Title	AI for Cyber Resilience
Long Title	AI for Cyber Resilience
Credits	**5**
NFQ Level	**Expert**
Module Author	**Mjeda Anila**

Module Description:

In this module, students will examine the role of Artificial Intelligence (AI) in improving cyber resilience in organizations, and addressing misuse by adversaries. Students will explore practical applications of AI in detecting, analysing, and responding to cyber threats, as well as understanding risks associated with their misuse. The module situates discussions within the context of cyber resilience in a rapidly evolving technological landscape, examining how AI can be leveraged to enhance security and defence mechanisms

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Evaluate how Artificial Intelligence (AI) technologies improve cyber resilience, emphasizing threat detection.

LO2 Analyse the misuse of AI by malicious actors, including deep fakes and malware, and its impact on organizational resilience.

LO3 Critically evaluate the challenges in securing AI systems and propose strategies for their secure implementation.

LO4 Evaluate the ethical considerations and societal impacts of using AI in enhancing cyber resilience.

LO5 Analyse AI-supported solutions for real-world challenges in cyber resilience.

Indicative Content

Use of AI to Improve Cyber Resilience

Understanding cyber resilience concepts; Role of AI in modern cyber resilience frameworks; AI-driven threat detection methods and anomaly analysis; Predictive analytics for proactive cybersecurity; Threat modelling and AI-based security implications; Real-world applications of AI in enhancing cyber resilience with case studies; AI-driven resilience testing of organizational systems.

Misuse of AI by Adversaries

Deep fakes including generation, detection, mitigation strategies, and implications for disinformation and identity fraud; Development and deployment of malware (including polymorphic malware) leveraging AI capabilities to evade detection; Adversarial attacks on AI systems including data poisoning and evasion tactics; Automated reconnaissance and attack tools powered by AI; Social engineering attacks amplified by AI-driven chatbots and impersonation techniques; Analysis of the ethical implications and challenges posed by adversarial use of AI.

Securing AI Systems

Addressing vulnerabilities within AI systems including identifying and mitigating adversarial threats; Ensuring data integrity, confidentiality, and robustness in AI applications; Challenges associated with democratized AI deployment and unvetted AI implementations; Principles for resilient AI system design; Monitoring and auditing AI systems for compliance and risk mitigation.

Ethical and Societal Implications

Understanding how AI decisions can be influenced by data and how this can lead to unexpected outcomes; Considering the impact of AI on people and society, including risks of misuse or unfair treatment; Ethical considerations and best practices for leveraging AI to strengthen organizational resilience; Analysing real-world examples to discuss common challenges and decisions faced when applying AI in cyber resilience.

AI-Supported Solutions for Organizational Resilience

AI-supported proactive defence mechanisms and early threat mitigation; Adaptive incident response frameworks leveraging AI-driven decision-making tools; Integration of predictive and prescriptive analytics for long-term resilience planning; Utilizing AI to simulate and test responses to potential cyber incidents; Enhancing business continuity through AI-automated recovery and system restoration; Continuous monitoring and optimization of resilience strategies using AI insights; Case studies on successful implementation of AI for organizational resilience in different industries.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	Analyse a real-world incident involving misuse of AI and propose a detailed mitigation strategy to enhance organizational resilience. Also discuss the ethical considerations and societal impacts of AI in enhancing cyber resilience.	2,4,5	40	Week 6
Project	Propose an AI-driven solution, whether as an ecosystem or a detailed strategy, to enhance cyber resilience in response to a specific challenge. Emphasize practical integration, ethical	1,3,5	60	Sem End

No End of Module Formal Exam	considerations, and organizational impact.

Assessment Breakdown	%
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2	Every Week	2.00
Lab	Lab to support the learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2	Every Week	2.00
Lab	Lab to support the learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student.	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

Todor Tagarev,Krassimir T. Atanassov,Vyacheslav Kharchenko,Janusz Kacprzyk. (2021), Digital Transformation, Cyber Security and Resilience of Modern Societies,

Springer, p.495, [ISBN: 9783030657215].

Supplementary Book Resources

National Academies of Sciences, Engineering, and Medicine,Division on Engineering and Physical Sciences,Intelligence Community Studies Board,Computer Science and

Telecommunications Board. (2020), Implications of Artificial Intelligence for Cybersecurity, National Academies Press, p.99, [ISBN: 978-0-309-49450-2].

Recommended Article/Paper Resources

Sadeghi, K., Ojha, D., Kaur, P., Mahto, R. V., & Dhir, A.. (2024), Explainable artificial intelligence and agile decision-making in supply chain cyber resilience, Decision

Support Systems, 180, 114194,

https://doi.org/10.1016/j.dss.2024.11419 4

Nikola Petrovic and Ana Jovanovic. (2023), Towards Resilient Cyber Infrastructure: Optimizing Protection Strategies with AI and Machine Learning in Cybersecurity

Paradigms, International Journal of Information and Cybersecurity, 7 (12),

https://publications.dlpress.org/index.p hp/ijic/article/view/75

Sarker, I. H., Furhad, M. H., & Nowrozy, R.. (2021), AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions, SN Computer Science, 2

(173),

https://link.springer.com/article/10.100 7/s42979-021-00557-0

Siva Subrahmanyam Balantrapu. (2024), A Comprehensive Review of AI Applications in Cybersecurity, International Machine learning journal and Computer Engineering, 7

(7),

https://mljce.in/index.php/Imljce/articl e/view/39

Supplementary Article/Paper Resources

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A.. (2024), Advancing cybersecurity: a comprehensive review of AI-driven detection techniques, Journal of Big Data,

11(1),

https://www.springerprofessional.de/en/a dvancing-cybersecurity-a-comprehensive-r eview-of-ai-driven-dete/27431634

Other Resources

website, OWASP. OWASP AI Exchange Flagship Project, online, OWASP,

https://owaspai.org/

website, SANS. Artificial Intelligence (AI) Cyber Security Training and Resources, online, SANS,

https://www.sans.org/ai