

References

- Alom, M. Z., Taha, T. M., Yakopcic, C., et al. (2020). *The history and present of deep learning in cybersecurity. IEEE Transactions on Neural Networks and Learning Systems*, 32(12).
- Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2021). *Quantum machine learning. Pearson*, 549(7671), 195–202.
- Chen, T., Cornelius, C., Sheatsley, R., Johnson, J., & Xiao, C. (2020). *Adversarial machine learning in network intrusion detection: A survey. IEEE Communications Surveys & Tutorials*, 22(1), 343–376.
- Cybersecurity and Infrastructure Security Agency. (2024). *Cost of a cyber incident: Systematic review and cross-validation (CISA Office of Cybersecurity Economics report). U.S. Department of Homeland Security. <https://www.cisa.gov/resources-tools/resources/cost-cyber-incident-systematic-review-and-cross-validation>*
- Dua, M., Du, X., & Zhang, N. (2021). *Machine learning in cybersecurity: A comprehensive survey. IEEE Access*, 9, 107597–107642.
- IBM Security. (2024). *Cost of a data breach report 2024. IBM. <https://www.ibm.com/reports/data-breach>*
- Lu, S., Kim, K., & Bae, J. (2023). *Hybrid quantum–classical neural networks for cybersecurity applications. Quantum Information Processing*, 22(4).
- Moore, T., Clayton, R., & Anderson, R. (2019). *The economics of cybersecurity. Journal of Economic Perspectives*, 23(3), 27–52.
- NIST. (2022). *Post-quantum cryptography standardization. Journal of Research of NIST*.
- Papernot, N., et al. (2022). *Practical black-box attacks against ML systems. ACM CCS*.

Rebentrost, P., Mohseni, M., & Lloyd, S. (2022). *Quantum support vector machine for pattern classification*. *Physical Review Letters*, 113(13).

Schuld, M., & Petruccione, F. (2020). *Supervised learning with quantum computers*. Pearson

Zou, X., Zhao, L., & Li, Y. (2021). *A survey on deep learning-based anomaly detection in cybersecurity*. *ACM Computing Surveys*, 54(7).