BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan hasil penelitian mengenai respon kebijakan keamanan siber India terhadap ancaman siber Tiongkok di kawasan Indo-Pasifik tahun 2020–2025, dapat disimpulkan bahwa meningkatnya ancaman siber yang dikaitkan dengan Tiongkok menjadi salah satu faktor yang memengaruhi perkembangan kebijakan keamanan siber India. Perkembangan digitalisasi India yang semakin pesat telah meningkatkan ketergantungan terhadap teknologi digital, infrastruktur jaringan, sistem pembayaran, layanan pemerintahan, serta berbagai infrastruktur strategis. Kondisi tersebut pada saat yang sama meningkatkan potensi kerentanan terhadap ancaman siber. Dalam hubungan India–Tiongkok yang semakin kompetitif, khususnya sejak tahun 2020, berbagai aktivitas siber yang dikaitkan dengan aktor berbasis Tiongkok turut memperkuat perhatian India terhadap keamanan infrastruktur digital dan teknologi nasional.

Respon kebijakan keamanan siber India terhadap kondisi tersebut dilakukan melalui tiga bentuk utama. Pertama, India memperkuat kapasitas keamanan siber domestik melalui pembangunan dan penguatan kelembagaan, regulasi, perlindungan infrastruktur informasi kritis, peningkatan sumber daya manusia, latihan keamanan siber, serta peningkatan koordinasi antar lembaga. Penguatan CERT-In, NCIIPC, I4C, *Defence Cyber Agency*, NSCS, serta berbagai mekanisme koordinasi keamanan siber menunjukkan upaya India untuk meningkatkan kemampuan nasional dalam mendeteksi, mencegah, dan menangani ancaman siber.

Kedua, India merespon ancaman dan kerentanan teknologi melalui penguatan kemandirian dan kedaulatan teknologi. Kebijakan seperti *Digital India*, Make in India, *Atmanirbhar Bharat*, Production Linked Incentive, pengembangan semikonduktor, 5G domestik, *Cloud* nasional, pengelolaan data, serta kebijakan trusted telecom menunjukkan upaya India untuk mengurangi ketergantungan terhadap teknologi asing yang dianggap memiliki risiko terhadap keamanan

nasional. Pembatasan terhadap sejumlah aplikasi dan teknologi Tiongkok juga menunjukkan bahwa pertimbangan keamanan nasional semakin menjadi bagian penting dalam menentukan penggunaan teknologi asing.

Ketiga, India memperkuat respon melalui kerja sama keamanan siber dengan negara-negara mitra, khususnya di kawasan Indo-Pasifik. Kerja sama dengan Amerika Serikat, Jepang, Australia, serta keterlibatan India dalam Quad dilakukan melalui pertukaran informasi ancaman, pembangunan kapasitas, perlindungan infrastruktur kritis, keamanan rantai pasok, dan pengembangan kemampuan keamanan siber. Kerja sama tersebut menjadi pelengkap bagi kemampuan domestik India dalam menghadapi ancaman siber yang bersifat lintas batas.

Jika dianalisis menggunakan teori Neorealisme, ketiga bentuk respon tersebut menunjukkan upaya India untuk mempertahankan keamanan nasional dalam lingkungan internasional yang bersifat anarkis. Penguatan kapasitas domestik menunjukkan prinsip *self-help*, yaitu upaya negara untuk meningkatkan kemampuan sendiri dalam menghadapi ancaman eksternal. Sementara itu, peningkatan kerja sama dengan negara-negara mitra menunjukkan upaya India untuk memperkuat posisinya dalam lingkungan keamanan Indo-Pasifik yang semakin kompetitif. Dengan demikian, India tidak hanya mengandalkan kemampuan internal, tetapi juga memanfaatkan kerja sama eksternal untuk memperkuat keamanan nasional.

Sementara itu, konsep *techno-nationalism* menjelaskan karakter respon India dalam bidang teknologi. India menghubungkan penguasaan teknologi dengan keamanan nasional, kemandirian strategis, dan kepentingan nasional. Pengembangan teknologi domestik, pengelolaan data, pembangunan infrastruktur digital nasional, penguatan industri semikonduktor dan telekomunikasi, serta pembatasan terhadap teknologi asing yang dianggap berisiko menunjukkan adanya upaya India untuk mengurangi ketergantungan teknologi dan mempertahankan kontrol terhadap infrastruktur digital strategis.

Dengan demikian, respon kebijakan keamanan siber India terhadap meningkatnya ancaman siber Tiongkok pada tahun 2020–2025 merupakan respon yang bersifat multidimensional, yaitu melalui penguatan kapasitas keamanan siber

domestik, penguatan kemandirian dan kedaulatan teknologi, serta peningkatan kerja sama keamanan siber dengan negara-negara mitra di kawasan Indo-Pasifik. Ketiga bentuk respon tersebut saling melengkapi dalam upaya India mengurangi kerentanan, meningkatkan kemampuan nasional, menjaga kepentingan keamanan, dan mempertahankan *strategic autonomy.*

Berdasarkan keseluruhan hasil penelitian, dapat dilihat bahwa keamanan siber bagi India telah berkembang menjadi bagian dari kepentingan keamanan nasional. India tidak hanya berupaya melindungi sistem dan infrastruktur digital dari ancaman eksternal, tetapi juga berupaya membangun kemampuan teknologi domestik dan memperkuat hubungan dengan negara-negara mitra. Hal tersebut menunjukkan bahwa respon India terhadap ancaman siber Tiongkok merupakan bagian dari upaya yang lebih luas untuk mempertahankan keamanan nasional dan posisi strategis India di kawasan Indo-Pasifik

6.2 Saran

Penelitian ini memiliki keterbatasan dalam memperoleh data mengenai aktivitas siber yang secara langsung dapat diatribusikan kepada Tiongkok karena sebagian informasi mengenai operasi siber bersifat terbatas dan tidak seluruhnya dapat diakses oleh publik. Oleh karena itu, penelitian ini lebih berfokus pada kebijakan dan respon India yang dapat diamati melalui dokumen pemerintah, laporan, serta sumber-sumber yang tersedia. Bagi peneliti selanjutnya diharapkan dapat mengembangkan kajian dengan menggunakan data yang lebih luas dan mendalam mengenai perkembangan ancaman siber serta hubungan antara aktivitas siber dengan perubahan kebijakan keamanan India. Selain itu, penelitian selanjutnya dapat mengkaji perkembangan respon kebijakan India setelah tahun 2025, khususnya dalam menghadapi perkembangan teknologi seperti *artificial intelligence*, 5G dan 6G, semikonduktor, *Cloud computing*, serta teknologi strategis lainnya. Penelitian selanjutnya juga dapat memperluas kajian dengan membandingkan respon keamanan siber India dengan negara-negara lain di kawasan Indo-Pasifik, sehingga dapat memberikan pemahaman yang lebih komprehensif mengenai bagaimana negara-negara di kawasan merespon ancaman siber dan persaingan teknologi. Dengan demikian, penelitian mengenai keamanan siber India diharapkan dapat terus dikembangkan untuk melihat hubungan antara

keamanan nasional, perkembangan teknologi, persaingan strategis India–Tiongkok, serta dinamika keamanan di kawasan Indo-Pasifik.