DO CIBERATAQUE POR IA AO APAGÃO - A CADEIA TÉCNICA DO IMPACTO NO SETOR ELÉTRICO

Autores: Marcelo Branquinho e Plataforma Safer

30/01/2026

Resumo: O setor elétrico é uma infraestrutura crítica essencial que sustenta diversos serviços da sociedade moderna. Com sua crescente digitalização — por meio de smart grids, IEDs e sistemas de controle interconectados — surgem novas vulnerabilidades, especialmente em protocolos legados sem segurança nativa.

A ameaça se intensifica com o uso da inteligência artificial (IA) por agentes maliciosos, que podem realizar ataques cirúrgicos, silenciosos e altamente eficazes, manipulando parâmetros operacionais sem serem detectados.

Esses ataques exploram falhas sistêmicas, promovendo degradações graduais que podem resultar em apagões regionais, afetando hospitais, transportes e comunicações. Em cenários mais críticos, usinas hidrelétricas podem ser comprometidas, pondo em risco a estabilidade energética e a segurança pública.

A IA transforma os ataques cibernéticos em ameaças assimétricas, sofisticadas e de difícil mitigação, exigindo atenção urgente à proteção do setor elétrico digitalizado.

Palavras-chave: Infraestruturas Críticas, Setor Elétrico, Ataques Cibernéticos, Inteligência Artificial (IA), Smart Grids, Protocolos Legados, Apagão, Segurança Operacional

POWERED BY SAFER

1. Introdução

O setor de energia elétrica ocupa uma posição singular no contexto das infraestruturas críticas, pois atua como **elemento estruturante e habilitador de praticamente todos os demais serviços essenciais da sociedade moderna**. Sistemas de telecomunicações, hospitais, transporte público e privado, saneamento básico, serviços financeiros, cadeias logísticas, data centers e operações industriais dependem diretamente de um fornecimento elétrico **estável, contínuo e previsível**. Qualquer degradação significativa nesse fornecimento tende a produzir efeitos em cascata, ampliando exponencialmente o impacto inicial de um incidente.

Essa centralidade transforma o setor elétrico em um **alvo estratégico prioritário** para ataques cibernéticos, sobretudo em cenários de conflito híbrido, terrorismo digital, sabotagem econômica ou extorsão em larga escala. Quando esses ataques passam a ser potencializados pelo uso de **inteligência artificial**, o risco deixa de ser meramente tecnológico e passa a assumir uma dimensão **sistêmica, social e até geopolítica**.

2. A Digitalização do setor elétrico e o surgimento de novas vulnerabilidades

A digitalização progressiva do setor elétrico, impulsionada por iniciativas de *smart grids*, automação avançada, integração de fontes renováveis intermitentes e necessidade de maior eficiência operacional, ampliou significativamente a superfície de ataque. Subestações digitais, centros de controle integrados, sistemas de proteção adaptativa, dispositivos de campo inteligentes (IEDs) e plataformas de análise em tempo real passaram a operar de forma altamente interconectada.

Em muitos casos, essa interconexão ocorre sobre **protocolos legados**, como IEC 60870-5-104, DNP3 ou Modbus, originalmente

concebidos para ambientes isolados, sem mecanismos robustos de autenticação, criptografia ou validação de integridade.

A introdução de conectividade — ainda que necessária para atender às demandas operacionais atuais — expôs **fragilidades estruturais profundas**, criando um ambiente no qual falhas cibernéticas podem se traduzir diretamente em falhas físicas. Em um contexto tradicional, um ataque exigiria conhecimento profundo e atuação manual intensa. Com o uso de IA, essa barreira técnica é drasticamente reduzida.

3. A IA aplicada a ataques no setor elétrico e suas consequências

A inteligência artificial aplicada a ataques contra o setor elétrico permite um **grau de compreensão sistêmica** que seria inviável por meios puramente humanos. Modelos inteligentes conseguem analisar grandes volumes de dados operacionais históricos e em tempo real, identificar padrões de carga, compreender ciclos de consumo, antecipar respostas automáticas de proteção e inferir relações de dependência entre ativos críticos. Com base nesse aprendizado, ataques podem ser **planejados de forma cirúrgica**, visando maximizar impacto com mínima intervenção direta e reduzida probabilidade de detecção imediata.

Por exemplo, em um **centro de controle de energia**, um ataque baseado em IA pode manipular sutilmente dados de telemetria, apresentando aos operadores uma visão aparentemente normal da rede enquanto, em segundo plano, limites operacionais são gradualmente tensionados. Pequenas discrepâncias em medições de tensão ou frequência podem induzir decisões equivocadas, levando ao desligamento preventivo de linhas ou à sobrecarga de transformadores. Para o operador humano, o evento se apresenta como uma sequência de falhas técnicas não relacionadas, dificultando a identificação de uma ação coordenada.

Em vez de provocar interrupções imediatas, abruptas e ruidosas — que acionariam alarmes, planos de contingência e investigações

rápidas — a IA favorece **estratégias de degradação progressiva**. Pequenos ajustes em parâmetros de proteção, alterações discretas em tempos de resposta de relés digitais ou manipulações sutis em lógicas de automação podem comprometer a confiabilidade do sistema ao longo de horas ou dias. Esses desvios tendem a ser interpretados inicialmente como desgaste natural de equipamentos, falhas de calibração ou efeitos colaterais da variabilidade das fontes renováveis.

Em uma **subestação**, por exemplo, a IA pode identificar quais relés de proteção são mais sensíveis a ajustes mínimos e quais alimentadores são críticos para o equilíbrio regional da carga. Uma alteração aparentemente insignificante nos tempos de atuação pode causar desligamentos em cascata quando o sistema entra em uma condição de estresse, como um pico de demanda ou uma contingência climática. O resultado pode ser um apagão regional cuja causa aparente é “instabilidade operacional”, quando, na realidade, foi cuidadosamente induzida.

Em **usinas hidrelétricas**, o impacto pode ser ainda mais grave. Sistemas de controle de turbinas, comportas e vertedouros dependem de automação precisa e sincronizada. Um ataque baseado em IA pode manipular leituras de nível, vazão ou pressão, levando o sistema a operar fora do ponto ótimo. Isso pode resultar em desligamentos de emergência, danos mecânicos, redução abrupta da capacidade de geração ou, em cenários extremos, riscos à segurança estrutural da barragem. Mesmo sem causar um desastre físico imediato, a simples retirada de grandes unidades geradoras do sistema pode desestabilizar todo o grid interligado.

Casos documentados de ataques ao setor elétrico em diferentes países já demonstraram que a exploração de **poucos pontos estratégicos** é suficiente para desencadear apagões em larga escala, afetando milhões de pessoas. A inteligência artificial amplia dramaticamente essa capacidade ao permitir **simulações prévias de cenários de falha**, avaliando impactos técnicos, operacionais e sociais antes mesmo da execução do ataque. Dessa forma, o agressor pode escolher o momento mais sensível — como períodos de pico de

consumo, eventos climáticos extremos ou grandes eventos públicos — para maximizar o efeito disruptivo.

As consequências para a população vão muito além da simples falta de energia. Apagões prolongados afetam hospitais e serviços de emergência, interrompem o fornecimento de água, paralisam sistemas de transporte, comprometem comunicações e geram perdas econômicas significativas. Em ambientes urbanos densos, a perda simultânea de energia e telecomunicações pode rapidamente evoluir para uma crise de ordem pública, colocando em risco a segurança e o bem-estar da sociedade.

4. Conclusão

Nesse contexto, ataques cibernéticos baseados em IA contra o setor elétrico representam uma **ameaça silenciosa, sofisticada e profundamente assimétrica**. São difíceis de detectar em estágios iniciais, complexos de mitigar após sua materialização e capazes de produzir impactos físicos e sociais desproporcionais ao esforço técnico empregado. A transição do ciberataque para o apagão deixa, assim, de ser um cenário hipotético e passa a constituir um risco concreto e iminente para infraestruturas críticas altamente digitalizadas.