Sistem pertahanan siber TNI AD dalam menghadapi ancaman cyber security (studi kasus kerjasama tni ad dengan institut teknologi del, sumatera utara tahun 2014) = Cyber defense system of the indonesian army forces in encountering cyber security threats (case study of indonesian army forces cooperation with technology institute of del, north sumatra in 2014)

Widiyatmoko, author

Abstrak

Kejahatan di dunia maya, sudah berkembang pesat dan membahayakan. Kejahatan tersebut muncul karena penyalahgunaan teknologi Internet atau jaringan komputer, seperti menyebar virus yang merusak akses informasi, membajak atau mencuri informasi, mengubah informasi secara ilegal, hingga memata-matai akses informasi. Salah satu kejadian yang terkait dengan terjadinya cybercrime diantaranya perentasan situs TNI AD pada Rabu, 15 Oktober 2013 melalui situs www.pusdikkav.mil.id yang merupakan situs Pusat Pendidikan Kavaleri TNI AD. Kasus tersebut menunjukkan bahwa dalam kerangka pertahanan di bidang siber, Indonesia masih belum optimal. Program pendidikan dan pelatihan cyberdefence diperlukan guna meningkatkan kompetensi sumber daya manusia SDM . Perlunya pemahaman langkah-langkah preventif dalam menangkal segala ancaman siber dengan membangun pertahanan siber yang kuat. Pengembangan kapasitas SDM dalam penangganan cyber-security, di tubuh TNI AD yaitu melakukan kerjasama dengan perguruan tinggi yang memiliki kemampuan di bidang Informasi Teknologi dan komunikasi seperti kerjasama yang dilakukan oleh TNI AD dengan Institut Teknologi Del IT Del , Sumatera Utara. Kerjasama ini berlangsung dalam tiga program, antara lain: penyiapan model perang cyber/cybercamp, seminar military cyber intelligence and cyber operation, serta pekan/lomba cyber. Penelitian ini menggunakan pendekatan kualitatif berupaya menganalisis sistem pertahanan siber TNI AD saat ini dan program kerjasama antara TNI AD dengan IT Del untuk meningkatkan kualitas SDM personil Disinfolahtad dalam rangka menghadapi ancaman cybersecurity sehingga dapat mendukung pertahanan negara.
.....Cybercrime grows rapidly and endangering in nature. This type of crime emerges due to malpractices of Internet technology or Computer Networks, such as computer virus contagion that destroys information access, information stealing and hacking, illegal information alteration, to information espionage. A cybercrime related incident occured on Wednesday, 15 October 2013, where the Indonesian Army 39 s Cavalry Education Centre website www.pusdikkav.mil.id was hacked. The incident shows lack of optimalization in Indonesia 39 s cyber defense framework. Cyber defense education and training programs are needed to increase the human resources competences. It requires comprehension on preventive ways as defenses from cyber threats by establishing a strong cyber protection. In the Indonesian Army, the human resources capacity building in cyber security is conducted through cooperation with higher education institution with capablilities in Technology and Information field, and communications such as cooperation between Indonesian Army Forces and Technology Institute of Del IT Del , North Sumatra. This cooperation run through three distinct programs such as cyber warfare modelling cybercamp , military cyber intelligence and cyber defense seminar, and cyberweek. This research utilizes qualitative approach, and determined to analyze current Indonesian Army cyber defense system and the cooperation with IT Del to increase human

resources quality of Disinfolahtad personnel, in order to anticipate cyber security threats for national defense.