قضايا

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

قراءات في العقيدة الإسرائيلية وأفعالها
حروب السايبر [4/2]

شهيرة سلوم

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 أربعة أجزاء 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. هنا الجزء الثاني.


آثار دمار سبّبه قصف إسرائيلي في خانيونس، جنوبي قطاع غزّة، في 2024/10/13 (الأناضول)

الاستراتيجية السيبرانية الإسرائيلية

تستعرض دراسة صادرة عن المعهد الدولي للدراسات الاستراتيجية (IISS)، (صدرت في جزأين، الأول [iv] في 2022 والثاني [v] في سبتمبر/ أيلول 2023)، القدرات السيبرانية لـ26 دولة متقدّمة في هذا المجال، وتوزّعها على أربع فئات. في الأولى، تقع الولايات المتحدة وحدها قوّةً سيبرانيةً رائدة دولياً، غير أنّها ليست قوّة احتكارية. تأتي أستراليا وكندا والصين والمملكة المتحدة وإسرائيل وفرنسا وروسيا وألمانيا وهولندا في الفئة الثانية. أمّا الفئة الثالثة، فتضم الهند، وإندونيسيا وإيران واليابان وماليزيا وكوريا الشمالية وفيتنام والسعودية وإستونيا والبرازيل وسنغافورة ونيجيريا وجنوب أفريقيا وتركيا والإمارات.

بحسب الدراسة، تتفوّق في تطوير القدرات السيبرانية الهجومية الصينُ وروسيا على مختلف القوى السيبرانية باستثناء الولايات المتحدة، استناداً إلى خبراتها العملياتية في التجسّس الإلكتروني والتوجهات السياسية والتفكير العقائدي في المجال السيبراني. وإذا كانت إسرائيل في نادي الدول السيبرانية الأولى حالياً، فإنّها لم تستثمر في التكنولوجيا العسكرية وتطوّر عقيدتها السيبرانية إلا في العقدين الأخيرين. ويعود ذلك بشكل أساسي إلى أنّ التهديدات الرئيسة لها ليست سيبرانية أو قوى سيبرانية، على خلاف دول مثل الولايات المتحدّة وروسيا والصين. وفي حين كان ثقل التهديدات الاستراتيجية يأتيها من الدول، العربية تحديداً، والجيوش النظامية في القرن الماضي، إضافة إلى المقاومة الفلسطينية، فإنّه انتقل إلى الحركات شبه النظامية، وإيران، في العقود الأخيرة.

في ورقة بعنوان «قوات الدفاع الإسرائيلية والدفاع الوطني السيبراني» (2020)، يحدّد الباحث في مركز الدراسات السيبرانية في جامعة تل أبيب ليور تابنسكي أربع ركائز تقوم عليها الاستراتيجية السيبرانية الأمنية الإسرائيلية، وهي: الإنذار المبكر، والانتصار الحاسم على أرض المعركة، والردع (التراكمي، وليس المطلق)، والدفاع عن الجبهة الداخلية الخلفية. بدايات عمل إسرائيل على الخطط والاستراتيجيات السيبرانية، جاءت في أواخر 2002، عبر إصدار تنظيمات وإنشاء هيئات لحماية أنظمة المعلوماتية. وكانت الهجمات التي شنّتها (الهجوم على الموقع النووي السوري في دير الزور وهجوم ستاكسنت) خلاصة عمل سرّي مع حلفاء لها بعد هذه الفترة. لكنها لم تبدأ التأسيس لاستراتيجية سيبرانية، وتصنّف الفضاء السيبراني مجالاً يحمل تهديداً لأمنها الوطني إلا في عام 2010، حين أنشأت مبادرة السايبر الوطني برئاسة إسحاق بن إسرائيل، لصياغة استراتيجية سيبرانية. وكان على هذه المبادرة أن تجيب عن ثلاث مسائل رئيسة: أولاً، كيفية تطوير التكنولوجيا السيبرانية، بحيث تتمكّن إسرائيل من أن تكون ضمن أول خمس دول في هذا المجال عالمياً. ثانياً، تحديد البنى التحتية المطلوبة لتحقيق ذلك، وثالثاً، تحديد الترتيبات المطلوبة للتعامل مع المخاطر والتهديدات في هذا الفضاء. واصلت المبادرة عملها ستة أشهر (كانت واحدة من لجانها سرّية)، ثم خرجت باستراتيجية للأمن السيبراني الوطني 2011، وقدّمت توصياتها بإنشاء لجنة حكومية متخصصة لقيادة الجهود السيبرانية على مستوى القطاعين الحكومي والخاص، إضافة إلى إنشاء مكتب السايبر الوطني، سيتبع مباشرة لرئاسة الحكومة.

وبعد فترة قصيرة من المبادرة السيبرانية، أعلنت إسرائيل جهوزيتها لاستخدام السلاح السيبراني في الميدان الحربي، بدون أن تفصح عن طبيعة هذا السلاح. وفي العام 2015، أشارت العقيدة العسكرية للجيش الإسرائيلي إلى أدوار سيبرانية وُصفت بالدفاعية لحماية المؤسسات والقوّات المسلّحة. وفي العام 2017، وحّدت الهيئات السيبرانية، وراجعت الخطط والاستراتيجيات لدمج القدرات الدفاعية والهجومية في مجال السايبر.

تجنّد الاستراتيجية السيبرانية الإسرائيلية قطاع التكنولوجيا الخاص والهيئات الأكاديمية والبحثية في خططها، بحيث يظهر وكأنّه لا خط فاصلاً بين المشاريع السيبرانية للدولة والهيئات المدنية. يتجلّى ذلك من خلال تأسيس مراكز الأبحاث السيبرانية وتمويلها في الجامعات الإسرائيلية، إضافة إلى تأسيس برامج الابتكار وتمويلها. كما يُلاحظ أنّ أغلب (إذا لم يكن جميع) المؤسسين والمديرين التنفيذيين لشركات التكنولوجيا الإسرائيلية بدأوا مسيرتهم من الذراع السيبراني لشبكة الاستخبارات العسكرية، الوحدة 8200 (منهم مؤسّسو شركة NSO، ذائعة الصيت بالتجسّس هي الأخرى، عبر تقنية بيغاسوس).

يسمح الانخراط القوي بين المؤسسات العسكرية والاستخبارية الإسرائيلية وشركات التكنولوجيا بتبادل المعلومات والخبرات والتقنيات؛ والأخطر من ذلك، أنّه يسمح بتجربة التقنيات المطوّرة حديثاً من قبل شركات التكنولوجيا الإسرائيلية على أرض المعركة، قبل إطلاقها إلى الأسواق.

وعلى الرغم من تفوّقها الإقليمي في مجال القدرات السيبرانية؛ الهجومية والاستخبارية، تفتقر إسرائيل إلى المعلومات الاستخبارية العالمية. لتعويض هذا النقص، تتبادل المعلومات مع حلفائها وشركائها، وفي المقدّمة هيئات الاستخبارات السيبرانية الأميركية، إضافة إلى الأذرع السيبرانية الاستخبارية في المملكة المتحدة وفرنسا وسنغافورة والإمارات العربية (تقرير معهد IISS، سبتمبر 2023: القدرات السيبرانية والقوة الوطنية)، كما تعقد شراكات سرّاً وعلانيةً مع شركات التكنولوجيا العالمية.

تقود الاستخبارات العسكرية (أمان) مجال التكنولوجيا السيبرانية الإسرائيلية، متقدّمةً خطوات على القدرات السيبرانية المدنية. تعتبر ذراعها السيبرانية الوحدة 8200 من أكبر وحداتها، بحيث يشكّل العاملون فيها حوالي 80% من موظفيها. كُلّفت الوحدة بتطوير القدرات السيبرانية الهجومية ابتداءً من العام 2009. وأنشأت بعدها فريقاً سيبرانياً خاصاً لتطوير وتوظيف الأسلحة السيبرانية الهجومية ثمّ مكتباً خاصاً للعمليات والقدرات السيبرانية. إضافة إلى الوحدة 8200، التي خدم فيها الرئيس الإسرائيلي إسحاق هرتزوغ، هناك الوحدة السيبرانية التابعة للقوات المسلّحة سي 4 آي C4I والمكلّفة بالدعم التكنولوجي للقوات الجوّية والبحرية والبرّية. وتُولي إسرائيل اهتماماً خاصّاً بالذكاء الاصطناعي وتوظيفه في المجال الحربي، وتُصنّف عالميّاً ضمن الدول العشر الأوائل. تقف الوحدة 8200 وراء أبرز الهجمات السيبرانية الإسرائيلية، بحسب ما تبيّن التحقيقات المنشورة حولها. وقبل تناول الذراع السيبرانية لإسرائيل وأساليب عملها، وكتاب قائدها (سارئيل يوسي) المنشور حديثاً، والذي يكشف الكثير عن العقيدة السيبرانية الإسرائيلية وطموحاتها، وما يجري تنفيذه فعلياً من المشاريع الواردة فيه؛ قبل الغوص في ذلك كله، نتناول اثنين من أبرز الهجمات السيبرانية الإسرائيلية: الهجوم على الموقع السوري في دير الزور (2007)، وهجوم البرمجية الخبيثة stuxnet على المفاعل النووي الإيراني.

> بدايات عمل إسرائيل على الخطط والاستراتيجيات السيبرانية جاءت في أواخر 2002، عبر إصدار تنظيمات وإنشاء هيئات لحماية أنظمة المعلوماتية

> أغلب المؤسسين والمديرين التنفيذيين لشركات التكنولوجيا الإسرائيلية بدأوا مسيرتهم من الذراع السيبراني لشبكة الاستخبارات العسكرية

تدمير الموقع السوري في دير الزور 2007

يعدّ هذا الهجوم الأوّل من نوعه في الفضاء الافتراضي. وتتعدّد فرضيات ما استبق تدمير الموقع السوري، ومنها أن يكون هجوم إلكتروني وليس سيبرانيّاً قد مهّد للغارة الإسرائيلية. والهجوم الإلكتروني ينشط في المجال الكهرومغناطيسي ويستهدف الاتصالات وأنظمة أجهزة الرادار، فيما يشتغل الهجوم السيبراني بشكل أساسي في المجال الرقمي ويستهدف أجهزة الحواسيب وشبكات الإنترنت والبنى التحتية المتصلة بها. في كتابه عن حرب السايبر، يسرد الباحث ريتشار كلارك المذكور سابقاً، تفاصيل الهجوم السيبراني cyberattack، كما يصفه، والذي استبق العمل العسكري، لكن من دون أن يدخل في التفاصيل التقنية للهجوم (سيبراني أم إلكتروني)، ويرى أنه شكّل عاملاً حاسماً في قصف المبنى الذي يقع على الجانب الشرقي من نهر الفرات، على بعد 75 ميلاً جنوباً من الحدود التركية. يقول إنه في تلك الليلة، كان عناصر الجيش السوري يراقبون شاشات راداراتهم، وإسرائيل كانت قد وضعت قواتها في مرتفعات الجولان المحتل في حالة تأهب قصوى على غير عادة. ومن مواقعه في الأراضي السورية المحتلة، كان لواء غولاني الإسرائيلي يراقب وسط مدينة دمشق عبر عدساته بعيدة المدى، لهذا توقع عناصر الجيش السوري أن أمراً ما قد يحصل، ومع هذا لم يظهر أي شيء غير عادي على شاشاتهم. كانت سماء سورية آمنة وخالية مع حلول منتصف الليل. هذا على شاشات الرادارات. أمّا على أرض الواقع، فقد كانت الطائرات الإسرائيلية تخترق المجال الجوي السوري من تركيا. وكان يفترض أن يضيء هجوم تلك الطائرات بهياكلها المصنوعة من الفولاذ والتيتانيوم وحافاتها وزواياها الحادة والقنابل والصواريخ المعلقة على أجنحتها، كما يصف، الرادارات السورية، لكن هذا لم يحصل. ما اكتشفه السوريون في صباح اليوم التالي، هو أنّ إسرائيل كانت قد سيطرت سيبرانياً على أنظمة الدفاع الجوي السورية في الليلة السابقة، وما ظهر على شاشات الرادارات لم يكن سوى صورة خادعة لسماء هادئة وضعها الإسرائيليون أنفسهم. ماذا حصل في الوقت الذي كان فيه السوريون يراقبون شاشاتهم ويرون سماء صافية؟ يضع كلارك ثلاث فرضيات. الأولى، أن يكون الهجوم الإسرائيلي قد استُبق بإرسال طائرة شبحية بدون طيار (UAV)، لتحلق عمداً في مجال رادار الدفاع الجوي السوري. وما دام الرادار لا يزال يعمل بالطريقة نفسها التي كانت قبل سبعين عاماً من ذلك التاريخ، سيرسل حزمة إذاعية اتجاهية، وإذا اصطدمت هذه الحزمة بأي شيء، فإنها سترتد إلى جهاز الاستقبال، عندها يقوم المعالج (الحاسوب) بحساب مكان الجسم الذي ضربه شعاع الراديو وارتفاعه وسرعته وربما حجمه.

يفترض الباحث هنا أنه ربما لم يرَ الدفاع الجوي السوري طائرة إسرائيلية بدون طيار، لأنها كانت مغطاة بمواد تمتص شعاع الرادار أو تنحرف عنه. وتمكّنت هذه الطائرة بطريقة ما من اكتشاف شعاع الرادار القادم من الأرض باتجاهها، ثم استخدمت التردّد اللاسلكي نفسه لإرسال حزم إلى حاسوب الرادار في شبكة الدفاع الجوي السورية. وفي اعتقاده، أن هذه الحزم سبّبت حدوث خلل في النظام، لكن في النتيجة أعطته تعليمات بعدم التصرّف. وربما ما فعله الإسرائيليون هو أنّهم أعادوا تشغيل لقطة من السماء لتبدو كما كانت قبل الهجوم. وفي حين أن شعاع الرادار ربما ارتد لاحقاً من الطائرات الإسرائيلية المهاجمة، غير أن إشارات العودة لم تُسجّل على أجهزة نظام الدفاع الجوي السوري. ولهذا بدت لهم السماء في تلك اللحظة كما لو أنها فارغة، في حين أنها في الواقع مليئة بالمقاتلات الإسرائيلية.

الفرضية الثانية تقدّر أن تكون شيفرات جهاز الحاسوب الروسي المتحكّمة في شبكة أنظمة الدفاع الجوّي السورية قد تعرّضت للاختراق من عملاء إسرائيليين؛ إما عبر اختراق الحاسوب الروسي نفسه، وإمّا عبر منشأة عسكرية سورية، وإمّا أن عميلاً لإسرائيل أو أحد حلفائها قد تسلّل إلى رموز الحاسوب، عبر خدعة تسمّى فيروس Trojan Horse، نسبة إلى خدعة «حصان طروادة» الشهيرة في ملحمة الإلياذة والأوديسة. الفرضية الثالثة ترجّح أن يكون عميل إسرائيلي قد عثر على كابل ألياف ضوئية لشبكة الدفاع الجوي بمكان ما في سورية، وشبك به، ليخلق صورة خادعة على شاشات الرادار السورية.

هجوم ستاكسنت stuxnet

أوّل هجوم سيبراني معروف لنا يتمكّن من إلحاق أضرار مادية مدمّرة في موقع الهجوم. وكان عبارة عن برمجية خبيثة استهدفت مفاعل نطنز النووي الإيراني. اكتُشفت في يونيو/ حزيران 2010. وبحسب التحقيقات اللاحقة للاكتشاف، كانت البرمجية دودة حاسوب بحجم 500 كيلوبايتس، تمكّنت من تخريب برامج 14 موقعاً صناعياً. وفي حين يبحث الفيروس الذي يصيب البرامج الحاسوبية عن ضحية تحمّل البرنامج المزروع فيه، تزحف الدودة الحاسوبية إلى شبكات الحواسيب من تلقاء نفسها؛ وهذا ما جرى مع ستاكسنت، التي انتشرت في عدّة مواقع وعاثت خراباً لسنوات (يرجّح أن تكون بداية هجومها ما بين 2005 و2007)، قبل أن يكتشفها Sergey Ulasen، وهو مهندس حاسوب وخبير في الذكاء الاصطناعي، كان يعمل حينها في شركة أمن سيبرانية بيلاروسية هي VirusBlokAda. وشنّت البرمجية المعقّدة والخبيثة هجومها على ثلاث مراحل، بحسب تحقيق لمعهد IEEE Spectrum [vi]؛ في الأولى، استهدفت أجهزة وشبكات برامج مايكروسوفت ويندوز، ثم انتقلت ثانياً إلى برنامج «سيمنز ستب 7»، الذي يشغّل أنظمة التحكّم الصناعية لتشغيل المعدّات، ومنها إلى أجهزة الطرد المركزي. في المرحلة الثالثة، اخترقت برامج التحكّم، وتمكّنت البرمجية (بالأحرى مالكها والمتحكّم فيها) من التجسّس على الأنظمة الصناعية، وسيطرت عليها، دافعةً بها نحو تسريع دوران أجهزة الطرد المركزي، إلى أن هشّمت نفسها. لم يتبنّ الجيش الإسرائيلي هجوم ستاكسنت غير المسبوق في تركيبته الخبيثة أو الدمار الذي ألحقه، لكن التسريبات وطبيعة عمل البرمجية، كشفت أنّه كان جزءاً من عملية مشتركة ضخمة بين الولايات المتحدة وإسرائيل استهدفت البرنامج النووي الإيراني وسُميت الألعاب الأولمبية Olympic games.

يؤكّد المشتغلون في شؤون حروب السايبر أنّ هجوم ستاكسنت نقل مفهوم الحرب إلى مستوى آخر لم يكن موجوداً، وطرح نقاشاً حول طبيعته بوصفه فعلاً حربياً وتبعات ذلك القانونية؛ إذ إنّه بموجب هذا التوصيف، فإنّ الدولة التي تعرّضت للهجوم يصبح لها الحق في الردّ دفاعاً عن النفس. وأجمع خبراء قانونيون في عدّة أوراق منشورة (ومنها تقرير للجنة مكلّفة من مركز الدفاع السيبراني التابع لحلف شمالي الأطلسي، مارس/ آذار 2013)، على أنّ الهجوم كان «فعل قوّة»، غير أنّهم انقسموا حول توصيفه هجوماً مسلّحاً يُتيح للدولة المُعتدى عليها، بموجب القانون الدولي، أن تستخدم القوّة للدفاع عن النفس. ويسلّط الهجوم الضوء على جوانب لم تكن في حسابات المهتمين بهذا المجال؛ ففيما كان النقاش سابقاً يدور حول ما يوفّره الفضاء السيبراني من أدوات وإمكانيات للطرف الأضعف (أفراد وجماعات ودول) في عالم غير متكافئ، فإنّ هجوم ستاكسنت طرح مسألة الضعف السيبراني للدولة، الذي قد يشلّ قدراتها الدفاعية، في مواجهة دولة متفوّقة عليها في هذا المجال.

لم يبق هجوم ستاكسنت Stuxnet وحيداً، وكان الأوّل (المعروف لنا على الأقل) في سلسلة هجمات لاحقة، نُسبت إلى إسرائيل واستهدفت التجسس على دول المنطقة (هجوم فلايم flame 2012، الذي هاجم أجهزة الحواسيب عبر برامج مايكروسوفت)، والبرنامج النووي الإيراني. ففي عام 2011، اكتُشفت برمجية دوكو الخبيثة Duqu، التي تملك العديد من الصفات المشتركة مع برمجية ستاكسنت. وفي عام 2015، عثرت مختبرات كاسبرسكي، وهي شركة أمن سيبراني روسية، على برمجية خبيثة أخرى محدّثة من دوكو هي Duqu 2.0. وقيل عن الأخيرة إنّها البرمجية الأكثر تعقيداً على الإطلاق حتى الآن، واستهدفت دولاً وكيانات على علاقة بمفاوضات الملف النووي الإيراني.

الذراع السيبرانية الإسرائيلية التي تُنسب إليها هذه الهجمات كما ذكرنا هي الوحدة 8200 التابعة لشبكة الاستخبارات العسكرية (أمان). نتناول في جزء ثالث من هذه القراءات عملها وأساليبها الفاشية في التجسّس، بحسب ما تبيّن شهادات جنودها، ونعرض قراءات موسّعة من كتاب قائدها «الفريق الآلي - البشري»، الذي يكشف الكثير من المشاريع السيبرانية الإسرائيلية، والتي يظهر لنا من مجريات الحرب في غزّة ولبنان أنّها موجودة فعليّاً.

دور شركات التكنولوجيا

تجنّد الاستراتيجية السيبرانية الإسرائيلية قطاع التكنولوجيا الخاص والهيئات الأكاديمية والبحثية في خططها، بحيث يظهر وكأنّه لا خط فاصلاً بين المشاريع السيبرانية للدولة والهيئات المدنية. كما يسمح الانخراط القوي بين المؤسسات العسكرية والاستخبارية الإسرائيلية وشركات التكنولوجيا، بتبادل المعلومات والخبرات والتقنيات؛ والأخطر من ذلك، أنّه يسمح بتجربة التقنيات المطوّرة حديثاً من قبل شركات التكنولوجيا الإسرائيلية، على أرض المعركة، قبل إطلاقها إلى الأسواق.