تقدير موقف

الحرب السيبرانية في المواجهة العسكرية الإيرانية (الإسرائيلية)
الإمكانيات وحدود التأثير

بقلم: الفريق الركن حسن سلمان خليفة البيضاني

مركز حمورابي للبحوث والدراسات الاستراتيجية

30 حزيران 2025

تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزا علميا بحثيا يهتم بدراسة الموضوعات السياسية والمجتمعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

للتواصل

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net

مركز حمورابي للبحوث والدراسات الاستراتيجية

الحروب السيبرانية والواقع القائم

مع بدايات القرن الحادي والعشرين المتعثرةسطع الحدث الأكثر دراماتيكية متمثلًا في هجمات 11 ايلول 2001 التي استهدفت شريان الاقتصاد الأمريكي وضرب القلب الاقتصادي النابض والمتمثل بأبراج التجارة العالمية في مانهاتن، وما أعقب ذلك من تصعيد غير مسبوق في أنماط الحروب والصراعات، إذ شكلت الولايات المتحدة الأمريكية تحالفًا دوليًا لإسقاط نظام طالبان في كابل، ثم سرعان ما تهاوى نظام استبدادي دموي آخر في العاصمة بغداد خلال عامين فقط، فغدت إنطلاقة هذا القرن شبيهة من حيث التصعيد بانطلاقة القرن السابق، مع فارق جوهري: فذاك القرن شهد ولادة الجيل الثاني من الحروب عبر الاستخدام المكثف للأسلحة الساندة والطائرات والدبابات، في حين شهد هذا القرن ولادة جيلًا مختلفًا كليًا، يعبّر عنه بالحروب اللامتماثلة، الهجينة، والسيبرانية، والأخيرة فرضت نفسها بقوة على كل الصراعات خلال الربع الأول من هذا القرن لتكون بمثابة إعلان أن هنالك ما يمكن أن نسميه الابتعاد عن الأرض والتركيز على القتال بالفضاء وبأدوات تجعل من المتعذر على الماكثين في الأرض أن تكون ردودهم القتالية المقابلة بمستوى الخطورة القادمة من الفضاء.

مفهوم الحرب السيبرانية:

كما هو معروف فإنها تلك الحرب الدائرة في الفضاء السيبراني والتي تنفذ بواسطة وسائل وأساليب سيبرانية (فضائية)، إذ يتم استعمال الهجمات الرقمية - مثل فيروسات الكمبيوتر والقرصنة أو ادخال معلومات خاطئةعن طريق أجهزة متخصصة في هذا المجال من قبل الجهات المتصارعة أو المشتبكة في حروب أو تلك التي بين بعضها البعض صراعات أو نزاعات غير محسومة غايتها تخريب أو تعطيل القدرات الفنية والتقنية وصولًا إلى شل قدرة الطرف الآخر في استخدام مقومات قوته بالشكل المطلوب لتحقيق غايات أو أهداف محددة لمرحلة أو مراحل لاحقة من الصراع، إذ باتت الحرب السيبرانية تشكل مفصل حيوي ومهم من مفاصل إدارة المعارك والحروب، ولا ينبغي الخلط بين الحرب السيبرانية والاستعمال الإرهابي للفضاء السيبراني أو التجسس السيبراني أو الجرائم السيبرانية، فعلى الرغم من استعمال وسائل تنفيذ مماثلة في جميع أنواع الأنشطة الأربعة أعلاه إلا أنه من الخطأ تفسيرها على أنها حرب سيبرانية، ورغم ذلك فإن الكثير من الدول ولاسيما في مناطق الصراع تعتمد التجسس السيبراني كأحد الاساليب الاستخبارية المكملة للحرب السيبرانية؛ لذلك فإن خطر الحرب السيبرانية وآثارها المتصاعدة تعد مصدر قلق كبير للدول وقياداتها العسكرية والأمنية.

أدوات القوة لدى طرفي الصراع

يمكن للمتابع الدقيق لتفاصيل هذه الحرب التي استمرت اثني عشر يومًا وليلة، أن يلحظ تفردها عن الحروب السابقة والحالية بكونها ابتعدت كثيرا عن الأرض، حيث حلقت الغالبية العظمى من أدواتها في فضاء مفتوح إلا

بعض مكونات منظومات القيادة والسيطرة التي كانت تشكل الجزء المكمل لمنظومات الإطلاق والتصدي، وإذا ما حاولنا المقارنة بين ما يمتلكه (اسرائيل) المدعوم أمريكيًا وغربيًا وحتى عربيًاوبين ما تمتلكه الجمهورية الاسلامية من إمكانيات عسكرية عملت لسنوات طويلة رغم الحصار على تكوينها وتوظيفها،فإن كل المؤشرات دلت في نهاية الحرب على أن الجمهورية الاسلامية لها الحظ الأوفر في الهيمنة على فضاء الصراع من خلال القوة الصاروخية والطائرات المسيرة التي كبحت جماح أربع من افضل منظومات الدفاع الجوي في العالم والتي يمتلكها الكيان وهي (منظومة ثاد المتطورة بإصدارها المحدّث ومقلاع داؤود بمكوناته ذات القدرات العالية على الكشف والتصدي والتدمير و منظومات الباتريوت التي تعد واحدة من أكثر المنظومات تطورًا واخيرًا القبة الحديدية التي تبجح الكيان بها بوصفها الضمانة الأساسية لسماء خالية من أي تهديد)، إيران والتي اعتمدت في عملياتها العسكرية كمرحلة أولى على الصواريخ البعيدة المدى ذات القدرات العالية في مجال السرعة وصعوبة في كشفها قبل انقضاضها على الهدف (فرط صوتية) وفي المرحة الثانية على المزاوجة بين أنواع مختلفة من الصواريخ معززة بأعداد من الطائرات المسيرة ذات المديات البعيدة مع مشاركة لم تكن متوقعة من أدوات الحرب السيبرانية التي عطلت ولمرات عديدة نظم الإنذار المبكر في الغالبية العظمى من المدن الإسرائيلية، فقد نجحت وإلى حد كبير في فرض السيطرة، قياسا بالقدرات المستخدمة لجيش الكيان لاسيما قواته الجوية والصاروخية مع التركيز في توجيه الضربات على قوتها الجوية ذات القدرات العالية والتجارب الطويلة لاسيما طائرات ال اف 35 الأمريكية التي تملك القوة الجوية الصهيونية 39 طائرة منها وكذلك مشاركة طائرات ال اف 15 والاف 16 مسندة بطائرات ارضاع جوي والبالغ عددها (11) طائرة، وبطائرات ايركنكغ السسنا كرفان للقيادة والسيطرة والاستطلاع والتحكم والحرب السيبرانية، وجي 550 لاعتراض الاتصالات والإنذار المبكر والتشويش الإلكتروني وهي الأخرى جزء من منظومة الحرب السيبرانية، هذا يؤكد إن الأجواء والفضاء الخارجي والفضاء السيبراني هي التي تولت زمام السيطرة خلال الأيام الاثني عشر من الصراع لتُفضي بلا أدنى شك إلى نتيجة حُسِمت لصالح الجمهورية الإسلامية في إيران.

القدرات السيبرانية (الإسرائيلية)

عمل (اسرائيل) وفي وقت مبكر على الاستفادة من الابتكارات السيبرانية المبكرة على مستوى العالم، إذ كان للكيان قصب السبق في عام 1997 بأنشاء وكالة حكومية متخصصة في مجال الإنترنت أطلق عليها تسمية Tehila، لضمان الاتصال الأمن بالإنترنت بين السلطات الحكومية، كما كان الكيان أيضًا أول دولة تستخدم الأسلحة السيبرانية لإخضاع ما تعده تهديدًا رئيسًالموجه إليها، أي البرنامج النووي الإيراني، من خلال فيروس "ستكسنت" والذي خصص لاستهداف البرنامج النووي الإيراني في عام 2010، وتسبب وقوع أضرار جسيمة من خلال اختراق أنظمة التحكم الإشرافي، والحصول على البيانات في منشآت تخصيب اليورانيوم الإيرانية، و تعطيل مكوناته

الرئيسة. كما استخدمت (إسرائيل) قدراتها السيبرانية، جنبا إلى جنب مع أنظمة الأسلحة التقليدية لأول مرة، من خلال عملية "البستان" في عام (2007) التي استهدفت نظام الدفاع الجوي السوري، وتضمنت أيضا تدميرا لموقع للأبحاث النووية يشتبه في أن تكون فيه بعض الأنشطة لتخصيب اليورانيوم، وهو منشأة "الكبر" للأبحاث الذرية السلمية في محافظة دير الزور، وقد نفذت العملية دون أن تتسبب في أي خسارة للجانب الصهيوني.

في 2 تموز 2020، أدى انفجار غامض في محطة "طنز " النووية في إيران إلى تدمير منشأة للطرد المركزي فيها، حينها اتهمتطهران (اسرائيل) بهذا العمل التخريبي وأكدت إن الكيان استخدم أدوات حربه السيبرانية لتحقيق ذلك، لكنها أي الإدارة الإيرانية في طهران لم تستطع تقديم أدلة موثوقة، كما إنها حملت وللمرة الثالثة (اسرائيل) في نيسان 2021 المسؤولية عن انقطاع التيار الكهربائي في المنشأة بعد لحظات من افتتاح أجهزة الطرد المركزي الجديدة، لكن لم يصدر أي تأكيد من حكومة (تل ابيب) بذلك وأعلنت لاحقا نفيها في تورطها بهذا العمل غير أن التحقيقيات الإيرانية اللاحقة أثبتت وبما لا يقبل الشك إن الكيان هو من قام بها وتجدر الإشارة هنا إلى أن الكيان ومنخلال الاستفادة من الإنكار واستهداف المنشآت النووية الإيرانية الحيوية على نحو متكرر، تمكن من تأخير جهود طهران النووية من دون ردود فعل سياسية عنيفة أو الدخول في مواجهة عسكرية مباشرة تكون لها تكلفتها العالية كالتي حصلت في منتصف حزيران من هذا العام.

الإستراتيجية (الإسرائيلية) للحرب السيبرانية

تنظر (إسرائيل) إلى الفضاء السيبراني بوصفه منصة لتحسين الفاعلية التشغيلية والدفاعية، وقد اتجهت أخيرًا إلى تعزيز إمكاناتها المتطورة في الفضاء السيبراني من خلال رسم إستراتيجية سيبرانية شاملة، وإنشاء وحدات أو مؤسسات سيبرانية الحماية بناها التحتية، وتحقيق أهدافها الداخلية والخارجية، والحفاظ على مكانتها وأمنها السيبراني.

يعتمد (اسرائيل) في مجال تطبيق إستراتيجية الحرب السيبرانية على ما يلي:

1. الوحدة 8200

تُعد إحدى أقوى أذرع هيئة الاستخبارات (الإسرائيلية) (أمان)، ويمتد عملها إلى كل أنحاء العالم تقريبا إلا أنها تركز على مناطق المسؤولية أولا (المتمثلة بغزة وجنوب لبنان والضفة الغربية و إيران والعراق واليمن) ثم مناطق التأثير (وتشمل مصر وتركياوالباكستان وسوريا قبل التغيير والأردن وباقي مناطق لبنان) ومن ثم تليها مناطق الاهتمام (وتشمل الغالبية العظمى من دول العالم إلا أنها ركزت خلال الحرب الأوكرانية الروسية على روسيا والدول المجاورة والمؤيدة لها)، ونظرًا إلى ما تملكه من إمكانات وخبرات فأنها تستطيع تزويد مختلف المؤسسات (الإسرائيلية) الأمنية والعسكرية والسياسية وحتى الاقتصادية بسيل متواصل من المعلومات اللازمة، بعد جمعها من خلال اختراقات وعمليات تجسس يعتمد معظمها على العمل السيبراني، الذي يتميز فيه

العاملون بها وتحويلها إلى استخبارات بدرجة موثوقية عالية.

في عام 2006 وبعد الفشل الذريع في الحرب الصهيونية ضد حزب الله في الجنوب اللبناني قرر مؤتمر هرتسيليا المنعقد في تشرين الأول من العام نفسه إعطاء أهمية أكبر لكل مفاصل الاستخبارات في (اسرائيل) وإدخال الأمن السيبراني والحرب السيبرانية كجزء حيوي وفعال في الهياكل التنظيمية لتلك الوكالات ومنها الوحدة 8200، في عام 2009، كُلفت هذه الوحدة التي تعادل في كثير من النواحي وكالة الأمن القومي الأميركية، بتعزيز القدرات السيبرانية الهجومية للجيش الصهيوني. ونظرًا إلى أهميتها بالنسبة إلى (إسرائيل)، فإن السرية تحيط بها إلى حد كبير، إذ لا تعرف هوية العاملين فيها، ولا حتى قائدها، كما اتضح هذا الأمر عند حفل تسليم قيادة الوحدة في 28 شباط / فبراير 2020؛ إذ حرص الجيش (الإسرائيلي) يومذاك على تمويه صورة وجه قائدها بين صور الحفل، فضلا عن ذلك فان هذه الوحدة ورغم مشاركتها في عمليات التوغل بعد طوفان الأقصى إلا أن التعتيم على فعالياتها لم يعطي للمتلقي صورة واضحة عن ما فعلته خلال هذه المرحة الخطيرة.

تعد هذه الوحدة قاعدة تجسس إلكترونية (إسرائيلية) الأهم والأكبر ومقرها (منطقة النقب) ضمن قاطع القيادة الجنوبية للجيش الصهيوني، إذ تشمل:

أولا: الطيف الهجومي للاستخدام العسكري للقدرات السيبرانية.

ثانيا: التنصت على البث الإذاعي.

ثالثا: المكالمات الهاتفية، والفاكس ووسائط التواصل الاجتماعي بمختلف برامجها.

رابعا: البريد الإلكتروني في قارات آسيا وأفريقيا وأوروبا.

خامسا: قيادة أنظمة التتبع للشخصيات المطلوب تصفيتها أو استهدافها

سادسا: المساهمة بشكل فعال ومدروس في برامج التواصل الاجتماعي لأغراض متناقضة إما الكشف عن هويات المؤيدين للقضية الفلسطينية أو تجنيد العرب والفلسطينيين وغيرهم لصالح دعم الكيان.

تشير تقارير إلى أن الوحدة لعبت دورا في تعقب مواقع قيادات حركة "حماس"، عبر استخدام أدوات تعتمد على تحليل الصوت، والتعرّف إلى الوجوه، ورصد اللغة العربية، إضافة إلى تطبيقات تعتمد على روبوتات المحادثة، وتظهر محاولة استهداف هذه الوحدة الأهمية المتزايدة للبنية المعلوماتية في (إسرائيل)، في ظل التحول المتسارع نحو الاعتماد على تقنيات الذكاء الاصطناعي في العمليات العسكرية، كما يكتسب هذا الهجوم بُعدا إضافيا في ضوء التعاون القائم بين الوحدة 8200 وعدد من شركات التكنولوجيا الكبرى مثل "مايكروسوفت"، و"غوغل"، و"ميتا"، وهو تعاون يُنظر إليه بوصفه عنصرا ذا حساسية أمنية، وتشير التقديرات إلى أن الهجوم ربما استهدف إضعاف البنية التحتية الرقمية (الإسرائيلية)، أو كشف بعض الأساليب المستخدمة في إدارة العمليات، أو تحقيق نوع من الردع السيبراني المتبادل.

2. الوكالة السيبرانية الوطنية (الإسرائيلية) (INCD)

جرى توحيد الوكالات المختلفة للأمن السيبراني المدني (الإسرائيلية) في كيان واحد يُسمى الوكالة السيبرانية الوطنية (الإسرائيلية) (INCD)، وهي وكالة الأمن القومي والتكنولوجي المسؤولة عن الدفاع عن الفضاء السيبراني الوطني للكيان، وعن إنشاء القوة السيبرانية (الإسرائيلية) وتطوير قدراتها، وتتبع المديرية مباشرة لمكتب رئيس الوزراء الصهيوني، وهنالك تنسيق عالي المستوى بينها وبين أهم مكونات الأمن الصهيوني من وكالات وهي (الشين بيت والموساد ولجنة الطاقة الذرية الإسرائيلية)، والغرض من رفع مستوى التنسيق إظهار مدى أهمية هذه الوكالة لأمن الكيان ولتنظيم مشهد الأمن السيبراني المدني، بناءً عليه، فإن مهامها تتلخص بما ياتي :

أولا: تنسق جوانب الدفاع السيبراني المدني جميعًا، بدءًا من الدفاع العملياتي إلى بناء القدرات التكنولوجية ومقترحات السياسة.

ثانيا: وكجزء من أدوارها، تعمل الوكالة على تطوير الحلول السيبرانية المبتكرة والحلول التكنولوجية الاستشرافية،

ثالثا: صوغ الإستراتيجيات والسياسات على الساحتين الوطنية والدولية،

رابعا: تطوير القوى العاملة السيبرانية.

ويبدو أن هناك ميلاً نحو مركزية مشهد الأمن السيبراني (الإسرائيلي) الذي كان لا مركزيا في ما سبق، ويكتمل الأمن السيبراني المدني بالدفاع السيبراني العسكري، الذي يقع تحت رعاية الجيش الصهيوني، وتتولى الوحدة 8200 في الجيش وكما بينا في أعلاه مسؤولية المهمات الهجومية، بينما يركز (فيلق المعالجة عن بعد C41) على التدابير الدفاعية .

3. مديرية C41، المعروفة أيضًا باسم C41 Corps، أي فيلق المعالجة من بعد

تتمثل مهمتها في حماية البنية التحتية للاتصالات (الإسرائيلية) وأنظمة المعالجة في الجيش الإسرائيلي، علاوة على ذلك، تدعم المديرية تطوير "التكنولوجيا السيبرانية ذات الصلة"، وهي تتبع من الناحية التنظيمية مديرية خدمات الحاسوب المعروفة أيضًا باسم Aka Atak، وقد تحولت مهمة C41 في الدفاع السيبراني نحو نهج "الدفاع النشط"، الذي يستلزم مجموعة من الهجمات الردعية والاستباقية.

4.القبة السيبرانية (Cyber Dome):

تهدف إلى رصد الهجمات السيبرانية المحتملة والدفاع عن المرافق الحيوية للكيان، ولا سيما تلك التي تدار إلكترونيا، لغرض توفير الحماية المطلوبة لمختلف المرافق (الإسرائيلية)، من خلال آليات استباقية حول سبل السيطرة على استخدام الإنترنت على نطاق واسع في (إسرائيل) في مجالات الحياة جميعا.

5. برامج تنمية المواهب في المجال السيبراني

لا يمكن إنكار أن (اسرائيل) قد قطع أشواط طويلة في مجال الحرب السيبرانية واكتسبت اعترافا عالميا بقدراتها السيبرانية، يمكن أن يُعزى جزء كبير من نجاحه إلى برامج تنمية المواهب وهي بمنزلة خط تجميع للمحاربين السيبرانية الموهوبين.

أولا: برنامج "ما غشيميم" (Magshimim) : وهو من أكثر البرامج أهمية في مجال الحرب السيبرانية والأمن السيبراني في (اسرائيل) والذي يركز على تعليم الأمن السيبراني وتطوير القدرات للأفراد الموهوبين في مجال الحرب السيبرانية، ويهدف إلى تحديد الطلاب المتميزين و الذين لديهم شغف بالتكنولوجيا والأمن السيبراني، ورفع قدراتهم من خلال التدريب والإرشاد المتخصص وتهيئتهم للعمل في مجال الأمن السيبراني، بما في ذلك الانضمام إلى وحدات النخبة السيبرانية في الجيش (الإسرائيلي).

ثانيا: برنامج "أتوداي" (Atudai) للمنح الدراسية الأكاديمية: وهو مخصص لدعم الطلاب المتفوقين الذين يسعون للحصول على درجات علمية متعلقة بالأمن السيبراني في الجامعات والكليات (الإسرائيلية) وهو يقدم الدعم المالي للأفراد الموهوبين، ما يمكنهم من التركيز على دراساتهم من دون تحمل عبء القيود المالية، ويهدف إلى جذب الأفراد الموهوبين والاحتفاظ بهم في مجال الأمن السيبراني، وتعزيز القدرات السيبرانية للدولة.

ثالثا: برنامج "موفيت" (Mofet)، أو ما يسمى "سايبر غيرلز" (Cyber Girls)، وهو برنامج التنمية المواهب مصمم خصيصًا للنساء في مجال الأمن السيبراني (107)

رابعا. وبرنامج "ماموريوت" (Mamriot) : الذي يركز على تدريب المدافعين السيبرانيين المتخصصين في مجال حماية البنية التحتية الحيوية، وهو يحدد الأفراد الموهوبين الذين لديهم اهتمام خاص بحماية الأنظمة الحيوية، ويوفر لهم تدريبا متخصصا في مجالات مثل أمن أنظمة التحكم الصناعية (ICS) وحماية الشبكات والاستجابة للحوادث (109))

خامسا: وبرنامج "أوديسي " (Odyssey): يهدف إلى تعزيز التعاون بين الجيش الصهيوني والمؤسسات الأكاديمية في مجال الأمن السيبراني، وبموجب هذا البرنامج، يشارك طلاب مختارون من الجامعات في مشاريع بحثية، ويعملون جنبا إلى جنب مع وحدات الإنترنت التابعة للجيش (الإسرائيلي)، بما يعزز تبادل المعرفة، ويسمح للطلاب باكتساب خبرة واقعية في عمليات الأمن السيبراني، ويسهل تطوير حلول مبتكرة للتحديات السيبرانية الناشئة.

سادسا: برنامج "غشارين" (Gsharin): هو برنامج لتنمية المواهب يركز على جذب الأفراد ذوي القدرة الفريدة على الأمن السيبراني ورعايتهم،ويبحث عن أفراد يتمتعون بمهارات استثنائية في حل المشكلات والإبداع والفهم العميق للتكنولوجيا، من خلال التدريب والإرشاد المتخصص في صناعة الأمن السيبراني، والمساهمة في تطوير القوى العاملة السيبرانية ذات المهارات العالية والمتنوعة.

موقع (اسرائيل) عالميا في مؤشرات التحول الرقمي

وفقا لمؤشر جودة الحياة الرقمية المنشور في عام 2024، حصل الكيان على أعلى الدرجات بين البلدان جميعا (0.76) من (1) حيث احرز المرتبة الرابعة لسنتين على التوالي، وهو الترتيب الذي يفحص بعض الميزات الرقمية في كل دولة وفق مؤشرات تصل إلى 95 مؤشر، بما في ذلك جودة خدمات الإنترنت والقدرة على تحمل تكاليفها، وفي عام 2021، صنف المعهد الدولي للدراسات الإستراتيجية (IISS) أفضل القوى السيبرانية في العالم إلى ثلاثة مستويات، بناءً على قدراتهاإ وقد وضع المعهد الولايات المتحدة وحدها في المستوى الأول، وجاءت (إسرائيل) في المستوى الثاني إلى جانب أستراليا والمملكة المتحدة وكندا والصين وفرنسا وروسيا، بحسب مؤشر الأمن السيبراني لعام 2020، الصادر عن الاتحاد الدولي للاتصالات (ITU)؛ فقد أشير فيه إلى الدور الذي تؤديه صناعة الأمن السيبراني الناضجة والمتنوعة في تعزيز القدرات السيبرانية للدول، وإلى دول رائدة أنشأت قطاعات قوية في صناعة الأمن السيبراني، مثل الولايات المتحدة الأميركية التي حازت المرتبة الأولى، والمملكة المتحدة التي حازت المرتبة الثانية، وأستراليا المرتبة الثانية عشرة و(اسرائيل) المرتبة السادسة والثلاثين.

القدرات السيبرانية الإيرانية

ركزت الدوائر المتخصصة بتطوير التقنيات الحديثة فيالجمهورية الإسلامية في ايران كثيرا على المفاصل المتعلقة بالحرب السيبرانية والأمن السيبراني، حيث تعد إيران منأكثر الدول ضمن منطقة الشرق الأوسط إلى جانب (اسرائيل) إهتمامًا بالملف السيبراني، إذ شهدت في السنوات العشرين الأخيرة تطورات ملحوظة في مجال القدرات السيبرانية؛ فقدراتها السيبرانية أصبحت محورًا رئيسًا في سياستها الوطنية والإقليمية، وتحتل مكانة بارزة في مشهد الأمن السيبراني العالمي، ويجمع مجالها السيبراني بين القدرات الهجومية والقدرات الدفاعية، ما يساهم في تعزيز قدرتها على الاستجابة للتحديات، وتحقيق أهدافها الوطنية والإقليمية فضلا عن تطوير القدرات الخلاقة للعناصر الشبابية المتميزة في هذا المجال.

تطور القدرات الإيرانية في مجال الحرب السيبرانية

بعد عام 1988 عملت الجمهورية الاسلامية بكل جهد على الاستفادة من تجربة الحرب مع العراق ورغم دخولها في أتون حصار جائر من قبل الولايات المتحدة الأمريكية إلا أنها استمرت وبنشاط مكثف في تطوير قدراتها الهجومية الدفاعية في مجال الحرب السيبرانية لاسيما بعد تعرضها للعديد من الهجمات السيبرانية من قبل (اسرائيل) والدوائر الاستخبارية الأمريكية، تمتلك إيران بالوقت الحاضر قدرات عسكرية غير متماثلة، أو ما يعرف بالقدرات السيبرانية للتكنولوجيا العسكرية المنخفضة التكلفة، وذلك لموازنة قوى خصومها العسكرية والتكنولوجية لاسيما (اسرائيل) على مستوى الجوار الإقليمي، أو الولايات المتحدة على المستوى الدولي.

وعلى الرغم من أن الحصار المفروض والعزلة الدولية المفروضة على الجمهورية الاسلامية بفعل العقوبات الدولية، قد حدت من قدرتها على شراء تكنولوجيا متقدمة في المجالات السيبرانية أو على تطوير تقنيات متقدمةكهذه، فإن ذلك لم يمنعها من امتلاك قدرة سيبرانية طورت وطنيا ومن قبل كوادر إيرانية متخصصة، أتاحت لها شن عدد من الهجمات وعمليات التجسس على خصومها، وقد اعتمدت في عقيدتها للأمن السيبراني على شبكة متطورة من المؤسسات التعليمية والبحثية، إضافة إلى بلورة إستراتيجية وتكتيك خاصين بها يجمعان بين بناء الهياكل المؤسساتية الرسمية القادرة على تحقيق الأهداف المرسومة وبين هياكل أخرى مكملة إلا أنها ليست ذات طابع رسمي.

تمكنت آلة الحرب السيبرانية الإيرانية طوال العقدين الماضيين من توظيف واستخدام التقنيات السيبرانية الجديدة للوقوف بوجه المنافسين والأعداء وفي مقدمتهم (اسرائيل) و الولايات المتحدة، وكذلك في الرد على الهجمات السيبرانية التي تتعرض لها، ومنذ هجوم "ستكسنت" ضد المنشآت النووية الإيرانية في عام 2010 المشار اليه آنفاء وهو الهجوم الذي نسب في ذلك الوقت إلى تعاون مشترك بين الموساد (الإسرائيلي) و وكالة ال CIAالأمريكية، مما دفع إيران للاستثمار في التقنيات السيبرانية "المقابلة ذات الطابع الهجومي، وعلى هذا النحو أولت إيران أهمية بالغة في خلق و تطوير صناعة سيبرانية وطنية وبالفعل فقد نجحت في الهجوم بفيروس "شمعون" ضد شركة "أرامكو" الأمريكية في السعودية في عام 2012، وكذلك في حملة التجسس السيبراني فوكس كيتن" (Fox Kitten) المستمرة ضد الولايات المتحدة و(إسرائيل).

الإستراتيجية الإيرانية للحرب السيبرانية

ما انفك النشاط السيبراني الإيراني يتزايد؛ فمنذ أواخر نيسان 2020، استهدفت إيران منشأة توزيع مياه (إسرائيلية) بهجوم سيبراني يهدف إلى زيادة مستويات الكلور في إمدادات المياه إلى مستويات خطرة، وقد جرى اعتراض الهجوم في وقت مبكر، ما أدى إلى الحد الأدنى من الأضرار الطويلة الأمد، ولكن بعد بضعة أسابيع، وبالتحديد في 9 أيار 2020، ردت (إسرائيل) بهجوم سيبراني على ميناء الشهيد رجائي الإيراني بالقرب من مضيق هرمز إن هذا التبادل الأخير للهجمات يمثل حقبة سيبرانية جديدة لأسباب متعددة؛ فقد كانت الهجمات أكثر علانية من العمليات السرية السابقة، وعلى الرغم من أن الهجمات تجاوزت الخط الأحمر " من خلال استهداف البنية التحتية المدنية، فإنها تسببت في أضرار مادية، إضافة إلى ذلك، يمثل التبادل مخططا محتملا للردع السيبراني في المستقبل.

إن إدراك إيران ما يوفره البعد السيبراني من قدرات، خصوصا بعد تعرض منشآتها النووية للهجمات السيبرانية في عام 2010 وتكرار ذلك في الحرب التي دارت للفترة من 13 حزيران وحتى 24 حزيران من هذا العام، دفعها إلى الدخول في معترك المنافسة السيبرانية، للحصول على المعرفة وتوظيف الفضاءالسيبراني في تعزيز قدراتها

السيبرانية وقوتها الاقتصادية، وذلك عبر اعتمادها إستراتيجية متطورة مبنية على أساس القدرات الوطنية المتيسرة دون الحاجة إلى الاستعانة بمتطلبات أو خبرات أجنبية، هذه الإستراتيجية أخذت بعين الاعتبار الوضع السياسي العام على مستوى العالم والأزمة الاقتصادية التي تعاني منها بسبب الحصار الاقتصادي الأمريكي والعقوبات المتوالية على أفرادها ومصالحها الاقتصادية، إذ إنتلك العقبات تمنعها إلى حد كبير من الحصول على الأسلحة أو المعدات أو التجهيزات التي تدخل ضمن منظومات الحرب السيبرانية والتي فرضت بموجب قرار حظر الأسلحة الذي فرضته الأمم المتحدة، ولكي تواصل الجمهورية الاسلامية الضغط على منافسيها على الرغم من هذه القيود اعتمدت على وسائل أقل تنظيمًا وغير حركية غالبيتها تعتمد على ما يمكن الحصول عليه من داخل إيران، وكذلك أخذت هذه الإستراتيجية بعين الاعتبار لتحقيق أهدافها من الخارج بأسلوب إدامة صراعات منخفضة المستوى ولفترات طويلة من الزمن، بتنفيذ هجمات سيبرانية ذات تأثير مباشر إلا أنها ليست ذات صدى إعلامي واسع.

الاستثمار في مجال الحرب السيبرانية

أدركت إيران أهمية الاستثمار في القدرات السيبرانية، ولا سيما أن الحالة الرقمية المتعلقة باستخدام الإنترنت تبدو مرتفعة؛ إذ تشير الاحصائيات المتيسرة بشأن اعتماد التقنية الرقمية في إيران واستخدامها في بداية عام 2023، إلى أن هناك نحو 71.56 مليون مستخدم للإنترنت في إيران حتى أيلول 2023؛ إذ بلغت نسبة انتشار الإنترنت 80.25 في المئة، وما مجموعه 126.9 مليون اتصال هاتفي خلوي نشط في إيران في بداية عام 2023، أي ما يعادل 142.8 في المئة من إجمالي السكان البالغ نحو 88.84 مليون نسمة في كانون الثاني 2023.

الجدير بالذكر أن على الرغم من ارتفاع نسبة الإيرانيين النشطين في الفضاء السيبراني من خلال الاتصال بشبكة الإنترنت، فإن الدولة في إيران تسيطر على الإنترنت من خلال بسط هيمنتها على الشركات الكبرى، خصوصا شركة TCI التي يجري من خلالها الاتصال بالعالم الخارجي، وهي تسيطر على المنافذ الدولية والكابلات البحرية كافة، كما أن الدولة تفرض رقابة شديدة على الإنترنت، وتحجب كثيرا من المواقع، ولا سيما مواقع التواصل الاجتماعي المنافية لطبيعة المجتمع الإيراني المحافظ وكذلك المواقع المتخصصة بالحريض للعنف الديني والكراهية أو المواقع التي تدار من داخل (اسرائيل) والموجهة للشعب الإيراني، فضلا عن ذلك فان هنالك دوافع مختلفة إما سياسية وإما دينية هي التي تجبر الحكومة الإيرانية على حجب تلك المواقع لاسيما تلك المواقع التي يستخدمها الناشطون السياسيون في المعارضة الإيرانية، ومن أجل فرض سيطرة أكبر، تقوم الحكومة، ومن خلال مجموعة من المؤسسات التي أنشأتها لهذه الغاية، بإنشاء ما أطلقت عليه صفة "الإنترنت الحلال"، إذ يجري إنشاء شبكة إنترنت محلية موازية للإنترنت العالمية، لاستضافة المواقع الإيرانية كافة على هذه الشبكة، وكذلك إنشاء نسخ محلية من مواقع التواصل الاجتماعي، تكون تحت الرقابة المستمرة من السلطات.

القدرات الإيرانية في مجال الحرب السيبرانية

تمتلك إيران العديد من المؤسسات والأذرع التي تعزز من قدراتها السيبرانية تؤازرها إستراتيجية سيبرانية لها أبعاد هجومية، وأخرى دفاعية، وفق الآتي:

1. المجلس الأعلى للفضاء السيبراني (SCC)

هو هيئة حكومية في إيران تمثل الجهود والسياسات الوطنية للأمن السيبراني تأسس المجلس في عام 2012 بوصفه هيئة تنظيمية رئيسة، تسعى للسيطرة على الأمور المتعلقة بالإنترنت والفضاء السيبراني في إيران وهو برئاسة الرئيس الإيراني، ويضم مجموعة من المسؤولين الحكوميين والخبراء في مجال الأمن السيبراني، ويهدف إلى تنسيق العمليات السيبرانية الهجومية والدفاعية، وتطوير السياسات والإجراءات الوطنية للأمن السيبراني، وحماية البنية التحتية الحيوية للبلاد من التهديدات السيبرانية، ويُعد من أهم الهيئات التي تعنى في إيران بمجال الأمن السيبراني ومراقبة الإنترنت، ويؤدي دورا حاسما في تحديد سياستها وإستراتيجيتها في هذا السياق .

2. قوات الباسيج السيبراني (مجلس الباسيج السيبراني)

يتركز هدفها بالدرجة الأولى على تنظيم دعاية موالية لإيران في المجال السيبراني، وتطوير قدرات متقدمة في هذا المجال، والدفاع عن رموز الدولة ضد المعارضين، سواء في شبكات التواصل الاجتماعي أو في المدونات الإلكترونية، وقد حصلت قوات الباسيج على دور مهم في المجال السيبراني للحرب الناعمة الإيرانية، وهي تقوم بهجمات سيبرانية أقل تطورًا، حيث إنها تضم عناصر غير محترفين يعملون تحت إشراف خبراء في الحرس الثوري يطلق عليهم اسم "كوماندوس الحرب السيبرانية"، مثل عمليات التسلل واختراق حسابات البريد الإلكتروني والمواقع الإلكترونية للناشطين والمعارضة السياسية، كما تعمل قوات الباسيج على تعزيز حملات التأثير من خلال نشر محتوى عبر الإنترنت يتماشى مع قيم الثورة الإسلامية.

3. المركز الوطني للفضاء السيبراني

هو تابع للمجلس الأعلى للفضاء السيبراني وتهتم لجنة التنسيق الوطنية فيه إلى حد كبير بمحتوى المعلومات وتطوير ضوابط أمن الإنترنت الداخلية.

4. فيلق الحرس الثوري الإسلامي فرع من القوات المسلحة الإيرانية

يشرف على الأنشطة السيبرانية الهجومية، وتتبعه كذلك منظمة الحرب السيبرانية والدفاع السيبراني، التي توفر دورات تدريبية في مجال الدفاعات السيبرانية، وتمنع الوصول إلى المحتوى والاتصالات عبر الإنترنت مع مراقبة هذه الاتصالات.

5. وزارة الاستخبارات والأمن

انشأت لمجابهة عمل وكالة الأمن القومي الأميركية والموساد داخل إيران وخارجها، فإن هذه الوزارة مسؤولة عن استخبارات الإشارات وجمع المعلومات من الاتصالات الإلكترونية.

6. الجيش السيبراني الإيراني

يتكون من مجموعة متخصصين في تكنولوجيا المعلومات ومتسللين محترفين ومن ذوي المهارة العالية، وهو غير مرتبط بالحرس الثوري الإيراني مباشرة، لكن مسؤولي الحكومة الإيرانية يشيرون إلى استخدامه في اختراق "مواقع العدو"، وتحويل حركة المرور في الإنترنت، واختراق مواقع وسائل الإعلام الحكومية الأجنبية ومنصات التواصل الاجتماعي.

7. المنظمة الوطنية للدفاع السلبي

هي منظمة سايبر للنخبة، تهدف إلى نشر المصالح الإيرانية، وتنظيم الوسائل غير الفتاكة"، بما في ذلك الأعمال النفسية واستخدام القنوات الإعلامية.

8. قيادة الدفاع السيبراني

تُعرف هذه المجموعة باسم المقر السيبراني في الجيش الإيراني أيضًا، وتقوم بعمليات هجومية سيبرانية، وتطوير إستراتيجيات ضد تهديدات الفضاء السيبراني، جنبا إلى جنب مع مجلس الباسيج السيبراني، تتألف على نحو رئيس من أفراد عسكريين، وتخضع لإشراف هيئة الأركان العامة للقوات المسلحة.

9. مركز أمن المعلومات

يعمل تحت سلطة وزارة الاتصالات وتكنولوجيا المعلومات، ويتمثل دوره الأساسي في الاستجابة الأولى للطوارئ في حالة وقوع هجمات سيبرانية.

تسعى إيران إلى إعادة تشكيل قوتها من خلال الاستفادة من مجالها السيبراني عبر أبعاده الدفاعية والهجومية ؛ إذ وفرت القدرات السيبرانية الهجومية الإيرانية خيارًا منخفض التكلفة لردع التهديدات الخارجية، وباتت إيران من أكثر الدول تقدمًا من ناحية الإمكانية السيبرانية؛ فقد صعدت بحسب مؤشر مركز بيلفر، من المركز 22 إلى المركز العاشر في عام 2024، وانتقل تصنيف قدراتها من المركز 28 إلى المركز 15 بسبب الزيادات في درجاتها التدميرية والمراقبة، وإلى المركز الثالث بحسب تقويم القدرة المالية، بناءً عليه، أصبحت إيران تمتلك القدرات السيبرانية المدعومة بتطبيقات الذكاء الاصطناعي، مثل الطائرات المسيرة، لتعزيز نفوذها الإقليمي ودعم حلفائها ضمن "محور المقاومة".

الصراع الأخير والاستخدام المباشر للحرب السيبرانية

كان من المتوقّع أن تحظى الحرب السيبرانية بحيّزٍ كافٍ من المشاركة في هذه الحرب، رغم قصر مدّتها التي لم تتجاوز اثني عشر يومًا، إذ سخّر (اسرائيل) كل إمكاناته في هذا المجال سعيًا للسيطرة على الفضاء السيبراني، خلال فترة الصراع ورغم كل الإمكانيات التي سخرت فضلا عن ما قدمته آلة الحرب السيبرانية الأمريكية للكيان، فإنه لم يستطع تحيق ما كان يبتغيه بالشكل الذي خطط له بالمقابل فإن إيران استطاعت أن تحقق نتائج أكثر تأثير في هذا الجانب ومع ذلك فإن أدوات الحرب السيبرانية التي استخدمت أثناء هذه الحرب من كلا الطرفين تُنبِئ بأن المستقبل سيكون لمن يمتلك القدرات الأكثر تأثير في مجال حروب الفضاء السيبراني.

فعاليات أدوات الحرب السيبرانية الإيرانية خلال المواجهة الأخيرة

أولا: جرى العمل على استغلال القدرات السيبرانية بوصفها وسيلة لجمع المعلومات الاستخباراتية حول أهداف حيوية تخدم مصالحها في صراعها مع الكيان، بدلا من التركيز على الهجمات التخريبية المباشرة ضد البنية التحتية الرقمية الإسرائيليةإ وقد برز هذا التوجه بوضوح بعد العملية العسكرية (الإسرائيلية) في منتصف حزيران 2025، حيث تحول الفضاء الرقمي إلى ساحة موازية للصراع.

ثانيا: شنت إيران سلسلة من الهجمات الإلكترونية المركزة من خلال مجموعات مرتبطة بـ"الحرس الثوري"، أبرزها مجموعة "سايبر أفينجرز"، التي عززت نشاطها بالتزامن مع مجموعات إلكترونية أخرى موالية لطهران.

ثالثا: استهدفت هذه العمليات بنى تحتية رقمية (إسرائيلية) حيوية، بما في ذلك أنظمة البث الإذاعي والخوادم الحكومية، حيث استطاعت تعطيل محطات إذاعية إسرائيلية مؤقت, والغالبية العظمى من وسائل الانذار المبكر.

رابعا: توسيع نطاق التهديدات ليشمل دولا أخرى في المنطقة، حيث وجهت بعض المجموعات تحذيرات واضحة إلى الأردن والسعودية، دعت فيها إلى عدم تقديم أي شكل من أشكال الدعم للكيان، مع تهديد صريح باستهداف المصالح الرقمية للبلدين في حال استمرار دعمهما للكيان الصهيوني، وفقا لرسائل نشرت عبر قنوات اتصال مشفرة.

خامسا. وثقت تقارير أمنية إرسال رسائل زائفة إلى آلاف المواطنين الإسرائيليين، احتوت على تحذيرات كاذبة من أزمات وشيكة، مثل نقص الوقود أو وقوع تفجيرات، وتم تصميمها لتبدو كأنها صادرة رسميا عن قيادة الجبهة الداخلية للجيش الصهيوني.

سادسا: في تطور غير مسبوق، أعلنت السلطات الصهيونية أن الجمهورية الاسلامية نجحت في اختراق كاميرات مراقبة خاصة داخل الكيان، في محاولة لجمع معلومات آنية عن مواقع سقوط الصواريخ وتحسين دقة الضربات المستقبلية.

سابعا: في ظل التصاعد الحاد في الهجمات السيبرانية المتبادلة بين إيران والكيان، اتخذت طهران إجراءات غير

مسبوقة بقطع الاتصال بالإنترنت العالمي عن أراضيها يوم الثلاثاء 18 حزيران تحسبا لأي اختراق أو محاولة لتمكين العدو من الوصول الى مواقع او اشخاص مخطط لاستهدافهم مسبقا.

ثامنا: سجلت تقارير أمنية ارتفاعا بنسبة 700% في الهجمات السيبرانية ضد أهداف الصهيونية خلال الأيام من 13 حزيران وحتى 24 حزيران 2025، نفذتها مجموعات إيرانية باستخدام أساليب متطورة تتراوح بين هجمات حجب الخدمة واختراق الخوادم.

تاسعا: أعاد الهجوم الإيراني الصاروخي على مركز "غاف يام نيغيف" التكنولوجي في بئر السبع، الذي استهدف منشآت عسكرية وسيبرانية تضم مقرا لشركة "مايكروسوفت"، تسليط الضوء على التحول الخطير لدور الشركة التكنولوجية العملاقة من مزود خدمات تقنية إلى شريك فعلي في الحرب الدائرة.

عاشرا: في تطور لافت ضمن المشهد المتصاعد للحرب السيبرانية بين إيران و(إسرائيل)، سُجّلت محاولة إيرانية لاستهداف الوحدة 8200، وهي إحدى أبرز وحدات الاستخبارات التقنية في الجيش الصهيوني، وتُعد هذه الوحدة مسؤولة عن تطوير وتنفيذ عمليات سيبرانية متقدمة، فضلا عن دمج تقنيات الذكاء الاصطناعي في التحليل الاستخباراتي واتخاذ القرار العسكري.

فعاليات (اسرائيل) في مجال الحرب السيبرانية خلال المواجهة الاخيرة

أولا: أعلنت مجموعة قرصنة معروفة باسم "Predatory Sparrow" والمشتبه في صلتها ب(اسرائيل) مسؤوليتها عن تعطيل خدمات "بنك سبه" الإيراني الحكومي، في هجوم وصفته بالرد على دعم البنك للحرس الثوري.

ثانيا: شهدت إيران في 17حزيران 2025 هجوما سيبرانيا واسعا نفذته مجموعة تطلق على نفسها اسم "الغراب المفترس"، وهي جهة "هاكرز" تُعرف بتأييدها للكيان الصهيوني.

ثالثا: أعلن عن تنفيذ هجوم آخر استهدف بورصة "نوبتيكس"، وهي منصة لتداول العملات الرقمية تُعد من الأكبر في إيران، ووفقا لما نشرته تقارير صحفية، فقد تعرضت لاختراق إلكتروني أدى إلى سرقة ما يعادل 90 مليون دولار، مما دفعها إلى تعليق خدماتها كإجراء احترازي.

رابعا: نفذ الكيان من خلال وكالة الموساد عملية معقدة تضمنت استخدام شبكة من الطائرات المسيّرة والصواريخ الدقيقة، تم تهريبها وتخزينها داخل الأراضي الإيرانية في إطار خطة طويلة الأمد جرى تدريب عناصر جندت لصالح الكيان لاستخدامها.

الخلاصة

نجح الطرفين المتصارعين في تنفيذ هجمات إلكترونية استهدفت منشآت حيوية داخل إيران وكذلك داخل الكيان، من بينها منشآت نووية ومؤسسات مالية ومراكز بحوث ومطارات، وتكمن أهمية هذه الهجمات في قدرتها

على إحداث خلل واسع في البنية التحتية من الداخل، دون الحاجة إلى تحريك وحدات عسكرية تقليدية من قبل طرفي النزاع، مما يعكس توجها متزايدا نحو توظيف أدوات الحرب السيبرانية في تحقيق أهداف إستراتيجية بأقل تكلفة ميدانية ممكنة، كما شملت الهجمات السيبرانية للطرفين أيضا وسائل تهدف لجمع معلومات استخباراتية حيوية تتعلق بالبرنامج النووي لكليهما، وقد أظهرت إيران قدرتها على شن هجمات واسعة النطاق على الأنظمة المصرفية والتجارية لتقويض الاستقرار الاقتصادي للكيان المستهدف وهذا ما سعى الكيان أيضا إلى تحقيقه، عليه يمكن القول : إن الهجمات المتبادلة في مستوياتالحرب السيبرانية بين إيران والكيان، ركزتعلى تعزيز قدراتهما الرقمية لضمان التفوق في هذا المجال الحيوي، فبينما يسعى الكيان إلى استخدام التقنيات الحديثة لتحقيق ضربات إستراتيجية دقيقة، فإن الإستراتيجية للحرب السيبرانية الإيرانية تهدف إلى تعزيز قدرتها على الصمود في وجه الهجمات والتوسع في استهداف القطاعات الحيوية للخصم، مما يزيد تعقيد المشهد الأمني في عموم منطقة الشرق الأوسط ويجعل من الصعب التكهن بطبيعة الحروب القادمة ونتائجها في بيئة أمنية استخدمت الفضاء و الحرب السيبرانية والسيطرة الجوية والحرب النفسية بشكل متقن ومتصاعد مستندة الى التطورات التقنية الحديثة التي امتلكها طرفي الصراع.