محمود محارب | *Mahmoud Muhareb

واقع وخطط "السايبر" والطائرات المسيّرة في إسرائيل

Reality and Plans of the Cyberspace in Israel

ملخص: تعالج هذه الدراسة واقع "السايبر" في إسرائيل، في المجالين المدني والعسكري، والرؤى والمقترحات الإسرائيلية لحمايته في الحاضر والمستقبل. وتستند في قراءتها لواقع السايبر في إسرائيل إلى العديد من الكتابات الإسرائيلية، وإلى ثلاث مذكرات صدرت عن معهد أبحاث الأمن القومي التابع لجامعة تل أبيب. وتعالج الحرب في مجال السايبر وتأثيرها في إسرائيل، ومسألة ضرورة تطوير استراتيجية إسرائيلية في مجال السايبر، وضرورة وضع تعليمات قانونية في مجال السايبر لحمايته وتنظيمه. كما تعالج واقع الطائرات المسيّرة العسكرية في إسرائيل، التي تعدّ من أهم ما توصلت إليه الصناعات الإسرائيلية الدقيقة، وتقف على إمكانية أن تصبح في السنوات والعقود القادمة ليس الأكثر استعمالًا في سلاح الجو الإسرائيلي في عملياته العسكرية فحسب، وإنما أيضًا القوة الأساسية في هذا السلاح.

كلمات مفتاحية: السايبر، الفضاء الإلكتروني، الطائرات المسيّرة، الجيش الإسرائيلي، حرب المستقبل.

Abstract: This study discusses civil and military uses of "Cyber" in Israel and Israeli proposals on how to protect it now and in the future. Its reading is based on numerous Israeli documents as well as three memoranda issued by Ben Gurion University's National Security Studies Institute. It discusses cyberwarfare and its effect on Israel and the necessity of developing an Israeli strategy in the cyber sphere as well as legal provisions to protect and regulate it. It also considers the reality of Israeli drone warfare, one of the most important achievements of Israeli precision engineering, assessing the possibility that it may become in coming decades not only Israel's most commonly used aerial weapon but the backbone of its air force.

Keywords: Cyber, Electronic Space, Drones, Israeli Army, Future War.

* باحث مشارك في المركز العربي للأبحاث ودراسة السياسات.

Associate researcher at the Arab Center for Research and Policy Studies.

مقدمة

الفضاء الإلكتروني، أو مجال "السايبر" Cyberspace[1]، هو مصطلح حديث، ظهر في العقود الأخيرة نتيجة لثورة تكنولوجيا المعلومات. ويشمل الفضاء الإلكتروني جميع الحواسيب والمعلومات التي بداخلها، والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة.

وتعدّ إسرائيل من أكثر الدول تقدمًا في التكنولوجيا الدقيقة وفي تكنولوجيا المعلومات. وقد باتت في العقدين الماضيين دولة "مُحوسبة"، تعتمد مؤسساتها الحكومية ومختلف مرافقها التابعة للقطاعين العام والخاص على شبكة الإنترنت. وأصبحت الغالبية العظمى من معاملات المواطنين في إسرائيل مع مؤسسات الدولة، والمرافق المختلفة فيها، تدار بواسطة الإنترنت. وكانت إسرائيل من أولى الدول التي اهتمت بإقامة شركات السايبر التي سرعان ما احتلت مكانة مهمة في شركات السايبر في العالم. فقد تبين وفق دراسة إحصائية أجرتها مجلة *Cyber Security Venture* عن أول 500 شركة تعمل في السنوات الأخيرة في مجال السايبر، أنّ عدد الشركات الأميركية يبلغ 354 شركة من بين أول 500 شركة في العالم، تليها الشركات الإسرائيلية ويبلغ عددها 42 شركة، ثم تليها الشركات البريطانية ويبلغ عددها 21 شركة، ثم يليها عدد من الشركات التابعة لدول أخرى. وتبيّن من هذه الدراسة أيضًا أنّ 40 شركة إسرائيلية مسجلة في الولايات المتحدة لاعتبارات ضريبية؛ أي أنّ عدد شركات السايبر الإسرائيلية الحقيقي الذي جاء في أول 500 شركة في العالم في مجال السايبر يبلغ 82 شركة، أي بنسبة 16.4 في المئة، وهذه نسبة مرتفعة بكل المعايير[2].

تعدّ إسرائيل مجال السايبر مركّبًا حيويًا في أمنها القومي. ويتعرض مجال السايبر في إسرائيل يوميًا لهجمات إلكترونية سايبرنية كثيرة ومتنوعة. وقد قدّر معهد أبحاث الأمن القومي، في إحدى دراساته، أنّ الأضرار الناجمة عن جرائم السايبر في إسرائيل تصل إلى نحو عشرة مليارات دولار في السنة. ويشمل ذلك عدة مليارات من الدولارات الناجمة عن سرقة معلومات من شركات صناعية وتجارية[3].

---

1 يعرّف الاتحاد الدولي للاتصالات التابع للأمم المتحدة ITU "الفضاء الإلكتروني" بأنه: "المجال المادي وغير المادي الذي أنشأته و/ أو يتألف من بعض أو كل ما يلي: أجهزة الكمبيوتر، وأنظمة الكمبيوتر، والشبكات وبرامج الكمبيوتر الخاصة بها، وبيانات الكمبيوتر، وبيانات المحتوى، وبيانات المرور، والمستخدمون"، يُنظر:

International Telecommunication Union, *ITU Toolkit for Cybercrime Legislation, Draft Rev.* (Geneva: International Telecommunication Union, 2010).

2 يغآل أونا، "الدفاع عن السايبر الوطني"، مجلة **سايبر ومخابرات وأمن**، مج 3، العدد 1 (أيار/ مايو 2019). (بالعبرية)

3 أفنير سمحوني، "معركة في السايبر أو سايبر في المعركة"، مجلة **سايبر ومخابرات وأمن**، مج 1، العدد 3 (كانون الأول/ ديسمبر 2017). (بالعبرية)

وقد تعاظم في العقد الأخير اهتمام الحكومة الإسرائيلية والمؤسسة الأمنية ومراكز الأبحاث والأكاديميا الإسرائيلية بالسايبر وبعلاقته بالأمن القومي الإسرائيلي؛ وتميّز معهد أبحاث الأمن القومي التابع لجامعة تل أبيب باهتمامه بهذا الموضوع. فقد نظّم هذا المعهد في العقد الأخير العديد من الأيام الدراسية عن السايبر، وعن مدى أهميته لإسرائيل، وعن علاقته بأمنها القومي. وأصدر هذا المعهد في العقد الأخير عدة مذكرات، أعدّها باحثون يعملون فيه، عالجت موضوع السايبر في إسرائيل من جوانبه المختلفة: المذكرة الأولى للباحثين، شموئيل إيفن ودافيد بن سيمان - طوف، وعنوانها **حرب الفضاء الإلكتروني: اتجاهات وتأثيرات في إسرائيل** (2011)[4]، أما الثانية فألفها الباحثان، غابي سيبوني وعوفر أساف، وجاءت بعنوان **خطوط توجيهية لاستراتيجية وطنية في مجال السايبر** (2015)[5]، وكانت الثالثة من إعداد الباحثين، غابي سيبوني وعيدو سيفان – سبيليا، وعنوانها **تعليمات في مجال السايبر** (2018)[6].

إلى جانب ذلك، أسّس هذا المعهد في السنوات الأخيرة "برنامج بحث أمن السايبر"، لما يكتسيه هذا الموضوع من أهمية بالنسبة إلى إسرائيل وأمنها القومي. وفي سنة 2017، بدأ هذا المعهد في إصدار مجلة دورية مختصة في السايبر تصدر ثلاث مرات في السنة، عنوانها: **سايبر ومخابرات وأمن**، ويرأس تحريرها غابي سيبوني رئيس برنامج "بحث أمن السايبر" في المعهد. وتعالج هذه المجلة، وفق ما جاء في مقدمة عددها الأول، جملةً واسعة من المواضيع ذات العلاقة بالسايبر والمخابرات والأمن، من بينها السايبر على الصعيد الدولي، واستراتيجية الدول تجاه السايبر، والتعليمات والقوانين في مجال السايبر، وحماية المناعة الوطنية في مجال السايبر، والدفاع عن البنى التحتية الحيوية، وبناء القوة في مجال السايبر بمركباتها المختلفة: الطاقات البشرية، ووسائل القتال، والعقيدة القتالية، والتنظيم والتدريب، والقيادة، وحرب السايبر الدفاعية والهجومية.

إلى جانب ذلك، أقام "تجمع السايبر الوطني" في إسرائيل، بالتعاون مع الجامعات الإسرائيلية ستة مراكز أبحاث أكاديمية في مجال السايبر، وذلك في سياق تعزيز التعاون بين الدولة والأكاديميا والصناعات في إسرائيل، ذلك أن إسرائيل إن لم تستثمر في الطاقات البشرية وفي الصناعة، فإنها لن تتمكن من الحفاظ على التميّز والتفوق في مجال السايبر[7].

---

4 شموئيل إيفن ودافيد بن سيمان - طوف، **حرب الفضاء الإلكتروني: اتجاهات وتأثيرات في إسرائيل** (تل أبيب: معهد أبحاث الأمن القومي، 2011). (بالعبرية)

5 غابي سيبوني وعوفر أساف، **خطوط توجيهية لاستراتيجية وطنية في مجال السايبر** (تل أبيب: معهد أبحاث الأمن القومي، 2015). (بالعبرية)

6 غابي سيبوني وعيدو سيفان - سبيليا، **تعليمات في مجال السايبر** (تل أبيب: معهد أبحاث الأمن القومي، 2018). (بالعبرية).

7 أونا.

أولًا: واقع السايبر في إسرائيل

الحرب في مجال السايبر

أشار مؤلفا مذكرة **حرب الفضاء الإلكتروني: اتجاهات وتأثيرات في إسرائيل**[8]، والتي جاءت في أربعة فصول وخاتمة، إلى أنّ مجال السايبر بات مجال قتال جديد، وانضم بذلك إلى مجالات القتال الأخرى، في اليابسة والبحر والجو والفضاء. فالدول المتطورة وجيوشها تزيد من نشاطاتها وأبحاثها في مجال السايبر الذي أصبح يمثّل بالنسبة إليها مصدر قوة عظيمة، ولكنه في الوقت نفسه يكشف خاصرتها الضعيفة؛ لأنّ البنى التحتية التي تقوم عليها الدول الحديثة مثل الكهرباء والمياه والمواصلات والاتصالات والبورصة والبنوك تعتمد في عملها على مجال السايبر. وتعتمد عليه كذلك شبكات القيادة والسيطرة والتحكم العسكرية ومختلف أنواع التكنولوجيا المتطورة في ساحات القتال، مثل أنظمة المعلومات واستعمال الأقمار الصناعية والطائرات من دون طيار. ونوّه إيفن وبن سيمان - طوف بميزات مجال السايبر بصفته مجال 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 مجال السايبر تجعله جذابًا للاستعمال في القتال خلال الحرب بالأسلحة التقليدية، مثلما فعلت روسيا، كما يقول المؤلفان، في حربها ضد جورجيا في سنة 2008. ويضيف المؤلفان أنه يمكن استخدام السايبر ضد أهداف استراتيجية، مثل الهجوم الذي شنّته إسرائيل، وفق العديد من المصادر، على المفاعل النووي الإيراني في سنة 2009، والذي يعدّه المؤلفان حدثًا تأسيسيًا في مجال حرب السايبر، ومرحلةً جديدة في تطور استعمال السايبر في مجال القتال[9].

كما اعتبر المؤلفان أنّ استعمال السايبر في القتال، إلى جانب عمليات التطوير والاستعدادات للقتال في مجال السايبر التي قامت وتقوم بها العديد من الدول، يؤكد أنّ سباق التسلح في السايبر قد بدأ فعلًا. وأشارا إلى أنّ العديد من الدول أقامت في السنوات الأخيرة مؤسسات وهيئات متعددة ومختصة باستعمال السايبر بوصفه مجال قتال، وطورت استراتيجيات أمنية في السايبر[10].

السايبر في استراتيجية الأمن الإسرائيلي

يؤكّد إيفن وبن سيمان - طوف أنّ إضافة مجال السايبر، بصفته ساحة قتال جديدة، إلى جانب ساحات القتال في البر والبحر والجو والفضاء، تستوجب دمج الحرب في مجال السايبر في استراتيجية ومفهوم

8 إيفن وبن سيمان - طوف.

9 المرجع نفسه.

10 المرجع نفسه.

الأمن الإسرائيلي؛ وهو ما يستدعي استحداث تغييرات في مفاهيم المصطلحات الأساسية المتعلقة بنظرية الأمن الإسرائيلي[11]. فمثلًا تختلف "البيئة الاستراتيجية" في مجال السايبر عن المفهوم التقليدي لها في نظرية الأمن الإسرائيلي القائم على التهديدات الجيوستراتيجية التقليدية. علاوةً على ذلك، يختلف الزمان والمسافة والمساحة في مجال السايبر عن المفاهيم التقليدية؛ لأن سرعة العملية الهجومية في مجال السايبر، ضد هدف يبعد مئات أو آلاف الأميال، تبلغ واحدًا على الألف من الثانية. ويرى المؤلفان أنه من الصعب للغاية أن تقوم إسرائيل بتطبيق سياسة الردع التي تعتبر حجر الزاوية في الاستراتيجية الإسرائيلية، في الحرب في مجال السايبر، لصعوبة تحديد هوية الطرف المهاجم في الحرب في هذا المجال.

ويرى المؤلفان أن الدفاع في الحرب في مجال السايبر يُعتبر تحدّيًا من نوع جديد لإسرائيل؛ وذلك أن العدو بمقدوره شن هجمات بسرعة البرق، ومن الصعوبة القصوى تحديد هوية المهاجم. ويوصي المؤلفان بأن تتعلم إسرائيل وتستفيد من مفهوم "الدفاع الفعال" في مجال السايبر الذي تتبعه الولايات المتحدة[12]؛ إذ يستند هذا المفهوم إلى قدرة مخابراتية متطورة لتحديد النشاطات في الإنترنت، وإلى أنظمة دفاع دينامية ذات رد تلقائي من دون تدخل الإنسان. ويستطرد المؤلفان قائلَين إن "الدفاع الفعال" لا يعتمد على التكنولوجيا المتطورة فحسب، وإنما على شبكة محكمة ذات قواعد وإجراءات صارمة، وثقافة تفهم المخاطر، وانضباط شديد، وحماية المواقع، ورقابة بشرية قوية. ويوصي المؤلفان، في ضوء اعتراف الجيش الإسرائيلي بمجال السايبر كساحة قتال إلى جانب الساحات الأخرى، بإجراء تغييرات في قوات الجيش الإسرائيلي والعمل على إقامة سلاح خاص بمجال السايبر، أسوةً بالأسلحة البرية والبحرية والجوية[13].

بداية تدابير إسرائيل للدفاع عن مجال السايبر

ذكر إيفن وبن سيمان - طوف، في مذكرتهما، أنّ إسرائيل اتخذت مجموعة من التدابير للدفاع عن مجال السايبر خلال العقدين الأخيرين من أجل حمايته والدفاع عنه[14]. في سنة 1997، أقامت إسرائيل مشروع "بنية الحكومة التحتية لعصر الإنترنت" في وزارة المالية الإسرائيلية. وأقيم في هذا المشروع "مركز حماية المعلومات لحكومة إسرائيل"، وأنيطت به مهمات متابعة تطور وسائل حماية المعلومات في العالم والتنسيق بين الوزارات والمؤسسات الحكومية، من أجل إيجاد حلول لمشكلات حماية المعلومات وكذلك إجراء أبحاث عن هذا الموضوع. وفي سنة 2002، أنشئت "السلطة الرسمية لحماية المعلومات" في جهاز المخابرات العامة الإسرائيلية (الشاباك)، وأنيط بها مهمات حماية البنى التحتية

11 المرجع نفسه.
12 المرجع نفسه.
13 المرجع نفسه.
14 المرجع نفسه.

للحواسيب الحيوية والمهمة في إسرائيل من مخاطر ما أطلق عليه "تهديدات إرهابية"، و"عمليات تخريب"، ونشاطات تجسسية.

وجرى الاتفاق على أن يتم تحديد المؤسسات المهمة والحيوية الخاضعة للحماية، من خلال لجنة مشتركة بين جهاز الشاباك وهيئة الأمن القومي الإسرائيلي. وفي آذار/ مارس 2011، صدّقت الحكومة الإسرائيلية على إقامة "وحدة إدارة المعلومات"، تتبع مدير وزارة المالية الإسرائيلية، وتكون مسؤولة - مسؤولية مباشرة - عن جميع أنظمة الاتصالات المحوسبة الحكومية، بما في ذلك مشروع "بنية الحكومة التحتية لعصر الإنترنت". وفي أيار/ مايو 2011، أعلن رئيس الحكومة الإسرائيلية بنيامين نتنياهو عن إنشاء "هيئة السايبر الوطنية" في ديوان رئيس الحكومة، بناءً على توصية مجموعة من الخبراء من قطاعات ووزارات مختلفة. وذكر نتنياهو أن الهدف الأساسي لهذه الهيئة هو تعزيز قدرات إسرائيل الدفاعية عن أنظمة البنى التحتية الحيوية تجاه "هجمات إرهابية" في مجال السايبر قد تقوم بها دول أجنبية أو "منظمات إرهابية". وأضاف أن إسرائيل مكشوفة لهجمات في مجال السايبر، فكل ما هو محوسب قد يتعرض للهجمات في هذا المجال، التي قد تشل أنظمة مرافق ومؤسسات حيوية للغاية تشغل الدولة مثل: الكهرباء والمياه والاتصالات والمواصلات.

كما أشار سيبوني وسيفان - سبيليا إلى أنّ الحكومة الإسرائيلية أقامت في سنة 2015 "السلطة الوطنية للدفاع عن السايبر" في ديوان رئيس الحكومة، من أجل الدفاع عن مجال السايبر في البنى التحتية والمرافق الحيوية في إسرائيل، والحفاظ على استمرار عملها بانتظام في حال تعرضها لهجمات سايبر معادية. وفي بداية سنة 2018، جرى توحيد "السلطة الوطنية للدفاع عن السايبر" و"هيئة السايبر الوطنية"، ليشكّلا سويةً مؤسّسةً واحدة أطلق عليها "تجمع السايبر الوطني"، وتقرر أن تكون تابعةً لديوان رئيس الحكومة[15].

واقترح إيفن وبن سيمان - طوف أن تتبنّى الحكومة الإسرائيلية استراتيجية وطنية للدفاع عن مجال السايبر في إسرائيل، وفق النقاط التالية:

- الاعتراف بمجال السايبر، بوصفه مجالًا وطنيًا جديدًا (إلى جانب مجالات البر والبحر والجو)، ينبغي حمايته والدفاع عنه من خلال رؤية شاملة وتعاون جميع الأطراف ذات الصلة.
- تأسيس مؤسسة وقيادة مركزية للدفاع عن مجال السايبر في إسرائيل على المستوى الوطني.
- وضع البنى التحتية الحيوية وأنظمة الأمن في قمة الأولويات التي ينبغي حمايتها، وفي الوقت نفسه القيام بمهمة الدفاع عن مركبات أخرى، مثل الدفاع عن المعلومات في الجامعات ومراكز

15 سيبوني وسيفان - سبيليا.

الأبحاث وعن الشركات المهمة التي لها تأثير في الاقتصاد الإسرائيلي ولكنها ليست مصنفة جزءًا من البنى التحتية الحيوية.

- بناء نظام دفاعي وشامل في مجال السايبر، مثل النظام الذي أقامته وزارة الدفاع الأميركية.
- التعاون الدائم في مجال السايبر بين القطاع الحكومي والقطاع الأمني والقطاع الخاص.
- التعاون مع دول أجنبية بشأن السايبر، وخاصة الدول الحليفة.
- سن قوانين في مجال السايبر وتطبيقها على أرض الواقع.
- مساعدة الجمهور العام في زيادة الوعي بالسايبر، وتطوير قدراته على الدفاع في هذا المجال، ومنح الشركات والأفراد محفزات لشراء برامج دفاع، وزيادة الرقابة على شركات الحماية.
- استعمال الوسائل والأجهزة التكنولوجية الأكثر تطورًا المتعلقة بالفضاء الإلكتروني.
- بلورة وتطوير سياسة ردع إسرائيلية، بما في ذلك قدرة الرد المباشر ضد من يهاجم مجال السايبر الإسرائيلي وإلحاق الأذى به، وهذا الأمر من مهمات المؤسسة الأمنية الإسرائيلية.

معالم الاستراتيجية الوطنية في مجال السايبر

أشار سيبوني وأساف، في مذكرتهما **خطوط توجيهية لاستراتيجية وطنية**، إلى وجود مركبين أساسيين في مجال السايبر وهما الدفاع والهجوم، ودعوَا إسرائيل إلى تبني استراتيجية الدفاع والهجوم في مجال السايبر، وأن تُعدّ الأرضية وكل ما يتطلب لتنفيذ هذه الاستراتيجية[16]. وقسم المؤلفان المؤسسات والمرافق في إسرائيل التي ينبغي الدفاع عنها في مجال السايبر إلى أربعة أقسام:

- المؤسسات العسكرية والأمنية التي تدافع عن الدولة.
- المرافق والمؤسسات التي تقدم خدمات حيوية.
- المرافق والمؤسسات التي لها الدور الأساسي في انتظام الحياة في الدولة على نحو سليم.
- المؤسسات التي إذا ما هوجمت وتضررت، كان لذلك تأثير في معنويات الشعب، وفي السيادة، وفي انتظام الحكم[17].

كما أكد المؤلفان أنّ جميع المرافق والمؤسسات المذكورة سابقًا معرضة للتهديد من أطراف؛ منها دول معادية، ودول منافسة، ومنظمات "إرهاب"، وقراصنة (الهاكرز). وإلى جانب ذلك، ذكر المؤلفان أنّ مجال

16 سيبوني وأساف.

17 المرجع نفسه.

السايبر في إسرائيل يتعرض لجرائم جنائية مختلفة؛ مثل التجسس على الشركات، وسرقة الملكية الروحية، واستعمال مجال السايبر في الاتجار بالمخدرات وبيع السلاح ... إلخ[18].

أكد المؤلفان أنّ الهدف المركزي في استراتيجية الدفاع الوطني، في مجال السايبر، هو الحفاظ على استمرار عمل جميع المرافق والمؤسسات في الدولة عند تعرضها لهجمات معادية في مجال السايبر من أي طرف. وأشارا كذلك إلى هدف آخر مهم في استراتيجية الدفاع الوطني يتمثّل في تمكين متخذي القرار في إسرائيل من اتخاذ القرارات والقيام بعمليات في مجال السايبر وفي مجال الحرب التقليدية ضد أعداء، من منطلق أن إسرائيل تستطيع الدفاع عن مرافقها المختلفة، إذا ما تعرضت هذه المرافق لهجوم في مجال السايبر ردًا على الهجوم الإسرائيلي[19].

وميّز المؤلفان في معالجتهما لاستراتيجية الدفاع بين ثلاثة أنواع هجومية:

- هجوم عمق، يهدف إلى الوصول إلى عمق حواسيب المؤسسات والمرافق.
- هجوم سريع وسطحي، تظهر نتائجه فورًا، ويهدف عادة إلى منع أو عرقلة الوصول إلى الموقع الذي تتم مهاجمته.
- هجوم على المركبات الفيزيائية في الحواسيب. وأوصى المؤلفان باتخاذ الإجراءات التالية للدفاع ضد مختلف أنواع الهجمات:

- التنسيق بين الطاقات الإسرائيلية المختلفة في مجال السايبر، وإعداد الطواقم المهنية التي تمتلك الخبرة بوسائل الهجمات لبناء بنية تحتية للدفاع ضد الهجمات.
- التواصل بين المؤسسات والمرافق الإسرائيلية المختلفة باستمرار وبشفافية بشأن هجمات السايبر التي تتعرض لها.
- إقامة مؤسسة لتقدير حالة السايبر في إسرائيل والاعتداءات التي تتم ضده، على مدار الساعة.
- إقامة هيئات مختصة للرد السريع على أي هجوم، من خلال استعمال المعلومات المتوافرة عن الأطراف والمجموعات التي تشن الهجوم.
- التعاون مع منظمات دفاع في القطاع التجاري، وكذلك مع المؤسسات الدولية المختصة بالسايبر.
- تطوير جمع المعلومات باستمرار عن أعداء وخصوم، من أجل ردعهم والتصدي لهم.
- بلورة ووضع خطط للرد الفوري ضد أعداء محتملين في إطار استراتيجية الردع.

---

18 المرجع نفسه.

19 المرجع نفسه.

- تطوير القدرة للانتعاش بعد التعرض لهجوم، من منطلق أنه مهما كانت احتياطات الدفاع في مجال السايبر، فإنه في الإمكان اختراق هذه الدفاعات. لذلك ينبغي أن تكون الجاهزية دومًا عالية، من أجل ترميم الأضرار بعد الهجمات المعادية والحفاظ على عمل المرافق والمؤسسات التي تتعرض لها.
- من الأفضل استعمال خطوط خدمات الإنترنت العريضة التي يكون بمقدورها التغلب على محاولات إغلاقها، أو عرقلة عملها، عند تعرضها للهجمات السطحية السريعة.
- من المهم التمتع بالقدرة على نقل المواقع التي تتعرض لهجوم إلى مواقع أخرى بديلة في الإنترنت.
- من الضروري تطوير القدرة في إسرائيل على التعرف إلى الهجمات التي تستهدف المركبات الفيزيائية للحاسوب، ومن المهم استعمال مركبات الحواسيب من إنتاج الصناعات الإسرائيلية التي يصعب إلحاق الأذى بها[20].

كما أكد المؤلفان أنّ القطاع المدني هو الأكثر عرضة للاعتداءات في مجال السايبر؛ لذلك دعوَا إلى إلزام الشركات، عند إنشائها أو عند تجديد ترخيصها، باتخاذ التدابير الضرورية من أجل الدفاع عن السايبر فيها، وجعله شرطًا لمنحها الترخيص بالعمل أو تجديده[21].

وفي ما يخص الهجوم في مجال السايبر، ميّز المؤلفان بين ثلاثة أنواع هجومية:

- هجوم علني.
- هجوم لإيصال رسالة.
- هجوم في سياق معركة سرية.

وأوصيا بالقيام بالخطوات التالية:

- ينبغي أن تقوم مختلف المؤسسات العسكرية والأمنية الإسرائيلية بالتنسيق التام في ما بينها في مجال السايبر، وتحضير كل ما هو ضروري، والبقاء دومًا على أهبة الاستعداد، لشنّ هجمات في مجال السايبر على الأعداء المحتملين.
- يجب أن تكون القدرة الهجومية في مجال السايبر جزءًا من خطة شاملة، كي يكون لها تأثير في المواجهة الشاملة.
- ليس بالضرورة أن يكون الهجوم الناجح والمؤثر جزءًا من هجوم عمق متطور. ومن المفضل تطوير القدرات على شن هجوم فعال ومركز بواسطة هجوم سطحي وسريع وواسع على أهداف متعددة.

---

20 المرجع نفسه.

21 المرجع نفسه.

- من المهم الاستعداد للقيام بشن هجوم في مجال السايبر ضد أعداء محتملين بواسطة "وسيط" Proxy مجهول ومن دون الإعلان عن المسؤولية.
- من أجل شن هجوم واسع وشامل ومؤثر في مجال السايبر، يجب بناء القوة اللازمة لذلك، ومعرفة الهدف بدقة، والتخطيط المسبق.
- في إمكان الهجوم في مجال السايبر أن يكون جزءًا من الحوار بين الدول، حيث يكون هدف الهجوم هو إيصال رسالة.
- من المفضل إدخال "مهاجمين" محترفين وذوي خبرة بالهجوم في الدفاع عن السايبر في إسرائيل[22].

تعليمات في مجال السايبر

ودعا سيبوني وسيفان - سبيليا في **تعليمات في مجال السايبر** الذي صدر في سنة 2018، إلى تنظيم مجال السايبر في إسرائيل، وإلى وضع تعليمات واضحة وشاملة بشأنه. وأكد المؤلفان أن مجال السايبر مركّب ومهم للغاية وديناميّ باستمرار، وأن قسمًا كبيرًا منه يستند إلى قطاع الأعمال المدني الذي تكمن فيه إمكانية التسبب بأذى شديد للأمن القومي الإسرائيلي. فهذا القطاع هو الحلقة الأضعف التي يتم من خلالها مهاجمة سايبر الدولة[23].

وقسّم المؤلفان المخاطر التي تهدد مجال السايبر في إسرائيل، ووضع حمايتها والجهة المسؤولة عنه، إلى ست مجموعات، كالتالي:

- المؤسسات التي تراقب وتحمي نفسها ذاتيًا، وهي المؤسسات الأمنية مثل جهاز المخابرات العامة (الشاباك) والموساد والجيش الإسرائيلي بمؤسساته المختلفة والشرطة. وتتخذ هذه المؤسسات الاحتياطات الضرورية لحماية نفسها من دون تدخل أي مؤسسة خارجية.
- المنشآت الحيوية الحساسة ومختلف الصناعات العسكرية، وهي تخضع لإشراف ومراقبة المسؤول عن الأمن في وزارة الأمن الإسرائيلية، ومهمته هي إصدار التوجيهات لحمايتها من هجمات سايبر معادية والحفاظ على سرية المعلومات التي بداخلها.
- البنى التحتية الحيوية في إسرائيل، وهي تخضع لإشراف شامل مشترك مكون من "تجمع السايبر الوطني" وجهاز المخابرات العامة. وتشمل البنى التحتية الحيوية مؤسسات وقطاعات كثيرة مثل قطاعات الغاز والطاقة والكهرباء والمياه والمواصلات والاتصالات والصحة والمطارات والموانئ ومؤسسة التأمين الوطني وغيرها. وتقوم لجنة مشتركة من "تجمع السايبر الوطني"

22 المرجع نفسه.

23 سيبوني وسيفان - سبيليا.

والمخابرات العامة بتحديد المؤسسات التي ينبغي أن تخضع لرقابتهما المشتركة وفق تقديرهما لخطورة الضرر الذي قد يتسبب، إذا ما تعرضت هذه المؤسسة أو تلك لهجمات سايبر معادية، في إيذاء انتظام الحياة على نحو عادي في إسرائيل.

- الوزارات الإسرائيلية بأجهزتها المختلفة، ويشرف "تجمع تكنولوجيا المعلومات والاتصالات الحكومي" على عملية الدفاع عن مجال السايبر فيها.
- قطاع الأعمال، وغالبيته العظمى، غير خاضعة لتعليمات بشأن الدفاع عن مجال السايبر فيها، باستثناء الرقابة على البنوك وسوق المال ومصانع الطاقة ومؤسسات الصحة.
- المواطنون، وهم غير خاضعين لتعليمات بشأن الدفاع عن السايبر.

إلى جانب ذلك، ذكر المؤلفان أنه صدرت في إسرائيل ست مبادرات وتوجيهات في ما يخص مجال السايبر، هي:

- زيادة الرقابة على الصادرات الإسرائيلية الأمنية، وزيادة عدد المنتجات العسكرية التي يتم وضعها تحت رقابة الدولة، بهدف الحفاظ على تفوق إسرائيل النسبي، ولا سيما في مجال صناعات السايبر الهجومية ومنتجاته. بيد أن المؤلفين ذكرا أن إسرائيل عادت وخففت من وطأة الرقابة على بعض منتجات السايبر، وسعت إلى إيجاد حل وسط بين الحفاظ على تفوق إسرائيل النسبي في مجال صناعات السايبر من ناحية، والحفاظ على قوة المنافسة والتصدير لشركات السايبر الإسرائيلية من ناحية أخرى.
- نشرت "هيئة السايبر الوطنية" في كانون الأول/ ديسمبر 2015، وثيقة سعت فيها إلى تطوير وبلورة الطاقات البشرية الإسرائيلية في مجال السايبر، من أجل ترقية عملية حماية السايبر في إسرائيل والدفاع عنه. وحددت هذه الوثيقة المستوى المهني المطلوب من الطاقات البشرية التي تعمل في مجالات السايبر المختلفة في إسرائيل. ورأت الوثيقة ضرورة رفع المستوى المهني للعاملين في السايبر، بواسطة تعليم مواضيع السايبر ومنح القوى العاملة فيه شهادات علمية، بعد تلقيهم الدراسة والتدريب في مجالات السايبر المختلفة.
- صدّقت وزيرة القضاء في سنة 2017 على تعليمات جديدة ملزمة، بشأن مخازن المعلومات وفق حساسية المعلومات. فكلما كانت حساسية المعلومات مرتفعة، كان ثمة تشديد في الالتزام بتعليمات صارمة في أنظمة حمايتها.
- نشر "تجمع السايبر الوطني" في نيسان/ أبريل 2017 وثيقة "نظرية الدفاع في مجال السايبر عن المؤسسة". وهذه الوثيقة موجهة إلى قطاع الأعمال المدني، وهي تزوده بطرق حماية المؤسسات

وأدواتها، وكيفية تخفيض المخاطر في مجال السايبر في القطاع المدني أساسًا، وذلك لرفع مناعة مؤسسات هذا القطاع.

- نشر "تجمع السايبر الوطني" في سنة 2017 وثيقة "الاستراتيجية الإسرائيلية للدفاع في مجال السايبر"، وهي المرة الأولى التي يتم فيها نشر وثيقة شاملة تعالج بالتفصيل كيفية الدفاع عن مجال السايبر في إسرائيل.
- بادر "تجمع السايبر الوطني" إلى وضع مسوّدة "قانون السايبر" من أجل سَنّه في الكنيست. وتنظم مسوّدة هذا القانون صلاحيات "تجمع السايبر الوطني" الحكومي، وتضع تحت مسؤوليته كل ما يتعلق بالدفاع عن السايبر في إسرائيل. وتعالج مسوّدة القانون مسألة تحديد المؤسسات التي يجب أن تخضع لتعليمات ملزمة في ما يخص احتياطات حماية مجال السايبر فيها. وتقسم المسوّدة المؤسسات في إسرائيل إلى ثلاث مجموعات، وتضم المجموعة الأولى نحو ألف مؤسسة حيوية وحساسة ينبغي أن تكون مهمة الدفاع عنها في يد الدولة، من بين الـ 600 ألف مؤسسة في إسرائيل. أما باقي المؤسسات فتقسم إلى مجموعة ثانية ومجموعة ثالثة، ويتم الحفاظ في هاتين المجموعتين على التعليمات القائمة تجاهها ولكن يتم منحها محفزات لكي تقوم هذه المؤسسات نفسها بوضع الاحتياطات اللازمة لحمايتها[24].

وتمنح مسوّدة القانون "تجمع السايبر الوطني" حق الدخول إلى جميع الحواسيب في إسرائيل، الخاصة والعامة، وأن يأخذ منها ما يشاء من الوثائق والمعلومات، من دون رقابة قانونية ومن دون علم أصحاب الحواسيب التي تؤخذ منها المعلومات. وقد أقر الكنيست مسوّدة هذا القانون في القراءة الأولى في حزيران/ يونيو 2017. وقد أثار طرح هذا القانون في الكنيست معارضة واسعة من جهات مختلفة في إسرائيل، بسبب منح "تجمع السايبر الوطني" صلاحيات واسعة للغاية ولاختراقه الخصوصية الفردية. وإلى جانب ذلك، ثمة خشية قائمة من مسألة سوء استعمال المعلومات التي يجمعها "تجمع السايبر الوطني" التابع رسميًا لديوان رئيس الحكومة، لأغراض سياسية حزبية داخلية، تحت غطاء ذرائع أمنية.

واقترح المؤلفان سيبوني وسيفان - سبيليا تنظيم مجال حماية السايبر في مختلف المؤسسات في إسرائيل. وقسّما هذه المؤسسات إلى ثلاثة أقسام، تخضع لثلاثة أنواع مختلفة من التعليمات، كالتالي:

- تعليمات ذاتية داخلية: ويشمل هذا النوع المؤسسات العسكرية والأمنية، مثل الجيش والمخابرات العامة والموساد والشرطة. وهذه المؤسسات تخضع لتعليمات ذاتية داخلية من أجل حماية مجال السايبر فيها.

---

24 المرجع نفسه.

- تعليمات ملزمة: تفرض الدولة تعليمات ملزمة من الجهات المختصة لحماية مجال السايبر في مختلف المرافق والمؤسسات المهمة والحيوية؛ مثل الصناعات العسكرية التابعة للقطاعين الخاص والعام، ومختلف قطاعات المواصلات والاتصالات والطاقة والمياه والصحة والموانئ والمطارات والبنوك والبورصة، وجميع المرافق الأخرى التي قد يؤدي مجال السايبر فيها، إذا ما تعرض لضرر، إلى تشويش سير الحياة الطبيعية في إسرائيل.
- تعليمات تقوم على التحفيز: تصدر الدولة تعليمات بمنح المرافق والشركات غير الحيوية صلاحية، كي تتخذ هي بنفسها الاحتياطات الدفاعية اللازمة لحماية مجال السايبر فيها[25].

السايبر في الجيش الإسرائيلي

منذ أكثر من عقد، يسود إجماع في المؤسسة العسكرية والأمنية الإسرائيلية مفاده أنّ السايبر بات مجال قتالٍ جديد، وأنه بذلك انضم إلى مجالات القتال الأخرى في البر والبحر والجو والفضاء. وفي العقد الأخير ظهرت في إسرائيل دعوات إلى إقامة سلاح سايبر في الجيش الإسرائيلي ذي قيادة خاصة به أسوةً بالأسلحة البرية والبحرية والجوية.

وفي سنة 2009، اعتبر رئيس أركان الجيش الإسرائيلي حينئذ، غابي أشكنازي، مجال السايبر مجالَ قتالٍ من الناحيتين الاستراتيجية والعملياتية. وبناء على ذلك، أقام الجيش الإسرائيلي في سنة 2009 "هيئة السايبر" في الوحدة 8200 التابعة لجهاز المخابرات العسكرية فيه (أمان). وفي كانون الأول/ ديسمبر 2009، ذكر عاموس يادلين، رئيس جهاز المخابرات العسكرية حينئذ، في محاضرة له في معهد أبحاث الأمن القومي، أن القيام بهجمات في مجال السايبر على أهداف خارجية من بين مهمات "هيئة السايبر" في جهاز المخابرات العسكرية.

وفي حزيران/ يونيو 2015، أعلن المتحدث باسم الجيش الإسرائيلي أنه في ضوء التحديات التي يواجهها الجيش في مجال السايبر، قرر رئيس هيئة الأركان العامة غادي آيزنكوت إقامة سلاح السايبر في الجيش الإسرائيلي، وأنه سيتم تنفيذ هذا القرار خلال عامين. وأشار رئيس الأركان إلى أنّ إقامة سلاح السايبر سيمكن الجيش الإسرائيلي من العمل على نحو أفضل في جبهات مختلفة وفي إظهار تفوقه التقني والبشري[26].

بيد أنّ هذا القرار لم ينفّذ وألغي بعد مداولات طويلة في هيئة أركان الجيش الإسرائيلي. وقد شرح رئيس هيئة الأركان آيزنكوت العوامل التي قادت إلى إقامة، ومن ثم إلغاء، تأسيس سلاح السايبر في الجيش الإسرائيلي، وذلك في مقال له نشره في أواخر سنة 2018[27]. وذكر آيزنكوت أنه جرت مداولات

---

25 المرجع نفسه.

26 مئير الران وغابي سيبوني، "معاني إقامة سلاح السايبر في الجيش الإسرائيلي" (مباط عال) معهد أبحاث الأمن القومي، 2015/7/7، شوهد في 2019/10/8، في: https://bit.ly/2ViQnPk (بالعبرية)

27 غادي آيزنكوت، "السايبر في الجيش الإسرائيلي"، مجلة **سايبر ومخابرات وأمن**، مج 2، العدد 3 (كانون الأول/ ديسمبر 2018)، شوهد في 2019/10/8، في: https://bit.ly/31Zvvz2 (بالعبرية)

مطولة في هيئة الأركان العامة في سنة 2014، بشأن كيفية تنظيم مجال السايبر في الجيش الإسرائيلي. وأضاف أنّ هيئة الأركان العامة فحصت عدة بدائل، وأن بعضها كان يُعتبر قفزة كبيرة؛ إذ دعت إلى جمع مختلف طاقات مجال السايبر في الجيش الإسرائيلي ووضعها تحت قيادة واحدة. أما بعضها الآخر فكان أكثر محافظة، وفي النهاية وبعد دراسة جميع البدائل جرى استخلاص أنه من الخطأ القيام بقفزة كبيرة في تنظيم مجال السايبر في الجيش الإسرائيلي تحت قيادة واحدة. لذلك تقرر قبول مقترح التقدم في تنظيم مجال السايبر في الجيش الإسرائيلي ببطء وعلى نحو مدروس. فتقرر توسيع صلاحيات "قسم المعلومات والاتصالات" في الجيش الإسرائيلي وتغيير اسمه إلى "قسم المعلومات والاتصالات والدفاع عن السايبر"، وأنيطت به مسؤولية الدفاع عن مجال السايبر. وفي موازاة ذلك، أعيد تنظيم عدة وحدات في جهاز المخابرات العسكرية وفي مقدمتها وحدة 8200، وأنيطت بها مهمات القيام بهجمات وجمع المعلومات[28]. وأكد آيزنكوت أنّ سير الجيش الإسرائيلي على نحو مدروس وببطءٍ في مجال السايبر لا يعني إطلاقًا إغلاق الباب أمام إقامة سلاح السايبر فيه في المستقبل[29].

وذكر آيزنكوت في مقاله أنّ الجيش الإسرائيلي تصدّى منذ تأسيس إسرائيل لعدة أخطار هددت أمن إسرائيل، وهي التهديد بالأسلحة التقليدية، والتهديد بالأسلحة النووية التي سعت وما زالت تسعى عدة دول معادية لامتلاكه، وتهديد الحرب غير المتناظرة Asymmetric warfare بين إسرائيل ومنظمات المقاومة. وأضاف أنّ التهديد الجديد الذي يهدد أمن إسرائيل في العقد الأخير هو تهديد السايبر. وأكد آيزنكوت أن السايبر هو أكثر المجالات تطورًا في الجيش الإسرائيلي في العقد الأخير، وقد خصص للسايبر موارد كثيرة للغاية من أجل تحقيق ثلاثة أهداف أساسية: أولًا، الدفاع عن مجال السايبر العسكري والمساعدة في الدفاع عن مجال السايبر المدني في إسرائيل؛ ثانيًا، بذل كل الجهد لتطوير القدرات في جمع المعلومات في مجال السايبر، فالتطورات التكنولوجية قادت إلى ازدياد توافر المعلومات الحيوية المختلفة في مجال السايبر، ولا سيما تلك التي تتعلق بالأمن القومي؛ ثالثًا، تعزيز القدرات الهجومية في السايبر ضد أعداء محتملين[30].

ثانيًا: واقع الطائرات المسيّرة في إسرائيل

واقع الطائرات المسيّرة الإسرائيلية العسكرية

تحتل إسرائيل منذ عدة عقود مكانةً مهمة للغاية في مجال إنتاج الطائرات المسيّرة العسكرية واستعمالها وتصديرها. لقد بدأت في استعمال الطائرات المسيّرة لأغراض التجسس، وتصوير مناطق في الدول العربية

28 المرجع نفسه.
29 المرجع نفسه.
30 المرجع نفسه.

المجاورة لها في أواخر ستينيات القرن الماضي وسبعينياته[31]. واستمرت في استعمال الطائرات المسيّرة في عقدي ثمانينيات القرن الماضي وتسعينياته، في حربها غير المتناظرة ضد القوات الفلسطينية في لبنان في حرب لبنان الأولى، وكذلك ضد حزب الله في لبنان. ومنذ عقد الثمانينيات، استعملت إسرائيل الطائرات المسيّرة؛ ليس فقط في جمع المعلومات، وإنما أيضًا في المشاركة الفعالة في الحرب بواسطة تزويد الجيش الإسرائيلي وسلاحه الجوي بالأهداف المتحركة والثابتة التي يجب استهدافها. وقد استخدمت إسرائيل منذ تسعينيات القرن الماضي الطائرات المسيّرة على نحو مكثف في عمليات اغتيال القادة والناشطين الفلسطينيين واللبنانيين.

وكان اغتيال إسرائيل للأمين العام لحزب الله اللبناني عباس الموسوي، في 16 شباط/ فبراير 1992، من أبرز العمليات التي شاركت فيها الطائرات المسيّرة الإسرائيلية في تلك الفترة. فقد مكثت طائرة إسرائيلية مسيّرة فوق جنوب لبنان في ذلك اليوم، ونقلت مباشرة إلى غرفة العمليات في قيادة الجيش الإسرائيلي في تل أبيب تحركات موكب الأمين العام لحزب الله، الموسوي، الذي كان يزور جنوب لبنان في ذلك اليوم. وفي الوقت نفسه، حددت هذه الطائرة المسيّرة الهدف لسلاح الجو الإسرائيلي الذي أرسل طائرتي أباتشي قصفتا أربع سيارات تابعة لموكب الأمين العام لحزب الله، ما أدى إلى استشهاده هو وزوجته وابنه البالغ من العمر ست سنوات وعددًا من مقاتلي حزب الله[32].

واستمرت إسرائيل في استعمال الطائرات المسيّرة في عمليات اغتيال عشرات القادة والناشطين الفلسطينيين منذ أواخر الانتفاضة الأولى، وفي الانتفاضة الثانية، وفي حروبها ضد قطاع غزة. ولم يقتصر استعمال إسرائيل للطائرات المسيّرة على البلدان المجاورة لها، بل قصفت في العقد الماضي، في كثير من الأحيان، أهدافًا تبعد عنها مئات الكيلومترات.

وصل استعمال إسرائيل للطائرات المسيّرة إلى إحدى ذراه في حرب لبنان الثانية في سنة 2006. فقد فاقت ساعات طيران الطائرات المسيّرة في هذه الحرب ساعات الطائرات الحربية التي يقودها طيارون. وشهدت هذه الحرب الحالة الأولى في التاريخ العسكري الذي استمر فيه عمل الطائرات المسيّرة فوق مسرح القتال طوال الحرب من بدايتها حتى نهايتها. وفي العقد الأخير، استعملت إسرائيل طائراتها المسيّرة على نحو مكثف ودائم في عملياتها العسكرية وفي حروبها الثلاث التي شنتها على قطاع غزة في السنوات 2009 و2012 و2014. وكذلك استعملت إسرائيل، وما انفكت تستعمل، طائراتها المسيّرة في

31 Jef Halper, *War against the People: Israel, the Palestinians and Global Pacification* (London: Pluto Press, 2015), p. 102.

32 رونين بيرغمان، **دولة إسرائيل تفعل كل شيء** (تل أبيب: كنيرت زمورا - بيتان، 2009)، ص 348-367. (بالعبرية)

اعتداءاتها المتكررة على لبنان وسورية والعراق، مستهدفةً الوجود العسكري الإيراني والميليشيات التابعة لإيران في هذه الدول.

إنتاج إسرائيل للطائرات المسيّرة

بدأت إسرائيل منذ عقد ثمانينيات القرن الماضي، وفي عقد التسعينيات، إنتاج أنواع مختلفة من الطائرات المسيّرة، قصيرة المدى ومتوسطة المدى وبعيدة المدى، لأغراض عسكرية مختلفة تشمل جمع المعلومات والتجسس وقصف أهداف قريبة من إسرائيل أو بعيدة عنها[33]. وقد أنتجت إسرائيل منذئذ عدة أنواع من الطائرات المسيّرة بكميات كبيرة، مثل طائرة "سكايلارك" التي تنتجها شركة "ألبيط" الإسرائيلية، وطائرة "هرمس 450" المتعددة الاستعمال للمدى المتوسط، والتي تنتجها أيضًا الشركة نفسها، وقد دخلت في الخدمة في الجيش الإسرائيلي في سنة 1999 ويصل مداها إلى 200 كيلومتر، ويمكنها المكوث في الجو حتى 20 ساعة، وتبلغ أقصى حمولتها 200 كيلوغرام من الأسلحة ومن منظومات التجسس والاتصال، وتبلغ أقصى سرعة لها 175 كيلومترًا/ الساعة[34].

وبدأت الصناعات الجوية الإسرائيلية في سنة 1994 في إنتاج طائرة "هيرون 1"، وشرعت في تصديرها إلى العديد من الدول في سنة 2000، وجرى في العام 2003 الكشف عن هذه الطائرة علنًا. وقد دخلت الخدمة في سلاح الجو الإسرائيلي في سنة 2005. ويبلغ طول هذه الطائرة 8.5 أمتار وارتفاعها 6.5 أمتار وطول جناحيها 16.6 مترًا ووزنها 1150 كيلوغرامًا. وتبلغ حمولتها القصوى 250 كيلوغرامًا، ويبلغ ارتفاع تحليقها في الجو 30 ألف قدم، ويصل مداها إلى 350 كيلومترًا[35].

وأنتجت الصناعات الجوية الإسرائيلية الطائرة المسيّرة "هيرون 2" (التي يطلق عليها أيضًا "إيتان")، ودخلت هذه الطائرة الخدمة في سلاح الجو الإسرائيلي في سنة 2010. وتشبه هذه الطائرة في شكلها طائرة "هيرون 1"، بيد أنها أكبر منها بأربعة أضعاف. وهي تعدّ أكثر الطائرات الإسرائيلية المسيّرة تطورًا. ويبلغ طولها 15 مترًا وارتفاعها 5.6 أمتار وطول جناحيها 26 مترًا، وهي تزن خمسة أطنان. وتبلغ حمولتها القصوى طنًا واحدًا، وتمكث في الجو من دون انقطاع 36 ساعة، ويبلغ ارتفاعها في الجو 45 ألف قدم. وتستعمل هذه الطائرة لأغراض كثيرة، منها جمع المعلومات والتجسس وتصوير مناطق واسعة مع إمكانية بث ذلك بثًا مباشرًا بواسطة القمر الصناعي، وقصف أهداف تبعد عن إسرائيل آلاف

---

33 للمزيد عن أنواع الطائرات المسيرة الإسرائيلية ومهماتها، يُنظر: Halper, pp. 102-104.

34 غيلي كوهين، "إسرائيل أكبر مصدر للطائرات من دون طيار في العالم"، **هآرتس**، 2013/5/19، شوهد في 2019/10/8، في: https://bit.ly/2noThp2 (بالعبرية)

35 المرجع نفسه.

الكيلومترات بالصواريخ أو بالقنابل[36]. ويراوح ثمن هذه الطائرة بين 20 مليون دولار و80 مليون دولار، بحسب ما تجهز به من منظومات مختلفة[37].

وقد صدّرت إسرائيل طائرات مسيرة، وخاصة طائرات "هيرون 1" و"هيرون 2" إلى الكثير من الدول، كان من بينها روسيا وأذربيجان والإكوادور والبرازيل وألمانيا والهند وتركيا واليونان وكندا والمغرب وكورية الجنوبية وسنغافورة والولايات المتحدة وفرنسا وأستراليا. واحتلت إسرائيل في الفترة 2005-2013 المرتبة الأولى عالميًا في تصدير الطائرات المسيّرة؛ إذ صدرت في هذه الفترة طائرات مسيّرة بقيمة 4.62 مليارات دولار[38].

وإلى جانب الفائدة المادية التي تجنيها من تصدير الطائرات المسيّرة إلى الكثير من الدول في العالم، تحقّق إسرائيل فوائد أخرى من ذلك؛ فتصديرها لهذه الطائرات أثّر (ويؤثّر) في تعزيز علاقاتها بالكثير من الدول، سواء على الصعيد السياسي أو على صعيد التعاون الأمني بينها وبين هذه الدول، مثل صفقات تصدير هذه الطائرات التي عقدتها إسرائيل مع الهند وروسيا والكثير من الدول الأخرى.

ويزداد حجم سوق الطائرات المسيّرة في العالم من عام إلى آخر على نحو سريع. ففي سنة 2015 مثلًا، قدّرت قيمة هذه السوق بنحو ستة مليارات دولار، ومن المتوقع أن تصل قيمة هذه السوق في سنة 2022 إلى نحو 22 مليار دولار[39]. ومن الملاحظ أنه حدثت في هذه السوق في السنوات الأخيرة تغييرات مهمة في ما يخص الدول التي تنتج الطائرات المسيّرة. فلم تعد إسرائيل تحتل المرتبة الأولى في تصدير هذه الطائرات، في الخمس سنوات الأخيرة، بيد أنها ما زالت في مصاف الدول الأولى القليلة التي تصدرها.

لقد بدأت الصين في العقد الأخير في إنتاج الطائرات المسيّرة العسكرية وتصديرها إلى الكثير من الدول، بشروط سهلة وبثمن أرخص من الطائرات الأميركية والإسرائيلية، يصل إلى النصف تقريبًا، مع الحفاظ على جودتها في المنافسة. ووفق تقرير لوزارة الدفاع الأميركية في سنة 2015، فإنّ الصين تهدف إلى إنتاج نحو 42 ألف طائرة مسيّرة عسكرية متطورة ومن أنواع مختلفة حتى سنة 2023[40]. كذلك، زادت الولايات المتحدة من إنتاجها للطائرات المسيّرة العسكرية وجعلته في السنوات الأخيرة من أولوياتها

---

36 للمزيد عن هذه الطائرة ومهماتها ودورها في سلاح الجو الإسرائيلي، يُنظر: إيتام ألمدون، "الأكبر منها جميعا، تشكيلات طائرة إيتان تتعاظم"، موقع سلاح الجو الإسرائيلي، 2017/11/1، شوهد في 2019/10/8، في: https://bit.ly/2IwAO1n (بالعبرية)

37 يوآب زيتون، "الطائرة من دون طيار طائرة إسرائيل في المستقبل: أقوى وأسرع"، موقع واي نت التابع لجريدة **يديعوت أحرونوت**، 2014/2/11، شوهد في 2019/10/8، في: https://bit.ly/31ZwjUA (بالعبرية)

38 ليران عنتيبي، "إسرائيل أمام تغييرات عالمية في انتشار الطائرات من دون طيار المسلحة: مخاطر وتحديات وفرص"، مجلة **سايبر ومخابرات وأمن**، مج 2، العدد 3 (كانون الأول/ ديسمبر 2018). (بالعبرية)

39 المرجع نفسه.

40 المرجع نفسه.

العليا، وأولت روسيا، أيضًا، في العقد الأخير إنتاج الطائرات المسيّرة العسكرية أهميةً كبيرة، كما هو الشأن بالنسبة إلى إيران التي أولتها أهمية كبيرة وأنتجت عدة أنواع منها. وفي إمكان بعض الطائرات المسيّرة العسكرية التي تنتجها إيران البقاء في الجو 11 ساعة متتالية، ويصل مداها إلى 200 كيلومتر. ولكن إيران لا تستطيع تفعيل طائراتها لمسافات بعيدة تزيد على 200 كيلومتر، لأنّ بث طائراتها المسيّرة وإمكانية تفعيلها والسيطرة عليها تبقى لمسافات قصيرة لا تتعدى 200 كيلومتر، لعدم امتلاك طهران الأقمار الصناعية اللازمة لذلك[41].

ازدياد حجم الطائرات المسيّرة في سلاح الجو الإسرائيلي وأهميتها

ارتفع في السنوات الأخيرة بسرعة كبيرة عدد الطائرات المسيّرة وعدد أسرابها في سلاح الجو الإسرائيلي، ولا سيما طائرات "هيرون 2"، وازدادت كذلك مهماتها المتعددة في ميادين مختلفة[42]. ومن الجدير ذكره أنّ قائد سلاح الجو الإسرائيلي قرر في سنة 2016 تغيير اسم الطائرات المسيّرة التي كان يطلق عليها في إسرائيل في البداية "طائرات من دون طيار" ثم "الطائرات غير المأهولة"، إلى "الطائرات المأهولة عن بعد"؛ وذلك بهدف التشديد على أهمية العامل البشري الذي يشغل هذه الطائرات المسيّرة، أي وضع الإنسان في المركز لتأكيد أن تشغيل هذه الطائرات يتم على أيدي مشغلين ذوي كفاءات عالية[43]. وقد أولى سلاح الجو الإسرائيلي موضوعَ مشغلي الطيارات المسيّرة أهميةً كبيرة، وأسس في سنة 2001 مدرسة في قاعدة "عين شيمر" شمالي تل أبيب، لتعليم مشغلي الطائرات المسيّرة وتدريبهم على قيادتها عن بعد وعلى قراءة المعلومات وتحليلها التي ترسلها هذه الطائرات مباشرة. وفي سنة 2004، نقل سلاح الجو الإسرائيلي هذه المدرسة إلى قاعدة سلاح الجو في "بلمحيم" الواقعة جنوبي تل أبيب. وجرى تقسيم المشغلين إلى قسمين أساسيين، وهما القسم الخارجي وهو القسم المسؤول عن انطلاق الطائرة المسيّرة وهبوطها. أما القسم الداخلي فهو المسؤول عن الطائرة، وعن توجيهها أثناء طيرانها، وعن تحليل المعلومات والصور التي تبثها[44].

وفي سنة 2016، صدّق قائد سلاح الجو الإسرائيلي على خطة كبرى للطائرات المسيّرة في سلاح الجو الإسرائيلي في العقد القادم. وتم وفق هذه الخطة إجراء تغييرات مهمة في سلاح الجو بمجمله، وتعزيز دور الطائرات المسيّرة فيه وحجمها. وتسعى هذه الخطة لتطوير مجمل المجالات المرتبطة بالطائرات

---

41 المرجع نفسه.

42 دافيد غرينفلد، "خلال سنة 2016 سيتضاعف عدد طائرات إيتان"، موقع سلاح الجو الإسرائيلي، 2015/12/30، شوهد في 2019/10/8، في: https://bit.ly/2p4eGUR (بالعبرية)

43 هداس لفاف وإيتام ألمدون، "ماذا يخبئ المستقبل للطائرات المأهولة عن بعد"، موقع سلاح الجو الإسرائيلي، 2018/2/4، شوهد في 2019/10/8، في: https://bit.ly/30Rnk6E (بالعبرية)

44 دافيد غرينفلد، "تحليق النسر"، **مجلة سلاح الجو**، العدد 222 (نيسان/ أبريل 2015). (بالعبرية)

المسيّرة في سلاح الجو الإسرائيلي مثل: الطاقة البشرية، والعمليات العسكرية، والصيانة، والتدريب، والبنى التحتية. وستزداد وفق هذه الخطة على نحو كبير الطاقات البشرية، وعدد الطائرات المسيّرة، وعدد أسرابها، وعدد ساعات طيرانها. وبناءً على هذه الخطة، ازدادت ساعات طيران الطائرات المسيّرة ووصلت في سنة 2018 إلى ثلث ساعات الطيران في سلاح الجو الإسرائيلي، ونفذت ثلثي ساعات الطيران في العمليات العسكرية التي يقوم بها هذا السلاح. إلى جانب ذلك، نُقلت في الأعوام الأخيرة العديد من مهمات الطائرات التي يقودها طيارون إلى الطائرات المسيّرة، مثل عمليات التجسس وجمع المعلومات التي كانت تقوم بها طائرات "بيتشكرافت كينغ إير بي 200". فقد أصبحت الطائرة المسيّرة من "هيرون 2" تقوم بهذه العمليات، وكذلك باتت تقوم بعمليات الاستطلاع فوق شاطئ البحر الأبيض المتوسط بدل الطائرات التي يقودها طيارون.

مستقبل الطائرات المسيّرة العسكرية

من المتوقع أن يتعاظم للغاية اعتماد سلاح الجو الإسرائيلي في السنوات والعقود القادمة على الطائرات المسيّرة العسكرية؛ وذلك يعود لجملة من الأسباب، من أبرزها أنّ هذه الطائرات تتمتع بالقدرة على العمل المتواصل فترةً تزيد على يوم كامل، وستزداد هذه الفترة في المستقبل زيادة كبيرة. ولها القدرة على العمل في مناطق خطرة ومناطق بعيدة توجد فيها مضادات للطائرات، من دون تعريض الطاقم البشري للخطر. كما أنّ الضرر الناجم عن سقوط طائرة مسيّرة أو فقدانها أقل بكثير من سقوط طائرة يقودها طيار، سواء كان ذلك الضرر ناجمًا عن الخطر على حياة الطيار ووقوعه في الأسر، أو لأنّ ثمن الطائرة المسيّرة أقلّ من ثمن الطائرة التي يقودها طيار. كذلك، فإنّ تكلفة تفعيل الطائرة المسيّرة أقلّ بنسبة كبيرة من تفعيل الطائرة التي يقودها طيار. وإلى جانب ذلك، تتمتع الطائرات المسيّرة المتطورة بقدرةٍ على تجنّب الأخطار أكثر من قدرة الطائرة التي يقودها طيار، واكتشافها على أيدي الجهات المعادية أصعب من اكتشاف الطائرة التي يقودها طيار. وتتمتع الطائرات المسيّرة المتطورة بمنظومة اتصالات وأجهزة متعددة أخرى يمكن تفعيلها بواسطة طاقم مشغليها في قاعدة انطلاق الطائرة المسيّرة، بطريقة أسرع من قيام الطيار الذي يقود الطائرة بتشغيل هذه المنظومات والأجهزة. وكذلك تتمتع الطائرات المسيّرة بالقدرة على الإقلاع والهبوط في أماكن لا تستطيع الطائرة التي يقودها الطيار الإقلاع والهبوط فيها.

ورغم وجود بعض المشكلات التي تواجه الطائرات المسيّرة المتطورة، مثل اعتمادها الكلي في عملية تفعيلها وقيادتها على شبكات اتصال بعيدة، ما قد يعرضها لخطر التشويش على شبكات الاتصال من أطراف معادية، فإنّ هذه المشكلات يمكن معالجتها، وتعد هذه الأخطار قليلة مقارنة بالإنجازات الكبيرة للغاية التي تحققها الطائرات المسيّرة.

ومن غير المتوقع الاستغناء في الفترة المنظورة في العقود القادمة عن الطائرات التي يقودها طيار، ولكن من الواضح أن الطائرات المسيّرة المتطورة والطائرات المسيّرة المستقبلية، التي من المتوقع أن تتعاظم سرعتها وفترة مكوثها في الجو ووزن حمولتها، ستزداد أهميتها ودورها في سلاح الجو الإسرائيلي، وأسلحة الجو الأخرى، عامًا بعد آخر، وأنه سيتم الاعتماد عليها أكثر فأكثر في معظم المهمات. كذلك من المتوقع أن يتم توجيه الميزانيات والجهود والاختراعات العلمية في تطوير الطائرات المسيّرة في سلاح الجو الإسرائيلي، وفي قسم كبير في الأسلحة الجوية للدول المتطورة.

خاتمة

باتت إسرائيل في العقدين الماضيين من أكثر الدول تطورًا في مجال السايبر، الذي تعدّه مركّبًا حيويًا للغاية في أمنها القومي. وقد اتخذت إسرائيل في العقدين المنصرمين مجموعة من التدابير الأمنية والمؤسساتية والإدارية والقانونية، من أجل حماية مجال السايبر فيها من هجمات واختراقات خارجية وداخلية. وفي الوقت نفسه، دأبت إسرائيل على تعزيز قدراتها الهجومية والمخابراتية في مجال السايبر إلى أبعد الحدود، وأولت هذا الموضوع أهميةً كبيرة وعدّته جزءًا من أمنها القومي. وفي سنة 2009، اعتبر الجيش الإسرائيلي مجال السايبر مجالَ قتالٍ من الناحيتين الاستراتيجية والعملياتية، وأقام هيئة السايبر في الوحدة 8200 في جهاز المخابرات العسكرية (أمان) بغرض تعزيز قدرات الجيش الإسرائيلي الهجومية والمخابراتية في مجال السايبر ضد أعداء محتملين.

وقد جرت مداولات مطولة في السنوات الأخيرة في هيئة الأركان العامة للجيش الإسرائيلي بشأن تأسيس سلاح السايبر فيه، ووضع جميع طاقات السايبر تحت قيادة واحدة، أسوةً بالأسلحة البرية والجوية والبحرية. ورغم أنه تقرر عدم إقامة سلاح خاص بالسايبر في الجيش الإسرائيلي في الفترة الحالية، فإنه جرى إعادة تنظيم وتوسيع عدة وحدات في جهاز المخابرات العسكرية، وتخصيص الميزانيات الوفيرة لها، وفي مقدمتها وحدة 8200، وأنيطت بها مهمات التخصص في الحرب في مجال السايبر وشن الهجمات وجمع المعلومات.

أما في ما يخص الطائرات المسيّرة العسكرية، فمن المتوقع أن يتعاظم جدًا اعتماد سلاح الجو الإسرائيلي عليها في السنوات والعقود القليلة القادمة، وأن يتمّ الاعتماد عليها أكثر فأكثر في الغالبية العظمى من عمليات سلاح الجو الإسرائيلي ومهماته.

المراجـع References

العبرية

- أونا، يغآل. "الدفاع عن السايبر الوطني". مجلة **سايبر ومخابرات وأمن**. مج 3. العدد 1 (أيار/ مايو 2019).
- آيزنكوت، غادي. "السايبر في الجيش الإسرائيلي". مجلة **سايبر ومخابرات وأمن**. مج 2. العدد 3 (كانون الأول/ ديسمبر 2018). في: https://bit.ly/31Zvvz2
- إيفن، شموئيل ودافيد بن سيمان - طوف. **حرب الفضاء الإلكتروني: اتجاهات وتأثيرات في إسرائيل**. تل أبيب: معهد أبحاث الأمن القومي، 2011.
- بيرغمان، رونين. **دولة إسرائيل تفعل كل شيء**. تل أبيب: كنيرت زمورا - بيتان، 2009.
- الران، مئير وغابي سيبوني. "معاني إقامة سلاح السايبر في الجيش الإسرائيلي". مباط عال معهد أبحاث الأمن القومي. 2015/7/7، في: https://bit.ly/2ViQnPk
- سمحوني، أفنير. "معركة في السايبر أو سايبر في المعركة". مجلة **سايبر ومخابرات وأمن**. مج 1. العدد 3 (كانون الأول/ ديسمبر 2017).
- سيبوني، غابي وعوفر أساف. **خطوط توجيهية لاستراتيجية وطنية في مجال السايبر**. تل أبيب: معهد أبحاث الأمن القومي، 2015.
- سيبوني، غابي وعيدو سيفان - سبيليا. **تعليمات في مجال السايبر**. تل أبيب: معهد أبحاث الأمن القومي، 2018.
- عنتيبي، ليران. "إسرائيل أمام تغييرات عالمية في انتشار الطائرات من دون طيار المسلحة: مخاطر وتحديات وفرص". مجلة **سايبر ومخابرات وأمن**. مج 2. العدد 3 (كانون الأول/ ديسمبر 2018).
- غرينفلد، دافيد. "تحليق النسر". **مجلة سلاح الجو**. العدد 222 (نيسان/ أبريل 2015).

الأجنبية

- Halper, Jef. *War against the People: Israel, the Palestinians and Global Pacification*. London: Pluto Press, 2015.
- International Telecommunication Union. *ITU Toolkit for Cybercrime Legislation. Draft Rev*. Geneva: International Telecommunication Union, 2010.