المقاومة الإلكترونية.. ماذا يحدث في حرب غير مرئية؟

منذ بدء طوفان الأقصى في 7 أكتوبر/تشرين الأول من العام الحالي، انشغل العالم بما حققته المقاومة الفلسطينية من نجاح كبير في الهجوم على "إسرائيل"، ولاحقًا أثبتت المقاومة نجاحًا ملحوظًا في التصدي لمحاولة اقتحام قطاع غزة بريًا.

تنوعت الأقوال عن حيثيات عمل المقاومة، وكيف انشغلت "إسرائيل" بأنفاق غزة تحت الأرض، كأنها كانت تمعن النظر بعينها أسفل أرض القطاع، وفوجئت بالمقاومة تمطر عليها اختراقًا للمستوطنات من أعلى.

خلال أكثر من شهرين ونصف منذ بدء الطوفان، نجحت المقاومة الفلسطينية في بعد آخر يحدد جزءًا كبيرًا من آليات الانتصار في هذه الحرب، لم تظهر أي أخبار عن إمكانية اختراق أجهزة التواصل بين المقاومة في الأنفاق، ولم يتوصل الجيش الإسرائيلي الأكثر تطورًا في التقنية والمؤسسات المتخصصة في التجسس ومقاومة هجمات الاختراق، إلى أي تقدمٍ في هذا الحقل خلال الحرب يمكن اعتباره تفوقًا، على العكس، زادت الهجمات الإلكترونية على مواقع البنية التحتية الاقتصادية والعسكرية لـ"إسرائيل".

الحرب الإلكترونية جانب مجهول من طوفان الأقصى، وربما من مختلف الحروب التي دخلتها المقاومة الفلسطينية ضد الاحتلال، لذلك يحاول هذا المقال أن يتتبع حيثيات الوصول إلى هذه النقطة الناجحة، التي تمثل نجاح تنظيم مقاوم يعمل بآليات محدودة تحت الأرض مقارنة بجيش دولة يكرس قطاعًا كاملًا يحفل بمئات الشركات لأجل النجاح في عمليات التجسس والاختراق.

تدفعنا أحداث الحرب الحاليّة إلى عدة أسئلة تتعلق بمحطات تطور الإنترنت وصعود آليات الاختراق الإلكتروني ضمن الحروب، وكيف طورت "إسرائيل" بنيتها التقنية؟ وبدورها، كيف تم تضمين المقاومة

الإلكترونية ضمن المقاومة الفلسطينية ومواكبة آليات وعوامل الانتصار في الحروب حاليًا؟ وكيف يمكن للحرب الإلكترونية أن تشكل سلاحًا عالميًا يمكن المساهمة فيه، من مختلف دول العالم، العربية وغيرها، لصالح القضية الفلسطينية؟

الوفرة التقنية في "إسرائيل"

مع ظهور الإنترنت وانتشاره عالميًا، ظهرت دعاوى مبشرة بنهاية السيادة العسكرية، وفتح آفاق العالم على بعضه. أصبح لدينا كبشر، أخيرًا، ما يجعلنا مرتبطين ببعضنا، كأن العالم استحال إلى قرية صغيرة، حيث كل حدث كبير يضرب صداه في البلاد البعيدة جغرافيًا، إضافة إلى أن مستقبل الإنترنت مع البشر يمكنه خلق حالة من المساواة، وفرص التعلم.

بدًلا من كل هذه الفرص، وقع الإنترنت تحت نصل العولمة والسيادة العالمية، انصاع لتحكمات سوق المال وشرطية الربح والتوجيه السياسي، فالتطبيقات التي نستخدمها برفاه مجاني الآن، ندفع ثمنها غاليًا عبر اقتحام الخصوصية وإعادة توجيه بياناتنا.

تم إدراج الرقمنة ضمن مقومات النجاح لدى الدول الاستعمارية بما فيها "إسرائيل"، التطور التقني في فلسطين خضع لارتباطه بالتطور التقني الإسرائيلي، الذي انفرد بسلطة حصرية تقيد تطور البنية التقنية في فلسطين.

دخلت "إسرائيل" صراع التقنية مع منطقة الشرق الأوسط في 1992، ورغم أنها سبقت الدول العربية في إدخال الإنترنت بسنوات قليلة، فإنها في العقد الأول من الألفية الجديدة صعدت إلى الصفوف المتقدمة ضمن الدول المعتمدة على التكنولوجيا فائقة التقنية، لدى "إسرائيل" مجموعة شركات تطوير تقني وتكنولوجي متعلق بتطوير قواعد البيانات ومعلومات الاتصال، يطلق عليه "وادي السيليكون"، يقع في المرتبة الثانية عالميًا من حيث الجودة والتطوير بعد وادي السيليكون في ولاية كاليفورنيا.

قبل اتفاقية أوسلو 1993، تحفظت شركات التقنيات الفائقة على الاستثمار في "إسرائيل"، باعتبار أن المنطقة غير مستقرة سياسيًا، لكن عقب الاتفاقية، سارع الاحتلال في استقطاب الشركات الكبرى لتكون مستثمرًا أساسيًا على أرضه.

ننظر مثًلا إلى شركة "إنتل"، وهي واحدة من كبار منتجي الرقائق الإلكترونية فائقة التقنية في العالم حاليًا، تدفع للولايات المتحدة سنويًا ما يقارب 30% من إجمالي دخلها كضرائب، وحينما طلبت "إسرائيل" أن تدخل هذه الشركة في سوقها الاستثماري، عرضت عليها العمل دون أي مقابل ضريبي، رغم أن العجز في 1996 داخل "إسرائيل" كان الأكبر بين جميع الدول، طبقًا لتقييم منظمة التعاون الاقتصادي والتنمية، ومع ذلك، اختارت "إسرائيل" أن تدعم الشركة بـ900 مليون دولار لإقناعها، لتشغل "إنتل" في 2012 نحو 10% من مجمل الصادرات الإسرائيلية الصناعية.

بفعل تدفق المساعدات الأمريكية إلى "إسرائيل"، تحول الاستثمار داخلها من إجمالي 100 مليون دولار سنويًا، إلى مضاعفة القيمة أكثر من عشرين ضعفًا خلال عشر سنوات فقط، ساعد في ذلك التوسع في استقبال المهاجرين اليهود من الاتحاد السوفييتي آنذاك، فقد كان لدى نحو الثلث منهم خبرة واسعة في القطاعات التقنية والمهنية.

على حد ذكر كتاب "الجهاد الرقمي: المقاومة الفلسطينية في العصر الرقمي"، دعمت "إسرائيل" نفسها تقنيًا بشكل موسع، لتبلور عمل نظام رقابي تقني واسع، عبر تخصيص نحو 416 شركة تكنولوجيا فائقة تعمل لصالح الأمن الوطني، معظم هذه الشركات تتخصص في المراقبة والاختراق، من خلال تجميع تسجيلات هاتفية وأرقام هواتف وعناوين بريد إلكتروني، ونقلها إلى وكالات أخرى، بما فيها القطاع التقني

في الجيش والموساد.

طورت "إسرائيل" قواعدها التقنية لصالح عمليات التجسس والاختراق، وأدرجت ضمن جيشها وحدات نخبة إلكترونية وفيالق إشارة، تعتمد على العمل التقني فقط، وتدخل أرض الحرب من بعيد. يوضح أستاذ العلوم السياسية طارق فهمي في أحد حواراته، أحد نماذج وحدات النخبة الإلكترونية التابعة للجيش الإسرائيلي، تعمل الوحدة 8200 على التجسس وجمع البيانات عن المحيط الإقليمي والعربي، وتقع تحت قيادة الحرب الإلكترونية في الجيش، وتتكون هذه الوحدة من قوة بشرية تعتمد على استقطاب عملاء مستوطنين في غلاف غزة، وما يمكن تجنيده من عرب 48، يقومون بنقل قياسات الرأي العام، ونقل أي بيانات خبرية تحدث داخل الضفة الغربية أو قطاع غزة.

تعمل الوحدة 8200 على اختراق المجتمع العربي من خلال وسائل إلكترونية، بداية من مواقع الويب التقليدية ومنصات التواصل الاجتماعي والتطبيقات شائعة الاستخدام، مع الحفاظ على تغيير عملاء الوحدة من وقت لآخر والتخلي عن العملاء السابقين لضمان تدفق الاختراق بنجاح.

يتم تدريب المشاركين في الوحدة، من شباب وفتيات، خلال اختبارات يومية، ويخضع نظام التجهيز في الوحدة لتعلم مستمر ودؤوب، يتدرب خلاله العملاء على وسائل تقنية حديثة في مجالات التجسس الدولي والاختراق الإلكتروني. ظهرت نجاحات الوحدة 8200 في اغتيال القيادي في حماس "حمزة أبو الهيجا" عن طريق تحديد موقعه عبر حسابه على فيسبوك.

المقاومة الفلسطينية.. صعود الجهاد الإلكتروني

عندما اختطفت الجبهة الشعبية في فلسطين، مطلع السبعينيات، طائرة دولية، علق جورج حبش زعيم الجبهة الشعبية على هذه العملية، بأنها أكثر تأثيرًا من قتل مئات الإسرائيليين في أرض الحرب، وعلى مدى عقود لم يكن الرأي العالمي العام مع فلسطين، أو حتى ضدها، فلم تكن مرئية، والآن، بسبب هذه الخطوة، على الأقل العالم يتحدث عن الفلسطينيين والمقاومة.

يشتبك حديث حبش مع محاولة قراءة نشوء وتطور المقاومة الإلكترونية داخل المقاومة الفلسطينية، من ناحية مواكبة وتتبع لغة الحرب، لأن فعل المقاومة لا يكتسب تأثيره من مدى بطولته فقط، لكن من القدرة على التقاط العوامل التي يمكنها أن تحقق نجاحات أكبر، وبحكم أن المقاومة ضد مستعمر، على امتداد التاريخ، لم تكن أبدًا بها أي عدالة في موازين القوى، فإن الأدوات التقنية في حالة المقاومة الفلسطينية مسألة ضرورية بنفس قدر القتال في أرض الحرب، لأنها تضرب في سردية "إسرائيل" التي تتحاكي بمدى جودتها التقنية غير القابلة للاختراق.

خلال بوادر الانتفاضة الثانية، بدا للفلسطينيين أن المجتمع الدولي فشل تمامًا في إيجاد حل للقضية، أو على الأقل المساهمة بشكلٍ عادلٍ فيها، لذلك اختلفت الانتفاضة الثانية عن الأولى وتميزت بعنف غاضب واشتباكات حادة، وهنا ظهر أوان إدخال المقاومة الإلكترونية كسلاح حرب.

في أكتوبر/تشرين الأول 2000، اخترق ناشطون برمجيون 40 موقعًا إسرائيليًا، وردت "إسرائيل" باختراق مواقع تابعة لحزب الله، وارتفعت وتيرة الشد والجذب في هذا الحقل، لتصل سريعًا إلى محاولات اختراق مواقع تابعة للكنيسيت والخارجية الإسرائيلية وبورصة تل أبيب.

كان وقت ظهور المقاومة التكنولوجية مع الانتفاضة الثانية مثاليًا، فمن ناحية سارعت المقاومة الفلسطينية بالمبادرة في إنشاء هذا الحقل لمواكبة مسببات مقاومة ناجحة ومعاصرة، ومن جهة أخرى، خلقت أرضية تعاونية واسعة عن طريق فتح مجال الاختراق من فرق "هاكرز" عربية وعالمية مناصرة لفلسطين.

تظهر نتائج ذلك في إحصائية ذكرتها موسوعة الجرائم الإلكترونية ومكافحة الحرب، بين 1999 و2002،

تم اختراق أكثر من 550 موقعًا إسرائيليًا، وعلى الأقل نجحت عمليات الاختراق في تعطيل هذه المواقع عن العمل لفترة.

يتضح من طريقة سرية العمل وتقسيمه بين فريق هاكرز غزة، أن هناك تشابهًا كبيرًا مع بنية المقاومة الفلسطينية

وضعت المقاومة الفلسطينية، على اختلاف فصائلها، رابطًا طرديًا بين مدى الاحتدام التقني والسيبراني ومدى الوضع الحربي على الأرض، حتى تستطيع أن تخلق شبكة واسعة من الهجوم الإلكتروني والتقني على بنى "إسرائيل" التقنية، وسنتطرق لنتائج ذلك في الجزء الأخير من المقال.

كانت ذروة الحضور التكنولوجي لدى المقاومة الفلسطينية عقب انتهاء حرب 2008 على قطاع غزة، حين تحولت طبيعة الهجوم العام على المواقع الإسرائيلية إلى محاولات مدروسة جيّدا، تشكلت فرق مختلفة داخل القطاع، مثل فريق "هاكرز غزة" وفريق "أمن غزة" وفريق "kdms"، وسنتطرق تفصيلًا إلى فريق هاكرز غزة، لأنه يمثل خلاصة ارتباط المقاومة الافتراضية إجمالًا، وعلاقتها ببنية المقاومة على الأرض.

تكون الفريق عام 2007 ولم تبدأ هجماته ومحاولات الاختراق إلا بعد سنة، حينما اخترق موقع حزب "كاديما" الإسرائيلي، ظهرت قوة عمل الفريق في أكتوبر/تشرين الأول 2012، حينما عطلوا جميع حواسيب الشرطة الإسرائيلية، وانتشرت البرمجيات الخبيثة في دوائر التقنية الحكومية داخل "إسرائيل"، لدرجة توقف خوادم الشرطة وانقطاع الوصول إلى الإنترنت عدة أيام، وفي فبراير/شباط 2014، كرر هاكرز غزة عملياته ونجح في اختراق وكالة الإدارة المدنية المسؤولة عن جزء من الضفة الغربية.

خلال تحضير أطروحته، حاور إيريك سكاري قيادة فريق هاكرز غزة، وتبين أنه يتشكل من ثلاثة أشخاص، أسفلهم فريق كامل من فلسطين ودول عربية أخرى، يتم تقسيمهم إلى مجموعات حسب التخصص، جزء مسؤول عن اختراق المواقع، وآخر مسؤول عن قرصنة الإعدادات واختراق الإيميلات، ورغم تركيبة العمل هذه، فإن أعضاء الفريق لا يعرفون بعضهم، ووسائل تواصلهم عادةً ما تكون افتراضية، وعمليات التحضير تخضع لسرية تامة.

يتضح من طريقة سرية العمل وتقسيمه بين فريق هاكرز غزة، أن هناك تشابهًا كبيرًا مع بنية المقاومة الفلسطينية، فضلًا عن الالتزام الأولي بشروط تكوين مقاومة نضالية ناجحة بشكلٍ عام، ومن جهة أخرى، تم الحفاظ على "تعميم" المقاومة الإلكترونية، وجعلها فرصة تتيح للمختصين في مختلف بقاع العالم مناهضتهم الاحتلال، عبر فعل مقاومة له تأثير، وهذا تحديدًا ما حدث في طوفان الأقصى الآن.

أنفاق إلكترونية

في حوارها المذكور سلفًا، لم توافق قيادة "هاكرز غزة" على الانتماء لأي فصيل مقاومة في فلسطين، وحددت هويتها بأنهم "شباب من غزة"، وهذا لا يعني انفصال الفرقة تمامًا عن المقاومة في فلسطين، خلال حرب 2014 على قطاع غزة، فقد أرفق الفريق صورة أحد مقاومي كتائب القسام على واجهة الموقع.

تعمل مختلف جهات المقاومة الإلكترونية في فلسطين، الشعبية منها والتنظيمية، من خلال إطار عام موحد، يخرج بالمقاومة عن التصنيف الإسرائيلي المعتاد للفلسطينيين، المتأرجح بين إرهابي ومدني ضحية حربٍ يسأل عنها الإرهابي، فقد خلقت المقاومة الإلكترونية بعدًا جديدًا للوجود الفلسطيني، يشمل أحقية المقاومة والاختراق وإزعاج "إسرائيل"، لمجرد أن المقاوم فلسطيني ينزع حقه في الوجود.

لنعرض معًا نتاج هذه السنوات من خلق بنية مركبة، ترتبط بالمقاومة التي تقاوم في القطاع حاليًا على الأرض، وتحتفظ باستقلاليتها في نفس الوقت. منذ بدء طوفان الأقصى، تعرضت "إسرائيل" إلكترونيًا

لحملات كبيرة غير مسبوقة، فظهرت مجموعة "أنون غوست" الداعمة لحركة حماس، وصرحت أنها عطلت تطبيقًا إسرائيليًا للتحذير في حالة الطوارئ والقصف، بينما قالت مجموعة "أنونيموس" من السودان، أنها تستهدف البنية التحتية الحيوية لـ"إسرائيل"، ورغم أنها لم تقدم إلا القليل من الأدلة على هذه الادعاءات، هناك دلائل على عمل إلكتروني شامل يستهدف مختلف الأنظمة الإسرائيلية.

لا تعد الحرب على غزة حاليًا منوطة فقط بالصمود على الأرض، هناك أبعاد جديدة، غير مرئية لكنها تدخل في عمق إمكانية الصمود، أهمها الحرب الإلكترونية

في تقرير نشره موقع الجزيرة، قالت شركة "ريكورديد فيوتشر" المعنية بالرصد المعلوماتي السيبراني إن هجمات الاختراق على المواقع والتطبيقات الإسرائيلية زادت بشكلٍ كبير منذ بدء طوفان الأقصى، إذ تمكن مهاجمون لم يعلن عنهم من إيقاف موقع "جيروزالم بوست" المعروف، وإيقافه عن العمل لفترات متفاوتة في أكثر من مرة.

خلال الحرب ظهرت مجموعة "سايبر طوفان الأقصى" أعلنت مسؤوليتها عن اختراق عدد من المواقع الإسرائيلية والحصول على ملفات تجارية مهمة منها، وظهر أحد قادة الفريق في فيديو على تيليجرام، ذكر فيه قدرة الفريق على اختراق موقع وزارة الدفاع الإسرائيلية، والحصول على ملايين البيانات عن جنود جيش الاحتلال.

إضافةً إلى تفصيلات تتعلق بمعلومات عن الفرق الموجودة بشمال غزة وأرقام خدمتها وأماكن سكنها، وضحت البيانات المخترقة وجود جنود مزدوجي الجنسية، بينها كندا وبلجيكا وأوكرانيا، بينما الجنود المرفقون بجيش الاحتلال من أصول إفريقية، كتب جوار أسمائهم ملحوظة "أسود"، في إشارة لعنصرية الجيش الإسرائيلي تجاه ذوي البشرة السمراء.

نهايةً، لا تعد الحرب على غزة حاليًا منوطة فقط بالصمود على الأرض، هناك أبعاد جديدة، غير مرئية لكنها تدخل في عمق إمكانية الصمود، أهمها الحرب الإلكترونية. حاول هذا المقال أن يضع متنًا مفصّلًا، قدر الإمكان، للمحطات التي جعلتنا نقرأ أخبارًا يومية عن اختراق مواقع إسرائيلية أو محطات إذاعية وتليفزيونية، وإظهار علم فلسطين على شرائط إعلانها، لم تأت هذه الاختراقات اعتباطًا، بل تطلبت سنوات طويلة وتعاونًا متعددًا وحشدًا لمختلف المختصين في هذا المجال عالميًا وعربيًا.

رابط المقال: https://www.noonpost.com/188215/