الحرب الإلكترونية: بين شركة سوني وكوريا الشمالية

ترجمة وتحرير نون بوست

كوريا الشمالية بلد تعيس ورجعي، وناتجه القومي حوالي 7٪ من الناتج القومي لنظيره الجنوبي، ولا يميّز حكمه إلا الدعاية الشمولية الصرفة وقمع الدولة التام، بيد أن هذا البلد الفقير والمغيّب نجح في ضرب شركة سوني بعد أن أنتجت فيلمًا ذا محتوى مسيء للنظام الكوري الشمالي.

ماذا يعني ذلك؟ يعني أننا ينشهد خلال السنوات المقبلة هجمات إلكترونية بهذا الشكل من جهات شتى، وستتزايد تكلفتها مع الوقت مقارنة بما تكبدته سوني حتى الآن جراء الهجوم الكوري. ليس هذا بمستغرب بالنظر للآلاف من حالات السرقة وانتحال الهوية التي اعترت الإنترنت منذ عشرين عامًا هي عمره تقريبًا كمكوّن رئيسي في حضارة اليوم.

تحول الأكواد واللوغاريتمات إلى أسلحة سيكون ربما أبرز تحوّل في عالمنا العسكري منذ اكتشاف القدرة على صناعة أسلحة من المواد الخصبة نوويًا، وهو تحوّل سهل نسبيًا مقارنة بغيره بالنظر لوجود عراقيل قليلة جدًا بوجه التمكّن منه. فالتحصل على تكنولوجيا نووية مثلا يتطلب أوّلا نظامًا سياسيًا ذا موارد اقتصادية، وهو أمر صعب بالنظر للمصاعب التي سيواجهها هذا النظام من المجتمع الدولي، وكذلك عدم القدرة على الحصول على اليورانيوم بسهولة من السوق. أما السلاح الإلكتروني فينشأ على أيدي مجموعة محترفين في أنظمة الحاسوب والإنترنت، ويمكن أن تستخدمه أي جهة، من الأنظمة المتهالكة وحتى الجماعات المتطرفة وعصابات المافيا والمخدرات، فقط مقابل المال.

ادفع إن استطعت لمحترفي الهجمات الإلكترونية وسينفذون لك ما تريد.

هذا التحول سيغيّر كثيرًا من طبيعية الصراعات الدولية، والتي تبتعد منذ سنوات عن نمط حروب الدول

القومية ذات السيادة، والجيوش النظامية بثقلها. الحروب الإلكترونية اليوم قد تكون موجهة لدولة، أو ربما شركة، أو جماعة.

إن عاجلًا أم آجلًا ستتمكن مجموعات المهندسين المحترفين في شتى البلدان والشركات من التعرّف على تلك الهجمات ووقفها، بل وربما ردعها بهجوم مضاد، وهو ما يطرح تساؤلًا هامًا، على سبيل المثال، ماذا لو كانت شركة سوني قد نجحت في فعل ذلك، وهاجمت إلكترونيًا مبرمجي كوريا الشمالية، هل كان النظام الكوري ليعتبر ذلك هجومًا من الشركة، أم من الولايات المتحدة نفسها حيث يقع مقر الشركة؟ النظام هناك مجنون بما يكفي ليتجه بتفكيره نحو اعتبار شيء كهذا إعلان حرب أمريكي، إلى ما قد يؤدي تطور كهذا؟

ستكشف لنا السنوات القادمة كيف يمكن لتلك الحوادث أن تؤثر على العلاقات بين الدول، وطبيعة الحروب، ولكن الأكيد هو أنها ستزداد شيوعًا، وهو ما يعني أن الشركات الكبرى تحتاج إلى أنظمة هجوم إلكتروني، لا دفاع إلكتروني فقط، إذ أن هجمات كهذه قد تدمر الشركات تمامًا.

البنوك أيضًا ستحتاج إلى هذه الأنظمة، وعلى العكس من حالة الهجوم على سوني مؤخرًا، قد يكون بعض مهاجمي البنوك من المتعاطفين مع روسيا، أو العاملين بتشجيع من الكرملين، ولننظر على سبيل المثال إلى "تارجت"، سلاح إلكتروني (كود أو شفرة) كتبه روسي يبلغ من العمر 17 عامًا، وأدخله إلى الشبكة الافتراضية لأحد مقاولي القطاع الخاص المتخصصين في التدفئة والتهوية، وهو ما أدى إلى أزمة في الشركة المعنية وكلف مديرها التنفيذي منصبه. في المستقبل، سيكون نطاق هجمات كهذه أوسع، وستكون الأهداف أكبر من مجرد شركة تدفئة.

منذ حوالي عشر سنوات، أصبح لزامًا على مجالس الإدارات في مختلف الشركات أن تضم على الأقل عضوًا واحدًا متخصصًا في التدقيق في الحسابات. في خمس سنوات، سيكون ربما لزامًا أن تضم مجالس الإدارات خبيرًا متخصصًا في الهجوم والدفاع الإلكتروني، وإلا أصبحت تلك نقطة ضعف شديدة للشركة في عالم الإدارة مستقبلًا.

بالنسبة للحكومات والدول القومية، ستحتاج الدول الأعضاء في الحلف الواحد، أو في الجوار الإقليمي الواحد، أن تطور منظومة من القواعد والأسس، كما حدث في الستينيات مع الأسلحة النووية، لضبط عالم التسلّح الإلكتروني.

بالطبع، سيستغرق هذا وقتًا طويلًا، مثلما استغرق تطوير اتفاقيات لحظر انتشار السلاح النووي وقتًا طويلًا بعد تطوير القنبلة النووية. بيد أن هذه الاتفاقيات كانت مهمة للحفاظ على السلام الدولي.

غياب إطار قانوني ودبلوماسي لحوكمة عالم التسلّح الإلكتروني سيعني ببساطة أن النظام الدولي سيتحوّل لغابة من الدول والشركات، البقاء فيه للأقوى، وهو ما يعني تكرر ما جرى سوني بوتيرة أعلى. المسألة فقط مسألة وقت.

المصدر: هافنغتون بوست