Kebijakan Cyber Defense dan Cyber Security di Indonesia dalam Menghadapi Kejahatan Perang Siber Global = Cyber Defense and Cyber Security Policies in Indonesia in Facing Global Cyber War Crimes

Farahdina Fairuz Iftinan, author

Abstrak

Perang siber adalah bentuk globalisasi kejahatan yang dilakukan oleh aktor yang berkuasa. Tesis ini menggunakan pendekatan kualitatif untuk menjelaskan bagaimana kebijakan cyber defense dan cyber security di Indonesia dan kesiapan Indonesia dalam menghadapi kejahatan perang siber global. Studi ini melibatkan 3 lembaga narasumber dari Kementerian Pertahanan, Kepolisian RI, dan Badan Siber dan Sandi Negara. Pengumpulan data dilakukan dengan tatap muka dan daring. Tesis ini menggunakan perspektif teori pilihan rasional dan kebijakan publik sebagai pijakan analisis. Teori pilihan rasional digunakan untuk menjelaskan bahwa aktor melakukan kejahatan melihat dari keuntungan dan kerugian yang didapatkan dari kejahatan yang dilakukan. Teori kebijakan publik memberikan penjelasan bagaimana tahapan pembuatan kebijakan agar menghasilkan kebijakan yang efektif dengan tujuan yang ingin dicapai. Hasil penelitian ini menunjukkan bahwa Indonesia masih memiliki banyak kekurangan pada cyber security<, cyber defense, dan kebijakannya. Berdasarkan analisis teori pilihan rasional, Indonesia berpotensi besar untuk diserang secara global dikarenakan lemah dan rentannya sistem keamanan dan pertahanan siber di Indonesia. Sehingga aktor penyerang akan mendapatkan keuntungan yang maksimal dan kerugian yang minimal. Dibutuhkan pembentuka kebijakan cyber security dan cyber defense sesuai dengan tahapan teori kebijakan publik, agar cyber security dan cyber defense dapat dijalankan dengan efektif. Temuan studi ini berkontribusi pada pembentukan kebijakan cyber security dan cyber defense yang komprehensif dan relevan sehingga dapat menghadapi kejahatan perang siber global.

.....Cyber warfare is a form of crime globalization perpetrated by powerful actors. This thesis uses a qualitative approach to explain how cyber defense and cyber security policies in Indonesia and Indonesia's readiness to face global cyber war crimes. This study involves three resource institutions that are the Ministry of Defense, the Indonesian National Police, and the National Cyber and Crypto Agency. Data collection was conducted both offline and online. This thesis uses the perspectives of rational choice theory and public policy as the basis of analysis. Rational choice theory explains that actors commit crimes by weighing the benefits and disadvantages of their crimes. Public policy theory describes the stages of policy-making to produce effective policies with the expected objectives. The results of this study indicate that Indonesia still has many shortcomings in cyber security, cyber defense, and its policies. Based on the analysis of rational choice theory, Indonesia has a high potential to be attacked globally due to the weak and vulnerable cyber security and defense systems in Indonesia. Thus, attacking actors will gain maximum benefits with minimal losses. It is necessary to formulate cyber security and cyber defense policies according to the stages of public policy theory so that cyber security and cyber defense can be implemented effectively. The findings of this study contribute to the formation of comprehensive and relevant cyber security and cyber defense policies to face global cyber war crimes.