ABSTRACT

This research analyzes the implementation of the Indonesia–Australia Cyber Cooperation as outlined in the 2018 Memorandum of Understanding (MoU), with a specific focus on the area of capacity building and strengthening institutional connections during the period of 2023–2024. The study employs a qualitative descriptive method, using primary data obtained through interviews with relevant officials from BSSN (Indonesia) and supported by secondary data such as official documents, literature studies, and institutional reports. The findings show that the Indonesia–Australia cyber cooperation has been actively realized through a number of strategic capacity-building programs, including the SANS Institute cybersecurity training, the CSIRO Data for Development (D4D) Fellowship, the Advanced Open Source Intelligence (OSINT) course, and the Practitioners Exchange in Disarmament and Non-Proliferation Policy short course. These programs contributed significantly to enhancing Indonesia's cybersecurity competencies, fostering inter-agency collaboration, and aligning domestic capabilities with international standards. Furthermore, the cooperation reflects Australia's strategic interest in promoting cyber stability in the Indo-Pacific and Indonesia's efforts to strengthen its human capital and national cyber resilience. However, challenges were identified in areas such as inter-agency coordination, knowledge application, and long-term sustainability. The study concludes that while the cooperation has produced measurable outcomes, its sustainability depends on stronger institutional integration, domestic investment, and a jointly developed long-term roadmap. This research contributes to the discourse on cyber diplomacy and provides practical insights for enhancing bilateral cooperation frameworks in the digital security sector.

Keywords: Cybersecurity, Capacity Building, Bilateral Cooperation, Cyber Diplomacy.

ABSTRAK

Penelitian ini menganalisis implementasi Kerja Sama Siber Indonesia–Australia sebagaimana tertuang dalam Nota Kesepahaman (MoU) 2018, dengan fokus khusus pada bidang peningkatan kapasitas dan penguatan koneksi kelembagaan selama periode 2023–2024. Penelitian ini menggunakan metode deskriptif kualitatif, dengan menggunakan data primer yang diperoleh melalui wawancara dengan pejabat terkait dari BSSN (Indonesia) dan didukung oleh data sekunder seperti dokumen resmi, studi pustaka, dan laporan kelembagaan. Temuan menunjukkan bahwa kerja sama siber Indonesia–Australia telah direalisasikan secara aktif melalui sejumlah program peningkatan kapasitas strategis, termasuk pelatihan keamanan siber SANS Institute, Beasiswa Data for Development (D4D) CSIRO, kursus Advanced Open Source Intelligence (OSINT), dan kursus singkat Practitioners Exchange in Disarmament and Non-Proliferation Policy. Program-program ini berkontribusi signifikan terhadap peningkatan kompetensi keamanan siber Indonesia, mendorong kolaborasi antarlembaga, dan menyelaraskan kapabilitas domestik dengan standar internasional. Lebih lanjut, kerja sama ini mencerminkan kepentingan strategis Australia dalam mendorong stabilitas siber di Indo-Pasifik dan upaya Indonesia untuk memperkuat sumber daya manusia dan ketahanan siber nasional. Namun, tantangan yang teridentifikasi meliputi koordinasi antarlembaga, penerapan pengetahuan, dan keberlanjutan jangka panjang. Studi ini menyimpulkan bahwa meskipun kerja sama ini telah menghasilkan hasil yang terukur, keberlanjutannya bergantung pada integrasi kelembagaan yang lebih kuat, investasi domestik, dan peta jalan jangka panjang yang disusun bersama. Penelitian ini berkontribusi pada wacana diplomasi siber dan memberikan wawasan praktis untuk meningkatkan kerangka kerja sama bilateral di sektor keamanan digital.

Kata Kunci: Keamanan Siber, Pengembangan Kapasitas, Kerja Sama Bilateral, Diplomasi Siber.