ARTEFACT COMMENTARY

This discussion explored the tension between automation and human-centred care within the UK healthcare system, using the 2017 NHS WannaCry ransomware attack as a focal point. My initial post examined how Industry 4.0's integration of digital systems, AI, and IoT improved efficiency but simultaneously exposed structural vulnerabilities in healthcare infrastructure (Mohamed and Al-Jaroodi, 2019; Ghafur et al., 2019). I argued that Industry 5.0's human-centric framework provides a necessary evolution one that restores resilience, social responsibility, and clinician oversight to technology-driven care (Saxena et al., 2024; Abdel-Basset, Mohamed and Chang, 2025).

Peer engagement expanded this understanding from theoretical reflection to practical application. Responses emphasised preventive measures such as consistent system patching, network segmentation, and regular staff training to address cybersecurity vulnerabilities (Department of Health and Social Care, 2018; National Cyber Security Centre, 2023). This feedback highlighted the importance of a holistic cyber-resilience strategy that integrates human factors alongside technical safeguards. Another peer underscored government initiatives aimed at embedding security within the NHS's digital transformation roadmap (Department of Health and Social Care, 2023), which helped me recognise the scale of coordinated policy needed for sustainable change.

The peer interactions also deepened my awareness of the ethical and organisational dimensions of Industry 5.0. Responding to others' posts on remote workforce monitoring and biotech cyberattacks allowed me to apply these principles beyond healthcare. I advocated for user-centred design, GDPR compliance, and Zero-Trust security frameworks (Anshari et al., 2021; Kosaraju, 2025). Through these exchanges, I saw how cross-sector collaboration and ethical governance are vital for fostering trust and inclusion in digital ecosystems.

The summary discussion enabled me to synthesise these insights. I concluded that cyber resilience extends beyond technical recovery it embodies organisational learning, ethical foresight, and continual adaptation. Integrating frameworks such as Merchán-Cruz et al.'s (2025) Trust by Design aligns with Industry 5.0's goal of ensuring technology augments, rather than replaces, human judgment.

This activity strengthened my knowledge of the legal, ethical, and social implications of digital healthcare while improving my ability to communicate complex ideas collaboratively. More importantly, it reinforced the importance of embedding human values into technological innovation, a principle that will guide my ongoing professional development in AI and healthcare.

REFERENCES

Abdel-Basset, M., Mohamed, R. and Chang, V. (2025) ‘A Multi-Criteria Decision-Making Framework to Evaluate the Impact of Industry 5.0 Technologies’, Information Systems Frontiers, 27(2), pp. 791–821.

Anshari, A., Hirtranusi, S.A., Sensuse, D.I. and Suryono, R.R. (2021) ‘Designing an Attendance System Model for Work from Home (WFH) Employees Based on User-Centered’,International Conference on Computer Science, Information Technology, and Electrical Engineering pp. 125-132.

Department of Health and Social Care (2018) Lessons Learned Review of the WannaCry Ransomware Cyber Attack. London: DHSC.

Department of Health and Social Care (2023) A Cyber Resilience Strategy for Health and Social Care: 2023 to 2030. London: DHSC.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019) ‘A Retrospective Impact Analysis of the Wannacry Cyberattack on the NHS’, *NPJ digital medicine 2*(1), p.98.

Kosaraju, P. (2025) ‘Safeguarding OT Networks in Biotech Manufacturing Plants’, Journal of Computer Science and Technology Studies, 7(3), pp. 972–981.

Merchán-Cruz, E.A., Gabelaia, I., Savrasovs, M., Hansen, M.F., Soe, S., Rodriguez-Cañizo, R.G. and Aragón-Camarasa, G. (2025) ‘Trust by Design: An Ethical Framework for Collaborative Intelligence Systems in Industry 5.0’ Electronics14(10), p.1952.

Mohamed, N. and Al-Jaroodi, J. (2019) ‘The Impact of Industry 4.0 on Healthcare System Engineering’, IEEE International Systems Conference, pp. 1–7.

National Cyber Security Centre (2023) Cyber Security for Healthcare Organisations. London: NCSC.

Saxena, A., Chauhan, S.P.S., Singh, H., Chauhan, U. and Kumari, P. (2024) ‘Impact of Industry 5.0 on Healthcare’, *Infrastructure Possibilities and Human-Centered Approaches with Industry 5.0* pp. 182-198.