Written evidence submitted by Dr Áine MacDermott (Liverpool John Moores University):

Cyber Security and Resilience (Network and Information Systems) Bill

Introduction

I am a Senior Lecturer specialising in Cyber Security and Digital Forensics in the School of Computer Science and Mathematics at Liverpool John Moores University (LJMU). This written evidence is based on my work at the research centre for Critical Infrastructure Computer Technology and Protection (PROTECT) at LJMU. I would be happy to appear in front of the Committee to give an oral submission, answer any questions, and provide the Committee with any more details if needed.

Scope

This written evidence examines critical gaps in the Cyber Security and Resilience (Network and Information Systems) Bill, focusing on the security obligations of cloud services, data centres, managed service providers, and wider third-party supply chains, all of which now form an integral part of UK organisational infrastructure. It highlights unresolved challenges around how compliance will be measured across these outsourced ecosystems, drawing on evidence that almost all organisations rely on external IT, cloud hosting, or data-centre providers. The submission also addresses the escalating threat environment (averaging four nationally significant cyber-attacks per week in the UK) and identifies key omissions in the Bill relating to attacker dwell-time detection, forensic-grade telemetry, and mandatory reporting standards needed to strengthen national cyber resilience.

1. Executive Summary

This submission critiques the Cyber Security and Resilience (Network and Information Systems) Bill (2024–26), focusing on key gaps relating to cloud and third-party transparency, attacker dwell time, and the absence of requirements for fine-grained telemetry (including keystroke-level monitoring).

While the Bill expands regulatory scope and amendments to NIS Regulation, to cloud services, digital infrastructure, managed service providers and critical suppliers, it does not set minimum visibility, audit, or compliance-measurement standards needed for effective oversight.

There is clear designation of critical suppliers and infrastructure. Research on hosting critical infrastructure services in cloud environments shows that organisations

increasingly rely on outsourced IT, data centres, and cloud providers, and therefore require stronger, standardised compliance expectations and detection capabilities.

The legislation does not specify standards for cross-provider evidence acquisition, harmonised log formats, forensic readiness obligations, or multi-party chain-of-custody protocols.

2. The Bill's Treatment of Cloud Services and Third-Party Providers

2.1 The Bill expands the scope of regulated entities to include cloud computing services, data centres, managed service providers (MSPs), and designated critical suppliers. This reflects the evolving threat environment and the concentration risk inherent in interconnected digital supply chains [1], [2], [3].

2.2 Addition on Managed Service Providers (MSPs): The expanded scope now also includes managed service providers, defined as organisations that deliver ongoing outsourced functions (such as IT help desks, remote administration, and operational IT support) to external clients. This inclusion is crucial: MSPs possess elevated and persistent access across multiple customer environments, making them high-value targets for cybercriminals. Attackers who compromise a single MSP can leverage that access to infiltrate numerous client organisations simultaneously, resulting in widespread disruption. This mirrors concerns raised in expert commentary highlighting systemic risks introduced by supply-chain dependencies [4].

2.3 Despite this justified expansion, the Bill provides no specific minimum transparency or security requirements for cloud or MSP providers. There is no statutory expectation for essential telemetry (e.g. privileged access logs, cloud API logs, configuration drift), nor any obligation to provide customers or regulators with audit-ready security data. Map controls and telemetry to recognised frameworks (NIST, ISO, Cloud Security Alliance (CSA) Cloud Controls Matrix (CSA CCM)) ensure consistency and auditability. Framework alignment also helps standardise how risk is measured across teams and clouds [5].

2.4 The designation-based model (regulatory/operational frameworks where specific entities, projects, or products are formally identified) may bring many suppliers into scope (especially supply chain/third party), but the Bill lacks clear mechanisms for verifying their compliance or ensuring they maintain adequate cyber maturity [6].

2.5 Because almost all organisations now rely on data centres, outsourced IT, supply-chain vendors, and MSPs, the government must define how compliance will be measured. An increased uptake of Cyber Essentials and alignment with the Government's Cyber Action Plan are essential to operationalise compliance expectations across these sectors.

3. Businesses and Government Reliance on Cloud and Outsourced IT

3.1 Although the Bill focuses on essential services, its impact extends to the wider UK economy. Most organisations now depend on outsourced digital infrastructure - including cloud hosting, data centres, managed service providers (MSPs), and third-party IT operations - which creates systemic exposure across entire supply chains. Cloud compromises affected by identity and single sign on (SSO) misconfigurations, with threat groups such as UNC3944 and UNC5537 exploiting cloud identity gaps [7].

3.2 This dependency heightens operational risk because these outsourced environments often contain privileged access pathways, remote administrative interfaces, and shared-tenant architectures that expand the attack surface. Threat actors increasingly exploit these interconnections, and UK incident data shows persistent targeting of critical infrastructure operators and local government bodies [8], [9].

3.3 A key challenge for regulated and non-regulated organisations alike is how to measure and demonstrate compliance when critical security controls are distributed across multiple external providers. Without mandated visibility standards (such as audit-ready logging, cross-tenant forensic access, and real-time telemetry) organisations may be unable to verify that their outsourced environments meet baseline security expectations. Broad cloud outages (though rare) can cause substantial business disruption and cross-sector cascading effects [10].

3.3a This risk is compounded by rising cyber-insurance pressures, as FTSE-listed firms face increasing premiums following major breaches, with insurers demanding stronger evidence of technical controls and attack-path clarity. At the same time, underwriters report growing difficulty pricing policies when vendors cannot fully explain the parameters of an intrusion or provide assurances for hypothetical attacks that have not yet occurred, resulting in exclusions or reduced coverage [10], [11].

3.4 Given the interconnected nature of UK digital infrastructure, wider adoption of structured baseline controls (such as those in Cyber Essentials) and alignment with national guidance will be essential to establish measurable and consistent security standards across organisations of all sizes.

4. Failure to Address Attacker Dwell Time

4.1 The UK recorded 204 nationally significant cyber incidents in the past 12 months, up from 89 the previous year, demonstrating a steep escalation in threat activity and the urgent need for earlier detection capabilities [12]. Despite this, the Bill does not require organisations to measure, report, or reduce attacker dwell time – a critical omission. Global median dwell time has risen to 11 days (from 10 days in 2023) [7].

4.1a Furthermore, dwell time for internally discovered intrusions remains shorter than for intrusions externally notified, indicating that many organisations still struggle to detect breaches themselves before adversaries disclose or weaponise the intrusion. Persistent, long-dwell intrusions are particularly common within cloud and MSP-hosted environments, where complex identity structures, remote administrative access, and shared-tenant architectures create additional blind spots [13].

4.2 Although the Bill's 24 hour reporting requirement is operationally demanding, expert analysis shows that accelerated reporting has minimal security impact if organisations lack the visibility and capability to detect intrusions promptly. Incident-response findings highlight that median dwell times still span multiple days (and often weeks) despite mandatory reporting frameworks. As a result, reporting obligations risk becoming procedural rather than protective if they are not paired with enforceable detection and monitoring standards [7], [13], [14].

4.3 Research on intrusion detection in cloud infrastructures consistently shows that the distributed, dynamic, and identity-centric nature of cloud environments significantly increases the difficulty of identifying malicious activity. Cloud ecosystems amplify detection challenges, including identity misuse, misconfigured access pathways, and unsecured data repositories: all of which are prominent themes in frontline cloud compromise investigations, such as those documented in M-Trends 2025. These structural complexities underscore the need for mandated, high-fidelity telemetry, including behavioural analytics, identity-centric audit trails, and real-time monitoring, across both cloud and hybrid deployments [7].

4.4 These factors underscore the need for mandated, high-precision detection and monitoring requirements across cloud and hybrid deployments. Moreover, growing interdependency, cross-platform interoperability, and the risk of cascading failures across shared cloud and MSP infrastructures demand further regulatory scrutiny to ensure a well-rounded and resilient national cyber-defence posture [8], [9], [15], [16].

5. Absence of Requirements for Fine-Grained Telemetry

5.1 The Bill does not set minimum logging or telemetry expectations, despite the prevalence of hands-on-keyboard intrusions and remote interactive attacks. Modern threat actors increasingly exploit real-time remote access channels, meaning detection often depends on behavioural signals rather than traditional signature-based monitoring.

5.2 While regulators may request information, the Bill establishes no statutory visibility baseline, leaving it unclear whether organisations must collect session-level telemetry, endpoint behavioural traces, or high-resolution interaction logs.

5.3 Recent incidents highlight why fine-grained telemetry is essential. Amazon uncovered a North Korean IT infiltrator after detecting an anomalous 110-millisecond keystroke input delay, far slower than the expected tens-of-milliseconds latency for genuine U.S. remote workers. This discrepancy revealed that the Amazon-issued laptop was being remotely controlled from overseas, triggering an investigation and removal of the operative. Amazon reports having blocked more than 1,800 similar infiltration attempts since April 2024, with attempts rising 27% quarter-over-quarter, underscoring how keystroke-timing analysis and behavioural telemetry are critical for detecting sophisticated state-sponsored impersonation schemes [17].

5.4 This case demonstrates that without mandated requirements for fine-grained telemetry such as keystroke timing, input-event analytics, session tracing, and anomaly detection, organisations may be unable to identify remote-access deception, identity hijacking, or covert operator-in-the-loop attacks, especially in distributed and hybrid cloud environments.

6. Insufficient Provisions for Cross-Provider Forensics and Joint Incident Response

6.1 While regulators can designate critical suppliers, the Bill does not specify how multiple vendors (e.g., cloud providers, MSPs) should coordinate forensic support or evidence disclosure during incidents. The focus heavily on expanding regulatory scope and enhancing incident-reporting obligations but does not address the operational requirements for coordinated forensic workflows across multiple service providers in complex, distributed environments.

6.2 Given the Bill's expansion to include managed service providers, data centres, and cloud services, modern incidents will almost certainly span multiple vendors. Yet the legislation does not specify standards for cross-provider evidence acquisition, consistent log formats, forensic readiness obligations, or multi-party chain-of-custody protocols. This is a notable gap, as contemporary research in federated and multi-cloud security consistently highlights the necessity of interoperable evidence-sharing models and jointly executed intrusion analysis (particularly in cases where attacks propagate laterally across service boundaries). The absence of such coordination requirements poses risks to timely and comprehensive incident investigation and may impede regulators' ability to form accurate situational awareness across the ecosystem.

7. Recommendations

Continue to raise awareness and strengthen organisational education. Government, regulators, and industry bodies should maintain ongoing efforts to educate organisations (particularly those operating in critical sectors) about emerging threats, best-practice security controls, and the responsibilities introduced by the Bill. Sustained

awareness-raising, sector-specific guidance, and accessible training resources will be essential to improving national cyber resilience and ensuring that all operators understand how to meet and evidence compliance expectations. In addition:

- Mandate cloud/MSP transparency (comprehensive audit logs, privileged-access monitoring, cloud API telemetry) and require providers to map security controls to NIST, ISO 27001, and CSA CCM.
- Require dwell-time reporting and a baseline of detection capabilities (behavioural analytics, anomaly detection, automated alerting).
- Set minimum endpoint-level telemetry standards, covering keystrokes (where appropriate), session activity logs, command execution visibility, and API-level analytics.
- Impose cross-provider forensic cooperation duties, ensuring timely evidence sharing, robust evidence-preservation obligations, and coordinated multi-vendor investigative workflows.
- Drive widespread Cyber Essentials adoption and align compliance with the Government's Cyber Action Plan to operationalise baseline controls across sectors.

Conclusion

The Cyber Security and Resilience (Network and Information Systems) Bill is a vital legislative step towards strengthening the UK's digital defences and resilience. However, without explicit requirements for cloud transparency, dwell-time mitigation, and fine-grained telemetry, the Bill risks failing to deliver the level of resilience demanded by the current threat landscape. I would be happy to work with the Committee further to discuss how these recommendations could be implemented in practice.

Please contact Dr Áine MacDermott: a.m.macdermott@ljmu.ac.uk

3rd February 2026

References

[1] T. Baker et al., 'A secure fog-based platform for SCADA-based IoT critical infrastructure', Softw. Pract. Exp., vol. 50, no. 5, 2020, doi: 10.1002/spe.2688.

[2] W. Hurst and Á. MacDermott, 'Evaluating the effects of cascading failures in a network of critical infrastructures', International Journal of System of Systems Engineering, vol. 6, no. 3, 2015, doi: 10.1504/IJSSE.2015.071458.

[3] K. E. Lever, A. MacDermott, and K. Kifayat, 'Evaluating Interdependencies and Cascading Failures Using Distributed Attack Graph Generation Methods for Critical Infrastructure Defence', in Proceedings - 2015 International Conference on Developments in eSystems Engineering, DeSE 2015, 2016.

[4] A. MacDermott, W. Hurst, Q. Shi, and M. Merabti, ‘Simulating critical infrastructure cascading failure’, in Proceedings - UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, UKSim 2014, 2014. doi: 10.1109/UKSim.2014.85.
[5] J. O’Donnell, ‘Enterprise Cloud Security: Best Practices and Guide’, Cymulate. Retrieved from: https://cymulate.com/blog/enterprise-cloud-security-best-practices/.
[6] R. Jeens and N. Donovan, ‘NCSC insights into what the CSRB means for the UK’s critical suppliers’, Law Business Research - Salughter and May. Retrieved from: https://www.lexology.com/library/detail.aspx?g=33ae8204-310e-4137-9f22-1665924a8e42.
[7] ‘Google Cloud Security M-Trends’, 2025.
[8] H. Riggs et al., ‘Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure’, Apr. 01, 2023, MDPI. doi: 10.3390/s23084060.
[9] S. Reddy Addula, S. Norozpour, and M. Amin, ‘Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing’, Jordanian Journal of Informatics and Computing, vol. 2025, no. 1, pp. 1–12, Mar. 2025, [Online]. Available: https://jjic.thestap.com/
[10] G. R. and M. R. C. Beazley, ‘Cyber Realistic Disaster Scenario Development and Modelling Triple threat: a new malware model for systemic cyber insurance industry losses’, Oct. 2024.
[11] N. Charles, ‘The rising stakes of cyber insurance’, Oryx Align. Retrieved from: https://www.oryxalign.com/blog/the-rising-stakes-of-cyber-insurance?hs_amp=true.
[12] National Cyber Security Centre, ‘UK experiencing four “nationally significant” cyber attacks every week’, National Cyber Security Centre (NCSC). Retrieved from: https://www.ncsc.gov.uk/news/uk-experiencing-four-nationally-significant-cyber-attacks-weekly.
[13] Information Security Forum, ‘ISF Threat Horizon 2025: Scenarios for an uncertain future’, May 2025. [Online]. Available: https://www.xenonstack.com/insights/big-data-challenges#:~:text=Data%20Growth%20
[14] National Audit Office, ‘Government cyber resilience Cabinet Office Report’, London, Jan. 2025.
[15] F. Abdullayeva, ‘Cyber resilience and cyber security issues of intelligent cloud computing systems’, Results in Control and Optimization, vol. 12, Sep. 2023
[16] C. O. Fjäder, ‘National security in a hyper-connected world: Global interdependence and national security’, in Advanced Sciences and Technologies for Security Applications, Springer, 2016, pp. 31–58. doi: 10.1007/978-3-319-27914-5_3.
[17] Anupriya, ‘Amazon Identifies North Korean IT Worker by Tracking Keystroke Activity’, Cybe Press. Retrieved from: https://cyberpress.org/amazon-identifies-north-korean-it-worker-by-tracking-keystroke-activity/.