Respon Kebijakan Keamanan Siber India Terhadap Ancaman Siber Tiongkok di Kawasan Indo – Pasifik Tahun 2020-2025

Ruth Michelle Christian

ABSTRAK

Penelitian ini bertujuan untuk menganalisis respon kebijakan keamanan siber India terhadap meningkatnya ancaman siber yang dikaitkan dengan Tiongkok di kawasan Indo-Pasifik pada periode 2020–2025. Penelitian ini menggunakan metode kualitatif dengan pendekatan interpretatif dan studi kepustakaan. Perspektif Neorealisme digunakan untuk menjelaskan respon India berdasarkan kepentingan keamanan nasional, prinsip *self-help*, dan *balancing*, sedangkan konsep *techno-nationalism* digunakan untuk menjelaskan upaya kemandirian teknologi dan kedaulatan *Digital India*. Hasil penelitian menunjukkan bahwa meningkatnya digitalisasi dan ketergantungan India terhadap infrastruktur digital menjadikan keamanan siber sebagai bagian penting dari keamanan nasional. Persepsi terhadap ancaman siber yang dikaitkan dengan Tiongkok mendorong India memperkuat kapasitas keamanan siber domestik melalui penguatan institusi, perlindungan infrastruktur kritis, pengembangan sumber daya manusia, serta peningkatan ketahanan digital. India juga mengembangkan kemandirian teknologi melalui pembangunan teknologi domestik, penguatan industri strategis, pengelolaan data, dan pembatasan terhadap teknologi asing yang dianggap berisiko. Selain itu, India memperluas kerja sama keamanan siber dengan Amerika Serikat, Jepang, Australia, dan negara lainnya melalui pertukaran informasi, pembangunan kapasitas, serta mekanisme Quad dan forum multilateral. Dengan demikian, respon India bersifat multidimensional dan diarahkan untuk mengurangi kerentanan, memperkuat kapabilitas nasional, serta mempertahankan strategic autonomy di Indo-Pasifik.

Kata kunci: Keamanan Siber, India, Tiongkok, Neorealisme, *Techno-nationalism*

India's Cybersecurity Policy Response To Cyber Threats From China In The Indo-Pasific Region, 2020-2025

Ruth Michelle Christian

ABSTRACT

This study aims to analyze India's cybersecurity policy responses to increasing cyber threats attributed to Tiongkok *in the Indo-Pacific region during the 2020–2025 period. This research employs a qualitative method with an interpretive approach and literature review. Neorealism is used to explain India's responses based on national security interests, the principle of self-help, and balancing, while the concept of techno-nationalism is applied to examine India's efforts to strengthen technological self-reliance and digital sovereignty. The findings show that India's rapid digitalization and growing dependence on digital infrastructure have made cybersecurity an important component of national security. Perceptions of cyber threats attributed to* Tiongkok *have encouraged India to strengthen its domestic cybersecurity capabilities through institutional development, critical infrastructure protection, human resource development, and enhanced digital resilience. India has also pursued technological self-reliance through domestic technology development, strengthening strategic industries, data governance, and restrictions on foreign technologies considered risky. In addition, India has expanded cybersecurity cooperation with the United States, Japan, Australia, and other partners through information sharing, capacity building, the Quad, and multilateral forums. Therefore, India's response is multidimensional and aimed at reducing vulnerabilities, strengthening national capabilities, and maintaining strategic autonomy in the Indo-Pacific*

Keywords: *Cybersecurity, India, Tiongkok, Neorealism, Techno-nationalism*