

Cyber Diplomacy and Data Governance: Legal Perspectives on India-Malaysia Cooperation in the Digital Indo-Pacific Knowledge Gaps, Definition of Methods and Analytical Procedure

Ausaf Ahmad Malik¹, Kittisak Wongmahesak²

¹Global Postdoctoral & Researcher Programme, Lincoln University College, Malaysia and Professor, UILS, Chandigarh University, Mohali, ²Faculty of Political Science, North Bangkok University, Thailand; Global Postdoctoral & Researcher Programme, Lincoln University College, Malaysia

ausafmalik111@gmail.com

kittisak.wongmahesak@gmail.com

Abstract: Though the Digital Indo-Pacific is becoming increasingly significant, cyber diplomacy and data governance have been developing as distinct research fields and the bilateral legal relationship between India and Malaysia has not been explored much (problem statement). In order to address these identified knowledge gaps, it is necessary to define a methodology for the analysis of the ASEAN-India legal landscape (solution), which, in this paper, is presented as a mix of doctrinal legal analysis, comparative legal method and normative document analysis. In response, this paper identifies the following five interrelated gaps in the knowledge base: limited bilateral legal research, the fragmented treatment of cyber diplomacy and data governance, weak analysis of ASEAN-India normative interaction, insufficient legal interoperability assessment and lack of research grounded in the implementation. The methodology is implemented at three stages of analysis: comparative legal mapping, interoperability assessment and normative gap analysis, all of which examine not only what the law offers, but how well it is able to assist in facilitating bilateral cooperation in the field (significant findings). The final framework provides a structured and interdisciplinary platform for the convergence of cyber-norms, law interoperability and building a trusted and resilient India-Malaysia digital partnership (applications).

Keywords: Cyber Diplomacy; Data Governance; India-Malaysia Cooperation; Legal Interoperability; Digital Indo-Pacific

Introduction

The Digital Indo-Pacific has become a new dimension of statecraft, with cyber diplomacy and data governance emerging as key enablers in the negotiation of sovereignty, security and cross-border exchanges in digital environments. In this changing environment, the Indian and Malaysian case stands out as a unique yet under-researched one and that is because these two Indo-Pacific nations have a number of strategic interests common to them, growing digital economies and relatively recent overhauls of their domestic data protection laws, but no legal literature that is dedicated to their bilateral cooperation. This paper reports Phase 2 of the study, the identification of gaps in existing knowledge and the identification of the methods, experiments and analytical procedures in which the research addresses gaps. The discussion starts with the identification of gaps, moves to methodological design and ends with

the analytical processes that are used to operationalize the study's objectives in the legal and comparative realm.

Related work

Based on a literature review, five related knowledge gaps were identified on the related topic of cyber diplomacy, data governance and Indo-Pacific digital cooperation. First, the existing literature focused on India's cyber diplomacy looks at the cyber cooperation between India and major powers like the United States, Japan, Australia and the European Union [11] and Malaysia's cyber diplomacy is studied more within the ASEAN cyber collective digital governance architecture as opposed to bilateral frameworks. Second, the study of "cyber diplomacy" and "data governance" [2] has so far taken place separately, resulting in a fragmented approach that calls for the harmonization of legal norms and institutional coordination in effective legal cooperation in the Digital Indo-Pacific. Third, the normative analysis of the interplay of ASEAN consensus-based digital governance with Indo-Pacific cyber diplomacy [3] of India is still minimal, which is important for the study of how ASEAN commitments are formulated from the consensus as well as bilateral engagement. Fourth, current scholarship provides some legal interoperability analysis of the two states' data governance and cybersecurity regimes, albeit with weak support. Fourth, current scholarship lacks a strong legal interoperability analysis of the two states' data governance and cybersecurity regimes. [1] Finally, there is a highly uneven focus of the literature on the design of legal norms and diplomatic commitments, paying only limited attention to their institutional implementation. The present work stands in relation to these groups of literature, as can be seen in Table 1.

Table 1. Compares this work with the clusters of existing literature on cyber diplomacy and data governance

	Bilateral India-Malaysia Focus	Integrates Cyber Diplomacy & Data Governance	Implementation-Focused Analysis
India-major power cyber diplomacy literature	No	No	No
ASEAN collective digital governance literature	No	No	No
Comparative India-Malaysia data protection studies	Partial	No	No
This work	Yes	Yes	Yes

Key Contribution

This study can make a contribution to the body of knowledge in three ways. First, it brings together a specific field of knowledge gaps unique to the India-Malaysia cyber-diplomacy and data-governance relationship, as opposed to considering the dyad as part of India's major-power partnerships or Malaysia's ASEAN engagements. [7] Second, it presents a methodology for the second principles of cyber diplomacy,

a qualitative, law-based approach, which combines doctrinal analysis, comparative legal method and normative document analysis [4], all in one analytical ‘box’. Third, it puts this methodology into practice by using three interrelated analytical steps (comparative legal mapping, interoperability assessment and normative gap analysis), which goes beyond the identification of legal challenges to provide a structured and replicable way of evaluating the legal interoperability between the two jurisdictions. [10]

Method

The study has a qualitative research design based on the law, using the doctrinal legal analysis approach, comparative legal approach and structured interoperability assessment. This addresses the lack of doctrinal analysis of bilateral legal research, an integrated analytical approach is developed to overcome the lack of interoperability between cyber diplomacy and data governance, the comparison of norms is developed to address the ASEAN-India interaction gap [7], the institutional/document-based triangulation is developed to overcome the implementation-focused research gap found and the interoperability assessment is structured to target cyber diplomacy and data governance. The research relies on primary legal sources, including national legislation, subsidiary legislation and guidance from the Indian and Malaysian regulators and ASEAN-India and broader Indo-Pacific digital cooperation frameworks, as well as secondary sources such as peer-reviewed legal and international-relations scholarship [8]. The following four methods are used:

- (i) doctrinal legal analysis of the main statutory and regulatory instruments governing data protection and cybersecurity in India and Malaysia;
- (ii) comparative legal method, focusing on the functionalist approach to comparison, which compares provisions based on their functions, not just form;
- (iii) normative and institutional document analysis of ASEAN, India and bilateral India-Malaysia policy documents to trace convergence and divergence; and
- (iv) qualitative content analysis of ASEAN/India and India-Malaysia joint statements, MoUs and regional frameworks on digital cooperation to assess practical, as opposed to declaratory, cooperation.

Analytical Procedure

The following three related analytical procedures are implemented as part of these methods. Comparative legal mapping is a systematic mapping of the data governance and cybersecurity instruments in India and Malaysia to a set of common regulatory functions such as scope of application, cross-border data transfer mechanisms, consent architecture, breach notification, enforcement powers and state access provisions [5]. The assessment of interoperability then considers how the two legal systems actually interoperate; each provision mapped is evaluated as substantively aligned, formally divergent with functional equivalence or as a genuine regulatory gap. Conducted through a normative gap analysis, this study compares India’s ‘flexible and partnership-based’ Indo-Pacific diplomacy with the ‘consensus-based digital governance framework’ of ASEAN, focusing on the gaps between the normative commitment of the two and the operationalization of the former through the latter.

Results

The results presented below are expected outcomes based on the procedure outlined above and are not directly empirical results of this stage of the study, which is focused on defining the knowledge gap and research design. It is hoped that comparative legal mapping will produce a matrix of all the data governance and cybersecurity instruments in India and Malaysia on a function-by-function basis. The

interoperability assessment is expected to determine the level of substantive alignment of each of the provisions covered in the map, formal divergence, but functional equivalent or a genuine regulatory gap [6] and generate an interoperability profile for bilateral relationships. The aim of the normative gap analysis is to create a list of areas where there has not yet been binding or workable legal cooperation between the bilateral and regional commitments declared. These expected outcomes will not only assess the content of the law but also its potential to facilitate actual bilateral cooperation between India and Malaysia and will provide the empirical footing for the next step in the study.

Discussions

Together, these five knowledge gaps suggest that the lack of a legally grounded, comparative and empirically triangulated account of the interaction between India's and Malaysia's data governance regimes [9] at the national level, with the new commitments they have made at the bilateral and regional level as cyber diplomatic actors. Diplomacy (norms, summits, joint statements) and the law (statutory comparison) are usually dealt with separately and neither is applied to institutional practice. The methodology of this study is developed to fill that gap, as it proposes to compare legal frameworks, assess their interoperability and do a normative gap analysis looking at what the law offers, but also at how well it can be used in practice in bilateral cooperation. The layered approach also helps define the areas where cooperation is legally possible under existing instruments and where new bilateral or regional instruments are needed, as opposed to those commitments that are merely declaratory.

Conclusions

The results of this stage of the research will be presented below, line by line:

1. Problem statement/motivation addressed: The scarcity of targeted legal research and literature on India-Malaysia cyber diplomacy and data governance and the disjointed coverage of the two within the broader Digital Indo-Pacific literature.
2. Method applied: qualitative, law-centred design based on the doctrinal legal approach, comparative legal approach and normative document analysis, that was operationalized through the layers of comparative legal mapping, interoperability assessment and normative gap analysis.
3. The five knowledge gaps that were revealed, but not necessarily mutually exclusive, are: limited bilateral legal research, fragmented ASEAN-India normative interaction analysis, limited research into legal interoperability and the absence of implementation-oriented research, all of which are connected to a method and analytical procedure within this framework.
4. Limitations of the work and future work: The analysis so far is doctrinal and comparative and needs to be triangulated with elite interviews with officials and practitioners of the respective jurisdictions and updated as the DPDP Rules in India and the subsidiary legislation in Malaysia are finalized following the amendments in both rules in 2024 [12].

References

1. A. Vafaei-Zadeh, D. Nikbin, K. Y. Teoh, and H. Hanifah, "Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia," *International Journal of Bank Marketing*, vol. 43, no. 3, pp. 476–505, 2025. Available: <https://doi.org/10.1108/IJBM-03-2024-0138>

2. A. Malik and K. Wongmahesak, "Cyber Diplomacy and Data Governance: Legal Perspectives on India–Malaysia Cooperation in the Digital Indo-Pacific," *Sustainable Global Societies Initiative*, vol. 1, no. 5, 2026. Available: <https://vectmag.com/sgsi/paper/view/483>
3. S. Bıçakçı, A. Gücüyener Evren, and A. G. Maail, "Cyber coercion in the Indo-Pacific: A comparative analysis of India's and Australia's responses," *Frontiers in Political Science*, vol. 8, Art. no. 1748496, 2026. Available: <https://doi.org/10.3389/fpos.2026.1748496>
4. W. Vosse and M. Dizon, "EU Influence on Cyber Governance in the Indo-Pacific: A Normative Power in a Contested Space," *The Hague Journal of Diplomacy*, vol. 20, no. 4, pp. 707–742, 2025. Available: <https://doi.org/10.1163/1871191X-bja10229>
5. M. B. F. Manantan, "Advancing cyber diplomacy in the Asia Pacific: Japan and Australia," *Australian Journal of International Affairs*, vol. 75, no. 4, pp. 432–459, 2021. Available: <https://doi.org/10.1080/10357718.2021.1926423>
6. I. A. Khan, A. A. Malik, and A. Agarwal, "Implementing AI, Big Data, and the IoT: Ethical and Regulatory Considerations," in *Harnessing AI Inference for Intelligent Decision-Making in Real-Time Dataflows*, IGI Global Scientific Publishing, Hershey, PA, USA, pp. 267–296, 2026. Available: <https://doi.org/10.4018/979-8-3373-7046-0.ch010>
7. K. Nachiappan, "India–ASEAN Relations: Riding and Transcending the 'Indo-Pacific' Wave," *The Journal of Indian and Asian Studies*, vol. 2, no. 2, Art. no. 2140004, 2021. Available: <https://doi.org/10.1142/S2717541321400040>.
8. C. Ogden, "India–ASEAN Relations: The Utility and Limits of a Norm-Based Approach," *International Studies*, pp. 1–21, 2023. Available: <https://doi.org/10.1177/00208817231162272>.
9. R. Gong, *Enhancing Data Governance in Malaysia: Prioritising Protections, Accountability, and Efficiency*. Kuala Lumpur, Malaysia: Khazanah Research Institute, 2024. [Online]. Available: <https://www.krinstitute.org/publications/enhancing-data-governance-in-malaysia-prioritising-protections-accountability-and-efficiency-cetvq>
10. IEEE and ISO, "IEEE/ISO International Standard—Health Informatics—Device Interoperability—Part 40101: Foundational—Cybersecurity—Processes for Vulnerability Assessment," *ISO/IEEE 11073-40101:2022(E)*, pp. 1–54, Mar. 18, 2022. Available: <https://doi.org/10.1109/IEEESTD.2022.9738537>
11. P. K. Chaudhary, "India's cybersecurity diplomacy: Building global alliances," *ShodhKosh: J. Visual and Performing Arts*, vol. 4, no. 2, pp. 2199–2203, 2023, <https://doi.org/10.29121/shodhkosh.v4.i2.2023.3386>
12. Parliament of Malaysia, *Personal Data Protection (Amendment) Act 2024 (Act A1727)*, Laws of Malaysia, Putrajaya, Malaysia, Oct. 2024.