lfe
GESEL UFRJ
http://gesel.ie.ufrj.br/ gesel@gesel.ie.ufrj.br

A Crescente relevância do tema segurança cibernética na sociedade: O caso do setor elétrico(1)

Lorrane Câmara (2)
Maurício Moszkowicz (3)
Mariana Freitas (4)

Assim como Isaac Asimov, em seu livro "Eu, Robô", apresentou as três leis da robótica, cinco leis foram enunciadas por Espinosa (2018) para a segurança cibernética: 1) se existir uma vulnerabilidade, ela será explorada; 2) de alguma forma, tudo é vulnerável; 3) os seres humanos confiam mesmo quando não deveriam; 4) com a inovação, surge a oportunidade de exploração; e 5) em caso de dúvida, veja a lei número um. Isto posto, se houver uma vulnerabilidade, ela será explorada, sem exceções.

O setor elétrico tem aplicado maciçamente a automação, a digitalização e técnicas avançadas de tratamento de dados, revolucionado os processos de produção, armazenamento, transporte e consumo de energia. As mudanças estruturais e operacionais decorrentes desse fenômeno e, apesar de terem promovido ganhos consideráveis de eficiência, passam, de maneira crescente, a demandaratenção à questão da segurança cibernética.

Tecnologias sofisticadas e inteligentes, como a utilização da inteligência artifical para controle e monitoramento de sistemas e o uso da rede 5G, são, cada vez mais, parte integrante das redes elétricas. Somam-se a estas as aplicações de IoT (internet das coisas), que promovem a troca de dados e a comunicação entre dispositivos e sistemas, tais como sistemas automatizados e redes e medidores inteligentes, e geram um aumento dos pontos de acesso operacionais, vulnerabilizando o setor.

O setor elétrico torna-se, portanto, gradativamente mais interconectado e complexo, com infraestruturas, sistemas, procedimentos e processos decisórios cada vez mais interdependentes, o que aumenta a sua suscetibilidade a ataques cibernéticos frequentes e variados. A magnitude do problema pode ser constatada pelo crescimento significativo, nos últimos anos, de ataques cibernéticos ao setor elétrico reportados (de 87, em 2015, para 155, em 2019).

Convém destacar que a infraestrutura elétrica foi considerada pela Comunidade Europeia com a de maior criticidade para o funcionamento da sociedade. Um ataque que provoque a interrupção de operações elétricas pode impactar severamente sistemas dependentes, como os setores de comunicações, água, saúde, financeiro e logístico.

Um exemplo marcante da preocupação com a segurança cibernética no setor elétrico pode ser observado mediante a análise das dez recomendações elaboradas pela Agência Europeia de Segurança de Rede e de Informação (ENISA) (ENISA, 2012) para os sistemas de redes inteligentes (smart grid). Este conjunto de recomendações foi fruto de uma abrangente consulta aos atores públicos e privados, na qual 304

especialistas foram contatados, 50 participaram da pesquisa e 23 entrevistas foram realizadas. No contexto das recomendações da ENISA, destacam-se:

i. Enfatizar a formação de conscientização do problema e o desenvolvimento de ações de treinamento de pessoal em diversos níveis de especialização;

ii. Aperfeiçoar o arcabouço regulatório e normativo do setor elétrico;

iii. Estabelecer mecanismos de intercâmbio de experiências e de cooperação entre as diversas empresas envolvidas;

iv. Implantar processos de certificação das empresas segundo normas de segurança cibernética;

v. Estabelecer mecanismos coordenados e centros de comunicação, tratamento e resposta a incidentes de segurança cibernética; e

vi. Promover, junto aos centros académicos, programas de pesquisas e desenvolvimento na área de segurança cibernética.

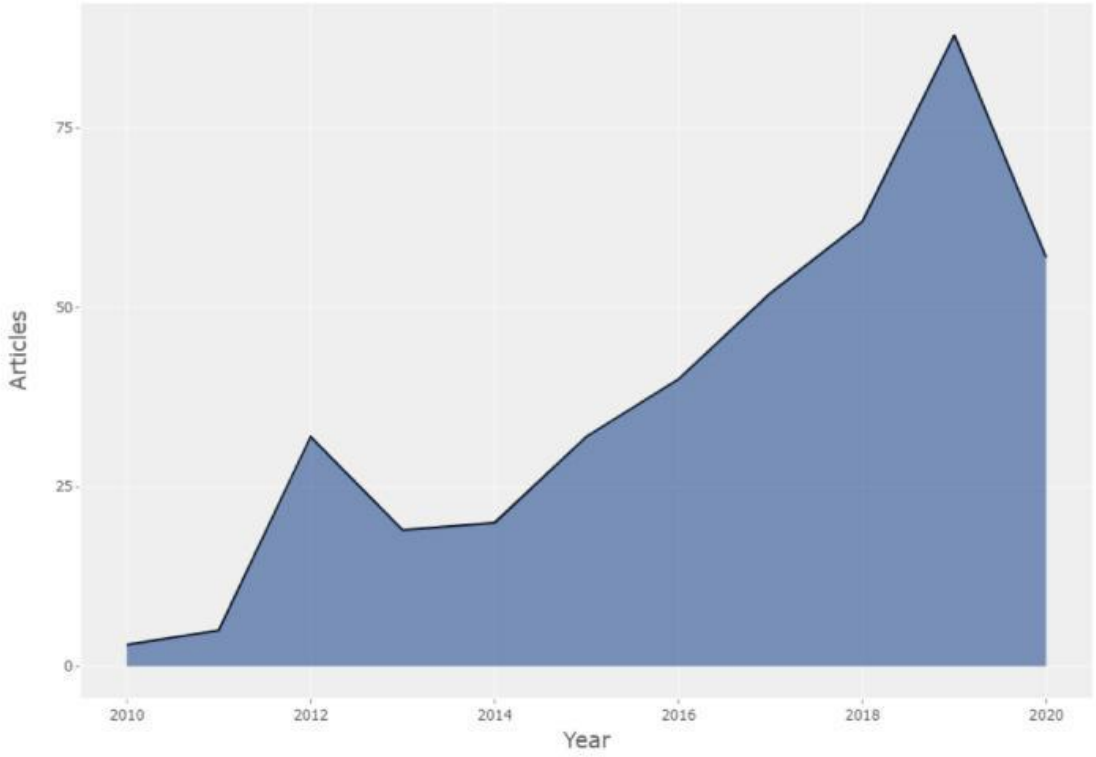
Em resposta à demanda referente ao combate direto a ataques cibernéticos, seja pela criação de legislação específica ou pelo desenvolvimento de tecnologias e softwares voltados à proteção, um número crescente de estudos e pesquisas relacionados ao tema tem sido gerado.

Esta tendência fica evidente na análise bibliométrica conduzida pelo Grupo de Estudos do Setor Elétrico (GESEL), realizada a partir do levantamento de trabalhos acadêmicos, publicados em inglês, entre os anos 2010 e 2020, em duas das principais bases de busca – Scopus e Web of Science. O portfólio final consistiu em 410 documentos, resultado de uma pesquisa filtrada com o uso de combinações das seguintes palavras-chave: segurança cibernética, digitalização, internet das coisas, rede inteligente, rede elétrica, setor elétrico, energia, infraestrutura crítica, protocolos de segurança, padrões e legislação. Apesar do número total de publicações ter sido limitado pela filtragem, sua evolução no decorrer dos anos acompanha a crescente preocupação acerca da segurança cibernética no setor elétrico.

As palavras mais recorrentes nas 410 publicações, apresentadas na nuvem de palavras abaixo (Figura 1), guardam elevada correspondência com temas associados ao contexto de transição do setor elétrico e com a emergência das questões relativas à segurança cibernética no setor.

A partir da bibliometria, foi possível definir que a taxa de crescimento anual de publicações acadêmicas foi de 34%, conforme apresentado na Figura 2, valor justificado, dentre outros fatores, pelos ataques recorrentes a infraestruturas elétricas observados a partir de 2015.

Figura 2. Produção científica anual – Segurança Cibernética



Fonte: Elaboração própria.

O portfólio analisado pela bibliometria sugere que a produção acadêmica sobre o tema é liderada pelos Estados Unidos. O país também se destaca pelos esforços para aprimorar a sua infraestrutura de segurança cibernética, inclusive direcionada especificamente ao setor elétrico. A Proteção de Infraestrutura Crítica (CIP) da Corporação Norte Americana de Segurança Elétrica (NERC) é um padrão que, hoje, consiste em uma lista de onze requisitos que garantem confiabilidade e consistência a operadores do setor elétrico na América do Norte. Este documento, publicado em 2008, foi modificado e atualizado no decorrer dos anos, em resposta à vulnerabilidade cada vez mais evidente do setor elétrico a ataques cibernéticos, espionagem e roubo de dados.

Além deste, os Estados Unidos criaram outros modelos específicos de enquadramento do setor elétrico a padrões de cibersegurança e têm combatido o problema com diversas medidas, tais como a criação de forças-tarefa e comitês estaduais, a participação do Instituto Nacional de Padrões e Tecnologia (NIST) e a atuação do Departamento de Energia, o qual, em 2018, criou um gabinete dedicado à cibersegurança, segurança energética e resposta de emergências.

Ademais, dentre os países que se destacam em publicações acadêmicas sobre o tema, encontram-se, também, a China, a Índia e nações que fazem parte da União Europeia, como o Reino Unido e a Alemanha. Para estes países, a segurança cibernética no setor elétrico tornou-se uma questão central, refletida tanto no universo acadêmico quanto no regulatório.

A posição da China com relação à proteção da rede está inserida em um arcabouço nacional mais amplo de tratamento da segurança cibernética no mais alto nível. Em 2016, foi promulgada a "Lei de Segurança Cibernética", a qual institui normas para a realização de simulações e determina que os operadores de infraestruturas críticas devem desenvolver planos de resposta a incidentes e conduzir exercícios regulares.

No mesmo ano, o Parlamento Europeu publica a Diretiva (UE) nº 1.148/2016, que estabelece regras transversais e um modelo de funcionamento do sistema de segurança cibernética na Europa, visando à proteção dos setores de serviços essenciais. Em 2019, a Diretiva foi complementada pelo Clean Energy for all

Europeans, pacote que inclui quatro atos legislativos voltados ao setor elétrico.

Conscientes das cinco leis da segurança cibernética enunciadas por Espinosa, diversos países estão estabelecendo estratégias e ações para garantir que o processo de digitalização não exponha os consumidores, os operadores do setor elétrico e a economia como um todo a ataques cibernéticos. Ao nível nacional, devem ser destacados:

i. O processo atualmente conduzido pelo Operador Nacional do Setor Elétrico (ONS), em conjunto com as empresas de geração e transmissão, para implementar um Procedimento de Rede de segurança cibernética para os Centros de Operação; e

ii. A Consulta Pública nº 007/2021, que visa estabelecer um diálogo com a sociedade a respeito da Análise de Impacto Regulatório nº 2/2021-SRT-SGI-SRD-SRG/ANEEL, que apresenta alternativas de solução para os problemas relativos à segurança cibernética no Setor Elétrico Brasileiro.

À medida que a digitalização avança e a vulnerabilidade da rede elétrica se torna mais evidente, a segurança cibernética concretiza-se como uma questão central para a sociedade e atrai, como demonstrado pela análise bibliométrica, a comunidade acadêmica para realizar estudos cada vez mais aprofundados. A iniciativa do ONS e a consulta pública sobre segurança cibernética, instaurada pela ANEEL, confirmam a centralidade que o assunto vem assumindo no setor elétrico e consistem em passos importantes para que seja criada uma regulamentação do tema específica para o setor, tal como verificado na China, Estados Unidos e União Europeia.

Referências bibliográficas:

ESPINOSA, Nick (2018). As cinco leis da segurança cibernética. TED Talk. Disponível em: https://www.ted.com/talks/nick_espinosa_the_five_laws_of_cybersecurity/transcript?language=pt-br.

ENISA, European Network and Information Security Agency (2012). Smart Grid Security: Recommendations for Europe and Member States. Disponível em: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations

(1) Artigo publicado na Agência CanalEnergia. Disponível em: https://www.canalenergia.com.br/artigos/53168641/a-crescente-relevancia-do-tema-seguranca-cibernetica-na-sociedade-o-caso-do-setor-eletrico. Acesso em 07 de abril de 2021.
(2) Pesquisadora Plena do GESEL (Grupo de Estudos do Setor Elétrico)
(3) Pesquisador Sênior do GESEL
(4) Pesquisadora Júnior do GESEL