

الحرب العالمية القادمة: هل ستكون الحرب العالمية القادمة حرباً غير مرئية؟

في الحروب الكبرى التي عرفها التاريخ، كان هناك دائماً شيء يمكن رؤيته. ففي الحرب العالمية الأولى تحركت الجيوش عبر الحدود، وامتألت الجبهات بالخنادق والمدافع. وفي الحرب العالمية الثانية أصبحت المدن نفسها ساحات للمعركة، وارتبط اندلاع الحرب في وعي الناس بصوت الطائرات وصفارات الإنذار وسقوط القنابل.

لكن ماذا لو كانت أولى علاماتها شاشة مصرفية لا تعمل، وشبكة كهرباء تتوقف، ومطاراً يعجز عن تشغيل أنظمتها، وميناءً يتعطل، واتصالات تنقطع عن ملايين البشر؟ ماذا لو اكتشف العالم، بعد أيام أو أسابيع، أن ما اعتقده سلسلة من الأعطال والهجمات المتفرقة لم يكن أعطالاً، بل حرباً بدأت من دون إعلان؟

هذه ليست نبوءة بأن الحرب العالمية المقبلة ستكون إلكترونية، ولا أن الدبابات والصواريخ ستختفي، لكنها فرضية تستحق أن تؤخذ بجديّة: لقد تغيرت طبيعة القوة، وبالتالي قد تتغير الطريقة التي تبدأ بها الحروب، حيث لم تعد الدولة مجموعة من الحدود والجيوش، والدولة الحديثة ليست فقط أرضاً وجيشاً وعاصمة، إنها شبكة هائلة من الأنظمة المترابطة: البنوك، الطاقة، الاتصالات، الأقمار الصناعية، الموانئ، النقل، المصانع، سلاسل الإمداد، أنظمة المياه والغذاء، والمعلومات.

وهذا الترابط منح الدول قدرات غير مسبوقة، لكنه خلق في الوقت نفسه نقاط ضعف غير مسبوقة؛ فالاقتصاد الذي يعمل في الزمن الحقيقي يمكن أن يتوقف إذا تعطلت إحدى حلقاته الأساسية، والميناء الذي يعتمد على أنظمة رقمية يمكن أن يصبح عاجزاً عن العمل من دون أن تُقصف رافعة واحدة، والمصرف الذي يخدم ملايين العملاء قد يتحول إلى مبنى سليم لا يستطيع أحد استخدامه.

وتؤكد الوكالة الأوروبية للأمن السيبراني أن الترابط الرقمي يوسّع مساحة الهجوم، وأن استغلال نقاط الاعتماد المشتركة يمكن أن يضاعف أثر الهجمات عبر سلاسل الإمداد. كما تشير أبحاثها إلى استمرار استهداف قطاعات الإدارة العامة والنقل والبنية الرقمية والمال.

وهنا يتغير مفهوم الاستهداف؛ من ضرب المدينة إلى ضرب شرايينها؛ ففي الحرب التقليدية، كان قطع شرايين الدولة يعني تدمير الطرق والجسور والموانئ أو حصار المدن، أما اليوم، فللدولة شرايين لا تُرى؛ فالإنترنت شريان والطاقة شريان والنظام المالي شريان والأقمار الصناعية شريان والإمداد شريان، حتى قاع البحر أصبح جزءاً من هذه المعادلة. فالكابلات البحرية تحمل الجزء الأكبر من حركة البيانات العابرة للقارات، فيما تحمل بعض البنى البحرية الأخرى الطاقة. وقد أصبحت حمايتها قضية أمنية مباشرة؛ فالتأثيرات التي تحدثها أدوات تستخدم الذكاء الاصطناعي لتحليل حركة السفن واكتشاف السلوكيات التي قد تشير إلى تهديد للبنية التحتية الموجودة تحت البحر.

المفارقة أن أكثر البنى أهمية في الاقتصاد العالمي قد تكون من أكثرها غيابة عن وعي الناس. فنحن لا نرى الكابل الذي يسمح لنا بتحويل المال، ولا نرى النظام الذي يربط الميناء بالمصنع، ولا نرى الشبكة التي تجعل المستشفى

يعمل، لكننا نعرف قيمتها فور توقفها. السلاح الذي لا يحتاج إلى انفجار! لهذا قد تكون الحرب المقبلة مختلفة في شكلها، لا في نتائجها.

هجوم سيبراني واسع على قطاع مالي قد لا يسرق المال بقدر ما يزرع الفوضى في حركة الأموال، وتعطيل أنظمة النقل قد لا يدمر الميناء، لكنه قد يمنع السفن والبضائع من الحركة. واختراق شبكة كهرباء قد لا يحرق محطة واحدة، لكنه قد يحرم مدناً من الطاقة، والهجوم على بنية اتصالات قد لا يقتل إنساناً مباشرة، لكنه قد يعزل مناطق كاملة عن الدولة والعالم. وهنا تظهر قاعدة جديدة في الحرب: السلاح قد يكون غير مرئي، لكن أثره سيكون مرئياً جداً. قد لا تُقطع شرايين البشر، وإنما شرايين الدولة التي يعتمد عليها البشر.

والذكاء الاصطناعي يضيف طبقة جديدة، لن يكون الذكاء الاصطناعي بالضرورة "السلاح" بحد ذاته، لكنه يمكن أن يصبح مضاعفاً لقدرة من يستخدمه، فهو قادر على تحليل كميات هائلة من البيانات، وتسريع اكتشاف نقاط الضعف، وأتمتة بعض العمليات، وتطوير أساليب التضليل والهندسة الاجتماعية. وتشير ENISA إلى أن مجموعات تهديد تستخدم أدوات الذكاء الاصطناعي لتعزيز عملياتها، فيما أصبح الذكاء الاصطناعي نفسه جزءاً من مساحة الهجوم مع اتساع اعتماده داخل المؤسسات. كما ترى الوكالة أن السنوات المقبلة قد تشهد مزيداً من الأتمتة والتصنيع واسع النطاق للعمليات السيبرانية.

لكن الأخطر ربما ليس قدرة الذكاء الاصطناعي على الهجوم، وإنما قدرته على تسريع الحرب. ففي السابق، كان إعداد عملية معقدة يحتاج إلى وقت طويل وعدد كبير من الأشخاص، أما عندما تدخل الخوارزميات في تحليل المعلومات واكتشاف الثغرات وصناعة الرسائل وتنفيذ عمليات واسعة، فقد تصبح المسافة بين اكتشاف الهدف وضربه أقصر بكثير.

المشكلة الكبرى أن الهجوم السيبراني لا يحمل دائماً توقيعاً واضحاً، فإذا سقط صاروخ، فهناك أثر مادي، أما إذا تعطلت شبكة مصرفية أو انقطعت الاتصالات، فقد يستغرق تحديد المسؤول وقتاً، وقد تتداخل فيه الجريمة المنظمة، والهجمات المدعومة من دول، والجهات غير الحكومية، والعمليات الاستخباراتية. وهذا يخلق ما يسمى بالحرب الهجينة أو المنطقة الرمادية: ضغط سياسي واقتصادي ومعلوماتي وسيبراني وتخريبي، يمكن أن يتدرج دون أن يصل مباشرة إلى الحرب التقليدية.

الناتو نفسه يصف التهديدات الهجينة بأنها تشمل التضليل والخداع والتخريب وغيرها من الوسائل غير العسكرية، ويشير إلى أن ما تغير في السنوات الأخيرة هو السرعة والحجم والشدة التي فرضتها التكنولوجيا والترابط العالمي. وهنا قد يصبح تعريف "بداية الحرب" أكثر صعوبة. هل تبدأ الحرب عندما تُطلق الصواريخ؟ أم عندما تُحترق الشبكات؟ أم عندما يبدأ طرف ما بتعطيل البنية التحتية الحيوية لخصمه؟ أم عندما يصبح الهدف من العمليات ليس التجسس، وإنما إجبار الدولة الأخرى على تغيير سلوكها؟

هل انتهى عصر الدبابات؟ بالطبع لا. وهنا يجب الحذر من المبالغة. فالحرب السيبرانية لا تلغي الحرب التقليدية؛ قد تكون تمهيداً لها؛ حيث يمكن أن تسبق الهجمات الرقمية ضربة عسكرية، أو تتزامن معها، أو تستخدم لإرباك

القيادة والاتصالات والنقل والدفاعات قبل دخول الطائرات والصواريخ. السؤال الأكثر دقة هو: كيف ستعمل الأدوات العسكرية والاقتصادية والسيبرانية والمعلوماتية معاً داخل حرب واحدة؟

قد تكون الطائرة في السماء، والجندي على الأرض، والقرصان أمام الحاسوب، والمضارب المالي أمام شاشة التداول، وحملة التضليل تعمل على التليفونات؛ وكلهم جزء من المعركة نفسها. وهنا تصبح الجبهة في كل مكان. والمرء قد لا يعرف أنه على جبهة، أما في الحرب التقليدية، فالناس يعرفون أين تقع الجبهة.

في الحرب غير المرئية، قد تكون الجبهة في التليفون والمصرف والمصنع والمستشفى. الشخص الذي لا يستطيع الوصول إلى حسابه المصرفي. المصنع الذي توقف لأن نظامه الرقمي تعطل. المستشفى الذي فقد جزءاً من خدماته. الشركة التي لم تصلها المواد الخام. الميناء الذي توقفت أنظمتها.

هذه ليست بالضرورة مشاهد حرب بالمعنى التقليدي، لكنها قد تكون نتائج حرب. ولهذا أصبحت "المرونة" جزءاً أساسياً من الأمن القومي؛ فالناتو يربط قدرة الدول على الصمود بحماية النقل والاتصالات والطاقة والغذاء والماء والدواء والإدارة الحكومية وتدفق المعلومات، بما في ذلك مواجهة الهجمات السيبرانية والتهديدات الهجينة.

والسؤال الأصعب: هل دخلنا الحرب بالفعل؟ ربما يكون هذا هو السؤال الذي يجب أن نطرحه اليوم. ليس بمعنى أن العالم يعيش حرباً عالمية معلنه؛ فهذا استنتاج لا تسمح به الوقائع الحالية. لكن إذا كانت الحرب الحديثة تعني أيضاً التجسس السيبراني، والهجمات على البنى التحتية، والتضليل، والتخريب، والضغط الاقتصادي، ومحاولات اختراق سلاسل الإمداد، فإن جزءاً من أدوات الحرب التي كان يُنظر إليها سابقاً باعتبارها استثنائية أصبح حاضراً بالفعل في المنافسة بين الدول. وقد وثقت الجهات الأوروبية آلاف الحوادث السيبرانية، فيما تشير التقارير إلى استمرار نشاط جهات مرتبطة بالدول، وتساعد استخدام الذكاء الاصطناعي في بعض العمليات الخبيثة.

إذا كنا ننتظر الدبابات كي نقول إن الحرب بدأت، فقد نكتشف أنها بدأت قبل ذلك بوقت طويل. أما إذا كنا نعتبر كل هجوم إلكتروني حرباً، فسوف نخلط بين الجريمة والتجسس والتخريب والصراع العسكري. لذلك تحتاج المرحلة المقبلة إلى معيار أكثر دقة: متى تنتقل الدولة من المنافسة والردع والعمليات السرية إلى استخدام منظم للقوة بهدف إكراه خصمها سياسياً واستراتيجياً؟

قد تبدأ الحرب من مكان لا يلتفت إليه أحد: خادم، شبكة، كابل في قاع البحر، قمر صناعي، نظام مصرفي، أو سلسلة إمداد. وقد لا يكون أول سؤال في الحرب القادمة: من قصفنا؟ ففي عالم شديد الترابط، ربما لم تعد الحرب تحتاج إلى عبور الحدود كي تدخل بلادك.

كتبه للمكتب الإعلامي المركزي لحزب التحرير

نبيل عبد الكريم