PERUMUSAN KEBIJAKAN PERTAHANAN SIBER RUSIA DALAM MENGHADAPI ANCAMAN SIBER GLOBAL PASCA SERANGAN SIBER RUSSIA TERHADAP ESTONIA (ESTONIAN CYBER ATTACK 2007) MELALUI REZIM TALLINN MANUAL

ZEFANYA PHYTO

NIM: 1710412070

Abstrak

Perkembangan zaman telah menjadikan ruang siber sebagai salah satu hal yang krusial bagi dunia. Ruang siber telah menjadi suatu bentuk dunia baru, tidak terlepas bagi politik internasional. Banyak komponen negara yang tersimpan dalam ruang siber. Karena adanya hal ini, maka timbullah adanya kejahatan dalam ruang siber, yang berdampak akan dilahirkannya keamanan siber. Salah satu kejahatan siber yang memiliki skala cukup besar adalah serangan siber terhadap Estonia yang dilancarkan oleh Russia pada tahun 2007. Sehingga NATO Cooperative Cyber Defense Centre of Excellence bersama para ahli internasional merumuskan Tallinn Manual sebagai pedoman dalam dunia siber. Penelitian ini akan berfokus pada bagaimana Rusia merumuskan kebijakan sibernya menghadapi ancaman serangan siber global pasca serangan siber Estonia mengacu kepada Tallinn Manual. Serta penyesuaian perumusan kebijakan siber Rusia dengan Black Letter Rules yang terdapat dalam Tallinn Manual. Penelitian ini menggunakan 5 kerangka pemikiran yaitu Kebijakan Pertahanan, Pertahanan Siber, Keamanan Siber, Sabotase Siber, Perang Siber. Dalam penelitian ini, penulis menggunakan pendekatan kualitatif dan jenis penelitian deskriptif. Hasil dari penelitian menyatakan bahwa perumusan kebijakan siber Rusia dalam menghadapi ancaman siber global telah disesuaikan dengan pedoman Tallinn Manual.

Kata Kunci : Ruang Siber, Kejahatan Siber, Keamanan Siber, Kebijakan Pertahanan, Tallinn Manual.

RUSSIAN CYBER DEFENSE POLICY FORMULATION IN FACING GLOBAL CYBER THREATS POST RUSSIAN CYBER ATTACK ON ESTONIA (ESTONIAN CYBER ATTACK 2007) THROUGH THE TALLINN MANUAL REGIME

ZEFANYA PHYTO

NIM: 1710412070

Abstract

The times have made cyberspace one of the most important things for the world. Cyberspace has become a new world form, inseparable from international politics. Many state components are stored in cyberspace. Because of this, there is a crime in cyberspace, which will result in the birth of cybersecurity. One of the cyber crimes that has a fairly large scale is the cyber attack on Estonia launched by Russia in 2007. So the NATO Cooperative Cyber Defense Center of Excellence together with international experts formulated the Tallinn Manual as a guide in the cyber world. This study will focus on how Russia formulates its cyber policy to face the threat of global cyber attacks after the Estonian cyber attack, referring to the Tallinn Manual. As well as adjustments to the formulation of Russian cyber policy with the Black Letter Rules contained in the Tallinn Manual. This study uses 5 frameworks of thought, namely Defense Policy, Cyber Defense, Cyber Security, Cyber Sabotage, and Cyber War. In this study, the author uses a qualitative approach and the type of descriptive research. The results of the study stated that the formulation of Russian cyber policies in dealing with global cyber threats had been adjusted to the guidelines of the Tallinn Manual.

Keywords : Cyberspace, Cybercrime, Cybersecurity, Defense Policy, Tallinn Manual.