BAB V

PENUTUP

A. Kesimpulan

Berdasarkan pembahasan maka dapat diperoleh kesimpulan untuk menjawab dua rumusan masalah dalam skripsi ini yaitu:

1. Pada umumnya modus pelaku kejahatan *cyber crime* (kejahatan siber) pada internet banking antara lain karena adanya faktor politik, misalnya dengan sabotase atau merusak data untuk menjatuhkan lawan politik untuk menduduki posisi/jabatan tertentu atau membobol program komputer milik Pemerintah dengan pembuatan website yang berisi informasi yang bersifat provokasi melawan Pemerintah. Faktor ekonomi, misalnya perbuatan *hacker* yang berhasil membobol sistem *online* perbankan yang kemudian dilanjutkan dengan mentransfer sejumlah uang ke rekening pribadinya. Faktor tantangan atau rasa ingin tahu, sebagai contoh dalam kasus Steven Haryanto yang membuat duplikat situs www.klikbca.com PT Bank Central Asia (BCA) karena ingin mengetahui seberapa kuat sistem keamanan dalam layanan internet banking bank tersebut. Dan pelakunya berkeyakinan bahwa perbuatannya dilandasi dengan tujuan yang mulia karena memberitahukan kepada nasabah bahwa sistem keamanannya amat lemah. Selanjutnya faktor kelalaian pengguna/nasabah layanan internet banking, misalnya dalam pengaplikasian *Password*/PIN yang dibuat oleh nasabah di ATM hanya digunakan pada login awal dan penggunaan

berikutnya tidak mengubah *Password*/PIN tersebut. Karena sistem keamanan dari pihak perbankan sendiri yang juga masih sangat lemah.

2. Peraturan yang dapat diterapkan terhadap terjadinya *cyber crime* (kejahatan siber) pada internet banking yaitu menggunakan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Namun, dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) belum ada pasal yang khusus menyebutkan dalam memberikan hukuman atau sanksi terhadap pelaku kejahatan pada internet banking itu sendiri. Sekalipun tidak ada pasal yang secara khusus mengatur tentang *cyber crime* pada internet banking, Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dapat diterapkan melalui unsur-unsur yang ada kaitannya dengan kejahatan yang dilakukan. Oleh karena itu, dalam menanggulangi *cyber crime* (kejahatan siber) pada internet banking tidak dapat menggunakan Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) saja tetapi dapat juga diterapkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan serta Pasal-Pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) yang unsur-unsurnya terkait dengan kejahatan yang dilakukan mengingat kejahatan dalam dunia maya khususnya IT sudah mengalami perkembangan yang begitu pesat. Penerapan sanksi dalam peraturan diatas belum sepenuhnya memberikan efek jera terhadap pelaku sehingga Pemerintah dan Badan Legislatif perlu

memperbaharui peraturan perundangan yang sudah ada untuk mengatasi *cyber crime* pada internet banking. Kejahatan yang terjadi di dunia Perbankan juga tidak sepenuhnya diselesaikan dengan jalur hukum melainkan dengan perdamaian karena pihak Bank merasa ingin menjaga nama baik Bank.

B. Saran

Semakin marak dan meningkatnya *cyber crime* (kejahatan siber) dalam Perbankan khususnya internet banking perlu adanya pembaharuan peraturan perundangan yang sudah ada dalam menangani kejahatan siber agar para pelaku jera yang tidak hanya menggunakan Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi dan Undang-Undang Nomor 10 tahun 1998 tentang Perbankan. Pemerintah dan Badan Legislatif harus menetapkan pembaharuan Rancangan Peraturan Perundangan dalam menangani *cyber crime* (kejahatan siber) pada internet banking mengingat akibat kerugiannya yang tidak sedikit. Berbagai kejahatan pada internet banking tentu menjadi perhatian khusus bagi aparat penegak hukum yaitu Penyidik khususnya Polri dalam menanggulangi kejahatan tersebut. Penanggulangan *cyber crime* (kejahatan siber) pada internet banking ini memerlukan strategi yang utuh dan tajam mengingat kerugian yang diderita nasabah maupun bank sangat tidak sedikit. Kualitas Sumber Daya Manusianya pun harus lebih ditingkatkan agar dapat mengimbangi perkembangan teknologi yang pesat. Meningkatkan sistem pengawasan terhadap pihak-pihak yang

berteknologi seperti pengusaha warnet, pengusaha komputer agar tidak melakukan kejahatan komputer lewat internet.