ABSTRAK

Cyber Warfare ialah suatu tindakan yang dilakukan oleh suatu negara atau organisasi internasional yang berkaitan dengan penyerangan yang disengaja kepada jaringan komputer atau jaringan informasi negara lain yang bertujuan untuk menyebabkan kerusakan atau gangguan dalam jaringan tersebut. Serangan *cyber warfare* dapat melumpuhkan website resmi dan juga jaringan informasi, mengacaukan atau melumpuhkan layanan vital suatu negara, mencuri atau merubah data rahasia, melumpuhkan sistem finansial, dan banyak juga kemungkinan lainnya. Banyak negara-negara sudah memberi perhatian khusus dalam isu *cyber warfare*, khususnya Indonesia. Untuk dapat menangani ancaman baru tersebut, Indonesia lewat pemerintah dan organisasi non-pemerintah memiliki beberapa upaya untuk menaikkan tingkat keamanan *cyber*-nya. Rumusan masalah dari skripsi ini ialah bagaimana upaya Indonesia dalam menangani ancaman keamanan *Cyber Warfare*. Untuk meneliti dan mempertajam analisis penelitian skripsi ini, digunakan kerangka pemikiran berisi konsep ketahanan non-tradisional, teori sekuritisasi, dan teori keamanan masyarakat. Metodologi penelitian yang digunakan ialah metode kualitatif. Sumber data yang digunakan untuk menyusun skripsi ini adalah dengan cara menggunakan teknik penelitian keperpustakaan (*Library research*) dimana data yang diperoleh berasal dari buku, skripsi yang sudah ada, jurnal, artikel dari media cetak dan media elektronik serta berbagai sumber tertulis lainnya. Pembahasan dari skripsi ini terdiri dari berbagai bab, yang berisi tentang pendahuluan, sejarah perkembangan *cyber warfare*, hal-hal teknis mengenai *cyber warfare*, dan upaya pemerintah Indonesia untuk menghadapinya.

ABSTRACT

Cyberwarfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyberwarfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities. Many countries have given special attention to the issue of cyber warfare, particularly Indonesia. To be able to deal with the new threats, Indonesia through government and non-governmental organizations have several attempts to raise the level of its cyber security. Formulation of the problem of this thesis is how Indonesia's efforts in addressing Cyber Warfare security threats. To examine and refine the analysis of this thesis research, the framework contains non-traditional concept of national resilience, securitization theory, and the theory of public safety. The research methodology used is qualitative method. Source of data used to compile this thesis is to use library research techniques, where the data obtained came from books, existing theses, journals, articles from various media as well as various other written sources. The discussion of this thesis consists of various chapters, which contains an introduction, the historical development of cyber warfare, technical matters regarding cyber warfare, and the Indonesian government's efforts to deal with it.