BAB VI
KESIMPULAN DAN SARAN

VI.1. Kesimpulan

Dengan adanya serangan virus Stuxnet,maka Iran harus mampu untuk meningkatkan kekuatan keamanan siber mereka dengan membuat prosedur operasi pencegahan kejahatan siber.Ketika Iran menyadari bahwa negara mereka telah menjadi sasaran serangan siber, tampaknya ada kebingungan di dalam otoritas Iran tentang cara untuk menanggapi serangan itu secara politis. Oleh karena itu, prosedur operasi standar di tingkat politik juga dapat membantu memberikan panduan kepada pihak berwenang tentang bagaimana menanggapi serangan siber yang dilakukan oleh Amerika Serikat dan Israel.Virus Stuxnet adalah bukti nyata perkembangan kejahatan siber dimasa depan.Stuxnet telah menggeser paradigma bahwa perang dimasa depan tidak lagi menggunakan kekuatan militer secara fisik dan menimbulkan korban jiwa. Stuxnet telah menciptakan revolusi di bidang perang karena salah satu senjata tersebut dapat digunakan untuk mendapatkan akses ke pusat nuklir negara lain, karena hal ini pula serangan siber dengan menggunakan virus sebagai senjata menjadi paling berbahaya dan mematikan kemajuan dalam taktik perang. Dunia internasional menjadikan peristiwa ini sebagai pelajaran pacuan untuk peningkatan kekuatan siber nasional negara untuk mencegahnya perkembangan peristiwa yang sama di masa depan dengan mengambil tindakan pencegahan ancaman siber.

VI.2. Saran

Kerusakan yang disebabkan oleh Stuxnet pada sentrifugal Iran menunjukkan bahwa infrastruktur penting dapat menjadi sasaran ancaman siber. Fakta bahwa jaringan Natanz terpisah dari jaringan lain dan tidak terhubung ke internet tidak cukup untuk melindungi program nuklir Natanz dari serangan virus Stuxnet.Oleh karena itu, negara harus mempertimbangkan bahwa infrastruktur penting harus diintegrasikan dalam strategi keamanan siber. Pertimbangan tersebut akan

menyiratkan peningkatan perlindungan terkait dengan ancaman siber, dengan standar keamanan siber.Hal ini juga bertujuan untuk meningkatkan perlindungan terhadap ancaman siber, dan juga untuk meningkatkan ketahanan jika terjadi serangan siber.

Negara harus meningkatkan kekuatan sibernya agar mampu untuk melindungi negaranya dari serangan negara lain untuk menyerang negaranya.Perlu adanya peningkatan keamanan siber dengan melibatkan kebijakan siber kedalam peraturan dan aturan militer sebuah negara.Melihat perkembangan perang tidak lagi menggunakan perang konvensial di masa depan,maka negara harus mampu untuk mempersiapkan dirinya secara matang agar mampu menghadapi ancaman serupa.