# Riscos de ataques cibernéticos no Setor Elétrico Brasileiro[1]

Nivalde de Castro[2]

Gustavo Esteves[3]

Rachel S. G. Almeida[4]

O setor elétrico vem passando por transformações substanciais em sua estrutura e em seus mecanismos de operação. Historicamente, o sistema organizou-se em torno de grandes usinas e de uma extensa malha de transmissão e distribuição de energia elétrica, com sistemas de controle relativamente centralizados. Todavia, nos últimos anos, o setor tornou-se progressivamente mais digitalizado, conectado e descentralizado, refletindo a própria dinâmica da transição energética.

A incorporação de novas tecnologias, como sensores e sistemas de comunicação, de supervisão e de controle remoto, ampliou a capacidade de monitoramento e operação das redes elétricas. Parte dessa transformação digital é atribuída à expansão dos recursos energéticos distribuídos, como a geração solar fotovoltaica nas residências, que multiplicou os equipamentos e agentes conectados ao sistema, exigindo, também, a modernização dos recursos de comunicação e coordenação do sistema elétrico.

Embora essas transformações representem avanços importantes, também introduzem novos desafios à segurança e à confiabilidade do sistema como um todo. Entre os desafios, destaca-se a crescente exposição da infraestrutura da rede elétrica às ameaças cibernéticas. Neste sentido, a maior conectividade entre sistemas digitais e equipamentos responsáveis pela operação física da rede elétrica amplia as possibilidades de acesso indevido, manipulação de comandos e comprometimento de dispositivos essenciais.

Para qualificar melhor o risco, convém distinguir dois tipos de tecnologia. A tecnologia da informação (TI) compreende os sistemas administrativos e bancos de dados. O segundo tipo é tecnologia operacional (OT, na sigla em inglês), que envolve o controle de equipamentos físicos, como disjuntores, subestações, geradores e turbinas. Invadir a OT é diferente de invadir a TI, uma vez que,

---

[1] Artigo publicado pelo Broadcast Energia. Disponível em: https://energia.aebroadcast.com.br/tabs/news/747/57739682. Acesso em: 27.10.2026

[2] Professor do Instituto de Economia da UFRJ e Coordenador-Geral do Grupo de Estudos do Setor Elétrico (Gesel-UFRJ). Escreve quinzenalmente para a Broadcast.

[3] Mestrando em Políticas Públicas, Estratégias e Desenvolvimento pela Universidade do Rio de Janeiro (UFRJ) e pesquisador do Gesel-UFRJ

[4] Mestranda em Ciências Militares na Escola de Comando e Estado-Maior do Exército (ECEME) e pesquisadora do Gesel-UFRJ.

neste caso, o ataque cibernético restringe-se ao vazamento de informações. Por outro lado, os ataques direcionados às tecnologias operacionais podem provocar danos a equipamentos, prejudicar a supervisão e o controle das instalações e, em situações mais graves, comprometer a continuidade do fornecimento de energia.

Um episódio recente ilustra a dimensão desse problema. Na Polônia, entre os dias 29 e 30 de dezembro de 2025, em pleno inverno europeu, cerca de 30 instalações de geração de energia foram alvo de ataques cibernéticos coordenados. Embora não tenha ocorrido uma interrupção generalizada do fornecimento de eletricidade, a invasão comprometeu os sistemas operacionais e provocou danos a equipamentos, com perda de comunicação e obstrução do controle remoto das instalações afetadas.

O ataque empregou um programa malicioso do tipo *wiper* (ou "apagador"). Ao contrário dos vírus, que roubam dados ou sequestram arquivos para exigir resgate, o *wiper* é mais destrutivo, pois apaga o conteúdo dos computadores e os deixa inutilizáveis. Segundo as autoridades polonesas, se a operação tivesse dado certo, cerca de 500 mil pessoas poderiam ter ficado sem eletricidade, em um período de baixas temperaturas e nevascas.

O ataque polonês foi considerado o primeiro grande ataque dirigido especificamente a sistemas de energia descentralizados. Essas instalações são numerosas, dependem de conexão remota e costumam receber menos investimento em segurança do que as grandes usinas. Um relatório elaborado por instituição polonesa constatou a existência de pouca proteção em computadores usados para monitorar e controlar parte da operação.
Esse caso atestou a vulnerabilidade de instalações conectadas e controladas remotamente, demonstrando que ameaças digitais podem ultrapassar os sistemas de informação e alcançar a infraestrutura física responsável pelo fornecimento de energia elétrica. Assim, a experiência polonesa oferece um alerta ao Brasil, cujo setor elétrico também atravessa um processo de crescente digitalização e expansão da geração distribuída.

Portanto, à medida que se multiplicam os equipamentos conectados e as interfaces de comunicação e interação, torna-se necessário criar protocolos e mecanismos de proteção cibernética que acompanhem a gradativa transformação digital do sistema elétrico, tanto no nível das distribuidoras quanto, principalmente, no nível da geração-transmissão sob coordenação direta do Operador Nacional do Sistema Elétrico (ONS). Nesse âmbito, cabe reconhecer que a segurança do suprimento não dependerá apenas da proteção das grandes instalações e dos centros de operação, mas também da capacidade de prevenir, identificar e responder a ameaças que alcancem os diferentes agentes e dispositivos conectados à rede.

A magnitude dos sistemas de micro e minigeração distribuída solar (MMGD), um dos principais vetores de transformação da operação do Setor Elétrico Brasileiro (SEB), merece atenção e dimensionamento. Segundo dados da Agência Nacional de Energia Elétrica (Aneel), a capacidade instalada dos painéis solares implantados no telhado de residências ou de grandes estabelecimentos, com potência de até 5 MW, ultrapassou a cifra de 50 GW, representando cerca de 20% do total do parque instalado de geração elétrica, considerando todas as fontes.

Como essa rápida expansão não ocorre sem fricções, dois pontos específicos merecem ser analisados. Primeiro é a característica de ser uma fonte intermitente, cuja geração varia ao longo do dia e que as condições que a afetam não são controláveis. Segundo, a MMGD é descentralizada e não controlada diretamente pelo ONS, cujas responsabilidades se restringem à operação do Sistema Interligado Nacional (SIN), que agrega o conjunto de unidades geradoras centralizadas e o sistema de transmissão de energia elétrica.

Assim, a principal e complexa atribuição do ONS é garantir o equilíbrio entre a oferta e a demanda de energia em todos os segundos, minutos e horas do dia, mas sem qualquer ingerência sobre a MMGD, pois seus detentores podem injetar a energia excedente na rede de distribuição sempre que não for diretamente consumida nas unidades de consumo associadas.

Portanto, a maior participação da geração solar modifica o comportamento da demanda líquida de eletricidade, sobretudo nos períodos de elevada produção durante o dia e de redução acentuada ao entardecer. Essas variações geram situações de estresse do ponto de vista da operação e ampliam a necessidade de flexibilidade operativa, isto é, da capacidade de ajustar a oferta e os recursos disponíveis às condições do sistema.

Garantir o equilíbrio do sistema é uma tarefa naturalmente sensível, e fazê-lo em meio a situações críticas em que a flexibilidade se mostra essencial é ainda mais complexo, com limites constantemente desafiados. Nesse cenário, a disponibilidade de informações confiáveis, a comunicação entre os agentes e a capacidade de executar ações céleres coordenadas de controle são cada vez mais importantes. Concomitante, entretanto, cresce o risco dos danos potenciais resultantes de ataques cibernéticos, tendo em vista que incidentes cibernéticos que comprometam essas funções podem dificultar a resposta a situações críticas e ampliar os riscos à segurança do suprimento de energia elétrica.

O Brasil, todavia, não parte do zero para endereçar esse risco. Em julho de 2021, o ONS publicou a Rotina Operacional RO-CB.BR.01, primeiro marco do SEB dedicado exclusivamente à segurança cibernética e que está em processo de revisão, a ser concluído ainda em 2026. A norma fixa requisitos mínimos para o Ambiente Regulado Cibernético, o conjunto de sistemas submetidos às regras de segurança do operador. Além disso, a Resolução Normativa Aneel nº

964/2021 define as diretrizes para a política de segurança cibernética dos agentes e, em fevereiro deste ano, a agência publicou as Portarias n.º 7.058/2026 e 7.062/2026 sobre o tema.

A existência desse arcabouço é importante, mas o episódio polonês suscita questões que merecem ser examinadas. A primeira é o estabelecimento de requisitos mínimos de segurança para equipamentos conectados à rede e acessíveis remotamente, como os inversores fotovoltaicos, incluindo atualizações de segurança e controle de acesso. A segunda é a definição das responsabilidades de fabricantes, instaladores, distribuidoras e operador pela manutenção dos equipamentos, correção de vulnerabilidades e resposta a incidentes. A terceira é a verificação dos mecanismos de proteção existentes para que abranjam toda a cadeia operacional, especialmente as interfaces de acesso remoto, e preparem o sistema para situações de crise, por meio de simulações, planos de resposta e segmentação de redes. Portanto, a eficácia do arcabouço de proteção e dos protocolos sobre segurança cibernética depende da aplicação dos requisitos de segurança aos diferentes equipamentos e agentes envolvidos.

O Setor Elétrico Brasileiro já lida com riscos hidrológicos e com o novo imperativo da flexibilidade, de modo que se deve atentar para que o risco cibernético não configure uma nova ameaça crítica. Dessa forma, é fundamental que a segurança cibernética seja cada vez mais reconhecida como uma dimensão da segurança de suprimento perante o dinâmico e irreversível processo de transição energética.