قضايا

**تستعرض هذه المطالعة في أربعة أجزاء قراءات في حروب السايبر الإسرائيلية؛ استراتيجيتها وعقيدتها وأساليبها الفاشية، مروراً بأبرز الهجمات غير المسبوقة من نوعها. هنا الجزء الأوّل.**

## قراءات في العقيدة الإسرائيلية وأفعالها

# حروب السايبر [1/4]

شهيرة سلوم

«حصان سيبراني» معروض عند مدخل مؤتمر أسبوع الإنترنت في جامعة تل أبيب في 20/ 6/ 2016 (فرانس برس)

تنخرط إسرائيل في هجماتٍ غير مرئية لنا تندرج في إطار حرب السايبر، ولا يختلف سلوكها فيها كثيراً عمّا هو عليه في حروبها المباشرة، لجهة انتهاك حقوق الإنسان وارتكاب جرائم الحرب والاعتداء على سيادة الدول. يتفق الباحثون في هذا المجال على توصيف هذا النوع من الحروب بالنظيفة، لأنّها تجري من دون إراقة الدماء، إلّا أنّ إسرائيل أدمتها عبر استخدام أدواتها للقتل الجماعي المباشر. تستعرض هذه المطالعة في جزأين قراءات في حروب السايبر الإسرائيلية؛ استراتيجيتها وعقيدتها وأساليبها الفاشية، مروراً بأبرز الهجمات غير المسبوقة من نوعها، والمنسوبة إلى ذراعها السيبرانية سيئة السمعة الوحدة 8200، وتبسط حيّزاً في العرض لهذه الوحدة، ولمشاريع الذكاء الاصطناعي الواردة في كتاب قائدها يوسي سارئيل، والتي يتبيّن أنّها موجودة فعلياً ويجري تنفيذها في حرب غزّة ولبنان، لكن بنسخة أكثر إجرامية.

■■■

يستأجر وينستون، بطل رواية جورج أورويل (1984)، غرفةً صغيرة من السيّد تشارينغتون، كي يختلي بها مع حبيبته جوليا، بعيداً عن أعين وزارة الحبّ. كانت الغرفة ملاذاً آمناً لهما، خصوصاً أنّ الوصول إليها وعرٌ وخطير. كان فيها أشياء عتيقة جداً، يستحيل أن تنفذ منها الرقابة أو شاشات الحزب؛ الساعة الغريبة. ثقالة الورق الزجاج. اللوحة المعلّقة على الجدار، والثقب المنخور أسفله، حيث يُتاح للجرذ أن يتلصّص ويختبئ. كان كلّ شيء فيها يؤكّد لهما أن يسكنا مطمئنَّين. كان وينستون يرى سطح الزجاج في ثقالة الورق كأنّه قوس السماء محيطاً بعالم صغير مكتمل. أحسّ أنه يستطيع الدخول إليه، بل أحسّ بأنه في داخله فعلاً. هو وجوليا وحياتهما والسرير الماهوغاني وكلّ أشياء الغرفة. ... في ملاذهما الآمن، أعلنا تمرّداً على الأخ الأكبر، وخطّطا ودبّرا لنخر الحزب بالفساد وإسقاطه.

في فصل متقدّم من الرواية، يقف وينستون وجوليا قبالة النافذة في الغرفة نفسها، يتأمّلان المرأة التي تردّد أغنية عتيقة بلا معنى في الشارع. يردّد وينستون وراءها «نحن هم الموتى». فجأة، يأتي صوتٌ حديدي من خلفهما «أنتما ميتان، لا تأتيا بأيّ حركة حتى تؤمرا». الصوت الحديدي يأتي من الجدار؛ من هناك، حيث الصورة المعلّقة. يُسمع بعدها صوت تحطّم زجاج على الأرض. كانت الصورة قد سقطت كاشفة عن الشاشة خلفها. يردّد الصوت «نستطيع رؤيتكما». يتوقف غناء المرأة في الشارع، ويتابع الصوت «المنزل محاصر... وها هو جلّادٌ ليقطع رأسك»، قبل أن يغزو الغرفة رجال بملابس سوداء، وأحذية حديدية، والهراوات في أيديهم... ومعهم السيّد تشاريغنتون.

أهلًا بكم في عقل التجسّس الإسرائيلي في زمن السايبر...

■■■

لا يختلف السلوك الحربي الإسرائيلي في الفضاء السيبراني عمّا هو عليه في مجالات البرّ والجوّ والبحر؛ سلوكٌ متفلّت، انتهاكي، مشبّع بعقد التفوّق. وإذا كانت الأفعال الإسرائيلية في المجالات الثلاثة مرئية، ونتائجها مباشرة محسوسة، فإنّ تلك التي تجري في الفضاء السيبراني غيرُ ذلك؛ هي هجماتٌ سرّية في غالبيتها وتجري خلف الأسوار، وليس بالضرورة أن تتزامن مع مجريات الحرب، قد تكون حاصلة حالياً بينما نحن منشغلون في تحليل تأثيرات ما اكتشفناه بالأمس، ويُماط عنها اللثام بعد سنوات.

تشتدّ الهجمات السيبرانية ويبلغ تأثيرها مع التطوّر التقني، وكثيراً ما تكون عملية تطوير هذه التقنيات في صلب الاستراتيجيات السيبرانية الهجومية والدفاعية للدول. وفي العقدين الأخيرين، تصاعد دورها إلى أن صار حاسماً في معارك كثيرة.

في حروب السايبر، تتحرّك الأنشطة الإسرائيلية في ثلاثة اتجاهات: يكون الأوّل عملاً هجوميّاً داعماً للهجوم العسكري المباشر، أو بديلاً عنه في أحيان أخرى، ويجري على عدّة مستويات. يبدأ بالاختراق، ويمرّ بالتعطيل والتخريب، ويصل إلى مستوى التدمير والقتل، كما حصل مع هجوم ستاكسنت stuxnet قبل أكثر من 15 عاماً، والهجوم على الموقع النووي السوري في دير الزور، وتفجيرات أجهزة اتصال حزب الله أخيراً. ويتمثل الاتجاه الثاني في التجسّس وجمع المعلومات الهائلة، التي تُستخدم لتغذية آلات ذكية تشارك في إعداد خطط الحرب ولوائح الأهداف للقوّات على جبهات الحرب. ويتطلّب جمع هذه المعلومات أنشطة واسعة في الفضاءين، المادي والسيبراني معاً، تتضمّن الاختراق والقرصنة والتنصّت وجمع معلومات من الشركاء الحكوميين وشركات التكنولوجيا. وتحاكي أساليب التجسّس لأجهزة الاستخبارات الإسرائيلية (خصوصاً ذراعها السيبرانية 8200 ذائعة الصيت)؛ الأنظمة الشمولية والفاشية. أضف إلى ذلك، أنّها تذهب مع التكنولوجيا الفائقة والسلوك المتفلّت، إلى ما هو أبعد وأكثر رعباً. ويتمثل الاتجاه الثالث في تطوير التكنولوجيا العسكرية داخل مؤسّساتها الحربية، محاولةً بذلك أن تسبق القطاع الخاص خطوةً إلى الأمام.

تمثل الحرب الإسرائيلية الجارية على غزّة ولبنان الحالة الأولى من نوعها، التي تُخاض عبر التكنولوجيا المتفوّقة والأسلحة السيبرانية جنباً إلى جنب مع الأسلحة المادّية، حيث تشكّل ساحاتها مختبر تجارب لأسلحة تقنية، نقلتها إسرائيل للمرّة الأولى من غرف التطوير والنظريات في معاملها الحربية والاستخبارية، إلى ساحة التنفيذ. ولنا في برنامجي لافندر lavender وغوسبل the gospel المستخدمين في حرب غزّة، وما لم يُكشف عنه بعد في صيرورات المعارك وكيفية إعداد لوائح الأهداف ضدّ حزب الله، منذ اغتيال القيادي فؤاد شكر، ما يكفي من الدلائل لسوق هذا الاستنتاج.

يضاف إلى ذلك، أنّ تفجيرات أجهزة اتصالات حزب الله في 17 و18 سبتمبر الماضيين، أظهرت بدورها شكلاً من حروب السايبر، يجمع بين الأساليب القديمة (التفخيخ) والحديثة (الهجوم الافتراضي)، ولم يسبق أحدٌ إسرائيل إليه، سواء في التفكير (الإجرامي) أو التخطيط أو التنفيذ. السيناريو الأخير المسرّب حولها، يشير إلى أنّ فكرة هجوم البيجر وُلدت قبل عامين، وتطلّب تنفيذها عملاً سرّياً عبر عدّة دول، وأنّ «الموساد» صمّم المفخّخة دقيقة الحجم التي نُصبت في الأجهزة، ثمّ جرى جمع الأجهزة وتجهيزها تقنياً لتنفجر عند لحظة تلقي رسالة مشفّرة محدّدة، قبل نقلها من إسرائيل وبيعها لحزب الله. أمّا عملية تفخيخ أجهزة الـ walkie talkie من نوع Icom IC-V82، فقد بدأ التخطيط لها من قبل «الموساد» أيضاً في عام 2015 أيّ قبل تسع سنوات، كان عناصر حزب الله خلالها يتنقلون بين لبنان وسورية وإيران رفقة أجهزتهم، ويتحادثون ويتبادلون المعلومات عبرها.

> لا يختلف السلوك الحربي الإسرائيلي في الفضاء السيبراني عمّا هو عليه في مجالات البرّ والجوّ والبحر؛ سلوكٌ متفلّت، انتهاكي
>
> الحرب الإسرائيلية على غزّة ولبنان الحالة الأولى من نوعها، التي تُخاض عبر التكنولوجيا المتفوّقة والأسلحة السيبرانية جنباً إلى جنب مع الأسلحة المادّية
>
> قوة الردع التي تمنع الحرب النووية، لا تُجدي في حرب السايبر

وبغض النظر عن الفرضيات المطروحة بشأن الهجمات المركّبة، سواء كان الهجوم المباشر اللاحق للتفخيخ إلكترونيّاً أم سيبرانيّاً، فإنّها تطرح مسائل غاية في الخطورة، تتمثل في انتقال نصب الفخاخ المتفجّرة booby traps إلى المساحات الإلكترونية، ليجري استخدامها لاحقاً سلاحاً للقتل والتدمير في فترة الحرب، فضلاً عن مسألة نصب تقنيات التجسّس في الأجهزة، من الدول المصنّعة لها أو المالكة براءة الاختراع، وهو ما يُعيد طرح مسألة السيادة الرقمية، جزءاً من الأمن الوطني عند الدول المتقدّمة، وهذا بحثٌ آخر.

### تقديم في حرب السايبر

تجري حروب السايبر، كما يدلّ اسمها، في الفضاء السيبراني. وهذا الأخير، لا تعريف موحّداً له. تركّز كل جهة على استخداماتها فيه لاشتقاق تعريف ينظّم علاقاتها معه؛ ففيما تعرّفه شركة غوغل مثلاً انطلاقاً من جوانبه التقنيّة البحتة بدءاً من الإلكترونيات إلى شبكات الحواسيب والاتصال، تراه الدول (تعريف وزارة الدفاع الأميركية) مجالاً حربيّاً خامساً، إلى جانب البرّ، والبحر، والجوّ، والفضاء، وتعدّه جزءاً من أمنها الوطني.

في دراسة تحت عنوان «من الفضاء السيبراني إلى السلطة السيبرانية: تعريف الإشكالية»، يتناول الأستاذ في كلية حرب المعلومات والاستراتيجية في جامعة الدفاع الأميركية، دانيال كيول، التعريفات المطروحة للفضاء السيبراني، قبل أن يقدّم تعريفاً واسعاً يجمع بين استخدام تكنولوجيا الإلكترونيات والطيف الكهرومغناطيسي، مشيراً إلى أنشطته المتمثلة في التبادل والإنشاء والتخزين والتعديل واستغلال المعلومات، عبر تكنولوجيا المعلومات والاتصالات، التي تشكّل العمود الفقري للفضاء السيبراني.

مؤلّف كتاب «حرب المعلومات: الفوضى على الطريق الإلكتروني السريع (1994)» وين شوارتاو، يقول عن هذا الفضاء بأنه «ذاك المكان غير الملموس بين أجهزة الحواسيب.. أنّه الواقع الأثيري، وعدد لا نهائي من الإلكترونيات، والفضاء السيبراني بلا حدود». ويقسّم هذا الفضاء إلى «فضاءات سيبرانية محلية أو إقليمية»، يشكّل مجموعها «الفضاء السيبراني الكلّي».

تشير حرب السايبر داخل هذا الفضاء إلى الأفعال التي تُقدم عليها دولة ما أو وكيل عنها، لاختراق أجهزة حواسيب أو شبكة إنترنت دولة أخرى، بهدف إحداث ضرر أو تعطيل أو الاستيلاء على بيانات. كما فضاؤها، لا إجماع بعد على تعريف حرب السايبر، وإشكالاتها القانونية. وتشكّل الأنشطة السيبرانية الهجومية، كالقرصنة والاختراق والجرائم السيبرانية، جزءاً من هذه الحرب، لكنّها ليست بحدّ ذاتها حرباً سيبرانية. وغير الدول، قد يشنّ هجمات القرصنة، أفراد أو تنظيمات أو شركات. وتتنوّع غاياتهم، قد تكون إجرامية (سرقة، تجسّس تجاري،...)، أو احتجاجاً سياسيّاً، وهو ما يسمّى hacktivism.

ورغم اختلاف طبيعة الحرب السيبرانية عن تلك التقليدية، هناك اتفاقٌ على أنّ القانون الدولي، بما في ذلك قوانين النزاع المسلّح، ينطبق عليها. ومع هذا، لا تزال مجالات الخلاف واسعة حول ما يمكن اعتباره اعتداءً سيبرانياً.

في ورقة عُرضت على اللجنة الخارجية في مجلس الشيوخ الأميركي عن الهجمات السيبرانية عام 2015، يقول الباحث جايمز لويس، مدير مركز الدراسات الاستراتيجية والدولية في واشنطن، إنّ أول هجوم سيبراني لأغراض عسكرية حصل في منتصف تسعينيات القرن الماضي، حين استخدمت الولايات المتحدة أدوات بدائية لشنّ هجوم سيبراني ضدّ صربيا. أمّا أوّل هجوم سيبراني مدمّر، فكان الذي شنّته إسرائيل لتدمير المفاعل النووي في دير الزور بسورية.

في إطار استراتيجيات حروب السايبر، قد تُقدم الهيئات العسكرية والاستخبارية على زرع متفجرات افتراضية في فضاءات تابعة لدول أخرى خلال فترة السلم، بحيث تنصب ما يطلق عليه «القنابل المنطقية» logic bombs (برمجية تتحوّل إلى خبيثة عند حصول أفعال محدّدة) والأبواب المفخّخة trapdoors (أبواب سرّية تُزرع في البرامج، وتمنح إمكانية الدخول إليها لاحقاً)، بحسب ريتشارد كلارك، الباحث والأكاديمي في جامعة هارفرد والذي عمل مع إدارات رونالد ريغان وجورج بوش وبيل كلينتون، في كتابه حول الحرب السيبرانية (صادر في عام 2010). ويرى كلارك أنّ الطبيعة الفريدة للحرب السيبرانية، تحفّز إلى توجيه الضربة الأولى. كما أنّ السرعة في ضرب آلاف الأهداف، وفي كلّ مكان تقريباً، تدفع نحو وقوع أزمات متقلّبة. أمّا قوة الردع التي تمنع الحرب النووية، فلا تُجدي في حرب السايبر. وتبدو الحرب الباردة، والتعبير للباحث نفسه؛ وكأنّها منفتحة وشفافة في ظل السرّية التي تحيط النشاط السيبراني للحكومة.

(من أسرة العربي الجديد)

### أول هجوم سيبراني

في ورقة عُرضت على اللجنة الخارجية في مجلس الشيوخ الأميركي عن الهجمات السيبرانية عام 2015، يقول الباحث جايمز لويس، مدير مركز الدراسات الاستراتيجية والدولية في واشنطن، إنّ أول هجوم سيبراني لأغراض عسكرية حصل في منتصف تسعينيات القرن الماضي، حين استخدمت الولايات المتحدة أدوات بدائية لشنّ هجوم سيبراني ضدّ صربيا. أمّا أوّل هجوم سيبراني مدمّر، فكان الذي شنّته إسرائيل لتدمير المفاعل النووي في دير الزور بسورية.