ABSTRAK

Departemen Keamanan Dalam Negeri AS telah mengidentifikasi semakin sering serangan pada jaringan cyber sebagai salah satu ancaman keamanan nasional yang paling parah pada Amerika Serikat. Bahkan, cyber sekarang dianggap sebagai domain,' warfighting bersama dengan tanah, laut, udara, dan ruang angkasa.

serangan cyber ditargetkan pada pembajakan infrastruktur penting (listrik, pipa, penerbangan, kereta api, perbankan, dll) hal tersebut sangat mengkhawatirkan. Dan sangat disesalkan, Amerika Serikat saat ini lebih rentan terhadap serangan cyber karena ketergantungan yang lebih besar pada sistem cyber yang dikendalikan untuk menjalankan infrastruktur nasional yang kritis.

Selain itu, ketergantungan militer pada infrastruktur sipil (system komputer dan jaringan, satelit) mempertinggi kerentanan AS. Ketergantungan yang tumbuh di infrastruktur *cyber* membuka jalan bagi ancaman keamanan nasional baru terhadap Amerika Serikat. Potensi musuh mencoba untuk diam-diam menghindari konfrontasi langsung dengan militer AS dapat menyerang Amerika melalui dunia *cyber*. Meskipun berbagai upaya telah dilakukan untuk menanggani ancaman *cyber* oleh Departemen Homeland Security, Departemen Pertahanan AS, Komando Satuan *Cyber* AS, dan FBI, kebijakan yang terkoordinasi harus dibentuk untuk melindungi infrastruktur penting dari serangan cyber.

Skripsi ini mengidentifikasikan pengaruh pengaruh yang timbul terhadap kemanan AS akibat serangan *cyber* yang semakin sering, yang juga akan mempengaruhi sikap politik AS baik da.

Kata kunci: Perang *Cyber*; Keamanan *Cybe*r; Keamanan Nasional, Infrastruktur Kritis AS, Satuan Komando *Cyber* AS, *Cyberstrategy* Departemen Pertahanan AS.