Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

# Master Thesis

# Connected Defense: Next-Generation Data Platform for Military Intelligence and Operations

Second lieutenant, Representative, Valentin Pfeil


BLUELION
LRZ@GCS

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

## ISO (International Organisation of Standardisation)

- Founded in 1947
- Largest development organisation for voluntary international standards production, technology, environmental protection, etc. (cross-industry)
- E.g. **ISO 27001** information security management; **ISO 27005** information security risk management; **ISO 31000** risk management

## Cyber Security and Cyber Resilience

- Traditional cybersecurity frameworks focus on **prevention and detection**
  - **Challenge:** Massive amounts of attacks are **inevitable**, their impact more **severe**
- Cyber resilience frameworks add **resistence, recovery and adaption** capabilities
  - **Objective:** Operational **continuity** and long-term **stability**

## Definition

- **ISO 31000:**
  - **Risk:** “Effect of uncertainty on objectives”
  - **Risk management:** “Coordinated activities to direct and control an organisation with regard to risk”
- **ISO 27005:**
  - Guidelines for managing security risks in digital context

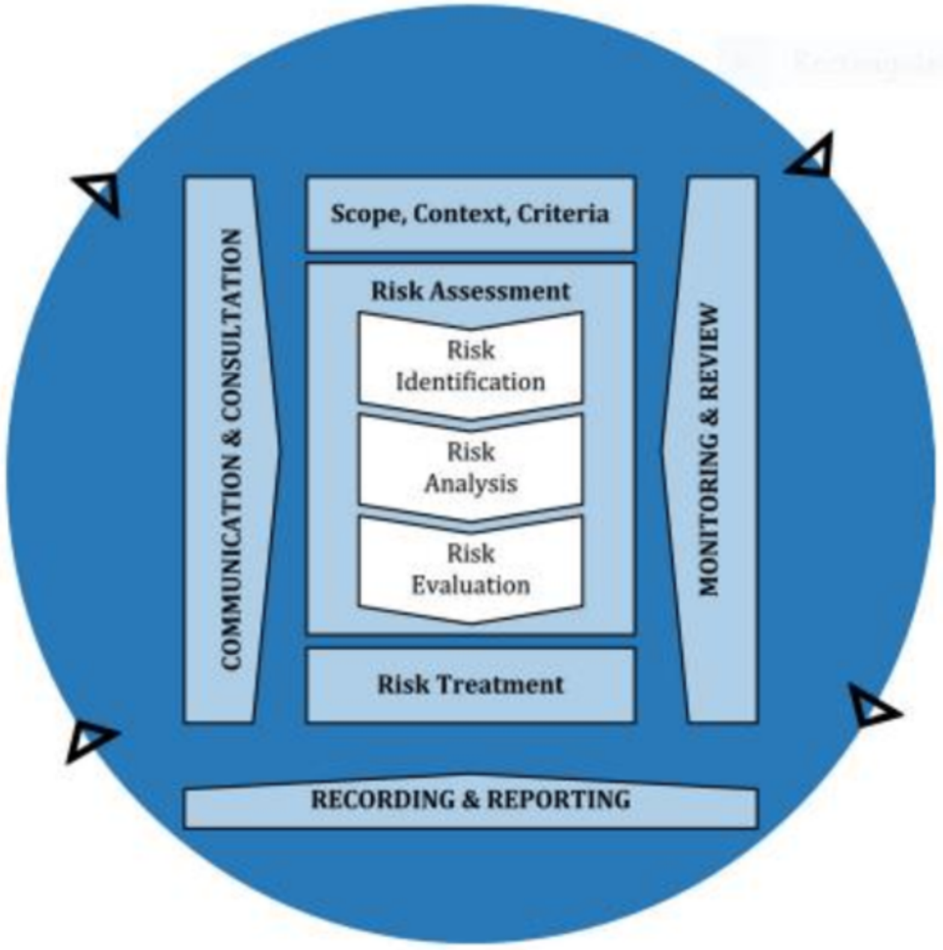



**Figure 1:** ISO 31000:2018 - Risk Management Process [1]

# Definition

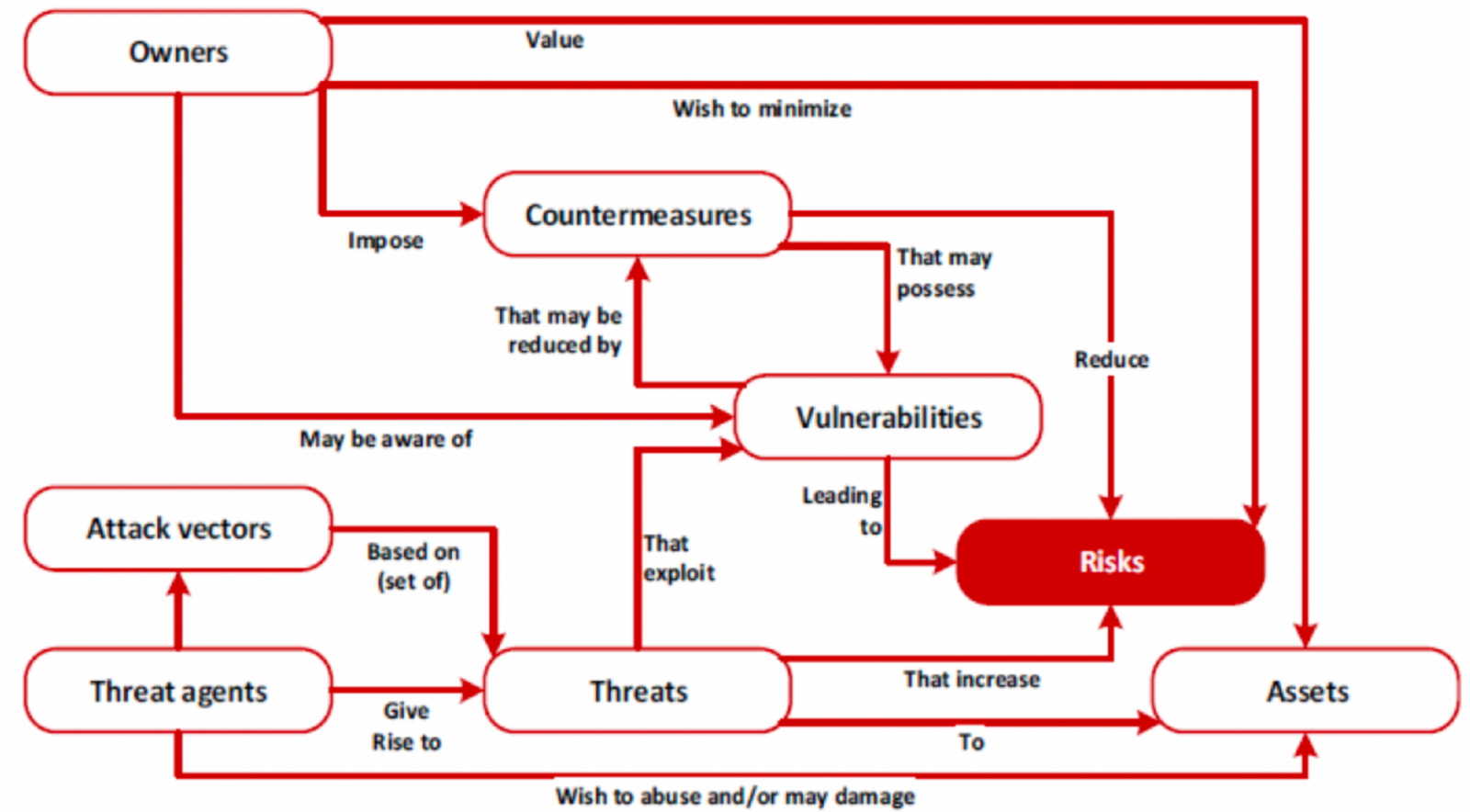



**Figure 2:** ISO/IEC 27005:2018 - Risk Management Methodology [2]

## Key Concepts

- Risk Assessment
- Mitigation Strategies
- Resilience

## Definition

- Context cyber defense: Application of advanced computational techniques
  - **Machine learning, neural network, natural language processing**
  - Improvement of detection, prevention and mitigation of cyber threats
  - **Enables Real-Time (RT) Analysis, Scalability, Automation and Efficiency and Predictive Capabilities**

## Key Concepts

- **Machine Learning (ML):** To learn from historical data, adapt to evolving threats and improve, contributes to GenAI
- **Natural Language Processing (NLP):** Analysis of textual data, e. g. security logs, extract valuable insights and enhances situation awareness, incl. advanced technologies, such as Large Language Models (LLMs), contributes to GenAI (text)
- **Neural Networks/Deep Learning:** Subset of ML designed to mimic human brain functionality, effective in image recognition and RT threat detection

## Concepts applied in Cybersecurity

- **Threat Detection:** ML models to treat malicious activities, neural networks for pattern recognition in network traffic
- **Predictive Capabilities:** leveraging historical data to predict emerging threats
- **Automation:** repetitive tasks, such as triaging alerts or threat classification can be automated
- **Improved Decision-Making:** AI data synthesis from multiple sources provides actionable insights more effectively

# Applications (Risk Management/AI) in Cybersecurity

## Broad Scope of Applications

- **Critical systems** (power grids, transportation, healthcare, etc.), **Predictive analytics, Automated operations**

## Enhancing Security

- **Compliance:** General Data Protection Regulation (GPDR), ISO 27001 to avoid penalties

## Industry Impact

- **Healthcare:** Information protection and incident response
- **Defense:** Monitoring threats and ensuring confidentiality
- **Financial sector:** Fraud detection and prot. customer data

# Challenges (Risk Management/AI) in Cybersecurity

## Evolving Threat Landscape:

- Advanced persistent threats (APTs, ransomware)
- Complex interconnected supply chains

## Technical Barriers:

- **Data quality:** Lack of diverse datasets for AI training
- **AI limitations:** Adversarial attacks, algorithmic bias
- Interoperability issues with legacy systems

## Organisational and Ethical Concerns:

- Compliance with GPDR/ISO 27001 adds complexity
- **Ethical concerns:** Data privacy, accountability
- Resistance to AI adoption due to trust and cost concerns

## Financial Constraints:

- High implementation costs and unclear Return on Investment (ROI)

## Definition

- **ISO 31000** defines risk management as

**"coordinated activities to direct and control an organisation with regard to risk."**

- **In AI-driven risk management**, this **is expanded** by leveraging AI to automate, enhance, and continuously refine these activities

**Alignment with ISO Standards (complements ISO 31000 and 27005)**

- Automating the *risk assessment* process through advanced ML models
- Supporting *risk treatment* with predictive analytics that prioritise mitigation strategies
- Enhancing *risk communication* by providing clear visualisations and actionable insights for stakeholders
- Facilitating *continuous improvement*, a core principle of ISO standards, by updating risk management practices in response to new data and threats.

# AI-Driven Risk Management for Cyber Resilience

## Summary

- Proactive Threat Mitigation
- Real-Time (RT) Response
- Scalable Risk Assessment
- Incident Recovery and Continuity
- Enhanced Decision-Making
- Adaptability to Evolving Threats

## Industry-Specific Contributions

- **Healthcare:** AI protects sensitive patient data, ensures system availability, maintaining the delivery of critical services during incidents
- **Finance:** RT fraud detection systems safeguard financial transactions, preserving trust and stability in financial markets
- **Energy:** Predictive maintenance powered by AI secures power grids and industrial control systems, reducing the risk of large-scale outages
- **Public Sector:** Governments leverage AI to ensure the resilience of critical infrastructure and digital services, enhancing national security

## EU AI Act - Key Points:

- Establishes stringent requirements for **high-risk AI systems** (e.g. transparency, robustness, governance)
- Focuses on **mandatory risk assessments**, bias mitigation, data privacy safeguards for critical applications
- Enforces accountability with **strict transparency obligations** and regular system updates
- Enhances **cyber resilience** by integrating ethical and technical measures into risk management
- Serves as a structured guideline for ensuring public trust while safeguarding organisational integrity

# AI-Technologies for Risk Assessment and Decision-Making

## Summary

- **Machine Learning (ML):** Supervised, Unsupervised, Reinforcement Learning for threat detection, categorisation, vulnerability discovery, optimisation of decision-making, contributes to GenAI
- **Natural Language Processing (NLP):** incl. LLMs to process and analyse unstructured data, contributes to GenAI
- Predictive Analytics: Statistical methods and ML for forecasting
- Anomaly Detection Systems: Autoencoders, Gaussian mixture models in network traffic, system logs, etc.
- **Visualisation and Decision Support Tools:** Dashboards and heat maps. Critical information, hightlighting of priorities

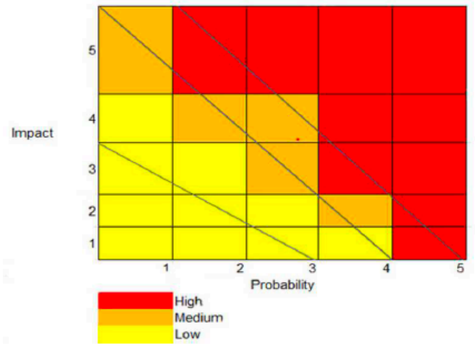
## GenAI and LLMs

- Significant advancements in AI-driven risk management tools, leverage massive datasets to enhance **unstructured data analysis** and provide insights for **risk assessment** and **mitigation**
  - **Unstructured Data Analysis:** e.g. GPT-based systems excel at processing and summarizing vast amounts of textual data, including incident reports, regulatory updates, and threat intelligence feeds
  - **Predictive Risk Scenarios:** Generative models simulate potential risk scenarios, enabling organisations to anticipate vulnerabilities and test mitigation strategies in a virtual environment
  - **Enhanced Decision-Making:** By synthesising contextual and historical data, GenAI facilitates strategic decision-making, improving

# Predictive Risk and Complexity Score Assessment Model (PRCSAM)


**Figure 3:** PRSCAM management framework - Risk Engine [5]

| 0-40% | 41-60% | 61-100% |
|---|---|---|
| Low | Medium | High |




| Category | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| Project Characteristics | *0-40% - Low* | *41- 60 % Medium* | *61-100% High* |
| Strategic Management Risks | | | |
| Procurement Risks | | | |
| Human Resources Risks | | | |
| Business Risks | | | |
| Project Management Integration Risks | | | |
| Project Requirements Risks | | | |

**Figure 4:** Risk and Complexity Assessment - Concept [5]

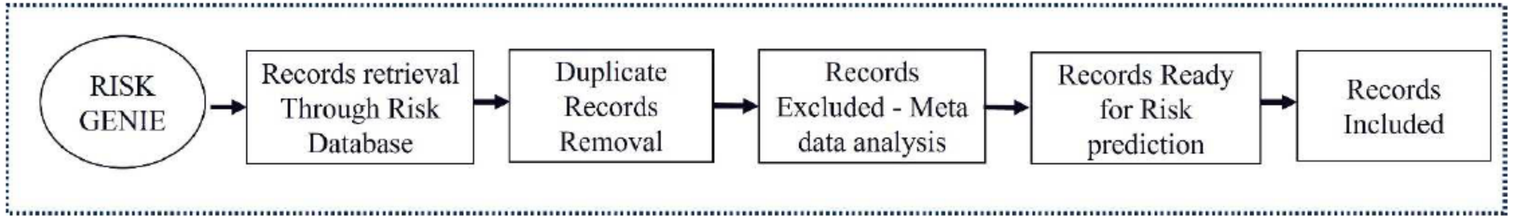



**Figure 5:** PRSCAM - Risk Prediction Genie [5]

# Business Continuity Management (BCM)

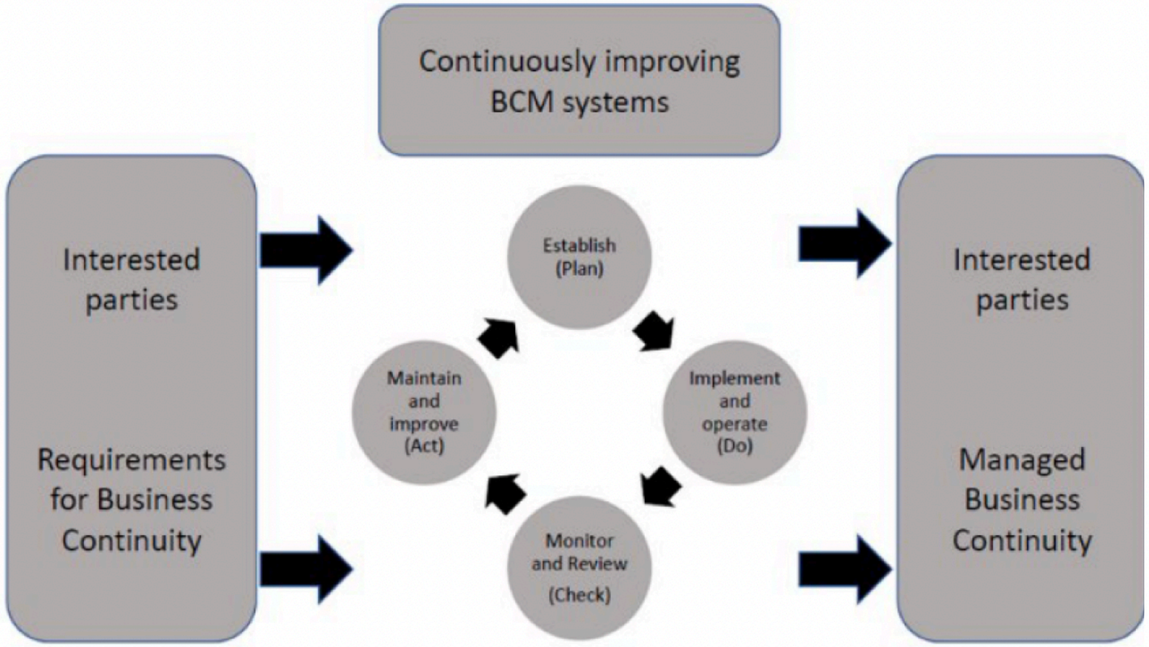



**Figure 6:** BCM - AI-enhanced Plan-Do-Check-Act (PDCA) cycle [9]

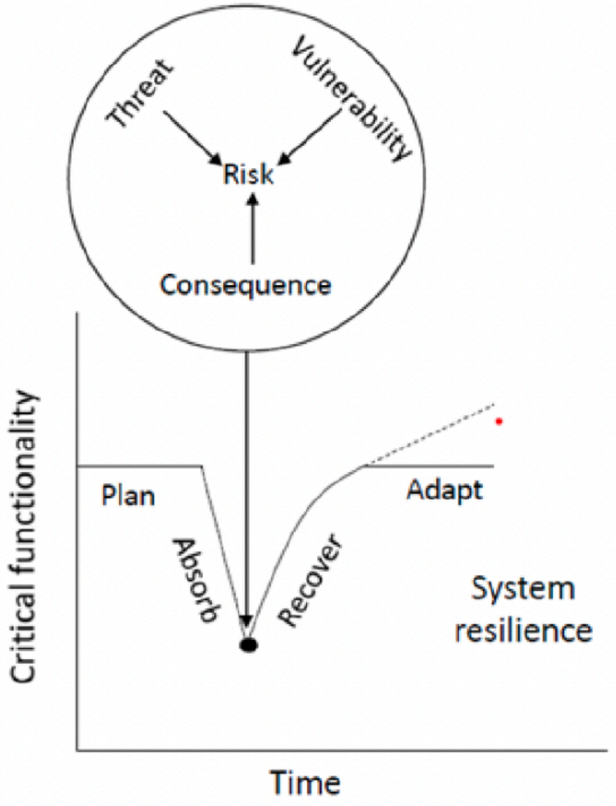



**Figure 7:** Resilience Management Framework [9]


**Figure 8:** BCM - AI-enhanced Resilience cycle [9]

## Benefits of AI-Driven Approach

- Enhances **efficiency and accuracy** by processing **large datasets** and **uncovering patterns** and **anomalies**
- Enables **proactive risk mitigation** through **predictive models** and **automated incident handling**
- Reduces **operational workload**, allowing teams to **focus on strategic decision-making**
- Ensures **cost-effectiveness** with long-term **savings from reduced incident costs** and **faster recovery times**
- Strengthens **collaboration** by providing **platforms for unified risk insights** and **strategies**
- Improves organisational **resilience** by **minimizing downtime** and **supporting** long-term **risk management**




# Challenges and Limitations

## Ethical, Technical and Regulatory Aspects and Limitations

- **Ethical:** AI systems face biases, lack of interpretability, and data privacy risks
- **Technical:** limited data quality, adversarial risks (e.g. data poisoning), high computational costs
- **Regulatory:** arise from compliance with evolving standards (e.g., EU AI Act) and adapting to global legal variations

## Outlook

- Advancements in AI (e.g., XAI, anomaly detection) will improve transparency, efficiency, and decision-making
- Proactive risk mitigation will focus on predictive strategies and resilience against evolving threats
- Collaboration between public and private sectors will drive ethical AI adoption and shared solutions
- **Goal:** build adaptive, sustainable risk management systems capable of thriving in uncertain environments

# Future Directions and Emerging Trends

## Potential Advancements

- **Explainable AI (XAI):** Enhances transparency and trust in decision-making processes
- **Large Language Models (LLMs):** Automate threat detection, optimise responses, and improve security awareness training
- **Domain-Specific AI Models:** Address sector-specific challenges, such as supply chain vulnerabilities and regulatory compliance
- **Integration with Emerging Technologies:** Blockchain for secure data sharing, Internet of Things (IoT)  for threat detection, and quantum computing for advanced security
- **Ethical AI Development:** Focuses on reducing bias, ensuring accountability, and aligning with societal values for reliable systems

# Future Directions and Emerging Trends

## Evolving Approaches

- **Integration of AI and Cybersecurity:** AI enables proactive threat detection and risk mitigation through advanced technologies
- **Tailored AI Solutions:** AI is increasingly customized for specific industries, such as finance, healthcare, and critical infrastructure
- **Focus on Ethics and Governance:** Emphasis on fairness, accountability, and transparency in AI systems, supported by robust framework
- **Sustainability in AI Deployments:** Sustainable AI practices reduce environmental impact and ensure long-term operational viability

## Regulatory and Ethical Developments

- Regulatory laws like the EU AI Act promote fairness, transparency, and accountability in AI
- Harmonized standards simplify compliance and encourage global adoption of ethical AI practices
- Regulatory efforts aim to foster trust in AI systems while minimizing risks and societal biases
- These developments ensure AI technologies remain innovative, socially responsible, and beneficial to society

- AI **transforms cybersecurity** by enabling **precise threat identification**, **assessment**, and **mitigation**
- AI-driven **frameworks** emphasize **resilience**, focusing on **recovery** and **adaptation** rather than just prevention
- Emerging technologies like **XAI** and **anomaly detection** expand **capabilities**, but introduce **challenges** such as **transparency, algorithmic bias**, and **compliance**
- **Collaboration** and continuous **innovation** are essential for **building adaptive** and **robust** risk management systems
- AI ensures **secure**, **sustainable**, and **adaptable strategies** for navigating the **evolving digital landscape**

# References


[1] ISO 31000:2018 Risk Management - Guidelines. ISO, 2018.

[2] ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management. ISO, 2018.

[3] World Economic Forum. Systemic cybersecurity risk and role of the global community: Managing the unmanageable, 2022.

[4] Paola Perrone, Francesco Flammini, and Roberto Setola. Machine learning for threat recognition in critical cyber-physical systems. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021, pages 298–303. Institute of Electrical and Electronics Engineers Inc., 7 2021.

[5] Kavitha Ayappan, J. M. Mathana, and J. Thangakumar. Predictive risk and complexity score assessment model for cloud computing. In 2024 International Conferenceon Advances in Data Engineering and Intelligent Computing Systems, ADICS 2024. Institute of Electrical and Electronics Engineers Inc., 2024.

[6] Adeel A. Malik and Deepak K. Tosh. Towards developing a scalable cyber risk assessment and mitigation framework. In SysCon 2024 - 18th Annual IEEE International Systems Conference, Proceedings. Institute of Electrical and Electronics Engineers Inc., 2024.



@FI_CODE

http://www.unibw.de/code

# References


[7] Artem Polozhentsev, Sergiy Gnatyuk, Rat Berdibayev, Viktoriia Sydorenko, and Oksana Zhyharevych. Novel cyber incident management system for 5g-based critical infrastructures. In Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, pages 1037–1041. Institute of Electrical and Electronics Engineers Inc., 2023.

[8] Publications Office of the European Union L and Luxembourg Luxembourg. Regulation(eu) 2024/1689 of the european parliament and of the council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (artificial intelligence act), 2024.

[9] Timo Savolainen, Nora McCarthy, Karen Neville, and Harri Ruoslahti. Business continuity management of critical infrastructures from the cybersecurity perspective. In IEEE Global Engineering Education Conference, EDUCON. IEEE Computer Society, 2024.

[10] Atif Ali, Abdul Razzaque, Usama Munir, Hina Shahid, Furqan Wali Khattak, Zain Rajpoot, Muhammad Kamran, and Zulqarnain Farid. Ai-driven approaches to cybersecurity: The impact of machine and deep learning. In 2nd International Conference on Cyber Resilience, ICCR 2024. Institute of Electrical and Electronics Engineers Inc., 2024.



@FI_CODE

http://www.unibw.de/code

# References


[11] K. K. Ramachandran, K. K. Karthick, Lakshmi Priya Vinjamuri, R. Ramesh, Mustafa Al-Taee, and Malik Bader Alazzam. Using ai for risk management and improved business resilience. 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023, pages 978–982, 2023.

[12] Sardar Muhammad Ali, Abdul Razzaque, Haider Abbass, Muhammad Yousaf, and Sardar Sadaqat Ali. A novel ai-based integrated cybersecurity risk assessment framework and resilience of national critical infrastructure. IEEE Access, pages 1–1, 2025.

[13] Raimir Holanda Filho and Daniel Colares. A methodology for risk management of generative ai based systems. 2024 32nd International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2024, 2024.

[14] Dalmo Stutz, Joaquim T De Assis, Asif A Laghari, Abdullah A Khan, Nikolaos Andreopoulos, Andrey Terziev, Anand Deshpande, Dhanashree Kulkarni, and Edwiges G H Grata. Enhancing security in cloud computing using artificial intelligence (ai), 2024.

# Q & A

Valentin Pfeil
Institute for Software Technology
Research Institute CODE
University of the Bundeswehr Munich
**valentin.pfeil@unibw.de**
https://www.unibw.de/code

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München