**Referencias documentales**

Cielo negro: Europa ante la posibilidad de un apagón general

*Electricidad, guerra híbrida, soberanía tecnológica, poder financiero y reconfiguración del orden geopolítico mundial.*

1. Reino Unido — National Risk Register 2025 Prioridad máxima Cabinet Office · 187 páginas Examina un escenario de ataque cibernético contra la red eléctrica nacional. Contempla pérdida generalizada de suministro, efectos sobre agua, combustibles, telecomunicaciones y servicios públicos. Estima que la recuperación completa podría requerir hasta siete días, mientras algunos servicios críticos podrían tardar meses en normalizarse.
2. Comisión Europea — Fortifying Defence: Strengthening Critical Energy Infrastructure Against Hybrid Threats (2025) Prioridad máxima Joint Research Centre · 2025 Estudia las dependencias entre infraestructura energética y defensa militar, así como las herramientas que podrían emplear actores adversarios para degradar su funcionamiento. Es particularmente importante para el análisis de la OTAN, la guerra híbrida y la vulnerabilidad de las instalaciones estratégicas.
3. Lloyd's — Business Blackout (2015) Prioridad máxima Lloyd's of London · Cambridge Centre for Risk Studies Construye una simulación de ataque informático contra generadores eléctricos del nordeste estadounidense. El escenario contempla 93 millones de personas sin electricidad y pérdidas económicas estimadas en 243.000 millones de dólares, que podrían superar el billón en una variante extrema. Es un documento especialmente valioso porque demuestra cómo una interrupción energética puede propagarse hacia mercados, seguros, industrias y finanzas.
4. Unión Europea — Risk Assessment Report on Cyber Resilience of Telecommunications and Electricity Sectors (2024) Comisión Europea · ENISA · Estados miembros Identifica vulnerabilidades en cadenas de suministro, redes 5G, infraestructuras renovables, sistemas operativos industriales, ransomware y amenazas respaldadas por Estados.
5. ACER — Security of EU Electricity Supply: 2025 Monitoring Report Agencia de Cooperación de los Reguladores de la Energía Evalúa suficiencia de generación, preparación ante riesgos, interdependencias sectoriales y coordinación transfronteriza.
6. Asamblea Parlamentaria de la OTAN — Strengthening the Protection of Critical Infrastructure Against Cyber Threats (2022) Comisión de Defensa y Seguridad. Examina amenazas contra energía, telecomunicaciones, bancos, hospitales y transporte, y reclama respuestas nacionales y colectivas.

**II. Documentos estadounidenses: inteligencia, infraestructura y amenazas estratégicas**

*Aquí encontramos material particularmente relevante para comprender cómo las grandes potencias analizan la posibilidad de que una crisis informática se transforme en una crisis física.*

7. Annual Threat Assessment of the U.S. Intelligence Community (2026). Elaborado por la comunidad de inteligencia estadounidense y presentado ante los comités de supervisión del Congreso. Es una fuente fundamental para estudiar las evaluaciones públicas de amenazas extranjeras, ciberoperaciones, rivalidad entre potencias y seguridad nacional.
8. CISA, NSA y FBI — PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024). Documento especialmente importante El informe conjunto analiza la actividad atribuida al grupo conocido como Volt Typhoon. Las agencias estadounidenses sostienen que actores vinculados con China habían conseguido introducirse en redes de organizaciones pertenecientes a sectores estratégicos, incluidos energía, comunicaciones, transporte y agua. La evaluación advierte sobre la posibilidad de que esos accesos previamente establecidos pudieran utilizarse para perturbar funciones operativas durante una crisis o conflicto. Es una de las fuentes más importantes para estudiar la diferencia entre espionaje informático y preparación de capacidades potencialmente disruptivas.
9. U.S. Department of Homeland Security — Homeland Threat Assessment 2025. Examina amenazas contra infraestructuras estadounidenses y operaciones de inteligencia extranjera. Incluye consideraciones sobre penetración de redes críticas y actividad atribuida a actores estatales.
10. Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (EMP Commission). Prioridad máxima. Esta comisión fue establecida para evaluar los efectos potenciales de un pulso electromagnético de gran altura sobre sistemas militares y civiles.

Sus investigaciones contemplan:

- Vulnerabilidad de redes eléctricas.
- Sistemas de comunicaciones.
- Infraestructura civil.
- Capacidad de recuperación nacional.
- Protección de instalaciones esenciales.
- Costos de endurecimiento de sistemas críticos.

*Es especialmente interesante para analizar escenarios en los cuales la interrupción eléctrica no se produce mediante un ataque informático convencional.*

11. U.S. Government Accountability Office — Electricity Grid Resilience. Examina vulnerabilidades derivadas de fenómenos meteorológicos extremos, ataques informáticos y acontecimientos electromagnéticos. También estudia las dificultades para mantener reservas de transformadores eléctricos.

12. GAO — Electricity Grid: DOE Could Better Support Industry Efforts to Ensure Adequate Transformer Reserves (2023). Este documento es particularmente interesante desde la perspectiva geoeconómica: estudia la escasez de grandes transformadores, los plazos de fabricación, los costos de transporte y las dificultades para mantener equipos de reemplazo.

**III. Los documentos del poder económico y la gobernanza global**

13. World Economic Forum — Global Risks Report 2026 Examina confrontación geoeconómica, conflictos entre Estados, inseguridad cibernética, desinformación, infraestructura y riesgos tecnológicos. Es importante porque permite estudiar qué preocupaciones comparten los dirigentes económicos y políticos que participan en los espacios de gobernanza internacional.
14. Directiva europea CER 2022/2557 y Directiva NIS2 2022/2555 constituyen dos instrumentos fundamentales para estudiar obligaciones jurídicas, seguridad informática, protección de entidades críticas y capacidad de continuidad de los servicios esenciales.
15. ENTSO-E — Winter Outlook 2025-2026 Analiza la suficiencia de recursos eléctricos en los sistemas europeos durante el invierno. Permite examinar las diferencias nacionales, la dependencia de interconexiones y las vulnerabilidades regionales.

**IV. Los documentos que verdaderamente debemos buscar bajo la categoría de «secretos de Estado»**

► MI5 / MI6: Evaluaciones de amenazas contra infraestructuras estratégicas y operaciones extranjeras
► GCHQ: Ciberamenazas, seguridad de redes y protección de comunicaciones
► NSA: Evaluaciones de amenazas cibernéticas y seguridad de sistemas críticos
► CIA: Análisis históricos desclasificados sobre vulnerabilidades estratégicas
► DIA: Evaluaciones de capacidades militares y amenazas híbridas
► NATO: Resiliencia nacional, protección de infraestructuras y continuidad operativa
► FEMA: Ejercicios de emergencia y recuperación de servicios esenciales
► CISA: Alertas de amenazas contra redes eléctricas e instalaciones críticas
► ENISA: Evaluaciones europeas de amenazas informáticas
► ENTSO-E. Escenarios de riesgo y suficiencia eléctrica continental
► IEA: Seguridad energética, reservas y vulnerabilidades de suministro

*Hay tres líneas especialmente interesantes:*

1. EMP y ataques electromagnéticos: informes desclasificados de comisiones estadounidenses, testimonios militares y documentación sobre recuperación de redes.
2. Continuidad gubernamental: programas de continuidad de operaciones, instalaciones alternativas, comunicaciones de emergencia y protección de autoridades.
3. Ejercicios de simulación: ejercicios de mesa y simulaciones de crisis energética, ataques cibernéticos, interrupciones financieras y emergencias transfronterizas.

*No debe confundirse un ejercicio de simulación con un plan operativo para ejecutar una catástrofe. Precisamente, su valor documental reside en revelar qué vulnerabilidades consideran importantes las instituciones y qué capacidades pretenden conservar.*