حريق سنترال رمسيس: عطل تقني أم هجوم إلكتروني؟ تحليل لسيناريوهات ما جرى

حمزة حسن | July 8, 2025

شهدت مصر خلال الأيام القليلة الماضية حادثة صادمة تمثلت في حريق ضخم في سنترال رمسيس، ما أدى إلى توقف العديد من الخدمات الإلكترونية الحيوية في البلاد، مع تأثير واسع على الاتصالات والإنترنت. هذا الحادث لم يكن مجرد عطل تقني عادي، بل يُعد كارثة بكل المقاييس تعكس هشاشة البنية التحتية الرقمية في مصر، وتكشف مدى الإخفاقات الحكومية المتراكمة خلال السنوات الماضية.

في ظرف أسبوع واحد فقط، تعرض نظام الانقلاب بقيادة عبد الفتاح السيسي لسلسلة من الصدمات: حوادث متكررة على الطرق السريعة، انقطاع متكرر للكهرباء، وأخيرًا حادثة حريق السنترال التي كشفت هشاشة الأجهزة والمعدات، رغم الإنفاق الضخم على مدار عشر سنوات. هذا الأمر دفع البعض إلى التساؤل عن احتمالية وجود أيادٍ خفية تحاول ضرب النظام وإضعافه، في ظل تزايد التوترات الداخلية والخارجية.

ولكن هل من الممكن أن يكون هذا الحريق نتيجة لهجوم إلكتروني متطور؟ الواقع أن التكنولوجيا اليوم تتيح سيناريوهات متعددة، حيث يمكن للهجمات السيبرانية المتقدمة أن تؤدي إلى أضرار فيزيائية خطيرة، وليس فقط

تعطيل البيانات أو الخدمات.

كيف يمكن للهجمات الإلكترونية أن تتسبب في حرائق؟

هناك نوع نادر ومتقدم من الهجمات الإلكترونية التي تستغل ثغرات في الأجهزة والأنظمة للتحكم في عملها بطرق تؤدي إلى أضرار فيزيائية، مثل:

- **تعطيل نظام التبريد:** قد يقوم المهاجم بإيقاف أو تعطيل نظام تبريد الأجهزة، مما يؤدي إلى ارتفاع درجة حرارتها بشكل مفرط، وبالتالي احتراقها.

- **زيادة الحمل على المعالج:** يمكن إرسال أوامر لجعل المعالج يعمل بأقصى طاقته لفترة طويلة، ما يرفع درجة حرارته إلى مستويات خطيرة.

- **الهجمات الكهرومغناطيسية (EM Attacks):** تستخدم أجهزة متخصصة لإرسال إشارات كهرومغناطيسية تؤثر على الدوائر الكهربائية داخل الأجهزة، مسببة تلفًا أو اشتعالًا.

تنفيذ هذه الهجمات عن بُعد يتطلب وجود ثغرات في نظام الحماية أو شبكة غير آمنة، بينما الهجمات التي تعتمد على تأثير كهربائي مباشر تحتاج إلى قرب مادي أو معدات متقدمة.

الدول التي تمتلك القدرة على تنفيذ مثل هذه الهجمات تشمل الولايات المتحدة، روسيا، الصين، إسرائيل، وغيرها من الدول المتقدمة في مجال الأمن السيبراني.

ماذا يعني هذا بالنسبة لمصر؟

حادثة حريق سنترال رمسيس ليست فقط عطلًا تقنيًا، بل مؤشر على ضعف بنية تحتية حيوية مُعرّضة لمخاطر متزايدة في عالم تزداد فيه الهجمات السيبرانية تعقيدًا وخطورة نتيجة لسوء الإدارة المالية في مصر والفساد المستشري منذ عشر سنوات. ومع هذا، تبقى هناك تساؤلات حول مدى استعداد النظام الانقلابي للتصدي لهذه التحديات، خاصة في ظل الشكوك المتزايدة حول وجود هجمات مقصودة تهدف إلى زعزعة الاستقرار السياسي والاقتصادي.

في نهاية المطاف، ما شهدته مصر مؤخراً من حوادث متكررة يضع البلاد أمام اختبار حقيقي لمدى قدرتها على حماية بنيتها التحتية الإلكترونية، والتي أصبحت عمادًا أساسيًا في الحياة اليومية والاقتصادية.