Pengembangan Sharing Cyber Threat Intelligence untuk Penguatan Keamanan Siber Nasional: Studi Pendekatan Collaborative Governance pada Lingkungan Pemerintah = Development of Sharing Cyber Threat Intelligence for Strengthening National Cybersecurity: A Study of the Collaborative Governance Approach in Government Environments

Sigiro, Farlin Hottua, author

Abstrak

Lanskap ancaman siber global dan nasional telah mengalami perkembangan signifikan dalam beberapa tahun terakhir, ditandai dengan serangan yang semakin canggih, kompleks, dan persisten, yang memengaruhi berbagai sektor strategis. Pemerintah Indonesia, melalui Badan Siber dan Sandi Negara (BSSN), telah merespons dengan membentuk lembaga keamanan siber, yaitu Computer Security Incident Response Team (CSIRT), untuk memperkuat pertahanan ruang digital. Namun, pendekatan reaktif yang masih dominan dalam pemantauan dan respons serangan terbukti kurang efektif dalam menghadapi dinamika ancaman yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis tren ancaman siber di tingkat nasional dan global serta mengidentifikasi strategi yang efektif dalam penanganannya, khususnya melalui kolaborasi antar lembaga keamanan siber. Dengan menggunakan pendekatan kualitatif, data diperoleh melalui wawancara mendalam, tinjauan pustaka, dan observasi langsung. Konsep-konsep seperti teori ancaman, Intelijen Ancaman Siber (Cyber Threat Intelligence/CTI), dan koordinasi lintas lembaga menjadi landasan analisis untuk memahami pola ancaman dan potensi kolaborasi. Hasil penelitian menunjukkan bahwa peningkatan ancaman siber membutuhkan kerja sama lintas lembaga dalam berbagi intelijen ancaman untuk menghadapi ancaman bersama. Sebagai langkah strategis, penelitian ini mengusulkan pembentukan model berbagi informasi intelijen ancaman yang kolaboratif serta tata kelola lintas lembaga yang terintegrasi guna memperkuat operasi keamanan siber nasional sekaligus meningkatkan ketahanan siber nasional.

.....The global and national cyber threat landscape has significantly evolved in recent years, marked by increasingly sophisticated, complex, and persistent attacks that impact various strategic sectors. The Indonesian government, through the National Cyber and Crypto Agency (BSSN), has responded by establishing a cybersecurity institution, namely the Computer Security Incident Response Team (CSIRT), to strengthen digital space defences. However, the dominant reactive approach in monitoring and responding to cyber incidents has proven inadequate in addressing the dynamic and complex nature of emerging threats. This study aims to analyze cyber threat trends at both national and global levels and to identify effective strategies for addressing these threats, particularly through collaboration among cybersecurity institutions. Using a qualitative approach, data were collected through in-depth interviews, literature reviews, and direct observation. Concepts such as threat theory, Cyber Threat Intelligence (CTI), and interagency coordination serve as the analytical foundation to understand threat patterns and potential collaboration mechanisms. The findings indicate that the increasing cyber threats necessitate interagency cooperation in sharing threat intelligence to tackle common challenges. As a strategic measure, this study proposes the establishment of a collaborative threat intelligence-sharing model and integrated interagency governance to enhance national cybersecurity operations and bolster national cyber resilience.