مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

2026/2/18

إدارة الحرب من الظل: جدلية الاستخبارات والفعل الاستراتيجي في المواجهة الامريكية _ الإسرائيلية مع إيران

د. مهند حميد الراوي

● **ورقة تحليلات**

سلسلة اصدارات مركز البيان للدراسات والتخطيط

إدارة الحرب من الظل: جدلية الاستخبارات والفعل الاستراتيجي في المواجهة الامريكية _الإسرائيلية مع إيران

سلسلة اصدارات مركز البيان للدراسات والتخطيط /قسم الأبحاث / الدراسات الامنية والعسكرية

الاصدار / ورقة تحليلات

الموضوع / شؤون اقليمية ودولية

د. مهند حميد الراوي/ دكتوراه في العلوم السياسية/ الاستراتيجية

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌّ، غيرُ ربحيٍّ، مقرُّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ، ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليلٍ مستقلٍّ، وإيجاد حلول عملية جليّة لقضايا معقدة تهمُّ الحقليْنِ السياسي والأكاديميٍ.

ملحوظة:

لا تعبّر الآراء الواردة في المقال بالضرورة عن اتجاهات يتبناها المركز، وإنّما تعبّر عن رأي كتابِها.

المقدمة

يمثل الصراع الاستخباراتي بين الولايات المتحدة وإسرائيل والجمهورية الإسلامية الإيرانية أحد أكثر الصراعات الاستخباراتية تعقيداً واستمراراً في التاريخ الجيوسياسي الحديث، وقد وُصف هذا الصراع لفترة طويلة بأنه «حرب خفية» تُخاض دون مستوى الصراع العسكري التقليدي. فعلى مدى عقود، دارت المواجهة بين الولايات المتحدة وإسرائيل من جهة وإيران من جهة أخرى في معظمها عبر عمليات سرية وهجمات إلكترونية وصراعات بالوكالة، وظلت المواجهة العسكرية المباشرة محدودة، إذ تجنب الطرفان حرباً واسعة النطاق قد تزعزع استقرار المنطقة، إلا أنها تصاعدت بشكل ملحوظ بين عامي 2024 و2025، لتبلغ ذروتها في مواجهات عسكرية مباشرة. ويُظهر هذا الصراع تحولاً جذرياً في أساليب الحرب الحديثة، حيث يتم دمج التخريب الإلكتروني، والاختراق الاستخباراتي البشري العميق، والاغتيالات المستهدفة بسلاسة مع الضربات العسكرية التقليدية لتحقيق الردع الاستراتيجي وإضعاف قدرات الخصم.

إذ تجدد الصراع بين إيران وإسرائيل والولايات المتحدة في فبراير/شباط 2026، لا سيما بعد أن أشارت الاحتجاجات الإيرانية في العام نفسه إلى استياء واسع النطاق من النظام، إذ تواجه إيران هجمات عسكرية وسيبرانية واستخباراتية أمريكية-إسرائيلية مشتركة ومتزامنة، تتسم بمستويات متعددة من التعقيد والعمق الاستراتيجي، وذلك بعد أن شنت الولايات المتحدة، بالتعاون مع إسرائيل، عملية عسكرية واسعة

النطاق استهدفت مواقع في أنحاء إيران. هذه المرة، صرحت الولايات المتحدة بأن هدفها هو تعطيل البرنامج النووي الإيراني ونزع سلاح قدراتها الصاروخية الباليستية والضغط من أجل تغيير القيادة الحكومية. في اليوم الأول للعمليات، اغتيل المرشد الأعلى علي خامنئي في الضربات الأمريكية-الإسرائيلية.

الحرب السيبرانية والتخريب الرقمي

يشير مفهوم الحرب السيبرانية والتخريب الرقمي ذي البُعد الاستخباراتي إلى استخدام العمليات السيبرانية ليس فقط كأداة تقنية أو عسكرية، بل أيضاً كأداة لجمع المعلومات الاستخباراتية، والقيام بالعمليات السرية، والتعطيل الاستراتيجي في الصراعات بين الدول. وفي سياق التوترات بين الولايات المتحدة وإسرائيل وإيران، أصبحت العمليات السيبرانية عنصراً أساسياً في الحرب الهجينة الحديثة، إذ تتضمن استخدام التقنيات الرقمية لاختراق أنظمة المعلومات الخاصة بدولة أو منظمة، أو تعطيلها، أو تدميرها. وعلى عكس الحروب التقليدية، يمكن تنفيذ العمليات السيبرانية سراً، وعن بُعد، وغالباً دون الكشف عن هوية منفذيها، مما يجعلها خياراً جذاباً للدول التي تسعى إلى إضعاف خصومها دون اللجوء إلى مواجهة عسكرية شاملة.

تتضمن الحرب السيبرانية في هذا السياق بُعداً استخباراتياً هاماً، ما يعني استخدام الأدوات السيبرانية لأغراض ترتبط تقليدياً بأجهزة الاستخبارات. وتشمل هذه الأغراض: التجسس السيبراني، حيث

تشن الدول عمليات اختراق سيبرانية للحصول على معلومات سرية حول القدرات العسكرية وبرامج تطوير الأسلحة النووية والاتصالات الدبلوماسية والديناميكيات السياسية الداخلية، إذ تُمكّن هذه المعلومات الاستخباراتية صانعي القرار من توقع سلوك الخصم بشكل أفضل وتصميم استراتيجيات أكثر فعالية. كما تعمل على تهيئة ساحة المعركة، إذ يمكن استخدام العمليات السيبرانية لتهيئة البيئة العملياتية قبل العمليات العسكرية؛ فمن خلال اختراق شبكات الاتصالات وأنظمة المراقبة أو البنى التحتية للدفاع الجوي، يستطيع المهاجمون السيبرانيون إضعاف القدرة الدفاعية للدولة قبل العمليات التقليدية. فضلاً عن ذلك، تدير العمليات السيبرانية العمليات المعلوماتية والنفسية؛ فقد تستهدف أيضاً منصات الإعلام وقنوات الاتصال الرقمية للتأثير على الرأي العام، ونشر المعلومات المضللة، أو إثارة البلبلة بين السكان والمؤسسات الحكومية.

في ظل الصراع الاستراتيجي بين الولايات المتحدة وإسرائيل وإيران، استُخدمت الحرب السيبرانية لاستهداف الشبكات الحكومية وأنظمة القيادة العسكرية والبنية التحتية للاتصالات والقطاعات المالية والطاقة، إذ تهدف هذه العمليات إلى تقويض قدرة الخصم على تنسيق الدفاع، وإدارة البنية التحتية الحيوية، والحفاظ على الاستقرار السياسي.

اختراق استخباراتي بشري عميق وعمليات مُستهدفة

يُشير دليل الجيش الأمريكي لعمليات مكافحة التمرد إلى أن للاستخبارات والعمليات علاقة ديناميكية، حتى في البيئات المتساهلة حيث تتوفر معلومات كثيرة عن العدو. إذ هناك جانب استخباراتي في جميع العمليات، فالاستخبارات تُوجّه العمليات، والعمليات الناجحة تُولّد معلومات استخباراتية إضافية.[1]

وعليه، لا تزال الاستخبارات تركز على المواضيع نفسها التي لطالما أثارت اهتمامها، ألا وهي نوايا الخصم وقدراته. ومع ذلك، فإن تأثير ثورة المعلومات على السلوك البشري يُلزمها بتحليل الظواهر البشرية العامة التي يتزايد تأثيرها على صنع القرار الاستراتيجي. وقد أوضح كلاوزفيتز مكانة «الشعب» في ثالوث الشعب والجيش والحكومة باعتباره يعبر عن «عنف وكراهية وعداء بدائيين، يُنظر إليهما كقوة طبيعية عمياء». وقد عزز عصر المعلومات بشكل كبير دور الشعب في هذا الثالوث، مما جعل نواياه وقدراته أكثر أهمية، وهذا يتطلب من الاستخبارات التعمق أكثر في العامل البشري لدى عامة الناس لفهمه بشكل أفضل.

ويتطلب «الفهم» في هذا السياق «إدراك وتفسير موقف معين لتوفير السياق والبصيرة والاستشراف اللازمين لاتخاذ قرارات فعالة». وعلى الرغم من عدم اتفاق جميع القادة العسكريين والمحللين على هذا المفهوم الجديد للاستخبارات، إلا أن أهميته تتزايد في جمع

1. The US Army and Marine Corps, Counterinsurgency Field Manual 3-24, (Chicago: The University of Chicago Press, 2007), pp. 117 - 135.

المعلومات الاستخباراتية والتحليل السياسي والاستراتيجي وحتى التكتيكي.[2]

إذ من السمات المميزة للاستراتيجية الإسرائيلية-الأمريكية التغلغل الاستثنائي في جهاز الأمن الداخلي الإيراني. وقد مكّن هذا التفوق الاستخباراتي البشري من تنفيذ عمليات سرية بالغة الدقة في عمق الأراضي الإيرانية، وذلك من خلال التنوع الموجود في إيران. إذ رأى المحللون الإسرائيليون في التنوع العرقي للبلاد فرصةً سانحة، لا سيما وأن نحو 40% من سكان إيران البالغ عددهم 90 مليون نسمة ينتمون إلى أقليات عرقية، كالعرب والأذربيجانيين والبلوش والأكراد وغيرهم. فقد كان الموساد في السابق يعتمد بشكل كبير على الإسرائيليين، أما الاستراتيجية الجديدة فقد قلبت الموازين، إذ أصبح العملاء بشكل متزايد من الإيرانيين والمهاجرين ومواطني الدول السبع المحيطة بإيران. وكان التجنيد يسير على مسارين: فبعض المجندين انضموا للتجسس التقليدي، أي جمع المعلومات ونقلها، بينما كان آخرون على استعداد للذهاب إلى أبعد من ذلك من خلال تنفيذ عمليات اغتيال وتخريب.

في المقابل، وعلى الرغم من القدرات الهجومية المتقدمة لإسرائيل، إلا أن جبهتها الداخلية أثبتت هشاشتها. فقد نجحت إيران، من خلال قوتها الاستخباراتية داخل إسرائيل، في رسم خرائط لمواقع حساسة مثل قاعدة «نيفا تيم» الجوية ومقر الاستخبارات العسكرية غليلوت، والتي استخدمتها لاحقاً لشنّ ضربات انتقامية دقيقة.

2. Carl von Clausewitz, On War, Howard, M. & Paret, Princeton University Press, 1976, p. 101.

كما ظهرت معلومات جديدة بشأن أنشطة المخابرات الإيرانية داخل إسرائيل خلال السنوات الثلاث الماضية. ووفقاً لتقرير نشرته «دروب سايت نيوز»، وصف مسؤولون إيرانيون هذه الأنشطة بأنها «عملية موازية للعملية الإسرائيلية». وتُظهر الوثائق التي تم الحصول عليها، بحسب التقارير، أن وزارة المخابرات الإيرانية استعانت بأفراد مقيمين في إسرائيل لنشر رسائل سياسية في الأماكن العامة، وشملت هذه الرسائل لافتات وملصقات تحمل شعارات سياسية محلية ورموزاً إيرانية مُنمّقة. وفي العامين الماضيين، اعتُقل نحو 30 مواطناً إسرائيلياً بتهم التجسس واستغلال النفوذ داخل إسرائيل لصالح الحكومة الإيرانية.[3]

الأمن النووي: الصراع الاستخباراتي لمنع الوصول إلى حافة القنبلة

في مجال الأمن النووي، يشير مصطلح «حافة القنبلة» أو ما يُعرف بـ»وقت الاختراق» إلى المدة التقديرية التي قد تستغرقها دولة ما لتجميع كمية كافية من المواد الانشطارية المستخدمة في صنع الأسلحة (عادةً اليورانيوم المخصب بنسبة 90% من اليورانيوم-235) لتصنيع جهاز متفجر نووي واحد.

وبقدر تعلق الأمر بإيران، فعلى مدى عقدين من الزمن، كان الهدف الرئيسي للاستخبارات الأمريكية والإسرائيلية هو إطالة هذا الجدول الزمني بشكل مصطنع، وهو ما يُشار إليه غالباً بإبعاد إيران عن «حافة

3. Jeremy Scahill and Murtaza Hussain, Behind the Bombs, New Details Emerge on Iran's Infiltration of Israel, Drop Site News, 2026, https://www.dropsitenews.com/p/iran-ministry-of-intelligence-israel-infiltration-spies?utm_source=publication-search .

القنبلة»، في حين تمثلت استراتيجية إيران في تقليص الوقت اللازم لامتلاك القنبلة باستمرار، مستخدمةً بنيتها التحتية النووية المدنية للوصول إلى وضع «دولة على العتبة». وبحلول أواخر عام 2024، أشارت تقييمات الاستخبارات الأمريكية، بما في ذلك تصريحات مدير وكالة المخابرات المركزية، إلى أن الوقت اللازم لامتلاك إيران للقنبلة قد تقلص إلى ما بين أسبوع إلى أسبوعين فقط.[4]

وعليه، ابتكرت استراتيجية الاستخبارات ضد البرنامج النووي الإيراني استخدام التخريب الإلكتروني لتحقيق تدمير مادي حركي، مما أدى إلى تأخير وقت الاختراق دون إشعال حرب تقليدية. إذ تُعتبر الحملة الاستخباراتية الأمريكية-الإسرائيلية ضد إيران على نطاق واسع واحدة من أهم الأبعاد الاستخباراتية التي ترعاها الدول، إذ شكّل نشر برمجية «ستوكسنت» الخبيثة (حوالي عام 2010) نقطة محورية، حيث تسلل فيروس ستوكسنت إلى الأنظمة المعزولة عن الشبكة في منشأة نطنز للتخصيب تحت الأرض، وقد عدّل بمهارة سرعات دوران أجهزة الطرد المركزي من شركة سيمنز، مما أدى إلى تمزقها، كل ذلك مع تزويد المشغلين الإيرانيين ببيانات خاطئة توحي بأن الأنظمة تعمل بشكل طبيعي.[5] والتي تُعزى—هذه العملية الاستخباراتية—على نطاق واسع إلى برنامج استخباراتي أمريكي-إسرائيلي مشترك «عملية الألعاب الأولمبية»، وكانت لحظة فارقة

4. Obama admin hid intel on Iran's nukes to protect JCPOA - ex-counterspy, (Iran: Iran international, 2024), https://www.iranintl.com/en/202408299915

5. Adam Bensaid, Here's how Israel hacked Iran's nuclear facility, (Turkey: TRT World, 2021), https://www.trtworld.com/article/12758517

في التاريخ العسكري. فقد كانت «ستوكسنت» أول سلاح إلكتروني يحقق تأثيرات حركية مادية، حيث دمّرت ما يقرب من 1000 جهاز طرد مركزي في منشأة نطنز النووية.[6] تشير الدراسات الأكاديمية حول عملية «ستوكسنت» إلى أنها أجبرت العالم على إعادة تقييم مدى ضعف أنظمة التحكم الصناعية المعزولة عن الشبكة. إذ تسللت البرمجية الخبيثة إلى أنظمة التحكم الصناعية في منشأة نطنز لتخصيب اليورانيوم، وتلاعبت بعمليات أجهزة الطرد المركزي، مما أدى إلى إلحاق أضرار مادية بالمعدات النووية. ومنذ ذلك الحين، اتسع نطاق البُعد السيبراني ليتحول إلى صراع ثنائي الاتجاه، حيث تستهدف إسرائيل والولايات المتحدة بشكل روتيني البنية التحتية للموانئ الإيرانية ومصانع الصلب والخدمات اللوجستية العسكرية، في حين شنت وحدات سيبرانية إيرانية هجمات انتقامية باستخدام برامج خبيثة لمسح البيانات، وحاولت اختراق البنية التحتية الحيوية الأمريكية والإسرائيلية. وقد أظهرت هذه الحالة أن الأسلحة السيبرانية قادرة على إحداث تأثيرات استراتيجية تُضاهي الهجمات التقليدية، مما يُشير إلى تحول جوهري في طبيعة الصراع بين الدول.[7] فضلاً عن عملية مداهمة الأرشيف النووي، ففي عام 2018، نجح عملاء الموساد في التسلل إلى مستودع في طهران، واستولوا على نصف طن من

6. Mariusz Antoni Kamiński, Operation “Olympic Games.” Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran’s nuclear program, (Warsaw: War Studies University, 2020), p. 68.
7. Mohanad Salloum, The Code is More Dangerous Than a Bullet: Cyber and Drone Warfare in the Middle East, (Iraq: NIRIJ for Investigative Journalism, 2025).

الوثائق السرية التي تُفصّل أبحاث إيران السابقة في مجال الأسلحة النووية. وقد غيّر هذا الإنجاز الاستخباراتي المشهد الدبلوماسي الدولي بشكل جذري، وبرّر تشديد العقوبات الاقتصادية.[8]

العمليات الاستباقية وتحييد القيادة العليا

في الدراسات الاستراتيجية والاستخباراتية، يُشير البُعد الاستخباراتي لعمليات استهداف القيادات إلى عملية جمع المعلومات الاستخباراتية وتحليلها وتطبيقها عملياً لتحديد مواقع القيادات الرئيسية لدى الخصم، ومراقبتها، واستهدافها. كما أن هذه العمليات نادراً ما تكون عسكرية بحتة، بل تعتمد اعتماداً كبيراً على أجهزة الاستخبارات، وشبكات المراقبة، والعملاء السريين، والقدرات التكنولوجية. وبحسب الدراسات الاستخباراتية، يعتمد نجاح عمليات استهداف القادة على ثلاث وظائف استخباراتية رئيسية:

أولاً: جمع المعلومات الاستخباراتية: تتضمن المرحلة الأولى تحديد موقع القائد المستهدف، وتحركاته، وترتيباته الأمنية، وأنماط اتصالاته، وتشمل هذه المرحلة عادةً عدة تخصصات استخباراتية: (الاستخبارات البشرية: تجنيد المطلعين، أو المخبرين، أو المنشقين من الدائرة المقربة للقيادة، استخبارات الإشارات: اعتراض الاتصالات، مثل الرسائل المشفرة أو الاتصالات عبر الأقمار الصناعية، استخبارات الصور: مراقبة المواقع التي يتردد عليها الهدف بشكل متكرر باستخدام الأقمار الصناعية والطائرات المسيّرة، الاستخبارات السيبرانية: اختراق

8. Betrayal from Within: Inside Israel's Covert War Built on Iranian Dissidents, (Baku: Baku Network, 2025)

الشبكات الرقمية لتتبع التحركات أو الترتيبات الأمنية)، إذ يؤدي دمج هذه المصادر الاستخباراتية إلى تكوين صورة شاملة للاستهداف، وهو أمر بالغ الأهمية لعمليات استهداف الأهداف عالية القيمة.[9]

ثانياً: تحليل المعلومات الاستخباراتية وتحديد الأهداف: فبعد جمع المعلومات الاستخباراتية، يُجري المحللون تحليلاً للأهداف، يشمل ما يلي: (التأكد من هوية الهدف، رسم خريطة لهيكل حماية القيادة، تحديد نقاط الضعف في البيئة الأمنية، تحديد التوقيت الأمثل والأسلوب الأنسب للعملية) إذ في علم الاستخبارات، تُعرف هذه المرحلة غالباً باسم (تطوير الهدف) ضمن دورة الاستخبارات الأوسع، كما يُقيّم المحللون الاستراتيجيون العواقب السياسية والاستراتيجية لاستهداف قائد، بما في ذلك مخاطر التصعيد واحتمالية زعزعة استقرار النظام.[10]

ثالثاً: الدعم الاستخباراتي العملياتي: تتضمن المرحلة الأخيرة دعم الوحدة العملياتية التي تنفذ الضربة أو محاولة الاغتيال، إذ توفر أجهزة الاستخبارات ما يلي: (المراقبة الآنية، بيانات تحديد الموقع الجغرافي، مراقبة الاتصالات، التنسيق العملياتي)، ففي الحروب الحديثة، قد تشمل هذه العمليات قوات خاصة، وطائرات مسيرة، وهجمات إلكترونية، أو عملاء سريين، ويتم تنسيق كل ذلك عبر شبكات استخباراتية[11].

9. Mark M. Lowenthal, Intelligence From Secrets to Policy, (Arlington: Intelligence & Security Academy, LLC, 2025), p.p.21-23.
10. Robert M. Clark, Intelligence Analysis: A Target-Centric Approach, (Canada: CQ Press, 2003).
11. للمزيد يُنظر: أساسيات التحليل الاستخباري، ترجمة: فراس الهورامي، (بغداد: دار شمس الأندلس، 2022)، ص 67.

وهناك العديد من الأهداف الاستراتيجية لاستهداف القيادات، ففي سياق الصراع بين الدول، قد ينظر مجتمع الاستخبارات إلى استهداف القيادات كوسيلة لتحقيق عدة أهداف استراتيجية، منها، تعطيل نظام القيادة والسيطرة لدى العدو وإحداث حالة من عدم الاستقرار السياسي الداخلي في النظام وتقليل قدرة الخصم على تنسيق الردود العسكرية، فضلاً عن إظهار الهيمنة الاستراتيجية والردع، ومع ذلك، فإن مثل هذه العمليات تنطوي على مخاطر استراتيجية جسيمة، بما في ذلك التصعيد، والرد الانتقامي، أو ترسيخ السلطة من قبل قيادات أكثر تطرفاً.

إذ يمثل البُعد الاستخباراتي وراء اغتيال المرشد الأعلى علي خامنئي في 28 شباط/فبراير 2026 أحد أكثر عمليات استهداف الأهداف تعقيداً وأهمية في التاريخ العسكري الحديث. ففي سياق عمليتي «الغضب الملحمي» و«الأسد الهادر»، لم يقتصر دور أجهزة الاستخبارات على دعم الحملة العسكرية فحسب، بل حددت توقيتها وتنفيذها بدقة متناهية. إذ يُعد نموذج «الحدث المُحفّز» في الحملات العسكرية شديدة المركزية اختراقاً استخباراتياً محدداً وحساساً للوقت، يُطلِق عملية أوسع نطاقاً مُخطط لها مُسبقاً.

فقد كانت الاستخبارات هي التي حددت التوقيت، وكان لدى المُخططين الأمريكيين والإسرائيليين الأصول العملياتية (قاذفات بي-2، مجموعات الضربات البحرية، والقوات الجوية الإسرائيلية) مُجهّزة مسبقاً. ومع ذلك، تم اختيار «منتصف الصباح في طهران» لأن

معلومات استخباراتية فورية أكدت وجود خامنئي في مُجمّعه شديد التحصين في منطقة باستور بطهران.

وقد شكّل التعاون بين وكالة الاستخبارات المركزية الأمريكية والموساد الإسرائيلي البعد الأساسي في هذه العملية، مما يعني أن اغتيال رئيس دولة شديد الحراسة أو شخصية بمنزلة المرشد الأعلى الإيراني يتطلب تعاوناً غير مسبوق بين الاستخبارات البشرية (HUMINT) واستخبارات الإشارات (SIGINT). كما أن ذلك يستلزم ما يُعرف بـ»التحقق الفوري»، الذي يتطلب ضرب هدف بهذا الحجم يقيناً مطلقاً. لذلك اضطرت أجهزة الاستخبارات إلى تجاوز أو فك تشفير الاتصالات الإيرانية الآمنة، ومن المرجح أنها اعتمدت على مصادر أرضية للتحقق بصرياً أو إلكترونياً من دخول هذه الشخصيات فعلياً إلى مجمع سعد آباد ومنشآت منطقة باستور قبل إصدار تصريح إطلاق الذخائر.

في المقابل، يُوحي هذا بفشل كبير للاستخبارات المضادة الإيرانية، إذ يُبرز نجاح هذه الضربة انهياراً بنيوياً في الأمن الداخلي الإيراني وبروتوكولات مكافحة التجسس، من خلال اختراق الدائرة المقربة. إن معرفة الولايات المتحدة وإسرائيل بدقة بمواعيد اجتماع المرشد الأعلى وكبار قادة الجيش في مكان واحد يُشير إلى اختراق عميق للقيادات العليا الإيرانية، وهو ما يُعرف بـ»التنبؤ والروتين». إذ تعتمد استراتيجيات استهداف القيادات على رسم خريطة لنمط حياة الخصم. ورغم العمل في ظل حالة تأهب قصوى تحسباً لحرب وشيكة، فشلت القيادة الإيرانية في إخفاء تحركاتها بشكل كافٍ، وفي تفريق قيادتها العليا، والحفاظ على أمن العمليات فيما يتعلق بجداول اجتماعاتها.

البعد الاستخباراتي وتحييد القدرات الاستراتيجية

يمثل البُعد الاستخباراتي لتحييد القدرات الاستراتيجية الإيرانية خلال حرب 2026 تحولاً جذرياً في الحروب الحديثة. فبينما تحقق التدمير الحركي للبنية التحتية النووية والصاروخية الإيرانية من خلال التفوق الجوي، كان أساس الحملة جهداً استخباراتياً ضخماً ومتعدد السنوات لدمج المعلومات. إذ لم تقتصر مهمة الأجهزة الاستخباراتية على تحديد الأهداف فحسب، بل شملت رسم خريطة منهجية، وتفكيك القاعدة الصناعية الدفاعية، والهيكل القيادي لإيران، وذلك من خلال الاستحواذ على الأهداف باستخدام الذكاء الاصطناعي، وما يُعرف في الدراسات الأمنية بـ»حفظ الأهداف".

إن النطاق الهائل لضربات 28 فبراير—التي استهدفت أكثر من 1000 هدف خلال أول 24 ساعة—أصبح ممكناً بفضل تحول جذري في كيفية معالجة المعلومات الاستخباراتية. ويُعد هذا جزءاً مما يُعرف اليوم بـ»الحرب الخوارزمية»، والتي مثّلت المرة الأولى التي تُستخدم فيها أدوات الذكاء الاصطناعي على نطاق واسع كهذا للاستهداف النشط ودعم المعلومات الاستخباراتية. إذ قامت أنظمة الذكاء الاصطناعي بمعالجة كميات هائلة من معلومات الإشارات (SIGINT) ومعلومات القياس والتوقيع (MASINT) وصور الأقمار الصناعية لتحديد مواقع الإطلاق المخفية ومراكز القيادة بسرعة تفوق قدرة المحللين البشريين.[12]

12. FREDERIC LEMIEUX, OPERATION EPIC FURY AND THE ARCHITECTURE OF IRANIAN RETALIATION, (Nicosia Cyprus: Strategy International, 2026), p.5.

من جهة أخرى، يستلزم تحييد القدرات الاستراتيجية استخباراتياً تحديد ما يُعرف بـ»بنك الأهداف». إذ أمضى الجيشان الأمريكي والإسرائيلي شهوراً في بناء بنك أهداف شامل بشكل تعاوني. وقد تطلب ذلك رسم خرائط للعقد المدفونة بعمق لشبكة الخدمات اللوجستية للحرس الثوري، بدءاً من مواقع إنتاج الصواريخ الباليستية في شاهرود، وصولاً إلى بطاريات الدفاع الجوي ومصانع تجميع الطائرات بدون طيار.[13] كما عملت الأجهزة الاستخباراتية على رسم خرائط الأهداف المدفونة في أعماق الأرض من خلال تحييد المنشآت تحت الأرض مثل فوردو ونطنز باستخدام معلومات استخباراتية جيوتقنية دقيقة للغاية. فقد عملت وكالات الاستخبارات على رسم خرائط دقيقة للعمق والتصميم ونقاط الضعف الهيكلية لهذه المخابئ، من أجل نشر قذائف GBU-5**7** الخارقة للدروع بشكل فعال.

فضلاً عن ذلك، شمل الاستهداف الديناميكي للأصول المتحركة تحديات استخباراتية خاصة. إذ بينما يسهل استهداف الأهداف الثابتة كالمنشآت الإنتاجية، يتطلب تحييد تهديد الصواريخ الباليستية تعقب الأصول المتحركة باستخدام القياس عن بُعد في الوقت الفعلي. وتعتمد استراتيجية إيران بشكل كبير على منصات إطلاق الصواريخ المتحركة وأسراب الطائرات المسيّرة المنتشرة، مما يمثل تحدياً استخباراتياً في تحديد مواقع هذه المنصات أثناء انتقالها من

13. Daniel Estrin, Greg Myre, Jane Arraf, Iran’s supreme leader, Ayatollah Ali Khamenei, has been killed, WUNC News, 2026, https://www.wunc.org/2026-02-28/irans-supreme-leader-ayatollah-ali-khamenei-has-been-killed .

مستودعاتها تحت الأرض إلى مواقع الإطلاق.

وقد تطلب التغلب على هذا التحدي الحصول على معلومات استخباراتية آنية، يُرجّح أنها تضمنت دمج مراقبة مستمرة بالطائرات المسيرة وعمليات اختراق إلكترونية لشبكات الدفاع الجوي الإيرانية، مما أدى إلى تدمير ما يقارب 300 منصة إطلاق متنقلة خلال الأيام الأولى من الحرب، وهو ما قلّل بشكل كبير من حجم وابل الصواريخ الإيرانية.[14]

14. Joseph Rodgers and Bailey Schiff, Operation Epic Fury and the Remnants of Iran's Nuclear Program, (Washington: Center for Strategic & International Studies, 2026), https://www.csis.org/analysis/operation-epic-fury-and-remnants-irans-nuclear-program#:~:text=This%20doesn't%20necessarily%20mean,in%20large%2Dscale%20capability%20degradation. .

الخاتمة

يُجسّد البُعد الاستخباراتي للصراع الأمريكي الإسرائيلي مع إيران شكلاً حديثاً من أشكال الحرب المعاصرة، فهو يُثبت أن الاستخبارات لم تعد مجرد عنصر داعم للعمليات العسكرية، بل أصبحت سلاحاً رئيسياً بحد ذاته. فمن خلال مزيج من التخريب الإلكتروني، والاختراق البشري العميق، والضربات العسكرية الدقيقة، تمكنت الولايات المتحدة وإسرائيل من إضعاف القدرات الاستراتيجية الإيرانية بشكل مستمر. في المقابل، يُسلّط هذا الصراع الضوء على هشاشة الأنظمة الاستبدادية المغلقة أمام الاختراق الداخلي، مما يُجبر إيران على الاعتماد على حرب الوكالة غير المتكافئة للحفاظ على نفوذها الإقليمي.

كما أظهرت إدارة هذه الحرب من خلال الظل أن القدرة على الاختراق والتنبؤ ومعالجة البيانات بسرعة تفوق سرعة الخصم لا تقل أهمية عن القوة العسكرية وحدها. فقد استند نجاح العمليات الاستباقية، والقضاء الدقيق على القيادة العليا، والتفكيك المنهجي للبنى التحتية النووية والصاروخية شديدة التحصين، إلى حملة استخباراتية منهجية استمرت لسنوات عديدة. وقد تطلب ذلك توليفاً غير مسبوق بين تحديد الأهداف المدعوم بالذكاء الاصطناعي، واستخبارات الإشارات متعددة المجالات، والاستخبارات البشرية المتعمقة التي استهدفت أكثر المستويات حراسة في إيران.

وعليه، تُظهر المواجهة أن الخط الفاصل بين عمليات الاستخبارات السرية والحملات العسكرية العلنية قد تلاشى بشكل دائم. وقد تحقق تعطيل القدرات الاستراتيجية الإيرانية بشكل استباقي من خلال قدرة الولايات المتحدة وإسرائيل على ارتباك جهاز الأمن العملياتي وصنع القرار للنظام من الداخل قبل إطلاق أولى القذائف. ومع تكيف الجهات الفاعلة، الحكومية وغير الحكومية، مع هذا النموذج الحربي القائم على الاستخبارات، سيعتمد الردع والهيمنة الاستراتيجية في المستقبل بشكل شبه كامل على السيطرة المستمرة وغير المرئية ذات البعد الاستخباراتي على الفضاء المعلوماتي.

لِدولةٍ فاعلةٍ ومجتمعٍ مُشارِك

www.bayancenter.org
info@bayancenter.org