أحمد قاسم حسين | *Ahmed Qasem Hussein

كيف تُحضّر إسرائيل حروبها المستقبلية

مراجعة كتاب السلاح السيبراني في حروب إسرائيل المستقبلية: دراسات لباحثين إسرائيليين كبار

How Israel is Preparing its Future Wars

Book Review of *The Cyber Weapon in Israel Future Wars: Studies by Senior Israeli Researchers*

مجموعة مؤلفين

السلاح السيبراني في حروب إسرائيل المستقبلية: دراسات لباحثين إسرائيليين كبار

إعداد: رندة حيدر (بيروت: مؤسسة الدراسات الفلسطينية، 2018)، 176 صفحة.

* باحث في المركز العربي للأبحاث ودراسة السياسات.

Researcher at the Arab Center for Research and Policy Studies.

يُعدّ مفهوم "القوة السيبرانية" من المفاهيم الجديدة التي احتلت مكانة أكاديمية في أدبيات العلوم السياسية، وبات يُستخدم في توصيف من توصيفات القوة "الصلبة"، أو "الناعمة"، أو "الذكية" وشرحها. ويرجع الفضل في التنظير لهذا المفهوم إلى عالم السياسة الأميركي جوزيف ناي الذي عرّف "القوة السيبرانية" بأنها القدرة على تحصيل نتائج مرجوّة من خلال الاعتماد على مصادر المعلومات المرتبطة بالفضاء السيبراني؛ أي إنها القدرة على استخدام الفضاء السيبراني بهدف إيجاد مزايا للدولة[1]، وتحقيق مصالحها، ومنحها قوة للتأثير في محيطها بما يضمن أمنها القومي. وجادل، في كتابه **القوة الناعمة**، أنه في عالم اليوم المتسم بالتطور المتسارع، ما عاد في الإمكان حساب قوة الدولة اعتمادًا على العناصر المادية، العسكرية والاقتصادية فحسب، حيث إنّ لتقدم العلم والتكنولوجيا آثارًا متناقضة في القوة المادية؛ فقد ظهر، مثلًا، عدد من التهديدات الأمنية، مثل الإرهاب والجرائم الدولية وانتشار الأوبئة والأمراض السارية، التي تتطلب امتلاك موارد القوة الناعمة لمواجهتها والتصدي لها[2].

تعمل وحدات النظام الدولي على اختلافها دولًا، ومنظمات، وأفرادًا على استشراف التحولات التي تطرأ على مفهوم القوة وأشكاله، وتحديد التهديدات التي تنتجها التطورات في مجال التكنولوجيا. بل إن دولًا باتت تتعامل مع هذه التحديات بمنطق السوق التجارية من خلال إنتاج أجهزة التجسس والتنصت وتدريب الأفراد للقيام بهجوم "سيبراني" والتصدّي لها، والتي تشمل عادةً المؤسسات الحيوية في الدولة، في ما بات يعرف اصطلاحًا بـ "الحرب السيبرانية". ويمكن اعتبار إسرائيل اليوم مصدرًا كبيرًا لأجهزة التجسس في العالم؛ حيث تُصدّرها من دون رقابة أو محاسبة إلى الحكومات الدكتاتورية والتسلطية في عدد من دول العالم لقمع المعارضة وملاحقة بعض الفئات الاجتماعية مثل المثليين جنسيًا. وفي تقرير صحافي أجرته جريدة **هآرتس**، نقلًا عن 100 مصدر في 15 دولة، جاء أنّ النظم الدكتاتورية في جميع أنحاء العالم تستغل هذه الأجهزة الإسرائيلية الصنع في التنصت على الناشطين الحقوقيين ومتابعة رسائل البريد الإلكتروني واختراق التطبيقات وتسجيل المحادثات، وذلك حتى في البلدان التي لا يربطها بإسرائيل تمثيل دبلوماسي. مع الإشارة إلى أن صفقات بيع أجهزة التجسس تعقد بإشراف وزارة الدفاع وحدها، مع عجز الكنيست على ممارسة الرقابة عليها، وعدم حصوله على التفصيلات الأساسية لهذه الصادرات[3].

يعالج هذا الكتاب تطور مفهوم الحرب السيبرانية في إسرائيل ودورها في العقيدة العسكرية للجيش الإسرائيلي، وذلك استنادًا إلى دراسات وأبحاث وضعها خبراء إسرائيليون في هذا المجال، ونشرتها مراكز

---

1 Joseph Nye, "Cyper Power," Harvard Kennedy School, Belfer center for Sciences and International affairs, 2010, p. 4, accessed on 31/3/2019, at : https://goo.gl/9yNekm

2 Joseph S. Nye, *Smart Power*, Adele Oliveri (Trans.) (Bari: Gius. Laterza & Figli, 2012), pp. 38-45.

3 Hagar Shezaf & Jonathan Jacobson, "Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays," *Haaretz*, 20/10/2018, accessed on 5/01/2019, at: https://bit.ly/2J4UgRT

أبحاث إسرائيلية أو مجلات عسكرية متخصصة، ونقلها إلى العربية مترجمون يتعاملون مع مؤسسة الدراسات الفلسطينية. غالبية الدراسات مأخوذة من منشورات معهد دراسات الأمن القومي[4] الذي يُصدِر نشرة متخصصة بالموضوع ثلاث مرات في السنة، إضافة إلى مؤتمر سنوي يعقده في هذا الشأن. يحظى المعهد بسمعة أكاديمية جيدة، ويعتبر مرجعًا مهمًا للمسؤولين الإسرائيليين وصانعي القرار. أما المصدر الثاني لهذه الدراسات، فهو مجلة **معراخوت**، وهي مجلة فصلية تصدر باللغة العبرية عن هيئة الأركان العامة للجيش الإسرائيلي.

أقسام الكتاب

يقع الكتاب في ثلاثة أقسام، يعرض القسم الأول بناء على مقاربة منهجية الأطر النظرية التنظيمية لهذا المجال الجديد، بدءًا من إعلان إنشاء سلطة للدفاع السيبراني في إسرائيل، أوكلت لها مهمة إدارة جميع الجهود الدفاعية والعملانية في الفضاء السيبراني وتشغيلها وتنفيذها وفق الحاجة إلى المستوى القومي، بما يتيح الرد الدفاعي الكامل والدائم على الهجمات السيبرانية؛ ومن ضمن ذلك التعامل مع تهديدات الفضاء السيبراني والحوادث السيبرانية في الوقت الحقيقي. في حين خُصّص القسم الثاني لعرض عقيدة القتال السيبراني ودورها في الحروب المقبلة، وتضمن أربع دراسات تتناول بالبحث تطور تكنولوجيا الحرب السيبرانية في بناء قوة إسرائيل وتطوير عقيدة للقتال السيبراني من أجل بلورة عقيدة متكاملة وناضجة. أما القسم الثالث، فتناول دراسة الدفاع السيبراني ومسألة الدفاع الإسرائيلي في عصر الحرب السيبرانية، مثل الهجمات التي تعرضت لها إسرائيل في عامي 2013 و2014، ومحاولتها تطوير نموذج جديد للدفاع السيبراني يرتكز على أربعة مبادئ أساسية في الدفاع: الردع والكشف والدفاع وإلحاق الهزيمة، إضافة إلى مفهوم القدرة على التعافي.

تُجمع الدراسات التي يتضمنها هذا الكتاب على أنّ استخدام السلاح السيبراني في المواجهات العسكرية لا يزال غير قادر على حسم هذه المواجهات على الرغم من أهميته المتزايدة، وعلى أن لهذا السلاح دورًا في مجال الدفاع عن المنظومات وعن شبكات المعلومات أكثر منه في المجال الهجومي.

لكن الحيّز السيبراني في إسرائيل لا يقتصر على الجيش والدولة، بل أصبح يكتسي أيضًا أهميةً كبرى في عمل الشركات السيبرانية الخاصة التي تعتبر من الشركات الرائدة في هذا المجال في العالم. فما دور الشركات السيبرانية الإسرائيلية الخاصة؟ وما علاقتها بالأجهزة السيبرانية الرسمية بالجيش الإسرائيلي؟ خصوصًا أن الأعوام الأخيرة شهدت تزايدًا مطّردًا في عدد الشركات السيبرانية الخاصة في إسرائيل التي تعمل في

4 لمزيد من المعلومات، انظر: موقع معهد دراسات الأمن القومي، في: https://bit.ly/2CYm9ZJ

مجال الأمن السيبراني من خلال إنتاج برامج حماية ودفاع عن أنظمة الكمبيوتر وشبكات المعلومات في المصارف والشركات الخاصة، حتى في المنشآت العامة. لكن النشاط الأهم لهذه الشركات هو إنتاجها برامج تجسسية هدفها المراقبة والرصد والتعقب، تبيعها لجميع دول العالم، وبخاصة لدول أفريقية وجنوب أميركية، ودول عربية، تستخدمها هذه الدول في ملاحقة المعارضين للنظام وفي التجسس عليهم.

القوة السيبرانية الإسرائيلية: القرارات والأطر التنظيمية

تقوم الاستراتيجية التكنولوجية الإسرائيلية على مفهوم أساسي، تجسد في ضرورة قيادة التطورات التي تحدث في المجتمع وتوجيهها والتحكم فيها، وتحقيق الاندماج الكلي الذي يحقق أهداف الدولة، خصوصًا أن نظام التعليم في إسرائيل يقوم على الربط بين العلوم النظرية والعلوم التطبيقية[5]. ويستدعي هذا الأمر تحديثًا وإنشاءً لعدد من الهياكل والمؤسسات لمواكبة التطورات التكنولوجية المتسارعة في مطلع القرن الحادي والعشرين التي باتت تؤثر مباشرة في الأمن القومي للدول. ذلك أن الفضاء السيبراني بات مصدر تهديدات حقيقية تشمل المؤسسات الحيوية في صلب العقيدة الدفاعية للدول؛ ما دفع رئيس الحكومة الإسرائيلية بنيامين نتنياهو، في 18 أيار/ مايو 2011، إلى إنشاء "هيئة السايبر الوطنية"، خصوصًا بعد أن أصبحت إسرائيل هدفًا لهجمات في الفضاء السيبراني. وقد تطلّب هذا الأمر تعزيز قدرات إسرائيل الدفاعية في هذا المجال؛ حيث بات كل ما هو محوسب عرضة للاختراق والهجوم، ما يهدد المرافق والمؤسسات الحيوية التي تقدم الخدمات الأساسية إلى المواطنين، مثل الكهرباء والمياه والاتصالات[6].

في هذا القسم من الكتاب، تناول شموئيل إيفين ودافيد سيمان الحوارات والنقاشات داخل مؤسسة الحكم في إسرائيل التي قادت إلى هيكلة سلطة الدفاع السيبراني القومية التي بدأت عملها في نيسان/ أبريل 2016. والوظيفة الأساس المنوطة بها هي إدارة الجهود الدفاعية والعملانية في الفضاء السيبراني، وتشغيلها وتنفيذها وفق الحاجة على المستوى القومي، وبناء مقاربة منهجية بما يتيح الرد الدفاعي الكامل والدائم على الهجمات السيبرانية في الوقت الملائم، وتقويم الوضع القائم وجمع المعلومات الاستخبارية وتدقيقها والعمل مع المؤسسات ذات الاختصاص؛ ويكون مدير هذه السلطة تابعًا لرئيس هيئة الأركان السيبرانية القومية الذي يُعرف بأنه رئيس عملية الفضاء السيبراني القومية (ص 27).

---

5 صفا محمود عبد العال، **التعليم العلمي التكنولوجي في إسرائيل**، ط 2 (القاهرة: الدار المصرية اللبنانية، 2004)، ص 261.

6 انظر: قراءة محمود محارب لكتاب شموئيل إيفين ودافيد سيمان طوف **حرب الفضاء الإلكتروني: تحديات على الصعيد العالمي والسياسي والتكنولوجي** (إسرائيل: معهد دراسات الأمن القومي، 2011)، في: محمود محارب، "إسرائيل والحرب الإلكترونية"، **مراجعات**، المركز العربي للأبحاث ودراسة السياسات، 2011/8/10، شوهد في 2019/3/31، في: https://bit.ly/2TLc5hg

إنّ المبدأ المنطقي الذي يحكم إنشاء السلطة، بحسب رأي الباحثين إيفين وسيمان، هو أنّ الدفاع السيبراني يستوجب التعاون الوثيق بين أجزاء القطاع المدني كلها؛ ومن ثمّ تبرز الحاجة إلى تأسيس هيئة مدنية تركز اهتمامها كلّيًا على الأمن السيبراني، تتولّى في المستقبل العمل الذي يقوم به في العادة جهاز الأمن الإسرائيلي للدفاع عن البنى التحتية القومية الحيوية. كما عرض الباحثان للخلافات التي رافقت تأسيس السلطة في ما يتعلق بتوزيع المسؤولية بين الهيئات المختلفة. وصيغت في 9 حزيران/ يونيو 2016 مذكرة تفاهم بين السلطة وجهاز الأمن الإسرائيلي بهدف تنظيم العمل، لكن التوتر بقي قائمًا، ومن المرجح أن يستمر في المستقبل.

على مستوى موازٍ، مرّ الجيش الإسرائيلي بتغيرات مفاهيمية وتنظيمية؛ إذ قرر رئيس هيئة الأركان الجنرال غادي إيزيكوت، في حزيران/ يونيو 2015، تأسيس فرع مستقل يقود نشاط الجيش الإسرائيلي، الدفاعي والهجومي، في الفضاء السيبراني. وفي مرحلة أولية، أسست شعبة "سيبر" جزءًا من هيئة الأركان العامة، وأنشئت فرقة دفاع في قسم الاتصالات اللاسلكية، وأجريت تغيرات تنظيمية في جهاز الاستخبارات.

في آب/ أغسطس 2016، أصدرت لجنة الشؤون الخارجية والدفاع في الكنيست تقريرًا بشأن توزيع المسؤولية وسلطة الدفاع السيبراني في إسرائيل. وعرض التقرير عمل لجنة فرعية خاصة بالدفاع الفضائي السيبراني يرأسها عضو الكنيست إفي ريختر، الرئيس السابق لجهاز الأمن الإسرائيلي. وهدف اللجنة الاطلاع على استعدادات الدولة للدفاع السيبراني والإشراف عليها، وتفحّص مغزى قرار الحكومة بشأن تأسيس السلطة وتنفيذ هذا القرار.

وفقًا لتقرير اللجنة، فإن إجراءات العمل، كما عرضت على اللجنة، تجعل من تبعية رئيس السلطة لرئيس عملية الفضاء السيبراني القومية أمرًا لا حاجة إليه في الممارسة العملية؛ لأنّ رئيس السلطة مستقل، يعمل في صميم التزامه المهني (الدفاع الفضائي السيبراني)، ويتخذ القرارات، ويقوم بإجراءات عملية على الأرض من دون الحاجة إلى تفويض من رئيس الدائرة. وإضافة إلى ذلك، لم تقتنع اللجنة بأن هناك ضرورة لوجود هيئتين مستقلتين في ديوان رئيس الحكومة، تتعامل كلتاهما مع الفضاء السيبراني. وتوصلت اللجنة إلى مجموعة من الاستنتاجات التي ترتبط بضرورة تحويل سلطة الدفاع السيبراني إلى وكالة أخرى لجمع المعلومات الاستخبارية؛ على اعتبار أنّ عملها يجب أن يستند إلى المعلومات التي تجمعها الهيئات الاستخبارية والبيانات المفتوحة. هذا مع ضرورة صوغ قانون "السيبر" بالتعاون مع جميع الأطراف ذات الصلة بالأنظمة الدفاعية والمدنية. وأن تخضع السلطة للقيود نفسها المفروضة على جهاز الأمن الإسرائيلي في ما يتعلق بالحقوق الفردية، والعمل على إعادة النظر في ترتيبات الأمن السيبراني بصفة دورية على مدى الأعوام الخمسة المقبلة؛ نظرًا إلى قوة التهديد وخبرة إسرائيل المحدودة نسبيًا على صعيد معالجة هذا التهديد.

غير أنّ التغيرات التنظيمية، مهما اتّصفت بالتعقيد، لا تشكل بالضرورة دليلًا على قدرات الدفاع عن الفضاء السيبراني، أو على تعزيز قوة هذا الدفاع. ولذلك يجب وضع المعايير والاختبارات العملية في ما له اتصال بقوة نظام الدفاع السيبراني، بما يتيح المجال لتقويم الوضع الحالي والقيمة المضافة إلى الفعل المستقبلي في الميدان.

عقيدة القتال السيبراني ودورها في الحروب المقبلة

يشمل هذا القسم أربعة أبحاث حول تطور تكنولوجيا الحرب السيبرانية وكيفية استخدام السلاح السيبراني في حروب إسرائيل المستقبلية. ففي بحثه "تطور تكنولوجيا الحرب السيبرانية في بناء القوة في إسرائيل"، حدّد جيل برعام الهدف من هذا البحث، في إظهار موقع تكنولوجيا الحرب السيبرانية في مفهوم الأمن القومي الإسرائيلي من خلال دراسة ثلاثة مجالات رئيسة: بلورة استراتيجية ملائمة لمواجهة التهديد الناجم عن تطور تكنولوجيا الحرب السيبرانية، وتخصيص الموارد والميزانيات المطلوبة، وإدخال تغييرات على بناء القوة العسكرية. وأشار برعام في بحثه إلى أنّ الركائز الثلاث لمفهوم الأمن القومي الإسرائيلي التقليدي لا تزال صالحة من أجل التصدي للتهديد السيبراني، وهي التالية:

- الردع: ذلك أنّ القدرات السيبرانية المتطورة تمكّن إسرائيل من ردع أعدائها.
- الإنذار المبكر: على اعتبار أنّ جمع إسرائيل معلومات عن أعدائها سيمنعهم في المستقبل من الوصول إلى قاعدة بياناتها.
- الحسم: تعتبر إسرائيل من الدول الرائدة من حيث قدراتها السيبرانية، وهو ما قد يمنحها تفوقًا في المعركة من خلال استخدام أدوات سيبرانية متقدمة لحسم المعركة.

أما في مجال الموارد والميزانيات، فنص قرار الحكومة الصادر في آب/ أغسطس 2016، المتعلق بإنشاء هيئة أركان سيبرانية قومية، على وجوب تخصيص اعتمادات محولة من وزارة المال عبر ديوان رئيس الحكومة. ويبرز برعام أنّ ميزانية هيئة الأركان السيبرانية تبلغ حاليًا 2.5 مليار شيكل، أي ما يعادل 1.2 مليار دولار أميركي، وهي موزعة على الأعوام الخمسة المقبلة، أي تبلغ 500 مليون شيكل سنويًا. مصدرها كالتالي: 100 مليون شيكل مرصودة من الميزانية العامة خصيصًا للهيئة، و400 مليون شيكل سيتم توفيرها من خلال تجميع للموارد من مصادر متعددة (ص 27).

يخلص برعام إلى أنّ إسرائيل أجادت استشراف خصائص التهديد الناجم عن تطور تكنولوجيا الحرب السيبرانية؛ فشرعت في إدخال التغيرات المطلوبة بناء على قوتها، على اعتبار الارتباط الوثيق بين طريقة معالجة التهديد السيبراني وأمن الدولة القومي، وارتكزت المعالجة على ثلاثة محاور:

- الأجهزة الأمنية والجيش ودوائر الاستخبارات والصناعة العسكرية والأمنية.
- الشبكات الوطنية الحساسة المعرضة لهجمات سيبرانية والخاضعة لتوجيهات "الهيئة الرسمية لحماية المعلومات".
- القطاع الخاص الذي يضم الشركات ومؤسسات مكشوفة أمام الهجمات السيبرانية.

في حين جادل رون تيرا، ضابط الاحتياط في الجيش الإسرائيلي، في بحثه "تطوير عقيدة للقتال السيبراني في المعركة التقليدية"، بأن المجال السيبراني يمر بسيرورة تطور تجعل منه نطاقًا جديدًا في القتال الذي تلجأ إليه الدولة على غرار الفروع القتالية الأخرى: البري والبحري والجوي أو الفضائي. وبناء عليه، يتطلّب ذلك تأسيس عقيدة عمل متكاملة وناضجة، تستمد، ولو جزئيًا، مكوّناتها من أنماط وتوجهات عسكرية شاملة، وتُدرج في المعركة التقليدية. ويرى أن القتال السيبراني يمر بمراحل تطور تكنولوجي أوّلية، يشبّهها بتطور الطيران العسكري، بظهور طائرة الاستكشاف الثنائية الجناح في الحرب العالمية الأولى، حيث اتضحت، منذ ذلك الوقت، القدرة الكامنة في الطيران على ضرب مراكز الثقل لدى العدو، فوق المنظومات الدفاعية الأرضية والمعطلات على الأرض.

يتسم الهجوم السيبراني اليوم وفي المستقبل المنظور بأفضلية كبيرة على المدافع ضد الهجوم السيبراني؛ ذلك أن على المدافع أن يدافع عن عدد أكبر من المنشآت والثروات، بدءًا بالخطط القتالية ومنظومات الأسلحة، مرورًا بمنظومات التحكم والمراقبة العسكرية، ومنظومات الاتصال العسكري، والبنى التحتية النظامية، والبنى التحتية الوطنية الحيوية. ويمتلك المهاجم أفضليتين: الأولى أنه يفرض على المدافع أن يدافع عن كل المؤسسات والمنشآت في حالة الهجوم السيبراني، والثانية أن في إمكان المهاجم تركيز جهده الهجومي على ما يختاره؛ وهو ما يتطلب حجمًا من القوى البشرية اللازمة للدفاع في المجال السيبراني أكبر من حجم القوى البشرية المطلوب للهجوم، على عكس القتال التقليدي.

وفي السياق ذاته، يتوصل إميليو إيزلو في بحثه "هل ثمة تأثير للسلاح السيبراني في الوسائل العسكرية التقليدية؟" إلى إجابة علمية وعملية عن هذا السؤال، من خلال سعي حكومات القوى الكبرى في النظام الدولي إلى تطوير قدراتها السيبرانية، سواء لتعزيز شبكة جمع معلوماتها الاستخبارية، أو لتكون أداة قوة سياسية. وتدل الكتابات الأكاديمية والعسكرية في ثلاث دول عظمى هي الولايات المتحدة الأميركية وروسيا والصين على دعم استخدام السلاح السيبراني في حالات وقوع مواجهات، خصوصًا ما يتعلق منها ببنى حساسة. ويرى إيزلو في بحثه أن الهجمات السيبرانية يمكن أن تكون سلاحًا مفيدًا يستخدم في الضربة الأولى، لأنها تتمتع بميزة المفاجأة وجهل المصدر، وذلك بسبب صعوبة عزو العملية إلى أي طرف. وفي المقابل، جرى في المواجهات التي تدخلت فيها قوة عسكرية استخدام الهجمات السيبرانية مرات معدودة من أجل تحقيق الهدف العسكري، سواء من حيث هي مكوّن مساعد أو مموّه. ليخلص إلى أنه

في المستقبل القريب سيكون السلاح السيبراني أشدّ ملاءمة للعمليات السرية، ولتمرير رسائل سياسية مما هو لحسم الحرب وتغيير قواعد اللعبة؛ ما يعني أنّ الوضع لن يتغير في المستقبل البعيد.

تناقش المقالة الأخيرة في هذا القسم التهديد الذي يمثله الإرهاب في الفضاء السيبراني، وتفحص حقيقة تصورات هذا التهديد التي تشكلت في الأعوام الأخيرة، كما تفحص القدرات التي يمكن أن تحققها جهة فاعلة غير حكومية، وما إذا كان يمكن هذه القدرات أن تمثّل تهديدًا حقيقيًا لأمن الدول القومي. وجاء هذا البحث بعنوان "التهديد الذي تمثله المنظمات الإرهابية في الفضاء السيبراني"، وخلص كتّابه، غابي سيبوني ودانيال كوهين وأفيف روتبات، إلى أنّ مفهوم الدفاع ضد التهديدات السيبرانية التي مصدرها جهات إرهابية يجب أن يقوم على عدد من العناصر: الاستخبارات ومقاربة الدفاع المتعدد الطبقات ومقاربة الهجوم والتوعية العامة والدفاع المدني.

الدفاع السيبراني والمواجهات المستقبلية

يبدأ القسم الثالث من الكتاب بتحليل لجيل برعام بعنوان "الدفاع الإسرائيلي في عصر الحرب السيبرانية - تحليل"، يعرض فيه لتطور مفهوم الأمن القومي للكيان الإسرائيلي في مواجهة التهديدات الكثيرة، خصوصًا أن مفهوم الأمن القومي يشير دائمًا إلى مصطلح الردع وتطوير قدرات دفاعية وهجومية تثبط عزيمة العدو. وتنظر إسرائيل إلى الردع على أنه تراكمي؛ لأنها تعتبر كل حرب حلقة واحدة في سلسلة حروبها . ثم ينتقل الباحث إلى مفهوم الأمن القومي في ظل الحرب السيبرانية، ذلك أن الدفاع الفاعل، بحسب رأيه، يضمن استمرار عمل الأنظمة الحيوية في بلد ما، وتطوير القدرات العملانية في الساحة السيبرانية لخدمة قوة إسرائيل. وقدم برعام طرحًا عن ضرورة دمج المتطلبات الثلاثة الأصلية الخاصة بمفهوم أمن إسرائيل التقليدي بالتحولات المتسارعة في مجال الحروب السيبرانية؛ وهي الردع والإنذار المبكر والانتصار العملاني الحاسم.

ويحاجج ماثيو كوهين وشاك فرايليخ وغابي سبيوني في مقالتهم، "نموذج جديد للدفاع السيبراني: مبادئ الردع والكشف والدفاع وإلحاق الهزيمة، مع القدرة على التعافي"، بأنّ التهديدات السيبرانية لا تختلف جوهريًا عن التهديدات الأخرى. ويقدم البحث أنموذجًا مفاهيميًا لتطوير استجابة بالاعتماد على المبادئ الأربعة الكلاسيكية للاستراتيجية العسكرية: الردع، والكشف المبكر، والدفاع، وإلحاق الهزيمة، إضافة إلى القدرة على التعافي. ويستنتج الباحثون أنّ الهجمات السيبرانية لا تختلف معالجتها عن معالجة التهديدات الأخرى، اعتمادًا على المبادئ التقليدية للاستراتيجية العسكرية.

في حين رسم أوري آورون في مقالته، "تأثير المجال السيبراني في تصميم المنظومات"، مساحات التماس المحتملة بين بيئة القتال السيبراني والتحديات الأمنية التي تواجه إسرائيل. وفي سبيل ذلك، حلل المجال السيبراني بصفته ساحة قتال تتكون من ثلاث بيئات: البيئة المادية التي توجد فيها منظومات وخوادم وخيوط وكابلات، أي كل ما هو ملموس؛ والبيئة البشرية التي تحدد متطلبات تنفيذ العمليات الحسابية وتستخدم نتائجها لأغراضها المنوعة؛ والبيئة الخوارزمية (اللوغاريتمية) التي يتم فيها توصيل الأرقام بعضها ببعض، فتجري العمليات الحسابية عمليًا. ويمكن وصف الفرق بين المجالين السيبراني والعسكري، بأنّ الأخير يستخدم، على المستوى المادي، الأدوات الحركية "العتاد الحربي المادي"، وعلى مستوى العنصر البشري، يصار إلى تفعيل أدوات علم النفس التي تؤثر في الوعي. أما المستوى الخوارزمي، فيستند إلى أدوات سيبرانية توثر في البيانات المخزّنة في أنظمة الكمبيوتر وفي الطريقة التي تجري بها برامج التشغيل حساباتها.

في السياق ذاته، يحاول إيتمار وايتان ونير واليشع في مقالتهما، "التكنولوجيا في ساحة القتال المستقبلي"، تلمس الفروق الجوهرية بين ساحة القتال المستقبلية المتصورة وساحة القتال الحالية؛ إذ يمثّل دور التكنولوجيا المتطورة التي سيتم استخدامها في المستقبل العامل الحاسم في تحديد شكل ساحات القتال المستقبلية. ويجادل الباحثان بأنّ النظم التكنولوجية الجديدة كالمعدات ذاتية القيادة، والأسلحة الكهرومغناطيسية، والمنظومات المتطورة في مجال القيادة والتحكم، ستعيد تشكيل الحرب المستقبلية ورسمها من جديد.

خاتمة

توظّف إسرائيل القوة السيبرانية في إجمالي قوتها الصلبة والناعمة في آن واحد، متفوقةً بذلك نوعيًا على مستوى دول المنطقة ككل. وتبلغ نسبة إنفاقها المحلي الإجمالي على البحث والتطوير بالنسبة إلى الناتج المحلي الإجمالي ما يعادل 4.21 في المئة من مجمل إنتاجها المحلي الإجمالي[7]، وهو أعلى بأضعاف مما تخصصه دول المنطقة العربية وسطيًا للبحث العلمي، حيث نسبة 0.3 في المئة فقط من الناتج المحلي الإجمالي (المُنتَقَص أصلا بفعل النظام التراكمي الريعي) هي مخصّصة للبحث والتطوير[8].

في الحصيلة، يتبيّن جليًا أنّ إسرائيل تعمل على استشراف التهديد المحدق ببناها التحتية نتيجة التهديدات السيبرانية، وفي تركيزها على إنشاء منظومة دفاع متطورة باستمرار على المستوى القطري، خصوصًا أنّ

7 Unesco, *Unesco Science Report: Towards 2030* (Paris: Unesco, 2015), p. 410.

8 Ibid., p. 27.

مفهوم الأمن القومي الإسرائيلي يعود إلى مرحلة تشكيل الوطن القومي اليهودي في ظل الانتداب البريطاني، وظلّ هذا المفهوم يتطور في مواجهة التهديدات الكثيرة التي كان على الكيان الاستعماري الوليد أن يعالجها بعد احتلاله فلسطين. كما أنّ إسرائيل تستخدم التكنولوجيا والقوة السيبرانية للتطبيع مع النظم الدكتاتورية في المنطقة، من خلال تصدير أجهزة التجسس والتنصت على المعارضين في الدول التي تعاني انعدام الحريات وغياب الديمقراطية والمحاسبة؛ ما يتسبب في اعتقالٍ وقتلٍ للمئات من الأبرياء، في مسعى منها للبقاء في محيط تمزّقه الحروب والصراعات الداخلية.