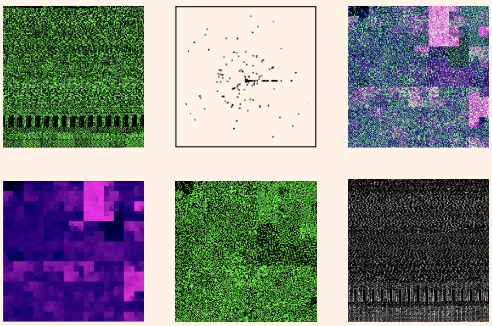
Artificial Intelligence for Cyber Defense in Emerging Threats

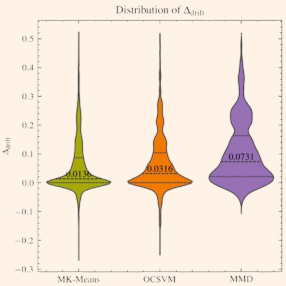
Springer

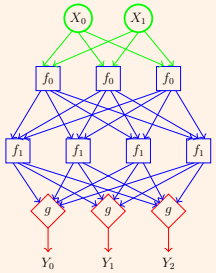
This book will deal with cutting-edge uses of Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Large Language Models (LLM), Generative AI, and related techniques in the field of cybersecurity. The emphasis will be on defenses against new and emerging threats to information security. Each chapter will consists of research-level work that is applicable and practical, with data-driven results that are designed to have a positive impact on real-world cybersecurity.

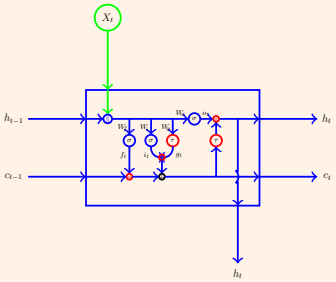
The cutting-edge AI-based techniques mentioned in the previous paragraph have been successfully applied in many domains. These techniques often provide dramatic improvements, as compared to more traditional methods, and have resulted in new industry standards in highly cognitive tasks, ranging from chatbots to self-driving cars. However, a relatively limited number of studies have applied these powerful techniques to problems related to cyber defense.

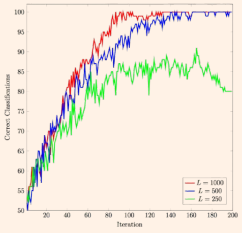
This book is designed to fill the gap between cutting-edge AI research and cyber defense. Proposed topics should include modern, practical, and timely AI-based techniques, as they apply to challenging cybersecurity problems.

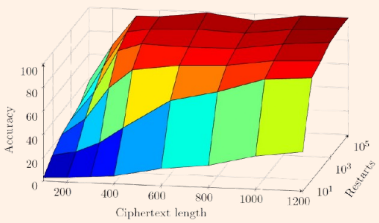












Editors:

- Mark Stamp (mark.stamp@sjsu.edu)
- Martin Jureček (martin.jurecek@fit.cvut.cz)
- Andrii Shalaginov (Andrii.Shalaginov@kristiania.no)

Timeline:

- June 1, 2026 — Chapters due to editors
- June 15, 2026 — Notification to authors
- August 15, 2026 — Camera ready chapters (typeset in LaTeX) due to editors
- January 2027 — Approximate publication date