Utilização de ontologia para auxílio na avaliação de segurança cibernética da infraestrutura crítica do setor elétrico: perspectiva brasileira

Márcio Rosostolato Machado[1],**Marcello Peixoto Bax**[1]

[1]ECI - PPGGOC - Universidade Federal de Minas Gerais (UFMG)
Av. Antônio Carlos, 6627 – Pampulha — Belo Horizonte – MG 31270-901 – Brasil

{marciorm,bax}@ufmg.br

Abstract. *This research project seeks to unify the cybersecurity terms of the fields of Information Technology and Operational Technology to organize knowledge of cybersecurity in the domain of the electric sector. It proposes the use of an ontology to build a conceptual model that considers terminologies from both fields and also cybersecurity requirements for the protection of critical infrastructure in the energy sector. In addition, it is expected that the use of ontology in cybersecurity assessments will enable a better understanding of cyber risk and the level of compliance with the cybersecurity best practices applicable to the energy sector.*

Resumo. *Este projeto de pesquisa busca unificar os termos de segurança cibernética dos campos de Tecnologia da Informação e Tecnologia Operacional para organizar o conhecimento de segurança cibernética no domínio do setor elétrico. Propõe o uso de uma ontologia para construir um modelo conceitual que considere terminologias de ambos os campos e também os requisitos de segurança cibernética para a proteção da infraestrutura crítica do setor de energia. Além disso, espera-se que o uso da ontologia nas avaliações de segurança cibernética possibilite melhor compreensão do risco cibernético e do nível de conformidade com as melhores práticas de segurança cibernética aplicáveis ao setor elétrico.*

1. Introdução

O setor de energia elétrica sempre foi considerado complexo e fortemente interconectado. O aumento da conectividade de redes, a convergência entre a Tecnologia da Operação (TO) e a Tecnologia da Informação (TI) e a transformação digital do modelo de negócio do setor elevaram a superfície de ataque a ser explorada por agentes maliciosos, bem como o risco para as organizações e para a sociedade, de forma geral [WEF 2019].

No setor elétrico, como em outros ramos da indústria, a incorporação de novos conceitos e tecnologias, característica do fenômeno Indústria 4.0, implica no surgimento de novas vulnerabilidades que demandam nova abordagem em relação à segurança cibernética [Ghobakhloo 2018]. A área de TI é a responsável pelo desenvolvimento, manutenção e uso dos sistemas computacionais, softwares e redes para o processamento de dados. Por outro lado, a área de TO compreende o hardware e software que detecta ou faz mudanças, por meio de monitoramento e/ou controle de dispositivos físicos, em processos e eventos no ambiente industrial.

Tanto as redes de TI quanto as de TO necessitam da segurança cibernética e o setor elétrico, nessa convergência das redes, ainda se depara com problemas relativos a conceitos e à terminologia, impossibilitando que os requisitos, os riscos, os controles e as relações entre eles sejam claramente compreendidos.

Para [Uschold et al. 1996], ontologias podem ser utilizadas como estruturas unificadoras para resolver questões semelhantes ao que se apresenta neste artigo.

2. Problema de Pesquisa

As diferenças existentes em cada domínio (TI e TO) apresentam desafios e restrições quando se trata de segurança cibernética aplicada na infraestrutura crítica, mais específico, no Sistema de Controle Industrial. Essas diferenças persistem em três níveis: operacional, técnico e gerencial, impondo limitações à atuação conjunta na adoção de medidas de segurança cibernética para a infraestrutura crítica do setor elétrico [Hahn 2016].

No Brasil, apesar de entidades como o Operador Nacional do Sistema (ONS) e a Agência Nacional de Energia Elétrica (ANEEL) atuarem para formalizar um documento que sintetize os procedimentos mínimos esperados para a proteção dos Sistemas de Controle Industrial no setor elétrico, não existe, atualmente, um guia único de implementação de controles, mas diversos documentos de requisitos de segurança utilizados em outros países que são utilizados em iniciativas isoladas pelos agentes.

Como exemplo temos o padrão *North American Electric Reliability Corporation - Critical Infrastructure Protection Standards* (NERC-CIP) , a norma ISO/IEC 27019:2017: *Information technology — Security techniques — Information security controls for the energy utility industry* e os padrões ISA/IEC 62443 - *Security for industrial automation and control systems*.

Assim, o questionamento que guia esta pesquisa é como oferecer um arcabouço conceitual unificando os termos de Tecnologia da Operação e Tecnologia da Informação relacionados à segurança cibernética, acrescido dos requisitos de segurança específicos para o setor, com o objetivo de apoiar a avaliação de segurança cibernética da infraestrutura crítica do setor elétrico brasileiro?

3. Objetivos

3.1. Objetivo Geral

O objetivo geral deste projeto é demonstrar a contribuição de um modelo conceitual, utilizando-se ontologia, para organizar o conhecimento relativo à segurança cibernética aplicável na proteção dos sistemas de controle industrial da infraestrutura crítica do setor elétrico brasileiro, tendo por base uma taxonomia criada à partir da unificação de termos pertinentes das áreas de TI e TO.

3.2. Objetivos Específicos

Os objetivos específicos deste projeto são:

- Criar uma taxonomia unificando termos relativos à segurança cibernética em TI e TO;
- Incorporar um conjunto de controles de segurança cibernética aplicáveis à infraestrutura crítica do setor elétrico;

- Desenvolver uma ontologia de domínio para a segurança cibernética em sistemas de controle industrial no setor elétrico;
- Validar a ontologia proposta com uma equipe de especialistas em TI e TO, responsável pela segurança cibernética em uma distribuidora de energia elétrica brasileira.

4. Justificativa

Infraestrutura crítica é um termo utilizado para descrever as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade [Brasil 2018].

O setor elétrico é categorizado como uma infraestrutura crítica, cujos Sistemas de Controle Industrial necessitam de proteção adequada para que ameaças cibernéticas não causem a interrupção ou degradação da prestação de serviço essencial à sociedade.

O crescente número de ataques cibernéticos ao setor, a grande quantidade de *frameworks* existentes em vários países, normas e padrões que apresentam requisitos de proteção e a convergência entre as áreas de TI e TO despertaram a necessidade de uma abordagem científica que apoie a organização do conhecimento referente à segurança cibernética no domínio do setor elétrico.

Por conseguinte, o setor elétrico brasileiro carece de uma base que contemple, de modo unificado, os conceitos e as relações dos termos relativos à segurança cibernética de TI e TO. Para [Noy et al. 2001], entre os motivos para o desenvolvimento de uma ontologia cita-se a análise do conhecimento de um domínio e a capacidade de tornar explícitas as suposições implícitas no conhecimento do domínio.

A despeito de um assunto em ascensão, o tema segurança cibernética no setor elétrico brasileiro é carente de regulamentação específica que trate a aplicação na infraestrutura crítica do setor. Além disso, o conhecimento do domínio deve ser abrangente e possuir o apoio de uma base conceitual que reflita o significado dos termos utilizados de modo compreensível por humanos e computadores, permitindo a remoção de ambiguidades nas avaliações de segurança e servindo como referência para o desenvolvimento de aplicações.

5. Trabalhos Correlatos

Alguns trabalhos refletem o interesse em representar o conhecimento sobre segurança cibernética. A pesquisa bibliográfica inicial revelou uma subdivisão em que foram utilizados termos como Sistema Físico-Cibernéticos (CPS), Sistema de Controle Industrial (ICS) e Sistema de Supervisão e Aquisição de Dados (SCADA), o que corrobora com a percepção do autor sobre a existência de diferentes perspectivas para abordar a questão.

Compreendendo essa heterogeneidade terminológica, cita-se [Bergner and Lechner 2017] que abordam o desenvolvimento de uma ontologia de segurança de TI como uma diretriz de implantação de proteção contra ataques hackers.

O trabalho de [Shaaban et al. 2019] trata da segurança cibernética de CPSs – sistemas cibernéticos que controlam entidades físicas – apresentando um conjunto de ferramentas de segurança baseado em ontologia capaz de ser integrado com os estágios iniciais do processo de desenvolvimento de sistemas críticos.

Com foco em ICS encontramos [Tebbe et al. 2016], que definem os requisitos sobre o conhecimento necessário para executar uma avaliação de segurança de

ICS e o ciclo de vida desse conhecimento. Com o foco voltado ao SCADA temos [Krauß and Thomalla 2016] que, considerando a grande dependências desses sistemas pelas infraestruturas críticas, propõem uma ontologia para especificar um modelo de eventos de segurança, ataques e vulnerabilidades.

Direcionado ao setor elétrico relacionamos o trabalho de [Vorozhtsova and Skripkin 2018] que apresenta uma análise ontológica da terminologia associada ao conceito de vulnerabilidade no setor e também possíveis meios de proteção para garantir a segurança cibernética no setor de energia.

6. Metodologia

Conforme citado por [Almeida and Bax 2003] metodologias têm sido desenvolvidas com o propósito de sistematizar a construção e a manipulação de ontologias.

Nos estudos iniciais foram vistos o método de Uschold e King, a metodologia de Grüninger e Fox e a metodologia Methontology, sendo esta última a escolhida para a construção da ontologia proposta neste estudo, composta pela etapas de especificação, conceitualização, formalização, implementação e manutenção [Gomez-Perez et al. 2006].

A seguir, são apresentadas as etapas previstas na condução desta pesquisa, entretanto adequações podem ser realizadas durante a execução.

6.1. Pesquisa bibliográfica

Iniciou-se o projeto com uma pesquisa bibliográfica, em bases de divulgação científicas, por trabalhos sobre o uso de ontologias para apoiar a segurança cibernética aplicada a sistemas de controle industrial (ICS), bem como estudo de normas e padrões de segurança cibernética aplicáveis ao setor elétrico.

6.2. Seleção de fontes para a criação do glossário de termos

Nesta etapa foram selecionados os documentos mais relevantes de padrões de segurança cibernética aplicáveis à TI, TO e específicos para o setor elétrico, conforme Tabela 1, sendo o critério de seleção a utilização de padrões reconhecidos internacionalmente, quando não encontradas referências nacionais.

Tabela 1. Fontes selecionadas para a criação do glossário de termos

Nome	Campo
North American Electric Reliability Corporation - Critical Infrastructure Protection Standards (NERC-CIP)	Setor Elétrico
ISA/IEC 62443 - Security for industrial automation and control systems.	TO
ISO/IEC 27019:2017: Information technology — Security techniques — Information security controls for the energy utility industry	Setor Elétrico
ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos	TI
ISO/IEC 27000:2018: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	TI

Na etapa seguinte foram selecionados os documentos nacionais que entende-se que podem contribuir para o desenvolvimento da ontologia ao incorporar ao glossário termos específicos do cenário brasileiro:

- Decreto nº 9.573, de 22 de novembro de 2018 - Política Nacional de Segurança de Infraestruturas Críticas;
- Vocabulário Controlado da ANEEL;
- PRODIST - documentos que normatizam e padronizam as atividades técnicas relacionadas ao funcionamento e desempenho dos sistemas de distribuição de energia elétrica.

6.3. Realização de entrevistas com os especialistas de domínio

Está prevista a realização de entrevistas com os especialistas do domínio em uma distribuidora de energia elétrica em Minas Gerais para colaborar com a criação das Questões de Competência que apoiarão na delimitação do escopo e no delineamento dos objetivos da ontologia.

6.4. Construção da taxonomia de conceitos

Em seguida, propõe-se extrair controles de segurança cibernética dos documentos da Tabela 1 antes da construção da taxonomia de conceitos. Como parte dessa pesquisa de mestrado, ressalta-se que ainda se encontra em estudo os métodos de construção de ontologias.

6.5. Desenvolvimento da ontologia

A ontologia será modelada com o apoio do software *Protégé*.

6.6. Avaliação da ontologia

A fase contempla a busca por metodologias que auxiliem em uma sistemática avaliação da ontologia visando a qualidade do conteúdo e da metodologia, em alinhamento ao trabalho de [Obrst et al. 2007].

7. Considerações Finais

Este artigo reflete os estudos realizados nas etapas iniciais da pesquisa e apresenta o planejamento das próximas fases. Entre outras atividades, serão realizadas ações para aquisição de conhecimento junto aos especialistas de domínio. Será ainda aprofundada a revisão da literatura e relacionados os trabalhos cujos objetivos se aproximem e/ou apoiem o resultado almejado por este projeto.

Os resultados esperados ao final deste projeto de pesquisa devem compreender as entregas: (1) sob uma visão pragmática da contribuição para a sociedade, a capacidade de apoiar e ampliar a compreensão dos operadores que atuam no setor elétrico e por conseguinte, elevar o nível de proteção da infraestrutura crítica do setor elétrico brasileiro; e (2) como contribuição científica, a manutenção de um vocabulário controlado de segurança cibernética aplicada ao setor elétrico, em língua portuguesa, que possa ser utilizado como referência na organização do conhecimento do domínio, com a visão de que o tema segurança cibernética em infraestruturas críticas vem ganhando relevância devido às mudanças que a tecnologia tem provocado na sociedade.

Referências

Almeida, M. B. and Bax, M. P. (2003). Uma visão geral sobre ontologias: pesquisa sobre definições, tipos, aplicações, métodos de avaliação e de construção. *Ciência da informação*, 32(3):7–20.

Bergner, S. and Lechner, U. (2017). Cybersecurity ontology for critical infrastructures. In *KEOD*, pages 80–85.

Brasil (2018). Decreto n. 9.573, de 22 de nov de 2018. aprova a política nacional de segurança de infraestruturas críticas. *Diário Oficial [da] República Federativa do Brasil*.

Ghobakhloo, M. (2018). The future of manufacturing industry: a strategic roadmap toward industry 4.0. *Journal of Manufacturing Technology Management*.

Gomez-Perez, A., Fernández-López, M., and Corcho, O. (2006). *Ontological Engineering: with examples from the areas of Knowledge Management, e-Commerce and the Semantic Web*. Springer Science & Business Media.

Hahn, A. (2016). Operational technology and information technology in industrial control systems. In *Cyber-security of SCADA and other industrial control systems*, pages 51–68. Springer.

Krauß, D. and Thomalla, C. (2016). Ontology-based detection of cyber-attacks to scada-systems in critical infrastructures. In *2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, pages 70–73. IEEE.

Noy, N. F., McGuinness, D. L., et al. (2001). Ontology development 101: A guide to creating your first ontology.

Obrst, L. et al. (2007). The evaluation of ontologies-toward improved semantic interoperability. semantic web, part ii, 139-158.

Shaaban, A. M., Gruber, T., and Schmittner, C. (2019). Ontology-based security tool for critical cyber-physical systems. In *Proceedings of the 23rd International Systems and Software Product Line Conference-Volume B*, pages 207–210.

Tebbe, C., Niemann, K.-H., and Fay, A. (2016). Ontology and life cycle of knowledge for ics security assessments. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, pages 32–41.

Uschold, M., Gruninger, M., et al. (1996). Ontologies: Principles, methods and applications. *TECHNICAL REPORT-UNIVERSITY OF EDINBURGH ARTIFICIAL INTELLIGENCE APPLICATIONS INSTITUTE AIAI TR*.

Vorozhtsova, T. and Skripkin, S. (2018). Ontological analysis of vulnerabilities in the energy sector. In *Vth International workshop"Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security"(IWCI 2018)*. Atlantis Press.

WEF (2019). Cyber resilience in the electricity ecosystem: principles and guidance for boards.principles and guidance for boards. `Disponivelem:http://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Electricity_Ecosystem.pdf`. "Acessado em 10 out. 2020".