Cybersecurity as an Application Domain for Quantum-Assisted FRAM Instantiation Analysis

David Slater

Cybersecurity provides a strong candidate application domain for the argument developed in the concept paper (Slater, 2026). Cyber incidents rarely arise from a single isolated technical defect. They often emerge from combinations of vulnerability, exposure, trust relationships, workload, timing, degraded monitoring, automation behaviour, human response and adversarial adaptation. This makes cybersecurity a natural domain for instantiation-space analysis.

Existing cyber frameworks already recognise this systems character. The NIST Cybersecurity Framework 2.0 organises cybersecurity outcomes around the functions Govern, Identify, Protect, Detect, Respond and Recover, emphasising risk management across the full lifecycle of cyber activity (NIST, 2024). NIST SP 800-160 Volume 2 further frames cyber resilience as the capability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises affecting systems that depend on cyber resources (Ross et al., 2021). MITRE ATT&CK provides a structured knowledge base of adversary tactics and techniques based on real-world observations, supporting threat modelling and defensive analysis (MITRE, n.d.). These frameworks are not FRAM models, but they show that cybersecurity is already understood as a dynamic interaction among functions, controls, adversary behaviours and organisational responses.

A FRAM-based cyber model would not merely list vulnerabilities or attack techniques. It would model the functions required to maintain cyber resilience and the ways in which

those functions interact. Examples of such functions include: to authenticate users, to manage access privileges, to monitor network activity, to detect anomalies, to triage alerts, to escalate incidents, to isolate affected assets, to patch vulnerabilities, to maintain asset visibility, to coordinate response, and to recover services. These functions are coupled through information flows, control decisions, resource constraints, timing conditions and dependencies on human and automated response.

In this framing, a hazardous cyber instantiation is not simply an exploit path. It is a realised configuration of functional conditions in which the cyber system becomes more vulnerable, less observable, less controllable or less recoverable. For example, a hazardous instantiation might involve a delayed patching function, incomplete asset visibility, excessive alert volume, weakened triage, over-trust in automated filtering, delayed escalation and an adversary exploiting the resulting window of opportunity. Each function may remain locally understandable, but their combined variability may produce a system-level cyber-resilience failure.

This is closely aligned with the logic of attack graphs, which model possible sequences of exploits or transitions through a system. Attack-graph research has long recognised that multi-stage cyber compromise can be represented as a structured space of possible paths (Sheyner et al., 2002; Mehta et al., 2006). However, a FRAM-based approach would extend this logic beyond technical exploit sequences. It would include the socio-technical functions that shape exposure, detection, response and recovery. The resulting model would therefore represent not only how an attacker may move through a technical environment, but how the defensive system may vary in ways that permit, amplify, dampen or recover from that movement.

The cyber-FRAM instantiation space could include variables such as:

- authentication state;
- privilege configuration;
- asset visibility;
- patch status;
- monitoring coverage;
- alert volume;
- analyst workload;
- automation trust;
- response delay;
- recovery capacity;
- adversary progress;
- control effectiveness.

A candidate instantiation could then be represented as a realised combination of these variables across the cyber-resilience functions. A hazardous evaluator could mark instantiations in which adversary progress exceeds detection and response capacity, or in

which recovery margin drops below a defined threshold. A resilience evaluator could mark instantiations in which detection, containment and recovery remain effective despite degraded resources or active attack.

This creates a natural mapping to the quantum-assisted forms discussed in the main paper (Slater, 2026). Search methods could be used, conceptually, to find one rare but credible hazardous cyber instantiation. Amplitude estimation could estimate the proportion of plausible operating states in which cyber-resilience functions become insufficient. Optimisation could search for worst-case combinations of degraded visibility, delayed response and privilege exposure, or for intervention configurations that most reduce hazardous regions. Quantum-walk formulations could be used cautiously to explore propagation through typed functional couplings, although care would be needed not to reduce socio-technical cyber functions to undifferentiated graph nodes.

Cyber-FRAM Question	Computational Form	Possible Quantum Analogue
Is there a credible hazardous cyber instantiation?	Search	Grover / amplitude amplification
How large is the vulnerable operating region?	Probability estimation	Quantum amplitude estimation
Which combination maximises loss of resilience?	Optimisation	QAOA / variational optimisation
How does degradation propagate through response functions?	Graph exploration	Quantum walks
Which intervention most reduces hazardous states?	Optimisation / estimation	Hybrid quantum-classical analysis

The main advantage of this cyber application is that cybersecurity already works with large state spaces, graph-based attack modelling, adversarial adaptation and probabilistic reasoning. It is therefore a more natural candidate for early conceptual demonstration than many physical domains. A small proof-of-concept could begin with a simplified enterprise cyber-resilience model containing a limited number of functions: to maintain asset inventory, to patch vulnerabilities, to monitor events, to triage alerts, to contain incidents and to recover services. Metadata could encode patch delay, alert volume, visibility, automation confidence, analyst capacity and response time. A simple evaluator could mark instantiations in which adversary progression exceeds detection and containment capability.The purpose of such a proof-of-concept would not be to claim operational quantum advantage. It would be to test whether a cyber-FRAM model can be transformed into a bounded instantiation-space problem and whether search, estimation or optimisation formulations remain interpretable in FRAM terms. The result would be

judged not only by computational performance, but by whether the discovered or estimated instantiations provide meaningful cyber-resilience insight.

Cybersecurity therefore strengthens the paper's central argument. It shows that the proposed quantum-FRAM bridge is not limited to abstract safety modelling. It may apply particularly well to domains where risk emerges from combinations of technical state, human workload, organisational control, automation behaviour and adaptive adversarial action. Cybersecurity is one such domain. A quantum-assisted FRAM approach would not replace existing cyber frameworks such as NIST CSF, MITRE ATT&CK or attack-graph analysis. Rather, it could provide a complementary metamodel for exploring how cyber-resilience functions vary, interact and sometimes resonate into hazardous instantiations.

References

- Aharonov, D., Ambainis, A., Kempe, J. and Vazirani, U. (2001) 'Quantum walks on graphs', Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, pp. 50–59.
- Brassard, G., Høyer, P., Mosca, M. and Tapp, A. (2000) 'Quantum amplitude amplification and estimation', arXiv:quant-ph/0005055.
- Farhi, E., Goldstone, J. and Gutmann, S. (2014) 'A quantum approximate optimization algorithm', arXiv:1411.4028.
- Grover, L.K. (1996) 'A fast quantum mechanical algorithm for database search', Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp. 212–219.
- Hollnagel, E. (2012) FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems. Farnham: Ashgate.
- Hollnagel, E. and Slater, D. (2018) A FRAM Handbook. FRAMsynt.
- Mehta, V., Bartzis, C., Zhu, H., Clarke, E. and Wing, J. (2006) 'Ranking attack graphs', Recent Advances in Intrusion Detection, pp. 127–144.
- MITRE (n.d.) MITRE ATT&CK®. Available at: https://attack.mitre.org/
- Montanaro, A. (2015) 'Quantum speedup of Monte Carlo methods', Proceedings of the Royal Society A, 471(2181), 2015030
- NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology.
- Patriarca, R., Di Gravio, G., Woltjer, R., Costantino, F., Praetorius, G., Ferreira, P. and Hollnagel, E. (2020) 'Framing the FRAM: A literature review on the Functional Resonance Analysis Method', Safety Science, 129, 104827.
- Preskill, J. (2018) 'Quantum computing in the NISQ era and beyond', Quantum, 2, 79.
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R. (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160 Volume 2 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology.
- Sheyner, O., Haines, J., Jha, S., Lippmann, R. and Wing, J. (2002) 'Automated generation and analysis of attack graphs', Proceedings of the IEEE Symposium on Security and Privacy, pp. 273–284.
- Slater, D., (2026) Quantum-Accelerated Exploration of Functional Instantiations: FRAM as a Candidate Metamodel for Quantum Computing Analysis, https://www.researchgate.net/publication/405181890_Cybersecurity_as_an_Application_Domain_for_Quantum-Assisted_FRAM_Instantiation_Analysis