

## BAB VI

### KESIMPULAN DAN SARAN

#### 6.1 Kesimpulan

Lingkungan ancaman dan risiko dunia maya saat ini dari dunia maya merupakan tantangan untuk menjaga keamanan Negara-Bangsa di negara mana pun di dunia. Namun, kawasan Amerika Latin tertinggal dalam membangun kapasitas siber untuk menangani konteks ini. Dalam hal ini, tindakan pertama yang harus diambil oleh pemerintah kelompok negara ini adalah memahami tingkat risiko dan ancaman terhadap keamanan nasional, yang dapat muncul dari domain ini untuk mempengaruhi Negara-Bangsa. Meksiko dan Brasil merupakan negara dengan tingkat kejahatan siber tertinggi di wilayah Amerika Latin, dengan angka Brasil 36%, Meksiko 17% dan diurutan ketiga adalah Kolombia dengan 12%.

Meksiko dan Brasil merupakan negara yang masih berusaha dalam mengembangkan keamanan siber di negaranya. Kebijakan yang belum matang atau bahkan belum ada ini dimanfaatkan oleh pengguna yang tidak bertanggung jawab (pelaku kejahatan) untuk mempengaruhi keamanan nasional Meksiko dan Brasil. Brasil ditahun 2019 telah melakukan ratifikasi undang-undang No. 2.295, 4 Agustus 1997, dan undang-undang tahun 2019 ini merupakan undang-undang pertama yang membahas keamanan informasi siber Brasil. Pada tahun 2020 juga Brasil menerbitkan strategi keamanan *E-siber* bertujuan untuk mengingatkan ketahanan terhadap ancaman siber dan memperkuat kinerja internasionalnya pada topik keamanan siber. Sementara itu, Meksiko ditahun 2019-2020 masih dalam tahap menyusun RUU keamanan siber dan belum melakukan penyesuaian undang-undang apapun. Sebagai gantinya, Meksiko rutin melakukan kampanye gerakan anti kejahatan siber di negaranya

mengenai penggunaan teknologi baru dan internet secara bertanggung jawab untuk mengurangi kerusakan yang disebabkan oleh kejahatan dunia maya. Dalam hal ini, Brasil bisa dikatakan lebih unggul dan lebih serius dalam menekan kejahatan siber di negaranya, dan lebih matang dalam menjadi anggota tetap Konvensi Budapest. Meksiko terhadap instrumen internasional seperti Konvensi Budapest tentang kejahatan dunia maya penting untuk mulai mengambil tindakan lebih lanjut di bidang ini. Perlu bagi pemerintah Meksiko untuk mengambil langkah pertama dengan membuat undang-undang keamanan siber yang cukup mengikat dengan untuk menghadapi ancaman keamanan siber. Pemerintah Meksiko dan Brasil pun memiliki caranya sendiri guna meredam kasus kejahatan dunia maya, Meksiko dengan mengeluarkan kampanye guna memberikan gambaran atau pengetahuan mengenai kejahatan siber dan pastinya dengan mengutamakan perlindungan manusia. Lain dengan Brasil yang lebih menerapkan kepada perancangan undang-undang guna ratifikasi agar Brasil cepat bergabung dalam Konvensi Budapest pada akhir tahun 2022 ini. Selanjutnya, dalam kesimpulan, teori dan konsep berfungsi sebagai pedoman penelitian agar lebih terarah, ini menghasilkan sebuah pembuktian bahwa dengan meningkatnya kasus phishing ini merupakan ancaman yang membahayakan keamanan nasional. Karena masalah keamanan bisa menjadi sebuah ancaman apabila telah merubah stabilitas politik dan keamanan dan juga berpotensi kehidupan sosial masyarakat. Dengan demikian teori sekuritisasi dirujuk karena adanya urgensi yang terjadi di Meksiko dan Brasil akibat dari kasus kejahatan siber Phishing, karena isu ini terbukti telah mengganggu stabilitas keamanan, politik dan masyarakat.

## 6.2 Saran Penelitian

Peneliti memberikan saran untuk penelitian ini menjadi dua aspek, yaitu; secara akademis dan juga secara praktis. Saran yang diberikan pada penelitian ini sebagai berikut.

### 6.2.1 Saran Akademis

Peneliti menyadari terdapat banyak kekurangan di dalam penelitian ini. Peneliti berharap pada penelitian berikutnya bisa lebih mendalami dan mempelajari mengenai keamanan siber atau *cybersecurity* di wilayah Amerika Latin akibat dampak dari kejahatan siber atau *cybercrime*, karena penting bagi suatu negara atau wilayah dalam membuat kebijakan yang mengatur mengenai keamanan siber guna menjaga keamanan nasional pada wilayah atau negara tersebut.

### 6.2.2 Saran Praktis

Peneliti mengharapkan agar penelitian ini bisa dijadikan acuan untuk pengambilan kebijakan berkenaan dengan *cybersecurity* terhadap *cybercrime* khususnya pada kejahatan phishing yang masih menjadi musuh utama di negara-negara yang kegiatan masyarakat dan pemerintahnya terkomputerisasi.