

ABSTRAK

Isu keamanan digital Huawei merupakan salah satu polemik penting dalam pengelolaan infrastruktur telekomunikasi global, terutama pada era kompetisi geopolitik teknologi antara Amerika Serikat dan Tiongkok. Bagi Indonesia, polemik ini tidak hanya berkaitan dengan pemilihan vendor teknologi telekomunikasi, tetapi menyangkut bagaimana negara menjaga kedaulatan digital di tengah ketergantungan pada teknologi asing dan kebutuhan mendesak mempercepat pembangunan jaringan 5G dan infrastruktur digital strategis. Penelitian ini bertujuan untuk memahami bagaimana institusi domestik membentuk respons Indonesia terhadap isu keamanan digital Huawei pada periode 2019–2024. Penelitian ini terdiri atas 4 Bab dengan 16.806 kata dan disusun dengan pendekatan instrumental single case study, dimana isu keamanan digital Huawei direpresentasikan dari persoalan yang lebih luas mengenai ketergantungan teknologi di tengah interdependensi global. Pengumpulan data dilakukan melalui analisis komprehensif terhadap dokumen pemerintah, publikasi sektor telekomunikasi, dan arsip pemberitaan yang menggambarkan perkembangan isu Huawei di ranah publik. Temuan menunjukkan bahwa tata kelola digital Indonesia dijalankan melalui struktur yang terdistribusi di antara berbagai lembaga dengan mandat berbeda. Kominfo, BSSN, BRIN, DPR, operator jaringan, asosiasi industri, dan Huawei membentuk konstelasi aktor yang saling mempengaruhi tanpa adanya pusat otoritas tunggal. Pola interaksi yang berlapis ini menciptakan ruang kompromi kebijakan, di mana kepentingan teknis dan kepentingan keamanan dinegosiasikan untuk menghasilkan respons yang adaptif, yaitu tidak menolak masuknya teknologi asing, tetapi juga tidak menerima tanpa syarat. Aktor teknis seperti Kominfo, operator, dan BRIN memiliki pengaruh implementatif yang dominan melalui sertifikasi perangkat, penilaian risiko teknis, dan kolaborasi riset. Sementara itu, DPR dan BSSN mendorong kewaspadaan strategis melalui wacana kedaulatan digital dan ancaman keamanan siber. Interaksi antara trust teknis dan persepsi risiko menghasilkan serangkaian mekanisme mitigasi, termasuk kebijakan multi-vendor, perluasan audit keamanan, diversifikasi teknologi, penguatan kapasitas SDM, serta perluasan standar perlindungan data. Temuan ini

menunjukkan bahwa Indonesia tidak menempuh jalur pelarangan vendor seperti Amerika Serikat dan Australia, maupun pendekatan liberal tanpa pengawasan seperti sebagian negara berkembang. Sebaliknya, Indonesia mengembangkan bentuk adaptive digital sovereignty, yaitu model kedaulatan digital yang dibangun melalui regulasi dan pengawasan negara terhadap penggunaan teknologi asing, bukan melalui substitusi teknologi atau proteksionisme. Model ini membuka ruang teoritis baru dalam kajian hubungan internasional dan kebijakan teknologi, terutama dalam memahami bagaimana negara berkembang menavigasi interdependensi global di tengah rivalitas kekuatan besar.

Kata kunci: Huawei, keamanan digital, kedaulatan digital, adaptive digital sovereignty, insitusi domestik, Neo Classical Realism.

ABSTRACT

Huawei's digital security issue has become one of the most significant controversies in the governance of global telecommunications infrastructure, particularly amid the intensifying geopolitical competition between the United States and China in the technology sector. For Indonesia, this controversy extends beyond the question of selecting a telecommunications vendor and instead raises a broader challenge concerning how the state safeguards digital sovereignty while remaining dependent on foreign technology and simultaneously facing the urgent need to accelerate the development of fifth generation networks and other strategic digital infrastructure. This study aims to examine how domestic institutions have shaped Indonesia's response to Huawei's digital security issue during the period from 2019 to 2024. The research is structured into four chapters with a total length of 16,806 words and employs an instrumental single case study approach, in which Huawei's digital security issue is treated as a representative case of the broader problem of technological dependence under conditions of global interdependence. Data collection relies on a comprehensive analysis of government documents, telecommunications sector publications, and media archives that capture the public evolution of the Huawei issue in Indonesia. The findings demonstrate that Indonesia's digital governance operates through a distributed institutional structure composed of multiple actors with distinct mandates. The Ministry of Communication and Information Technology, the National Cyber and Crypto Agency, the National Research and Innovation Agency, the House of Representatives, network operators, industry associations, and Huawei itself form a constellation of actors that interact without a single central authority. This layered pattern of interaction creates space for policy compromise, in which technical considerations and security concerns are continuously negotiated to produce an adaptive response that neither rejects foreign technology outright nor accepts it without conditions. Technical actors such as the Ministry of Communication and Information Technology, network operators, and the National Research and Innovation Agency exercise dominant influence at the level of implementation through device certification, technical risk assessment, and research collaboration.

At the same time, the House of Representatives and the National Cyber and Crypto Agency promote strategic caution through discourse on digital sovereignty and cyber security threats. The interaction between technical trust and risk perception generates a set of mitigation mechanisms, including multi vendor policies, expanded security audits, technological diversification, capacity building for domestic human resources, and the strengthening of data protection standards. These findings indicate that Indonesia has not pursued vendor exclusion strategies as adopted by countries such as the United States and Australia, nor has it followed a liberal approach with minimal oversight as seen in some developing countries. Instead, Indonesia has developed a form of adaptive digital sovereignty, defined as a model of digital sovereignty constructed through state regulation and oversight of foreign technology use rather than through technological substitution or protectionism. This model opens new theoretical space within international relations and technology policy studies, particularly for understanding how developing countries navigate global interdependence amid intensifying great power rivalry.

Keywords: Huawei, digital security, digital sovereignty, adaptive digital sovereignty, domestic institution, Neo Classical Realism.