BAB IV

PENUTUP

IV.1 Kesimpulan

Masalah keamanan cyber saat ini telah mampu menjadi salah satu masalah yang diprioritaskan oleh negara. Amerika Serikat pada masa pemerintahan Presiden Obama juga memprioritaskan keamanan cyber kedalam kebijakannya. Hal itu disebabkan oleh proliferasi teknologi informasi dan komunikasi berbasis jaringan internet yang semakin meningkat dan meluas diseluruh lapisan masyarakat didunia dan menyebabkan hubungan didunia menjadi tanpa batas (*borderless*). Hal ini juga membuat masyarakat menjadi ketergantungan kepada ruang cyber, dengan ketergantunga tersebut maka membuat celah bagi para aktor-aktor tidak bertanggung jawab untuk mengambil keuntungan yang berbeda-beda.

Pencurian data teknologi pesawat yang merupakan proyek pertahanan militer paling mahal Amerika Serikat menjadi bukti bahwa keamanan cyber amat sangat diperlukan. Teknologi pesawat *Lockhead Martin* F-35 *Lightning II* menjadi incaran para peretas Cina untuk mengembangkan teknologi pesawat J-20 dan J-31 yang kelak akan digunakan oleh militer Cina. Teknologi pesawat yang dicuri ternyata bukan hanya dari *Lockhead Martin* saja, tetapi ada juga teknologi pesawat F-22 Raptor dan C-17 yang diproduksi oleh Boeing. Informasi rahasia yang diincar dari kontraktor pertahanan ini meliputi data uji terbang pesawat, sistem persenjataan, dan sistem radar.

Dampak dari aksi spionase cyber Cina mempengaruhi banyak hal di Amerika Serikat. Secara nilai ekonomi dampak mengarah pada kerugian fiansial atau pendapatan serta hilangnya daya saing perdagangan oleh perusahan-perusahaan Amerika Serikat dalam persaingan pasar internasional. Sementara dampak pada segi militer, hilangnya label negara sebagai pemilik kemampuan militer paling kuat dan modern didunia. Hal ini menyebabkan Amerika Serikat

kehilangan posisi tawar yang kuat dalam perpolitikan internasional dan negara-negara yang selama ini bergantung kepada Amerika Serikat akan berpindah dan lebih memilih Cina atau Rusia. Selain itu spionase cyber Cina terhadap Amerika Serikat juga menyebabkan hubungan diplomatik antara kedua negara menjadi renggang dan sangat berpotensi berubah menjadi konflik terbuka dalam ruang cyber. Apabila konflik terbuka dalam ruang cyber atau perang cyber antara Amerika Serikat dan Cina memang terjadi maka dampak pada kerusakan fisik dan terganggunya aktivitas negara dalam memberikan pelayanan pada publik.

Dalam mengatasi masalah spionase cyber Cina yang mengancam keamanan nasional dan perekonomian Amerika Serikat ini, Presiden Obama mengubah fokus kebijakan Amerika Serikat dalam bidang keamanan yaitu dengan memprioritaskan keamanan cyber nasional. Fokus dalam keamanan cyber ini juga tidak semata-mata untuk mengatasi ancaman cyber dari Cina saja, Amerika Serikat mengambil langkah yang lebih futuristik dengan memperhitungkan ancaman-ancaman cyber yang lebih besar dan tidak hanya untk menjaga stabilitas dalam masa damai. Dalam hal ini penulis melihat secara keseluruhan upaya Amerika Serikat dalam mengatasi masalah dan ancaman cyber baik internal maupun eksternal masih dalam tahapan awal yang mana masih perlu pengembangan secara berkala. Amerika Serikat lebih menekankan kepada upaya *self-defense* dalam lingkup internal dengan meningkatkan keamanan nasional dalam bidang cyber. Penulis juga belum melihat bahwa adanya upaya-upaya yang menimbulkan efek secara konkrit dalam mengatasi ancaman cyber ini. Amerika Serikat juga harus memastikan upaya-upaya awal yang sudah dibentuk ini dapat berjalan dan berkelanjutan sehingga masyarakat Amerika Serikat akan merasa aman dan terlindungi dalam memanfaatkan keuntungan yang diberikan oleh ruang cyber ini. Pertukaran informasi menjadi kunci utama yang ditekankan oleh Amerika Serikat untuk bisa mempertahankan diri dan mengantisipasi akan bahaya dan ancaman yang datang.

Selain itu adanya komitmen yang dibangun oleh Amerika Serikat untuk melakukan pendekatan secara internasional melengkapi upaya peningkatan keamanan nasional cyber Amerika Serikat. Dengan melakukan peningkatan

hubungan diplomatik secara bilateral yaitu dengan Cina sebagai negara yang terlibat langsung dalam masalah spionase cyber dengan Amerika Serikat dan multilateral yaitu dengan partisipasi Amerika Serikat kedalam UN GGE. Melalui UN GGE ini Amerika Serikat mempromosikan kepentingannya untk menciptakan lingkungan cyber yang aman secara internasional dan mendorong negara-negara didunia untuk memilki perilaku yang bertanggung jawab dalam memanfaatkan ruang cyber tanpa mengganggu stabilitas dan integritas nasional negara-negara lainnya. Selain itu mendorong pertukaran informasi antar negara terkait adanya potensi-potensi bahaya dan ancaman agar bisa diatasi secepat mungkin

IV. Saran

Masalah keamanan cyber saat ini telah menjadi permasalahn bagi banyak negara didunia. Maka dari itu penting bagi negara-negara didunia untuk mulai memperhatikan lingkungan ruang cyber sebagai wilayah baru yang bisa membawa dampak buruk pada keselamatan negara. Melalui penelitian ini, penulis memberikan beberapa saran. Pertama, negara sudah harus membuka mata bahwa ruang cyber saat ini tidak bisa dianggap lagi sebagai suatu tempat untuk bermain semata, banyak ancaman dari aktor-aktor tidak bertanggung jawab yang mengintai para penggunanya. Kebijakan dan undang-undang harus dibentuk dan ditegakan untuk membatasi ruang gerak aktor-aktor jahat ini dalam bermanuver diruang cyber yang sangat luas. Kedua, bagi negara-negara yang ingin memulai atau baru memulai membangun keamanan cyber nasional, sangat perlu melakukan persiapan sebagaimana yang dilakukan oleh Amerika Serikat agar tidak terjadi masalah tumpang tindih tugas dan tanggung jawab dari para pemegang kepentingan. Ketiga adalah masalah penegakan hukum, kejahatan cyber pada dasarnya adalah perbuatan yang melanggar hukum, Maka dari itu hukum yang ada perlu diperbaharui untuk menyesuaikan dengan perkembangan tindak kejahatan yang juga terus berkembang. Keempat, negara juga harus bergerak aktif melakukan pendekatan secara internasional, hal ini menjadi satu kunci penting karena ancaman cyber ini tidak hanya berasal dari satu negara, ancaman cyber memilki sifat lintas batas negara.