كيف حوّلت "إسرائيل" كاميرات المراقبة بإيران إلى سلاح اغتيال؟

بعد اغتيال عدد من قادة الصف الأول في إيران، انشغل كثيرون بالسؤال عن الكيفية التي تمكنت بها "إسرائيل" من الوصول إلى هذا المستوى من الاختراق داخل دولة مشبعة بالأمن والمراقبة.

وكانت المفارقة الأكثر إثارة أن كاميرات الشوارع التي بُنيت لإحكام القبضة على المجتمع الإيراني، تحولت في زمن الحرب إلى عين استخبارية يُشتبه بأنها ساعدت العدو على التعقب والرصد وتحديد الأهداف.

وتحدثت تقارير غربية، لا سيما من وكالة أسوشييتد برس و"فاينانشال تايمز"، عن اختراق إسرائيلي لشبكة كاميرات المرور في طهران واستخدامها في تعقب حراسات المقرات الحساسة وبناء ملفات رقمية عن تحركاتهم.

فكيف نشأت هذه الشبكة؟ ولماذا كانت قابلة للاختراق؟ وما الذي تكشفه القصة عن الدولة المراقبة حين تنقلب بنيتها الرقمية إلى ضعف إستراتيجي؟

كيف بنت إيران دولة مراقبة؟

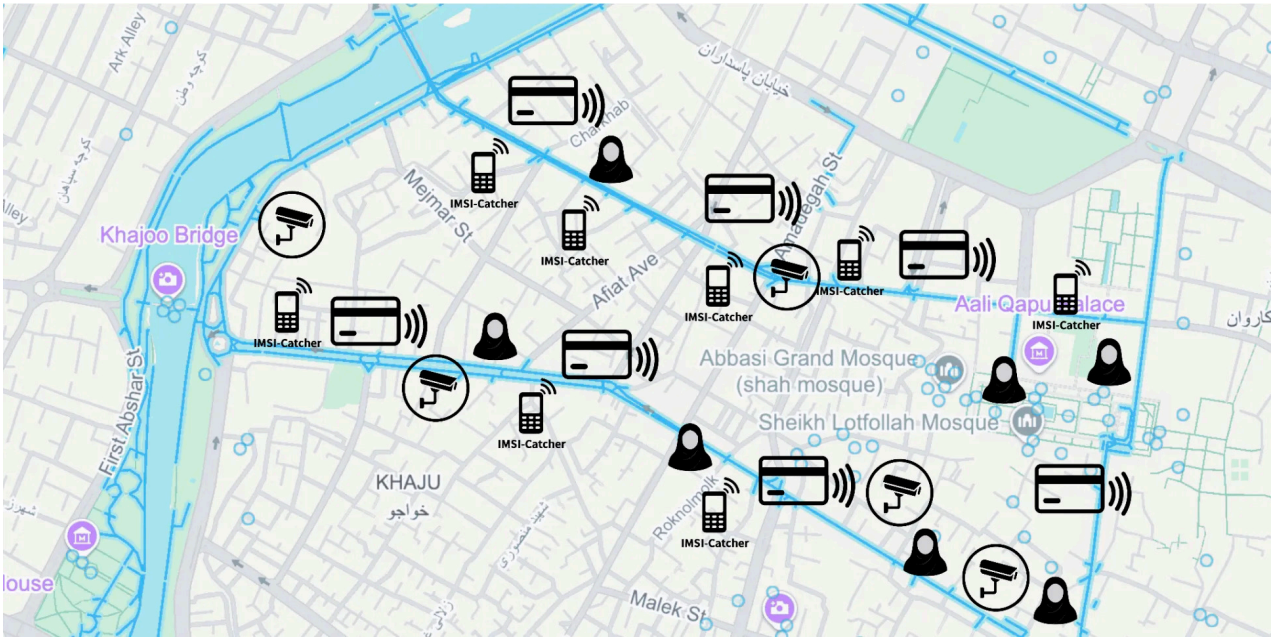
في أعقاب احتجاجات "المرأة، الحياة، الحرية" أواخر 2022 بعد قتل ما تسمى "شرطة الأخلاق" للشابة مهسا أميني (لعدم التزامها بالحجاب الشرعي)، صعدت السلطات الإيرانية مشروع مراقبة رقمي واسع.

وأعلنت الشرطة في أبريل/نيسان 2023 عن تثبيت كاميرات ذكية في الشوارع لإرسال رسائل تحذيرية إلى النساء غير الملتزمات بالحجاب، بهدف "منع المقاومة ضد القانون".

وأوضح تقرير لوكالة رويترز وقتها أن السلطات تخطط لاستخدام تقنية التعرف على الوجوه لمطابقة

الصور مع قاعدة البيانات الوطنية ومعاقبة من يخالف قواعد الحجاب، في ظل غياب قانون لحماية البيانات الشخصية، لكن لم يقتصر هذا التوسع على اللباس.

فقد أشارت تقارير حقوقية إلى أن الحكومة استخدمت الشبكة لتعقب المعارضين، فكانت تجمع بيانات مواقع الهواتف وتتعاون مع تطبيقات التوصيل وتشجع المواطنين على الإبلاغ عبر تطبيق "ناظر" التابع للشرطة والذي يتيح إرسال أرقام لوحات السيارات وعناوين "النساء المخالفات".



خريطة تخطيطية لأدوات المراقبة المستخدمة في المنطقة السياحية في أصفهان، استنادًا إلى معلومات شهود عيان تم تبادلها مع Filterwatch

وهو ما أكده تقرير للأمم المتحدة في مارس/آذار 2025، إذ قال إن إيران تستخدم كاميرات الطرق والدراجات المسيرة وتقنيات التعرف على الوجوه وتطبيق "ناظر" لفرض اللباس الشرعي، وأنها صعدت العقوبات والإقصاء الاجتماعي للمخالفين.

وفي المدن الكبرى أظهرت شاشات مترو مشهد في ديسمبر/كانون الأول 2023 الوجه والعمر والجنس لكل راكب، في مشهد يُظهر الإمكانات الهائلة للذكاء الاصطناعي دون رقابة، ما أثار احتجاجًا داخل المجلس البلدي.

واستعانت الحكومة في بناء هذا النظام بقدرات شركات صينية وفنية من الخارج، إذ ذكرت دراسة لمركز ستيمسون أن ثماني شركات صينية على الأقل تزود إيران بتقنيات التعرف على الوجوه وكاميرات المراقبة.

وبينت أن السلطات استخدمت أجهزة اعتراض الاتصالات ومناطيد وطائرات مسيرة لرصد المحتجين، فيما أرسلت مليون رسالة نصية وغرمت أصحاب السيارات المخالفة للحجاب خلال 2023.

توسع الشبكة وتشتتها على عشرات الآلاف من الكاميرات في المدن والجامعات والطرق السريعة، حول الفضاء المدني الإيراني إلى فضاء مُراقب بشكل مكثف.

كيف انقلبت الكاميرات إلى "بنك أهداف"؟

في مارس/آذار 2026، نشرت وكالة أسوشييتد برس تحقيقًا مستندًا إلى مسؤول استخباراتي وشخص

مطلع، أفاد بأن "تل أبيب" اخترقت معظم كاميرات المرور في طهران ونقلت بياناتها إلى خوادم في "إسرائيل"، واستخدمت الذكاء الاصطناعي لبناء "أنماط حياة" للحراسات الشخصية.

كانت أحد هذه الكاميرات بزاوية تشاهد السيارات التي يركنها حراس القادة قرب المجمعات الأمنية، فعرف الإسرائيليون عناوينهم ومساراتهم وأوقات حمايتهم. وفق التقرير، سرّع المخططون عملية الاغتيال عندما رصدت الكاميرات وصول المسؤولين إلى مقر القيادة، وجرى إقفال أجهزة الاتصال المحمولة لإحكام التنفيذ.

لم تكن هذه الرواية هي الأولى من نوعها، فقد نقلت "فاينانشال تايمز" عن مسؤولين إسرائيليين أن وحدة 8200 الاستخباراتية الإسرائيلية تمكنت من اختراق شبكة الكاميرات قبل سنوات.

وأوضحت أنها استخدمت كاميرا في شارع باستور لرصد أماكن توقف سيارات حراس المرشد الأعلى السابق علي خامنئي وبناء ملفات لأسماء وعناوين وسلوكيات طاقم الحماية، مستعينة بخوارزميات متقدمة ونماذج مسارات الحركة.

كما أشارت إلى أن "تل أبيب" وواشنطن عطّلتا أبراج الهواتف المحمولة قرب الموقع يوم اغتيال خامنئي لمنع التحذيرات. وأعادت صحيفة "تايمز أوف إسرائيل" سرد الرواية وأكدت عنصر تحليل البيانات عبر الذكاء الاصطناعي.

وانتقد نواب إيرانيون أداء وزارة الاتصالات وألمح عضو البرلمان محمود نبويان، إلى أن "جميع كاميرات تقاطع الطرق بيد إسرائيل"، ما يُعد إقرارًا ضمنيًا بالمشكلة. وبدورها، لم تقدم وسائل الإعلام الإيرانية تفاصيل تقنية، واكتفت باتهام "الحرب الهجينة" وتحدثت عن تدمير البنية التحتية للاتصالات.

فيما يلي عرض مبسّط لأبرز الثغرات التي قد تكون طاولت بنية المراقبة الرقمية في زمن الحرب، من الكاميرات نفسها إلى الخوادم ومنصات الإدارة التي تتحكم بها.

الشركة	النظام	نوع الثغرة	ماذا تتيح؟	الأثر المحتمل
هيكفيجن	كاميرات المراقبة الشبكية	مصادقة غير سليمة	الوصول إلى بيانات الجهاز ووظائفه	فتح البث والتلاعب بالإعدادات
هيكفيجن	خادم الويب	حقن أوامر عن بعد	تنفيذ أوامر عبر الشبكة	السيطرة على الجهاز أو التسلل إلى الشبكة
هيكفيجن	نظام البث الداخلي	حقن أوامر	التحكم في نظام مساند	توسيع الهجوم إلى أنظمة الإدارة والاتصال
هيكفيجن	منصة الإدارة المركزية	تنفيذ أوامر دون مصادقة	التحكم بعدة أجهزة أو مواقع	اختراق شبكة مراقبة كاملة
داهوا	منتجات متعددة	تجاوز المصادقة	الدخول إلى الجهاز أو البث	الوصول إلى البث المباشر ومراقبة الحركة

أبرز الثغرات المحتملة التي قد تكون طاولت بنية المراقبة الرقمية في الحرب على إيران

لماذا كانت المنظومة قابلة للاختراق؟

يشير تاريخ الرقابة في إيران إلى أن الدولة توسعت في تلك التقنيات بشكل أسرع مما تستطيع تأمينه. وبحكم العقوبات الدولية، تعتمد السلطات على أجهزة صينية ومنتجات رخيصة أو نسخ مقلدة من برمجيات غربية.

وأشار تقرير أسوشييتد برس إلى أن العقوبات تجعل إيران تستخدم عتادًا قديمًا وبرمجيات مقرصنة، ما يسهل اختراقها. وتحتوي الشبكة الواسعة على آلاف الأجهزة المترابطة دون معيار أمني موحد، مما يسمح بثغرات كبيرة.

وعندما كشف قراصنة معارضون عام 2021 مقاطع من داخل سجن إيفين، وأعلنوا عام 2022 اختراق 5000 كاميرا، كان الدرس أن الأنظمة القديمة غير المحمية تصبح نقاط ضعف إستراتيجية.

وأسهمت الأطراف الإيرانية نفسها، في اتساع الثغرات، ففي مايو/أيار 2024، طرحت الحكومة مشروع قانون يفرض على القطاع الخاص ربط كاميراته بشبكة الشرطة وإبقاء التسجيلات لمدة 20 يومًا، مع استخدام تقنيات التعرف على الوجوه لمعاقبة من يرفضون التصوير.

مثل هذا التشبيك بين المنظومة العامة والخاصة يخلق سطح هجوم أوسع، ويُدخل أجهزة لا تخضع لرقابة صارمة. ونقلت وكالة رويترز عن خبراء أمنيين عام 2022 تحذيرهم من أن غياب قانون حماية البيانات يسمح بإساءة استخدام المعلومات ويزيد من احتمالات التسرب.

كما أن كثافة المراقبة تشجع الهجمات، إذ أوضح تقرير لشركة Point Check أن قراصنة إيرانيين حاولوا بدورهم اختراق مئات الكاميرات في الشرق الأوسط، ما يشير إلى أن هذه التقنية باتت جزءًا من كتاب الحرب الإلكتروني.

كاميرا مراقبة في أحد شوارع طهران 9 أبريل/نيسان 2023 (وكالة أنباء غرب آسيا -WANA)

حين تصبح الكاميرا سلاح حرب

لم تكن إيران وحدها في هذا المأزق، ففي السنوات الأخيرة، أصبحت عمليات اختراق الكاميرات مشهدًا متكررًا في الحروب الهجينة.

تقول مجلة "ويرد" الأمريكية المتخصصة بالمجال التقني إن كل طرف في الحروب الحديثة يرى في كاميرات الخصم عينًا رخيصة؛

الروس استهدفوا كاميرات المراقبة في أوكرانيا.

"حماس" حاولت اختراق كاميرات في "إسرائيل".

كشفت "إسرائيل" عن هجمات إيرانية على عشرات الكاميرات الإسرائيلية.

وصرح الجنرال الأمريكي دان كاين في مؤتمر أمني بأن العمليات السيبرانية، منها تعطيل الاتصالات واختراق الكاميرات، كانت جزءًا من التحضير للحرب ضد إيران. وحذر الخبراء من أن الأجهزة غير المحدثة وغياب بروتوكولات الأمان يجعل الاختراق مسألة وقت.

وتكشف هذه الظاهرة تناقضات الدولة المراقب، فالكاميرا ليست مجرد أداة لضبط الشارع بل عقدة ضمن شبكة رقمية عالمية يراقبها الخصوم. وحين تتسع الشبكة بلا ضوابط وتصبح الأداة السياسية بيد السلطة، تتحول في لحظة الحرب إلى مصدر معلومات لصالح الخصم.

كما أن مراكمة البيانات عن ملايين المواطنين، دون حماية قانونية أو تقنية، يخلق مخزونًا جذابًا للقراصنة الخارجيين والداخليين. وفي الشرق الأوسط، حيث يختلط الصراع الأمني بالقمع الاجتماعي، يصبح التحكم بالأجهزة الذكية جزءًا من الصراع على القوة.

رابط المقال: https://www.noonpost.com/362795/