CHAPTER VI
CONCLUSION AND SUGGESTIONS

6.1 Conclusion

This research has examined the implementation of Indonesia–Australia cyber cooperation under the 2018 Memorandum of Understanding (MoU), with a focus on capacity building and strengthening connections during the 2023–2024 period. Through qualitative analysis and interviews with key institutional actors, particularly from BSSN (Indonesia) and DFAT (Australia), this study concludes that while the partnership has yielded tangible progress in building cyber capabilities, several institutional and structural challenges remain.

The cooperation between Indonesia and Australia has evolved from initial diplomatic dialogue into actionable programs such as the SANS Institute training**,** CSIRO's D4D Fellowship**,** the Open Source Intelligence Course**,** and the Short Course in Disarmament and Non-Proliferation Policy. These initiatives have directly contributed to enhancing technical competencies, establishing cross-agency connections, and creating a pipeline of trained cybersecurity personnel. Programs funded under DFAT's Cyber and Critical Tech Cooperation Program have enabled Indonesian participants to gain international certifications, implement strategic knowledge transfer mechanisms, and integrate new methodologies such as OSINT, malware analysis, and NIST frameworks into their national practices.

However, the research also finds that implementation challenges persist. Indonesia continues to face limitations in skilled human resources, digital infrastructure, and policy coherence. Despite Presidential Regulations such as Perpres No. 28/2021**,** No. 47/2023, and the Personal Data Protection Law (UU PDP 2022), enforcement remains inconsistent, and inter-agency coordination often fragmented. Additionally, Indonesia’s heavy reliance on personnels that have more

skills than other and the reliance on Australia's technical and financial assistance highlights a critical gap in domestic cybersecurity self-sufficiency.

Nevertheless, these cooperation initiatives have successfully fostered strategic trust and mutual benefit. Australia's involvement is motivated by its interest in regional cyber stability and a secure Indo-Pacific, while Indonesia leverages the partnership to accelerate its cyber resilience goals. The partnership aligns with Indonesia's National Cybersecurity Strategy 2021–2025, emphasizing capacity building, knowledge sharing, and institutional reform.

In conclusion, while not without limitations, the 2023–2024 phase of the Indonesia–Australia cyber cooperation demonstrates meaningful progress in developing Indonesia's cybersecurity ecosystem. The partnership serves as a model for how middle powers can collaborate in the digital era, balancing geopolitical interests with normative goals. Moving forward, both countries must prioritize sustainability by embedding these programs into long-term policy frameworks, increasing domestic investment. Only through such sustained and reciprocal efforts can Indonesia transform from a cyber-capacity recipient into a regional cybersecurity leader.

6.2 Suggestions

6.2.1 Practical Suggestions

Based on the research findings, several practical recommendations are proposed to strengthen the implementation and sustainability of Indonesia–Australia cyber cooperation. First, BSSN is encouraged to institutionalize the outcomes of technical programs such as SANS training, CSIRO D4D fellowships, and OSINT courses into its internal capacity-building curriculum and functional training schemes. This will ensure that the skills and knowledge acquired by individual participants are embedded

within the agency's long-term development strategy and not lost through staff turnover.

Second, the Indonesian government should expand the reach of similar capacity-building initiatives to other critical infrastructure sectors, including finance, energy, transportation, and healthcare. A broader cross-sectoral approach would promote a whole-of-government cybersecurity strategy and enhance overall national resilience. Third, stronger coordination is needed between BSSN, the Ministry of Foreign Affairs, Bappenas, and sectoral institutions to align cooperation programs with national cybersecurity priorities and ensure that these initiatives are integrated into Indonesia's medium-term national development planning (RPJMN).

6.2.2 Academical Suggestions

The author recognizes the need for further research on the extent to which BSSN has successfully applied the knowledge and skills acquired through its cooperation with Australia in the field of cybersecurity. Such studies would benefit from more complex methodologies and the development of specific indicators to evaluate long-term institutional impact and practical application of training outcomes.

In addition, future research could explore the implementation of the other eight areas of cooperation listed in the 2018 Indonesia–Australia Cyber Cooperation MoU, which were not covered in this thesis. Given that the bilateral partnership is expected to continue and evolve, it would be valuable to examine whether there have been new innovations or shifts in program design and implementation over time. Researchers interested in this topic could also investigate how changes in political leadership, cybersecurity threats, or global trends—such as the rise of AI or data sovereignty issues—have influenced the trajectory of this bilateral cyber cooperation.