Title:

From Compute to Coercion: Infrastructure-Based Responsibility for AI-Enabled Grey-Zone Harm

Abstract:

The governance of AI-enabled grey-zone operations suffers from a timing gap. Domestic liability regimes usually respond after deployment and harm, while international law often becomes practically actionable only when conduct crosses thresholds such as prohibited intervention or the use of force and can be attributed to a State. Yet AI-enabled influence operations, cyber operations, and autonomous surveillance may produce cumulative below-threshold effects that constrain another State's choices without clearly triggering those rules. Existing cyber-law frameworks, including Tallinn Manual 2.0, help classify individual operations but do not fully address this form of cumulative coercion (Schmitt 2017, 30-38, 84-100, 312-338).

This paper shifts the inquiry from the legal classification of isolated conduct to the governance of the infrastructure through which high-risk AI capabilities are trained, scaled, accessed, and deployed. Compute providers and cloud service providers occupy a distinctive position because they can identify customers, preserve records, monitor certain uses, and restrict access in defined cases. Recent compute-governance literature therefore describes them as regulatory intermediaries and treats cloud infrastructure as a possible control point for upstream oversight (Egan and Heim 2023, 1-3, 7).

The paper develops an infrastructure-based due-diligence framework. It does not claim that private providers directly bear a general due-diligence obligation under international law. Rather, it asks how State due-diligence obligations, where applicable, may be operationalised through risk-based and proportionate regulation of infrastructure providers. The proposed framework calibrates regulatory duties according to the severity and likelihood of harm, knowledge of the risk, the degree of control over the relevant infrastructure, the means reasonably available, and the provider's leverage over the customer or workload. Possible measures include customer identification, record preservation, reporting of defined high-risk activity, and targeted suspension or restriction of access (Ridings 2024, 146-147, 153; OECD 2023, 2, 44-46).

The central claim is modest. AI-enabled grey-zone operations should not be artificially reclassified as uses of force merely to close a governance gap. At the same time, they should not be left solely to ex post liability after harm has materialised. International due diligence provides the legal structure, while compute governance provides the operational tools, for a proportionate form of upstream risk management.

Short Bibliography:

Egan, Janet, and Lennart Heim. 2023. *Oversight for Frontier AI through a Know-Your-Customer Scheme for Compute Providers*.

Heim, Lennart, et al. 2024. *Governing Through the Cloud: The Intermediary Role of Compute Providers in AI Regulation*.

OECD. 2023. *Advancing Accountability in AI*.

Ridings, Penelope. 2024. "Due Diligence in International Law," Annex II to ILC Report A/79/10.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.