1. Record Nr. UNINA9911022159003321

Autore	Bayer Markus
Titolo	Deep Learning in Textual Low-Data Regimes for Cybersecurity / / by Markus Bayer
Pubbl/distr/stampa	Wiesbaden : , : Springer Fachmedien Wiesbaden : , : Imprint : Springer Vieweg, , 2025
ISBN	3-658-48778-X
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (445 pages)
Collana	Technology, Peace and Security I Technologie, Frieden und Sicherheit, , 3004-9326
Disciplina	620
Soggetti	Engineering mathematics Engineering - Data processing Machine learning Data protection Mathematical and Computational Engineering Applications Machine Learning Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Research Design -- Findings -- Discussion -- Conclusion -- Information Overload in Crisis Management: Bilingual Evaluation of Embedding Models for Clustering Social Media Posts in Emergencies -- ActiveLLM: Large Language Model-based Active Learning for Textual Few-Shot Scenarios -- A Survey on Data Augmentation for Text Classification -- Data Augmentation in Natural Language Processing: A Novel Text Generation Approach for Long and Short Text Classifiers -- Design and Evaluation of Deep Learning Models for Real-Time Credibility Assessment in Twitter -- CySecBERT: A Domain-Adapted Language Model for the Cybersecurity Domain -- Multi-Level Fine-Tuning, Data Augmentation, and Few-Shot Learning for Specialized Cyber Threat Intelligence -- XAI-Attack: Utilizing Explainable AI to Find Incorrectly Learned Patterns for Black-Box Adversarial Example Creation.
Sommario/riassunto	In today's fast-paced cybersecurity landscape, professionals are

increasingly challenged by the vast volumes of cyber threat data, making it difficult to identify and mitigate threats effectively. Traditional clustering methods help in broadly categorizing threats but fall short when it comes to the fine-grained analysis necessary for precise threat management. Supervised machine learning offers a potential solution, but the rapidly changing nature of cyber threats renders static models ineffective and the creation of new models too labor-intensive. This book addresses these challenges by introducing innovative low-data regime methods that enhance the machine learning process with minimal labeled data. The proposed approach spans four key stages: Data Acquisition: Leveraging active learning with advanced models like GPT-4 to optimize data labeling. Preprocessing: Utilizing GPT-2 and GPT-3 for data augmentation to enrich and diversify datasets. Model Selection: Developing a specialized cybersecurity language model and using multi-level transfer learning. Prediction: Introducing a novel adversarial example generation method, grounded in explainable AI, to improve model accuracy and resilience. About the Author Dr. rer. nat. Markus Bayer is a research associate and post-doctoral researcher at the Chair of Science and Technology for Peace and Security (PEASEC) in the Department of Computer Science at the Technical University of Darmstadt.