Cyber Diplomacy and Data Governance: Legal Perspectives on India-Malaysia Cooperation in the Digital Indo-Pacific

Ausaf Ahmad Malik[1], Kittisak Wongmahesak[2]
[1] LGPR, Programme, Lincoln University College, Malaysia
[2] Professor, Faculty of Political Science, North Bangkok University, THAILAND
ausafmalik111@gmail.com , kittisak.wongmahesak@gmail.com

Abstract: The advent of a digital revolution has turned cyberspace into a new arena of international relations, which requires the combination of the legal system with diplomacy. The concept of cyber diplomacy and data governance has become the primary part that contributes to the formation of state behaviour, guaranteeing cybersecurity and controlling international data transfer. India and Malaysia are two emerging digital economies that experience sophisticated legal and geopolitical issues in the Indo-Pacific region. This research is an analysis of the legal systems of cyber diplomacy and data governance in the two nations, the areas where harmonisation and enforcement are weak, and how the two countries can work jointly to address this problem. The research examines statutory frameworks, institutional approaches and policy approaches, using a doctrinal and comparative research approach and varying regimes of data protection, cybercrime legislation, and diplomatic involvement. It turns out that India is a country with a disjointed yet developing legal framework, whereas Malaysia is a country characterized by a high degree of statutory consistency and a low global orientation. This research states that to ensure that cyber diplomacy in the Digital Indo-Pacific is improved, it is imperative to bridge these gaps by having bilateral agreements, regional cooperation and alignment with international norms.
Keywords: Cybersecurity, Digital Indo-Pacific, bilateral agreements, and regional cooperation

1. Introduction

Cyberspace has become central to international relations through the digitalisation of economies and regimes, as the digital era has significantly transformed the nature of diplomatic and international interactions. The concept of cyber diplomacy, as the application of diplomatic resources to address cyber-related issues such as cybersecurity, online trade and data management, has emerged as a crucial tool for states to balance national security with economic development. The Indo-Pacific region, with its rapid technological progress and strategic competition, presents challenges for cyber governance.

As emerging digital economies, India and Malaysia have been placing a greater emphasis on cyber diplomacy within the framework of their foreign policy models. The cyber statecraft of India demonstrates its aspiration to influence global cyber standards and advocate for digital sovereignty, whereas Malaysia has focused on enhancing national regulatory frameworks and promoting regional cooperation processes. Nonetheless, even with the increased interaction, both nations have massive legal and institutional loopholes that do not allow them to cooperate in cyberspace effectively.

Besides, the absence of harmonised laws governing data flows and the non-existence of binding international agreements complicate cross-border data flows and the enforcement of cybercrimes. The importance of cyber diplomacy is restricted by the fact that states tend to use non-binding norms and bilateral agreements, as global cyber governance has been mostly informal and disjointed.

This research aims to examine how legal frameworks in India and Malaysia affect their cyber diplomacy policies and to determine areas for enhancing collaboration in the Digital Indo-Pacific.

Related Work

Current research on cyber diplomacy and data governance in the Indo-Pacific primarily focuses on regional cooperation frameworks, reviews of national legislation, and general legal policy comparisons. As the evaluated papers suggest, previous studies offer valuable conceptual insights but do not address the cross-border legal interoperability necessary for bilateral engagement. One paper highlights multilateral policy alignment without assessing the domestic legal framework, while another provides descriptive coverage of national legislation but neglects diplomatic processes. The third is more analytical; however, it does not cover operational issues such as regulatory dissimilarity, incident-response coordination, and data-sharing obstacles, which are central to operational cyber diplomacy.[1] [3]

Table 1. Comparison of the proposed work with the previous research

Ref.	Approach	Focus Area	Limitations	Key Contribution
[1]	Regional cyber cooperation analysis	Multilateral cyber diplomacy mechanisms	No assessment of national legal structures	Highlights regional policy alignment only
[2]	National cybersecurity law review	Domestic cyber legislation and governance	No examination of diplomacy or bilateral mechanisms	Establishes legal foundations but not cooperation models
[3]	Legal–policy comparative study	National law + regional cooperation frameworks	No bilateral cyber diplomacy analysis	Provides broad comparative insights
Proposed Work (2025)	Bilateral legal & diplomatic analysis	Cyber diplomacy + data governance between India and Malaysia	Does not address broader regional mechanisms	Introduces a focused bilateral, legally grounded cooperation framework

2. Contribution

This study contributes to the current body of research on cyber diplomacy and data governance in several ways.

Firstly, it gives a comparative legal study of India and Malaysia, which are understudied but strategically significant players in Indo-Pacific cyber governance. Although major powers are central in the existing literature, this research presents the importance of the middle powers in defining digital norms in the region. [1]

Second, the research combines the concepts of cyber diplomacy and data governance into a single analytical framework, showing the direct effect of the domestic legal system on international relations. It claims that cyber diplomacy cannot be interpreted without considering data protection laws, cybersecurity regulations and institutional capacity.

Third, the study finds evidence of certain legal gaps, such as the disjointed nature of legislation, lack of effective cross-border enforcement arrangements and limited treaty membership to limit effective collaboration between India and Malaysia.[2]

Fourth, the research presents policy-based recommendations, such as bilateral legal frameworks, regional harmonisation in ASEAN and alignment with international cyber norms, thus adding value to the academic field and policy debate.[3]

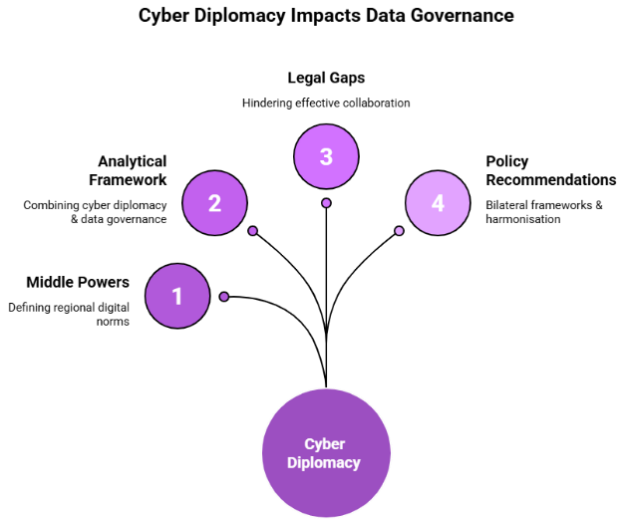

Fig 1. Syber Diplomacy and Data Governance

3. Method, Experiments and Results

The research approach chosen in this study is the method of doctrinal and comparative research, which is based on analyzing the texts of the law, policy documents and literature. The study is based on secondary sources, such as peer-reviewed articles in the journal, government reports and international policy reviews.

Key legislative tools that are studied using the doctrinal approach include India's Information Technology framework and laws on data protection, as well as Malaysia's cyber and data control laws. This includes the examination of legal requirements, institutional requirements and regulatory systems of cybersecurity and data flows.[4]

The comparative approach is used to determine similarities and differences between the two nations.

- ❖ Law coherence, law structure.
- ❖ Institutional coordination
- ❖ Data governance frameworks
- ❖ Cyber diplomacy by other nations.

Fig 2. Comparative approach of two Nations

Moreover, the interpretation of how such legal frameworks affect diplomatic behaviour and cooperation is conducted with the help of a qualitative analytical approach. The research also relies on the available literature on cyber diplomacy that underscores the importance of norms, multilateral interactions and legal harmonisation in developing international cyber policies.

4. Experiments and Results

4.1 Legal Frameworks and Institutional Structures

The discussion shows that the cyber legal framework in India is incomplete, comprising various laws and bodies that deal with various issues of cybersecurity and data regulation. Although this enables flexibility, it proves to be difficult in terms of coordination and enforcement. The quick digitization of India has exposed it to more cyber-attacks, causing it to need more legal consolidation.

However, it is comparatively less in the case of Malaysia's framework, which shows more law coherence, with structured legislation that covers cybercrime, communications, and data protection. Its legal system is, however, mostly domestically based and does not have effective mechanisms of international cooperation.[5]

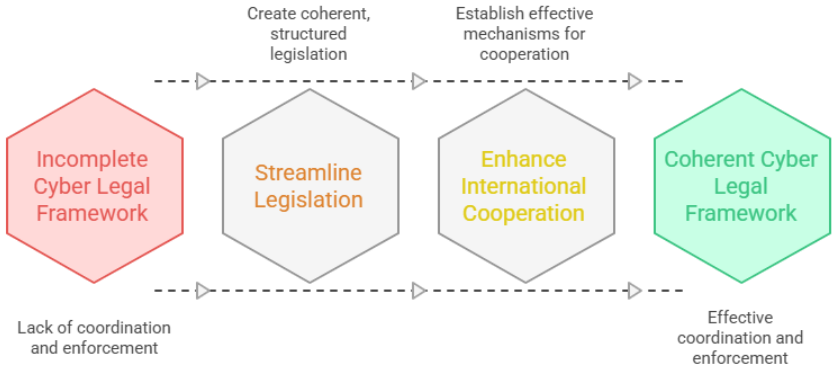

Fig 3. Strengthening Cyber Legal Frameworks

4.2 Data Governance Divergence

The second important aspect is the difference in the data governance strategies:

India is focusing on the sovereignty of the data and regulatory control, which relates to its overall geopolitical approach. Malaysia is more of a compliance model, which lays emphasis on the enforcement of regulations within the national borders. Such a divergence puts obstacles in the flow of data across borders and restricts the possibility of harmonious digital trade and collaboration.[6]

4.3 Cyber Diplomacy Engagement

India has become an active player in global cyber diplomacy, promoting multilateralism and norm-building at the international level. It aims at balancing openness and sovereignty, and places itself at the forefront of the Global South in digital governance. Though active in both ASEAN and regional creativities, Malaysia is more regionalised regarding cyber diplomacy, with its importance on capacity building and cooperative security frameworks.[1] [3]

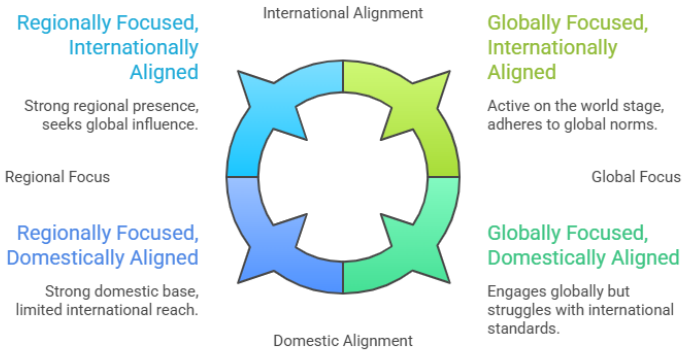

Fig 4. Cyber Diplomacy Engagement

5. Discussions

The outcomes indicate that the legal, political, and technological factors influence the development of cyber diplomacy in the Indo-Pacific in a complicated way. Perhaps the greatest difficulty is that global cyber governance is informal, with states not depending on binding legal systems but adhering to informal norms.

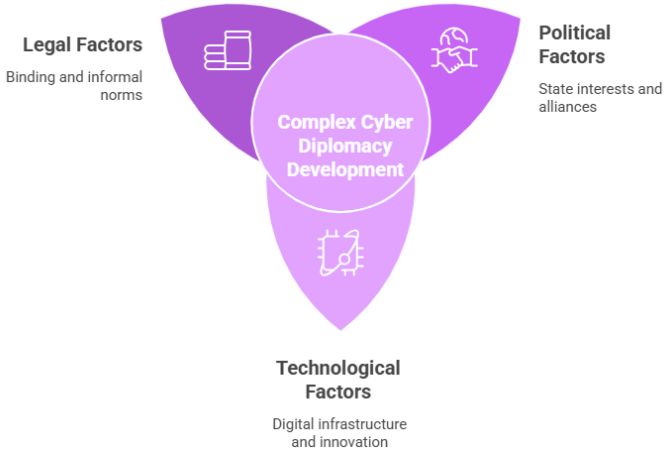

Fig 5. Factors Shaping Cyber Diplomacy in the Indo-Pacific

In the case of India, the main issue is that the nation is faced with the problem of legal fragmentation, which negatively impacts its capability to establish coherent cyber diplomacy strategies. Although it is an active participant in international forums, the lack of a common legal framework does not allow the country to operate effectively in cross-border cooperation. On the other hand, Malaysia is struggling with the problem of international alignment. Its domestic legislation is quite organized although it is not integrated with international standards, limiting its power to impact the development of international cyber standards.[7]

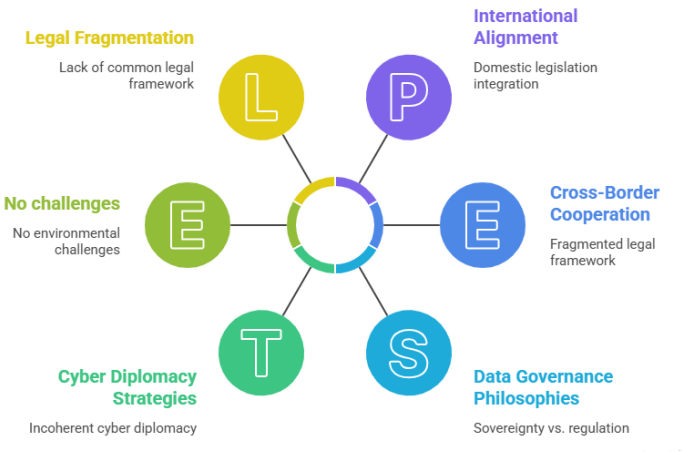

Fig 6. Challenges of Cyber Diplomacy in two nations

The second matter of concern is the difference in data governance philosophies. The focus on sovereignty and control in India, as opposed to the regulatory approach by the Malaysians, poses a problem in bilateral cooperation.[8] This point of disagreement indicates the wider debates in the world on data localisation, privacy, and digital trade. Moreover, regional frameworks, especially ASEAN, are important in the study as they help in cyber diplomacy.[9] The location of the Malaysian country in ASEAN gives India the chance to participate in the systems of cyber governance in the region even more deeply.[10]

6. Conclusions

This research dealt with the increasing law incompatibility and regulation gaps in cyber diplomacy and international data flows between India and Malaysia in the fast-changing Digital Indo-Pacific. It discussed the impediments to smooth digital interaction through varying data protection strategies, readiness to cybersecurity, sovereignty standards, and global collaboration in cybersecurity. Its rationale was the growing strategic necessity to have trusted digital relationships, geographical stability, and digital interoperability between cyber laws to help in trade, digital infrastructural support, and new technologies. The study took a comparative policy analysis of legal policies based on texts of statutes, regulatory frameworks and bilateral-multilateral digital cooperation tools. Substantive laws that were analyzed using the doctrinal approach included India's data protection framework and Malaysia's Personal Data Protection Act (PDPA), cybersecurity laws and regulations and cybercrime laws and regulations. An analytical-normative technique measured policy convergence in broader Indo-Pacific governance frameworks such as ASEAN norms, United Nations cyber procedures and local security discourses. To recognize areas of compliance and non-compliance, qualitative document analysis was used on government reports, strategic doctrines, and international law sources.

The complementary interests in secure and rules-based digital cooperation are well-suited in India and Malaysia, whereas the two countries have vastly different regulatory frameworks and institutional preparedness's.

Data governance: Malaysia's PDPA is broad but covers a smaller area, whereas India's model focuses on data sovereignty and introduces concerns about inter-operability.

Cybersecurity: The CSA of Malaysia is centralized in incident response frameworks, and the model of the CERT in India is more decentralized, resulting in uneven application to cross-border situations.

Cybercrime: India is not a signatory to the Budapest Convention and Malaysia draws on local statutes, which means that there is a lack of harmonization of transnational cyber investigation.

Diplomatic connection: These two countries are part of the mechanisms of ASEAN-India but do not have a bilateral treaty on cyber and data regulation, which restricts organized collaboration.

Convergence as a strategy: Despite the divergences, the Indo-Pacific scenario offers great prospects of convergence capacity building, critical infrastructure security, digital supply chain security, AI governance, and regional cyber norms.

The researchers determine that the partnership bilateral structures may play a significant role in improving trust, predictability, of legal predictability and compatibility of operations in the Digital Indo-Pacific.

The research is mainly a work of statutory and policy analysis and is not accompanied by any empirical evaluation of such variables as industry compliance behaviour, data on cyber incidents or interviews with stakeholders, which would enrich the practical consideration. Areas that were swiftly undergoing developments like AI regulation, quantum resilient cybersecurity, and cross-border data transfer technologies were not exhausted as far as the scope was constrained. The research in the future would entail empirical case studies of digital trade flows between India and Malaysia, collaborations in CERT, and collaborations in digital public infrastructure.

The study of comparative research needs to incorporate ASEAN digital frameworks, QUAD cyber principles and Indo-Pacific data corridors to determine how India and Malaysia are placed in broader partnerships. The possible models of bilateral cyber diplomacy pact, such as the mutual recognition of data adequacy, coordinated cybercrime processes, and collaborative digital capacity-building efforts, have yet to be studied further. The longitudinal study would determine how the changing geopolitical conditions, such as technological competition and the fragmentation of the supply chain, would affect cyber diplomacy in the area.

References

1. Amel Attatfa, Karen Renaud and Stefano De Paoli, “Cyber Diplomacy: A systematic Literature Review,” *Procedia Computer Science*, vol. 176, pp. 60-69, 2020. 10.1016/j.procs.2020.08.007
2. Chin Y-C, Zhao J., “Governing Cross-Border Data Flows: International Trade Agreements and Their Limits,” *Laws*, vol. 11, no. 4, pp. 1-22, 2022. https://doi.org/10.3390/laws11040063
3. Ali, A.S., Zaaba, Z.F., Singh, M.M. *et al.* Advancing cybersecurity in ASEAN: current trends, emerging challenges, and opportunities for enhanced resilience. *Int. J. Inf. Secur.* 24, 200 (2025). https://doi.org/10.1007/s10207-025-01111-2
4. Yudhistira Nugraha and Andrew Martin, “Cybersecurity service level agreements: understanding government data confidentiality requirements,” *Journal of Cybersecurity*, vol. 8, no. 1, pp 1-19, 2022. https://doi.org/10.1093/cybsec/tyac004
5. J. S. Nye, “Deterrence and dissuasion in cyberspace,” *International Security*, vol. 41, no. 3, pp. 44–71, 2017. https://doi.org/10.1162/ISEC_a_00266

6. Xiaowu Gao, Xiaoning Chen, Yiquan Fang and Hua Cheng, “A Data Governance Model Based on Multi-Agents System,” IEEE 7th International Conference on Communications, Information Systems and Computer Engineering, 2025.
7. Yunusa Adamu Bena, Roliana Ibrahim, Jamilah Mahmood and Matthew O. Ayemowa, “Big Data Governance Challenges Arising from Data Generated by Intelligent Systems Technologies: A Systematic Literature Review,” *IEEE Access* vol. 13, pp. 12859-12888, 2025. 10.1109/ACCESS.2025.3528941
8. Didier Wernli, “Fostering interdisciplinary collaboration in computational diplomacy: A multi-layered network approach to improve our understanding of institutional complexity and effective governance design,” *Journal of Computational Science*, vol. 72, pp. 1-12, 2023. https://doi.org/10.1016/j.jocs.2023.102096
9. M. Ferracane and E. van der Marel, “Do data policies inhibit trade in services?” *The World Economy*, vol. 44, no. 8, pp. 2210–2233, 2021. https://doi.org/10.1111/twec.13067
10. Naughton, J. “The evolution of the Internet: from military experiment to General Purpose Technology,” *Journal of Cyber Policy*, vol. 1, no. 1, pp. 5–28, 2016. https://doi.org/10.1080/23738871.2016.1157619