ABSTRAK

Negara Iran adalah salah satu negara yang memiliki kapabilitas nuklir besar di dunia. Dengan kapabilitas tersebut, Iran menjadi ancaman bagi negara – negara lain terutama Israel dan sekutunya Amerika Serikat. Perkembangan teknologi nuklir Iran beriringan dengan majunya teknologi komunikasi dan informasi. Hal tersebut menyebabkan Iran menerima serangkaian serangan *malware* berbahaya. Tujuan serangan *malware* kepada Iran adalah untuk memperlambat laju pertumbuhan pengayaan nuklir Iran yang dianggap berbahaya bagi negara Israel dan Amerika Serikat. Namun Iran menerapkan kebijakan – kebijakan untuk menangkal serangan – serangan tersebut. Skripsi ini bertujuan untuk membahas tentang apa saja kebijakan *cyber security* yang diambil oleh Iran. Metode yang digunakan adalah library research dan teknik pengumpulan data.

Kata Kunci: *Malware*, *Cyber Security* di Iran, Amerika Serikat, dan Israel.

IRAN CYBER SECURITY POLICY IN FACING CYBER WARFARE THREATS (2012-2017)

ABSTRACT

Iran, is one of the countries that have a big nuclear capability in the world. With that Capability, Iran is a threat to other country especially Israel and their ally United States. The development of Iran's nuclear technology goes hand in hand with the advancement of communication and information technology. This caused Iran received several dangerous malware attacks. The aim of the malware attack on Iran is to slow the rate of growth of Iran's nuclear enrichment facility which is considered dangerous for Israel and the United States. This thesis discusses about the cyber security policies in Iran. The method used is library research and data collection techniques.

***Keywords*:** Malware, Cyber Security in Iran, Amerika Serikat, Israel