عصر الحرب الرقمية: مراكز البيانات تتحول إلى أهداف عسكرية

ترجمة وتحرير نون بوست

في إطار الرد على الحرب الأمريكية الإسرائيلية المستمرة، لجأت إيران إلى نمط مستحدث من الهجمات المضادة، حيث تعرضت مراكز البيانات التابعة للقطاع الخاص لهجمات متعمدة، وذلك لأول مرة في التاريخ العسكري. وفي عصر باتت فيه الشركات الشهيرة بمنصات التجارة الإلكترونية، وشبكات التواصل الاجتماعي، ومحركات البحث، شريكًا وثيقًا للمؤسسات العسكرية، يبرز السؤال الجوهري: هل أصبح قصف خوادم هذه الشركات "هدفًا مشروعًا"؟

بعد ثلاثة أيام من بدء القصف المشترك بين الولايات المتحدة وإسرائيل، شن الحرس الثوري الإيراني هجمات بطائرات مسيرة انتحارية استهدفت مراكز بيانات مملوكة لشركة "أمازون" في الإمارات والبحرين، وهي المراكز التي تقدم مجموعة واسعة من خدمات الحوسبة السحابية للعملاء في جميع أنحاء الشرق الأوسط. وحسب بيان لشركة أمازون، أدت تلك الضربات والحرائق الناجمة عنها إلى "أضرار هيكلية، وتعطيل إمدادات الطاقة للبنية التحتية، وتطلب الأمر في بعض الحالات تفعيل أنظمة إخماد الحرائق التي تسببت بدورها في أضرار إضافية بسبب المياه"، مما أسفر عن انقطاع الخدمات في جميع أنحاء المنطقة.

وفقًا للتلفزيون الرسمي الإيراني، لم يكن الدافع وراء الهجوم عرقلة طلب السلع أو النشر على وسائل التواصل الاجتماعي، بل "تسليط الضوء على دور هذه المراكز في دعم الأنشطة العسكرية والاستخباراتية للعدو". وعلى الرغم من أن مراكز أمازون هي الوحيدة التي تأكد تعرضها للقصف، إلا أن تغريدة نشرتها وكالة أنباء "تسنيم" شبه الرسمية في 11 مارس/ آذار أدرجت عشرات المرافق الإقليمية، بما في ذلك مراكز بيانات مملوكة لشركتي "مايكروسوفت" و"غوغل" وغيرهما، تحت تصنيف "بنية تحتية تكنولوجية تابعة للعدو" صالحة للاستهداف.

من غير الواضح ما إذا كانت مراكز بيانات "أمازون" التي استهدفتها المسيرات الإيرانية تُستخدم لأغراض

عسكرية أم مدنية، أو لكليهما معاً. ومن غير المعروف ما إذا كانت هذه الهجمات قد نجحت في عرقلة استخدام الجيوش الأمريكية أو الإسرائيلية أو حلفائهم في الخليج لتقنيات الذكاء الاصطناعي أو الخدمات السحابية الأخرى في جهودهم الحربية. ولكن في ظل تهافت شركات مثل "أمازون" و"غوغل" وحتى "ميتا" (الشركة الأم لفيسبوك) على الشراكة مع البنتاغون لتعزيز القوة التدميرية للولايات المتحدة في إيران وغيرها، فقد أصبحت "مزارع الخوادم" تتمتع اليوم بذات المكانة الاستراتيجية التي تحظى بها مصانع القنابل والطائرات الحربية.

يرى باحثون في القانون الدولي وقوانين النزاعات المسلحة أنه عندما يعتمد الجيش في عملياته على "الحوسبة السحابية"، فإنها تتحول قانونياً إلى "هدف عسكري مشروع"، لكنها تظل مفهوماً تجريدياً وليست موقعاً فيزيائياً واحداً، فهي شبكة عالمية تضم ملايين الرقائق الإلكترونية الموزعة على مئات المباني الضخمة حول كوكب الأرض، وتخدم في آنٍ واحد التطبيقات المدنية وأدوات حكومية تُستخدم للمراقبة والقتل. لذا، فإن الفصل بين الاستخدام المدني والعسكري يمثل مهمة في غاية الصعوبة.

وأوضح ليون كاستيلانوس-يانكيفيتش، المحامي في معهد "أسر" للقانون الدولي والأوروبي في لاهاي، أن "الشرعية تتوقف على ما إذا كانت المنشأة المحددة، في تلك اللحظة بالذات، تخدم بالفعل العمليات العسكرية لأحد أطراف النزاع بطريقة توفر ميزة ملموسة ومحددة للمهاجم".

وفي بعض الأحيان، يكون الفصل بين الاستخدامين العسكري والمدني واضحاً ومباشراً. فعلى سبيل المثال، تساهم شركة "مايكروسوفت" في تشغيل "قدرات الحوسبة السحابية المشتركة للمحاربين"، والتي صرح البنتاغون بأنها تمنحه "قدرة تدميرية أكبر". ويتضمّن هذا العمل معالجة البيانات السرية، التي لا تريد الحكومة خلطها بالتقنيات المدنية. وعادةً ما تُقدّم خدمات الحوسبة السحابيّة عبر "مناطق" جغرافية متميزة، تتكون كل منها من العديد من مراكز البيانات الفيزيائية، حيث يختار العملاء المنطقة الأقرب إليهم لتقليل زمن الاستجابة. ووفقًا لشركة مايكروسوفت، فإن منطقتي "وسط وشرق وزارة الدفاع الأمريكية" هما منطقتان "محجوزتان للاستخدام الحصري لوزارة الدفاع"، وتخدمهما مراكز بيانات في "دي موين" بولاية آيوا، وشمال فرجينيا، على التوالي.

وتقدم شركة "أمازون" أقاليم سحابية مماثلة مخصصة حصراً للبنتاغون، رغم أن مواقع هذه المراكز غير معلنة. كما تدير شركة "أوراكل"، وهي مزود آخر لبرنامج "قدرات الحوسبة السحابية المشتركة للمقاتلين"، مرافق خاصة بالبنتاغون في شيكاغو وفينيكس وفرجينيا. وتلتزم الشركات، لأسباب مفهومة، بتكتم شديد حول المواقع الدقيقة لهذه المرافق على الخريطة، ويرجع ذلك إلى حد كبير إلى أن إيران، أو أي دولة في حالة حرب مع الولايات المتحدة، سيكون لديها سبب لاستهدافها.

وفي هذا الصدد، يقول يوانيس كالبوزوس، باحث القانون الدولي والأستاذ الزائر في كلية الحقوق بجامعة هارفارد: "إن مركز البيانات الذي يُستخدم حصرياً أو بشكل أساسي للتطبيقات العسكرية هو هدف محتمل، والمركز الذي يدعم برنامج "قدرات الحوسبة السحابية المشتركة للمقاتلين" التابع للبنتاغون يندرج تحت هذه الفئة".

أصبح التوسع المتسارع في بناء مراكز البيانات محل نزاع في الولايات المتحدة وجميع أنحاء العالم، حيث تتحرك المجتمعات المحلية في كثير من الأحيان، وبنجاح أحياناً، لعرقلة ما تعتبره عيوباً شائنة والتي تستنزف الموارد الضخمة. لكن بالنسبة لأولئك الذين يعيشون في ظل هذه المراكز الآخذة في التوسع، سواء المخطط لها أو القائمة بالفعل، فإن تصنيفها كأهداف عسكرية قد يثير قلقاً يتجاوز المخاوف التقليدية المتعلقة باستهلاك المياه والطاقة.

ومع إصرار وزير الدفاع "بيت هيغسيث" على دمج أدوات الذكاء الاصطناعي في المؤسسة العسكرية بكل قوة وحيثما أمكن، فإن التوسع السريع لمراكز البيانات يعني بالتبعية احتمال انتشار "الأهداف

العسكرية المشروعة" في جميع أنحاء الولايات المتحدة.

مع تزايد المقارنات بين القوة التدميرية للحروب المعززة بالذكاء الاصطناعي والأسلحة النووية، فإن شبكة مراكز البيانات الأمريكية المتنامية قد تعيد إحياء مخاوف الحرب الباردة المتعلقة بتوزيع صوامع الصواريخ الباليستية العابرة للقارات. ومن الشائع استراتيجياً أن ترسانة الردع النووي للبلاد كانت تتركز في مناطق الغرب الأوسط العلوي ذات الكثافة السكانية المنخفضة، لتشكل ما يُعرف بـ "الإسفنجة النووية" التي تهدف لجذب الصواريخ السوفيتية بعيداً عن التجمعات السكانية الكبرى نحو المناطق الريفية والأراضي الزراعية.

لكن الحسابات القانونية المتعلقة بمعظم مراكز البيانات ستكون أقل وضوحاً، فشركة "غوغل"، على سبيل المثال، توضّح أن البنتاغون يستخدم كلاً من سحابتها العامة للأغراض العامة، وشبكات أصغر متخصصة ومعزولة لا تتصل بشبكة الإنترنت العامة، وذلك حسب حساسية البيانات. وحتى الأعمال السحابية التي تتضمن بيانات عسكرية "سرية للغاية" يمكن أن تُدار داخل مراكز بيانات غوغل الموثوقة والمؤمنة. كما تبيع الشركة "مراكز بيانات مصغرة متنقلة" لاستخدامها في مواقع قريبة من ساحات القتال أو القواعد العسكرية.

هذه الترتيبات، المحاطة بالسرية العسكرية والتجارية، تجعل من الصعب تقييم ما إذا كان الخادم يستضيف واجبات منزلية لطالب أم أبحاثاً ومشروع تطوير تابع للقوات الجوية، مما يربك مشروعية مهاجمة مراكز البيانات التي قد تستضيف الاثنين معاً. وقد لا تملك غوغل سيطرة تذكر على كيفية استخدام الحكومات لأدواتها السحابية، إذ سبق لـ "الإنترسبت" أن كشفت عن مخاوف داخلية لدى المسؤولين التنفيذيين في غوغل من عدم قدرتهم على معرفة كيفية توظيف الجيش الإسرائيلي لخدماتهم السحابية.

وقال كاستيلانوس-جانكيفيتش: "التحدي العملي يكمن في أن البنية التحتية السحابية غالباً ما تكون غامضة من الناحية التقنية، حتى بالنسبة للمزودين أنفسهم؛ فمن الصعب التحقق من الخدمات التي يدعمها مركز بيانات معين، سواء من الخارج أو حتى من الداخل، مما يضاعف من تعقيد الالتزامات القانونية الملقاة على عاتق الطرف المهاجم".

وبالمثل، يوفر "مشروع نيمبوس" التابع لشركتي أمازون وغوغل خدمات الحوسبة السحابية لمختلف قطاعات الحكومة الإسرائيلية، بما في ذلك الوكالات المدنية ووزارة الدفاع، جنباً إلى جنب مع شركات الأسلحة المملوكة للدولة.

وقد صرح كاستيلانوس-جانكيفيتش لصحيفة "الإنترسبت" قائلاً: "تصبح الصورة أكثر تعقيداً من الناحية القانونية عندما يعمل مركز البيانات "ككائن مزدوج الاستخدام"، حيث يستضيف بيانات أو قدرات عسكرية بالتزامن مع الخدمات المدنية. وبمجرد اكتشاف مساهمة المرفق بشكل فعال في العمل العسكري، فإن المرفق المادي بأكمله يمكن اعتباره، وفقاً للرؤية القانونية السائدة، هدفاً عسكرياً".

وأوضح كاستيلانوس-جانكيفيتش أن اعتماد الولايات المتحدة وغيرها على الحوسبة السحابية التجارية قد زاد من ضبابية المشهد القانوني المعقد بالفعل، وأضاف أن "قرار الجيش بتخزين بيانات سرية أو تشغيل أنظمة عسكرية مدعومة بالذكاء الاصطناعي على بنية تحتية سحابية تجارية مشتركة مع الخدمات المدنية قد يثير في حد ذاته مخاوف قانونية، خاصة إذا كان هذا الخلط بين الاستخدامات العسكرية والمدنية يجعل احتمال وقوع ضربة عسكرية أكثر ترجيحاً، أو يضاعف من الضرر المتوقع على المدنيين في حال وقوعها".

تعتمد عملية تحديد مشروعية مهاجمة مركز بيانات معين بموجب القانون الدولي الإنساني، الذي يتألف

هو نفسه من معاهدات متنوعة لا تلتزم بها جميع الدول، على سلسلة معقدة من اختبارات الموازنة التي نادرًا ما تفضي إلى إجابات حاسمة. في بادئ الأمر، يُفترض بموجب هذا الإطار القانوني بصفة عامة أن كل شخص مدني يُستثنى من الهجوم. وقبل شن أي ضربة، يُفترض بالدولة أن تملك سببًا قابلًا للتحقق للاعتقاد بأن مركز البيانات يساهم في المجهود الحربي للعدو، وسببًا آخر للاعتقاد بأن الهجوم سيلحق ضررًا ملموسًا بهذا المجهود. وبطبيعة الحال، سيظل تعريف ما يشكل "مساهمة فعالة في العمل العسكري" موضع خلاف دائم.

لقد وردت تقارير تفيد باستخدام نموذج اللغة الضخم "كلود" التابع لشركة "أنثروبيك" لتسريع وتيرة الغارات الجوية الأمريكية ضد إيران، علمًا بأن "كلود" قد بُني جزئيًا باستخدام 500 ألف شريحة إلكترونية مستضافة في مركز بيانات تابع لأمازون في ولاية إنديانا بقيمة 11 مليار دولار. فإذا كان "كلود" يُعتبر الآن سلاحًا، فهل يعد موقع إنديانا هو المكافئ الرقمي لمصنع قنابل؟ وفي تصريح لصحيفة "الإنترسبت"، قال كالبوزوس، الأستاذ الزائر في كلية الحقوق بجامعة هارفارد، إن الأمر يعتمد على الوقائع في لحظة سقوط القنبلة، وليس على الاستخدام السابق. وأضاف: "إذا كان المرفق يُستخدم حاليًا في تدريب نموذج لغوي ضخم يُوظف في تنفيذ العمليات العسكرية، على سبيل المثال، من خلال الضبط الدقيق لتصنيف الأهداف أو ميزات التفاعل مع المستخدم، فإن هذا قد يجعله قابلا للاستهداف".

وفي مقال نُشر مؤخرًا على موقع "جست سيكيوريتي"، أكد كل من كلوديا كلونوفسكا ومايكل شميت أن القانون يقتضي "التناسب" و"ضبط النفس" حتى عند استهداف الأهداف العسكرية. وجادلا بأن أي هجوم ضدّ مركز بيانات يوفّر حوسبة عسكرية ومدنية في آن واحد يجب أن يكون دقيقًا بما يكفي لتدمير الشق العسكري مع تقليل الضرر بالشق المدني إلى أدنى حد. لكن القانون الدولي قد يطالب بدرجة من الحذر قد لا تبدي الجيوش اهتمامًا كبيرًا بها، حيث كتبا: "إذا كان من الممكن مهاجمة المنطقة التي تضم الخوادم التي تستضيف البيانات العسكرية فقط داخل مركز البيانات دون تدمير المركز بأكمله، فإنه يتعين على المهاجم القيام بذلك".

قد يكون من الصعب الالتزام بهذه المتطلبات في الواقع. وبينما تتفاخر كل من الولايات المتحدة وإسرائيل بالدقة المتناهية لغاراتهما الجوية، فإن هذه الغارات تحصد أرواح المدنيين بانتظام. علاوة على ذلك، فإن أيًا من الدولتين، ولا حتى إيران، ليست طرفًا موقعًا على بعض الأطر القانونية الجوهرية التي تشكل ما يُعرف بـ "قوانين النزاعات المسلحة" في المقام الأول.

ومن المفارقات أن ممارسات الحرب العشوائية التي تنهجها الولايات المتحدة وإسرائيل كانت وسيلة فعالة في إعادة صياغة كيفية تفسير هذه القوانين، بل وفي تخفيف قيودها فعليًا. فخلال حرب الإبادة الجماعية الإسرائيلية في غزة، أوضح كل من الجيش الإسرائيلي والبنتاغون أن تدمير مجمع سكني أو مستشفى يعد أمرًا "مقبولًا" إذا ما ادعى الطرف المهاجم وجود هدف عسكري حقيقي بداخله.

وقد أبدت إدارة ترامب الثانية، على وجه الخصوص، حرصًا شديدًا على دمج "سيليكون فالي" بشكل أوثق في آلة القتل الأمريكية العالمية، وهي الخطة التي أظهر قطاع التكنولوجيا استجابة واسعة لها. وحتى بعد تعرضه لهجوم حاد من الإدارة في أعقاب انهيار صفقة البنتاغون بسبب خلافات مزعومة حول "ضمانات السلامة"، أصدر داريو أمودي، الرئيس التنفيذي لشركة "أنثروبيك"، بيانًا عامًا أكد فيه رغبته في نيل حصة من الإنفاق العسكري، قائلًا: "إن نقاط الاتفاق بين أنثروبيك ووزارة الحرب أكثر بكثير من نقاط الاختلاف، فكلينا ملتزم بتعزيز الأمن القومي الأمريكي والدفاع عن الشعب، ونتفق على الحاجة الملحة لتطبيق الذكاء الاصطناعي في كافة مفاصل الحكومة". إن هذا التوجه، الذي بات شائعًا الآن في قطاع التكنولوجيا، سيؤدي إلى مزيد من الخلط بين التكنولوجيا الاستهلاكية وأدوات الحرب، سواء

على المستوى النظري أو تحت الأسقف الشاسعة لمراكز البيانات الموزعة في أنحاء البلاد.

وفي هذا السياق، قال كالبوزوس: "إن مراكز البيانات هذه تعمل على دمج البنية التحتية العسكرية بالمدنية بشكل أكبر. ومع تبني الولايات المتحدة وإسرائيل لقواعد اشتباك متساهلة بشكل متزايد، فإن ذلك قد يؤدي إلى جر قطاعات أوسع من الاقتصاد والمجتمع إلى دائرة الاستهداف والدمار".

المصدر: الانترسبت