعة الهجوم الافتراضي، وهذه الاستجابة قائمة في نظرية «الحماية الفعالة»، والتي تشكل أحد المكونات البارزة في إستراتيجية الدفاع الشاملة في الحيز الافتراضي لوزارة الدفاع الأميركية. وتستند هذه النظرية على قدرات استخباراتية متقدمة لرصد أي نشاطات في الشبكة، وعلى منظومات حماية ممكننة لرصد أي هجوم والرد عليه بصورة أوتوماتيكية دون تدخل بشري وكذلك على قدرات هجومية لأغراض الإحباط.

يتضح مما ذكر أن مفهوم حماية المعلومات (والذي يتعلق منطقه بحماية المعلومات من السرقة والإتلاف والخلل) لا يستنفد مجال الدفاع عن الحيز الافتراضي ذاته وعن الشبكات المرتبطة به. ويشار في هذا السياق إلى أن النشاطات الأشد ضررا وتدميرا- استخدام الحيز بغية إلحاق ضرر بالشبكات والبنى التحتية الحيوية والحساسة ومن ضمنها العسكرية- يمكن أن تتم من دون المس نهائيا ببرامج الحاسوب.

الإنذار الاستخباراتي:

لا يتطلب استخدام هذا المصطلح تلاؤما كبيرا مع الحيز الافتراضي فيما يتعلق بالإنذار الأولي، والمستند إلى تحليل نوايا إستراتيجية وطرق عمل ووسائل متاحة للعدو. مع ذلك يختلف التحدي فيما يتعلق بالإنذارات التنفيذية والتكتيكية، والتي تتطلب تعاملا مع تفاصيل الهجوم وتوقيته. فالتحضيرات لهجوم في الحيز الافتراضي يمكن أن تتم سرا، على عكس التحضيرات الواسعة، اللازمة لإعداد جيوش تقليدية للحرب، والمرتبطة غالبا بتسرب معلومات. أحيانا من الصعب أن يعرف الطرف المستهدف في زمن حقيقي أن الهجوم الافتراضي قد بدأ، قبل أن تظهر نتائجه، وفي بعض الأحيان لن

تظهر نتائجه إطلاقا (ستعتبر بمثابة خلل). من هنا يطرح السؤال بشأن جدوى الإنذار في واقع يتم فيه الهجوم (الافتراضي) بسرعة البرق، وبشأن ماهية الخطوات الدفاعية العملية التي يمكن لهذا الإنذار أن يخدمها.

التعاون الدولاني الداخلي ومع دول أخرى:

يعتبر التعاون الافتراضي موضوعا مركزيا لأغراض الدفاع والحماية، ذلك لأن الحيز الافتراضي يجتاز الحدود والقطاعات والمنظمات.

وفي هذا السياق هناك نوعان من التعاون: تعاون داخلي- دولاني: فالتعاون في الحيز الافتراضي له أهمية خاصة في مجال الدفاع والحماية، وخلافا للمجال الهجومي، الذي يخضع لمسؤولية قوات أمن الدولة واختصاصها ، فإن إقامة منظومة دفاعية قومية فعالة يستوجب تعاونا عميقا بين القطاعين المدني (العام والخاص) والعسكري، ذلك لأن من الصعب كما هو معروف الفصل بين الشبكات والبنى التحتية الافتراضية المدنية وبين الشبكات والبنى العسكرية، كما أن جزءا كبيرا من القدرات الافتراضية للدولة موجود في أيدي جهات خاصة. في ضوء ذلك هناك حاجة لتعاون متعدد الأبعاد، على المحور الأول- تعاون وتنسيق داخل القطاع العام- بين القطاعين المدني والعسكري، وعلى المحور الثاني- تعاون بين القطاعين العام والخاص (شركات تكنولوجيا متقدمة، شركات اتصالات، شركات حراسة.. إلخ).

والنوع الثاني هو التعاون مع دول أجنبية، وهو يشكل عنصرا مهما في مواجهة التهديدات الجديدة، وذلك في ضوء الطابع العالمي للحيز الافتراضي. وعلى سبيل المثال، يمكن بواسطة شبكات مراقبة مشتركة وتعاون استخباراتي تحسين قدرة الإنذار والتعقب والرد.

أهمية تكنولوجيا المعلومات والحيز الافتراضي بالنسبة لإسرائيل

تنطوي تقنيات المعلومات، والحيز الافتراضي ذاته، على أهمية ومساهمة إستراتيجية بالنسبة لإسرائيل. فالاقتصاد الإسرائيلي، وعلى غرار الدول الأكثر تقدما في العالم، يرتكز بدرجة كبيرة على بنى وشبكات الحيز الافتراضي. وتقدم فروع تكنولوجيا المعلومات مساهمة مباشرة وغير مباشرة في النمو الاقتصادي في إسرائيل التي تعتبر من الدول الرائدة في العالم في مضمار تطوير التقنيات المعلوماتية. ووفقا لدراسة أجرتها شركة الاستشارات الدولية «ماكينزي» فإن «اقتصاد الانترنت» في إسرائيل ينقسم إلى قسمين أو مجالين، وأن الجزء الأعظم منه يتركز في مجال صناعة تقنيات المعلومات والاتصالات (ICT)، ويشمل ذلك إنتاج وبيع معدات وبرمجيات وخدمات، أما الجزء الأصغر، والذي يشهد نموا سريعا، فيتمثل في مجال التجارة الالكترونية، والذي يعنى بشراء بضائع وخدمات عن طريق الانترنت.

وبحسب الدراسة فقد بلغت قيمة المساهمة المباشرة (في الإنتاج) لاقتصاد الانترنت في إسرائيل حوالي ٥٠ مليار شيكل في العام ٢٠٠٩، ما يشكل قرابة ٥ر٦٪ من الناتج المحلي الخام. هذا المعطى يضع إسرائيل في مصاف اقتصادات الانترنت المتصدرة عالميا. وتشير الدراسة ذاتها إلى أن "اقتصاد الانترنت" الإسرائيلي سيشهد، وفقا للتوقعات، نموا بوتيرة سنوية تصل إلى ٩٪، أي ضعفي وتيرة نمو الاقتصاد في إسرائيل. ومن المتوقع أن تصل قيمة مساهمة "اقتصاد الانترنت" الإسرائيلي في العام ٢٠١٥ إلى حوالي ٨٥ مليار شيكل، ستشكل قرابة ٥ر٨٪ من الناتج المحلي الخام. وتحتل فروع تكنولوجيا المعلومات أهمية خاصة نظرا لقدرتها العالية على المنافسة في السوق العالمية (جزء كبير من الناتج الإسرائيلي موجه إلى أسواق الخارج) ولأن السبيل الوحيد المتاح أمام إسرائيل كي تحقق نمواً سريعا هو زيادة الصادرات.

إلى ذلك فإن "اقتصاد الانترنت" يساهم بدرجة كبيرة في التشغيل في مرافق الاقتصاد الإسرائيلي، وخاصة تشغيل الأكاديميين من مجالات التكنولوجيا. بالإضافة إلى ذلك تقدم فروع تكنولوجيا المعلومات مساهمة مباشرة وغير مباشرة في القطاع الأمني/ العسكري في إسرائيل. كما وتشكل فروع تكنولوجيا المعلومات والاتصالات جزءا مهما من قدرات إسرائيل التكنولوجية، والتي تحظى بتقدير كبير من جانب خبراء كثيرين في أنحاء العالم، مما يساهم في تعزيز مكانة إسرائيل وسمعتها في العالم.

ويتيح الحيز الافتراضي لإسرائيل كسر عزلتها الجغرافية في الشرق الأوسط وإقامة علاقات وثيقة ومنتظمة مع العالم. كذلك تكمن في الحيز الافتراضي طاقة لتقوية الصلة والترابط بين الهامش والمركز في الدولة، وهو يشكل عنصرا مركزيا في النشاط الاجتماعي وعاملا مهما في تمتين أواصر العلاقة بين سلطات الحكم والمواطن.

إلى ذلك فإن "اقتصاد الانترنت" يساهم بدرجة كبيرة في التشغيل في مرافق الاقتصاد الإسرائيلي، وخاصة تشغيل الأكاديميين من مجالات التكنولوجيا. بالإضافة إلى ذلك تقدم فروع تكنولوجيا المعلومات مساهمة مباشرة وغير مباشرة في القطاع الأمني/ العسكري في إسرائيل. كما وتشكل فروع تكنولوجيا المعلومات والاتصالات جزءا مهما من قدرات إسرائيل التكنولوجية، والتي تحظى بتقدير كبير من جانب خبراء كثيرين في أنحاء العالم، مما يساهم في تعزيز مكانة إسرائيل وسمعتها في العالم.

استعداد إسرائيل لحماية الحيز الافتراضي

عند الحديث عن الاستعدادات التي قامت بها إسرائيل لحماية الحيز الافتراضي فإن من الممكن الإشارة إلى عدد من النقاط البارزة.

ففي العام ١٩٩٧ أقيم مشروع البنية التحتية الحكومية لعصر الانترنت (مشروع «تهيلاه»). والهدف من المشروع، الذي أقيم في قسم المحاسب العام في وزارة المالية، هو تزويد خدمات تصفح محمية لوزارات الحكومة ومؤسساتها ودوائرها.

وبحسب ما ورد في الموقع الالكتروني لهذه الهيئة، فإنها تحتوي على شبكة ملقمات (خوادم) يتلقى عن طريقها شهريا مئات آلاف المواطنين خدمات حكومية متاحة ومعلومات عن نشاطات وزارات الحكومة. وتستخدم «تهيلاه» وسائل وتدابير لحماية أمن شبكة الانترنت الحكومية، ابتداء من طاقم خبراء حماية معلومات واتصالات وانتهاء بمنتجات وتقنيات شركات عالمية رائدة. كما أقيم في إطار تهيلاه «مركز حماية معلومات حكومة إسرائيل»، الذي تشمل مهامه متابعة ورصد حوادث حماية معلومات على مستوى العالم، مع إيلاء اهتمام لهجمات داخل الشبكة تتعلق بإسرائيل؛ التنسيق بين هيئات حكومية من أجل حل مشاكل حماية وتنسيق العلاقة بين هذه الهيئات وبين جهات خارجية إضافة إلى إجراء أبحاث ودراسات في هذا المجال، كما ويصدر المركز إنذارات حماية معلومات للمنظمات العاملة في مجال تكنولوجيا المعلومات والتي تقيم علاقات مع «تهيلاه»، أو لجهات حكومية غير مصنفة. كذلك يقيم المركز علاقات مع جهات دولية بهدف القضاء على هجمات محوسبة. ويعمل في هذا الإطار طاقم (CERT (Computer Emergency Response Team الذي تتمثل مهمته في تقديم إجابات وحلول فورية لحوادث حماية معلومات في المؤسسات الحكومية. ويدير طاقم CERT مركز ردود فيما يتعلق بظواهر الهجمات داخل الشبكة وإدارة المخاطر وإيجاد تدابير حماية معلومات ومراقبة مرور ومنع أعمال القرصنة وتزوير الهوية داخل الشبكة، بالإضافة إلى المحافظة على خصوصية المعلومات ورفع مستوى الوعي بالحماية. وتشمل أنشطة الطاقم ومهامه أيضا إقامة صلات التعاون والتنسيق مع الشرطة وسائر أذرع المؤسسة الأمنية الإسرائيلية. ومما لا شك فيه أن هذه الهيئة أخذت على عاتقها مهام جسيمة، علما أن صلاحيات عملها تتعلق بصورة رئيسة بتوفير خدمات تصفح محمية في شبكة الانترنت لوزارات الحكومة ودوائرها ومؤسساتها، كما أن المركز ليس هيئة تنفيذية مشتركة للجهات المسؤولة عن أمن الحيز الافتراضي، مثلما هي الحال في دول غربية.

في آذار ٢٠١١ صادقت الحكومة على إقامة وحدة "منمار" (مديرية منظومات المعلومات) الحكومية، وهي هيئة بين وزارية مهمتها تركيز وتنسيق مجال الاتصالات الالكترونية في الحكومة. ويفترض بهذه الهيئة، التي تخضع لمسؤولية المدير العام في وزارة المالية، أن تقوم بتوجيه وحدات الاتصال الالكتروني في وزارات الحكومة وأن تتحمل المسؤولية المباشرة عن جميع مشاريع الحوسبة الحكومية ومن ضمن ذلك مشروع «تهيلاه». ويشكل تركيز مشاريع الحوسبة الحكومية في مكان واحد تقدما كبيرا في استعدادات الدولة في مجال الاتصالات الالكترونية، غير أن من الأفضل أن تكون الجهة المسؤولة عن إدارة أمن منظومات المعلومات من خارج الجهة أو المؤسسة المنشأة والمشغلة لهذه البنى والشبكات.

في العام ٢٠٠٢ أقيمت السلطة الرسمية لحماية المعلومات في جهاز الأمن العام (الشاباك)، وهي مسؤولة عن التوجيه المهني

في العام ٢٠٠٢ أقيمت السلطة الرسمية لحماية المعلومات في جهاز الأمن العام (الشاباك)، وهي مسؤولة عن التوجيه المهني للهيئات ذات الصلة بنطاق مسؤوليتها، في مجال حماية شبكات حاسوب حيوية من التهديدات الإرهابية والتخريب في مجال حماية المعلومات المصنفة (السرية) وتهديدات التجسس والكشف. وعلى ما يبدو فإن المنطق خلف كون هذه السلطة تعمل كوحدة في جهاز "الشاباك" مرتبط بمسؤولية الجهاز عن إحباط أنشطة التجسس والإرهاب. هذا الأمر، المتعلق بموقع "السلطة" ذاتها، ينطوي، كما يبدو الآن، على أفضليات وثغرات.

للهيئات ذات الصلة بنطاق مسؤوليتها، في مجال حماية شبكات حاسوب حيوية من التهديدات الإرهابية والتخريب في مجال حماية المعلومات المصنفة (السرية) وتهديدات التجسس والكشف. وعلى ما يبدو فإن المنطق خلف كون هذه السلطة تعمل كوحدة في جهاز "الشاباك" مرتبط بمسؤولية الجهاز عن إحباط أنشطة التجسس والإرهاب. هذا الأمر، المتعلق بموقع «السلطة» ذاتها، ينطوي، كما يبدو الآن، على أفضليات وثغرات. إحدى الأفضليات المهمة تتمثل في العلاقة الوثيقة بين «السلطة» وبين باقي القدرات والصلاحيات التي يتمتع بها جهاز «الشاباك» (بموجب ما ينص عليه القانون الخاص بجهاز «الشاباك») ومؤسسة الاستخبارات التي يشارك فيها جهاز «الشاباك». في المقابل هناك أطر وهيئات في القطاع الخاص يمكن أن تحجم عن كشف نفسها لـ «السلطة الرسمية لحماية المعلومات» التي تعمل كوحدة في جهاز يتولى مهمات وصلاحيات واسعة جداً لا تتعلق فقط بهذا الجانب. إضافة إلى ذلك فإن جهاز «الشاباك» هو بطبيعته منظمة تنفيذية تزاول أنشطة إحباط سرية، وليس مكلفا بمهام أخرى مطلوبة من اجل مواجهة التحدي الافتراضي، مثل إقامة علاقة وثيقة مع القطاع الخاص وزيادة وعي السكان بالحماية الافتراضية والاعتناء بمؤسسات لحقت بها أضرار جراء هجوم افتراضي.. إلخ.

وتتلقى "السلطة الرسمية لحماية المعلومات في جهاز الشاباك" التعليمات من قبل لجنة توجيهية لحماية المنظومات المحوسبة في «هيئة الأمن القومي» ويقف على رأس اللجنة رئيس هيئة مكافحة الإرهاب في هيئة الأمن القومي. ومن مهام اللجنة التوجيهية إعطاء الإذن لسلطة حماية المعلومات بتوسيع قائمة الهيئات الموجهة أو المحمية المطالبة بتعميق حمايتها والالتزام بتوجيهات السلطة.

لكن هذا النشاط لم يرتكز على عملية قانونية ومنهاجية في تحديد هذه الهيئات وإعطاء الإذن بشأنها، ولذلك نجد أن القائمة تضم شركات كبيرة وحيوية في قطاعات معينة، في حين تركت خارج القائمة شركات كبيرة تعمل في قطاعات أخرى (مثلا في مجالات المواد الغذائية والعقاقير الطبية)، على الرغم من مساهمتها الكبيرة في التشغيل وفي نسيج الحياة. هناك خلل آخر في هذه الطريقة وهو تركيزها على توجيه شركات منتقاة من قطاعات معينة، وعدم قيامها بتوفير حماية شاملة والتي تتطلب تغطية أوسع لهيئات وشركات مرتبطة بالشبكة الحيوية نفسها. وعلى سبيل المثال شبكة المياه: فحماية منشآت ضخ المياه وجودتها في إسرائيل لا تتعلق فقط بالإجراءات في شركة «مكوروت»، التي تظهر في القائمة، بل تتعلق أيضا بعشرات من مزودي المياه الآخرين (جمعيات وشركات) ومنشآت تحلية ونقل ومنشآت معالجة المياه العادمة وغيرها، ويشغل القسم الأكبر من هذه المنشآت بواسطة مقاولين وشركات خاصة لا يولون أهمية لوسائل وتدابير الحماية. هذا الوضع ينطبق على مجالات كثيرة أخرى.

في المقابل، هناك مثال على التوجيه، يعكس إدراكا عاليا تجاه أمن منظمات المعلومات، نجده لدى المسؤولين عن الهيئات المالية في وزارة المالية و«بنك إسرائيل». فقد أصدرت وزارة المالية (قسم سوق المال والتأمين والادخار) توجيهات مفصلة للمؤسسات المالية المهتمة بحماية المعلومات ونظم المعلومات. كذلك أصدر مراقب البنوك في «بنك إسرائيل» نشرة شاملة ومفصلة، أكدت من ضمن أشياء أخرى على أن «تكنولوجيا المعلومات تشكل عنصرا مركزيا في التشغيل والإدارة السليمة لأي إتحاد مصرفي، وذلك بكون المعلومات على اختلاف أبعادها وانعكاساتها، لها تأثير حاسم على

في ١٨ أيار ٢٠١١ أعلن رئيس الحكومة بنيامين نتنياهو عن إقامة "هيئة سايبر قومية". وبحسب بيان صدر عن ديوان رئيس الحكومة فإن الغاية الرئيسة لهذه الهيئة هي توسيع القدرات الدفاعية للدولة عن شبكات البنى التحتية الحيوية إزاء هجمات إرهابية افتراضية، تشن من جانب دول أجنبية أو من جانب عناصر إرهابية. وكانت هذه الهيئة قد أقيمت في أعقاب توصيات طاقم ترأسه رئيس المجلس القومي لشؤون البحث والتطوير الجنرال احتياط إسحق بن يسرائيل. وقال رئيس الحكومة نتنياهو، الذي تبنى هذه التوصيات بأكملها: إن إسرائيل مكشوفة، في المجال الدفاعي، لهجمات افتراضية قادرة على شل منظومات الحياة التي تدير وتفعل الدولة.

استقرار الاتحاد وتطوره». مثل هذا التوجيه يمكن أن يشكل نموذجا للوزارات الحكومية الأخرى فيما يتعلق بالهيئات والمؤسسات التي تعمل مقابلها في الدولة.

هيئة الـ «سايبر» التابعة للجيش الإسرائيلي: في العام ٢٠٠٩ وصف رئيس هيئة الأركان العامة، الجنرال غابي أشكنازي، الحيز الافتراضي كحيز قتالي استراتيجي. بناء على ذلك أقيمت هيئة الـ «سايبر» في الجيش الإسرائيلي، لكي تستخدمها هيئة الأركان العامة في تنسيق وتوجيه نشاطات الجيش في الحيز الافتراضي. وقد أقيمت الهيئة في إطار الوحدة ٨٢٠٠ التابعة لشعبة الاستخبارات العسكرية («أمان») وتضم ممثلين من هذه الشعبة ومن شعبة الاتصالات الالكترونية في الجيش.

رئيس شعبة الاستخبارات العسكرية (سابقا) الجنرال عاموس يادلين تطرق لهذا الموضوع في محاضرة ألقاها في معهد دراسات الأمن القومي (جامعة تل أبيب) في كانون الأول العام ٢٠٠٩، بقوله إن «الجيش الإسرائيلي يعتزم توفير حماية جيدة للشبكات والقيام أيضا بشن هجمات افتراضية». إلى ذلك فإن في إمكان الهيئة الافتراضية التابعة للجيش الإسرائيلي المشاركة في حماية الحيز الافتراضي للدولة، على غرار القيادة الافتراضية في الولايات المتحدة، لكنها أيضا ليست الهيئة المخصصة لتوفير الحماية القومية الشاملة للحيز الافتراضي القومي للدولة.

«هيئة السايبر القومية»: في ١٨ أيار ٢٠١١ أعلن رئيس الحكومة بنيامين نتنياهو عن إقامة «هيئة سايبر قومية». وبحسب بيان صدر عن ديوان رئيس الحكومة فإن الغاية الرئيسة لهذه الهيئة هي توسيع القدرات الدفاعية للدولة عن شبكات البنى التحتية الحيوية إزاء هجمات إرهابية افتراضية، تشن من جانب دول أجنبية أو من جانب عناصر إرهابية. وكانت هذه الهيئة قد أقيمت في أعقاب توصيات طاقم ترأسه رئيس المجلس القومي لشؤون البحث والتطوير الجنرال احتياط إسحق بن يسرائيل. وقال رئيس الحكومة نتنياهو، الذي تبنى هذه التوصيات بأكملها: إن إسرائيل مكشوفة، في المجال الدفاعي، لهجمات افتراضية قادرة على شل منظومات الحياة التي تدير وتفعل الدولة مثل الكهرباء والمياه والاتصالات والنقل وبطاقات الاعتماد. فكل مجال من هذه المجالات محوسب ولذلك فهو قابل للتعطيل أو الضرر، وهناك ضرورة لبلورة رد دفاعي إزاء هذا التهديد. وبحسب ما نشر أيضا فإن الهيئة المستحدثة ستعمل على رعاية شركات إسرائيلية متخصصة في حماية الحيز الافتراضي، وذلك في محاولة لاقتطاع حصة من السوق الواسعة المتنامية في هذا المجال في أرجاء العالم. إن قيام هذه الهيئة سيشكل إضافة نوعية مهمة نظرا لأنه لا توجد في إسرائيل حتى الآن هيئة مسؤولة عن معالجة حماية الحيز الافتراضي وفق رؤية قومية شاملة.

توصيات

ثمة ثلاثة أسباب وجيهة تستدعي من إسرائيل تكثيف استعدادها الأمني في الحيز الافتراضي:

١. على غرار دول غربية متطورة أخرى، فإن الحيز الافتراضي يكشف إسرائيل لمخاطر أساسية ملموسة، ومن ضمنها إلحاق الضرر ببنى تحتية حيوية وبالمؤسسة الأمنية وبعمل وأداء مرافق الاقتصاد، وما شابه ذلك.

٢. خلافا لدول كثيرة، فإن إسرائيل تواجه أعداء لديهم دوافع واضحة ومعلنة للمس بها قدر الإمكان. فهناك على سبيل المثال إيران التي تسعى أيضا لامتلاك قدرات افتراضية

هجومية. كذلك من المحتمل قيام منظمات إرهابية بنشاطات هجومية في الحيز الافتراضي توجه ضد إسرائيل.

٣. تمتلك إسرائيل، التي تعتبر من الدول المتصدرة في مجالات تكنولوجيا المعلومات والحضور في الحيز الافتراضي، الإمكانية لتطوير حماية متقدمة واستنفاد الأفضليات التي ينطوي عليها الحيز الافتراضي في ساحة القتال.

وفي إطار حث وتسريع الاستعدادات الإسرائيلية، لا بد من القيام بعدد من الخطوات ومنها على وجه الخصوص:

أولا- وضع استراتيجيا قومية لأمن الحيز الافتراضي الإسرائيلي، وتطبيق هذه الاستراتيجيا بقيادة "هيئة السايبر القومية".

ثانيا- دمج الحرب الافتراضية كعنصر أو مكون في الاستراتيجيا الأمنية لإسرائيل.

إن قرار إقامة «هيئة السايبر القومية» يشكل في الحقيقة خطوة مهمة إضافية في مواجهة إسرائيل للتحدي الافتراضي، لكن ينبغي ضمان أن تعمل الهيئة بناء على استراتيجيا افتراضية قومية، تتم بلورتها لهذا الغرض. كذلك من الأهمية بمكان، في ضوء تخلف إسرائيل في هذا المجال، أن تقام الهيئة المذكورة على وجه السرعة، وأن توكل إليها مسؤولية وصلاحيات ملائمة بغية سد الفجوة القائمة على المستوى القومي فيما يتعلق بالإدارة الإستراتيجية والدمج والتكامل بين سائر الجهات التنفيذية - المدنية والعسكرية- العاملة في الحيز الافتراضي في الصدد الدفاعي.

إستراتيجيا لحماية الحيز الافتراضي الإسرائيلي- اقتراح

هنا اقتراح لبلورة إستراتيجيا قومية لأمن وحماية الحيز الافتراضي الإسرائيلي، والتي يمكن لها أن تحقق الأهداف الإستراتيجية بالحد الأدنى من الموارد وأن تشكل إطار عمل لسائر الجهات المشاركة في حماية هذا الحيز الافتراضي.

كذلك فإن هذه الإستراتيجيا ستشكل خطًا موجها للعمل المشترك لسائر الهيئات مجتمعة ولنشاط كل منها على حدة طبقا لمسؤوليتها ومجال عملها.

أهداف الإستراتيجيا

أولا- إيجاد وتوفير حيز افتراضي آمن في إسرائيل يتيح للدولة تحقيق أهدافها القومية في مجالات الحكم والأمن والاقتصاد والمجتمع والشؤون الخارجية والعلوم وغيرها.

ثانيا- تعزيز الأمن في الحيز الافتراضي الإسرائيلي والمحافظة على حرية العمل والنشاط فيه بما يخدم عامة السكان.

ومن المفترض أن تعمل هذه الإستراتيجيا على دفع تحقيق هذه الأهداف بواسطة دمج وتضافر الطاقات والجهود لكافة الجهات ذات الصلة في الدولة وذلك بموجب مبادئ العمل التالية:

١. اعتبار الحيز الافتراضي حيزا قوميا جديدا ينبغي الدفاع عنه وحمايته بشكل خاص (خلافا للمجالات- الحيزات- التقليدية) من خلال رؤية شاملة وتعاون بين جميع الجهات ذات العلاقة.

٢. إنشاء قيادة وجهاز مركزي للدفاع الافتراضي على المستوى القومي (إقامة منظمة على المستوى الدولاني).

٣. إدارة المخاطر من خلال رؤية شمولية، ومن ضمن ذلك وضع البنى التحتية الوطنية الحساسة والأجهزة والمنظومات الأمنية على رأس سلم الأولويات، إلى جانب معالجة حماية مكونات وعناصر إضافية في مجالي الاقتصاد والمجتمع، مثل حماية مستودعات المعرفة والخبرة لدى الجامعات ومراكز الأبحاث، وحماية شركات ذات تأثير على الاقتصاد (والتي ما زالت غير مشمولة ضمن قائمة البنى التحتية)، وكذلك حماية الشركات المرتبطة بشركات بنى وشبكات تحتية حيوية. .

٤. بناء نظام حماية مدمج وشامل، ومن ضمن ذلك دمج بين منظومات دفاع سلبية ومنظومات دفاع إيجابية؛ دمج بين دفاع عن أهداف حيوية وبين عناصر «حماية إقليمية»، تحسين هندسة الشبكات والربط الوثيق بين منظومات حماية سلبية ومنظومات الحماية الافتراضية.

٥. تضافر قوى وطاقات في القطاع العام (الحكومي) بين القطاعين الأمني والمدني، وكذلك بين وحدات داخل كل قطاع من هذين القطاعين، مثلا تضافر الجهود والتعاون بين الجيش وبين قوى الأمن الأخرى.

٦. تعاون وثيق بين القطاع الحكومي (الأمني والمدني) وبين القطاع الخاص في حماية الحيز الافتراضي، بما في ذلك في الخبرة والقدرات، بحيث تكون كل مؤسسة، حكومية أو خاصة، مدركة للمخاطر ولقدرات الحماية الجديدة.

٧. تعاون وثيق مع جهات خارجية، مثلا بناء منظومات رصد ومراقبة جماعية مع جهات حليفه.
٨. سن تشريعات تتيح النشاط الدفاعي وتطبيقها.
٩. مساعدة السكان بصورة عامة في مجال الحماية الافتراضية وذلك مثلا بواسطة نشاطات دعائية لزيادة وعي الجمهور بالتهديدات والحلول؛ تقديم حوافز لشراء وامتلاك برمجيات حماية؛ زيادة الرقابة على شركات الحراسة ومزودي الاتصالات للجمهور في البعد المذكور.
١٠. بناء قدرة على الانتعاش السريع من هجوم افتراضي.
١١. استخدام الطرق والوسائل التكنولوجية الأكثر تقدما.
١٢. بلورة سياسة ردع وإحباط هجمات ورد كعناصر مكملة للاستراتيجيا، ومن ضمن ذلك قدرة رد مباشر وفوري ضد منظومات افتراضية معتدية وقدرة على المس بالمعتدي، والجهة المسؤولة عن هذا الموضوع هي المؤسسة الأمنية.

ومن أجل تطبيق هذه الاستراتيجيا، نقترح أن تشمل مهام "هيئة السايبر القومية"، ما يلي:

١. مساعدة المستوى السياسي في اتخاذ القرارات ورسم سياسة في مجال حماية الحيز الافتراضي القومي، ومن ضمن ذلك بلورة اقتراح لاستراتيجيا قومية لحماية الحيز الافتراضي، يصادق عليها المجلس الوزاري للشؤون السياسية والأمنية.
٢. وضع تقديرات مخاطر، دائمة وآنية، اعتمادا على معطيات وتقديرات توفرها أجهزة الاستخبارات والهيئات التنفيذية والتكنولوجية ذات الصلة، وتقديم توصيات للعمل بناء على تحليل بدائل.
٣. تنسيق نشاطات سائر الجهات الحكومية والخاصة، المتعلقة بأمن الحيز الافتراضي، ويشمل ذلك إلقاء مسؤولية على الوزارات الحكومية المدنية في دفع وتعزيز الأمن الافتراضي في مجالها (كما تفعل مثلا وزارة المالية ومراقب البنوك في "بنك إسرائيل" تجاه هيئات مالية مؤسسية).
٤. إقامة مركز تنفيذي دولاني («مركز عمليات» افتراضي) وإدارته، ومهمته توفير تقويم ديناميكي لتهديدات افتراضية، وإيجاد تنسيق وتبادل معلومات بين كافة الجهات ذات العلاقة بالأمر والمساعدة في إدارة الحماية.
٥. تحديد شبكات البنى التحتية والأطر والمؤسسات المدنية التي يتعين على الدولة توجيهها أو حمايتها في المجال الافتراضي، وذلك بموجب الاستراتيجيا القومية.
٦. المبادرة لسن قوانين وأنظمة ضرورية لأنشطة حماية الحيز الافتراضي في الأحوال الاعتيادية وفي أوقات الطوارئ.
٧. المبادرة والوقوف على رأس مشاريع حكومية في مواضيع من قبيل تطوير وتحسين طرق ووسائل حماية لشبكات المعلومات (ومن ضمن ذلك حماية مادية)، إنشاء جهاز ممأسس لإرشاد العاملين والموظفين في القطاع الحكومي، تحسين قدرة الانتعاش بعد هجوم افتراضي، إدارة مناورات حماية افتراضية على المستوى القومي.
٨. وضع معايير لتطوير وشراء وتركيب وسائل اتصالات الكترونية، وذلك ضمن أبعاد الأمن الافتراضي، وإعطاء أذون وتصاريح لإقامة بنى وشبكات اتصال الكترونية تبعا لتأثيرها على أمن الحيز الافتراضي القومي
٩. مبادرة وتوجيه في مجال تطوير وسائل الحماية وتأهيل القوة البشرية المهنية والبحث العلمي ارتباطا بأمن الحيز الافتراضي.
١٠. المبادرة لإقامة تعاون استراتيجي بين القطاعين الحكومي والخاص، ومن ضمن ذلك تعاون مع شركات اتصال وتكنولوجيا في مجالات التشغيل والبحث والتطوير.
١١. تنسيق التعاون مع دول أخرى فيما يتعلق بأمن الحيز الافتراضي.
١٢. مراقبة تطبيق الاستراتيجيا والنشاط في مجال حماية الحيز الافتراضي، والتأكد من وجود رقابة ملائمة على الوزارات المختلفة والسلطات المدنية، ومزودي الاتصالات من ناحية التجهيزات وتطبيق مبادئ الأمن الافتراضي.
١٣. أن تشكل الهيئة مركزا قوميا للخبرة والمعرفة في مجال حماية الحيز الافتراضي وأن يكون متصلا بمراكز مشابهة في البلاد والخارج، مع الاستفادة من طرق مواجهة الدول الأخرى للتحدي الافتراضي.

دمج الحيز الافتراضي في إستراتيجيا الأمن الإسرائيلية

إن إضافة مجال قتالي جديد للمجالات التقليدية (البر والبحر والجو والفضاء) يتطلب دمج الحيز الافتراضي في الاستراتيجيا،

أو النظرية الأمنية لإسرائيل.

في نيسان ٢٠٠٦ (قبل حرب لبنان الثانية) قدمت لجنة برئاسة دان مريدور، عينها وزير الدفاع في حينه عمير بيرتس، اقتراحا تضمن نظرية أمنية محدثة. وقد أشارت اللجنة من ضمن جملة أشياء إلى الصلة المحدودة لمصطلح الردع في سياق مكافحة الإرهاب، والصعوبة في تجسيد مدلول مصطلح الحسم، وأوصت بإضافة الدفاع (أو الحماية) كمكون إضافي للمكونات التقليدية الثلاثة (الردع، الإنذار والحسم) في عقيدة الأمن الإسرائيلية. في كانون الأول ٢٠٠٩ قال رئيس شعبة الاستخبارات العسكرية، في حينه، الجنرال عاموس يادلين إن «مجال الحرب الافتراضية يلائم تماما النظرية الهجومية لإسرائيل. إنه مجال إسرائيلي خالص، لا يعتمد على مساعدة أو تكنولوجيا أجنبيين».

وقد أظهر تفحص المصطلحات ذات الصلة بنظرية الأمن الإسرائيلية، أن مضامين مصطلحات نظرية الأمن التقليدية لا تلائم مجال الحرب الافتراضية.

على سبيل المثال فإن من الصعب جدا تجسيد الردع في الحيز الافتراضي، والإنذار التنفيذي لا قيمة له بدون حماية أو دفاع فعال، والدفاع الافتراضي يتطلب مواءمة عميقة للسمات الخاصة للحيز. كذلك فإن التعاون المطلوب لحماية الحيز يعتبر منقطع النظير بالمقارنة مع أشكال تعاون أخرى بين القطاعين الأمني والمدني لغرض النشاط العسكري.

إلى ذلك هناك حاجة، في ضوء الاعتراف بالحيز الافتراضي كحيز قتالي، إلى تفحص قدرات إستراتيجية جديدة، وربما إلى إحداث تغيير في تشكيل القوى، بمعنى الاستثمار أكثر في إقامة جيش افتراضي.

أخيرا، فإن إسرائيل تحوز على طاقة وإمكانية في أن تكون بين الدول المتصدرة في العالم في مجال الأمن الافتراضي، وذلك بالنظر إلى ما تمتلكه من ثروة بشرية وخبرة تكنولوجية عالية. إن استنفاد هذه الطاقة يمكن أن يساهم في تعزيز قدرة الدولة ومناعتها في مجالي الأمن والاقتصاد.