CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1. Conclusion

The collected data has been thoroughly analyzed and processed so that it can be linked to various theories and previous research for a more in-depth discussion. Following a discussion of the research findings, the following conclusions can be drawn:

5.1.1. The Implementation of Cyber Cooperation in DCA and MoU in Terms Of Cyber Defense Capacity Building From 2018 To 2022

Over the past four years, Indonesia and Australia have been cooperating in the field of cyber security (2018-2022). This partnership is part of the Defense Cooperation Arrangement (DCA) and the Memorandum of Understanding (MoU) on Cyber Cooperation on Emerging Technologies. This cooperation's has helped to increase cyber defense capacity building. This was accomplished through a variety of actions aimed at improving human competency in cyber. This partnership has included awareness raising, cyber security education, and cyber security professional training.

However, the implementation of cyber cooperation between Indonesia and Australia in the defense sector is still in the stage of establishing cyber defense capacity building. It is based on existing aspect indicators, and evidence shows that they work. However, there is no well-thought consideration of the relative allocation of resources. Especially Pushansiber's involvement in this collaboration. Support from the Ministry of Defense has been made regarding this cooperation. Although only in the aspect of education and training. But the aspects are functional and defined.

5.1.2. Ministry of Defense's Course of Action in Order to Improve Cyber Defense Capacity Building Through Cyber Cooperation

The course of actions of the Ministry of Defense in order to improve cyber defense capacity building have been implemented. This is realized by cyber cooperation with Australia through DCA. The Ministry of Defense's participation in forums such as ADMM, ADMM Plus and Asean Our Eyes also indicates this condition. Inter-agency partnership has also been carried out, especially with BSSN on cybersecurity issues. Although, the Ministry of Defense has been rather inactive in engaging or working with BSSN. Especially, in the implementation of cyber cooperation under the terms of the MoU of BSSN with DFAT.

However, the Ministry of Defense currently faces several obstacles and challenges in strengthening cyber defense capacity building. One of them is the absence of national cyber security regulations. Also, the level of maturity of cyber organizations in the defense sector, in this case Pushansiber, influences this. This is a challenge for the defense sector to be able to carry out defense diplomacy with Australia regarding cyber cooperation.

5.2. Recommendation

Based on the findings of this study, the researchers make recommendations that can be used as input and considerations in developing and implementing strategies and policies to achieve national interests, as well as triggers in the development of defense science studies, particularly defense diplomacy.

5.2.1. Theoritical Recommendation

This research is still far from comprehensive. It is only focus on cyber defense capacity building. Further follow-up research on other aspect of cyber security in the defense sector is required. As is known, the cyber security framework has five agendas: legal, organizational, technical,

capacity building, and cooperation. Of course, research is needed on other agendas so that more comprehensive recommendations can be produced for increasing cyber security in the defense sector.

5.2.2. Practical Recommendation

Researchers present several recommendations to the Ministry of Defense in an effort to strengthening cyber capacity building in the defense sector, namely:

a. The Ministry of Defense as the leading defense sector in Indonesia can submit a review of cyber cooperation contained in the Defense Cooperation Arrangement. This is intended so that cyber cooperation in DCA can be more extensive and comprehensive.
b. The Ministry of Defense can optimize cyber cooperation between Indonesia and Australia at this time, both based on DCA and MoU, by increasing its participation in its implementation.
c. Collaboration between the Ministry of Defense, Pushansiber, and BSSN to build the cyber defense coordination and communication forum. This aims to reduce sectoral ego among cyber security stakeholders in the country.
d. For Indonesia's defense diplomacy, especially related to cyber security issues, it will not be achieved if only the Ministry of Defense takes responsibility. Again, collaboration from all relevant stakeholders is required regarding this issue.