BAB IV

PENUTUP

1.1. Kesimpulan

1. Mengenai pengaturan tindak pidana *cyber espionage* dalam hukum positif di Indonesia bahwa hukum positif yang ada menunjukkan adanya kekosongan normatif dan belum adanya regulasi khusus yang secara tegas dan terperinci mengatur *cyber espionage* sebagai tindak pidana tersendiri. Untuk menjamin kepastian hukum dan efektivitas penegakan hukum terhadap kejahatan ini, dibutuhkan pembaruan hukum, baik melalui revisi Undang-Undang yang ada maupun pembentukan instrumen hukum baru yang spesifik mengatur kejahatan siber lintas negara dan berdimensi intelijen seperti *cyber espionage*.
2. Meskipun belum ada aturan yang secara eksplisit menyebut istilah "*cyber espionage*". Namun, beberapa ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, dapat dijadikan dasar pertanggungjawaban pelaku. Pasal-Pasal yang mengatur tentang akses ilegal (Pasal 30), intersepsi ilegal (Pasal 31), dan manipulasi data atau sistem elektronik (Pasal 32 dan Pasal 33) dapat digunakan untuk menjerat pelaku *cyber espionage*. Selain itu, jika tindakan tersebut mengancam keamanan negara atau membahayakan kepentingan nasional, pelaku juga dapat dijerat dengan Pasal-Pasal dalam Kitab Undang-Undang Hukum Pidana (KUHP) tentang kejahatan terhadap keamanan negara. Oleh karena itu, meskipun

adanya kekosongan hukum terkait regulasi yang khusus mengenai *cyber espionage*, pelaku tetap dapat dimintai pertanggungjawaban pidana berdasarkan ketentuan yang ada dalam hukum positif Indonesia.

1.2. Saran

1. Pemerintah diharapkan melakukan pembaruan dan harmonisasi peraturan perundang-undangan yang relevan, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), agar secara eksplisit mencakup tindak pidana spionase siber.
2. Pemerintah perlu membentuk satuan tugas khusus di bawah lembaga penegak hukum yang memiliki kompetensi teknis di bidang keamanan siber guna mempercepat proses identifikasi, investigasi, dan penindakan pelaku. Kerja sama internasional juga harus diperkuat, mengingat *cyber espionage* sering melibatkan aktor lintas negara.