ABSTRAK

Penelitian ini membahas strategi keamanan siber Indonesia dalam melindungi sistem teknologi informasi (*IT)* energi listrik melalui kerja sama internasional pada tahun 2018-2023. Latar belakang penelitian ini didasarkan pada meningkatnya ketergantungan sektor ketenagalistrikan terhadap sistem IT pra operasional yang berperan penting dalam proses perencanaan, pengolahan data, pemantauan jaringan, dan pengambilan keputusan strategis. Ketergantungan tersebut diiringi dengan meningkatnya ancaman siber yang bersifat lintas batas, non-militer, dan berpotensi menimbulkan dampak sistemik terhadap infrastruktur kritis nasional. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka dan analisis dokumen terhadap kebijakan nasional, laporan institusi terkait, serta bentuk kerja sama internasional Indonesia di bidang keamanan siber pada periode 2018–2023. Hasil penelitian menunjukkan bahwa Indonesia memandang ancaman siber terhadap sistem IT pra operasional energi listrik sebagai bagian dari ancaman keamanan non-tradisional yang memerlukan pendekatan kebijakan komprehensif. Respons Indonesia diwujudkan melalui penguatan tata kelola keamanan siber nasional serta keterlibatan aktif dalam kerja sama bilateral dan multilateral guna meningkatkan kapasitas, pertukaran informasi, dan koordinasi penanganan insiden siber. Dengan demikian, perlindungan sistem IT pra operasional energi listrik merupakan hasil sinergi antara kebijakan domestik dan kerja sama internasional dalam menghadapi dinamika ancaman siber global.

KATA KUNCI

Keamanan Siber; Sistem IT Pra Operasional; Energi Listrik; Infrastruktur Kritis; Keamanan Non-Tradisional; Kerja Sama Internasional

ABSTRACT

This study examines Indonesia's cybersecurity strategy for protecting its electrical energy information technology (IT) systems through international cooperation in 2018–2023. The background of this study is based on the increasing dependence of the electricity sector on pre-operational IT systems, which play a crucial role in planning, data processing, network monitoring, and strategic decision-making. This dependence is accompanied by increasing cyber threats that are cross-border, non-military, and have the potential to cause systemic impacts on national critical infrastructure. This study uses a qualitative approach with a literature review and document analysis of national policies, reports from related institutions, and forms of Indonesian international cooperation in the field of cybersecurity in the 2018–2023 period. The results show that Indonesia views cyber threats to pre-operational IT systems for electrical energy as part of a non-traditional security threat that requires a comprehensive policy approach. Indonesia's response is realized through strengthening national cybersecurity governance and active involvement in bilateral and multilateral cooperation to increase capacity, information exchange, and coordination in handling cyber incidents. Thus, protecting pre-operational IT systems for electrical energy is the result of synergy between domestic policies and international cooperation in addressing the dynamics of global cyber threats.

KEYWORDS

Cybersecurity; Pre-Operational IT Systems; Electrical Energy; Critical Infrastructure; Non-Traditional Security; International Cooperation