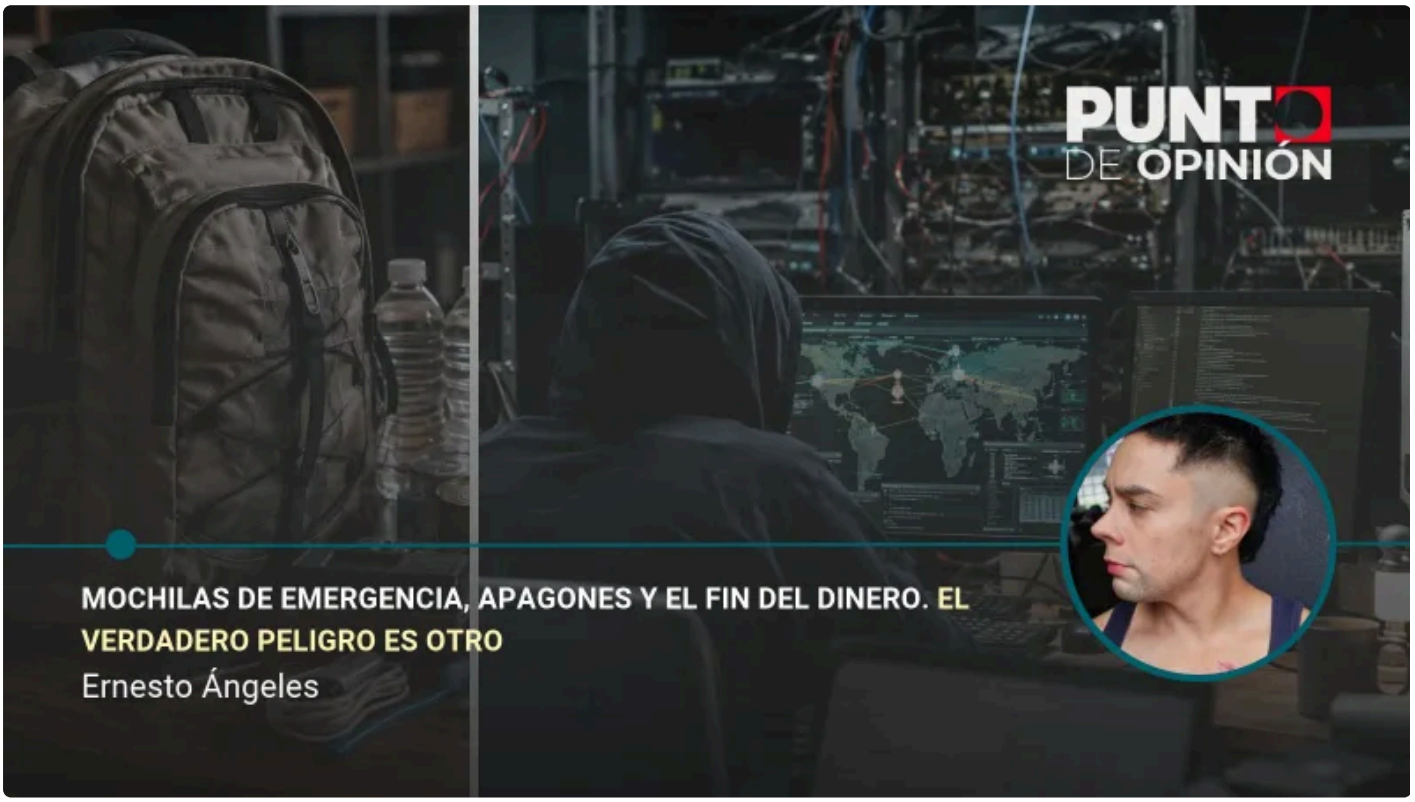
OPINIÓN

Mochilas de emergencia, apagones y el fin del dinero. El verdadero peligro es otro

Por Ernesto Ángeles · 12 de noviembre de 2026 · 6 min de lectura



Desde hace días ha circulado en las redes sociales cierta sensación de paranoia sobre un cataclismo inminente, la cual se disparó con las publicaciones de diversos gobiernos llamando a su población a mantener una mochila con provisiones en caso de alguna emergencia. No obstante, pronto la paranoia cobró tintes tecnológicos, en parte debido a los incidentes cibernéticos en bancos japoneses y en parte a los ciberataques sufridos en Europa.

Esta situación culminó en una fusión de eventos y preocupaciones que dieron como resultado teorías como: que hay una IA fuera del control que necesitan eliminar, por lo que apagarán la electricidad en el mundo; que hay hackers con inmensas capacidades y ganas de destruir todo; así como un supuesto “apagón” masivo que iniciaría en sistemas críticos como la banca japonesa y se extendería rápidamente, dejando al mundo sin dinero y en caos...

Para comenzar, es importante separar las razones detrás del porqué los gobiernos hacen llamados a su población a la prevención, las cuales no son por un cataclismo inminente como tal, sino para la preparación ante escenarios complejos que se vislumbran en el panorama: calentamiento global, crisis geopolíticas, problemas cibernéticos. Esto no implica el fin del mundo o siquiera de Estados o regiones, pero sí un riesgo latente y perenne a peligros específicos, los cuales son difíciles o imposibles de prever.

Si hablamos del riesgo tecnológico, gobiernos y empresas han emitido alertas por la inteligencia artificial: desde el miedo cotidiano usado para vender acciones, hasta una preocupación real por el uso de IA para cometer crímenes. Y si bien el riesgo no es tan exagerado como para acabar con el mundo, sí existen una serie de indicadores que

apuntan a que la tecnología será un asunto de seguridad nacional cada vez más preocupante.

Diversas agencias de seguridad como la alianza de los Cinco Ojos o la Agencia de Ciberseguridad de la Unión Europea (ENISA), constatan que la IA está "acelerando la velocidad, escala y sofisticación de los ciberataques". Gracias a modelos más potentes de IA, una persona o grupo de personas pueden hacer el trabajo que antes requería equipos enteros altamente especializados. En un contexto con actores no sólo con conocimiento, sino más capacidades, esto se puede traducir en problemas para la seguridad nacional, regional y mundial.

En este contexto es donde suceden los incidentes en Europa, mismos que son atribuidos a Rusia y su ecosistema cibernético, y en menor medida a China e Irán: ataques contra la infraestructura de energía en Polonia; ataques a sistemas de refrigeración en 11 países y el uso de IA (Claude) para evadir defensas en más de 20 organizaciones de la UE.

El panorama se complica aún más si no solo consideramos el aumento de la capacidad de ataque habilitada por la IA, sino también la obsolescencia de las infraestructuras físicas y digitales. Solemos olvidar que los espacios digitales también son construcciones humanas: aunque se muestren abstractos, numéricos y sintácticos, son estructuras socio-técnicas que se han construido, reproducido y transformado históricamente mediante la coordinación de millones de personas.

Diariamente habitamos y utilizamos espacios digitales de diversa naturaleza; sin embargo, no todos cuentan con las mismas condiciones. Mientras las grandes plataformas corporativas suelen disponer de presupuestos, equipos especializados y recursos para mantener sus infraestructuras, muchos sistemas públicos, municipales y pequeños operan con recursos limitados, lo que reduce su capacidad de mantenimiento, defensa y respuesta.

Esta desigualdad también se reproduce entre y al interior de regiones, países e instituciones. Quienes se encuentran fuera de los principales centros de poder tecnológico suelen tener menos recursos para proteger sus infraestructuras y una mayor dependencia de proveedores y tecnologías que no controlan.

Es aquí donde el incidente de Japón cobra sentido, ya que no se trató de un ciberataque, sino de una masiva avería técnica que reveló una vulnerabilidad estructural en su sistema financiero: la concentración de infraestructura, de las 254 cooperativas de crédito *shinkin* del país, el 93% dependen de una misma plataforma compartida[1].

Este incidente, aunque no fue un ciberataque, ilustra la lógica que subyace a los ataques europeos: infraestructuras concentradas y mal mantenidas. Y si un centro como Japón es vulnerable por concentración, la periferia lo es aún más por falta de mantenimiento, personal y capacidad de recuperación.

Si tomamos en consideración ambos factores —mayor capacidad de ataque y sistemas obsoletos, vulnerables y poco atendidos—, aún falta el factor de la voluntad. La IA amplía la capacidad, la obsolescencia crea la vulnerabilidad, pero sin voluntad no hay ataque. Esa voluntad puede apuntar a objetivos económicos, políticos o sociales, ya sea a nivel local, nacional o internacional. El problema es que no todos tienen la misma capacidad de respuesta o defensa, pero sí hay más capacidad de ataque disponible para quien quiera usarla.

¿Y todo esto qué significa? ¿Por qué es importante en el contexto de riesgos y crisis a futuro? Porque el orden global está en un proceso de transformación, del orden unipolar hacia la multipolaridad; esto se traduce en el sistema tecnológico global en una fractura parcial hacia múltiples sistemas tecnológicos -con una capa funcional global de fondo, con capacidades limitadas-. Esto puede traducirse en un aumento de la inseguridad, ya que no habrá tantas limitantes por la interdependencia y sí más incentivos para buscar una ventaja.

El resultado no es un mundo sin restricciones, sino un mundo con restricciones asimétricas: alta cooperación intrabloque, alta competición interbloque. El problema es que, tanto entre bloques como en su interior, habrá centros con capacidad de absorción y periferias vulnerables de este nuevo mundo.

Por tanto, en lugar de entregarnos a la paranoia, haríamos mejor en buscar respuestas a cuestiones como: ¿son las infraestructuras digitales del Estado lo suficientemente seguras? ¿Existe corresponsabilidad real entre Estado y empresas? ¿Y quién protege a los municipios, hospitales y cooperativas que no tienen ni el capital ni el personal para defenderse? La pregunta no es si habrá un cataclismo, sino cuántos cataclismos locales estamos dispuestos a tolerar antes de actuar.

[1] https://www.negocios.com/actualidad/japon-descubre-nuevo-fallo-apagon-128-bancos/20261109202327497630.html

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/opinion/mochilas-de-emergencia-apagones-y-el-fin-del-dinero-el-verdadero-peligro-es-otro
Descargado el 21 de noviembre de 2026.