KERJASAMA *CYBER SECURITY* INDONESIA-AUSTRALIA DALAM MENGHADAPI ANCAMAN *CYBER TERRORISM* TAHUN 2018-2022

Oleh : Yesika Yulin Andari

ABSTRAK

Serangan *cyber terrorism* yang mengancam stabilitas keamanan, menunjukan bahwa suatu negara memiliki urgensi untuk mengembangkan aspek keamanan nasionalnya dari keamanan tradisional menjadi keamanan non-tradisional atau siber. Salah satu caranya yaitu suatu negara dapat menjalin kerjasama *cyber security* dengan negara lain. Indonesia dan Australia merupakan dua negara yang menjalin kerjasama cyber security dalam menghadapi ancaman cyber terrorism. Penelitian ini bertujuan untuk mengetahui bagaimana implementasi dan pengaruh dari adanya kerjasama tersebut. Meminjam konsep cyber security milik Barry Buzan yang kemudian dikembangkan oleh Lene Hansen dan Helen Nissenbaum, penelitian ini menemukan bahwa dalam implementasi kerjasama cyber security dibutuhkan tiga modalitas utama dalam cyber security yaitu *hypersecuritization, every day security practice*, dan *technification*. Penelitian ini dilakukan dengan menggunakan metode penelitian kualitatif yang menghasilkan data deskriptif. Penelitian ini menemukan bahwa kerjasama cyber security Indonesia-Australia telah menerapkan tiga modalitas cyber security dalam implementasi kerjasamanya. Modalitas pertama dalam kerjasama ini yaitu hypersecuritization yang dideskripsikan dengan urgensi-urgensi pembentukan kerjasama cyber security antara Indonesia dengan Australia. Kedua, everyday security practice dipresentasikan dengan pembentukan *Memorandum of Understanding on cyber cooperation* antara kedua negara. Modalitas ketiga, technification diimplementasikan dengan dibentuknya Program Cyber Policy Dialogue yang kemudian dikembangkan dalam program lainnya seperti *cyber boot camp, ASPI cyber policy workshop,* dan *cyber business connection*. Dengan suksesnya implementasi kerjasama ini, berpengaruh terhadap meningkatnya keamanan internal dan regional, serta peringkat komitmen kedua negara terhadap *cyber security* atau *global cybersecurity index* dalam *International Telecommunication Union*.

Kata Kunci : Kerjasama, *cyber security, cyber terrorism*, *hypersecuritization, every day security practice*, *technification*.

INDONESIA-AUSTRALIA CYBER SECURITY COOPERATION IN DEALING WITH CYBER TERRORIST THREATS IN 2018-2022

By : Yesika Yulin Andari

ABTRACT

Cyber terrorism attacks that threaten security stability, show that a country has an urgency to develop aspects of its national security from traditional security to non-traditional or cyber security. One of the ways is that a country can establish cyber security cooperation with other countries. Indonesia and Australia are two countries that have established cyber security cooperation in dealing with the threat of cyber terrorism. This study aims to find out how the implementation and influence of the existence of interlinked cyber security cooperation between Indonesia and Australia in dealing with the threat of cyber terrorism. Borrowing Barry Buzan's concept of cyber security which was later developed by Lene Hansen and Helen Nissenbaum, this study found that in the implementation of cyber security cooperation, three main modalities are needed in cyber security, namely hypersecurity, every day security practice, and technification. This research was conducted using qualitative research methods that produce descriptive data. This study found that the Indonesia-Australia cyber security cooperation has implemented three cyber security modalities in the implementation of its cooperation. The first modality in this collaboration is hypersecurity which is described by the urgency of establishing cyber security cooperation between Indonesia and Australia. Second, everyday security practices are presented by forming a Memorandum of Understanding on cyber cooperation between the two countries. The third modality, technification is implemented with the establishment of the Cyber Policy Dialogue Program which is then developed in other programs such as cyber boot camp, ASPI (Australian Strategic Policy Institute) cyber policy workshop, and cyber business connection. With the successful implementation of this cooperation, it will affect the increase in internal and regional security, as well as the ranking of the two countries' commitment to cyber security or the global cybersecurity index in the International Telecommunication Union.

Keywords: *Cooperation, cyber security, cyber terrorism, hypersecuritization, every day security practice, technification.*