Unit 12 Seminar Preparation

Seminar 6: The Great Debate - The Future of SRM

Each team will choose a trend that they think will be the most influential in the next 5 years and will prepare a 10-minute presentation on that trend that summaries the key points and argues why they believe it will be the most influential in the next 5 years. Each team will be given a slot in this week's seminar where they will be able to present their slides and their arguments. Following the presentations, all attendees will be given a chance to ask questions and discuss their own views. At the end of the discussion the tutor will run a poll and all attendees will be given the chance to vote for their favourite.

Learning Outcomes

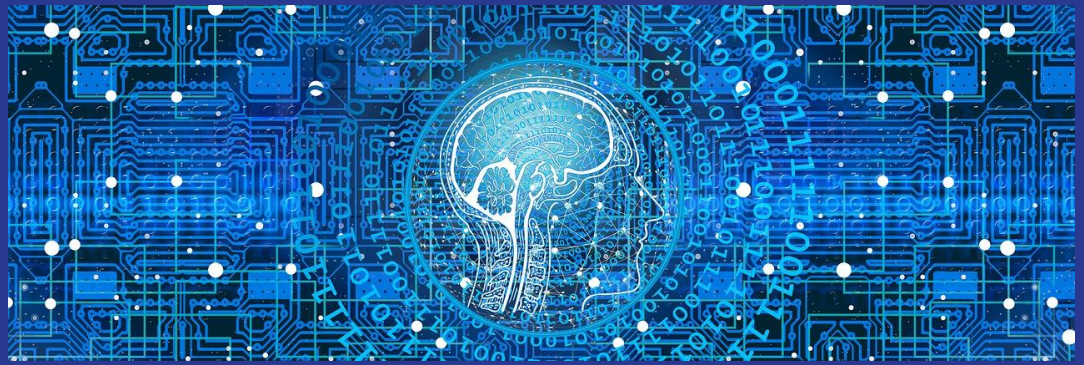
- Identify and analyse critically, security risks, threats and vulnerabilities in information systems, accounting for the current threat landscape
- Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of risks & security issues
- Critically determine appropriate methodologies, tools and techniques to mitigate and/or solve security risks and their business impact
- Articulate the legal, social, ethical, and professional issues faced by information security and risk professionals

---

Risk Management of the Future:
AI for Cyber Risk Quantification

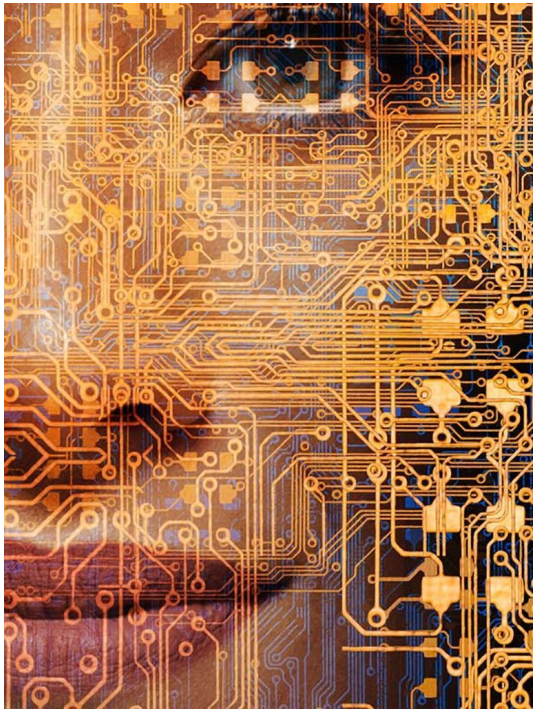
SRM_PCOM7E September 2022

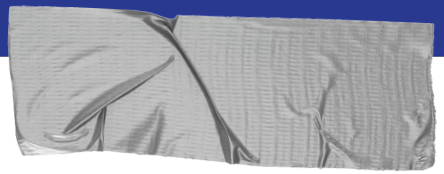
Group 1 (The A Team)



What is Artificial Intelligence (AI)?

- Fundamentally, a machine that can solve complex problems usually reserved for human intelligence (Cold Fusion, 2016).
- Examples:
    - Deep Blue vs. Kasparov (AFP, 2022)
    - Medicine - treatment prediction (ForeSeeMed, n.d.)
    - Education - personalized learning (Harper, 2021)





Recipe for Success:

Machine Learning (ML)

- **Algorithms**
  Allow AI to data mine / adjust to new trends in real time
- **Automation and Iterative Processes**
  Make AI independent from human involvement
- **Ensemble Modelling**
  Improves the accuracy of predictive analytics and data mining applications

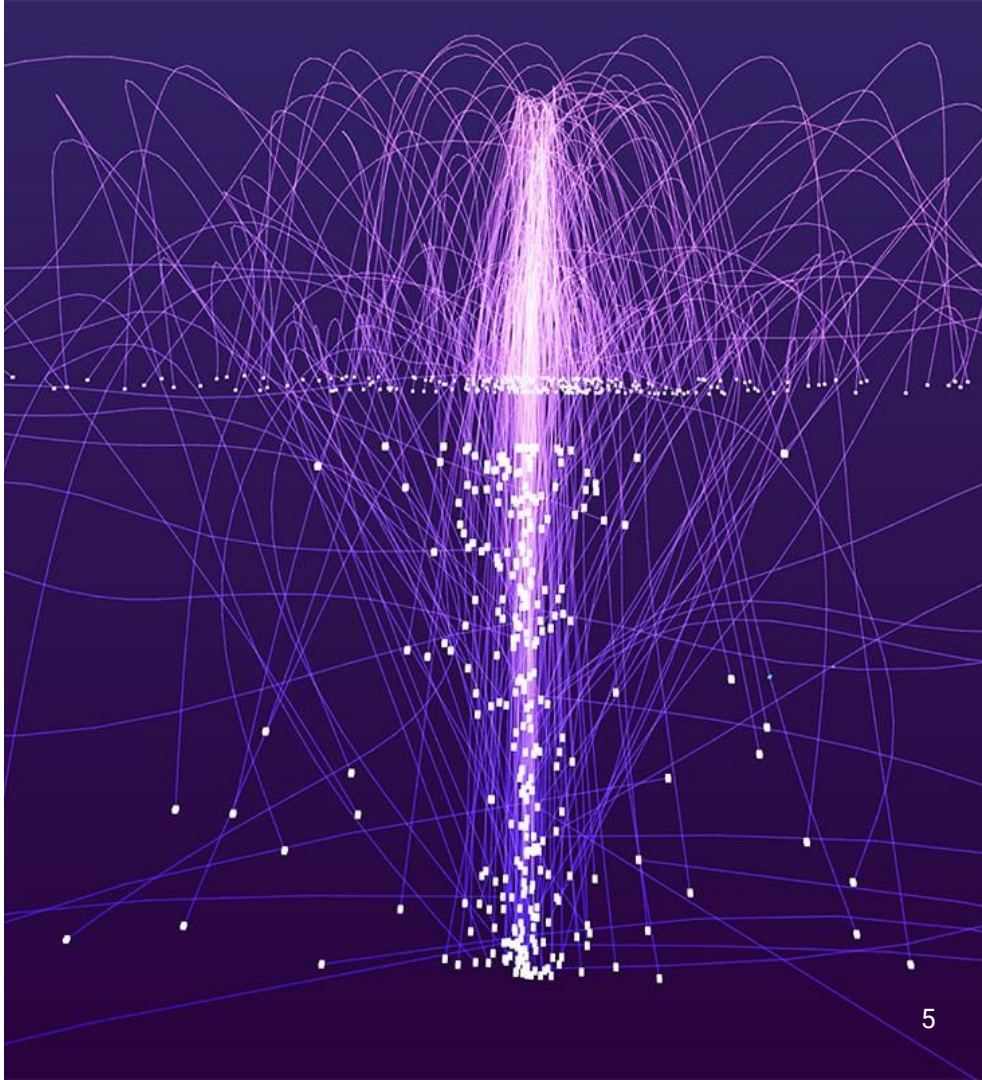
(SAS, 2022; Burns, 2015)

How is AI being utilized in quantitative risk analysis to aid in disaster probability calculations & recovery?

Five AI Risks

- Lack of Employee Trust
- Biases/Errors are magnified by volume of AI transactions
- AI can have unintended consequences/automate unethical practices
- Key skills may be a risk of erosion
- Poor training data, lack of monitoring can sabotage AI systems

(Pratt, 2020)



AI and ML threats

1. Data Corruption and Poisoning
    - Concerns: Dataset accuracy & integrity
    - Result: Inaccurate / malevolent AI predictions
    - Cause: “Poisoning" / distorting" the learning data
2. System Manipulation
    - Result: Incorrect predictions
    - Cause: Feeding malicious inputs via deceiving high-volume ML algorithms
3. Transfer Learning Attacks
    - Common: pre-trained ML models
    - Specialized training
    - Devastating window of opportunity for attack
    - Trick a well-known task-specific ML model

(Erma, 2022)

What Companies can gain from AI-based Cyber Risk Quantification

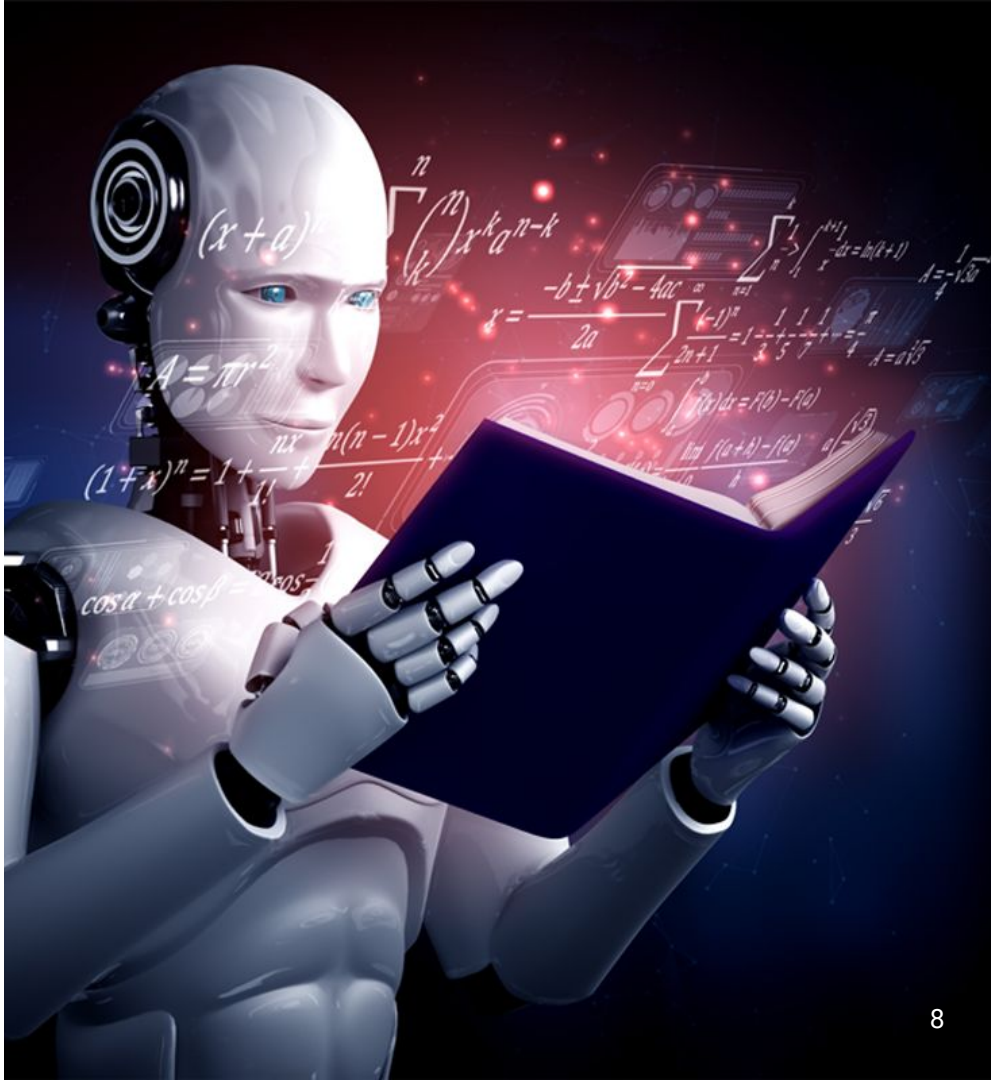
1. Cybersecurity risk score
    - Macro-level: network devices
    - Micro-level: IP addresses
2. Risk exposure
    - Assessment used by CISOs
    - Understand data, assets
    - Protective technologies, security policies
3. Security posture
    - ML-based probabilistic models
        i. Random Forest (RF)
        ii. Recursive Neural Network (RNN)
    - Personalised stakeholder security reports
4. Risk ratings
    - Can account for 3rd-party risk elements

(manageengine, n.d)

Current Use of AI in DR

- Simulations of possible attack scenarios
- Potential costs and likely disaster scenarios
- Pattern isolation and report
- Data mining
- Can be autonomous if desired

(Burns, 2022)



US AI Bill of Rights

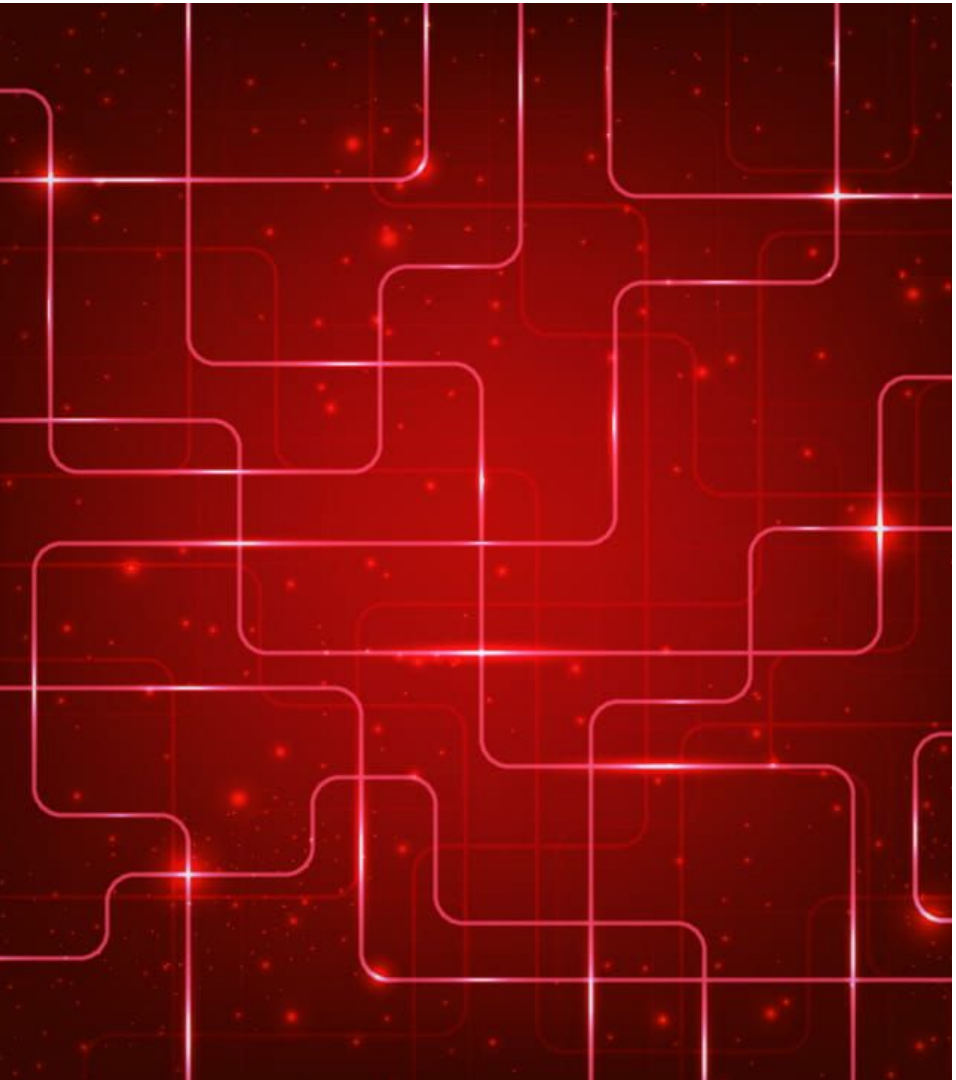
- Transparent and explainable AI for consumers
  - Mortgage
  - Credit
  - Insurance
- Challenges:
  - What is ‘ethical AI’?
  - Can ‘fairness’ be quantified?
  - Reproduction of unwanted inequities and discrimination

(Holland, 2021)

EU/UK Efforts

- Can take a leadership position, not unlike the GDPR.
- Can focus on these principles:
  - AI should be human centric/socially beneficial
  - AI should be fair in its decision making
  - AI should be transparent and explainable
  - AI should be safe and secure
  - AI should be accountable

(ibid, 2021)



AI, IoT & Blockchain Convergence

- Currently in Development
- “A Holy Trinity”
- Meant to serve as a sort of nervous system (IoT), brain (AI), and memory (Distributed Ledger Technology)
- Meant to provide “immutable record-keeping” and an audit trail (Groopman, n.d)
- Improve transparency

(Groopman, 2019)

References

- Manageengine (n.d) How AI can improve how you assess the cyber risk of your organization. Available from:https://www.manageengine.com/log-management/ueba/resources/how-ai-can-improve-how-you-assess-the-cyber-risk-of-your-organization.html [Accessed 7 December 2022]
- Erma (2022) Poisoned AI: A Threat to Cyber Security. Available from:https://www2.erm-academy.org/publication/risk-management-article/poisoned-ai-a-threat-to-cyber-security/ [Accessed 7 December 2022]
- OpenAI(2022) ChatGPT. Available from https://beta.openai.com/ [Accessed 8 December 2022]
- Holland, M. (2021) *Efforts to craft AI regulations will continue in 2022: TechTarget*, *Enterprise AI*. TechTarget. Available at: https://www.techtarget.com/searchenterpriseai/feature/Efforts-to-craft-AI-regulations-will-continue [Accessed: December 8, 2022].
- Burns, E. (2015) *What is ensemble modeling?: Definition from TechTarget*, *Business Analytics*. TechTarget. Available at: https://www.techtarget.com/searchbusinessanalytics/definition/Ensemble-modeling [Accessed: December 8, 2022].

References

- SAS (n.d.) *Machine learning: What it is and why it matters*, *SAS*. Available at: https://www.sas.com/en_th/insights/analytics/machine-learning.html [Accessed: December 8, 2022].
- ForeSeeMed (n.d.) *Artificial Intelligence (AI) in Healthcare & Hospitals*, *ForeSee Medical*. Available at: https://www.foreseemed.com/artificial-intelligence-in-healthcare [Accessed: December 8, 2022].
- Harper, T. (2022) *Top 7 ways artificial intelligence is used in education*, *Training Mag*. Available at: https://trainingmag.com/top-7-ways-artificial-intelligence-is-used-in-education/ [Accessed: December 8, 2022].
- AFP. (2022) *Man vs. machine: The 1997 chess game that brought AI into view*, *Daily Sabah*. Daily Sabah. Available at: https://www.dailysabah.com/sports/man-vs-machine-the-1997-chess-game-that-brought-ai-into-view/news [Accessed: December 8, 2022].
- Pratt, M.K. (2020) *5 AI risks businesses must confront and how to address them: TechTarget*, *Enterprise AI*. TechTarget. Available at: https://www.techtarget.com/searchenterpriseai/feature/5-AI-risks-businesses-must-confront-and-how-to-address-them [Accessed: December 8, 2022].

References

- Groopman, J. (2019) *AI, Blockchain, and IoT Convergence Improves Daily Applications: TechTarget*, *Enterprise AI*. TechTarget. Available at: https://www.techtarget.com/iotagenda/tip/AI-blockchain-and-IoT-convergence-improves-daily-applications [Accessed: December 8, 2022].

- Burns, S. (2022) *Where Does AI Fit into a Risk Assessment Strategy?: TechTarget*, *Enterprise AI*. TechTarget. Available at: https://www.techtarget.com/searchdisasterrecovery/tip/Where-does-AI-fit-into-a-risk-assessment-strategy [Accessed: December 8, 2022].

- ColdFusion (2016) *What is Artificial Intelligence Exactly?:* Youtube. Available at: https://www.youtube.com/watch?v=kWmX3pd1f10 [Accessed: December 8, 2022]

- Ba Balasubramanian, R., Libarikian, A. and McElhaney, D. (2021) *Insurance 2030--the impact of AI on the future of Insurance*, *McKinsey & Company*. McKinsey & Company. Available at https://www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance (Accessed: December 7, 2022).