BAB V

KESIMPULAN DAN SARAN

5. 1 Kesimpulan

1. Perkembangan internet semakin hari semakin trend baik dari teknologinya maupunya penggunanya dan hampir setiap manusia didunia menggunakan teknologi, di Indonesia pengguna teknologi pada tahun 2014 mencapai 88 juta pengguna internet selanjutnya data pada baru-baru ini pada tahun 2013 naik mencapai 132,7 juta orang yang terhubung dengan internet. Dengan menggunakan internet di Indonesia maupun dunia ini tidak semua pengguna menggunakan internet dengan baik dan positif dengan apa yang seharunya. Di Indonesia *cybercrime* menurut data CIA menyebutkan bahwa Indonesia telah mencapai 1.20% kerugian akibat *cybercrime* yang terjadi di dunia.
2. Dengan adanya *cybercrime* yang sedang dibicarakan sekarang-sekarang ini, penanganan *cybercrime* ini tidak lah mudah untuk mengatasi permasalahan *cyber* yang terjadi, maka dari itu Indonesia membutuhkan kerjasama *cyber security* dengan negara lain salah satunya yaitu kerjasama *Korea International Coorporation Agency* (KOICA) dan pemerintah Indonesia dalam mengebangkan *cyber security*, dalam kerjasama tersebut dapat mencetak para Sumber Daya Manusia (SDM) yang dapat mampu dalam dunia *cyber*.
3. *Cyber security* telah ada dan berjalan pada tahun 2007 dengan dibetuknya Indonesia *security incident response team on internet*

infrastructure adalah tim yang tugaskan oleh Menteri komunikasi dan informatika (kominfo) yang bertujuan untuk membantu mengawasi permasalahan jaringan yang berbasis *protocol* internet. Dengan adanya kebijakan pada tahun 2007 ini masih saja Indonesia mendapatkan serangan *cyber* dari negara lain, dikarenakan Indonesia mengalami kurangnya Sumber Daya Manusia (SDM). Maka dari itulah Indonesia membutuhkan bantuan dari luar yaitu Korea Selatan untuk kerjasama dengan Indonesia dalam mengatasi serangan *cyber* dari luar.

Dalam penelitian ini tentang kerjasama *Korea International Coorporation Agency* (KOICA) dan Institut Teknologi Bandung (ITB) dalam pengembangan *cyber security* yang dipercayakan dan bertempat di Institut Teknologi Bandung (ITB) sebagai penyelenggara kegiatan pendidikan, riset dan pengembangan dimana kedua program tersebut telah berjalan dan memiliki hasil yaitu pendidikan *cyber security center, e-learning* tentang *cyber security* terhadap guru dan polisi keamanan, militer, *warlless* "*camp kids"* untuk anak – anak SD, 3 (tiga) tahap kelulusan magister dalam dunia *cyber security* dan dengan kelulusan tersebut telah langsung bergabung dengan *cyber security* Indonesia dengan tujuan mencegah serangan *cyber* dari luar maupun dari dalam negeri sendiri.

4. Dalam melakukan kejasama upaya-upaya yang di lakukan yaitu dengan *joint conference*, kekeluargaan, mencari peluang kerjasama riset, pendanaan dan mempunyai kendala dalam melakukan kerjasama

yaitu kendala manajerial, kendala sumber daya manusia, kendala teknikal dan dengan keingin untuk mengembangkan *cyber security* di Indonesia dan mencetak Sumber Daya Manusia (SDM) dalam pengembangannya maka timbulah prospek bagi kerjasama yaitu *network security, mobile, ditation malware development, information manajement*. Dengan adanya kerjasama ini memberikan harapan kepada Indonesia agar terjaga dari *hacking* yang dilakukan oleh pengguna yang tidak dikenal dari dalam negeri maupun datang dari laur negeri.

Pada tahun 2013 kerjasama dalam mengembangkan *cyber security* antara Korea Selatan dan Indonesia telah berjalan dengan lancar. program-program ini dapat membantu Indonesia untuk meningkatkan pengetahuan dan *skill* kepada masyarakat dalam menigkatkan wawasan mengenai *cyber*. Dengan adanya program-program yang dijalankan dapat menghasilkan beberapa hasil dari kerjasama antara Indonesia dengan Korea Selatan dimana hasil tersebut merupakan tujuan bagi indonesia dari kerjasama yaitu mencetak Sumber Daya Manusia yaitu sebagai berikut yaitu : yang pertama peningkatan Sumber Daya Manusia (SDM) dalam meningkatkan keamanan dalam *cyber* maka permasalahan utama dalam mengatasi ancaman yang datang dibutuhkan para ahli *cyber* yang mampu mengatasi ancaman-ancaman yang dilakukan oleh para *hacker*. Ancaman-ancaman tersebut berupa, pembobolan data pribadi, data pemerintah yang bersifat penting dan

rahasia, tidak hanya para instansi pemerintah saja melainkan instansi-instansi non pemerintah pun dapat di *hack* oleh para *hacker*. Biasanya para *hacker* menggunakan kemampuan atau ahli yang mereka punya untuk melihat mengeskpor keahlian mereka dengan meng *hacking* contohnya yaitu pembobolan kartu kredit yang terjadi pada tahun 2013 lalu. Berdasarkan data dari *Indonesia security incident response team on internet infrastructure* (ID-SIRTII/CC) Menkominfo serangan dunia *cyber* di Indonesia pada tahun 2015 mencapai 28 juta serangan.

Dengan terciptanya hasil kerjasama ini yang menimbulkan pertukaran informasi yang dilakukan merupakan hal yang sangat baik dikarenakan Indonesia dan Korea Selatan sering mendapatkan serangan *cyber* dari luar.

5.2 Saran

1. Dalam menghambat pergerakan *cybercrime* maka perlu ditingkatkan *standart of procedure* terkait *security* dalam mengembangkan aplikasi yang berbasis web dan *application programming interface*.
2. Dalam mencegah terjadinya *hacker* maka negara pun membenahi hukum nasional yang ada dengan ketat sehingga para pelaku hacker tidak leluasa dalam beroperasi, tidak cukup dengan membenah hukum dengan ketat.
3. kurang kesadaran dari masyarakat mengenai pengamanan dalam aktiktivitas di dunia maya. Maka lebih bagus lagi apabila diadakan pendidikan bagi masyarakat mengenai *cyber security*, karena tidak

semua masyarakat Indonesia mengetahui apa itu keamanan maupun *hacker*, para pengguna hanya mengetahui menggunakannya saja tidak memikirkan keburukan yang terjadi nantinya.