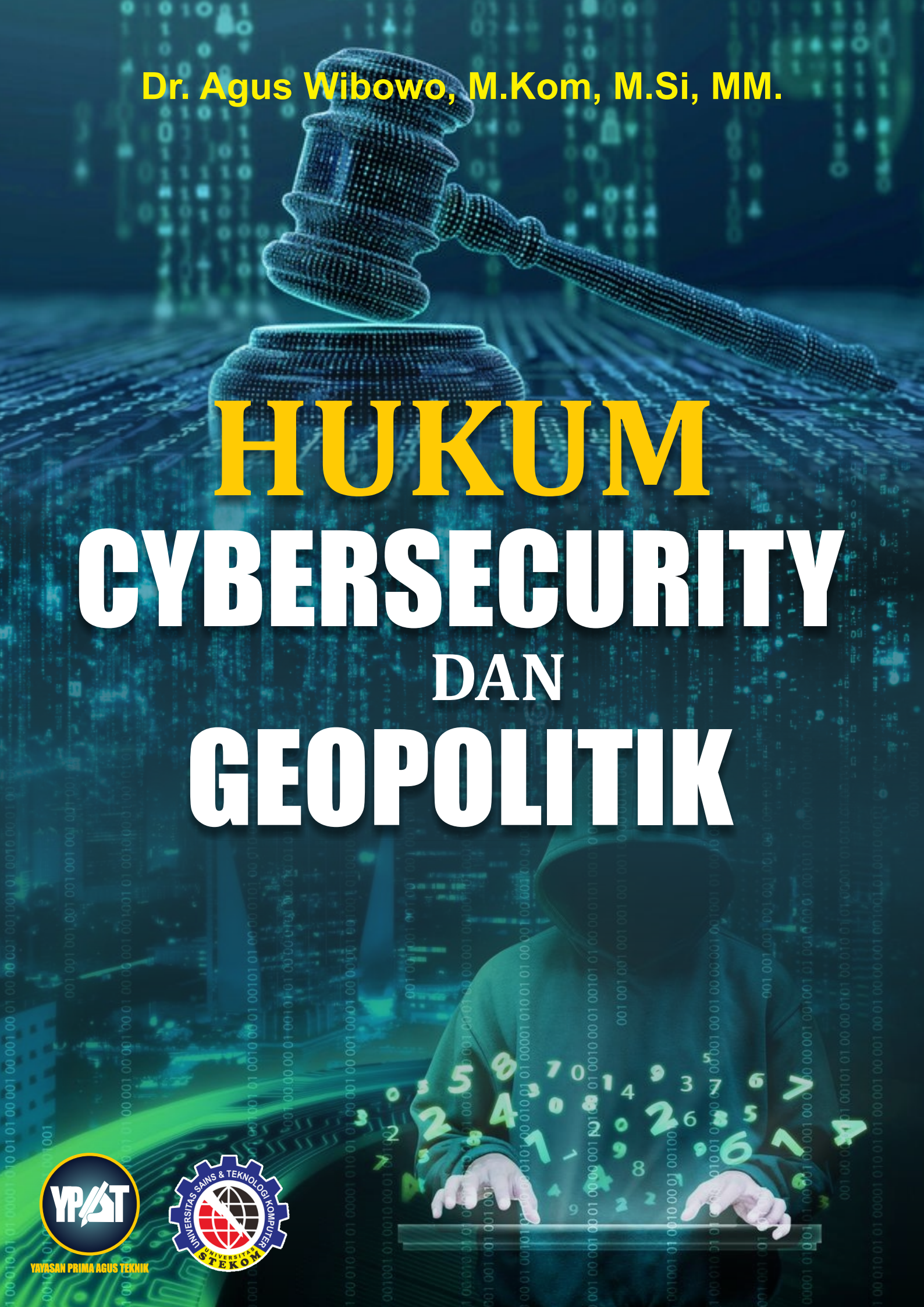
Dr. Agus Wibowo, M.Kom, M.Si, MM.



HUKUM CYBERSECURITY DAN GEOPOLITIK

YAYASAN PRIMA AGUS TEKNIK

Dr. Agus Wibowo, M.Kom, M.Si, MM.

HUKUM CYBERSECURITY DAN GEOPOLITIK

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-97-7 (PDF)
9 786238 642977

HUKUM CYBERSECURITY DAN GEOPOLITIK

Penulis :
Dr. Agus Wibowo, M.Kom, M.Si, MM.

ISBN : 978-623-8642-97-7

Editor :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Anggota IKAPI No: 279 / ALB / JTE / 2023

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga buku berjudul ***Hukum Cybersecurity Dan Geopolitik*** ini dapat diselesaikan dengan baik. Buku ini hadir sebagai upaya untuk memberikan wawasan komprehensif mengenai berbagai aspek keamanan siber yang semakin relevan di era digital, serta kaitannya dengan dinamika geopolitik global.

Buku ini disusun dengan tujuan untuk membantu pembaca memahami konsep mendasar keamanan siber, implikasi hukum internasional, serta pengaruh geopolitik terhadap kebijakan dan strategi keamanan siber. Dalam penyusunan buku ini, penulis berusaha untuk memberikan analisis mendalam melalui berbagai studi kasus, seperti serangan siber terhadap infrastruktur kritis, konflik geopolitik yang melibatkan teknologi, hingga peran individu dan korporasi dalam menghadapi tantangan dunia maya.

Adapun isi buku ini terbagi ke dalam beberapa bab yang saling terintegrasi. Bab pertama memberikan pengantar tentang keamanan siber sebagai dasar pemahaman. Bab-bab berikutnya mengupas definisi keamanan siber, dampak terorisme digital, hingga kasus peretasan yang menjadi perhatian global. Selanjutnya, buku ini membahas hubungan antara geopolitik dan keamanan siber, hukum internasional terkait serangan siber, serta pengembangan kebijakan yang efektif. Bab terakhir menawarkan perspektif masa depan keamanan siber dengan menyoroti potensi kerentanan dan peluang di era digital.

Penulis mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan buku ini, baik secara langsung maupun tidak langsung. Ucapan terima kasih khusus penulis sampaikan kepada para ahli hukum, praktisi keamanan siber, dan akademisi yang telah memberikan masukan berharga untuk memperkaya isi buku ini.

Penulis menyadari bahwa buku ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran dari pembaca sangat penulis harapkan demi penyempurnaan di masa mendatang. Semoga buku ini dapat bermanfaat bagi para pembaca, baik dari kalangan akademisi, praktisi hukum, maupun masyarakat umum yang memiliki minat terhadap isu keamanan siber dan geopolitik.

Akhir kata, semoga buku ini dapat memberikan kontribusi positif dalam meningkatkan pemahaman dan kesadaran akan pentingnya keamanan siber di tengah perkembangan teknologi dan dinamika global.

Selamat Membaca

Semarang, April 2025

Penulis

Dr. Agus Wibowo, M.Kom, M.Si, MM

DAFTAR ISI

BAB 1
PENGANTAR KEAMANAN SIBER

Menakutkan. Membingungkan. Mengganggu. Mengancam.
Tak terlihat. Ampuh. Mengganggu. Invasif.

Daftar di atas hanyalah contoh kata-kata yang terkait dengan keamanan siber dan terorisme siber. Daftar ini mencerminkan kurangnya keseragaman mengenai esensi istilah-istilah tersebut, khususnya definisi yang kurang sempit dan dapat diterapkan. Tentu saja daftar di atas tidak lengkap atau disetujui oleh semua pihak. Itu jelas. Itulah realitas keamanan siber dan terorisme siber. Jelas terorisme siber menimbulkan ancaman yang signifikan; yang jauh dari jelas adalah bagaimana menanggapinya, baik secara proaktif maupun reaktif. Komunikasi dengan para ahli—yang tersebar di seluruh buku ini—menyoroti realitas kembar ini. Meskipun ancaman-ancaman tersebut dipahami secara luas, ada kurangnya suara bulat mengenai minimalisasi ancaman.

Percakapan dengan para akademisi, pakar siber, pejabat pemerintah, dan pemimpin perusahaan di Amerika Serikat, Inggris Raya, dan Israel secara meyakinkan menyoroti kompleksitas ini. Dalam mengeksplorasi realitas kembar ini—ancaman diketahui; tanggapan tidak jelas—saya berfokus pada aspek hukum dan kebijakan keamanan siber. Saya melakukannya karena tidak mungkin memahami keamanan siber secara eksklusif melalui lensa salah satu dari keduanya.

Pendekatan terpadu—hukum dan kebijakan—sangat penting untuk memfasilitasi diskusi mengenai kemungkinan cara untuk melawan ancaman yang ditimbulkan oleh penggunaan siber yang jahat. Yang tidak saya bahas adalah aspek teknis-teknologis siber; menurut rancangannya, hal itu diserahkan kepada orang lain yang lebih kompeten untuk melakukannya. Selama proses penulisan, yang mengejutkan saya adalah pengakuan akan ancaman yang ditimbulkan tetapi rasa ingin mendapatkan jawaban.

Banyak interaksi saya dengan profesional siber—mereka yang terlibat dalam upaya tanpa henti untuk melawan ancaman siber terhadap pelanggan dan klien mereka—berfokus pada tindakan taktis daripada pemikiran strategis yang berbasis luas. Ini bukan kritik, melainkan pengamatan. Mungkin ini adalah realitas ancaman siber. Penekanan pada tanggapan taktis menunjukkan tindakan sementara, pendekatan menang satu hari, kalah hari berikutnya. Dalam banyak hal, itu mirip dengan kontraterorisme operasional tradisional.

1.1 PENDAHULUAN

Tindakan negara-bangsa—pencegahan atau reaktif—tunduk pada konvensi, perjanjian, dan hukum. Yang mempersulit penanggulangan keamanan siber, dibandingkan dengan penanggulangan terorisme operasional tradisional, adalah bahwa target yang dituju mungkin adalah perusahaan-aktor swasta, yang mengakibatkan dilema kritis: Apakah negara-bangsa berkewajiban untuk bertindak atas nama, misalnya, entitas perusahaan yang berkantor

di wilayahnya? Sederhananya: Apakah serangan siber terhadap perusahaan Amerika merupakan serangan terhadap Amerika? Berbeda dari serangan teroris yang mengakibatkan kerusakan fisik—terhadap orang dan properti—serangan siber menimbulkan kerugian bagi infrastruktur, pasar keuangan, dan privasi pribadi.

Meskipun kerusakan fisik dapat terjadi, serangan siber merupakan produk sampingan, tidak seperti serangan fisik yang tujuannya adalah untuk membunuh orang-orang yang tidak bersalah. Ini, tentu saja, merupakan perbedaan yang signifikan antara keduanya. Namun, pada keduanya, aktor nonnegara—terkadang dengan dukungan aktif dan kerja sama negara-bangsa—secara sadar berusaha menimbulkan kerugian, baik secara fisik maupun lainnya. Mungkin, terorisme tradisional lebih mudah diproses karena kerugiannya bersifat fisik dan mendalam. Hal ini berbeda dari serangan siber yang dilakukan dengan baik yang konsekuensinya mungkin tidak langsung dikenali dan dipahami.

Pembahasan mengenai keamanan siber ditandai dengan ketidaknyamanan dan firasat buruk. Banyak percakapan yang saya lakukan dengan berbagai pakar di Amerika Serikat, Israel, dan Inggris mencerminkan adanya batas baru. Namun, tidak seperti citra positif yang secara tradisional dikaitkan dengan batas baru, realitasnya adalah campuran yang mencerminkan, lebih dari apa pun, kekhawatiran mengenai bahaya yang ditimbulkan oleh keamanan siber. Artinya, manfaat nyata dari siber dikurangi—mungkin diimbangi adalah istilah yang lebih baik—oleh terorisme siber.

Ratusan juta orang menikmati Facebook, Instagram, pesan teks, dan bentuk komunikasi kontemporer lainnya. Demikian pula, siber sangat meningkatkan akses kita terhadap informasi dan secara signifikan memudahkan banyak aspek kehidupan kita sehari-hari. Hal ini terdokumentasi dengan baik dan mudah terlihat. Namun, sisi lain dari dunia maya itulah yang menjadi fokus kami dalam buku ini. Meskipun manfaatnya jelas, pertanyaannya adalah bagaimana menanggapi kerugian yang disebabkan oleh mereka yang menggunakan dunia maya untuk tujuan ilegal, berbahaya, dan merusak.

Percakapan tersebut menunjukkan firasat buruk, yang mencerminkan ketidakpastian mengenai sifat khusus serangan di masa mendatang tetapi kepastian mengenai keniscayaan serangan tersebut. Dualitas ini disorot bagi saya dalam percakapan yang saya lakukan pada bulan Mei 2016 dengan seorang eksekutif senior dari sebuah perusahaan Amerika yang baru-baru ini diretas. Eksekutif tersebut mengatakan kepada saya bahwa peretasan tersebut benar-benar tidak mengejutkan dan mencerminkan konsekuensi dari keputusan yang diperhitungkan. Perusahaan tersebut telah menyadari bahwa peretasan merupakan kemungkinan yang berbeda tetapi pencegahannya mahal dan memberatkan.

Oleh karena itu, pejabat eksekutif memutuskan untuk mengambil risiko dan berinvestasi dalam perlindungan minimal dan berharap bahwa peretasan, jika terjadi, tidak akan terlalu parah. Ini berarti bahwa perusahaan bersedia menoleransi peretasan tetapi tidak bersedia menginvestasikan aset keuangan yang signifikan untuk melindungi dirinya sendiri. Sederhananya: beberapa perlindungan dengan sumber daya terbatas dialokasikan dibandingkan dengan perlindungan yang signifikan dengan respons maksimal. Harus diakui, itu adalah pertaruhan.

Konsekuensinya signifikan di berbagai tingkatan: finansial, perhatian pelanggan, dan citra publik. Namun, saya sangat terkejut dengan penilaiannya terhadap tiga biaya tersebut, khususnya terkait reaksi pelanggan. Eksekutif tersebut berbagi dengan saya bahwa pelanggan kurang peduli dari yang diharapkan, mungkin mencerminkan kepasrahan bahwa peretasan—dan konsekuensinya—telah diharapkan oleh publik. Hal ini menimbulkan pertanyaan apakah keamanan siber semakin dianggap dapat diprediksi dan ditoleransi serta diterima dengan rasa kepasrahan.

Mungkin kenyataan yang mungkin itu mencerminkan pemahaman bahwa hilangnya privasi adalah salah satu konsekuensi yang tidak diinginkan dari era digital tempat kita hidup. Pertanyaan tentang privasi dibahas dalam kursus Kelas I Prosedur Pidana. Sebagian besar, tetapi tidak dengan suara bulat, para siswa saya menyatakan pemahaman bahwa privasi mereka telah diminimalkan.

Bagi mereka, itulah realitas mereka. Mungkin ini menjelaskan hal berikut: menurut teman saya, sejumlah besar klien menolak rencana perlindungan data yang ditawarkan perusahaan. Tidak semua, tetapi sebagian besar ditolak.

Saya merasa ini sangat menarik sehubungan dengan proyek buku ini. Dalam beberapa hal, buku ini menangkap kompleksitas luar biasa dari teknologi dan persimpangannya dengan individu. Tantangannya adalah untuk mendamaikan bahaya teknologi dengan keuntungannya; pertanyaannya adalah, bagaimana pertemuan antara keduanya memengaruhi artikulasi dan implementasi strategi keamanan siber? Untuk melakukannya, kita perlu memahami fakta bahwa siber, di tangan yang salah, menimbulkan bahaya yang signifikan bagi individu, perusahaan, negara, dan masyarakat.

Tentu saja, ada peringatan: tidak ada perlindungan yang sangat aman yang tersedia. Serangan akan terjadi, dan kerugian akan terjadi. Dalam beberapa hal, ini adalah inti dari percakapan saya dengan eksekutif perusahaan dan reaksi pelanggannya terhadap peretasan tersebut.

Mereka tidak terkejut; dia juga tidak terkejut. Namun, ini tidak berarti kita harus angkat tangan dalam kesengsaraan kolektif, tidak ada yang bisa dilakukan. Kekalahan kita akan menguntungkan mereka yang berniat menyakiti kita. Pertanyaan yang akan dibahas dalam buku ini adalah sebagai berikut: Langkah apa yang dapat diambil untuk meminimalkan risiko dan dampak serangan?

Seperti yang dibahas di halaman berikutnya, penting bagi kita untuk menyadari perlunya melakukan perubahan besar dalam pendekatan kita terhadap keamanan siber. Meminimalkan ancaman—baik secara proaktif maupun reaktif—memerlukan pengakuan terhadap ancaman dan pembentukan mekanisme kerja sama dan kolaborasi di antara sektor dan populasi yang berbeda, terlepas dari kepentingan yang bersaing apa pun yang mungkin menunjukkan keengganan untuk bergabung.

Konsep kerja sama—baik secara abstrak maupun konkret—sangat penting untuk memerangi keamanan siber. Ini adalah tema yang dibahas dalam buku ini; meskipun pengulangan dapat menjengkelkan, konsep ini sangat penting untuk melawan ancaman yang ditimbulkan oleh serangan siber secara efektif sehingga konsep ini akan kita rujuk pada

sejumlah kesempatan.

Keamanan siber dan terorisme siber bagaikan cermin satu sama lain: Keamanan siber merupakan respons terhadap terorisme siber; terorisme siber hanya dapat diredakan melalui keamanan siber yang efektif. Untuk mengkaji salah satunya, diperlukan pembahasan tentang yang lain. Pembahasannya tidak lengkap. Akan tetapi, pembahasan tersebut terhambat secara signifikan oleh kenyataan yang rumit: istilah-istilah terus berkembang, lebih tidak pasti daripada pasti, dan lebih tidak jelas daripada jelas.

Hal ini memberikan beban yang signifikan bagi penegak hukum, pejabat keamanan nasional, pemimpin perusahaan, dan pembuat kebijakan. Fluktuasi yang melekat pada terminologi tersebut mencerminkan ketidakpastian mengenai ancaman yang ditimbulkan oleh siber. Penggunaan siber yang jahat jelas memiliki dampak yang sangat kuat bagi individu, pemerintah, dan perusahaan. Kesulitan dalam menghadapi ancaman yang ditimbulkan oleh siber bertambah parah karena siber masih relatif baru.

Saat menulis buku ini, saya dikejutkan oleh keengganan para pemimpin perusahaan untuk sepenuhnya mengakui ancaman yang ditimbulkan oleh siber. Saya sulit menerima kenyataan bahwa kegagalan tersebut mencerminkan ketidakmampuan untuk memahami; Sebaliknya, saya percaya bahwa kegagalan tersebut mencerminkan keengganan untuk secara langsung menghadapi ancaman yang ditimbulkan oleh dunia maya dan beban serta tanggung jawab yang dibebankan dunia maya kepada para pemimpin perusahaan. Saya merasa ini sangat meresahkan, jika tidak bisa dikatakan tidak masuk akal. Keyakinan itu berulang kali ditegaskan dalam percakapan dengan para pejabat perusahaan. Terus terang, ini adalah jalan yang berbahaya untuk ditempuh.

Bagaimanapun, ancaman itu nyata dengan konsekuensi yang berpotensi menghancurkan. Mengabaikan—atau sengaja meminimalkan—konsekuensi dari potensi serangan dunia maya sama saja dengan bermain api. Para pemimpin perusahaan dan pejabat pemerintah memiliki kewajiban: perusahaan kepada pemegang saham dan pelanggan, dan pemerintah kepada warga negara. Ini adalah kewajiban yang tidak dapat dikurangi atau dikurangi. Memahami ancaman yang ditimbulkan oleh dunia maya mengharuskan kita untuk melihat langsung ke mata harimau.

Metafora ini tidak berlebihan; penggunaan dunia maya yang berbahaya, secara harfiah, adalah harimau yang menimbulkan ancaman signifikan bagi masyarakat kontemporer. Secara harfiah, tidak ada pilihan. Untuk melakukannya, diperlukan kerja sama di antara para pelaku yang berbeda. Ini terdengar sederhana dan logis. Namun, kerja sama harus terjadi di antara para aktor yang secara alamiah saling curiga atau yang DNA organisasinya tidak setara dengan upaya kerja sama dengan pihak lain. Kedua kenyataan tersebut sangat disayangkan.

Sayangnya, bukan hanya para pemimpin perusahaan yang harus diperhatikan. Beberapa tahun yang lalu, sebuah pertemuan yang menyadarkan terjadi saat makan siang dengan FBI dan pejabat penegak hukum setempat. Para pejabat FBI sangat jelas bahwa kerja sama dengan yang terakhir tidak akan berhasil. Saya tercengang dengan keterusterangan pernyataan tersebut; tidak perlu dikatakan bahwa para pejabat setempat merasa terhina. Apakah itu niat para pejabat FBI tidak jelas; terus terang, itu juga tidak relevan. Yang relevan

adalah isinya: kerja sama penegakan hukum federal-lokal bermasalah dan menantang, untuk sedikitnya.

Namun, keamanan siber yang efektif mengharuskan penegak hukum—federal, negara bagian, dan lokal—mengakui tugas mereka kepada publik, dan memerlukan kerja sama yang dilembagakan. Artinya, tingkat kerja sama—baik minimal maupun maksimal—tidak dapat bergantung pada keinginan dan fantasi individu tertentu. Tanpa pendekatan keamanan siber yang komprehensif dan dilembagakan, terorisme siber akan menjadi yang teratas selama bertahun-tahun mendatang.

Namun, kerja sama harus terjadi di luar penegakan hukum yang didefinisikan secara sempit; perusahaan, lembaga negara, dan penegak hukum harus melakukan upaya yang dilembagakan untuk mengembangkan pendekatan sistematis dan sistemik guna meminimalkan ancaman yang ditimbulkan oleh terorisme siber.

Percakapan telepon dengan pejabat penegak hukum setempat menyoroti tantangan yang dihadapi. Dengan cara yang sangat langsung dan jujur, pejabat tersebut dengan tegas menyoroti dua kelemahan kritis terkait pengembangan keamanan siber yang efektif: perebutan wilayah yurisdiksi antara berbagai lembaga lokal dan kurangnya kemauan perusahaan untuk bekerja sama dengan penegak hukum. Saya meminta contoh dan dia memberikan dua contoh, satu untuk setiap paradigma. Keduanya menyedihkan. Pejabat itu menceritakan bahwa dalam operasi pencucian uang yang rumit, dua lembaga penegak hukum lokal (bukan negara bagian atau federal) yang berbeda, termasuk lembaganya, gagal bekerja sama. Ketika saya mendesaknya untuk mengetahui penyebabnya, jawabannya jujur dan menyusahkan: karena tidak menguntungkan kepentingan kami untuk melakukannya. Kami berbicara pada dua kesempatan berbeda; pada keduanya, ia mengulang cerita dan penjelasannya.

Saya yakin ia memahami bahwa perilaku kedua lembaga tersebut membahayakan publik. Pada tingkat tertentu, jawabannya setara dengan frasa yang menjengkelkan, begitulah adanya. Menjengkelkan? Tidak diragukan lagi. Tidak bertanggung jawab? Benar-benar. Menuntut perubahan yang mendalam? Benar-benar. Yang mengejutkan saya adalah kurangnya otoritas kelembagaan yang menyeluruh, apalagi kepemimpinan di lapangan, yang dapat—secara harfiah—memaksa kerja sama. Itu adalah kelemahan yang kuat dalam kebijakan dunia maya.

Cerita kedua difokuskan pada perusahaan.

Pejabat itu tidak henti-hentinya mengkritik kepemimpinan perusahaan. Ia menyalahkan mereka karena berfokus pada pendapatan kuartalan jangka pendek daripada kerentanan jangka panjang. Meskipun mengakui kewajiban kepada pemegang saham merupakan kewajiban utama para pemimpin perusahaan, ia menolak paradigma hitam-putih yang menyatakan bahwa perusahaan memilih untuk tidak bekerja sama dengan penegak hukum segera setelah terjadinya penetrasi dunia maya. Desakannya mengenai masalah ini menyentuh hati saya. Saya sepenuhnya setuju dengannya.

Saya ngelantur: Beberapa tahun yang lalu, saya ditunjuk sebagai penasihat hukum untuk Gugus Tugas Kongres yang diberi mandat untuk mengembangkan keamanan dalam

negeri nasional. Saya bekerja di bawah naungan Komite Keamanan Dalam Negeri DPR. Penunjukan tersebut mencakup pemberian kesaksian di hadapan Komite dan penyerahan makalah penelitian. Berikut ini adalah kutipan dari salah satu makalah; secara analogi, hal tersebut secara langsung relevan dengan pertanyaan tentang kerja sama yang menjadi inti penting buku ini:

Menganalisis ancaman

1. *Apa ancaman yang dihadapi negara?*
2. *Siapa yang bertanggung jawab untuk merencanakan ancaman?*
3. *Siapa yang bertanggung jawab untuk membiayai ancaman?*
4. *Siapa yang bertanggung jawab untuk melaksanakan ancaman?*
5. *Kapan ancaman kemungkinan akan dilaksanakan?*

Gambar 1.1 Menganalisis ancaman.

Langkah pertama dalam menciptakan tindakan antiterorisme yang efektif adalah menganalisis ancaman. Untuk itu, pertanyaan yang diajukan pada Gambar 1.1 harus dijawab.

Setelah pertanyaan-pertanyaan ini dijawab, ancaman dapat ditempatkan pada kontinum yang akan segera terjadi dengan pemahaman bahwa satu ancaman besar mungkin terdiri dari ancaman yang lebih kecil dan lebih mudah dikelola. Kontinum yang akan segera terjadi memiliki empat ancaman utama sebagai tolok ukur: segera terjadi, dapat diperkirakan, jangka panjang, dan tidak pasti.

Ancaman yang akan segera terjadi adalah ancaman yang akan segera terjadi; sebagai contoh, laporan intelijen terkini menunjukkan bahwa sebuah bom akan diledakkan besok pukul 9:11 pagi di terminal domestik di Bandara JFK.

Ancaman yang dapat diperkirakan adalah ancaman yang akan terjadi dalam waktu dekat (tanpa kekhususan); oleh karena itu, ancaman tersebut lebih jauh dari ancaman yang akan segera terjadi. Misalnya, ancaman yang dapat diperkirakan akan didasarkan pada intelijen yang valid, yang menunjukkan teroris akan segera mulai membawa bahan peledak ke pesawat dalam bentuk zat cair.

Ancaman jarak jauh adalah ancaman yang dapat mencapai hasil pada waktu yang tidak diketahui; misalnya, pelatihan teroris tanpa tindakan operasional yang direncanakan secara khusus akan masuk dalam kategori ini.

Ancaman yang tidak pasti merupakan ancaman yang menimbulkan ketakutan umum akan ketidakamanan. Sebagai akibat dari pengeboman kereta api di Inggris dan Spanyol, para pelancong di Indonesia mungkin secara potensial atau mungkin merasa tidak aman saat naik kereta api tanpa keamanan yang diperkuat. Hal ini akan berlaku terlepas dari apakah ada intelijen yang valid, yang menunjukkan teroris bermaksud untuk menargetkan kereta api.

Dalam menentukan di mana ancaman tertentu cocok dengan kontinum yang akan segera terjadi, keseimbangan harus dicapai antara keamanan nasional dan kepentingan hak yang bersaing. Gambar 1.2 berikut menggambarkan kontinum yang akan segera terjadi secara grafis. Ancaman serangan teroris dicantumkan dari kiri ke kanan, berkembang dari yang akan

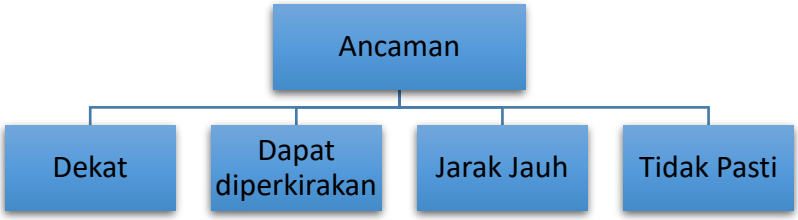
segera terjadi ke yang tidak pasti. Kolom vertikal di sebelah kiri mencantumkan tujuh faktor yang harus diseimbangkan oleh tindakan kontraterorisme dalam mempertimbangkan ancaman-ancaman ini.

Faktor-faktor penyeimbang tersebut meliputi kerusakan kolateral, kebebasan sipil, intelijen yang valid, frekuensi pelaporan, tanggung jawab fiskal, masalah geopolitik, dan supremasi hukum. Memahami faktor-faktor ini sangat penting; penjelasan terperinci diuraikan di bawah bagan. Batang-batang segitiga di badan grafik mewakili prioritas relatif yang diberikan pada masing-masing faktor ini jika terjadi ancaman serangan teroris yang akan segera terjadi, dapat diperkirakan, dalam jangka panjang, atau tidak pasti. Semakin tebal batang segitiga, semakin besar pentingnya faktor yang sesuai.

Misalnya, batang segitiga yang mewakili faktor pertama, kerusakan kolateral, lebih tebal untuk ancaman yang akan segera terjadi dan menjadi lebih tipis saat mencapai ancaman yang tidak pasti. Batang ini menunjukkan bahwa kerusakan kolateral lebih mungkin terjadi untuk tindakan kontraterorisme yang akan segera terjadi daripada untuk tindakan yang dapat diperkirakan, dalam jangka panjang, atau tidak pasti.

Kuncinya adalah memahami pentingnya bagaimana menyeimbangkan faktor-faktor yang bersaing menentukan efektivitas (Gambar 1.2 dan 1.3). Dalam banyak hal, percakapan saya dengan pejabat hukum setempat merupakan bagian penting dari proyek buku ini. Dorongan kedua adalah undangan dari National Cyber Partnership nirlaba untuk mengajar kursus, perspektif global tentang kejahatan dunia maya dan terorisme dunia maya, sebagai bagian dari program pelatihan jalur cepat inovatif yang menargetkan militer yang sedang dalam masa transisi dan veteran yang mencari pekerjaan di industri dunia maya.

Dengan berfokus pada aspek hukum dan kebijakan keamanan dunia maya, saya berusaha menyoroti isu-isu penting yang akan menjadi pokok bahasan diskusi bagi keempat audiens yang saya tuju: pemimpin perusahaan, pejabat penegak hukum, pembuat kebijakan, dan masyarakat umum. Tidak ada audiens yang lebih menonjol atau relevan daripada yang lain. Dalam banyak hal, keempat audiens perlu memahami bagaimana dunia maya memengaruhi dirinya sendiri dan tiga audiens lainnya.



Gambar 1.2 Karakteristik ancaman.

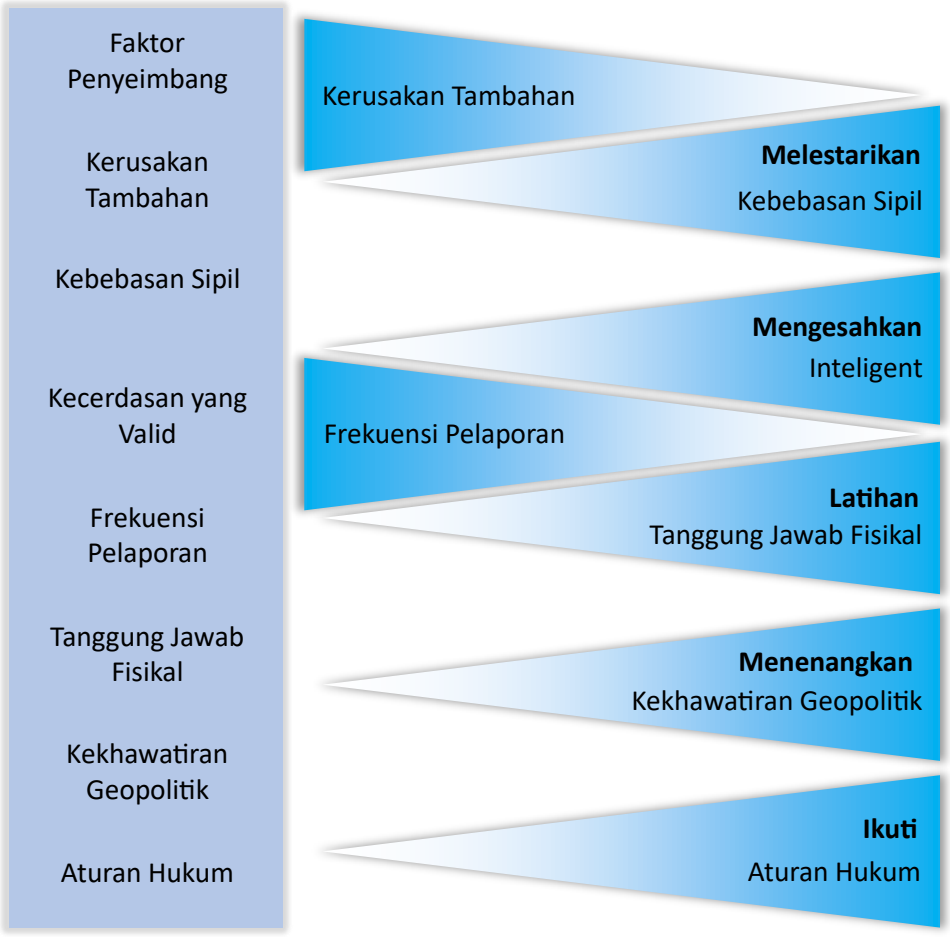
Ancaman yang ditimbulkan oleh penjahat dunia maya dan terorisme dunia maya sangat memengaruhi kita semua. Itu tidak dimaksudkan sebagai pernyataan berlebihan atau mantra kosong.

Saya teringat akan kenyataan itu ketika sebuah email muncul di kotak masuk saya pada bulan Desember 2015. Pengirimnya adalah perusahaan kartu kredit saya. Sistem pelacakan

mereka yang sangat efektif dan mengesankan, yang didasarkan pada algoritma yang canggih, memicu kecurigaan bahwa akun saya telah diretas. Pembelian tersebut, baik konten maupun lokasinya, tidak mencerminkan kebiasaan tradisional saya. Sistemnya benar: Saya tidak pernah mengunjungi lokasi yang dimaksud dan tidak melakukan pembelian.

Ini berarti bahwa sistem tersebut berfungsi. Berbicara dengan manajer akun saya, saya mengungkapkan rasa terima kasih saya atas keefektifan model mereka. Ketika kami mengakhiri percakapan kami, saya—sekali lagi—dikejutkan oleh betapa umum terjadinya persimpangan yang tidak menguntungkan antara dunia maya dan penggunaannya yang tidak diinginkan.

Meskipun saya hanya sedikit kesal, ceritanya sangat menarik. Ceritanya menarik karena mengingatkan kita betapa dunia maya memengaruhi kehidupan kita sehari-hari, entah kita menginginkannya atau tidak.



Gambar 1.3 Faktor penyeimbang.

Pertanyaan yang lebih luas yang dibahas dalam buku ini jauh melampaui ketidaknyamanan yang saya alami. Kartu baru saya tiba di pos dalam beberapa hari; saya tidak mengalami kerugian finansial. Semuanya baik-baik saja.

Yah, tidak juga. Penjahat dunia maya dan teroris dunia maya canggih, maju, dan bertekad. Itulah kenyataannya. Bagaimana keempat audiens yang disebutkan di atas mengatasi ancaman ini—semoga secara proaktif, daripada reaktif—adalah kunci untuk

meminimalkan penggunaan dunia maya yang jahat.

Saya bertekad untuk menyoroti isu-isu kritis dalam buku ini dengan harapan dapat memicu percakapan di antara audiens yang berbeda. Untuk melakukannya, seorang penulis paling baik—menurut saya—mendapatkan layanan dengan menarik perhatian pada isu-isu kritis dan menyarankan cara-cara khusus untuk menyelesaikannya.

Dalam upaya menjangkau audiens yang berbeda, buku ini mengadopsi nada percakapan; buku ini bukanlah buku teks klasik yang ditujukan khusus untuk akademisi atau buku panduan, yang hanya berfokus pada perusahaan dan penegakan hukum. Tujuannya adalah untuk secara sengaja bersifat interdisipliner dan multidisipliner (keduanya adalah istilah yang berbeda) guna membahas aspek hukum dan kebijakan keamanan siber.

Buku ini disusun sedemikian rupa sehingga dapat menghidupkan kompleksitas keamanan siber. Hal ini dilakukan melalui serangkaian cerita pendek, yang dibuat sebagai latihan yang dimaksudkan untuk menghadapkan pembaca dengan dilema yang terlibat dalam keamanan siber. Cerita pendek tersebut, dapat dikatakan, merupakan contoh pengajaran yang lebih efektif daripada sekadar teks; cerita pendek tersebut merupakan alat untuk menghidupkan masalah tersebut. Yang penting untuk ditambahkan adalah bahwa cerita pendek tersebut juga berlaku untuk audiens korporat, baik eksekutif tingkat C maupun eksekutif yang kurang senior.

Demikian pula, saya berharap agar penegak hukum—lokal, negara bagian, dan nasional dan mitra terkait di negara lain—akan menganggap cerita pendek ini relevan dalam upaya berkelanjutan mereka untuk lebih memahami keamanan siber dalam upaya meningkatkan kemampuan mereka untuk meminimalkan dampak buruknya. Akhirnya, saya berharap masyarakat umum akan menganggap diskusi dan cerita pendek ini bermanfaat dalam meningkatkan pemahaman mereka tentang ancaman yang signifikan ini.

Cerita pendek ini menyoroti ancaman keamanan siber yang terus-menerus dan evolusi ancaman yang cepat terhadap berbagai audiens. Kedekatan keamanan siber berkembang pesat dengan begitu banyak ketidakpastian. Dengan demikian, cerita pendek ini dimaksudkan untuk memfasilitasi diskusi dan reaksi terhadap peristiwa yang sebenarnya dan mungkin terjadi. Selain itu, cerita pendek ini akan digunakan untuk mendorong percakapan di antara individu, rekan bisnis, dan lembaga penegak hukum serta pemerintah.

Dalam semangat ini, Bab 8 sebagian besar terdiri dari cerita pendek. Ini disengaja. Hal ini dimaksudkan untuk memaksakan penerapan dan proses saat pembaca menghadapi apa yang ditulis dalam bab-bab sebelumnya dan bagaimana menerapkannya dalam skenario kehidupan nyata.

Secara keseluruhan, tujuan dari sketsa-sketsa ini adalah untuk menyoroti kompleksitas keamanan siber, memfasilitasi diskusi, dan mudah-mudahan mengarah pada penyelesaian banyak masalah yang tidak memiliki akhir. Sketsa-sketsa ini relevan bagi empat audiens yang berbeda: pemimpin perusahaan, akademisi, penegak hukum, dan masyarakat umum.

Dengan semangat ini, saya berharap bahwa materi yang diajarkan dalam buku ini akan dipandang sebagai praktik terbaik yang direkomendasikan. Kata direkomendasikan sengaja dipilih: mengingat kompleksitas yang menyertai dunia maya, jika proposal atau pokok bahasan

diskusi tertentu berkontribusi untuk menyelesaikan teka-teki tertentu, maka tujuan saya menulis buku ini akan tercapai. Oleh karena itu, saya bermaksud agar pembaca akan melihat pokok-pokok diskusi sebagaimana dimaksudkan untuk memfasilitasi pemeriksaan yang jujur dan terbuka terhadap ancaman yang ditujukan kepada individu, perusahaan, dan pemerintah. Untuk memfasilitasi diskusi ini, buku ini dibagi sebagai berikut.

1.2 SUSUNAN BUKU

Bab Dua: Apa Itu Keamanan Siber?

Definisi sangat penting untuk membuat dan menerapkan kebijakan siber yang didasarkan pada aturan hukum. Untuk tujuan tersebut, keamanan siber adalah upaya untuk melindungi informasi, komunikasi, dan teknologi dari bahaya yang disebabkan baik secara tidak sengaja maupun sengaja; penting untuk menekankan bahwa serangan siber sangat berbeda dari serangan fisik. Lebih jauh, keamanan siber adalah upaya untuk memastikan kerahasiaan, integritas, dan ketersediaan data, sumber daya, dan proses melalui penggunaan kontrol administratif, fisik, dan teknis.

Bab Tiga: Geopolitik Dan Keamanan Siber

Dalam bab ini, hubungan antara keamanan siber dan geopolitik akan diperiksa dengan menganalisis contoh-contoh tertentu yang mencerminkan kompleksitas pertemuan keduanya. Analisis akan menyentuh hukum internasional, khususnya pembelaan diri dan proporsionalitas. Pengambilan keputusan negara-bangsa, yang mencerminkan prediktabilitas dan konsistensi, secara signifikan meningkatkan tatanan global. Namun, ancaman—baik yang nyata maupun yang dipersepsikan—secara dramatis memengaruhi stabilitas regional dan global. Dalam konteks ini, menilai bagaimana negara-bangsa merespons, baik secara unilateral, bilateral, atau multilateral, terhadap titik-titik krisis tertentu sangat penting untuk memahami dampak praktis dari pertimbangan geopolitik.

Bab Empat: Hukum Internasional Dan Latar Belakang Keamanan Siber

Pertanyaan penting yang perlu diajukan adalah apakah hukum berlaku untuk keamanan siber atau tidak, dan jika hukum berlaku untuk keamanan siber, apa saja struktur hukum yang relevan?

Bagaimana negara-bangsa merespons serangan siber mencerminkan esensi hukum internasional, yang didasarkan pada hak negara-bangsa untuk membela diri—ketika diserang—sesuai dengan Pasal 51 Piagam PBB.

Bab Lima: Pengembangan Dan Implementasi Kebijakan Keamanan Siber

Dalam bab ini, fokusnya adalah pada pengembangan dan implementasi kebijakan keamanan siber. Kebijakan memerlukan analisis menyeluruh dan interdisipliner terhadap masalah tersebut untuk mengembangkan respons paling efektif terhadap ancaman yang ditimbulkan oleh serangan siber.

Bab Enam: Bagaimana Perusahaan Menanggapi Kejahatan Siber?

Perusahaan besar dan kecil rentan terhadap peretas dan jelas diserang, meskipun tidak setiap hari, tetapi sangat teratur. Beberapa serangan sangat besar, memengaruhi puluhan juta pelanggan yang privasinya jelas dilanggar. Informasi pribadi mereka diretas; mereka rentan,

terekspos, dan khawatir, jika tidak marah.

Bagaimana perusahaan menanggapi keamanan siber sangat penting. Kepentingan yang luar biasa ini mencakup pertimbangan taktis dan strategis. Tidaklah berlebihan untuk mengatakan bahwa ancaman siber adalah titik fokus utama perusahaan saat ini. Jika tidak, maka itu mencerminkan salah tafsir yang serius terhadap bahaya yang jelas dan nyata. Bahaya itu—yang nyata bagi pengamat yang paling biasa—tidak dapat disangkal.

Bab Tujuh: Bagaimana Individu Dapat Memitigasi Keamanan Siber?

Beralih dari perusahaan, selanjutnya kita dapat mempertimbangkan siapa saja yang membentuk perusahaan. Setiap individu dapat mengurangi ancaman, bahaya, dan kerentanan yang ditimbulkan oleh keamanan siber. Masing-masing dari kita, secara individu, memainkan peran dalam konteks keamanan siber. Berikut ini adalah contoh kecilnya. Banyak dari kita yang pernah diretas, baik kartu kredit kita dibobol atau email kita diretas. Jadi, masing-masing dari kita memiliki pengalaman pribadi. Keamanan siber dapat dilihat pada tingkat pribadi dan umum.

Bab Delapan: Bagaimana Penegakan Hukum Memitigasi Keamanan Siber?

Bab ini membahas hubungan antara penegakan hukum dan keamanan siber, khususnya bagaimana penegakan hukum dapat bekerja lebih efektif dengan perusahaan, individu, dan negara untuk membantu mereka melindungi diri dari serangan siber. Penekanannya adalah pada apa yang dapat dilakukan penegakan hukum untuk mengurangi keamanan siber atau ancaman siber.

Bab Sembilan: Keamanan Siber Di Masa Depan

Bab ini menekankan keamanan siber di masa depan, besarnya risiko, dan langkah-langkah yang harus diambil untuk mengurangi risiko tersebut. Penggunaan berbagai skenario akan membuat percakapan lebih realistis dan tidak terlalu teoritis. Hal ini dilakukan untuk membantu pembaca memahami keamanan siber pada tingkat yang paling praktis.

Bab Sepuluh: Isu Sosial

Pada halaman-halaman sebelumnya, sejumlah isu yang relevan dengan keamanan siber telah diangkat dengan fokus khusus pada pertanyaan hukum dan kebijakan. Meskipun pertanyaan teknis merupakan hal yang paling penting, pertanyaan tersebut bukanlah fokusnya. Pertanyaan yang lebih besar, dan karenanya diberi judul "ISU SOSIAL", adalah ke mana kita akan melangkah dari sini? Mungkin, lebih dari apa pun, ini adalah titik kritis pertanyaan bagi pembaca dan penulis.

BAB 2
PENGERTIAN KEAMANAN SIBER?

2.1 PENDAHULUAN

Pertanyaan yang diajukan dalam judul bab ini menjadi pokok bahasan diskusi, dugaan, dan tulisan yang tak ada habisnya. Istilah ini banyak dibahas, menimbulkan kecemasan besar dan menimbulkan lebih banyak pertanyaan daripada jawaban. Baik pakar maupun nonpakar sama-sama menyuarakan kekhawatiran yang mencerminkan kerentanan, perasaan bahwa privasi mereka terancam dan bahwa kekuatan tak terlihat sedang menjauh. Privasi yang diminimalkan adalah realitas zaman modern yang digerakkan dan berbasis teknologi. Pertanyaan dalam konteks keamanan siber adalah sebagai berikut: Apakah minimisasi menimbulkan ancaman, membahayakan individu dan masyarakat? Asumsi umum menunjukkan bahwa jawabannya adalah ya.

Namun, teknologi modern juga memiliki manfaat besar yang, tanpa diragukan lagi, telah berdampak dramatis, jika tidak meningkatkan, kehidupan kita. Contoh-contohnya berlimpah dan familier bagi semua orang, mulai dari yang biasa hingga yang rumit. Dalam banyak hal, kita semua mendapat manfaat dari hidup di zaman teknologi. Namun, manfaat tersebut sayangnya diimbangi oleh konsekuensi negatif yang berasal dari penyalahgunaan—terutama yang disengaja—teknologi.

Penyalahgunaan ini menjadi fokus buku ini; fokus pada penggunaan teknologi yang negatif memfasilitasi diskusi mengenai bagaimana masyarakat dan individu dapat membangun mekanisme perlindungan secara lebih efektif. Melakukan hal itu membutuhkan pengakuan bahwa bahaya yang berasal dari penerapan teknologi yang jahat menuntut perhatian individu dan kolektif mereka.

Dalam perjalanan meneliti dan menulis buku ini, saya tersirat bahwa ancaman dunia maya dibesar-besarkan, dan bahwa keamanan dunia maya mencerminkan industri rumahan yang salah kaprah. Meskipun orang-orang yang waras dapat tidak setuju, saya menganggap perspektif itu tidak benar. Sekilas pandang pada tajuk berita dengan tegas menunjukkan bahwa ancaman itu tidak dapat diabaikan atau berlalu begitu saja. Justru sebaliknya.

Sejauh mana bahayanya bergantung pada apa, dan kapan, tindakan perlindungan dilakukan. Ini adalah pedang bermata dua: Perlindungan dibenarkan jika sumber bahaya diidentifikasi dengan benar. Namun, tindakan gegabah terhadap ancaman yang dirasakan atau potensial menimbulkan pertanyaan yang meresahkan mengenai penerapan kekuatan negara secara preemptif dan tidak proporsional. Mirip dengan ancaman dan bahaya tradisional, upaya untuk mengurangi potensi bahaya tunduk pada pembatasan yang diberlakukan oleh hukum domestik dan internasional.

Transisi dari peperangan tradisional ke terorisme siber dan peperangan siber mencerminkan perubahan signifikan dalam sifat konflik dan cara serta tata krama pertahanan. Jika peperangan tradisional antara negara-bangsa melibatkan tank, pesawat, dan kapal, maka serangan siber, baik yang dilakukan oleh negara-bangsa atau aktor non-negara, memerlukan

kecanggihan dan kecerdasan laptop dan komputer.

Serangan siber ditujukan pada infrastruktur negara-bangsa tetapi juga dapat ditujukan pada infrastruktur yang bergerak maju. Seperti yang akan dibahas di halaman-halaman berikutnya, mencegah dan menanggapi serangan siber menimbulkan tantangan signifikan bagi negara-bangsa. Siber—yang mencakup keamanan siber, terorisme siber, dan serangan siber—mencerminkan teknologi mutakhir.

Sepuluh tahun lalu, apalagi dua puluh tahun lalu, percakapan ini sebagian besar akan dipandang futuristik. Perubahan dari peperangan tradisional menjadi terorisme konvensional dan siber mencerminkan perubahan signifikan dalam cara konflik dilakukan. Dari sudut pandang para pengambil keputusan, transisi ini dramatis; dari sudut pandang publik, serangan siber merupakan sumber kekhawatiran dan ketidaknyamanan yang sangat besar.

Konflik, baik saat ini maupun di tahun-tahun mendatang, terutama akan berfokus pada aktor non-negara yang terlibat dengan aktor negara. Inilah esensi terorisme sebagaimana terwujud dalam serangkaian serangan yang dilakukan terhadap negara-bangsa dan warga sipil yang tidak bersalah. Kemampuan siber aktor non-negara dan negara membebani organ-organ negara-bangsa—militer, komunitas intelijen, dan penegak hukum—untuk menciptakan tindakan balasan defensif dan ofensif yang canggih. Respons tersebut paling tepat digambarkan sebagai keamanan siber.

2.2 DEFINISI DAN DAMPAK KEAMANAN SIBER

Definisi sangat penting untuk membuat dan menerapkan kebijakan siber yang didasarkan pada aturan hukum. Untuk tujuan tersebut, keamanan siber adalah upaya untuk melindungi informasi, komunikasi, dan teknologi dari bahaya yang disebabkan baik secara tidak sengaja maupun sengaja; yang penting untuk ditekankan adalah bahwa serangan siber sangat berbeda dari serangan fisik. Lebih jauh, keamanan siber adalah upaya untuk memastikan kerahasiaan, integritas, dan ketersediaan data, sumber daya, dan proses melalui penggunaan kontrol administratif, fisik, dan teknis.

Serangan siber adalah tindakan agresif yang disengaja dan langsung yang dimaksudkan untuk merusak infrastruktur penting. Lebih jauh, serangan siber adalah setiap upaya yang disengaja untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, sumber daya, atau proses melalui penggunaan sarana elektronik. Sasaran yang jelas berkisar dari sistem air atau sistem transportasi kota hingga rekening bank atau kartu kredit seseorang. Meskipun peretasan rekening bank pribadi tidak diragukan lagi menjengkelkan, dampak serangan siber pada sistem air kota atau infrastruktur lalu lintas udara dapat menyebabkan kekacauan, yang jauh melampaui tindakan terorisme konvensional, terlepas dari kenyataan bahwa dampak mendalamnya sangat berbeda.

Misalnya, beberapa tahun yang lalu, saya bertemu dengan seorang wakil presiden senior dari sebuah lembaga keuangan terkemuka di AS yang menceritakan bahwa sebuah organisasi teroris telah berhasil meretas firewall canggih dan membuat lebih dari 400 akun fiktif dengan menggunakan nomor jaminan sosial fiktif yang sama. Sebagai hasil dari peretasan yang sangat berhasil itu, kelompok tersebut berhasil mentransfer ratusan juta dolar secara

ilegal dari Amerika Serikat ke Timur Tengah melalui sejumlah negara yang berbeda. Insiden tersebut menyoroti bahwa satu serangan siber dapat, dalam jangka panjang, memiliki dampak strategis yang jauh lebih besar, daripada tindakan terorisme tradisional tertentu yang mengakibatkan hilangnya nyawa yang tidak bersalah.

Keamanan siber dimaksudkan untuk melindungi masyarakat dan individu dari serangan yang sangat canggih dan agresif; pertanyaan pentingnya adalah menentukan prioritas dari apa yang ingin kita lindungi. Jawabannya sangat rumit karena penentuan prioritas memerlukan jawaban atas serangkaian pertanyaan, termasuk yang diberikan pada Gambar 2.1.

- *Sejauh mana negara wajib melindungi warga sipil?*
- *Sejauh mana negara wajib melindungi infrastruktur publik?*
- *Sejauh mana negara wajib melindungi aset luar negeri, publik dan swasta?*

Gambar 2.1 Pertanyaan prioritas.

Dengan keamanan siber sebagai perlindungan informasi, komunikasi, dan teknologi dari bahaya, dan serangan siber didefinisikan sebagai tindakan agresif yang disengaja dan langsung yang dimaksudkan untuk merusak infrastruktur penting, setiap bagian dari definisi tersebut harus dipecah dalam menentukan apakah serangan siber telah terjadi, dan apakah keamanan siber terlibat.

Pertama, pertimbangkan contoh berikut: Seseorang mengakses rekening banknya dan menyadari bahwa uangnya telah hilang. Tidak hanya itu, ia menerima surat penagihan dan panggilan dari lembaga yang mengklaim bahwa mereka berutang sejumlah besar uang di berbagai kota. Orang ini adalah korban pencurian identitas. Pencurian identitas adalah penyalahgunaan nomor jaminan sosial seseorang. Apakah itu sesuai dengan definisi keamanan siber—dengan perlindungan informasi, komunikasi, dan teknologi dari bahaya? Tentu saja. Penyalahgunaan nomor jaminan sosial seseorang berkaitan dengan kurangnya perlindungan informasi dari bahaya.

Apakah pengalaman itu sesuai dengan definisi serangan siber—dengan tindakan agresif langsung dan disengaja yang dimaksudkan untuk merusak infrastruktur penting? Infrastruktur kritis adalah kata kunci dalam analisis ini. Tidak diragukan lagi bahwa mencuri informasi pribadi seseorang, khususnya nomor jaminan sosial mereka, adalah tindakan agresif yang langsung dan disengaja yang dimaksudkan untuk merugikan individu tersebut. Namun, apakah individu tersebut termasuk dalam definisi infrastruktur kritis? Itu akan dibahas dalam bab-bab selanjutnya. Kedua, perhatikan contoh berikut. Seseorang menyalakan pancuran untuk bersiap berangkat kerja dan, sayangnya, tidak ada air. Orang tersebut tahu bahwa mereka telah membayar tagihan, dan air seharusnya mengalir, tetapi tidak. Ternyata—sebuah organisasi telah membobol komputer di stasiun air setempat—menghentikan semua akses air ke masyarakat. Apakah itu termasuk dalam definisi keamanan siber—dengan perlindungan informasi, komunikasi, dan teknologi dari bahaya? Tentu saja. Penyalahgunaan sistem air dalam menghentikan air berkaitan dengan kurangnya perlindungan komunikasi dan teknologi

dari bahaya.

Apakah pengalaman itu sesuai dengan definisi serangan siber—dengan fokus pada aspek definisi yang berhubungan dengan infrastruktur penting? Tentu saja. Memutus akses masyarakat terhadap air tidak diragukan lagi merupakan tindakan agresif yang langsung dan disengaja yang dimaksudkan untuk merusak infrastruktur penting masyarakat: pasokan airnya. Dengan demikian, contoh ini lebih mudah dimasukkan ke dalam ranah pelanggaran keamanan siber sebagai korban serangan siber.

Seperti yang terlihat di atas pada kedua contoh, sulit untuk memastikan apakah keamanan siber telah dilanggar dan apakah itu cukup sebagai serangan siber. Namun, yang tidak sulit untuk dipastikan adalah seberapa dahsyat dampak serangan siber, dan seberapa cepat hal itu dapat memengaruhi sejumlah besar individu.

Jawaban mudahnya adalah bahwa tugas mendasar negara-bangsa adalah melindungi penduduk sipil yang tidak bersalah dari bahaya langsung. Inilah mengapa keamanan siber begitu rumit karena serangan siber tidak harus selalu berupa serangan langsung. Meskipun peretasan akun kartu kredit saya merupakan serangan langsung (terhadap saya), kemungkinan sistem air kota akan diserang mengharuskan pejabat kota, negara bagian, dan federal untuk mengevaluasi dampak pada berbagai tingkatan serangan siber.

Dalam konteks prioritas dan penentuan prioritas, keamanan siber mengharuskan penentuan kembali prioritas sumber daya yang sudah terbatas. Keamanan siber rumit tidak hanya dalam hal tingkat serangan tetapi juga kerusakan jangka panjang yang dapat disebabkan oleh serangan tersebut.

Untuk memperjelas maksudnya: Serangan siber, meskipun berbeda dari terorisme fisik, membawa terorisme ke pintu depan negara. Daripada melibatkan teroris di Pakistan, Suriah, dan Yaman, kerentanan siber tercermin dalam serangan terhadap aset domestik yang berharga. Realitas serangan siber adalah bahwa orang yang bertanggung jawab atas serangan tersebut secara fisik dapat berada sedekat di seberang jalan, duduk di sebelah Anda di kedai kopi, atau ribuan mil jauhnya. Selain itu, serangan siber merambah jauh melampaui Internet yang kita pahami saat ini, sejauh menyangkut kemampuan dan dampak kita pada kehidupan sehari-hari.

Orang tersebut memiliki sistem komputer, atau laptop, iPhone, atau iPad, yang memungkinkannya untuk meretas basis data pribadi atau sistem air kota. Tidak seperti terorisme konvensional, yang memerlukan tindakan kekerasan fisik, serangan siber memerlukan mesin sehari-hari dan keterampilan teknis yang dibutuhkan. Kombinasi komputer dan serangan siber yang terampil menonjolkan kerentanan individu dan kolektif yang berbeda dari serangan konvensional. Serangan siber jelas digunakan untuk mengirim pesan, yang dilihat sebagai diplomasi pesan.

Pesan ini secara khusus memengaruhi psikologi kerentanan, kepercayaan dan keyakinan yang dimiliki orang dalam memerangi serangan semacam itu. Salah satu perbedaan utama adalah bahwa teroris yang melakukan serangan tradisional dapat terlihat, sedangkan mereka yang bertanggung jawab atas serangan siber sebagian besar tidak terlihat. Perbedaan antara keduanya menimbulkan pertanyaan mendalam tentang kerentanan dan perlindungan.

2.3 TERORISME

Meskipun secara harfiah, ada banyak sekali definisi terorisme, saya sarankan terorisme didefinisikan sebagai tindakan, oleh individu atau kelompok, yang dimaksudkan untuk membunuh orang yang tidak bersalah, terutama sebagai cara untuk menanamkan rasa takut pada orang lain, dengan tujuan memajukan salah satu dari empat tujuan—politik, agama, sosial, dan budaya—sehubungan dengan kebijakan pemerintah. Sebagian besar serangan teroris mengakibatkan hilangnya nyawa orang yang tidak bersalah secara acak; namun, dari perspektif organisasi teroris, penduduk sipil didefinisikan sebagai target yang sah. Namun, keamanan siber sangat berbeda bagi orang yang tidak terbunuh atau terluka secara fisik.

Namun, dampak jangka panjang dari serangan siber lebih kuat daripada satu tindakan terorisme. Terorisme siber mencerminkan keahlian dan pendekatan yang sangat berbeda; sedangkan teroris tradisional bersedia mati demi tujuan tersebut, penyerang siber tidak terlibat secara fisik dan, oleh karena itu, tidak mempertaruhkan nyawa atau anggota tubuh. Namun, penyerang siber dapat secara drastis memengaruhi kehidupan sehari-hari, dengan cara yang lebih berdampak daripada terorisme tradisional. Meskipun teroris tradisional dan penyerang dunia maya sama-sama mengabdikan diri pada tujuan mereka, teroris yang memanipulasi komputer tidak bermaksud untuk mati saat melakukan aksinya.

Hal itu dapat dikatakan membuatnya lebih berbahaya: karena kecanggihan komputer dan keterampilan analisis mereka, dampak mereka pada infrastruktur negara-bangsa jauh melampaui dampak seorang pelaku bom bunuh diri. Dalam konteks ini, salah satu pertanyaan penting adalah sebagai berikut: Apakah cara yang cukup telah diambil untuk melindungi masyarakat dari apa yang pada hakikatnya merupakan bentuk baru terorisme? Salah satu pertanyaan terpenting adalah pertanyaan tentang biaya; jika dijabarkan kembali, seberapa mahalnya menerapkan tindakan anti-siber.

Tidak diragukan lagi, biayanya sangat mahal, terutama karena memerlukan respons yang canggih terhadap serangan canggih. Mengingat definisi target yang sah secara harfiah tidak terbatas, konsekuensi dalam konteks serangan dunia maya sangat mengejutkan: keberhasilan penetrasi pesawat komersial atau sistem bandara berpotensi menjadi serangan teroris yang luar biasa. Konsekuensi dari kerugian, baik jangka pendek maupun jangka panjang, secara dramatis melampaui terorisme tradisional.

Dampak serangan siber terhadap negara-bangsa sangat signifikan. Serangan siber tidak hanya menjadi ancaman signifikan bagi infrastruktur negara-bangsa, tetapi juga membutuhkan biaya yang sangat besar untuk melindunginya. Karena biayanya sering kali lebih besar daripada ancamannya, banyak titik infrastruktur penting yang menjadi rentan. Hal ini membuat kita bertanya—apa yang akan saya lakukan jika terjadi serangan seperti itu?

Pertimbangkan rutinitas pagi Anda—apa salah satu hal pertama yang Anda lakukan di pagi hari? Biasanya, Anda akan bangun, bangkit dari tempat tidur, dan menyalakan lampu. Namun, bagaimana jika Anda tidak dapat menyalakan lampu? Selain itu, bagaimana jika semua makanan di lemari es Anda rusak karena kekurangan listrik? Ini adalah situasi yang baru-baru ini terjadi di Ukraina, yang dikatakan menjadi sasaran serangan siber. Suatu wilayah di Ukraina menjadi gelap selama tiga jam, tetapi bukan karena "sambungan yang berkarat atau pohon

yang tumbang menimpa kabel listrik, tetapi tampaknya merupakan contoh langka penggunaan malware untuk memutus jaringan listrik."

Contoh serangan siber ini dengan jelas menunjukkan ketidakstabilan yang dapat disebabkan oleh terorisme siber. Selain itu, hal ini mengarah pada kesimpulan bahwa malware tidak hanya dapat mematikan jaringan listrik, malware serupa juga dapat "memanipulasi mesin yang mengendalikan peralatan industri" dan "menyebabkannya berperilaku berbahaya." Dengan contoh tersebut—apakah biayanya masih lebih besar daripada ancamannya?

2.4 PEMBIAYAAN DALAM KEAMANAN SIBER

Berapa banyak uang yang harus dialokasikan untuk keamanan siber? Selain itu, seberapa besar kerusakan yang dapat ditimbulkan oleh serangan siber? Dan terakhir, yang lebih penting, seberapa besar kerusakan yang bersedia kita toleransi? Untuk memulai proses menjawab pertanyaan-pertanyaan ini, penting untuk menyadari bahwa transisi dari model terorisme atau kontraterorisme konvensional akan memerlukan perumusan ulang mendasar tentang definisi ancaman, dan apa dan siapa yang menimbulkan ancaman. Model kontraterorisme operasional AS saat ini terutama didasarkan pada serangan pesawat nirawak terhadap target teroris yang diduga. Apakah model tersebut legal, bermoral, dan efektif merupakan hal terpenting yang perlu dipertanyakan.

Akan tetapi, karena ancaman yang ditimbulkan oleh dunia maya berbeda dengan ancaman yang ditimbulkan oleh calon pelaku bom bunuh diri, merumuskan kembali operasi kontraterorisme menjadi hal yang penting. Jika perang pesawat nirawak merupakan senjata pilihan dalam menghadapi terorisme konvensional, maka mencegah atau menanggapi serangan dunia maya akan sangat berbeda terutama karena penyerang dunia maya tidak mudah terlihat. Perbedaan dalam hal fisik memerlukan pemikiran ulang tentang pemahaman dasar kita tentang terorisme dan merumuskan kembali kontraterorisme untuk menanggapi ancaman dunia maya. Selain itu, diperlukan pemikiran ulang tentang apa yang menjadi target selama serangan dunia maya, khususnya dengan mempertimbangkan infrastruktur yang paling penting untuk dilindungi.

Salah satu pertanyaan penting adalah menentukan apakah individu yang terlibat dalam terorisme dunia maya merupakan target yang sah, sama seperti mereka yang terlibat dalam terorisme konvensional. Saya akan menyarankan hal berikut: seorang individu yang terlibat dalam terorisme dunia maya, yang memiliki kemampuan untuk meretas sistem air kota, merupakan target yang sah seperti halnya teroris yang bermaksud melakukan bom bunuh diri. Dasar pemikiran untuk kesetaraan ini adalah potensi bahaya yang ditimbulkannya dan bahaya aktual yang dapat ditimbulkannya.

Pentingnya informasi intelijen yang sangat besar tidak dapat diremehkan. Mirip dengan terorisme konvensional, keputusan untuk menargetkan individu yang terlibat dalam terorisme siber akan ditentukan oleh analisis informasi intelijen yang relevan. Baik dalam terorisme konvensional maupun terorisme siber, komunitas intelijen terdiri dari dua cabang yang berbeda: pengumpulan informasi dan analisis informasi. Namun, karena siber merupakan

bentuk peperangan baru, ada persyaratan untuk memikirkan kembali model pengumpulan intelijen tradisional.

Perbedaannya mencolok: siber didasarkan pada individu yang memegang laptop tanpa niat untuk mati, sedangkan pelaku bom bunuh diri berniat untuk mati saat melakukan tindakan terorisme. Meskipun kedua individu tersebut merupakan ancaman bagi keamanan nasional, perbedaan dalam kemampuan, sarana, dan konsekuensi mereka signifikan.

Terorisme siber berbeda dari terorisme tradisional, seperti yang telah dijelaskan sebelumnya, khususnya oleh individu yang memulai serangan. Teroris siber sering kali adalah individu yang memegang laptop tanpa bermaksud untuk mati. Ia tidak mudah dikenali. Hal ini secara langsung terkait dengan masalah biaya. Pertimbangkan hal berikut:

> *Sebagai kelanjutan dari contoh sebelumnya, seseorang bangun dan menyalakan keran air untuk mandi pagi, lalu tidak menemukan air. Orang tersebut mengetahui bahwa serangan siber telah dilakukan terhadap sistem air di komunitas tersebut, dengan komputer yang diretas, dan semua akses ke air telah diputus. Seperti yang dibahas sebelumnya, hal ini merupakan serangan siber karena merupakan tindakan agresif yang langsung dan disengaja serta berdampak buruk terhadap teknologi dan komunikasi.*

Pertanyaannya kemudian adalah, seberapa signifikan serangan tersebut? Sering kali, signifikansi serangan memengaruhi analisis biaya kita. Pertanyaan utama yang muncul di awal bagian ini adalah berapa banyak uang yang harus dialokasikan untuk keamanan siber? Bayangkan Anda adalah individu yang tinggal di komunitas dengan kelangkaan air yang tiba-tiba. Lupakan keinginan untuk menjaga kebersihan yang baik; Tiba-tiba, pilihan makanan Anda menjadi sangat terbatas. Tidak hanya itu, meskipun Anda bisa memasak, kemampuan Anda untuk mencuci piring agar bisa digunakan kembali juga terganggu karena kekurangan air. Selain itu, Anda tidak dapat menggunakan toilet. Tanpa air bersih, kehidupan sehari-hari kita tidak lagi normal dan kemungkinan akan berubah menjadi kacau.

Jadi, dengan pertanyaan tentang seberapa signifikan serangan itu, bagaimana Anda menilai kurangnya air bersih? Apakah itu akan menjadi 10 pada skala signifikansi? Apakah itu sama signifikannya dengan pengeboman teroris di hotel terdekat? Apakah ancamannya sama nyatanya? Apakah itu lebih atau kurang mungkin memengaruhi kehidupan sehari-hari Anda? Kurangnya air bersih tidak hanya bagi individu tetapi juga bagi bisnis, atau sistem rumah sakit, merupakan ancaman yang sangat signifikan.

Tampaknya alokasi dana merupakan pertanyaan yang mudah. Namun, pertanyaan lanjutan menimbulkan kesulitan dalam skenario tersebut. Seberapa besar kerusakan yang dapat ditimbulkan oleh serangan siber? Seperti yang terlihat dalam contoh ini, jumlah kerusakannya signifikan. Tanpa air yang mengalir, masyarakat seperti yang kita ketahui tidak dapat berfungsi. Jadi, jumlah kerusakan yang dapat ditimbulkan oleh serangan siber sangat besar. Meskipun kerusakannya tidak bersifat fisik, dan mungkin tidak langsung terlihat oleh mata manusia, kerusakannya tampaknya lebih besar daripada bentuk terorisme yang lebih tradisional karena sifatnya yang meluas dan jumlah individu yang akan terpengaruh.

Pertanyaan lanjutan terakhir menanyakan seberapa besar kerusakan yang bersedia kita

toleransi? Pertanyaan biaya ini sulit dijawab, khususnya, karena jumlah kerusakan yang bersedia kita toleransi sering kali sebanding dengan jumlah kerusakan yang telah kita alami, dan bersumpah untuk tidak mengalaminya lagi. Hingga serangan siber terjadi, banyak orang mengabaikan ancaman tersebut, atau menganggapnya tidak mungkin atau tidak mungkin terjadi. Namun, begitu serangan tersebut terjadi, seperti yang terlihat dalam contoh sebelumnya, dengan lampu padam di sebagian wilayah Ukraina, jumlah kerusakan yang bersedia ditoleransi oleh suatu kelompok berkurang drastis. Oleh karena itu, sangat penting untuk mengatasi masalah biaya terlebih dahulu agar dapat menanggulangi dampak serangan siber secara efektif.

2.5 TINDAKAN TERORISME

Sebuah bom bunuh diri yang berhasil memerlukan sekitar empat hingga lima pelaku yang berbeda: pemimpin sel; orang yang bertanggung jawab atas logistik; pemodal; pelaku bom; dan orang yang menciptakan lingkungan yang berkontribusi pada legitimasi bom bunuh diri. Bergantung pada tingkat dan waktu keterlibatan masing-masing, kelima pelaku tersebut merupakan target yang sah. Pertanyaannya adalah, kapan mereka menjadi target yang sah? Sebaliknya, keamanan siber tidak memerlukan infrastruktur yang sama untuk serangan yang berhasil terhadap sistem air kotamadya. Sebaliknya, yang mungkin diperlukan hanyalah individu yang paham komputer dengan laptop dan kemampuan untuk meretas sistem air kota tersebut.

Sebuah bom bunuh diri memerlukan empat atau lima pelaku yang bekerja sama, menciptakan sel, merencanakan operasi yang canggih; sebaliknya, serangan siber memerlukan satu orang yang kemungkinan besar tidak akan terbunuh atau meninggal saat melakukan peretasan.

Ancaman yang ditimbulkan oleh siber memerlukan model pengumpulan dan analisis intelijen yang berbeda dari terorisme konvensional. Demikian pula, model perlindungan siber berbeda dari model yang dimaksudkan untuk melindungi negara-bangsa dari terorisme konvensional. Alasan utama untuk pembedaan ini didasarkan pada persyaratan untuk membuat firewall canggih yang dimaksudkan untuk melindungi sistem komputer. Ini berbeda dari, dan lebih rumit daripada, melindungi gedung dan lokasi fisik lainnya.

Realitas keamanan siber adalah bahwa hal itu menimbulkan beban, kewajiban, dan tanggung jawab pada pemerintah dan perusahaan yang secara signifikan berbeda dari model perlindungan aset tradisional. Model perlindungan konvensional didasarkan pada perlindungan kekuatan yang intensif tenaga kerja sebagai respons terhadap penilaian risiko tertentu dan analisis biaya-manfaat. Dalam model tradisional, tentara melindungi pangkalan, polisi melindungi gedung, dan penegak hukum melindungi individu. Keamanan siber dan serangan siber sama sekali berbeda: meskipun kerusakan fisik dapat terjadi, dorongan untuk serangan tersebut adalah peretasan ke dalam jaringan komputer.

Serangan fisik yang merupakan inti dari terorisme konvensional semakin digantikan oleh terorisme, di mana sistem akan diserang; oleh karena itu, upaya utamanya adalah mengamankan informasi digital. Itu bukan untuk meminimalkan atau meniadakan

kemungkinan bahaya dan kerugian fisik yang diakibatkan oleh serangan siber; Namun, pada hakikatnya, serangan siber sangat berbeda dari serangan tradisional. Pada hakikatnya, bahaya yang ditimbulkan oleh serangan siber adalah sistem infrastruktur inti akan terpengaruh; konsekuensi yang mungkin terjadi sangat mengejutkan. Upaya untuk mengamankan informasi digital yang sangat rumit dan kompleks itu mahal, menakutkan, dan penting. Biaya pertahanan siber sangat besar dan bervariasi tergantung pada keadaan.

Kegagalan mengamankan informasi digital akan menimbulkan konsekuensi yang dramatis: hilangnya privasi, peningkatan kerentanan, dampak finansial yang signifikan, dan ketakutan mendasar yang berasal dari musuh yang tak terlihat. Terorisme konvensional dapat digambarkan sebagai bahaya yang ditimbulkan oleh musuh yang tak terlihat di gang belakang, yang secara eksplisit menunjukkan ancaman fisik.

Sebaliknya, keamanan siber adalah serangan terhadap yang tidak berwujud, serangan oleh yang tak terlihat terhadap yang tak terlihat. Menangani ancaman ini secara efektif memerlukan penerapan artikulasi ulang mendasar dari model intelijen untuk lebih memahami ancaman dan pemahaman yang lebih baik tentang kerentanan individu dan kolektif kita. Secara gamblang, laptop pada dasarnya adalah mekanisme atau saluran yang digunakan teroris untuk menyerang. Membuka laptop dan memasukkan kata sandi mengharuskan kita untuk bertanya apakah tindakan perlindungan yang memadai telah dilakukan.

Jika mempertimbangkan bentuk terorisme tradisional, yang melibatkan empat hingga lima pelaku berbeda, biaya upaya semacam itu besar, khususnya dalam hal serangan siber yang melibatkan satu orang. Empat hingga lima pelaku berbeda dalam terorisme tradisional terdiri dari (1) pemimpin sel; (2) orang yang bertanggung jawab atas logistik; (3) pemodal; (4) pelaku bom; dan (5) orang yang menciptakan lingkungan yang berkontribusi pada legitimasi bom bunuh diri. Setiap orang menanggung biaya. Pemimpin sel membutuhkan uang untuk melibatkan dan menarik anggota lain untuk bergabung dengan tujuan mereka. Orang yang bertanggung jawab atas logistik membutuhkan uang untuk mendanai operasi, termasuk pembelian ponsel, senjata, sumber daya investigasi, dan mobil. Pemodal adalah pendukung finansial operasi tersebut.

Pada akhirnya, dalam terorisme tradisional, tujuan mereka adalah membuat pernyataan terbesar, dan sering kali semakin besar pernyataannya semakin besar biayanya. Tugas pemodal adalah memperoleh uang untuk mendanai operasi. Selain itu, pelaku bom menanggung biaya terbesar. Meskipun pelaku bom kemungkinan tidak dibayar untuk jasa mereka karena mereka kemungkinan tidak akan hidup setelah operasi, ada sejumlah besar uang yang digunakan untuk merayu orang tersebut agar berperan sebagai pelaku bom. Dan terakhir, orang yang menciptakan lingkungan yang mendukung legitimasi bom bunuh diri membutuhkan uang untuk menciptakan lingkungan tersebut untuk membuat pernyataan terbesar.

Pembahasan tentang uang memainkan peran penting dalam terorisme tradisional. Empat hingga lima orang yang berperan dalam tindakan tersebut, dan uang yang dibutuhkan untuk membuat tindakan tersebut terjadi, menciptakan beberapa peluang bagi kelompok antiteroris untuk mengetahui serangan tersebut dan menggagalkan keberhasilannya. Tanpa

uang atau komunikasi, unit antiteroris dapat menghentikan perkembangan serangan teroris konvensional. Dengan demikian, penggunaan lebih banyak orang dan kebutuhan akan uang menciptakan titik penetrasi yang lebih besar bagi intelijen antiteroris untuk menghentikan operasi.

Sebaliknya, serangan siber memiliki titik penetrasi yang jauh lebih sedikit dan membutuhkan biaya awal yang lebih besar dalam perlindungan untuk menggagalkan serangan. Tidak seperti terorisme konvensional, serangan siber hanya dapat melibatkan satu orang. Dengan demikian, peluang untuk menembus sel dan menggagalkan serangan menjadi lebih sedikit. Selain itu, uang yang mengalir melalui individu untuk serangan teroris konvensional tidak terjadi pada serangan siber, sehingga menciptakan titik penetrasi yang lebih sedikit.

Seorang individu dapat membuat serangan siber terhadap infrastruktur penting, yang menyebabkan kerusakan pada sistem air kota, menara kontrol penerbangan, atau informasi keuangan. Karena sifat individu, secara keseluruhan titik penetrasi atau peluang untuk menggagalkan operasi lebih sedikit. Dengan demikian, biayanya lebih besar, dan sering kali diabaikan. Mudah untuk meyakinkan seseorang untuk membayar perlindungan terhadap serangan fisik—kerusakannya tidak terbantahkan dan dapat langsung dipahami oleh publik. Di sisi lain, ancaman siber, meskipun sama signifikannya, jika tidak bisa dibilang lebih signifikan, lebih meremehkan dan sulit dibayangkan; oleh karena itu, tuntutan akan perlindungan yang memadai sering kali diabaikan.

Seperti yang disebutkan sebelumnya, kemampuan untuk masuk ke internet, memasukkan kata sandi, dan mengakses informasi rekening bank Anda adalah alat yang hebat untuk membantu efisiensi aktivitas kita sehari-hari. Namun, kemampuan untuk melakukan hal tersebut harus disertai dengan perlindungan yang memadai terhadap serangan siber. Perlindungan ini belum memadai saat ini.

2.6 KASUS PERETASAN

Kasus-kasus terkini, termasuk peretasan Sony Pictures* atau dugaan peretasan media sosial Komando Pusat AS (CENTCOM), hanyalah contoh serangan siber yang berhasil dan banyak dipublikasikan. Apakah serangan itu sedramatis dan berdampak seperti pembuatan 400 akun fiktif bergantung pada perspektif dan kepentingan; tidak diragukan lagi, ketiganya menyoroti persyaratan untuk mengartikulasikan ulang model perlindungan tradisional. Namun, ada peringatan penting: negara-bangsa tidak dapat melakukan semua yang diperlukan untuk melindungi kita. Bagaimanapun, ada batasan pada kekuasaan negara; kegagalan untuk memberlakukan batasan pasti akan melanggar hak-hak individu secara signifikan. Demokrasi harus menemukan keseimbangan yang tepat antara perlindungan dan hak-hak individu.

- *Siapa aktor yang bertanggung jawab atas serangan siber?*
- *Sejauh mana kita ingin privasi kita dilanggar?*
- *Apakah individu bersedia privasinya dibatasi atas nama melindungi diri mereka sendiri dan orang lain?*

Gambar 2.2 Pertanyaan individu.

Jadi dalam konteks itu, penting untuk mengajukan pertanyaan yang diajukan pada Gambar 2.2. Respons naluriah, khususnya setelah 9/11 dan budaya yang diciptakannya, menunjukkan keinginan untuk menoleransi pemaksaan privasi individu atas nama perlindungan kolektif dan individu. Tentu saja, ada bahaya besar dalam mengadvokasi, apalagi menciptakan, mekanisme yang secara signifikan meminimalkan hak-hak individu. Sejarah yang dapat dipahami mungkin menunjukkan bahwa pendekatan semacam itu sarat dengan bahaya dan risiko karena konsekuensi dari pemberian kewenangan pengawasan pemerintah yang signifikan dapat menimbulkan konsekuensi yang meresahkan bagi individu dan masyarakat. Sederhananya: Setelah kewenangan diberikan kepada pemerintah, merebut kembali kewenangan adalah tugas dan beban yang paling sulit.

Apakah kita sepakat bahwa privasi kita dilanggar secara tidak perlu? Jawabannya adalah bahwa sejarah menunjukkan bahwa segera setelah serangan teroris, kita dengan senang hati melanggar hak-hak orang lain. Pertanyaannya adalah, apakah meminimalkan hak individu efektif dalam konteks keamanan siber dan model apa yang paling tepat untuk melindungi individu dan masyarakat? Jawabannya tergantung pada seberapa besar privasi yang bersedia dikorbankan individu atas nama perlindungan siber. Dalam beberapa tahun terakhir, ada kritik signifikan terhadap Badan Keamanan Nasional (NSA) karena memantau sejumlah besar percakapan telepon

Privasi, seperti yang disebutkan sebelumnya, adalah percakapan sulit yang berkembang dari percakapan dunia maya. Seperti yang disebutkan sebelumnya, setelah serangan, individu lebih mungkin, dan lebih bersedia, untuk melanggar hak-hak mereka yang terlibat. Namun, dalam skenario baru-baru ini, situasinya tidak seperti itu.

Pada tanggal 2 Desember 2015, Syed Rizwan Farook dan Tashfeen Malik melakukan penembakan massal dan percobaan pengeboman di sebuah pesta liburan kerja. Dari serangan ini, 14 orang tewas dan 22 orang terluka parah. Perebutan privasi yang berasal dari serangan ini melibatkan akses ke iPhone milik Farook. FBI tidak dapat membuka kunci ponsel dan meminta Apple untuk membuat versi baru dari sistem operasi yang dapat diinstal untuk menonaktifkan fitur keamanan tertentu. Apple awalnya menolak, yang mengakibatkan FBI mengajukan perintah pengadilan, yang mewajibkan Apple untuk membuat dan menyediakan perangkat lunak yang diminta. Apple menentang perintah mereka, dengan menekankan risiko keamanan yang akan ditimbulkan oleh pembuatan pintu belakang bagi pelanggan mereka.

Hubungan antara kepentingan perusahaan dan keamanan nasional merupakan inti dari ketegangan saat ini antara Apple dan FBI. Mengatasi, apalagi menyelesaikan, ketegangan ini merupakan tantangan. Hal ini juga penting. Menghormati salah satu pihak tidak boleh mengorbankan pihak lainnya. Perintah Pengadilan Distrik AS (California Tengah) yang

mengharuskan Apple membuat pintu belakang hanyalah serangan awal dalam apa yang tampaknya merupakan pertempuran hukum yang berkepanjangan. Tidak dapat diprediksi bagaimana pertempuran hukum ini akan diselesaikan.

Terlepas dari hasil akhir, garis pertempuran telah ditarik. Apple berpendapat bahwa FBI terlibat dalam tindakan yang melampaui batas; Departemen Kehakiman menegaskan bahwa informasi yang disimpan di ponsel sangat dibutuhkan untuk melindungi publik. Kedua belah pihak memberikan argumen yang meyakinkan. Namun, diskusi tersebut melampaui pertanyaan yang saat ini diajukan ke pengadilan. Isu strategis yang lebih mendalam adalah kerja sama sektor swasta-pemerintah mengenai keamanan dalam negeri dan penanggulangan terorisme.

Pertanyaannya banyak dan rumit:

- Jika sebuah perusahaan menjadi target serangan teroris, apakah pemerintah berkewajiban untuk menanggapi atas nama keamanan nasional?
- Apakah ada kewajiban yang harus dipenuhi oleh pemegang saham di perusahaan yang diperdagangkan secara publik atau kepada investor dan pemilik di perusahaan swasta?
- Apakah serangan terhadap perusahaan Amerika sama dengan serangan terhadap pemerintah AS?
- Apa hubungan antara dampak ekonomi dan keamanan nasional?

Menjawab pertanyaan-pertanyaan ini—atau setidaknya berusaha untuk membingkainya—memerlukan pengakuan fakta bahwa terorisme menimbulkan ancaman langsung terhadap entitas perusahaan. Apakah ancaman teroris bersifat kinetik atau siber tidaklah relevan. Yang pertama menunjukkan hilangnya nyawa dan kerusakan fisik; banyak contoh yang terakhir bersifat strategis, ekonomis, dan berdampak jangka panjang.

Serangan siber mengharuskan perusahaan untuk bermitra dengan pelanggan dan penegak hukum. Kemitraan itu, harus diakui, memberatkan; beban itu sekaligus eksistensial dan praktis. Agar penegak hukum dapat secara efektif melindungi perusahaan, diperlukan perubahan mendasar dalam konteks dan konsep kerja sama. Ini akan mengharuskan perusahaan untuk lebih terbuka kepada penegak hukum. Hal ini hanya dapat terjadi jika korporasi lebih terbuka. Dalam hal ini, beban berada di pundak mereka. Kegagalan untuk bekerja sama dengan penegak hukum mencegah pengembangan—apalagi implementasi—model kerja sama penegakan hukum korporasi yang canggih.

Namun, syarat untuk pendekatan ini adalah kemauan korporasi untuk memandang penegak hukum sebagai mitra penuh, baik secara preemptif maupun reaktif. Untuk itu, diperlukan model tata kelola korporasi untuk keamanan siber; meskipun saat ini belum dimanfaatkan, beban pengembangannya berada di pundak korporasi.

Pembelaan diri merupakan pertanyaan penting dalam diskusi siber. Pertanyaannya adalah apakah negara-bangsa memiliki kewajiban terhadap korporasi dan individu yang telah menjadi korban serangan siber. Ini bukanlah pertanyaan abstrak, melainkan pertanyaan yang dimaksudkan sebagai pertanyaan konkret.

Jawabannya tidak jelas. Meskipun jawaban yang mudah adalah ya, jawabannya jauh lebih rumit dari itu. Demikian pula, tidak adalah respons yang tidak dapat diterima karena

kepentingan nasional memang membenarkan keterlibatan negara dalam keamanan siber, bahkan ketika target negara tidak diserang secara langsung. Keseimbangan sulit didefinisikan dan tidak diragukan lagi sulit diterapkan.

Dalam konteks kewajiban negara terhadap perusahaan dan individu, akan menjadi hal yang tidak praktis untuk memaksakan kewajiban kepada pemerintah untuk menanggapi setiap serangan siber. Saran itu tidak akan berhasil sejak awal.

Sebaliknya, menyarankan bahwa pemerintah tidak memiliki kewajiban melanggar kontrak sosial yang menjadi dasar masyarakat sipil. Itu juga tidak akan berhasil. Ada risiko besar dalam memaksakan beban respons kepada negara-bangsa setelah serangan siber. Jika serangan itu dapat ditelusuri kembali ke agen negara lain, maka muncul pertanyaan yang sah mengenai batas kedaulatan, pembelaan diri, dan konflik.

Masalah-masalah ini menunjukkan di mana karet menyentuh jalan. Sampai para pemimpin negara dan pejabat perusahaan benar-benar menghadapi ancaman luar biasa yang ditimbulkan oleh terorisme siber, kita, secara individu dan kolektif, akan terus rentan dan berisiko.

Konflik Apple–FBI menyoroti berbagai masalah penting; kita harus memanfaatkan sorotan yang difokuskan pada isu-isu ini dan mencari jawaban yang dapat diterapkan untuk pertanyaan-pertanyaan yang diajukan.

2.7 BATASAN PERLINDUNGAN

Sehubungan dengan perlindungan siber, pertanyaannya adalah seberapa efektif dan legal didefinisikan, apalagi diterapkan. Pertanyaan tentang legalitas memerlukan fokus pada Amandemen ke-4 Konstitusi AS; sehubungan dengan efektivitas, jawaban yang mudah adalah jika tidak ada tindakan terorisme, maka ya itu efektif. Perhatian khusus perlu diberikan pada tiga konsep penting: (1) kebutuhan, (2) efektivitas, dan (3) legalitas.

Ancaman yang ditimbulkan oleh siber menuntut hal-hal berikut untuk dilindungi (Gambar 2.3):

- *Individu (baik warga negara maupun bukan warga negara) dari ancaman eksternal dan internal*
- *Properti: fisik dan tidak berwujud*
- *Infrastruktur*

Gambar 2.3 Tuntutan perlindungan.

Sejauh mana perlindungan tersebut masih dalam tahap penentuan. Kerusakan yang disebabkan oleh serangan siber terhadap kekayaan intelektual atau tak berwujud jelas sangat besar; salah satu pertanyaan terpenting dalam konteks keamanan siber adalah bagaimana kita melindungi kekayaan intelektual atau tak berwujud tersebut secara lebih efektif. Perusahaan yang berfokus pada perlindungan entitas atau rahasia dagang mereka menghabiskan sumber daya yang signifikan untuk melakukannya.

Sejauh mana mereka efektif atau tidak efektif masih menjadi pertanyaan terbuka.

Bahkan mereka yang berniat melindungi kekayaan intelektual atau tak berwujud mereka harus memahami bahwa perlindungan tidak 100% anti gagal karena serangan dapat, dan akan, terjadi. Bagaimanapun, peretas terus-menerus terlibat dalam menembus firewall yang ada.

Melindungi jalan raya, jalan kecil, sistem air, bandara, dan sebagainya membutuhkan biaya yang signifikan; menentukan prioritas memerlukan penilaian risiko, analisis biaya-manfaat yang canggih, dan pengambilan keputusan alokasi sumber daya. Prosesnya rumit karena pemerintah gagal mendidik masyarakat secara terbuka mengenai biaya perlindungan infrastruktur dari serangan siber. Proses ini juga rumit karena teknologi yang dapat diakses oleh masing-masing pemerintah. Setiap negara memiliki kemampuan untuk bertahan secara berbeda, tergantung pada teknologi dan biaya.

Serangan Siber Dan Tindakan Kekuatan?

Dalam membahas hubungan antara keamanan siber dan kekuatan, mungkin kita perlu menggunakan kata "kekuatan" dalam tanda kutip, karena ini adalah kekuatan tersirat atau tidak langsung yang sama dengan kekuatan intelektual atau tidak berwujud. Gambar 2.4 adalah daftar periksa yang disarankan dalam menganalisis kekuatan dalam konteks serangan siber.

Misalnya, peretasan Pentagon memiliki konsekuensi dan implikasi yang jelas bagi keamanan nasional Amerika. Demikian pula, serangan terhadap perusahaan yang menyebabkan akun jutaan orang diretas dan catatan medis serta keuangan dibocorkan adalah contoh serangan siber yang parah. Mengenai kedekatan: Jika 70 juta orang terkena dampak karena serangan terhadap perusahaan besar, seperti yang terlihat dalam pelanggaran Target baru-baru ini, jelas ada rasa kedekatan karena peretas memiliki akses ke catatan pelanggan yang akan mengharuskan perusahaan yang terkena dampak untuk mengambil tindakan segera guna meminimalkan kerugian dan dampak.

Bertindak segera, dan efektif, memerlukan perencanaan proaktif yang memastikan rencana respons yang dimaksudkan untuk meminimalkan dampak telah dikembangkan terlebih dahulu. Itu jelas membebankan biaya pada perusahaan dan pemerintah untuk memiliki rencana untuk bereaksi segera.

Poin berikutnya adalah keterusterangan. Di ketiga level, Pentagon yang diretas, perusahaan besar yang terkena dampak, dan akun individu yang diretas, ada rasa keterusterangan. Dalam ketiga contoh, dampaknya tidak terjadi di kemudian hari tetapi jelas sekarang. Dengan cara yang sama, serangan fisik memiliki dampak langsung; peretasan rekening bank juga memiliki kedekatan yang jelas. Kedekatan dan keterusterangan dikurangi oleh tingkat keparahannya. Selanjutnya, penting untuk mempertimbangkan tingkat invasifnya: Jika rekening bank seseorang telah diretas dan akibatnya kartu kredit digunakan (disalahgunakan), jelas ada kesan invasif. Jika Pentagon telah diretas, diperlukan pakar untuk menentukan tingkat invasifnya.

Penting untuk dicatat bahwa tingkat keparahan, kedekatan, dan keterusterangan tidak serta-merta berubah menjadi invasif. Hal yang sama berlaku untuk korporasi. Respons yang tepat memerlukan penilaian sejauh mana peretasan telah menyerang; karena invasif dapat diukur, sangat penting bagi korporasi dan pemerintah untuk menentukan kerusakan yang

ditimbulkan. Bagi korporasi, sangat penting, dalam hal kepatuhan, untuk bersikap terbuka dalam mengartikulasikan tingkat dampak dan invasifnya. Mengartikulasikan yang dapat diukur akan ditingkatkan secara signifikan dengan membuat matriks.

Matriks tersebut harus mencerminkan berbagai lapisan invasif, dan juga akan memungkinkan korporasi untuk menentukan sejauh mana praperencanaan mereka efektif atau tidak efektif. Salah satu persyaratan terpenting adalah menerapkan matriks keterukuran yang memastikan penentuan dampak yang konkret. Dalam konteks legitimasi dan tanggung jawab, korporasi memiliki tanggung jawab utama kepada klien dan pemegang sahamnya, sedangkan pemerintah memiliki tanggung jawab kepada publik. Dalam hal keamanan siber, korporasi dan pemerintah harus menerapkan mekanisme pencegahan yang memungkinkan pemantauan upaya penetrasi, terlepas dari biayanya.

Hal terakhir adalah menanyakan apakah beberapa tingkat kerusakan dapat ditoleransi. Kenyataannya adalah bahwa meskipun korporasi memiliki rencana perlindungan yang canggih, tidak dapat dihindari, atau hampir tidak dapat dihindari, bahwa akan ada upaya serangan, yang beberapa di antaranya akan berhasil. Sangat penting bagi korporasi, pemerintah, dan individu untuk melakukan hal berikut (Gambar 2.5). Berikut ini adalah pertanyaan-pertanyaan yang perlu dipertimbangkan dalam meninjau Bab 2 (Gambar 2.6).

1. *Membuat rencana perlindungan;*
2. *Melakukan pemantauan terus-menerus;*
3. *Ketika upaya peretasan atau peretasan berhasil teridentifikasi, target (perusahaan atau pemerintah) harus segera berupaya mengidentifikasi sumbernya, meminimalkan dampaknya, dan terlibat dalam berbagi informasi dengan pemegang saham, penegak hukum, dan perusahaan lain.*

Gambar 2.5 Rencana perlindungan.

Latihan Soal

1. Bagaimana kita mengukur kekuatan dalam serangan keamanan siber?
2. Tingkat bahaya apa yang dianggap sebagai serangan keamanan siber?
3. Siapa yang bertanggung jawab untuk mencegah serangan keamanan siber?
4. Apakah tingkat keparahan dan urgensi serangan memengaruhi respons terhadap serangan keamanan siber?
5. Haruskah keamanan siber menjadi masalah keamanan nasional?

Gambar 2.6 Pertanyaan tinjauan.

BAB 3
GEOPOLITIK DAN KEAMANAN SIBER

3.1 PENDAHULUAN

Sehubungan dengan hubungan antarnegara-bangsa, menanggapi serangan siber merupakan hal yang sangat penting dan terus berkembang. Salah satu poin analisis terpenting mengenai geopolitik adalah kemungkinan tanggapan terhadap serangan siber atau serangan balasan siber, dan bagaimana tindakan tertentu akan dipersepsikan. Diartikulasikan ulang: Tanggapan seperti apa yang dapat diharapkan dalam menghadapi ancaman siber atau selama serangan yang sebenarnya? Mengingat berbagai tanggapan yang disebutkan sebelumnya, para pengambil keputusan nasional harus menilai bagaimana negara-bangsa akan bereaksi; karena alasan itu, geopolitik menyoroti pentingnya memahami tanggapan aktual dan reaksi terhadap tanggapan tersebut.

Contoh serangan dan aktivitas terkait siber berikut menyoroti hubungan penting antara keamanan siber dan geopolitik:

Contoh 1: Beberapa pihak menduga pemerintah Rusia menyerang atau mendorong serangan kejahatan terorganisir terhadap situs web resmi di negara Georgia selama pertikaian militer pada tahun 2008 yang mengakibatkan invasi Rusia ke Georgia.

Contoh 2: Pada tahun 2009–2010, muncul kecurigaan bahwa cacing komputer canggih buatan pemerintah yang disebut Stuxnet dilepaskan untuk menonaktifkan sentrifus pabrik nuklir Iran yang dapat digunakan untuk membuat uranium yang diperkaya untuk senjata. Sumber dan spekulan yang tidak disebutkan namanya berpendapat bahwa pemerintah Amerika Serikat dan Israel mungkin telah merancang dan menyebarkan cacing tersebut.

Contoh 3: Departemen Pertahanan Amerika telah menciptakan struktur komando siber yang membangun strategi siber defensif dan ofensif yang didukung Internet sebagai bagian integral dari perencanaan dan pembuatan perang.

Contoh 4: Pada bulan Mei 2014, lima pejabat militer Tiongkok didakwa di Pennsylvania Barat atas peretasan komputer, spionase, dan pelanggaran lainnya yang ditujukan pada enam korban AS, termasuk pembangkit listrik tenaga nuklir, logam, dan industri produk surya. Dakwaan ini muncul setelah beberapa tahun terungkapnya fakta bahwa militer Tiongkok dan agen-agen lainnya telah membobol komputer di sejumlah perusahaan besar AS dan perusahaan media dalam upaya untuk mencuri rahasia dagang dan mengetahui berita apa yang sedang dikerjakan oleh para jurnalis.

Contoh 5: Pada bulan Oktober 2014, para peretas Rusia diduga telah mengeksploitasi kelemahan pada Microsoft Windows untuk memata-matai NATO, pemerintah Ukraina, dan bisnis-bisnis Barat.

Contoh 6: Ponemon Institute yang disegani melaporkan pada bulan September 2014 bahwa 43% perusahaan di Amerika Serikat telah mengalami pelanggaran data pada tahun lalu. Pelanggaran ritel, khususnya, telah meningkat dalam skala dan tingkat keparahannya pada tahun sebelumnya. Salah satu pelanggaran yang paling mengerikan ditemukan pada bulan Juli

2014 di JP Morgan Chase & Co., di mana informasi dari 76 juta rumah tangga dan 7 juta bisnis kecil telah disusupi. Para pejabat pemerintahan Obama bertanya-tanya apakah pelanggaran tersebut merupakan pembalasan oleh rezim Putin di Rusia atas peristiwa yang terjadi di Ukraina.

Contoh 7: Di antara jenis eksploitasi individu yang menjadi bukti saat ini adalah nomor identitas nasional yang dicuri, kata sandi dan informasi pembayaran yang dicuri, identitas daring yang dihapus, dan alat mata-mata yang merekam semua percakapan daring dan penekanan tombol, dan bahkan peretasan mobil tanpa pengemudi.

Contoh 8: Beberapa hari sebelum laporan ini diterbitkan, sistem penyimpanan data berbasis cloud iCloud milik Apple menjadi target dari apa yang disebut serangan man-in-the-middle di Tiongkok yang ditujukan untuk mencuri kata sandi pengguna dan memata-matai aktivitas akun mereka. Beberapa aktivis dan pakar keamanan mengatakan mereka menduga bahwa pemerintah Tiongkok telah melancarkan serangan tersebut, mungkin karena iPhone 6 baru saja tersedia di negara tersebut. Yang lain menganggap serangan itu tidak cukup canggih untuk diprakarsai oleh pemerintah.

Geopolitik mengacu pada hubungan antarnegara-bangsa dan keterlibatan mereka dengan komunitas global yang lebih luas dengan penekanan khusus pada hubungan antara geografi dan politik negara-bangsa:

> *"Geopolitik mengambil tugas untuk mengganggu wacana geopolitik: untuk mempelajari bukan geografi politik dalam tempat-tempat yang sudah ada sebelumnya atau masuk akal, tetapi untuk menonjolkan politik dari spesifikasi geografis politik. Keamanan dan geopolitik berfungsi secara dualistik. Di satu sisi, diplomasi dan kebijakan luar negeri umumnya dipahami sebagai isu-isu tingkat tinggi yang diselimuti kerahasiaan. Di sisi lain, dan sejalan dengan ketergantungan pada bahasa khusus ini, wacana keamanan dan geopolitik sangat bergantung pada narasi akal sehat tentang tempat dan identitas. Sebagian besar penalaran geopolitik tidak formal tetapi praktis. Ia mengandalkan akal sehat alih-alih argumen akademis dan teknis yang esoteris."*

Dalam bab ini, hubungan antara keamanan siber dan geopolitik akan dikaji dengan menganalisis contoh-contoh tertentu yang mencerminkan kompleksitas pertemuan keduanya. Analisis akan menyentuh hukum internasional, khususnya pembelaan diri dan proporsionalitas. Pengambilan keputusan negara-bangsa, yang mencerminkan prediktabilitas dan konsistensi, secara signifikan meningkatkan tatanan global. Namun, ancaman—baik yang nyata maupun yang dipersepsikan—secara dramatis memengaruhi stabilitas regional dan global. Dalam hal ini, menilai bagaimana negara-bangsa merespons, baik secara unilateral, bilateral, atau multilateral, terhadap titik-titik krisis tertentu sangat penting untuk memahami dampak praktis dari pertimbangan geopolitik.

Geopolitik yang efektif membutuhkan pertemuan antara yang teoretis dan yang praktis. Yang pertama menuntut para pemimpin nasional untuk memahami berbagai masalah, termasuk hukum internasional, hubungan internasional, keuangan, geografi, dan kekuatan militer, khususnya, batas-batasnya. Yang terakhir membutuhkan penerapan disiplin ilmu yang

berbeda ini dengan kepekaan, baik terhadap politik dalam negeri maupun komunitas global, sambil mengakui pentingnya masalah taktis dan strategis. Meskipun, pada pandangan pertama, pertimbangan taktis dan strategis menunjukkan adanya ketidaksesuaian, para pemimpin nasional yang efektif mampu menggabungkan keduanya dalam proses pengambilan keputusan.

Seperti yang disebutkan sebelumnya, geopolitik adalah hubungan antarnegara-bangsa dan keterlibatan mereka dengan komunitas global yang lebih luas, dengan penekanan khusus pada hubungan antara geografi dan politik negara-bangsa. Penekanan pada geografi dan komunitas global yang lebih luas memainkan peran penting dalam geopolitik.

Pertimbangkan hal berikut: Pada tahun 1924, gempa bumi yang mengerikan telah melanda Asia, mempengaruhi ratusan ribu orang dan berpotensi menyebabkan tsunami ribuan mil jauhnya. Namun, karena kurangnya sistem informasi, tidak ada cara yang memadai untuk memperingatkan mereka yang berada di jalur tsunami, atau memperingatkan mereka untuk meminta bantuan bagi individu yang terkena gempa bumi.

Sekarang, pertimbangkan tahun 2020. Tidak hanya cepat untuk memberi tahu orang lain yang berada di jalur tsunami, bahkan lebih cepat untuk meminta bantuan orang lain bagi mereka yang terkena dampak gempa bumi. Namun, meminta bantuan itu mungkin tidak selalu membuahkan hasil. Kita hidup di dunia di mana berita diproses 24/7, dan ada informasi yang konstan di ujung jari kita. Karena itu, ada kesadaran terus-menerus akan kekejaman dan ketidakadilan yang tak berkesudahan yang terjadi setiap hari di berbagai belahan dunia. Pada hari apa pun, ada krisis pengungsi, virus medis, bencana fisik, atau serangan yang disebabkan manusia. Sering kali sulit untuk mengikuti semua ini.

Jadi, geopolitik adalah hubungan antara negara-bangsa dan keterlibatan mereka dengan komunitas yang lebih besar, yang sangat dipengaruhi oleh dunia yang semakin mengglobal tempat kita hidup. Pertimbangkan dampak dunia yang semakin mengglobal dalam arti keamanan siber.

Seperti yang terlihat pada Contoh 2, virus Stuxnet dilepaskan untuk menonaktifkan kemampuan nuklir Iran. Penerapan virus ini dilaporkan secara luas di saluran berita dan sesuatu yang diakui oleh individu di seluruh dunia. Tidak hanya itu, kemampuan siapa pun untuk memasukkan virus ke dalam kemampuan nuklir suatu negara hanya dimungkinkan karena teknik yang terus inovatif yang diadaptasi oleh siber. Di Iran, kemungkinan besar negara-negara lain mengetahui kemampuan nuklir baik melalui laporan mereka sendiri, atau lebih mungkin melalui informasi pengawasan yang mencatat dokumentasi fasilitas nuklir yang sedang dibangun atau yang saat ini ada. Teknologi ini hadir dalam bentuk pesawat nirawak atau pengawasan satelit lainnya. Dengan demikian, sebagai dunia yang semakin mengglobal, negara-negara merasa khawatir mengetahui bahwa suatu negara, seperti Iran, memiliki kemampuan ini.

Seperti yang terlihat pada contoh sebelumnya, bagaimana jika ini terjadi pada tahun 1924? Bagaimana jika tidak ada cara untuk mengetahui kemampuan nuklir ini? Apakah itu masih menjadi ancaman yang besar? Apakah kita akan menanggapinya dengan cara yang berbeda? Apakah kita akan mempersiapkan diri menghadapi ancaman dengan cara yang

berbeda? Pertemuan teknologi tidak hanya memungkinkan kita untuk menciptakan ancaman yang lebih besar, tetapi juga memungkinkan kita untuk memantau ancaman yang lebih besar.

Selain itu, jika pengenalan informasi mengenai fasilitas nuklir terjadi pada tahun 1924, apakah ada kemungkinan untuk menghancurkan atau merusak fasilitas nuklir tersebut, seperti yang dilakukan oleh virus Stuxnet. Dengan demikian, bukan saja pengenalan informasi telah mengubah persepsi kita terhadap geopolitik secara besar-besaran, tetapi cara kita bereaksi terhadap informasi tersebut juga memainkan peran yang bahkan lebih besar.

Pemikiran taktis mencerminkan pengambilan keputusan, yang hanya berfokus pada hal-hal yang langsung, sedangkan pemikiran strategis mencerminkan pemahaman yang tajam tentang, dan penghargaan terhadap, jangka panjang, tanpa hasil dan dampak langsung. Mungkin, keadaan membenarkan, atau mendikte, perspektif yang sempit. Komunitas global menyiratkan peningkatan kerja sama dalam berbagai masalah, termasuk keuangan, keamanan, kontrol perbatasan, lingkungan, perawatan kesehatan, dan sumber daya alam. Para pemimpin nasional, dapat dimengerti, terutama menekankan pertimbangan dalam negeri; meskipun demikian, geopolitik yang efektif menunjukkan kepentingan nasional ditingkatkan secara signifikan ketika urusan internasional diperhitungkan dalam pengambilan keputusan dalam negeri. Bersamaan dengan itu, analisis geopolitik yang menyeluruh mencakup hubungan antara negara-bangsa dan perusahaan, dan apakah ada kewajiban untuk melindungi perusahaan dalam suatu negara-bangsa.

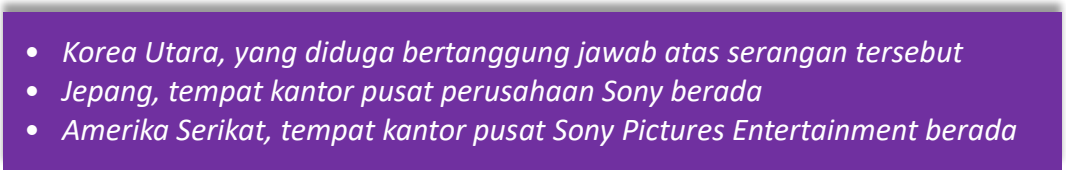
Selain itu, negara-bangsa tertentu khususnya dan komunitas internasional, secara umum, dihadapkan pada dilema mengenai batas kedaulatan dalam menghadapi ancaman nyata atau yang dipersepsikan. Misalnya: Tantangan yang ditimbulkan oleh komitmen Iran untuk mengembangkan program nuklir telah memaksa masyarakat internasional untuk mempertimbangkan berbagai pilihan terkait batas kedaulatan Iran dan intervensi internasional. Mayoritas masyarakat internasional mengakui ancaman yang ditimbulkan oleh nuklir Iran, baik secara regional maupun internasional. Meskipun demikian, kekhawatiran mengenai dampak dari serangan bersenjata terhadap Iran telah berkontribusi signifikan terhadap penerapan sanksi ekonomi dan diplomatik yang luas, yang efektivitasnya masih menjadi pertanyaan terbuka.

Dalam menentukan respons yang tepat terhadap ancaman yang ditimbulkan oleh nuklir Iran, masyarakat internasional telah menunjukkan ketidaknyamanan yang luar biasa terkait tindakan militer. Meskipun dapat dimengerti, pertanyaan yang lebih luas adalah, apa konsekuensinya, jika masyarakat internasional tidak mencegah Iran memenuhi program nuklirnya? Bagaimana para pemimpin nasional terlibat dalam, dan menyelesaikan, proses pengambilan keputusan sangat penting untuk memahami implementasi praktis geopolitik.

3.2 SONY DAN KOREA UTARA

Misalnya, dalam mempertimbangkan serangan siber terhadap Sony, yang tampaknya dilakukan oleh Korea Utara, tiga negara berbeda menjadi pemangku kepentingan (Gambar 3.1). Apakah itu berarti bahwa dua negara, Jepang dan Amerika Serikat, diserang? Menjawab pertanyaan itu memerlukan pembahasan apakah serangan siber mirip dengan tindakan

perang tradisional. Dalam perang tradisional, negara A menyerang target fisik di Negara B dengan tank dan pesawat, sedangkan serangan siber terutama merupakan serangan terhadap infrastruktur pribadi atau publik. Konsekuensi serangan dapat meluas jauh melampaui serangan fisik: dampak dari kemungkinan penutupan jaringan atau sistem melampaui kerusakan pada bangunan tertentu, bahkan jika individu terbunuh.



Gambar 3.1 Negara pemangku kepentingan.

Dengan demikian, kerentanan korporasi, dan hubungan mereka dengan negara-bangsa, mengakui rasa kewajiban yang meningkat kepada negara-bangsa atas korporasi mereka. Ini memperluas definisi geopolitik dengan cara yang terpisah dari terorisme tradisional. Untuk itu, konsekuensi dari serangan siber dapat melampaui serangan fisik; menyerang infrastruktur penting melampaui serangan tradisional yang mengakibatkan kerusakan properti atau hilangnya nyawa.

Dampak signifikan dari serangan siber dan kerentanan yang ditimbulkannya membenarkan pengartikulasian ulang prinsip-prinsip inti termasuk ancaman, pembelaan diri, dan ruang lingkup serta batasan respons. Salah satu pertanyaan terpenting dalam konteks geopolitik adalah apakah serangan siber membenarkan respons fisik; jika diartikulasikan ulang, dapatkah negara-bangsa menyerang peretas—negara atau individu—yang bertanggung jawab atas serangan siber?

Dalam mempertimbangkan pertemuan geopolitik, keamanan siber, dan pembelaan diri, serangan siber menimbulkan ancaman bagi individu, perusahaan, dan negara-bangsa. Meskipun ini melegitimasi pembelaan diri, pertanyaannya tentu saja adalah proporsionalitas. Menurut Pasal 51 Piagam PBB, negara-bangsa memiliki hak untuk terlibat dalam pembelaan diri setelah diserang:

> *"Tidak ada satu pun dalam Piagam ini yang akan merusak hak yang melekat pada pembelaan diri individu atau kolektif, jika serangan bersenjata terjadi terhadap Anggota Perserikatan Bangsa-Bangsa, hingga Dewan Keamanan telah mengambil tindakan yang diperlukan untuk menjaga perdamaian dan keamanan internasional. Tindakan yang diambil oleh anggota dalam menjalankan hak pembelaan diri ini harus segera dilaporkan kepada Dewan Keamanan dan tidak akan dengan cara apa pun memengaruhi kewenangan dan tanggung jawab Dewan Keamanan berdasarkan Piagam ini untuk mengambil tindakan yang dianggap perlu untuk menjaga atau memulihkan perdamaian dan keamanan internasional."*

Ketika Perserikatan Bangsa-Bangsa dibentuk, setelah Perang Dunia II, negara-bangsa, sebagian besar, tidak berkonflik dengan aktor non-negara dan organisasi teroris. Namun, dalam

beberapa dekade berikutnya, konflik telah berubah dari negara-bangsa yang berhadapan dengan negara-bangsa menjadi negara-bangsa yang berhadapan dengan aktor non-negara. Oleh karena itu, titik kritis penyelidikan setelah serangan siber yang berhasil adalah menentukan apakah pihak yang bertanggung jawab adalah aktor negara-bangsa atau aktor non-negara, yang bertindak atas nama dirinya sendiri atau atas nama negara-bangsa.

Ada empat pilihan berbeda yang menentukan bagaimana dan kapan negara bereaksi terhadap serangan siber (Gambar 3.2).

Pilihan #1: *aktor nonnegara yang bertindak atas namanya sendiri: jika penyerang menimbulkan ancaman langsung atau di masa mendatang, maka negara-bangsa dapat menetapkan individu tersebut sebagai target yang sah. Penentuan ancaman di masa mendatang memerlukan intelijen yang cukup yang membenarkan keputusan negara-bangsa untuk "melibatkan" individu tersebut.*
Pilihan #2*: aktor nonnegara yang bertindak sebagai proksi (penghubung) atas nama negara-bangsa: negara-bangsa yang diserang harus menentukan apakah target yang sah adalah aktor nonnegara dan/atau negara-bangsa yang atas namanya aktor nonnegara melakukan serangan.*
Pilihan #3: *negara-bangsa yang terlibat dalam serangan siber: jika negara-bangsa yang terlibat terlibat dalam serangan siber, hal itu dapat dianggap sebagai tindakan perang dan negara-bangsa yang menanggapi harus bertindak sesuai dengan Pedoman PBB.*
Pilihan #4: *negara-bangsa yang bertindak sebagai proksi (penghubung) atas nama negara-bangsa lain.*

Gambar 3.2 Pilihan status.

Dengan opsi-opsi yang tercantum di atas, akan sangat membantu jika kita menerapkan setiap opsi pada situasi nyata untuk lebih memahami cara kerja opsi-opsi tersebut. *Opsi 1* berfokus pada aktor nonnegara yang bertindak atas namanya sendiri. Ini akan terjadi ketika sebuah perusahaan, misalnya Sony, melakukan serangan siber terhadap negara lain. Ini adalah pembalikan peran dari situasi yang kita bahas nanti dalam bencana Korea Utara atau Sony. Namun, ini merupakan pertimbangan penting untuk direnungkan.

Jika Sony melakukan serangan siber terhadap Korea Utara, apakah mereka dianggap sebagai ancaman yang sah, sehingga memungkinkan Korea Utara untuk terlibat dalam pembelaan diri sesuai dengan Piagam PBB? Korea Utara harus memiliki intelijen yang cukup yang membenarkan keputusan mereka untuk melibatkan Sony, tetapi jika mereka memiliki intelijen tersebut, tindakan pembelaan diri akan tepat.

Opsi 2 berfokus pada aktor nonnegara yang bertindak sebagai proksi (penghubung) atas nama negara-bangsa. Jadi, pertimbangkan, misalnya, jika Apple, yang bertindak di bawah arahan pemerintah AS, meretas ribuan ponsel pengguna di Tiongkok. Dapatkah Tiongkok membalas dendam terhadap Amerika Serikat, sesuai dengan Piagam PBB yang mendukung

pembelaan diri? Tiongkok harus menentukan apakah target tersebut dibenarkan pada Apple atau pemerintah. Ini memerlukan intelijen yang memadai, seperti yang dipersyaratkan dalam Opsi 1, dan penguraian tambahan untuk menentukan siapa target yang tepat dan sah.

Opsi 3 berfokus pada negara-bangsa yang sebenarnya terlibat dalam serangan siber. Skenario ini tampaknya paling mudah dalam menentukan apakah negara yang diserang dapat menyerang negara-bangsa lain dengan kedok pembelaan diri. Jika negara-bangsa yang sebenarnya terlibat dalam serangan siber, kemungkinan besar hal itu dapat diperlakukan sebagai tindakan perang, dan negara yang diserang dapat bertindak sesuai dengan Pedoman PBB.

Opsi terakhir, *Opsi 4* membahas paradigma jika suatu negara-bangsa bertindak sebagai proksi, atau penghubung bagi negara-bangsa lain. Ambil contoh, katakanlah Amerika Serikat melakukan serangan siber terhadap Rusia, yang bertindak untuk Ukraina. Apakah Rusia memiliki kemampuan, dalam pembelaan diri, untuk melakukan serangan siber balasan terhadap Amerika Serikat? Atau, berdasarkan Piagam PBB, apakah perlu melakukan serangan balasan terhadap Ukraina, karena Amerika Serikat bertindak untuk Ukraina. Ini menimbulkan pertanyaan yang lebih sulit dan, seperti semua pilihan lainnya, memerlukan intelijen yang memadai sebelum terlibat dalam bentuk pembelaan diri apa pun.

3.3 SASARAN YANG SAH

Misalnya—meskipun tidak dalam ranah keamanan siber: Beberapa tahun lalu serangan teroris di Israel mengakibatkan hilangnya nyawa orang yang tidak bersalah; ditetapkan bahwa organisasi yang bertanggung jawab atas serangan itu bermarkas di Suriah. Meskipun Angkatan Udara Israel (IAF) menyerang pangkalan pelatihan organisasi teroris di Suriah, pejabat Israel mengklaim bahwa Suriah maupun kedaulatan Suriah bukanlah sasaran yang dimaksud. Hal penting yang perlu diselidiki adalah apakah organisasi teroris itu bertindak atas kemauannya sendiri atau sebagai perantara bagi Suriah atau Iran. Keputusan untuk menyerang pangkalan pelatihan menunjukkan bahwa pertanyaan yang lebih besar mengenai kemungkinan peran Suriah atau Iran telah dikesampingkan. Meskipun demikian, analisis geopolitik yang canggih memerlukan penentuan hubungan antara aktor negara-bangsa dan aktor non-negara untuk menilai identitas sasaran yang sah untuk serangan balik dengan paling akurat.

Argumen ini tampaknya tidak jujur karena kedaulatan Suriah jelas dilanggar oleh pelanggaran wilayah udara Suriah oleh IAF.

Sebaliknya, serangan IAF terhadap fasilitas yang diidentifikasi sebagai instrumen bagi upaya Suriah untuk mengembangkan kemampuan nuklir dapat dikatakan berbeda karena serangan sebelumnya diarahkan ke pangkalan teroris (yang berlokasi di Suriah), sedangkan serangan terakhir ditujukan pada target Suriah tertentu. Meskipun demikian, kedua serangan tersebut melanggar kedaulatan Suriah; pertanyaannya adalah apakah terorisme atau kontraterorisme membenarkan pelanggaran kedaulatan negara-bangsa ketika negara-bangsa bukanlah target yang dituju.

Serangan Korea Utara yang dilaporkan terhadap Sony: Jika aktor non-negara (Kelompok X) melakukan serangan atas nama Korea Utara, Amerika Serikat harus menyelesaikan dilema

berikut dalam menentukan siapa yang bertanggung jawab atas serangan tersebut: (1) Apakah Kelompok X bertanggung jawab atas serangan tersebut, dan (2) apakah komunitas intelijen dapat mengidentifikasi para aktor tersebut, atau apakah mereka target yang sah, atau apakah Korea Utara target yang sah? Jika Amerika Serikat menganggap Korea Utara bertanggung jawab atas serangan terhadap Sony, keputusan untuk menyerang Korea Utara mengharuskan penentuan serangan terhadap Sony Pictures sama dengan menyerang Amerika Serikat. Namun, realitas geopolitik dan militer dengan tegas menunjukkan bahwa menyerang Grup X berbeda dengan menargetkan Korea Utara.

Meskipun Sony, tidak diragukan lagi, merupakan perusahaan besar dan penting yang menyerang kekayaan intelektualnya, hal itu tidak sama dengan melakukan tindakan terorisme fisik terhadap target sipil Amerika. Perlu dicatat, seorang pembaca yang membaca draf sebelumnya tidak setuju dengan saran tersebut dan berpendapat bahwa serangan terhadap perusahaan sama dengan serangan terhadap negara-bangsa, karena perusahaan sangat penting bagi negara-bangsa. Perbedaan antara terorisme siber, terorisme konvensional, dan peperangan tradisional disorot oleh pertanyaan-pertanyaan yang diberikan kemudian.

Seperti yang terlihat dari contoh-contoh sebelumnya, baik dengan terorisme konvensional maupun contoh Korea Utara atau Sony, menentukan target yang sah sering kali menjadi isu yang paling diperdebatkan. Namun, hal itu bukan hanya yang paling diperdebatkan, tetapi juga yang paling penting. Untuk menanggapi, dan menanggapi secara proporsional, tanggapan itu harus diarahkan terhadap target yang sah. Mari kita pertimbangkan contoh-contoh berikut untuk melanjutkan pembahasan kita tentang apa yang merupakan target yang sah.

Pertimbangkan hal berikut: Anda sering bepergian untuk bekerja; minggu ini Anda duduk di Bandara dan Anda mengakses Wi-Fi gratis di bandara. Ini adalah fasilitas yang telah diterapkan oleh banyak bandara selama beberapa tahun terakhir, dan banyak pelancong tidak hanya sering mengaksesnya, tetapi juga sangat diuntungkan olehnya. Banyak pelancong menggunakan waktu ini untuk mengejar ketinggalan pekerjaan, menanggapi korespondensi, atau menonton episode terbaru acara favorit mereka di Netflix.

Namun, banyak ahli berpendapat bahwa zona Wi-Fi gratis merupakan sarang empuk bagi peretas dunia maya. Mereka mengatakan, dengan mengakses Wi-Fi gratis, Anda secara bersamaan membuka pintu depan dan memungkinkan penyerang dunia maya menembus sistem komputer Anda. Sekarang, bayangkan lebih jauh bahwa seorang penyerang dunia maya, yang mengakses informasi Anda melalui layanan Wi-Fi gratis di Bandara, mengaksesnya melalui komputer kantor mereka di kantor tempat mereka bekerja.

Orang ini tidak bertindak dalam lingkup pekerjaannya; Namun, ia menggunakan laptop yang dikeluarkan kantor, perangkat lunak kantor, dan berada di lokasi fisik milik perusahaan. Apakah perusahaan tersebut merupakan target yang sah? Sebagai respons terhadap serangan siber, dapatkah individu yang diserang, korban dalam kasus ini, merespons secara proporsional terhadap perusahaan? Jika tidak, mengapa tidak? Bukankah peretas tersebut menggunakan komputer yang dikeluarkan kantor, perangkat lunak kantor, dan menempati lingkungan milik kantor? Target yang sah sulit didefinisikan, tidak hanya untuk contoh sebelumnya tetapi juga

karena ketidakmampuan untuk mendefinisikan penyerang siber.

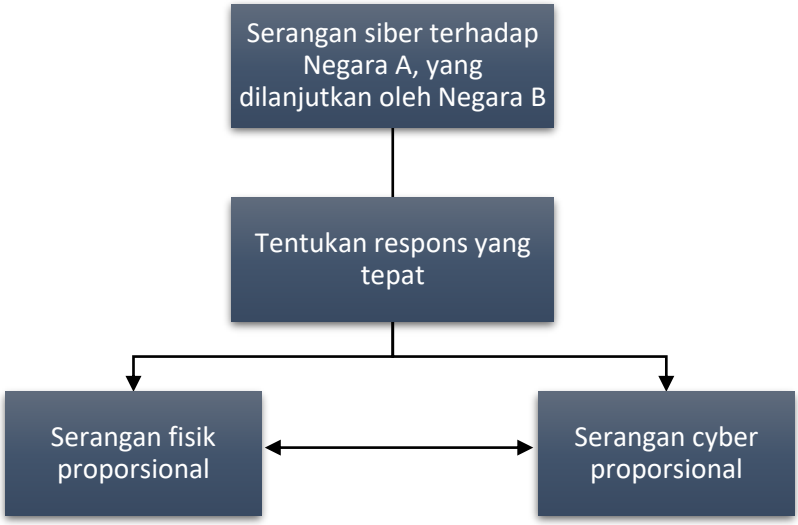
Pertimbangkan hal berikut. Bayangkan Anda adalah korban pencurian identitas. Seperti yang terlihat pada contoh-contoh selanjutnya dalam buku ini, ini adalah masalah yang sangat umum di Amerika Serikat, karena individu mencuri nomor jaminan sosial orang lain, dan menggunakan informasi tersebut untuk membuka kartu kredit, rekening bank, mengambil pinjaman, dan sepenuhnya menggunakan identitas mereka sebagai milik mereka sendiri. Kesulitan setelah ini terjadi adalah dalam perbaikan. Alat apa yang dapat diakses untuk menentukan serangan siber, siapa yang awalnya mencuri identitas? Setelah ditentukan, dapatkah individu tersebut merespons secara proporsional terhadap individu tersebut? Apakah mereka target yang sah? Tidak hanya itu, bayangkan jika informasi Anda dilanggar melalui serangan keamanan siber yang ditujukan terhadap Target, sebuah pusat perbelanjaan populer. Dalam beberapa tahun terakhir, Target telah menjadi korban pelanggaran keamanan siber, yang mengakibatkan 70 juta orang kehilangan privasi kartu kredit mereka akibat peretas.

Akibatnya, identitas Anda telah dicuri. Jadi, berbeda dari contoh di atas, Anda sekarang dapat memastikan perusahaan yang bertanggung jawab atas pencurian identitas Anda; namun, orang yang sebenarnya melakukan peretasan tersebut masih belum teridentifikasi. Karena perusahaan tersebut telah teridentifikasi, apakah mereka merupakan target yang sah? Apakah mereka telah melanggar beberapa tugas, yang mengakibatkan mereka bertanggung jawab atas peretasan tersebut? Apakah wajar dan sah bagi korban untuk membalas mereka? Kemungkinan besar, pada titik ini, tidak.

Tanggapan

Pertanyaan yang paling mendasar adalah apakah tanggapan fisik proporsional dalam menanggapi serangan siber, atau apakah tanggapan yang lebih tepat terhadap serangan siber adalah serangan balik siber? Diartikulasikan ulang: Apakah serangan siber terhadap Negara A oleh Negara B hanya memerlukan serangan balik siber atau apakah keterlibatan fisik merupakan tanggapan yang sah dan proporsional? (Gambar 3.3).

Tanggapan Amerika terhadap serangan terhadap Sony adalah serangan balik siber; menurut sumber yang dapat dipercaya, serangan tersebut dua kali berdampak pada infrastruktur Internet Korea Utara selama setidaknya dua hari. Oleh karena itu, hal itu menunjukkan bahwa tanggapan terhadap serangan siber akan menjadi serangan balik siber, bukan serangan yang secara fisik menargetkan orang yang bertanggung jawab atas serangan awal. Model ini, yang berbeda dari tanggapan kontraterorisme operasional tradisional, memiliki konsekuensi geopolitik yang signifikan karena model ini menjelaskan perbedaan antara pembelaan diri siber dan pembelaan diri tradisional.



Gambar 3.3 Pilihan respons.

Daripada menargetkan individu yang bertanggung jawab atas serangan teroris, kontraterorisme siber berfokus pada infrastruktur, baik milik organisasi penyerang maupun negara. Dalam konteks geopolitik dan hukum internasional, pertanyaannya ada dua: (1) apakah negara telah diserang dan (2) apa batasan respons yang sah?

Jika targetnya adalah korporasi, maka menyerang infrastruktur Internet negara-bangsa tidak proporsional; serangan balik semacam itu memiliki kemampuan untuk berdampak signifikan pada rumah sakit, sistem air, dan moda transportasi. Dalam konteks geopolitik, serangan balik semacam itu secara berbahaya meningkatkan taruhannya. Dalam konteks hukum internasional, hal itu menunjukkan respons yang tidak proporsional.

Meskipun demikian, negara-bangsa memiliki hak dan kewajiban untuk merespons: pertanyaannya adalah apa batasan yang dapat ditoleransi dari respons terhadap serangan siber. Kontur geopolitik dan hukum internasional menunjukkan bahwa pengekangan strategis dan hukum melekat pada proses pengambilan keputusan.

Ada tiga kemungkinan respons yang mencerminkan sensitivitas pertimbangan geopolitik yang lebih luas: (1) menyerang target Korea Utara secara langsung yang menyebabkan kerusakan infrastruktur yang signifikan, (2) serangan terbatas yang paling baik didefinisikan sebagai pengiriman pesan dengan kerusakan infrastruktur yang terbatas, atau (3) menyerang anak perusahaan atau saluran Korea Utara daripada Korea Utara secara langsung.

Mari kita pertimbangkan opsi pertama: menyerang target Korea Utara secara langsung, yang menyebabkan kerusakan infrastruktur yang signifikan. Dalam skenario ini, Amerika akan meluncurkan serangan siber terhadap infrastruktur inti Korea Utara. Ini dapat melibatkan jaringan listrik, sistem air, kontrol lalu lintas (untuk pesawat atau mobil), dan sejumlah opsi lain yang akan sangat memengaruhi kehidupan sehari-hari penduduk Korea Utara. Dengan demikian, dampaknya akan signifikan, lebih dari sekadar serangan balik fisik terbatas yang menargetkan individu tertentu. Apakah itu tepat?

Ketika mempertimbangkan opsi untuk menyerang infrastruktur Korea Utara, satu hal yang perlu dipertimbangkan adalah dampak yang dapat ditimbulkan oleh serangan tersebut.

Serangan siber terhadap infrastruktur memiliki kemampuan untuk menghentikan kehidupan, seperti yang terjadi saat ini. Apakah hal itu tepat dalam situasi yang mirip dengan pertikaian antara Sony dan Korea Utara? Siapa yang akan memutuskan apakah hal itu tepat? Dan terakhir, apakah ada barometer untuk mengukur ketepatan serangan balik siber?

Pilihan kedua melibatkan serangan terbatas terhadap Korea Utara, lebih ke arah pengiriman pesan. Pilihan ini memicu beberapa pertanyaan—apa yang dimaksud dengan pesan yang memadai? Apakah pesan tersebut bervariasi tergantung pada tingkat keparahan tindakan awal? Bagaimana cara memastikan pesan tersebut diterima dengan baik? Apakah memengaruhi jaringan listrik di satu area negara mengirimkan pesan yang efisien? Bagaimana suatu negara dapat menentukan area mana yang menjadi target saat mengirimkan pesan tersebut? Pilihan ini membuka kotak Pandora berisi pilihan yang sulit dikendalikan atau diukur efektivitas atau kebutuhannya dibandingkan yang lain.

Pilihan ketiga mengalihkan dari serangan balik siber terhadap Korea Utara dan berfokus pada serangan balik siber terhadap anak perusahaan atau saluran Korea Utara. Dalam skenario ini, Amerika Serikat telah bertindak atas nama Sony. Secara keseluruhan, Korea Utara tidak mengejar Amerika Serikat, melainkan mereka mengejar Sony. Jadi, tindakan Amerika Serikat dalam menanggapi tindakan tersebut dilakukan atas nama Sony.

Oleh karena itu, opsi ketiga melibatkan Amerika Serikat yang mengejar anak perusahaan atau saluran yang serupa, seperti Sony milik Korea Utara. Hal ini menimbulkan pertanyaan yang sama dari opsi kedua. Saluran apa yang tepat untuk ditindaklanjuti oleh Korea Utara? Tingkat korelasi seperti apa yang harus ada antara Korea Utara dan saluran tersebut agar menjadi mata rantai yang memadai untuk tindakan? Secara keseluruhan, opsi ini juga menciptakan serangkaian opsi yang sulit diatur.

3.4 STUXNET

Menurut sumber terpercaya, fasilitas nuklir Iran diserang oleh virus komputer canggih bernama Stuxnet. Sebagian besar pakar berpendapat bahwa virus tersebut disebarkan oleh Israel dan/atau Amerika Serikat.

- *Apakah Israel dan Amerika Serikat melanggar kedaulatan Iran?*
- *Apakah Israel dan Amerika Serikat terlibat dalam pembelaan diri yang sah?*
- *Apakah Israel dan Amerika Serikat menyatakan tindakan perang terhadap Iran?*

Gambar 3.4 Pertanyaan geopolitik.

Pertanyaan geopolitik dan hukum internasional yang relevan tercantum dalam Gambar 3.4. Menjawab pertanyaan-pertanyaan ini memerlukan kepastian apakah industri nuklir Iran yang baru lahir menimbulkan ancaman bagi Amerika dan/atau Israel dan/atau dunia yang lebih luas. Saat baris-baris ini ditulis, negosiasi yang rumit sedang dilakukan mengenai kemampuan nuklir Iran. Negosiasi tersebut, terlepas dari hasilnya, tidak membahas pertanyaan hukum internasional dan geopolitik yang lebih luas mengenai tanggapan operasional terhadap

ancaman yang ditimbulkan Iran, baik yang dipersepsikan, maupun yang nyata. Selama beberapa tahun terakhir para pemimpin Iran berulang kali mengancam akan menyerang Israel dengan senjata nuklir.

Peringatan Perdana Menteri Netanyahu yang diartikulasikan dengan jelas bahwa Israel tidak akan ragu untuk bertindak lebih awal meyakinkan para pemimpin dunia dan bahwa negosiasi batas kemampuan nuklir Iran sangat penting. Dari perspektif hukum internasional, alasan peringatan Netanyahu adalah hak Israel untuk membela diri. Meskipun Netanyahu mengandalkan Pasal 51, dasar negosiasi tersebut mencerminkan kekhawatiran bahwa ancaman dan peringatan akan benar-benar terwujud, sehingga berdampak signifikan terhadap kawasan sekitar dan komunitas internasional yang lebih luas.

Geopolitik yang efektif menunjukkan pentingnya menahan ancaman dalam konteks manajemen krisis dan pengendalian kerusakan. Namun, meskipun stabilitas regional sangat penting, kewajiban utama kepemimpinan nasional adalah keamanan dan kesejahteraan penduduk sipilnya. Maka, ada ketegangan alami antara keamanan nasional sebagaimana didefinisikan dan diterapkan oleh negara-negara tertentu dan kepentingan regional dan internasional yang lebih luas yang melampaui negara-bangsa tertentu. Siber secara signifikan menyoroti ketegangan ini:

> *"Meskipun isu keamanan siber telah menjadi salah satu yang sangat penting dalam hubungan AS-Tiongkok, langkah-langkah untuk mengatasinya masih bersifat dasar. Pada tanggal 13 April 2013, Menteri Luar Negeri AS John Kerry mengumumkan bahwa kedua belah pihak telah sepakat untuk membentuk kelompok kerja keamanan siber. Seminggu lebih sedikit kemudian, ketua Kepala Staf Gabungan AS, Jenderal Martin Dempsey, mengadakan konferensi bersama dengan Jenderal Tiongkok Fang Fenghui, yang berjanji untuk bekerja sama dengan Amerika Serikat karena konsekuensi dari serangan siber besar 'mungkin seserius bom nuklir.' Jenderal Fang, kepala Staf Umum Tentara Pembebasan Rakyat dan anggota Komisi Militer Pusat, mengindikasikan bahwa ia bersedia untuk membentuk 'mekanisme' keamanan siber, dengan peringatan bahwa kemajuan mungkin tidak cepatlah."*

Percakapan dengan para ahli terkemuka menjelaskan kecanggihan dan kompleksitas Stuxnet. Namun, aspek teknis virus komputer berada di luar jangkauan kami; yang menarik adalah sifat konflik siber. Dalam hal ini, sementara teknologi Stuxnet yang mengesankan telah menarik perhatian yang signifikan, penyelidikan yang lebih luas berfokus pada pembenaran dan konsekuensinya. Dalam hal ini, keputusan yang diambil oleh Kepala Staf Pasukan Pertahanan Israel (IDF), Letnan Jenderal Gadi Eizenkot, untuk mendirikan Cabang Siber† mencerminkan ancaman dan bahaya yang ditimbulkan oleh perang siber dan terorisme. Cabang tersebut akan menggabungkan kemampuan defensif dan ofensif yang mencerminkan signifikansi strategis yang ditingkatkan secara dramatis dari keamanan perang siber-terorisme.

Kombinasi kemampuan ofensif-defensif, dalam konteks prinsip proporsionalitas hukum internasional, menunjukkan bahwa menyerang sistem komputer negara-bangsa adalah bentuk pembelaan diri yang sah, jika target menimbulkan ancaman yang layak. Peringatan: Dampak

virus komputer dan tindakan tambahan lainnya dibatasi pada target yang dianggap sebagai ancaman. Mengenai Iran, memperkenalkan virus komputer mencerminkan proporsionalitas jika tindakan pembelaan diri dibatasi pada industri nuklir yang dapat digunakan untuk tujuan ofensif dan agresif. "Menempatkan serangan siber dalam konteks pengambilan keputusan militer (dan mengasumsikan bahwa aktor negara dan nonnegara secara keseluruhan memiliki proses perencanaan militer yang sama) memiliki implikasi untuk penggunaan serangan siber.

Negara-negara tidak lebih mungkin untuk meluncurkan serangan siber yang menyebabkan kerusakan fisik terhadap AS atau sekutunya setelah Stuxnet daripada sebelum penemuannya, mereka juga tidak mungkin berhenti menggunakan teknik siber untuk spionase dan pemaksaan politik. Kami belum melihat serangan yang merusak secara fisik yang dapat menyebabkan kerusakan, kehancuran, atau korban (berbeda dengan spionase dan kejahatan) terhadap AS dan sekutunya dari negara-negara dengan kemampuan ini karena mereka menilai risiko respons kekerasan terlalu tinggi. Ini adalah alasan yang sama yang mencegah mereka meluncurkan pesawat terbang atau rudal terhadap AS. Namun, praktik dan hukum internasional tidak membenarkan penggunaan kekuatan dalam menanggapi spionase dan kejahatan, sehingga risiko respons kekerasan menjadi kecil dan dapat diterima. Untuk penghargaan kepada perancang Stuxnet, itu ditulis dengan hati-hati untuk menghindari kerusakan tambahan. Penyerang lain mungkin tidak begitu berhati-hati, tetapi ini tidak ada hubungannya dengan akses ke kode Stuxnet.

Lawan potensial masih mempertimbangkan kalkulasi manfaat dan risiko yang sama dalam memutuskan apakah akan menggunakan kekuatan terhadap AS, dan mereka terhalang oleh kemungkinan respons militer AS dengan menggunakan semua aset militer yang dimilikinya, bukan hanya serangan siber. Mereka sekarang dapat mengutip Stuxnet sebagai bagian dari pembenaran publik atas serangan tersebut, tetapi ini akan menjadi alasan, bukan bagian dari pengambilan keputusan mereka. Negara-negara tidak lebih mungkin melancarkan serangan siber terhadap AS atau sekutunya setelah Stuxnet daripada sebelum penemuannya.

Meskipun tingkat keterlibatan AS dalam Stuxnet tidak jelas, artikulasi luas keamanan nasional AS menunjukkan bahwa kepentingan Amerika yang signifikan akan terpengaruh jika Iran menjadi negara berkekuatan nuklir. Lebih langsung—dan mungkin lebih tajam—para pemimpin nasional Israel secara konsisten berpendapat bahwa Iran yang memiliki senjata nuklir menimbulkan ancaman eksistensial terhadap keamanan Israel. Meskipun masih menjadi pertanyaan terbuka, yang menjadi subjek perdebatan intensif dan beragam pendapat, pengenalan Stuxnet dengan jelas menunjukkan konsekuensi operasional dari hubungan antara siber, geopolitik, dan pertahanan diri.

Peringatan yang disebutkan di atas sangat penting: Dampak virus komputer dan tindakan tambahan lainnya dibatasi pada target yang menimbulkan ancaman yang dirasakan. Namun, dapatkah dampak virus komputer dibatasi sedemikian rupa sehingga hanya ditujukan pada target yang menimbulkan ancaman yang dirasakan? Apakah kemampuan untuk menerapkan virus komputer mengurangi kemampuan untuk membatasi virus komputer tersebut? Selain itu, peringatan tersebut menekankan ancaman yang dirasakan. Pertanyaan tambahannya kemudian menjadi, bagaimana seseorang dapat menentukan ancaman yang

dirasakan? Ada banyak hal yang ada yang dapat dianggap sebagai ancaman, tetapi jika negara-negara bereaksi terhadap setiap hal yang mungkin dapat dianggap sebagai ancaman, mereka akan kehabisan waktu dan uang. Oleh karena itu, pertanyaannya kemudian menjadi, ancaman apa yang merupakan ancaman yang dirasakan, dan pada tingkat apa ancaman yang dirasakan itu membenarkan dampak virus komputer?

Untuk menjawab pertanyaan itu, apakah mungkin untuk memastikan bahwa virus komputer benar-benar dibatasi pada ancaman yang ditimbulkan oleh ancaman yang dirasakan? Selain itu, muncul pertanyaan, apakah mungkin untuk mengakses teknologi dan informasi yang diperlukan untuk mengakses dan menjalankan virus komputer yang dapat dibatasi pada ancaman yang dirasakan dan benar-benar dapat memperbaiki ancaman yang dirasakan tersebut? Kita hidup di dunia teknologi yang terus beradaptasi dan berkembang, dan untuk tetap menguasainya diperlukan ketekunan dan uang. Sering kali, mereka yang mampu menjalankan virus komputer atau teknik yang diperlukan terbatas pada beberapa individu.

Jadi, kita tidak hanya memiliki pertanyaan tentang apa yang dianggap sebagai ancaman, dapatkah virus memengaruhi ancaman itu, dapatkah virus yang sama hanya memengaruhi ancaman itu dan tidak menimbulkan dampak yang terlalu signifikan, tetapi dapatkah kita mengakses virus itu, dan dapatkah kita melakukannya dengan aman dan melalui tangan individu yang tepercaya?

Melangkah Ke Depan

Secara taktis dan jangka pendek, ada konsensus luas bahwa Stuxnet dianggap efektif karena berdampak pada pengembangan program nuklir Iran. Namun, apa sebenarnya yang efektif dan berapa lama efektivitas dianalisis? Mungkin yang lebih penting, dari perspektif geopolitik, hal itu menyoroti persyaratan bahwa negara-negara dengan kepentingan bersama yang dapat diidentifikasi mengakui serangan siber, dan terorisme siber menimbulkan ancaman bagi masing-masing negara dan komunitas internasional yang lebih luas.

Pengembangan aliansi strategis—mirip dengan NATO yang dibentuk setelah Perang Dunia II untuk melindungi negara-negara Eropa Barat dari Uni Soviet dan negara-negara Pakta Warsawa—dalam menghadapi perang siber atau terorisme menunjukkan upaya untuk melindungi negara-negara dari serangan yang tidak berwujud, dibandingkan dengan serangan yang berwujud.

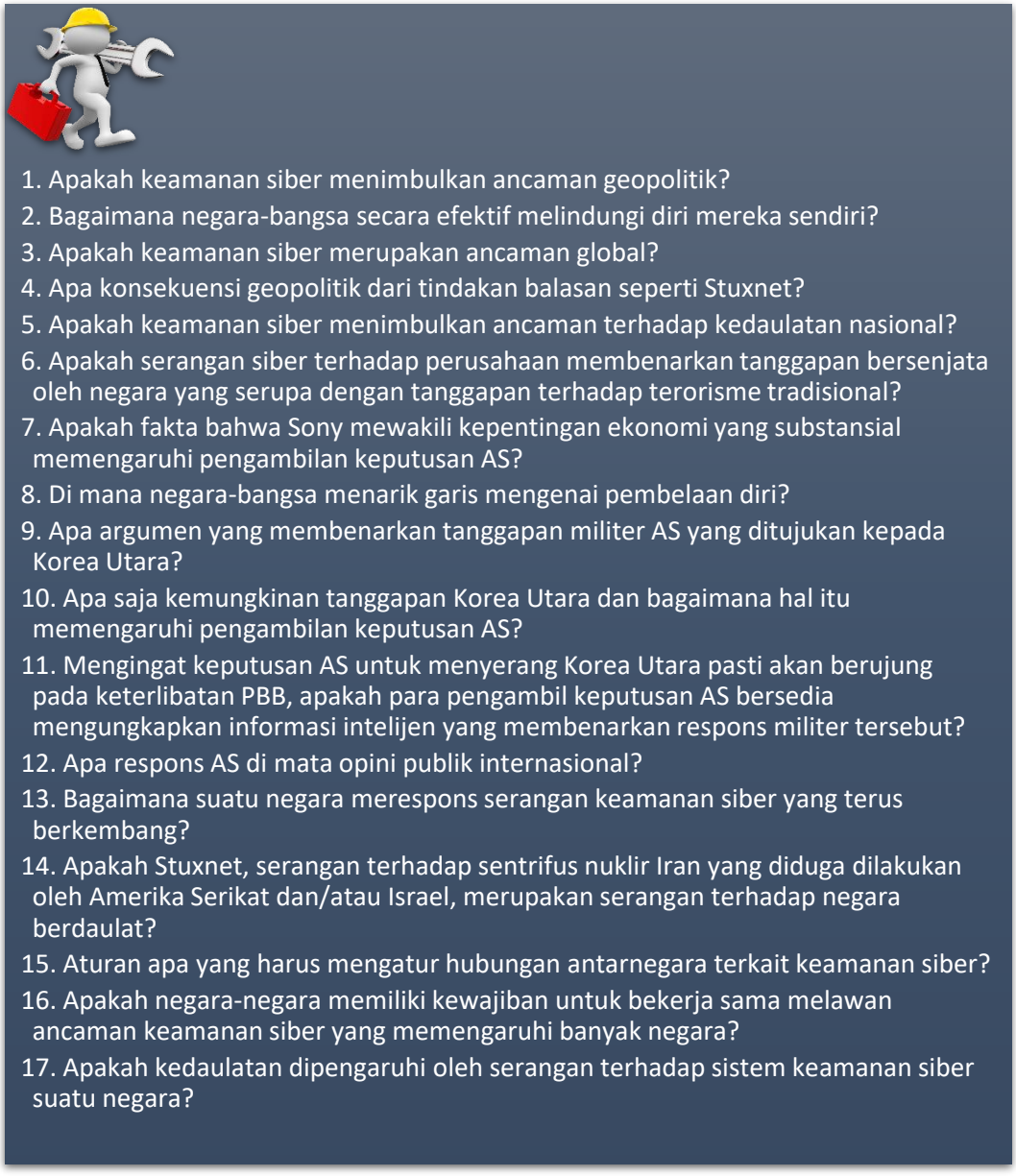
Aliansi semacam itu tidak hanya relevan dengan serangan yang datang dari negara lain, tetapi juga terkait dengan serangan siber yang dilakukan oleh aktor non-negara. Misalnya: ISIS (IS) dapat merekrut anggota baru di Eropa melalui Internet dan, sebagai tambahan, menggunakan Internet untuk tujuan hasutan siber.

Dalam konteks geopolitik, pertanyaan yang relevan adalah apakah negara-negara yang memiliki pemikiran yang sama harus bertindak secara seragam untuk mencegah konsekuensi dari perekrutan siber dan hasutan siber dengan menutup situs web. Untuk melakukannya, diperlukan pengartikulasian ulang ancaman dan pemahaman tentang risiko yang ditimbulkan oleh Internet serta pengakuan bahwa terorisme perang sedang berubah dari serangan fisik tradisional menjadi serangan yang tidak berwujud.

Pada kenyataannya, negara-negara bangsa menghadapi ancaman dari dua sumber

yang berbeda: serangan fisik dan serangan yang tidak berwujud. Transisi ini, dalam konteks stabilitas internasional dan geopolitik, memberikan tantangan baru yang signifikan kepada para pembuat keputusan nasional. Kekuatan Internet, berkenaan dengan perang siber atau terorisme, memerlukan pemahaman tentang kompleksitas geopolitik dan hubungan antara geopolitik dan keamanan siber.

Hal ini menunjukkan, dalam konteks aliansi dan geopolitik internasional, bahwa tindakan sementara termasuk Stuxnet tidak cukup secara strategis. Untuk tujuan itu, aliansi seperti NATO perlu diartikulasikan kembali, diimplementasikan kembali, dan dinyatakan kembali untuk mencerminkan ancaman baru serangan siber ini. Pertanyaan-pertanyaan yang harus dipertimbangkan dalam meninjau Bab 3 diberikan di halaman berikutnya (Gambar 3.5).



Gambar 3.5 Pertanyaan tinjauan.

BAB 4
HUKUM INTERNASIONAL DAN KEAMANAN SIBER

4.1 PENDAHULUAN

Pertanyaan penting yang perlu diajukan adalah apakah hukum tersebut berlaku untuk keamanan siber atau tidak, dan jika hukum tersebut berlaku untuk keamanan siber, apa saja struktur hukum yang relevan?

Bagaimana negara-bangsa menanggapi serangan siber mencerminkan hakikat hukum internasional, yang didasarkan pada hak negara-bangsa untuk membela diri—ketika diserang—sesuai dengan Pasal 51 Piagam PBB. Bahasa Piagam tersebut menunjukkan bahwa hak negara-bangsa untuk terlibat dalam pembelaan diri terbatas pada tanggapan terhadap serangan, yang mencerminkan disonansi intelektual dan praktis. Namun, pembacaan yang lebih luas menunjukkan bahwa hak untuk membela diri sah dalam konteks pembelaan diri preemptif.

Hak tersebut, sesuai dengan pemahaman yang lebih mendalam tentang Pasal 51, didasarkan pada ketersediaan informasi intelijen yang menunjukkan bahwa serangan akan segera terjadi. Kedekatan dalam konteks kontraterorisme operasional terbatas pada individu tertentu yang dianggap menimbulkan ancaman langsung dan segera terhadap keamanan nasional. Mengenai keamanan siber, target yang dituju adalah infrastruktur internet negara-bangsa. Berbeda dengan kontraterorisme tradisional, serangan siber menargetkan infrastruktur negara-bangsa, bukan untuk membunuh individu atau mengebom gedung.

Target yang dituju dari serangan siber adalah infrastruktur—baik negara-bangsa maupun individu—bukan kerusakan fisik atau fisik. Meskipun fokusnya pada infrastruktur, bukan kerusakan fisik atau fisik, kerusakan psikologisnya melemahkan. Konsekuensinya, tentu saja, tidak kalah berbahaya dan dramatis. Bagaimanapun, menargetkan sistem air kotamadya memiliki konsekuensi dan akibat yang signifikan, meskipun fisik serangan tidak disamakan dengan bom bunuh diri.

Mungkin perbedaan itu—fisik bom bunuh diri dibandingkan dengan cara serangan siber—menunjukkan bahwa pembelaan diri yang diterapkan pada yang pertama tidak berlaku untuk yang terakhir. Akan tetapi, dalam konteks potensi bahaya bagi negara bangsa dan hak untuk terlibat dalam pembelaan diri, perbedaan tersebut tidak berlaku karena tidak perlu membatasi diri. Penerapan model semacam itu menunjukkan bahwa negara bangsa tidak akan sepenuhnya terlibat dalam kewajiban utamanya untuk melindungi penduduk sipilnya. Seperti yang dibahas kemudian, pertanyaannya adalah tentang penerapan praktis dan penafsiran hukum internasional.

Pertimbangkan hal berikut:

Pembelaan diri adalah tepat menurut Pasal 51 Piagam PBB dengan asumsi bahwa serangan akan segera terjadi. Istilah operasional yang harus dipenuhi dalam menyimpulkan apakah serangan pendahuluan diperlukan adalah penentuan kedekatan. Menganalisis situasi dan menentukan apakah persyaratan kedekatan terpenuhi atau tidak adalah hal yang sulit.

Perdebatan ini muncul khususnya dalam konteks pembunuhan yang ditargetkan. Untuk membenarkan pembunuhan yang ditargetkan, yaitu, serangan pesawat tanpa awak, kedekatan harus dipenuhi. Secara khusus, individu tersebut harus dianggap menimbulkan ancaman langsung dan segera terhadap keamanan nasional.

Jadi, berikut ini dipertimbangkan:

Mendefinisikan kedekatan sangat penting untuk mengartikulasikan dan menerapkan paradigma pembunuhan yang ditargetkan yang didasarkan pada aturan hukum. Tidak perlu dikatakan, itu jauh lebih mudah diucapkan daripada dilakukan. Kesulitannya ada pada praktik dan prinsip; yang pertama karena para pengambil keputusan lebih suka ruang gerak, yang kedua karena istilah tersebut, pada dasarnya, sulit dipahami, bermasalah, dan dapat ditafsirkan secara luas.

Seperti yang terlihat pada definisi sebelumnya, menentukan kedekatan seringkali sulit tetapi perlu dalam mengevaluasi kebutuhan untuk membela diri. Pembelaan diri tampaknya hanya diperlukan jika individu tertentu menimbulkan ancaman langsung dan segera terhadap keamanan nasional. Lebih mudah bagi pesawat nirawak untuk melihat seseorang mempersiapkan bom atau mengumpulkan pendukung yang berencana untuk mengancam keamanan nasional negara tersebut. Sangat berbeda bagi sistem pemantauan, pesawat nirawak, atau alat lain untuk melihat seseorang mempersiapkan serangan siber, atau saat ini terlibat dalam serangan siber.

Dengan ketidakmampuan untuk melihat individu tertentu yang siap untuk menimbulkan ancaman langsung dan segera, apakah itu berarti membela diri terhadap serangan siber tidak pernah dibenarkan? Bayangkan seorang pelaku bom bunuh diri berhasil melaksanakan rencananya dan membunuh dirinya sendiri, dan beberapa orang lainnya, di pasar yang ramai di dekat pusat kota. Dengan pengawasan, jika intelijen militer mengetahui rencana tersebut, mengenal individu yang melaksanakan rencana tersebut, dan melihatnya berjalan ke pusat kota dengan membawa bom, hanya sedikit yang akan membantah bahwa militer tidak memiliki hak untuk menghilangkan ancaman pada saat itu.

Jelas, pada titik ini, bahwa tanpa tindakan pencegahan untuk membela diri, akan ada korban. Jadi, menurut Pasal 51 Piagam PBB, membela diri tidak hanya pantas tetapi juga diharapkan. Sekarang mari kita pertimbangkan contoh yang berbeda. Bayangkan bahwa di pusat kota yang sama ada kafe pinggir jalan yang ramai. Di dalam kafe itu, seorang individu sedang duduk sendirian di meja mengetik di laptopnya. Di seluruh kafe, beberapa orang lain melakukan hal yang sama, mengetik di laptop mereka dengan intens. Apakah mudah untuk memprediksi siapa, jika ada, dari mereka yang merupakan ancaman? Pada titik ini, apakah ada cara untuk menghilangkan ancaman? Apakah ada kebutuhan untuk tindakan pencegahan untuk membela diri? Mungkin tidak.

Sekarang, bayangkan pada saat yang sama ketika seseorang sedang duduk di kafe sambil mengetik di laptopnya dengan intens, sebuah virus terlepas ke dalam sistem air kota, mematikan sistem penyaringan yang membersihkan dan memurnikan air. Karena itu, air yang terkontaminasi sekarang mengalir melalui semua pipa yang menghubungkan kota, sehingga menghasilkan air yang terlalu tidak aman untuk dimakan, diminum, atau bahkan digunakan

untuk mencuci.

Apakah orang itu sekarang telah melewati ambang batas yang dianggapnya sebagai ancaman langsung dan segera terhadap keamanan nasional? Bayangkan dia memiliki kemampuan untuk melepaskan virus yang sama pada setiap sistem air di Amerika. Namun, hampir mustahil bagi kita untuk mempersempit pekerja komputer mana yang menyebarkan virus tersebut. Jadi, apakah dibenarkan untuk mengambil langkah pencegahan, sebelum kita sampai pada titik ini, untuk menghilangkan ancaman kontaminasi sistem air?

Bayangkan hanya ada sedikit orang di Amerika yang memiliki keahlian dan kemampuan untuk memasukkan virus semacam itu ke dalam sistem air. Apakah pemerintah AS dibenarkan untuk memantau orang-orang tersebut? Apakah dibenarkan untuk melacak pergerakan dan tindakan mereka di komputer? Jika tidak, apa cara terbaik untuk melakukan serangan pendahuluan terhadap serangan siber yang akan segera terjadi?

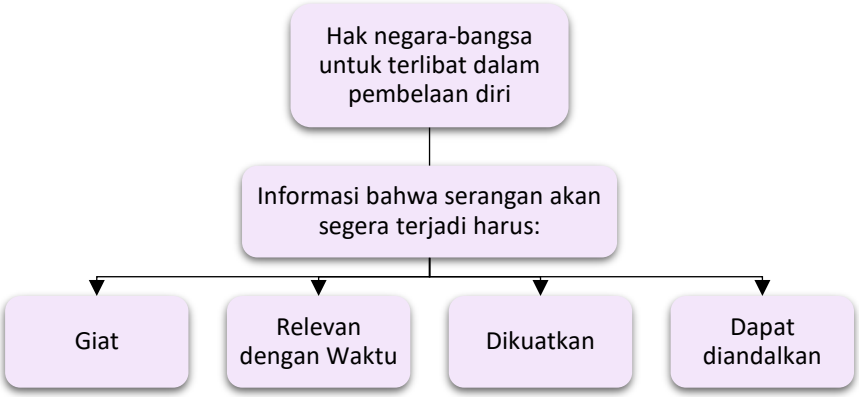
4.2 HAK UNTUK MEMBELA DIRI

Untuk tujuan tersebut, baik dalam konteks terorisme—tradisional (bom bunuh diri) maupun nontradisional (serangan siber)—hak negara-bangsa untuk terlibat dalam pembelaan diri didasarkan pada hal berikut. Jika informasi intelijen yang layak, relevan dengan waktu, didukung, dan dapat diandalkan diterima bahwa suatu serangan akan segera terjadi, maka Pasal 51 Piagam PBB dapat diterapkan yang mencerminkan pembelaan diri yang sah sesuai dengan standar dan prinsip hukum internasional yang dapat diterima. Secara praktis, penerapan Pasal 51 memberikan hak kepada negara-bangsa untuk menyerang secara proaktif guna mencegah serangan keamanan siber yang berhasil.

Analisis tersebut sangat mirip dengan hak negara-bangsa untuk bertindak secara preemptif terhadap suatu serangan sebagaimana didefinisikan secara tradisional dan serangan siber harus dipahami serupa dengan serangan fisik. Dalam konteks tersebut, baik serangan bersenjata maupun serangan tak bersenjata harus dianggap—berkaitan dengan pembelaan diri—sebagai hal yang serupa secara intelektual dan praktis, terlepas dari cara yang digunakan. Oleh karena itu, hak sah negara-bangsa untuk melakukan tindakan pencegahan meluas ke kedua bentuk serangan tersebut (Gambar 4.1).

Perubahan dari serangan kekerasan menjadi serangan tanpa kekerasan, dalam konteks pembelaan diri yang sah, merupakan inti dari serangan siber. Baik serangan tradisional maupun nontradisional mencerminkan serangan terhadap negara-bangsa, dan dalam kedua paradigma tersebut negara-bangsa memiliki hak untuk bertindak secara proaktif. Hak tersebut meluas ke potensi serangan yang berasal dari aktor negara maupun aktor non-negara.

Dalam kedua contoh tersebut—baik serangan oleh aktor negara maupun nonnegara—negara-bangsa memiliki hak untuk melakukan pembelaan diri secara preemptif. Keduanya didasarkan pada analisis empat bagian yang serupa mengenai informasi intelijen, dalam konteks serangan siber, terlepas dari titik asal. Jika tersedia informasi intelijen yang menunjukkan bahwa seorang peretas tengah merencanakan serangan yang dimaksudkan untuk menembus infrastruktur komputer negara-bangsa, sehingga berpotensi menyebabkan kerugian yang signifikan, individu tersebut merupakan target yang sah dalam konteks Pasal 51.



Gambar 4.1 Hak negara-bangsa.

Dari perspektif operasional, individu yang terlibat dalam potensi serangan siber merupakan target yang sah, sama halnya dengan individu yang terlibat dalam potensi serangan fisik, sehingga memperluas Pasal 51 untuk memasukkan serangan bersenjata nonfisik.

Artikulasi Pasal 51 yang luas ini menggabungkan aktor siber negara maupun nonnegara, yang diidentifikasi sebagai pihak yang bertanggung jawab atas potensi serangan siber, sehingga mendefinisikan keduanya sebagai target yang sah. Oleh karena itu, pertanyaan penting dalam diskusi ini adalah apakah seorang peretas merupakan target yang sah, mirip dengan seorang individu yang modus operandinya adalah meledakkan gedung perkantoran, khususnya dan dengan sengaja menargetkan penduduk sipil. Perbedaan antara kedua pelaku ini signifikan dan harus diakui: seorang pelaku bom bunuh diri jelas-jelas berniat membunuh sebanyak mungkin orang. Sebaliknya, seorang penyerang siber tidak berfokus pada pembunuhan orang, sedangkan kematian mungkin merupakan akibat sampingan dari serangan siber.

Gambar 4.1 menunjukkan bahwa negara-bangsa memiliki hak untuk terlibat dalam pembelaan diri jika informasi tentang serangan yang akan segera terjadi layak, relevan dengan waktu, didukung, dan dapat diandalkan. Setiap faktor memainkan komponen penting dalam analisis kedekatan. Selain itu, seperti yang disebutkan sebelumnya, kedekatan adalah kunci dalam menentukan apakah pembelaan diri preemptif merupakan tindakan yang dibenarkan. Untuk memahami sepenuhnya apa yang diperlukan untuk tindakan pembelaan diri preemptif, dan apa yang diperlukan untuk membuktikan kedekatan, mari kita pertimbangkan setiap faktor secara individual.

Faktor pertama melibatkan kelayakan. Agar sesuatu dapat layak, itu berarti sesuatu harus layak, atau dapat terjadi. Misalnya, jika ancaman yang dirasakan akan segera terjadi, para pengambil keputusan harus menganalisis tidak hanya apakah ancaman tersebut benar-benar akan segera terjadi, tetapi yang lebih penting adalah apakah ancaman tersebut layak. Analisis khusus ini akan bergantung pada apakah ancaman tersebut benar-benar dapat dilakukan atau tidak.

Saya membayangkan bahwa banyak pengambil keputusan, termasuk presiden, menerima banyak ancaman setiap hari. Pihak yang menerima ancaman kemudian

berkewajiban untuk menelaah dan menentukan apakah ancaman tersebut mampu dilaksanakan atau layak dilaksanakan. Analisis serupa harus dilakukan terhadap ancaman serangan siber yang akan segera terjadi. Dengan demikian, komponen penting dari analisis kemungkinan terjadinya adalah kemungkinan ancaman tersebut, yang berarti kemampuan ancaman tersebut benar-benar terjadi.

Faktor kedua menekankan relevansi; khususnya ancaman tersebut relevan dengan waktu. Ini melanjutkan poin kemungkinan terjadinya. Agar ancaman dapat segera dilaksanakan, ancaman tersebut tidak hanya harus layak dilaksanakan, tetapi juga harus sesuai dengan waktu. Secara khusus, ancaman yang akan terjadi 10 tahun ke depan kemungkinan besar tidak dianggap segera dilaksanakan dibandingkan dengan ancaman yang akan terjadi besok. Selain itu, ancaman yang telah melewati tanggal kedaluwarsanya juga tidak dianggap relevan dengan waktu. Penekanan pada relevansi waktu berjalan seiring dengan komponen kemungkinan terjadinya. Artinya, ancaman tersebut tidak hanya harus mampu dilaksanakan, tetapi juga harus dilaksanakan dengan segera, yang berarti sesuatu yang akan segera berlalu.

Jika ancaman, baik konvensional maupun siber, akan dilaksanakan dalam lima tahun, ada alasan kuat mengapa tingkat stres terkait ancaman tersebut akan lebih rendah. Sebagian besar berpendapat bahwa ada situasi yang lebih kritis untuk dibahas sebelum ancaman tersebut. Selain itu, banyak yang berpendapat bahwa situasi dan keadaan pada saat itu kemungkinan besar akan berubah, dan ada kemungkinan besar bahwa ancaman tersebut tidak akan dilaksanakan pada saat itu. Pada akhirnya, relevansi waktu, seperti kelayakan, merupakan komponen penting dalam analisis kedekatan.

Faktor ketiga menekankan apakah ancaman tersebut didukung. Ada banyak metode untuk memperkuat, dan tergantung pada bagaimana atau kapan ancaman tersebut didukung, hal itu memengaruhi analisis akhir tentang kedekatan. Bayangkan sebuah ancaman datang dari sumber yang mampu melaksanakan ancaman tersebut. Oleh karena itu, ancaman tersebut layak. Selain itu, ancaman yang sama akan terjadi besok. Oleh karena itu, ancaman tersebut sensitif terhadap waktu. Namun, ancaman tersebut penuh dengan bukti yang tidak berdasar dan tidak jelas apakah akan benar-benar dilaksanakan.

Cara umum untuk menguatkan ancaman teroris konvensional adalah dengan memantau obrolan di antara individu yang terlibat. Sering kali, tim pengawasan dapat memastikan informasi penting melalui kabel telepon, rantai email, atau akun media sosial. Ini adalah bentuk utama dari penguatan. Namun, jika ancaman yang masuk adalah ancaman yang layak dan sensitif terhadap waktu, tetapi tidak didukung, haruskah itu dibenarkan sebagai ancaman yang akan segera terjadi? Haruskah analisis pembenaran yang sama dilakukan baik ancaman tersebut adalah terorisme konvensional atau dunia maya?

Secara keseluruhan, kesulitan dengan penguatan adalah bahwa hal itu ada sebagai kombinasi dari kelayakan dan relevansi waktu. Karena kelayakan menekankan kemampuan atau kapabilitas, penguatan berperan dalam bidang yang sama karena penguatan yang bergantung pada sumber lain menekankan kapabilitas atau aktualitas ancaman. Selain itu, penguatan berkorelasi dengan relevansi waktu karena penguatan dari sumber lain sering kali mengonfirmasi relevansi atau signifikansi ancaman, dan apakah itu benar-benar relevan.

Dengan demikian, pembuktian bukan hanya merupakan elemen penting yang terpisah, tetapi juga mencakup komponen lain dari analisis kedekatan.

Faktor terakhir yang perlu dipertimbangkan adalah keandalan. Keandalan berperan dalam kelayakan, relevansi waktu, dan pembuktian, tetapi juga ada sebagai faktornya sendiri. Keandalan ancaman, dan sumber yang menyajikan ancaman, menekankan perlunya pembuktian. Untuk melakukan pembuktian, langkah pertama adalah menentukan keandalan sumber. Dengan demikian, kedua faktor tersebut saling terkait.

Bayangkan hal berikut: sebuah ancaman telah dikeluarkan terhadap sebuah kota di Amerika Serikat. Ancaman ini berasal dari organisasi teroris yang dikenal yang telah melakukan serangan di masa lalu dan telah bersumpah untuk melakukan serangan di masa mendatang. Kelompok tersebut telah menjanjikan kerusakan fisik terhadap kota tertentu pada tanggal tertentu. Apakah ancaman tersebut akan segera terjadi? Apakah ancaman tersebut memenuhi kelayakan, relevansi waktu, pembuktian, dan keandalan?

Tentu saja. Jika ancaman tersebut berasal dari organisasi teroris yang dikenal, maka pembuktian dan kelayakan sudah cukup. Ancaman tersebut terbukti benar karena berasal dari sebuah organisasi yang sebelumnya ditetapkan sebagai organisasi teroris, yang berarti mereka telah melakukan serangan sebelumnya atau bersumpah untuk melakukan serangan di masa mendatang. Selain itu, ancaman tersebut dapat terjadi karena organisasi tersebut sebelumnya telah menunjukkan kemampuannya dan sifat destruktifnya di masa lalu.

Ancaman yang sama cukup relevan dengan waktu karena merupakan peristiwa yang sedang berlangsung. Karena kelompok tersebut telah melakukan serangan di masa lalu, dan bersumpah untuk melakukannya di masa mendatang, tampaknya ancaman serangan serupa merupakan ancaman yang sedang berlangsung yang tentunya relevan dengan waktu. Dalam hal keandalan, ancaman cukup menjadi pokok yang dapat diandalkan karena merupakan sesuatu yang telah dilakukan di masa lalu dan dapat dengan mudah diciptakan kembali di masa mendatang. Dengan demikian, mudah untuk mengatakan bahwa ancaman tersebut sudah dekat, dan pembelaan diri preemptif dibenarkan berdasarkan Pasal 51 Piagam PBB.

Sekarang, pertimbangkan organisasi yang sama yang telah melakukan serangan teroris konvensional di masa lalu dan telah bersumpah untuk membobol sistem air kota dan telah menutup sistem penyaringan untuk mencemari pasokan air. Apakah ancaman tersebut memenuhi persyaratan yang sama dengan ancaman terorisme konvensional? Apakah penting bahwa ancaman tersebut berbeda dari tindakan teroris sebelumnya? Analisis apa yang harus dilakukan untuk menentukan apakah ancaman tersebut layak? Bagaimana seseorang memastikan apakah organisasi teroris benar-benar mampu melakukan hal tersebut?

Pada akhirnya, analisis kedekatan semakin sulit karena sering kali, dalam dunia maya, ini merupakan situasi baru yang belum pernah ditangani sebelumnya. Selain itu, sering kali sulit untuk mengukur apakah individu atau organisasi benar-benar memiliki kemampuan untuk mengukur serangan tersebut. Secara keseluruhan, analisis kedekatan yang melibatkan kelayakan, relevansi waktu, pembuktian, dan keandalan masih merupakan komponen penting dari analisis, baik dalam terorisme konvensional maupun serangan dunia maya.

4.3 DAMPAK SERANGAN SIBER DAN KERENTANAN INFRASTRUKTUR

Serangan siber berpotensi menyebabkan kerusakan signifikan pada infrastruktur negara-bangsa, mulai dari sistem air hingga menara kontrol lalu lintas udara.

Meskipun film Die Hard 2* menggambarkan bahaya dan konsekuensi peretasan yang berhasil terhadap sistem keamanan bandara, realitas bahaya ini terbukti dengan sendirinya ketika saya diundang untuk mengamati proses pendaratan pesawat jet komersial. Meskipun kompetensi, profesionalisme, dan pelatihan ekstensif para pilot terlihat jelas, namun, yang juga tampak adalah kompleksitas luar biasa dari berbagai bagian yang bergerak yang diperlukan untuk menjamin keselamatan penumpang dan memastikan pendaratan pesawat yang aman.

Hal ini dapat diartikulasikan kembali sebagai berikut: Interaksi antara pilot dan stasiun kontrol lalu lintas udara di berbagai negara, yang berkomunikasi dengan pilot pesawat tambahan yang terbang dalam jarak kontak mata satu sama lain, menyoroti potensi ancaman yang ditimbulkan oleh serangan siber. Realitas ini diutarakan dengan jelas dalam percakapan saya dengan mantan kepala Badan Keamanan Israel.

Ketika ditanya apa satu insiden yang membangunkan Anda pada pukul 3 pagi, tanggapannya langsung dan ringkas. Tanpa pertimbangan apa pun, lawan bicara saya menjawab: serangan terhadap EL-AL.

Ketika saya memintanya untuk menjelaskan tanggapannya, ia menjawab: "Serangan itu tidak hanya akan mengakibatkan hilangnya ratusan nyawa, tetapi juga akan menuntut tanggapan operasional yang luar biasa dari pemerintah."

Meskipun saya mengajukan pertanyaan yang berfokus pada serangan fisik, pertanyaan—dan tanggapan—mencerminkan pendekatan yang berlaku untuk serangan nonfisik. Dalam kedua contoh—serangan fisik dan siber—konsekuensinya akan serupa: hilangnya nyawa yang luar biasa dan tanggapan yang kuat dalam konteks kontraterorisme operasional yang agresif. Namun, sering kali negara-bangsa berbeda dalam memprioritaskan—tentang apa yang paling banyak menuntut sumber daya—serangan fisik atau siber.

4.4 PERANG DAN KEAMANAN SIBER MENURUT HUKUM INTERNASIONAL

Oleh karena itu, dalam mempertimbangkan hubungan antara hukum internasional dan keamanan siber, kesimpulan bahwa peretas siber juga dapat dianggap sebagai target yang sah dalam konteks kontraterorisme operasional dapat dibenarkan. Namun, peringatan dan batasan sangat penting.

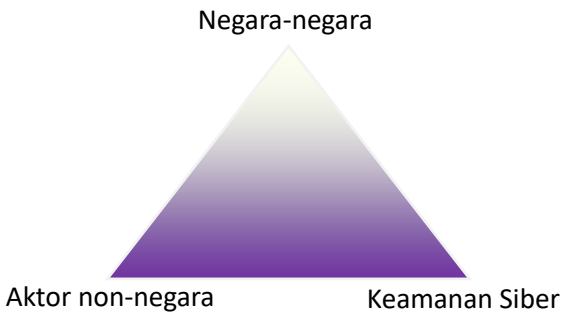
Sehubungan dengan terorisme tradisional, mendefinisikan seorang individu sebagai target yang sah berpotensi menimbulkan konsekuensi dramatis dalam konteks pembunuhan yang ditargetkan atau serangan pesawat nirawak. Memperluas serangan pesawat nirawak atau pembunuhan yang ditargetkan untuk mencakup penyerang siber mencerminkan perluasan signifikan dari penerapan operasional Pasal 51; perluasan yang diusulkan ini menunjukkan bahwa penyerang siber dianggap sama dengan individu yang terlibat dalam serangan fisik.

Perluasan ini dipertimbangkan dengan saksama karena konsekuensinya, baik secara prinsip maupun operasional, signifikan: Seorang individu yang bertanggung jawab atas serangan nonfisik akan dianggap sama beratnya dengan individu yang bertanggung jawab atas serangan fisik yang secara langsung mengakibatkan hilangnya nyawa. Pentingnya hal ini tidak dapat ditekankan secara memadai: akibat sampingan dari serangan siber dapat berupa hilangnya nyawa; maksud langsung dari serangan fisik adalah hilangnya nyawa, namun, sesuai dengan model yang diusulkan ini, mereka yang bertanggung jawab atas kedua jenis serangan tersebut akan dianggap sebagai target yang sah dari serangan pesawat nirawak atau pembunuhan yang ditargetkan.

Keputusan untuk menetapkan peretas tertentu sebagai target yang sah untuk kontraterorisme operasional yang agresif akan bergantung pada penilaian bahwa tidak ada cara lain untuk menetralkan individu tersebut.

Seperti halnya dengan calon pelaku bom bunuh diri, preferensi—dan penekanan—adalah pada penahanan individu tersebut. Namun, jika hal itu terbukti tidak layak secara operasional dan serangan siber yang membahayakan keamanan nasional sudah dekat, maka pembelaan diri preemptif membenarkan tindakan yang serupa dengan yang diterapkan terhadap individu yang merencanakan serangan fisik. Ini adalah esensi dari target yang sah, terlepas dari sifat serangan yang direncanakan (Gambar 4.2). Pembahasan sebelumnya difokuskan pada hubungan segitiga antara negara-bangsa, aktor non-negara, dan keamanan siber dalam konteks Pasal 51.

Dalam mengkaji batasan Pasal 51, selanjutnya kita akan mempertimbangkan apakah serangan siber yang dilakukan oleh negara-bangsa, atau pihak ketiga yang bertindak atas nama negara-bangsa terhadap negara-bangsa lain, membenarkan penerapan Pasal 51. Hal ini dapat dirumuskan kembali sebagai berikut: Apakah serangan siber oleh negara-bangsa yang ditujukan kepada negara-bangsa lain sama dengan tindakan perang tradisional?



Gambar 4.2 Segitiga negara-bangsa.

Dampak dan konsekuensinya signifikan: Jika negara-bangsa yang diserang menyimpulkan bahwa serangan siber oleh negara-bangsa (atau penghubung) setara dengan serangan bersenjata, maka kesimpulan logisnya adalah bahwa keadaan perang mungkin terjadi antara kedua negara-bangsa tersebut. Jika negara-bangsa menyimpulkan bahwa serangan siber setara dengan tindakan perang—dan akibatnya menyatakan perang—maka signifikansi serangan siber telah meningkat secara mendalam.

Konsekuensi dari interpretasi yang diperluas ini, dan penerapan Pasal 51 dan Hukum Perang selanjutnya, menunjukkan paradigma yang kompleks dan rumit mengenai konsekuensi dari melakukan serangan siber. Dalam menerapkan hukum internasional, Indonesia akan diminta—jika menyimpulkan bahwa serangan siber setara dengan serangan bersenjata—untuk menyajikan argumen yang meyakinkan bahwa serangan siber memang merupakan serangan yang membenarkan serangan balik.

Pertanyaan lanjutan yang diperlukan adalah apakah serangan balik akan dibatasi pada serangan balik siber, atau apakah hukum internasional akan menoleransi serangan bersenjata sebagai respons terhadap serangan siber. Jika menentukan bahwa serangan siber awal merupakan tindakan perang, maka keputusan untuk terlibat—untuk menentukan cara dan metode—akan sesuai dengan prinsip dan praktik perang internasional yang diterima.

Kita kembali ke pertanyaan tentang cara respons terhadap tindakan perang dilakukan. Sederhananya: Apakah respons yang sah terhadap serangan siber oleh negara-bangsa adalah serangan balik siber atau serangan bersenjata tradisional sah? Pertanyaan pentingnya adalah menentukan batas-batas pembelaan diri yang sah. Meskipun jawabannya bergantung pada banyak keadaan, kriteria, dan kerugian yang ditimbulkan, parameter umum mungkin menunjukkan bahwa respons yang paling tepat terhadap serangan siber adalah serangan balik siber, bukan serangan bersenjata. Kriteria yang perlu dipertimbangkan bervariasi dari bagaimana kerusakan itu disebabkan dan jumlah kerusakan yang ditimbulkan.

Contoh 1: *Jika para pengambil keputusan menyimpulkan bahwa serangan terhadap Sony setara dengan serangan terhadap Amerika Serikat, maka serangan siber tersebut (baik secara langsung oleh Korea Utara atau tidak langsung oleh pihak ketiga) membenarkan deklarasi perang Amerika Serikat terhadap Korea Utara;*
Contoh 2: *Jika para pengambil keputusan menyimpulkan peretasan terhadap infrastruktur komputer pemerintah Amerika Serikat dilakukan oleh peretas Tiongkok saat itu, dan peretasan ini sama saja dengan serangan terhadap Amerika Serikat, maka pada prinsipnya, Amerika Serikat dapat menyatakan perang terhadap Tiongkok.*

Gambar 4.3 Contoh kritis.

Kesesuaian ini dilihat baik melalui lensa hukum internasional maupun pengadilan hukum internasional; diragukan bahwa masyarakat internasional akan memandang positif serangan militer sebagai respons terhadap serangan siber. Pihak yang menentang sebagian besar akan berfokus pada prinsip-prinsip hukum internasional tentang proporsionalitas dan kebutuhan militer.

Namun, respons militer terbatas—yang secara khusus menargetkan aktor negara atau aktor nonnegara yang bertindak sebagai penghubung bagi negara-bangsa—mungkin dipahami sebagai cerminan respons negara yang terukur dalam konteks pembelaan diri terbatas. Meskipun demikian, legitimasi dan keabsahan tindakan negara akan bergantung pada keberhasilan, dan meyakinkan, pembuktian hubungan antara negara penyerang dan serangan

siber.

Sehubungan dengan paradigma Korea Utara–Amerika Serikat, legitimasi respons Amerika Serikat akan ditingkatkan secara signifikan jika responsnya adalah serangan Internet terhadap Korea Utara daripada serangan militer tradisional terhadap Korea Utara. Ini berarti bahwa paradigma tank versus tank yang berlaku untuk peperangan tradisional tidak akan relevan dengan keamanan siber atau pembelaan diri siber. Sebaliknya, respons yang dapat diterima akan dibatasi pada serangan balik siber terhadap infrastruktur negara tersebut.

Alih-alih menyerang target fisik, target yang sah (dalam paradigma negara-negara) akan dibatasi pada sistem komputer negara-bangsa, bukan target fisik. Usulan ini mencerminkan pendekatan yang seimbang yang secara bersamaan mengakui fakta bahwa serangan siber mirip dengan tindakan perang sekaligus membatasi pembelaan diri pada serangan balik siber, bukan fisik. Penerapan model ini mengharuskan negara-bangsa yang diserang memiliki tindakan balasan siber yang sangat canggih yang mampu menembus infrastruktur negara-bangsa yang menyerang.

4.5 PARADIGMA PENERAPAN PRAKTIS HUKUM INTERNASIONAL

Maka, ada tiga paradigma yang relevan berkenaan dengan pertemuan antara hukum internasional dan keamanan siber (Gambar 4.4).

Penerapan praktis dari ketiga paradigma tersebut mengharuskan negara-bangsa untuk mengembangkan kebijakan dan kemampuan serangan balik siber yang layak secara operasional. Dengan demikian, negara-bangsa akan memastikan bahwa mereka melakukan pembelaan diri sesuai dengan prinsip-prinsip hukum internasional yang berlaku; Hal ini penting untuk penerapan prinsip proporsionalitas yang sah.

Negara-bangsa yang diserang, untuk memenuhi proporsionalitas dalam konteks hukum internasional, harus mengembangkan kemampuan penanggulangan siber dalam menanggapi serangan siber. Pentingnya kemampuan penanggulangan siber adalah bahwa hal itu sekaligus memfasilitasi pembelaan diri sambil menghormati prinsip-prinsip hukum internasional.

1. *Negara-bangsa memiliki hak untuk melindungi dirinya sendiri terhadap negara-bangsa yang menyerang dan aktor non-negara yang bertanggung jawab atas serangan siber;*
2. *Menyerang infrastruktur negara-bangsa membenarkan adanya respons; pertanyaan operasionalnya adalah apakah respons yang sah dibatasi pada serangan balik siber terhadap infrastruktur Internet negara penyerang atau keterlibatan fisik yang menargetkan negara yang secara khusus diidentifikasi sebagai pihak yang bertanggung jawab atas serangan siber;*
3. *Saluran, yang bertindak atas nama negara-bangsa, menghadirkan dilema yang berbeda dari aktor non-negara dan lebih mirip dengan model negara-bangsa; pengambilan keputusan operasional mengenai saluran, dalam konteks pembelaan diri, bergantung pada sejumlah faktor termasuk apakah infrastruktur Internet merupakan target yang mudah diidentifikasi, tingkat keterlibatan yang dapat ditentukan oleh individu tertentu, dan kerusakan yang disebabkan pada negara-bangsa.*

Gambar 4.4 Paradigma yang relevan.

Paradigma pertama menekankan negara-bangsa memiliki hak untuk melindungi dirinya sendiri terhadap negara-bangsa yang menyerang dan aktor non-negara yang bertanggung jawab atas serangan siber. Pertama, mari kita asumsikan, demi asumsi saja, Rusia meluncurkan senjata nuklir terhadap Indonesia.

Tampaknya sangat sedikit orang, jika ada, yang akan berpendapat bahwa Indonesia sekarang memiliki hak untuk tanggapan yang proporsional dalam membela diri. Sekarang, mari kita asumsikan, Rusia telah meluncurkan serangan siber terhadap Indonesia; khususnya, Rusia telah mematikan semua sistem komputer di menara kontrol lalu lintas udara di setiap bandara. Karena itu, tidak ada teknisi penerbangan yang mampu mengarahkan pesawat lepas landas, mendarat, atau terbang di langit.

Ini adalah risiko yang signifikan. Tanpa menara pengawas lalu lintas udara, pesawat tidak tahu apakah mereka dapat mendarat dengan sukses, apakah mereka terbang di jalur penerbangan yang sama dengan pesawat lain, atau apakah mereka diizinkan untuk lepas landas. Hal ini dapat mengakibatkan sejumlah besar kematian. Jadi, seperti senjata nuklir yang membenarkan respons proporsional dalam membela diri, demikian pula penutupan menara pengawas lalu lintas udara. Dalam hal serangan siber balasan, serangan siber oleh negara-bangsa terhadap negara-bangsa lain adalah pertanyaan yang lebih mudah dijawab dalam hal membela diri secara proporsional.

Sekarang, mari kita asumsikan sebagai contoh, menara pengawas lalu lintas udara ditutup, tetapi bukan oleh Rusia. Kali ini ditutup oleh badan independen yang dioperasikan di Rusia, dengan karyawan Rusia, tetapi bertindak secara independen. Apakah Indonesia dibenarkan dalam serangan siber balasan terhadap Rusia? Apakah dibenarkan dalam serangan siber balasan terhadap badan independen? Apakah harus salah satu atau yang lain, atau apakah Indonesia dibenarkan dalam serangan balik siber terhadap Rusia, badan independen, atau keduanya? Ini adalah pertanyaan sulit yang harus dijawab terkait serangan siber.

Dengan paradigma kedua, pertanyaan operasionalnya adalah apakah respons yang sah dibatasi pada serangan siber balasan terhadap infrastruktur Internet negara penyerang atau keterlibatan fisik yang menargetkan negara yang bertanggung jawab atas serangan siber. Jadi, melanjutkan contoh sebelumnya, bayangkan Rusia telah meluncurkan serangan siber terhadap menara pengawas lalu lintas udara.

Jika respons dibenarkan, yang menurut sebagian besar orang memang demikian, dapatkah respons hanya berupa serangan siber, atau dapatkah respons itu dibenarkan sebagai pembelaan diri dengan melakukan serangan fisik terhadap pasukan Rusia? Apakah tindakan perang fisik merupakan respons proporsional terhadap serangan siber? Terakhir, dengan paradigma ketiga, kita akan melanjutkan contoh sebelumnya. Bagaimana jika, setelah serangan terhadap menara pengawas lalu lintas udara, ditentukan bahwa badan independen tersebut bertindak atas nama Rusia.

Dapatkah melakukan serangan balik proporsional terhadap Rusia? Atau haruskah itu dilakukan terhadap badan independen? Lebih jauh, dapatkah melakukan serangan fisik, baik terhadap Rusia, atau badan independen, atau haruskah tetap melakukan serangan siber balasan proporsional? Ini semua adalah pertanyaan sulit yang muncul akibat serangan siber.

Melangkah Maju

Jika berargumen bahwa serangan terhadap setiap aset, perusahaan, atau individu Amerika sama saja dengan menyerang Indonesia, maka pintu pembelaan diri terbuka melampaui apa yang seharusnya ditoleransi oleh hukum internasional.

Untuk tujuan tersebut, berikut ini direkomendasikan sebagai cerminan pendekatan yang seimbang: Serangan terhadap Sony—jika didefinisikan sebagai serangan terhadap Indonesia—harus ditanggapi hanya dengan serangan balik siber. Respons tersebut harus proporsional, ditujukan secara eksklusif pada infrastruktur siber negara penyerang dan bukan pada target fisik. Tidak ada argumen yang masuk akal bahwa individu tertentu—penghubung atau aktor negara—dapat menjadi target dalam menanggapi serangan terhadap perusahaan.

Namun, jika individu yang terlibat dalam serangan siber memiliki potensi yang mendesak untuk menyebabkan kerugian fisik, maka orang tersebut adalah target yang sah sesuai dengan peringatan yang telah dibahas sebelumnya. Sesuai dengan hukum internasional, respons terhadap serangan siber harus proporsional, informasi intelijen harus menunjukkan bahwa serangan akan segera terjadi, dan negara-bangsa harus menunjukkan tidak ada alternatif selain keterlibatan fisik.

Jika kriteria ini terpenuhi secara keseluruhan, maka negara-bangsa memiliki kemampuan untuk melibatkan secara fisik seseorang yang berpotensi menyebabkan kerugian fisik terhadap penduduk sipil negara tersebut termasuk serangan siber. Itu memang memerlukan pengakuan bahwa hukum internasional, berkenaan dengan pembelaan diri, perlu diartikulasikan ulang untuk memperhitungkan serangan siber dan konsekuensinya. Berikut ini adalah pertanyaan yang perlu dipertimbangkan saat meninjau Bab 4 (Gambar 4.5).

Latihan Soal

1. Apakah hukum internasional berlaku untuk keamanan siber?
2. Apakah hukum internasional mengizinkan negara-bangsa untuk melindungi diri dari serangan siber?
3. Apakah serangan terhadap korporasi sama dengan serangan terhadap negara-bangsa?
4. Bagaimana target yang sah didefinisikan dalam serangan siber?
5. Haruskah ada tingkat kerja sama tertentu antara badan pemerintah, penegak hukum setempat, dan badan korporasi?
6. Apakah negara-negara memiliki kewajiban untuk saling berbagi informasi yang relevan mengenai masalah atau serangan keamanan siber?

Gambar 4.5 Pertanyaan tinjauan.

BAB 5
PENGEMBANGAN DAN IMPLEMENTASI KEBIJAKAN KEAMANAN SIBER

5.1 PENDAHULUAN

Dalam bab ini, fokus akan diberikan pada pengembangan dan implementasi kebijakan keamanan siber. Kebijakan memerlukan analisis menyeluruh dan interdisipliner terhadap masalah tersebut untuk mengembangkan respons yang paling efektif terhadap ancaman yang ditimbulkan oleh serangan siber.

Dalam konteks pemeriksaan kebijakan, pertanyaan pertama yang harus kita tanyakan pada diri sendiri adalah apakah kita benar-benar dapat mempertahankan diri terhadap penyerang siber. Dalam konteks kebijakan, jika tidak ada tindakan balasan yang efektif terhadap siber, maka mengembangkan kebijakan balasan siber menimbulkan tantangan yang luar biasa. Oleh karena itu, kebijakan bergantung pada tindakan praktis yang efektif untuk menanggapi serangan siber dan ancaman siber.

Salah satu pertanyaan penting dalam mengembangkan kebijakan balasan siber adalah menentukan definisi tindakan balasan siber yang efektif. Pentingnya hubungan antara kebijakan dan efektivitas tindakan balasan tidak dapat cukup ditekankan. Dalam banyak hal, keduanya harus kongruen, mencerminkan koherensi dan simetri. Hal ini khususnya sulit ketika baik sifat ancaman siber maupun penanggulangan ancaman yang diperlukan didefinisikan sebagai terdiri dari beberapa bagian yang bergerak. Hal ini tidak hanya mirip dengan teka-teki gambar tetapi juga teka-teki gambar yang mencerminkan lebih banyak hal yang tidak diketahui daripada yang diketahui.

Pertanyaan Yang Perlu Ditanyakan

Pertanyaan yang menuntut perhatian kita bersifat kompleks; pertanyaan tersebut juga menyoroti ketidakpastian yang melekat pada keamanan siber, apalagi artikulasi dan implementasi kebijakan yang koheren. Pertanyaan **pertama** mempertimbangkan apakah semua serangan siber dapat dicegah atau tidak.

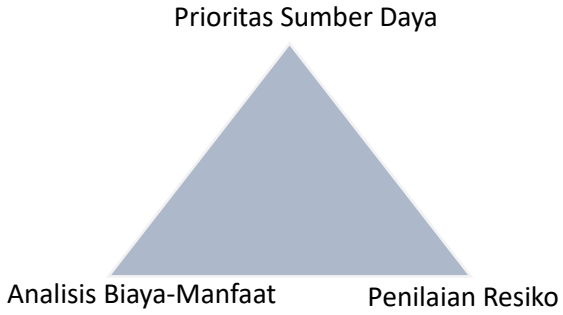
Meskipun jawabannya, jelas, tidak, penting untuk diingat bahwa para pengambil keputusan nasional terlibat dalam retorika yang menciptakan ilusi bahwa terorisme dapat dikalahkan, sehingga menciptakan harapan yang salah dan tujuan yang tidak dapat dicapai. Hal ini pada dasarnya berbahaya karena masyarakat, setelah pengumuman tersebut, dapat secara wajar (dari sudut pandangnya) berasumsi bahwa mereka sepenuhnya terlindungi dari terorisme dan serangan siber. Ini, tentu saja, adalah paradigma yang salah dengan konsekuensi negatif dari sudut pandang kebijakan dan publik.

Pertanyaan **kedua** mempertimbangkan apakah keamanan siber efektif, jika 50% atau 75% serangan yang diketahui berhasil dinetralkan. Pertanyaan **ketiga** menentukan apakah tolok ukur yang tepat mengenai efektivitas murni kualitatif? Jika, misalnya, serangan besar berhasil dicegah tetapi serangkaian serangan kecil berhasil (dari sudut pandang penyerang),

apakah itu berarti kebijakan keamanan siber tidak efektif?

Keempat, apakah pencegahan satu serangan besar mencerminkan kebijakan keamanan siber yang efektif? Selain itu, apakah ada beberapa target—Pentagon sebagai contoh—yang menganggap bahwa pencegahan serangan siber yang berhasil sangat penting dari perspektif keamanan nasional sehingga untuk memastikan pencegahannya, serangan lain dapat ditoleransi? Meskipun sulit untuk menentukan serangan mana yang memenuhi syarat sebagai dapat ditoleransi dan mana yang tidak, hal itu menimbulkan pertanyaan tentang berapa biaya yang bersedia kita tanggung untuk menghindari serangan terhadap infrastruktur penting, seperti Pentagon.

Pertanyaan tersebut diajukan dalam konteks prioritas sumber daya, analisis biaya-manfaat, dan penilaian risiko (Gambar 5.1). Demikian pula, dalam konteks segitiga yang diusulkan ini, apa dampak signifikan dari peretasan kartu kredit perorangan? Sejauh mana, dari perspektif kebijakan, hal ini (peretasan kartu kredit perorangan) memerlukan perhatian dan sumber daya yang signifikan? Dan terakhir, dari perspektif kebijakan, apa dampak peretasan yang berhasil terhadap perusahaan asuransi atau kesehatan besar yang mengakibatkan terungkapnya catatan pribadi?



Gambar 5.1 Segitiga sumber daya.

Menjawab pertanyaan-pertanyaan ini mengharuskan pejabat keamanan nasional, eksekutif bisnis senior, pemimpin pemikiran, pejabat penegak hukum, dan politisi untuk merumuskan kebijakan keamanan siber/anti-keamanan siber yang dapat diimplementasikan, praktis, dan legal. Hal ini menimbulkan tantangan besar, karena hakikat kebijakan yang didasarkan pada supremasi hukum tentu mencerminkan pengakuan terhadap batas-batas kekuasaan negara.

Dalam mempertimbangkan pertanyaan-pertanyaan di atas, contoh akan membantu menunjukkan kesulitan yang muncul pada setiap pertanyaan. Pertanyaan pertama mempertimbangkan apakah semua serangan siber dapat dicegah atau tidak. Bayangkan sebuah perusahaan besar, khususnya yang bergerak dalam bisnis penyimpanan catatan pribadi individu, seperti sistem rumah sakit. Anda adalah kepala eksekutif (CEO) sistem rumah sakit ini dan kepala intelijen Anda memberi tahu Anda bahwa akan dibutuhkan biaya yang sangat besar setiap tahun untuk membangun perlindungan terhadap potensi serangan keamanan siber.

Selain itu, tidak ada jaminan bahwa serangan itu akan terjadi atau bahwa perlindungan itu akan efektif. Jika Anda bergerak dalam bisnis yang membuat perusahaan Anda menguntungkan, seperti kebanyakan CEO, apakah Anda akan membayar jumlah yang sangat besar untuk perlindungan terhadap potensi serangan dengan kemungkinan bahwa perlindungan itu bahkan tidak efektif? Kemungkinan besar tidak.

Pertanyaan kedua mempertimbangkan efektivitas sistem keamanan siber. Apakah sistem perlindungan keamanan siber efektif, jika hanya menetralkan 50%–75% serangan siber? Bayangkan Anda adalah CEO perusahaan pada paragraf sebelumnya dan biaya perlindungan keamanan siber jauh lebih besar daripada kerugian yang diderita oleh 50% serangan siber. Artinya, sebagai perusahaan, Anda membayar lebih banyak untuk perlindungan, namun, ancaman kerugian tidak terlalu signifikan. Apakah layak untuk terus membayar perlindungan keamanan siber? Mungkin tidak. Apakah bijaksana? Tentu saja.

Pertanyaan ketiga mempertimbangkan tolok ukur yang memadai dalam menentukan efektivitas kebijakan keamanan siber. Tampaknya efektivitas akan diukur dari berapa banyak serangan siber yang digagalkan oleh kebijakan tersebut, untuk menentukan apakah suatu kebijakan efektif. Namun, seringkali sulit untuk menentukan berapa banyak serangan yang digagalkan, karena serangan tersebut tidak terjadi; oleh karena itu, tidak ada data yang menunjukkan efektivitas kebijakan tersebut. Kesulitan dalam mengukur efektivitas lebih lanjut berperan dalam keputusan CEO dalam menentukan apakah layak untuk berinvestasi dalam mekanisme perlindungan tersebut.

Pertanyaan terakhir yang perlu dipertimbangkan adalah apakah pencegahan satu serangan keamanan siber besar mencerminkan kebijakan keamanan siber yang efektif. Hal ini lebih cenderung mendorong CEO untuk berinvestasi dalam kebijakan semacam itu.

Dengan menunjukkan kepada CEO maupun pemegang saham bahwa kebijakan tersebut menghemat ribuan dolar, waktu yang dihabiskan untuk memulihkan data yang hilang, dan poin reputasi, CEO dan pemegang saham akan lebih cenderung berinvestasi dalam biaya yang sangat besar.

Masing-masing pertanyaan paradigma ini menunjukkan kesulitan dalam menciptakan kebijakan keamanan siber. Kesulitan-kesulitan ini ada di setiap level dan sering kali sulit diatasi dan menemukan titik temu di antara para direktur.

5.2 MEMBUAT KEBIJAKAN

Menciptakan kebijakan siber yang efektif dan berakar pada batasan kekuasaan memerlukan definisi yang sempit mengenai aset apa yang perlu dilindungi. Hal ini menuntut para pemangku kepentingan untuk menganalisis kerentanan dan kapabilitas secara menyeluruh dan realistis. Analisis tersebut ditingkatkan secara signifikan dengan penerapan model triangulasi yang dijelaskan di bagian sebelumnya.

Kebijakan tidak dapat dipandang begitu saja; harus ada pertimbangan cermat terhadap pertimbangan taktis dan strategis yang mencerminkan pengakuan terhadap tujuan jangka pendek dan jangka panjang. Mengenai keamanan siber, kebijakan dipengaruhi oleh skala kerentanan yang ditunjukkan oleh jumlah serangan dan kegagalan berbagai pemangku

kepentingan untuk mengartikulasikan tindakan pencegahan yang dapat diterapkan secara lengkap. Pertukaran dengan para ahli dari berbagai negara menunjukkan paradigma yang mencerminkan coba-coba.

Meskipun dapat dimengerti mengingat ancaman yang relatif baru dikombinasikan dengan ketidakpastian yang ditunjukkan mengenai mekanisme respons, hasilnya sebagian besar adalah kebijakan yang menunjukkan petinju kelas berat yang linglung di atas ring. Ini bukan berarti para pemangku kepentingan tidak akan mengembangkan kebijakan dan model respons yang lebih efektif, tetapi serangkaian serangan siber yang berhasil menunjukkan bahwa model pencegahan-respons siber yang efektif memerlukan perhatian yang signifikan.

Secara keseluruhan, siber tidak dapat dicegah 100%, dan ada konsekuensi psikologis yang signifikan. Mendefinisikan istilah sangat penting untuk pengembangan kebijakan; pada diskusi itulah kami mengarahkan perhatian penulis.

5.3 MENDEFINISIKAN ISTILAH EFEKTIVITAS

Definisi ini menggabungkan premis berikut: (1) terorisme tidak dapat dicegah 100%; (2) kontraterorisme harus memiliki komponen jangka pendek (taktis) serta jangka panjang (strategis); dan (3) kontraterorisme harus dilakukan sambil menyeimbangkan kepentingan yang bersaing dari kehidupan manusia, biaya finansial, dan kebebasan sipil.

Terorisme tidak dapat dicegah 100%

Analis keamanan cenderung membingkai tindakan kontraterorisme yang direkomendasikan dalam paradigma efektivitas yang menuntut perlindungan yang sangat aman. Akan tetapi, harus dinyatakan dengan jelas bahwa terorisme tidak dapat dicegah 100%. Hanya karena serangan teroris berhasil tidak berarti tindakan penanggulangan terorisme yang ada tidak efektif. Kebalikannya juga benar: Tidak adanya serangan teroris tidak serta merta menunjukkan tindakan penanggulangan terorisme yang ada efektif.

Pertimbangkan poin pertama ini bahwa dalam menganalisis efektivitas, konsep penting yang harus diterima adalah bahwa terorisme tidak dapat dicegah 100%. Selain itu, seperti yang disebutkan di atas, lebih sulit lagi untuk mengukur efektivitas tindakan antiterorisme berdasarkan ada atau tidaknya serangan teroris. Jadi, cabang pertama definisi efektivitas, bahwa terorisme tidak dapat dicegah 100%, sangat penting untuk diterima sebelum kebijakan keamanan siber yang solid dapat dibuat.

Jadi, dengan penerimaan bahwa terorisme tidak dapat dicegah 100%, apa tolok ukur yang harus digunakan? Berapa persentase yang kita setujui? Lebih khusus lagi, jika tindakan antiterorisme keamanan siber mencegah 50% serangan teroris, apakah itu cukup? Atau apakah 75% cukup? Atau, apakah ada jumlah yang ditetapkan, atau apakah itu lebih didasarkan pada jenis serangan yang dicegah?

Pada akhirnya, sangat sulit untuk mengukur efektivitas kebijakan keamanan siber berdasarkan angka atau persentase tertentu. Pemahaman bahwa terorisme tidak dapat dicegah 100% diperlukan, karena pemahaman tersebut akan memperkuat kemampuan kebijakan jika ada pemahaman yang melekat bahwa sesuatu dapat menjadi salah. Misalnya, katakanlah ada serangan keamanan siber yang mungkin dapat dicegah tetapi tidak dapat

dicegah. Pada titik tersebut, banyak pembuat undang-undang mungkin berpendapat bahwa tidak ada gunanya menginvestasikan ratusan ribu dolar dalam kebijakan keamanan siber antiterorisme, karena kebijakan tersebut tidak berfungsi, tidak efektif, dan karenanya, hanya membuang-buang uang.

Namun, itu tidak akurat. Dengan demikian, penerimaan bahwa terorisme, baik konvensional maupun siber, tidak dapat dicegah 100% memungkinkan adanya kelemahan atau kesalahan dalam kebijakan dan kemampuannya untuk bergerak maju.

Antiterorisme harus memiliki perspektif jangka pendek dan jangka panjang. Jika strategi kontraterorisme hanya menargetkan ancaman jangka pendek, kemungkinan besar strategi tersebut akan mengabaikan ancaman nyata (jangka panjang) lainnya. Penting untuk dicatat bahwa organisasi teroris mendefinisikan efektivitas melalui prisma pertimbangan strategis jangka panjang. Untuk memahami pola pikir teroris, penting untuk menghargai tekad, ketahanan, dan keteguhan hati yang dimiliki teroris. Teroris bersedia terlibat dalam perang yang melelahkan dengan kesulitan pribadi yang sangat besar bagi individu dan keluarganya untuk mencapai tujuan tertentu.

Pemahaman ini penting. Dalam mendukung definisi efektivitas, cabang kedua menekankan perspektif jangka pendek dan jangka panjang. Tidak hanya itu, cabang kedua berjalan beriringan dengan cabang pertama, dalam mengakui bahwa terorisme tidak dapat dicegah 100%. Untuk lebih memahami cabang kedua definisi efektivitas ini, penting untuk meninjau definisi terorisme, seperti yang tercantum dalam bab-bab sebelumnya.

Sebelumnya penulis mendefinisikan terorisme sebagai tindakan, oleh individu atau kelompok, yang dimaksudkan untuk membunuh orang yang tidak bersalah, terutama sebagai cara untuk menanamkan rasa takut pada orang lain, dengan tujuan memajukan salah satu dari empat tujuan—politik, agama, sosial, dan budaya—sehubungan dengan kebijakan pemerintah. Dengan demikian, terorisme tidak memiliki tanggal akhir yang spesifik; sebaliknya, mereka yang bersumpah untuk tujuan tersebut akan terus melakukannya saat mereka memajukan salah satu dari empat tujuan tersebut, dan akan terus melakukannya hingga mereka merasa telah berhasil.

Jadi, jika kebijakan keamanan siber berupaya untuk menjadi efektif, dan hanya memiliki mentalitas jangka pendek, kebijakan itu bahkan tidak akan menyentuh permukaan dari berbagai tindakan kontraterorisme yang perlu disertakan. Namun, jika kebijakan keamanan siber hanya berfokus pada tujuan jangka panjang, kebijakan itu kemungkinan akan kehilangan titik-titik kritis penetrasi yang ada dalam pola pikir jangka pendek. Jadi, agar kebijakan keamanan siber benar-benar efektif, kebijakan itu harus memiliki perspektif jangka pendek sekaligus jangka panjang.

Pertimbangkan contoh berikut: Sebuah organisasi teroris yang dikenal, yang ditetapkan oleh pemerintah sebagai organisasi teroris, telah menguasai menara pengawas lalu lintas udara di Detroit dan sekarang mengarahkan pesawat, memberi tahu mereka di mana harus mendarat, pada ketinggian berapa harus terbang, dan kapan harus lepas landas. Selain itu, dengan teknologi suara yang disempurnakan, pesawat yang dikomunikasikan tidak menyadari bahwa menara pengawas lalu lintas udara telah disusupi dan mengikuti semua arahan yang

diberikan kepada mereka. Kini, untuk kebijakan keamanan siber antiterorisme jangka pendek, kebijakan tersebut hanya akan berfokus pada cara mendapatkan kembali kendali atau akses ke menara pengawas lalu lintas udara.

Situasinya mendesak dan memerlukan respons segera untuk meminimalkan ancaman terhadap nyawa. Akan tetapi, penting juga untuk menyadari bahwa kebijakan keamanan siber antiterorisme yang berfokus pada jangka pendek juga harus berfokus pada jangka panjang. Jika kebijakan hanya berfokus pada jangka pendek dan hanya menyelesaikan masalah ini, insiden tersebut kemungkinan akan terjadi lagi.

Jadi, sangat penting bagi kebijakan untuk memahami motivasi organisasi teroris, dan dengan demikian, menerapkan tujuan keamanan siber antiterorisme jangka panjang dan jangka pendek agar benar-benar efektif.

Penanggulangan terorisme harus dilakukan dengan menyeimbangkan kepentingan yang saling bersaing, yaitu nyawa manusia, biaya finansial, dan kebebasan sipil.

Menemukan keseimbangan antara keamanan nasional dan hak-hak individu merupakan isu paling penting yang dihadapi oleh negara-negara demokrasi liberal yang sedang mengembangkan strategi antiterorisme. Tanpa keseimbangan antara kedua ketegangan ini, masyarakat demokratis kehilangan etos yang mereka perjuangkan.

Seperti yang pernah dikatakan Benjamin Franklin, "mereka yang akan menyerahkan kebebasan hakiki, untuk membeli sedikit keamanan sementara, tidak pantas mendapatkan kebebasan maupun keamanan." Memang, sangat penting bagi demokrasi untuk menghindari pelanggaran terhadap kebebasan politik dan kebebasan sipil. Namun, tanggung jawab utama pemerintah adalah melindungi warga negaranya. Perjuangan untuk menyeimbangkan kepentingan yang saling bersaing ini mungkin merupakan dilema paling mendasar yang dihadapi oleh demokrasi saat ini.

Antiterorisme, baik secara strategis maupun taktis, harus didasarkan pada kenyataan ini. Terlibat dalam siklus kekerasan yang tidak pernah berakhir adalah salah satu cara organisasi teroris memberi sinyal kepada berbagai khalayak (masyarakat umum, pengikut, dan pemerintah terkait) tentang komitmen mereka terhadap tujuan tersebut. Dari perspektif geopolitik teroris, tekanan yang diberikan oleh masyarakat yang diserang dan terpengaruh pada pemerintah terkait membenarkan serangan berkelanjutan terhadap warga sipil yang tidak bersalah. Langkah pertama dalam menciptakan tindakan kontraterorisme yang efektif adalah menganalisis ancaman. Untuk tujuan itu, pertanyaan yang diajukan pada Gambar 5.2 harus dijawab.

- *Ancaman apa yang dihadapi negara?*
- *Siapa yang bertanggung jawab untuk merencanakan ancaman?*
- *Siapa yang bertanggung jawab untuk membiayai ancaman?*
- *Siapa yang bertanggung jawab untuk melaksanakan ancaman?*
- *Kapan ancaman kemungkinan akan dilaksanakan?*

Gambar 5.2 Pertanyaan kontraterorisme.

Setelah pertanyaan-pertanyaan ini dijawab, ancaman dapat ditempatkan pada kontinum yang akan segera terjadi dengan pemahaman bahwa satu ancaman besar mungkin terdiri dari ancaman yang lebih kecil dan lebih mudah dikelola. Kontinum yang akan segera terjadi memiliki empat tolok ukur utama:

Ancaman yang akan segera terjadi adalah ancaman yang akan segera dilakukan; misalnya, laporan intelijen terkini menunjukkan bahwa sebuah bom akan diledakkan besok pukul 9:11 pagi di terminal domestik di bandara JFK.

Ancaman yang dapat diperkirakan adalah ancaman yang akan dilakukan dalam waktu dekat (tanpa kekhususan); Oleh karena itu, ancaman tersebut lebih jauh daripada ancaman yang akan segera terjadi, misalnya, ancaman yang dapat diperkirakan akan didasarkan pada intelijen yang valid yang menunjukkan teroris akan segera mulai membawa bahan peledak ke pesawat dalam bentuk zat cair.

Ancaman jarak jauh adalah ancaman yang dapat mencapai hasil pada waktu yang tidak diketahui; misalnya, pelatihan teroris tanpa tindakan operasional yang direncanakan secara khusus akan masuk dalam kategori ini.

Ancaman yang tidak pasti merupakan ancaman yang menimbulkan ketakutan umum akan ketidakamanan. Sebagai akibat dari pengeboman kereta api di Inggris dan Spanyol, para pelancong di Indonesia mungkin secara potensial atau mungkin merasa tidak aman saat naik kereta api tanpa keamanan yang diperkuat. Hal ini akan berlaku terlepas dari apakah ada intelijen yang valid yang menunjukkan teroris bermaksud untuk menargetkan kereta api.

Agar tindakan antiterorisme keamanan siber efektif, harus diakui bahwa pencegahan 100% tidaklah praktis, dan harus mempertimbangkan jangka panjang dan jangka pendek. Namun, cabang ketiga dan yang mungkin paling penting dari efektivitas kebijakan keamanan siber menekankan keseimbangan antara keamanan nasional dan hak-hak individu. Seperti disebutkan di atas, dalam menerima dan memahami ancaman keamanan siber, hal pertama yang harus dilakukan adalah menjawab pertanyaan berikut. Mari kita bahas setiap pertanyaan dengan contoh yang relevan.

Pertimbangkan sejenak bahwa ini adalah Selasa pagi di bulan April; Gedung Putih telah menerima video daring dari organisasi intelijen terkenal yang mempromosikan bahaya bagi Indonesia. Pesan tersebut menggembar-gemborkan penutupan jaringan listrik negara bagian Texas dalam 24 jam, kecuali tuntutan tertentu dipenuhi. Langkah pertama, seperti disebutkan di atas, adalah membahas pertanyaan-pertanyaan yang relevan dalam mengukur ancaman.

Pertanyaan **pertama** menekankan ancaman yang sebenarnya dan mempertimbangkan apa ancaman yang dihadapi negara tersebut. Dalam hal ini, ancamannya adalah pemutusan jaringan listrik. Ini adalah ancaman yang signifikan. Ancaman ini tidak signifikan, bukan hanya karena besarnya ancaman (yang menyebabkan seluruh negara bagian Texas menjadi gelap), tetapi juga karena konsekuensi yang muncul akibat pemutusan seluruh jaringan listrik.

Tanpa listrik, sistem kereta bawah tanah tidak dapat berfungsi, kantor tidak dapat beroperasi, dan turunnya kegelapan sering kali mengakibatkan perilaku yang melanggar hukum dan kacau. Dengan demikian, ancaman tersebut nyata dan tampak mendesak.

Pertanyaan **kedua** dalam menganalisis ancaman membahas siapa yang bertanggung

jawab untuk merencanakan ancaman tersebut. Jika ancaman ini datang dari organisasi tanpa nama, bukan dari individu yang tinggal di kota kecil di suatu tempat yang jauh yang mungkin tidak memiliki kemampuan untuk melaksanakan ancaman tersebut, analisis tersebut akan dinilai lebih rendah. Namun, jika ancaman ini datang, seperti yang terjadi, dari organisasi teroris yang ditunjuk dengan kemampuan yang terbukti di masa lalu, ancaman tersebut akan diberi bobot yang lebih besar.

Pertanyaan **ketiga** melibatkan keuangan dan mempertimbangkan siapa yang bertanggung jawab untuk membiayai ancaman tersebut. Ini memajukan analisis di atas, karena pembiayaan dari satu individu cenderung kurang efektif dibandingkan dengan pembiayaan dari organisasi teroris yang ditunjuk. Pertanyaan keempat, siapa yang bertanggung jawab untuk melaksanakan ancaman tersebut, juga memajukan analisis di atas. Kemampuan individu yang sendirian sangat terbatas dibandingkan dengan organisasi teroris yang ditunjuk, dalam hal tenaga kerja, tenaga kerja, dan keuangan. Dengan demikian, ancaman yang datang dari organisasi teroris yang ditunjuk untuk mematikan seluruh jaringan listrik Texas akan sangat bergantung pada efektivitasnya.

Pertanyaan **terakhir** membahas, khususnya, kapan ancaman tersebut akan dilakukan. Ancaman ini diterima pada pagi hari, dengan janji bahwa ancaman tersebut akan dilakukan dalam 24 jam ke depan. Oleh karena itu, kemungkinan besar akan segera terjadi. Secara keseluruhan, analisis efektivitas ancaman tersebut cukup mudah, sehingga sangat dibutuhkan model kontraterorisme keamanan siber yang efektif untuk memerangi ancaman yang ada. Jadi, setelah pertanyaan-pertanyaan tersebut terjawab, komponen terakhir adalah menempatkan ancaman pada kontinum yang akan segera terjadi.

Seperti yang dinyatakan di atas, kontinum yang akan segera terjadi memiliki empat tolok ukur utama: segera terjadi, dapat diperkirakan, jangka panjang, dan tidak pasti. Saat kita membahas pertanyaan-pertanyaan di atas, jelas bahwa ancaman khusus ini akan segera terjadi. Latihan di atas menunjukkan penerapan pertanyaan-pertanyaan yang diperlukan untuk mengevaluasi ancaman, dan memahami perlunya kebijakan antiterorisme keamanan siber yang sudah ada sebelum ancaman tersebut terjadi.

5.4 KERJASAMA INTERNASIONAL

Pembuat kebijakan harus menentukan apakah kebijakan keamanan siber akan berpusat di Jakarta atau akan mencerminkan kerja sama yang signifikan, berkelanjutan, dan dilembagakan dengan sekutu yang berpikiran sama. Jawaban atas pertanyaan ini bergantung pada penilaian sejauh mana keamanan siber menimbulkan ancaman terhadap keamanan nasional dan ketertiban umum. Dampak yang mungkin terjadi pada keduanya mengharuskan (dalam paradigma Amerika) baik pejabat keamanan nasional maupun penegak hukum memiliki tempat di meja respons siber. Secara kebetulan, adanya diskusi siber dengan keamanan nasional menunjukkan efektivitas serangan siber.

Dikatakan bahwa perlu ada peringatan. Sebelum mengalokasikan sumber daya yang signifikan dan menentukan alokasi aset, perlu ditentukan apakah serangan siber menimbulkan ancaman jangka panjang dan berkelanjutan yang didefinisikan sebagai serius dan mengerikan.

Atau, mungkinkah keamanan siber merupakan mode sesaat yang perlu dilihat dari perspektif sementara, dan bahwa ancaman tersebut telah dibesar-besarkan oleh pihak-pihak yang berkepentingan dengan kepentingan finansial dalam membesar-besarkan ancaman tersebut?

Peringatan ini tidak dimaksudkan begitu saja. Konsekuensi dari penentuan ancaman bersifat strategis, bukan sekadar taktis, dan memiliki konsekuensi yang signifikan, termasuk implikasi ekonomi, perjanjian internasional, yang memengaruhi alokasi sumber daya (sering kali mengakibatkan salah alokasi sumber daya), dan meningkatkan kerentanan yang ditimbulkan oleh ancaman fisik.

Menjalin kerja sama internasional

Langkah pertama menuju kerja sama internasional yang efektif dalam keamanan siber adalah menjalin kemitraan internasional yang langgeng dengan berbagai negara dan organisasi multinegara seperti Uni Eropa. Indonesia harus berusaha untuk melanjutkan hubungan perdagangan yang positif dengan berbagai negara, karena perdagangan sangat penting bagi keamanan. Untuk mempromosikan kemitraan yang benar dan efektif, Indonesia harus menjaga komunikasi terbuka dengan penghubung antara negara dan organisasi mitra.

Negara-negara mitra dan organisasi-organisasi harus berkomunikasi melalui penghubung dari badan-badan, departemen-departemen, dan organisasi-organisasi mitra (seperti Palang Merah) dari setiap negara atau organisasi multinegara untuk memastikan komunikasi aktif mengenai penilaian keamanan dan ancaman dan untuk mendorong penggunaan kerja sama internasional yang efektif dalam kontraterorisme.

Pertimbangkan contoh sebelumnya: Katakanlah seorang penyerang siber menguasai menara pengawas lalu lintas udara, tetapi bukan Detroit, di Bandara Heathrow London. Secara khusus, menara pengawas lalu lintas udara yang dimanipulasi tersebut hanya mengarahkan penerbangan internasional, yang terbang ke berbagai negara di Asia, Eropa, Amerika Serikat, dan Afrika. Dengan demikian, efektivitas kebijakan keamanan siber akan sangat terbatas, jika bukan karena kerja sama internasional.

Jika tidak ada kerja sama internasional, respons yang mungkin terjadi adalah setiap negara berusaha menerapkan kebijakan pribadi mereka sendiri, tanpa berkonsultasi dengan negara lain dan pada saat yang sama mengganggu negara lain. Hal ini sangat membatasi efektivitas kebijakan keamanan siber.

Sekarang, bayangkan skenario yang sama, namun contoh serupa telah dibahas sebelumnya, dan ada kesepakatan bersama di antara mayoritas negara tentang praktik terbaik untuk menanggapi serangan siber dan tugas serta kewajiban yang ditetapkan untuk setiap negara yang terlibat. Skenario mana yang akan lebih efektif? Saya yakin itu jawaban yang mudah.

Berbagi informasi intelijen

Sangat penting untuk mendorong berbagi informasi intelijen yang diperlukan secara aktif dan efektif kepada individu yang perlu tahu—kepada individu yang ditetapkan sebagai penghubung intelijen dalam rencana keamanan internasional yang lebih terkoordinasi (diuraikan di bawah). Khususnya, harus ada kerja sama internasional dalam berbagi informasi yang penting untuk keamanan perjalanan, seperti daftar pantauan yang menguraikan

beberapa ancaman yang diketahui terhadap keamanan dalam negeri.

Sejauh mungkin, negara-negara harus berbagi informasi intelijen tentang kemungkinan ancaman atau informasi intelijen tentang ancaman yang tidak diketahui oleh beberapa negara tetapi diketahui oleh negara lain, untuk mendorong kerja sama internasional dalam penilaian ancaman. Harus ada juga berbagi informasi intelijen untuk memastikan keamanan perbatasan yang efektif agar penegakan internasional terhadap perbatasan yang aman dapat dilakukan.

Selain itu, negara lain dapat mengintegrasikan produk intelijen dengan produk mereka sendiri dalam upaya mengidentifikasi, mengganggu, dan mencegah serangan dan aktivitas teroris di wilayah mereka sendiri. Menemukan cara untuk berbagi informasi intelijen dengan negara lain akan menciptakan peluang untuk menerima dan mengintegrasikan produk intelijen dari negara lain.

Ini berlanjut dengan contoh sebelumnya. Bayangkan di Bandara Heathrow London, seorang penyerang siber telah menguasai menara pengawas lalu lintas udara. Banyak penerbangan internasional kini terancam, dan warga dari lebih dari 50 negara langsung berada dalam bahaya. Jadi, tampaknya lebih dari 50 negara ingin terlibat dalam penyelesaian skenario secara damai. Bayangkan lebih jauh, tidak hanya Indonesia yang menggunakan semua kemampuan intelijen yang mereka miliki, tetapi juga masing-masing negara yang terlibat turut menyumbangkan kemampuan mereka.

Gambaran ini menyentuh. Sekarang, alih-alih satu negara mencoba menggunakan kemampuan sibernya untuk melawan penyerang siber, kekuatan lebih dari 50 negara disatukan untuk melawan penyerang siber perorangan. Tampaknya ini bukan hal yang sulit.

Sekarang, mari kita pertimbangkan contoh lain. Stasiun kereta bawah tanah, Tube, di London baru-baru ini dibobol. Penyerang siber memperoleh akses dan berhasil mengendalikan beberapa kereta—yang memengaruhi kemampuan mereka untuk menyalakan, menghentikan, dan membuka atau menutup pintu. Karena situasi ini baru saja terjadi di London, pemerintah Inggris tidak tahu harus berbuat apa untuk mengatasi situasi ini.

Sebaliknya, bayangkan saja kejadian yang sama persis terjadi di Washington awal tahun ini. Sayangnya, penyerang dunia maya berhasil mengakses sistem Metro Washington dan mampu memanipulasi kereta, sama seperti yang dilakukan di London. Jadi, pertanyaannya mudah saja, Washington harus berbagi pelajaran yang mereka peroleh dari situasi ini kepada mereka yang terdampak di London. Apalagi, Washington baru saja mengalaminya dan mungkin dapat meminimalkan kerusakan yang ditimbulkan terhadap Inggris.

Negara-negara tidak hanya harus berbagi informasi intelijen tentang potensi ancaman, atau daftar pantauan terkini, mereka juga harus berbagi informasi intelijen tentang ancaman di masa lalu, dan tanggapan yang gagal, serta tanggapan yang membantu mereka.

Rencana keamanan internasional yang terkoordinasi

Negara-negara mitra harus bekerja sama untuk mengembangkan rencana keamanan internasional yang terkoordinasi. Rencana ini harus menguraikan langkah-langkah untuk keamanan perjalanan yang terkoordinasi, keamanan perbatasan, dan untuk menentukan dan bertindak atas ancaman yang diketahui dan tidak diketahui.

Negara-negara mitra harus mengomunikasikan kemungkinan ancaman terhadap

keamanan perjalanan dan harus membuat rencana tindakan yang ditetapkan untuk skenario bencana, serangan teroris, dan ancaman teror. Rencana tersebut harus menguraikan peran setiap organisasi multinegara/negara dalam rencana keamanan yang lebih besar. Rencana tersebut harus mengartikulasikan koordinasi lembaga, departemen, dan organisasi khusus negara dan menguraikan bagaimana setiap entitas harus bertindak dalam menghadapi ancaman teror. Rencana yang terkoordinasi sangat penting untuk kerja sama internasional yang efektif dalam keamanan dalam negeri.

Latihan bersama

Keempat, negara-negara mitra harus bekerja sama untuk membuat dan menjalani prosedur pelatihan dan simulasi internasional. Perwakilan dari negara-negara mitra harus mengambil langkah-langkah untuk menjalani pelatihan bencana, skenario serangan teror, dan simulasi khusus untuk memastikan bahwa setiap anggota mengikuti rencana keamanan yang diartikulasikan. Lebih jauh, pelatihan harus memastikan bahwa setiap negara mitra mengikuti rencana di negaranya, dan juga bahwa rencana terkoordinasi diikuti di antara semua negara anggota.

Kelangsungan yang dilembagakan

Indonesia dan mitra internasionalnya harus memastikan kelangsungan yang dilembagakan baik antara para pemimpin negara dan lembaga utama serta penghubung departemen masing-masing negara.

Kelangsungan yang dilembagakan pada tingkat internasional mengacu pada gagasan bahwa harus ada proses yang ditetapkan untuk melanjutkan, untuk meneruskan, rencana keamanan yang diartikulasikan dari satu pemimpin negara ke pemimpin negara berikutnya. Setiap pemimpin, penghubung, perwakilan, harus memastikan bahwa mereka memahami rencana keamanan terkoordinasi dan harus terus meningkatkan teknologi, intelijen, dan pelatihan agar tidak hanya mengembangkan tetapi juga mempertahankan tingkat keamanan internasional yang tinggi.

Hal ini memerlukan dialog antara negara-negara mitra untuk menanyakan, apakah strategi keamanan berhasil? Hal ini memerlukan penciptaan dan kelangsungan parameter untuk mengukur efektivitas internasional. Apa tujuan akhirnya, apa harapan mengenai pelatihan keamanan dan kemampuan finansial? Pada akhirnya, harus ada rencana yang diartikulasikan dan dilembagakan untuk memastikan kesinambungan keamanan antara para pemimpin negara, dan semua mitra lembaga/departemen dalam rangka untuk mempromosikan kerja sama internasional yang efektif dan memastikan strategi keamanan dalam negeri yang efektif.

Potongan ini menekankan tujuan yang diartikulasikan dalam contoh-contoh sebelumnya. Kesinambungan yang dilembagakan diperlukan dalam dunia maya, sama seperti halnya diperlukan dalam aspek-aspek kehidupan lainnya. Bayangkan Anda sedang melakukan perjalanan darat. Saat Anda melintasi batas negara bagian—Anda langsung ditilang. Anda tidak melampaui batas kecepatan, Anda tetap berada di jalur Anda, dan semua lampu depan dan lampu rem Anda berfungsi dengan baik. Petugas mendekati mobil dan bertanya, "Apakah Anda tahu mengapa Anda ditilang?" Dengan tercengang, Anda menjawab, "Tidak."

Tanggapan petugas itu sederhana, di negara bagian ini, hukum dibalik dan mobil melaju di sisi kiri jalan, bukan kanan; oleh karena itu, dengan mengemudi di sisi kanan jalan, Anda menciptakan bahaya yang luar biasa terhadap pengendara lain dan harus diberi surat tilang. Ini tampaknya tidak masuk akal, bukan? Bagaimana mungkin dari satu negara bagian ke negara bagian lainnya, mobil melaju di sisi jalan yang berbeda? Bagaimana Anda bisa mengingat sisi mana yang mana? Perbedaan ini penting karena mengemudi di sisi jalan yang salah kemungkinan besar akan mengakibatkan kecelakaan serius.

Hal ini menunjukkan perlunya kesinambungan yang dilembagakan. Sama seperti kesinambungan yang diperlukan dalam aturan lalu lintas, kesinambungan juga diperlukan dalam ranah dunia maya. Dan kesinambungan ini harus terus berlanjut di seluruh Indonesia dan negara-negara lain. Tanpa hal ini, negara-negara akan terus tertinggal dalam kebijakan keamanan dunia maya antiterorisme mereka.

5.5 PRIVASI

Kita semua berkomunikasi dengan teman, kolega, dan keluarga, di luar negeri. Kita melakukannya melalui Internet, telepon seluler, dan telepon rumah. Kita terlibat dalam interaksi terus-menerus dengan orang lain. Kita melakukannya dengan pemahaman bahwa privasi semakin menjadi konsep yang kuno. Seperti yang telah berulang kali dilaporkan, Badan Keamanan Nasional jelas memantau percakapan telepon untuk mencegah tindakan terorisme.

Pertanyaannya adalah apakah percakapan dipantau semata-mata dan secara eksklusif untuk tujuan keamanan nasional yang sah. Kekhawatirannya adalah bahwa upaya yang sah—dan dapat dipahami—dilakukan dengan giat sehingga menghasilkan jaring pengaman, sehingga percakapan yang tidak terkait secara luas dipantau secara teratur. Dalam berbicara dengan para ahli materi pelajaran, jelas bahwa jutaan percakapan telepon didengarkan dan dipantau.

Perlindungannya, saya telah diyakinkan, adalah bahwa pemantau komunitas intelijen dilatih untuk berhenti mendengarkan setelah jelas bahwa percakapan tersebut tidak terkait dengan keamanan nasional. Berbagai pejabat senior telah memberi tahu saya hal ini pada sejumlah kesempatan. Saya yakin maksudnya adalah untuk meyakinkan bahwa percakapan yang tidak terkait dengan keamanan nasional tidak dipantau dan privasi—dalam konteks pengawasan—dilindungi.

Selain upaya tersebut, saya merasa percakapan tersebut mengganggu karena dua alasan, yang ditunjukkan pada Gambar 5.3. Harus diakui, di era teknologi pengawasan yang sangat canggih, harapan privasi yang wajar telah diminimalkan secara signifikan (Gambar 5.4).

Siber, dan keamanan siber, lebih dari apa pun, menonjolkan, memperburuk, dan menyoroti ketegangan yang kuat antara hak atas privasi dan kewajiban untuk melindungi keamanan nasional. Sementara kita, mungkin, secara wajar mengharapkan perlindungan privasi dalam empat dinding rumah kita, harapan itu diminimalkan secara signifikan ketika terlibat dalam ranah publik. Yang secara signifikan mempersulit paradigma saat ini adalah perubahan yang jelas antara publik dan privat karena media sosial. Pentingnya dan relevansi hal ini terhadap keamanan siber tidak boleh diremehkan. Realitasnya diringkas dengan rapi

sebagai berikut: Saat seseorang terlibat dalam diskusi elektronik, interaksi itu berada di ranah publik.

- *Ketika diberitahu bahwa pemantauan untuk tujuan keamanan nasional itu luas, telinga dan antena saya yang skeptis menjadi "siaga penuh"; Saya sangat khawatir bahwa keamanan nasional didefinisikan secara luas, yang secara langsung menunjukkan bahwa kebijakan keamanan siber didefinisikan secara luas.*
- *Mendefinisikan keamanan siber secara luas membuka pintu bagi pengawasan berskala luas yang mengakibatkan penyebaran jaring yang luas, sehingga secara jelas memengaruhi hak privasi individu.*

Gambar 5.3 Alasan.

Standar privasi

- *Katz versus Amerika Serikat: Amandemen keempat melindungi ekspektasi privasi yang wajar yang siap diakui oleh masyarakat, karena perlindungan yang wajar secara objektif berlaku untuk orang, bukan tempat*
- *Dalam penerapannya, pengadilan menekankan ekspektasi privasi yang wajar*
- *Deklarasi universal hak asasi manusia: Tidak seorang pun boleh dikenai campur tangan sewenang-wenang terhadap privasi, keluarga, rumah, atau korespondensi…*
- *Kovenan internasional tentang hak-hak sipil dan politik: Tidak seorang pun boleh dikenai campur tangan sewenang-wenang atau melanggar hukum terhadap privasi, keluarga, rumah, atau korespondensi…*

Gambar 5.4 Standar privasi.

Pengguna Facebook yang aktif memberi tahu saya bahwa halaman pribadi atau halaman publik tersedia. Namun, bahkan jika pengguna memilih halaman pribadi, rata-rata pengguna Facebook memiliki 600 teman. Jadi, jika pengguna memiliki 600 teman, menganggap bahwa semua teman pribadi akan merahasiakan informasi adalah ilusi, paling banter. Dalam konteks dunia maya, delta yang kritis adalah perubahan pribadi-publik, dan sejauh mana informasi benar-benar tidak dilindungi. Dalam mengembangkan kebijakan dunia maya, sejauh mana privasi telah diminimalkan merupakan bagian penting dari teka-teki yang sangat rumit.

Diskusi ini, toleransi yang dimiliki individu untuk mengabaikan privasi dalam hal keamanan nasional, telah dibahas sebelumnya dalam perdebatan antara Apple dan FBI mengenai ponsel penembak San Bernardino. Apakah individu bersedia memberikan akses pintu belakang kepada pemerintah atas nama perlindungan? Apakah individu yang terbuka di media sosial mereka lebih bersedia memberikan akses kepada pemerintah, atau apakah mereka merasa privasi, meskipun mereka terbuka di media sosial? Kesulitannya terletak pada tujuan akhir. Selain itu, apakah tujuan akhir itu altruistik, dapatkah itu diputarbalikkan jika

jatuh ke tangan individu yang tidak altruistik?

Ini adalah argumen yang digunakan untuk menentang gagasan Apple menciptakan pintu belakang. Jika Apple menciptakan sistem operasi seperti itu, kemungkinan itu bisa jatuh ke tangan individu dengan tujuan jahat ada, dan itu adalah ancaman yang tidak dapat diterima oleh banyak orang di Dunia.

Inti dari perdebatan privasi-keamanan nasional adalah keseimbangan. Keseimbangan adalah persamaan yang tidak sempurna yang mencerminkan realitas ancaman yang terus bergerak dan upaya yang tidak pernah berakhir dari para penyerang dunia maya untuk meningkatkan jangkauan, cakupan, dan kemampuan mereka. Kegigihan para penyerang dunia maya—besar dan kecil, domestik dan internasional—menimbulkan pertanyaan penting mengenai efektivitas kebijakan anti-siber dan sejauh mana masyarakat bersedia menoleransi pelanggaran privasi. Persamaan keseimbangan terhambat oleh perasaan yang meresahkan bahwa para pembuat keputusan nasional terus-menerus terkejut, ketika para peretas berhasil menembus firewall yang dianggap aman.

Keamanan Dalam Negeri, subkomite Intelijen, Pembagian Informasi, dan Penilaian Risiko Terorisme. Penilaian penulis dapat diringkas seperti yang diberikan pada Gambar 5.5. Sehubungan dengan pengembangan kebijakan keamanan siber nasional, pertanyaan utamanya adalah seberapa besar pemaksaan atas nama keamanan nasional yang dapat ditoleransi oleh individu dan masyarakat? Pertanyaannya tidak mengenakkan: Pada intinya, hal itu menuntut penyelesaian sifat hubungan individu dengan negara. Kebijakan keamanan siber bergantung pada keberhasilan mengatasi pertanyaan ini yang, tidak diragukan lagi, meluas jauh melampaui Internet, keamanan nasional, dan privasi. Dari perspektif eksistensial dan praktis, menjawab pertanyaan tersebut menuntut penyelidikan dilema kontrak sosial: kepada siapa negara berutang kewajiban?

- *Kegagalan pemerintahan dan Kongres untuk mengembangkan, apalagi mengartikulasikan, kebijakan keamanan dalam negeri yang kohesif, koheren, dan berkelanjutan*
- *Kegagalan untuk memahami dan mengonseptualisasikan ancaman masa depan; pepatah lama mengenai jenderal yang berperang kemarin masih berlaku*
- *Keengganan untuk mendefinisikan istilah, sehingga membatasi kekuasaan negara dan meningkatkan hak individu*

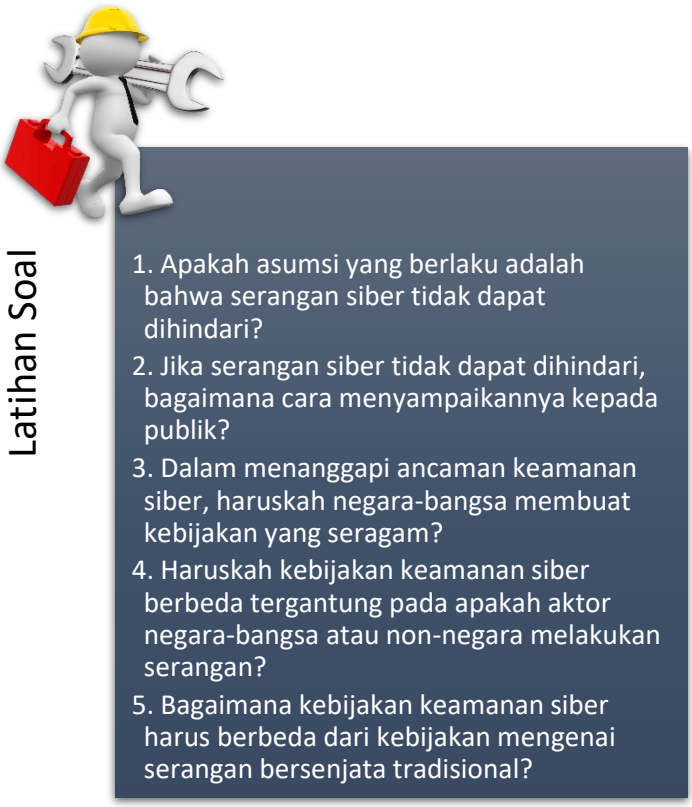
Gambar 5.5 Penilaian komite.

Namun dalam hal kebijakan, kita perlu bertanya pada diri sendiri apakah kita sebagai masyarakat, korporasi, dan pemerintah perlu lebih Proaktif dalam hal memberlakukan persyaratan untuk membuat dan menerapkan langkah-langkah perlindungan. Bagi saya, ini merupakan bagian tak terpisahkan dari pembahasan kebijakan yang menekankan persyaratan untuk memahami ancaman, mengenali ancaman, mengartikulasikan ancaman, dan akhirnya menerapkan langkah-langkah perlindungan terhadap ancaman tersebut. Langkah-langkah ini

dilakukan dengan peringatan bahwa langkah-langkah perlindungan tidak 100% efektif. Realitas ini—mungkin tidak mengenakkan—mengharuskan pemerintah untuk hadir di hadapan publik dan menjelaskan batasan inheren kebijakan keamanan siber (Gambar 5.6).

Pertanyaan-pertanyaan yang harus dipertimbangkan dalam meninjau Bab 5 diberikan dalam Gambar 5.7.

Gambar 5.6 Kebijakan keamanan siber.



Gambar 5.7 Pertanyaan ulasan.

BAB 6
TANGGAPAN KORPORASI KEJAHATAN DUNIA MAYA

6.1 PENDAHULUAN

Korporasi, besar dan kecil, rentan terhadap peretas dan jelas diserang, meskipun tidak setiap hari, tetapi sangat teratur. Beberapa serangan sangat besar, proporsinya memengaruhi puluhan juta pelanggan yang privasinya jelas dilanggar. Informasi pribadi mereka diretas; mereka rentan, terekspos, dan khawatir, jika tidak marah. Bagaimana korporasi menanggapi keamanan dunia maya sangat penting. Kepentingan yang luar biasa ini mencakup pertimbangan taktis dan strategis. Tidaklah berlebihan untuk menyatakan bahwa ancaman dunia maya adalah titik fokus utama korporasi saat ini. Jika tidak, maka itu mencerminkan salah tafsir serius terhadap bahaya yang jelas dan nyata. Bahaya itu—yang dapat diraba oleh pengamat yang paling biasa—tidak dapat disangkal.

Namun, kejelasan tidak sama dengan tindakan; mengartikulasikan pengakuan ancaman tidak selalu diterjemahkan menjadi tindakan konkret. Sayangnya, ada risiko dalam mengakui ancaman; pengakuan kerentanan dapat memiliki konsekuensi finansial yang signifikan. Meskipun dapat dimengerti, kekhawatiran yang dinyatakan dan tidak dinyatakan mengenai pengakuan kerentanan justru merugikan diri sendiri dan sangat kontraproduktif. Hal ini mirip dengan pendekatan menutup mata, yang mencerminkan ketidaktahuan yang disengaja yang memunculkan aturan monyet tidak melihat kejahatan, tidak mendengar kejahatan.

Pertimbangkan hal berikut: Apa yang dimaksud dengan serangan siber terhadap perusahaan? Selain itu, tingkat perlindungan seperti apa yang Anda, sebagai konsumen di perusahaan, harapkan dari perlindungan privasi Anda?

Banyak dari kita beroperasi dalam suatu pola—kita sering mengunjungi pom bensin, toko kelontong, dan bioskop yang sama. Asumsikan sejenak bahwa Anda adalah tipe orang yang sangat senang pergi ke bioskop, sehingga Anda menontonnya setidaknya seminggu sekali. Setiap kali menonton film, Anda menggesek kartu kredit untuk membayar tiket dan konsesi. Perlindungan seperti apa yang Anda harapkan dari bioskop dalam menyimpan informasi kartu kredit? Apakah perlindungan tersebut serupa dengan yang Anda harapkan dari toko kelontong? Apakah perlindungan tersebut serupa dengan yang Anda harapkan dari lembaga keuangan, seperti bank?

Sekarang, pertimbangkan sistem rumah sakit Anda. Bayangkan Anda harus sering pergi ke rumah sakit. Anda berjuang melawan penyakit kronis yang memaksa Anda untuk melakukan pemeriksaan bulanan. Bayangkan juga bahwa penyakit ini adalah penyakit yang tidak diketahui oleh kebanyakan orang, khususnya atasan Anda, dan penyakit yang ingin Anda rahasiakan. Sistem rekam medis rumah sakit ini memiliki catatan riwayat medis dan informasi pembayaran Anda. Perlindungan apa yang Anda harapkan dari sistem rumah sakit dalam menyimpan rekam medis? Apakah perlindungannya sama dengan perlindungan yang Anda harapkan dari sistem penyimpanan informasi kartu kredit Anda? Apakah perlindungan itu lebih

besar atau lebih kecil daripada perlindungan yang Anda harapkan di bioskop?

Terakhir, pertimbangkan jenis respons yang Anda harapkan dari sistem bioskop dan rumah sakit. Kemungkinan besar Anda akan mengharapkan respons dan pemulihan tambahan jika sistem rumah sakit diretas dibandingkan dengan sistem bioskop; mengingat di bioskop, Anda hanya kehilangan informasi kartu kredit.

6.2 REALITAS DAN MENGUNGKAPKAN ANCAMAN

Realitanya adalah bahwa korporasi diserang setiap hari dan secara mendalam, dengan dampak dan konsekuensi yang signifikan baik jangka pendek maupun jangka panjang. Namun, gambaran yang jelas—dan mengganggu—adalah para pemimpin korporasi yang mengungkapkan keterkejutan setelah serangan siber yang berhasil. Respons umum bahwa kami telah menginvestasikan sumber daya yang signifikan untuk melindungi klien dan aset kami, paling banter, mencerminkan manipulasi dan pengendalian kerusakan. Hal itu juga menunjukkan kegagalan untuk mengenali realitas. Citra keterkejutan secara tegas diperparah ketika menyadari bahwa serangan terhadap korporasi tampaknya merupakan serangan terhadap negara-bangsa.

Kegagalan itu, diasumsikan, tidak didasarkan pada ketidakmampuan para pemimpin korporasi untuk memahami keberadaan bahaya yang jelas. Namun, hal itu menunjukkan keengganan untuk menginternalisasi bahaya itu. Secara praktis, pemahaman tidak sama dengan menginternalisasi; yang pertama hanya memerlukan membaca koran, yang kedua menuntut tindakan konkret yang memerlukan pengeluaran finansial, alokasi sumber daya, dan pengakuan publik atas kerentanan. Bahkan dengan membaca sekilas di Internet, ketiga hal tersebut merupakan kutukan bagi para pemimpin perusahaan, terlepas dari lokasi dan ukurannya.

Pendekatan tersebut merugikan diri sendiri, picik, dan kontraproduktif. Pendekatan tersebut berdampak negatif terhadap pelanggan dan investor; membebani penegakan hukum; memengaruhi perusahaan lain dan masyarakat umum. Barangkali yang paling mengganggu—dan signifikan—pendekatan tersebut membuat para penyerang dunia maya semakin berani menerjemahkan kegagalan para pemimpin perusahaan untuk secara terbuka menangani dan mengakui realitas serangan dunia maya menjadi kelemahan, jika bukan ketidakmampuan.

Ketidakmampuan yang dipersepsikan adalah kegagalan untuk mencegah serangan; kelemahan yang diasumsikan adalah kegagalan untuk mengakui ancaman. Salah satu pelajaran utama yang dipelajari dari keterlibatan saya selama dua dekade dalam kontraterorisme operasional adalah kebutuhan—persyaratan adalah istilah yang tepat—bagi pemerintah untuk secara rasional dan konsisten mengartikulasikan ancaman terhadap masyarakat. Artikulasi tidak menunjukkan rasa takut; justru sebaliknya: Artikulasi menunjukkan kemauan untuk mengakui dan menyatakan kebenaran. Ini adalah kebijakan yang jauh lebih efektif dalam hal menginformasikan kepada masyarakat, pihak-pihak yang berkepentingan langsung, dan para penyerang yang sebenarnya dan potensial.

Pertimbangkan manfaat yang diperoleh dari artikulasi ancaman. Skenario berikut ini, sayangnya, merupakan situasi yang terjadi setiap hari di seluruh negeri dan dapat dicegah jika

artikulasi ancaman terjadi sebelumnya, dan tindakan diambil untuk menanggapi ancaman tersebut.

Pertama, bayangkan seseorang berjalan di gang belakang setelah meninggalkan shift malamnya di restoran lokal. Area khusus tempat restoran tersebut berada berada di area yang rawan serangan kekerasan, khususnya, banyak serangan semacam itu telah terjadi di gang tersebut. Sekarang, bayangkan dua orang lain mendekati orang tersebut—keduanya berbadan besar dan jauh lebih besar daripada orang yang meninggalkan pekerjaannya di gang belakang.

Jika mengamati ini dari sudut pandang atas, penonton hanya akan berasumsi bahwa orang yang sendirian itu akan datang dengan persiapan, dengan mekanisme untuk mencegah serangan seperti itu, baik semprotan merica atau tongkat. Tampaknya sulit untuk memahami mengapa seorang individu berjalan sendirian di gang belakang larut malam, khususnya di tempat yang pernah terjadi serangan sebelumnya, tanpa menyadari perlunya membawa alat pencegah. Penangkalan tersebut tidak menunjukkan tanda kelemahan dari individu tersebut. Sebaliknya, hal itu menunjukkan artikulasi ancaman yang memadai dan pengakuan akan perlunya menggagalkan serangan potensial.

Kedua, bayangkan seseorang masuk ke koneksi Wi-Fi publik, baik di bandara atau kafe pusat kota yang populer. Dengan pandangan menyeluruh seperti yang digunakan di atas, kita dapat melihat bahwa di sisi berlawanan dari Wi-Fi publik tersebut terdapat peretas yang menunggu individu untuk memasukkan informasi kartu kredit mereka. Dengan pandangan menyeluruh ini, kita semua sangat sadar untuk menghentikan individu tersebut memasukkan informasi kartu kredit mereka dan tidak membiarkan mereka menjadi mangsa peretas.

Jadi, dengan artikulasi ancaman peretas yang mengakses informasi kartu kredit, hal itu tidak membuat individu menjadi lebih lemah. Sebaliknya, hal itu menekankan perlunya artikulasi pada ancaman yang sebenarnya, dan yang dirasakan, dan menanggapinya secara proporsional.

Contoh *ketiga* dan *terakhir* melibatkan sistem rumah sakit. Pada zaman sekarang, beberapa sistem rumah sakit telah diretas, baik dengan mendistribusikan catatan atau menyandera sistem, hingga tebusan tertentu dibayarkan.

Ini adalah kejadian yang, sayangnya, telah terjadi beberapa kali. Jadi, dengan satu orang yang berjalan di gang atau seseorang yang menggunakan Wi-Fi publik, tampaknya sistem rumah sakit dapat belajar dari pengalaman orang-orang sebelumnya dan mengartikulasikan ancaman tersebut dan menanggapinya dengan tepat. Namun, artikulasi ini tidak terjadi di antara banyak perusahaan karena alasan apa pun dan harus ditangani.

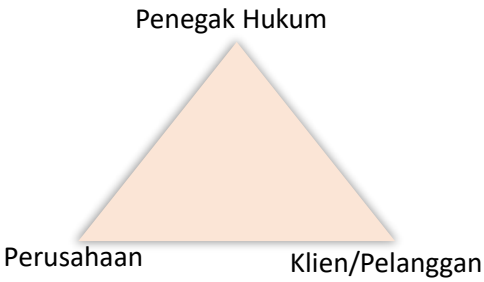
6.3 KEMITRAAN

Ini merupakan pendekatan yang matang, yang menandakan pengakuan terhadap ancaman, yang mencerminkan pelaksanaan langkah-langkah untuk meminimalkan ancaman, tanpa mengabaikan kemungkinan serangan, atau meremehkan kemungkinan konsekuensi dan ramifikasinya. Selain itu, ini menciptakan lingkungan di mana pelanggan menjadi mitra dalam konteks penanggulangan terorisme siber karena pelanggan diperlakukan sebagai orang dewasa yang matang.

Konsep pelanggan sebagai mitra dalam memerangi terorisme siber di mana hubungan segitiga tercipta antara perusahaan dan klien/pelanggan—penegakan hukum jauh lebih efektif daripada meminimalkan—jika tidak menyangkal—ancaman secara tidak perlu (Gambar 6.1).

Masyarakat adalah mitra penuh sehubungan dengan penanggulangan terorisme. Paket mencurigakan yang ditinggalkan tanpa pengawasan menyebabkan individu yang khawatir menelepon polisi; masuk ke pusat perbelanjaan dikondisikan dengan melewati detektor logam; dan perjalanan sekolah memerlukan pendampingan oleh orang dewasa yang bersenjata.

Itulah kenyataannya. Dalam konteks yang sama—dengan analogi—ancaman yang ditimbulkan oleh serangan siber mengharuskan perusahaan untuk membentuk kemitraan dengan pelanggan dan penegak hukum. Kemitraan itu, harus diakui, memberatkan; beban itu sekaligus eksistensial dan praktis. Akan tetapi, itu perlu. Itulah, lebih dari apa pun, tema utama bab ini: Ancaman serangan siber terhadap perusahaan tidak dapat disangkal; untuk meminimalkannya, ancaman itu memerlukan upaya bersama, langsung, dan berkelanjutan oleh mereka yang terkena dampak langsung dan tidak langsung.



Gambar 6.1 Hubungan segitiga dengan korporasi.

Penting untuk dicatat bahwa upaya itu difokuskan pada meminimalkan, bukan memberantas ancaman. Meminimalkan adalah dalam ranah yang mungkin; memberantas adalah ilusi dan menyimpan harapan itu berdampak negatif pada upaya realistis untuk meminimalkan.

Dalam menanggapi ancaman keamanan siber, mudah untuk meminimalkan tingkat keparahan ancaman jika seseorang tidak memiliki pengalaman pribadi dengan konsekuensi serangan siber. Pertimbangkan sejenak bahwa individu berikut ini tidak pernah menjadi korban pencurian identitas. Selain itu, individu ini bahkan tidak pernah mengalami peretasan kartu kredit. Individu ini tidak pernah menjadi korban pelanggaran perusahaan, yang mengakibatkan informasi pribadinya dipublikasikan di Internet. Secara keseluruhan, individu tersebut tidak memiliki pengalaman dengan keamanan siber.

Sekarang, pertimbangkan individu yang telah menjadi korban pencurian identitas, khususnya nomor jaminan sosialnya digunakan untuk membuka banyak akun, yang mengakibatkan individu tersebut tidak dapat mengambil pinjaman karena kreditnya yang buruk, semuanya disebabkan oleh penyerang siber. Tampaknya mudah untuk berasumsi bahwa individu yang telah mengalami tingkat keparahan serangan siber akan lebih cenderung

meminimalkan ancaman, karena bagi mereka itu adalah ancaman yang rasional dan nyata.

Mari kita pertimbangkan banyak hal yang kita lakukan saat ini yang merupakan akibat dari suatu serangan, ancaman potensial yang terwujud dengan cara yang tidak menguntungkan. Bagi siapa pun yang baru-baru ini naik pesawat, atau dalam sepuluh tahun terakhir, mereka sangat menyadari keamanan yang harus dilalui untuk mengakses gerbang mereka. Lewatlah sudah hari-hari menjemput orang-orang terkasih di gerbang—sebaliknya mereka harus menunggu di luar keamanan. Setiap orang harus melewati detektor logam, dan banyak yang kemudian diperiksa dengan alat penggeledahan. Upaya-upaya ini dilaksanakan setelah 9/11—dan menjadi bagian yang diharapkan dari perjalanan.

Mudah untuk berargumen bahwa penerapan keamanan kemungkinan besar tidak akan terjadi jika tidak ada serangan pada 11/9. Keamanan tambahan, serta pintu pilot yang terkunci, dipandang sebagai reaksi terhadap 11/9—dan banyak, jika tidak semua, individu memahami kebutuhannya. Sekarang, mari kita kembali ke perbandingan kedua individu tersebut.

Orang yang tidak memiliki pengalaman dengan serangan keamanan siber kemungkinan akan bereaksi sama seperti individu yang tidak hidup pada saat serangan 11/9. Secara konseptual akan sulit untuk mengartikulasikan dan menyadari ancaman asing seperti itu, terutama jika itu tidak pernah terjadi pada Anda. Namun, individu yang menjadi korban pencurian identitas sangat mirip dengan mayoritas dunia yang hidup selama serangan 11/9. Individu tersebut jelas memahami beratnya ancaman dan dengan sukarela mengartikulasikan ancaman tersebut dalam upaya untuk meminimalkannya.

Itu harus menjadi kemitraan agar efektif. Seperti terlihat pada Gambar 6.1, diperlukan kerja sama antara korporasi, klien/konsumen, dan penegak hukum untuk secara efektif menjalankan strategi keamanan siber yang sukses.

6.4 CONTOH CERITA

Beberapa tahun lalu, saya bekerja di sebuah perusahaan besar. Sebagai penghargaan bagi para pemimpin, sebuah latihan simulasi yang canggih telah dilakukan. Tujuan yang dinyatakan dari usaha tersebut adalah untuk menentukan titik-titik kerentanan perusahaan, dengan penekanan khusus pada tindakan terorisme yang terlokalisasi. Di permukaan, simulasi tersebut berhasil, sedemikian rupa sehingga pada akhir simulasi, kepala eksekutif (CEO) mengungkapkan kepuasannya yang besar dalam momen yang memuji diri sendiri. Dalam melakukannya, ia membuka pintu bagi kritik. Salah seorang karyawan mengangkat tangan dan berkata, "Kami melakukan simulasi dan itu hebat, tetapi kami lupa detail ini, dan kami lupa untuk mengatasi potensi kejadian ini." CEO tersebut berkata bahwa "tidak apa-apa, kami dapat mengatasinya." Namun kemudian, karyawan lain mengangkat tangannya dan berkata sebagai tindak lanjut, "Anda lupa untuk mengatasi detail lainnya."

Kedua poin yang disampaikan oleh karyawan yang berbeda tersebut membahas masalah-masalah kecil yang terkait dengan perlindungan dan respons perusahaan; masalah-masalah tersebut tidak besar atau dahsyat tetapi agak kecil. Meskipun demikian, CEO tersebut segera menyadari beberapa hal. Pertama, ia terlalu dini terlibat dalam perilaku memuji diri sendiri. Kedua, jika Anda benar-benar akan terlibat dalam latihan simulasi yang efektif, baik di

dunia maya maupun di luar dunia maya, hal terpenting adalah detailnya. Tidak ada yang dapat menggantikan perencanaan yang matang, harapan yang realistis, dan penilaian diri yang jujur.

CEO gagal dalam ketiga hal tersebut; khususnya, saya sangat terganggu oleh rasa percaya diri yang tidak beralasan mengenai tingkat kesiapan perusahaan untuk semua kemungkinan serangan. Hal yang dapat diambil—bagi saya (semoga juga bagi CEO)—adalah bahwa dalam menghadapi ancaman dunia maya, pimpinan perusahaan perlu lebih sadar diri mengenai tingkat ancaman dan tingkat kesiapan baik secara proaktif maupun reaktif. Hal ini khususnya terjadi mengingat sifat serangan dunia maya yang canggih dan keinginan yang jelas dari para peretas untuk secara konsisten terlibat dalam serangan yang semakin berani.

Dengan cerita di atas, pertanyaannya adalah, apa tanggung jawab CEO jika ia tidak menangani detail yang terlupakan dalam simulasi. Jika detail tersebut diketahui dan diabaikan, dan terjadi insiden yang menimbulkan kerugian siber yang signifikan, dapatkah CEO atau perusahaan bertanggung jawab, karena mereka menyadari masalah tersebut? Selain itu, haruskah ada tanggung jawab hukum bahwa ketika seorang direktur mengetahui suatu masalah, mereka memiliki kewajiban hukum untuk menangani masalah tersebut dalam jangka waktu tertentu?

Jika bukan kewajiban hukum yang dapat ditegakkan, apakah ada kewajiban moral? Apa pun itu, pertanyaan yang perlu dipertimbangkan adalah apakah kesadaran akan detail kecil yang dapat mengakibatkan serangan siber yang signifikan mengakibatkan peningkatan tanggung jawab bagi perusahaan. Jika tidak, haruskah demikian? Kekhawatiran yang muncul dengan meningkatnya tanggung jawab adalah perusahaan memilih untuk menutup mata untuk menghindari tanggung jawab daripada menyadari masalah.

Kisah kedua menekankan kenyataan yang mengganggu mengenai kemauan—atau lebih tepatnya keengganan—dari para pemimpin perusahaan untuk secara proaktif menangani masalah keamanan siber.

Pada sebuah konferensi di Amerika Serikat, seorang wakil presiden (VP) bidang keamanan untuk sebuah perusahaan besar di AS. Membahas ancaman yang ditimbulkan oleh dunia maya. Dengan cepat menjadi jelas bahwa kami berdua memiliki bahasa yang sama dan sama-sama menyadari kelemahan yang mencolok. Sebelum bergabung dengan perusahaan, VP tersebut pernah bertugas di bidang penegakan hukum; berdasarkan pengalaman dan latar belakang kami yang serupa, kami sepakat bahwa perusahaan akan sangat diuntungkan dengan melakukan latihan simulasi dunia maya yang canggih yang akan menunjukkan kepada para pemimpin senior titik-titik kelemahan dan kerentanan.

VP tersebut jujur; tanggapannya menyedihkan. Meskipun ia memahami dengan baik manfaat besar yang akan diperoleh dari usaha semacam itu, tidak ada keraguan dalam benaknya bahwa CEO perusahaan tersebut akan dengan tegas menentang latihan semacam itu. Ketika saya bertanya kepadanya mengapa CEO-nya menolak latihan tersebut, jawabannya ada dua. Saya pikir pria itu sangat jujur: pertama, latihan simulasi memakan banyak waktu dan tidak murah untuk dilakukan; kedua, jika Anda melakukan latihan simulasi dan kerentanannya terindikasi, bagaimana pemegang saham Anda akan menanggapinya?

Bagaimana pesaing Anda akan menanggapinya? Bagaimana peretas akan

menanggapinya? Intinya, dia memberi tahu saya bahwa CEO lebih suka menutup mata. Saya menemukan bahwa itu menjadi tema yang berulang ketika berbicara dengan pejabat senior di perusahaan dalam konteks dunia maya. Ini mencerminkan dan mengartikulasikan, secara aktif dan pasif, penolakan untuk benar-benar mengakui ancaman yang ditimbulkan oleh dunia maya.

Dalam mempertimbangkan tanggapan VP, penekanan pada keraguannya untuk bertindak adalah pada biaya untuk membuat simulasi tersebut dan tanggapan pemegang saham. Apakah ada cara potensial untuk meminimalkan atau mengurangi salah satu dari kekhawatiran tersebut. Jika cara tersebut ada, siapa yang berkewajiban untuk menyediakan mekanisme tersebut? Selain itu, siapa yang akan membayar agar mekanisme tersebut efektif? Jika setiap kekhawatiran VP diredakan, apakah kurangnya tanggapannya akan mengakibatkan beberapa bentuk tanggung jawab? Mari kita uraikan setiap masalah dan tentukan berbagai cara untuk meminimalkan biaya ekonomi dan sosial bagi VP dan perusahaannya.

Kekhawatiran pertama yang ditekankan VP adalah biaya ekonomi—khususnya bahwa latihan simulasi memakan banyak waktu dan tidak murah untuk dilakukan. Jadi, apa saja cara untuk meminimalkan biaya tersebut? Saat ini, untuk menjadi perusahaan di Amerika, individu diharuskan terlebih dahulu mengajukan sertifikat pendirian, yang merinci dewan direksi, alamat umum, dan informasi penting lainnya.

Informasi ini diajukan ke sekretaris negara. Sekarang, pertimbangkan, bagaimana jika pelatihan kemudian diperlukan bagi dewan direksi yang baru untuk terlibat dalam latihan simulasi untuk menanggapi serangan siber. Itu akan meminimalkan biaya bagi perusahaan, karena akan dibayar oleh kantor sekretaris negara dan akan meminimalkan waktu yang dihabiskan di kemudian hari untuk menanggapi serangan potensial yang sebenarnya.

Namun, kesulitan utama dalam opsi ini adalah simulasi hanya akan berlaku untuk dewan direksi yang baru. Dan, seperti yang kita ketahui, sering kali direktur di dewan direksi bersifat fleksibel, selalu berubah, dan tidak konsisten dalam jangka waktu yang lama.

Menanggapi kekhawatiran kedua, VP menekankan biaya sosial yang lebih besar—kekhawatiran akan respons pemegang saham. Menunjukkan kelemahan perusahaan dalam hal keamanan siber bukanlah sesuatu yang CEO atau dewan direksi ingin pemegang sahamnya sadari, khususnya karena hal itu hanya menunjukkan kepada pemegang saham kelemahan terbesar perusahaan.

Namun, ada dua cara potensial untuk meredakan kekhawatiran ini yang berdampak negatif pada pemegang saham. Cara pertama adalah menjadikan simulasi tersebut wajib, sesuai dengan aturan pendirian. Artinya, agar perusahaan dapat mempertahankan status korporasinya, mereka harus mematuhi simulasi wajib setiap beberapa tahun. Ini akan menyamakan kedudukan dan memaksa semua perusahaan untuk terlibat dalam menunjukkan kelemahan mereka, yang diharapkan akan meredakan kekhawatiran pemegang saham dari satu perusahaan tertentu, karena mereka dapat melihat kelemahan serupa di organisasi sekitarnya.

Cara kedua untuk meminimalkan biaya sosial adalah dengan membiarkan informasi tersebut tetap rahasia. Secara logistik, ini mungkin lebih sulit, mengingat tidak banyak yang

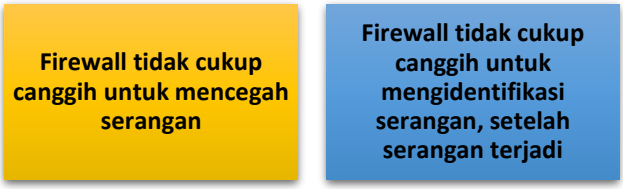
bisa dirahasiakan di dunia yang semakin mengglobal ini, tetapi ini adalah pilihan yang tidak akan mengejutkan para pemegang saham sebanyak mempublikasikan informasi tersebut. Pada akhirnya, dengan kedua pilihan tersebut, biaya dampak negatif terhadap pemegang saham dapat diminimalkan, sedangkan kesadaran akan perlunya perlindungan keamanan siber meningkat.

6.5 KERENTANAN

Dalam konteks ancaman yang ditimbulkan oleh dunia maya, terdapat berbagai model kerentanan yang dapat diterapkan oleh perusahaan. Saya mengusulkan untuk menganalisis hubungan antara perusahaan dan dunia maya melalui model kerentanan 12 poin yang memeriksa kerentanan dari awal hingga akhir produksi.

Ketika berfokus pada kerentanan produk terhadap potensi serangan dunia maya, pimpinan perusahaan harus terlibat dalam penilaian diri yang ketat. Penerapan model 12 poin dari awal hingga akhir secara signifikan memudahkan penilaian titik-titik kerentanan. Efektivitas pendekatan ini ditingkatkan ketika prioritas dan alokasi sumber daya disertakan dalam penilaian. Namun, meskipun mengidentifikasi titik-titik kerentanan merupakan hal yang paling penting dalam mengembangkan strategi perlindungan/pencegahan preemptif, sama pentingnya untuk mengembangkan mekanisme yang efektif yang dengannya serangan dunia maya dapat diidentifikasi dengan cepat.

Model pencegahan yang diartikulasikan ulang sangat penting, tetapi yang sama pentingnya adalah menerapkan langkah-langkah yang dengannya penetrasi dunia maya dapat diidentifikasi dengan cepat. Serangan yang tak terhitung jumlahnya terhadap korporasi—baik yang besar maupun kecil—memiliki tema yang meresahkan dan berulang: waktu yang signifikan yang berlalu setelah serangan sebelum korporasi menyadari bahwa peretasan telah terjadi. Hal ini menunjukkan kelemahan bermata dua seperti yang ditunjukkan pada Gambar 6.2.

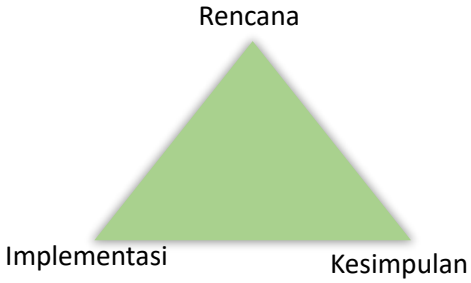


Gambar 6.2 Kelemahan bermata dua.

Fakta bahwa suatu serangan tidak ditanggapi selama jangka waktu tertentu meningkatkan kerentanan yang berasal dari satu serangan; dari perspektif model kontinum kerentanan, serangan yang tidak dilaporkan mencerminkan kerentanan yang berkelanjutan. Berbeda dari serangan terorisme tradisional, yang didasarkan pada satu serangan yang mencerminkan model tiga bagian: perencanaan, implementasi, kesimpulan, seperti yang ditunjukkan pada Gambar 6.3.

Apa risiko dalam kerentanan berkelanjutan? Artinya, transaksi saat ini dan masa mendatang rentan, dan pelanggan yang ada dan potensial berisiko. Pertanyaannya adalah,

bagaimana korporasi mulai merespons? Pertanyaan diajukan sehubungan dengan penetrasi spesifik dan ancaman umum.



Gambar 6.3 Model tiga bagian.

Namun, sebelum menjawab kedua pertanyaan tersebut, perlu diajukan pertanyaan awal: Mengapa perusahaan begitu ragu untuk mengakui bahwa peretasan telah terjadi? Jawaban mudahnya adalah pengakuan seperti itu berdampak negatif pada kondisi keuangan perusahaan, berpotensi menghalangi pelanggan baru, memberi pesaing kesempatan untuk mencetak poin, dan dapat meyakinkan pelanggan lama untuk beralih ke tempat lain. Itulah yang paling penting, yang disarankan oleh VP keamanan dalam percakapan kami. Kekhawatiran ini dapat dimengerti. Sampai batas tertentu, kekhawatiran ini dapat dipertahankan. Namun, kekhawatiran ini juga pada dasarnya tidak tepat.

Seperti yang disebutkan di atas, ada perbedaan yang jelas antara terorisme tradisional dan ancaman serangan siber. Terorisme tradisional mencerminkan model tiga bagian: perencanaan, implementasi, dan kesimpulan. Namun, ancaman serangan siber mengakibatkan perusahaan terus-menerus rentan. Jadi, pertanyaannya tetap, bagaimana seseorang, atau perusahaan, terus-menerus waspada terhadap ancaman yang terus-menerus? Pertimbangkan lari maraton. Untuk berlari maraton, seseorang harus berlatih.

Mungkin beberapa orang dapat memutuskan sehari sebelumnya untuk berlari sejauh 5K, 10K, atau setengah maraton. Yang lain akan membutuhkan waktu yang cukup untuk berlatih untuk perlombaan tersebut. Namun, maraton adalah perlombaan yang sebagian besar, jika tidak semua orang, akan membutuhkan setidaknya beberapa waktu untuk berlatih. Dan, dalam pelatihan itu, orang tersebut harus terus-menerus waspada. Mereka harus melakukan lari selama seminggu dengan lari jarak jauh yang berpuncak pada akhir pekan. Mereka harus makan dengan benar, cukup tidur, dan menghindari cedera sebaik mungkin.

Melindungi diri dari serangan siber juga sama. Perusahaan-perusahaan bertindak tepat dengan menjaga firewall mereka—memastikan kemampuan mereka untuk menggagalkan penyakit (serangan siber) atau penyakit sebaik mungkin. Perusahaan-perusahaan harus melakukan yang terbaik untuk menghindari cedera dengan memeriksa firewall secara berkala untuk menentukan apakah telah terjadi pelanggaran. Dan terakhir, perusahaan-perusahaan harus berlatih dengan waspada dengan terlibat dalam simulasi dan latihan untuk memvisualisasikan kelemahan mereka dan mengatasinya. Pada akhirnya, perusahaan-perusahaan terus-menerus berlatih maraton ketika mereka melindungi diri dari serangan siber

di masa mendatang.

6.6 KURANGNYA TANGGAPAN DAN KETERBUKAAN

Bagi sebuah perusahaan, lebih murah untuk bereaksi atau menangani peretasan daripada menghabiskan uang untuk pertahanan dan perlindungan. Jumlah perusahaan yang setelah peretasan—berhasil atau tidak—langsung melapor dan berkata, "Kami telah diretas, kami rentan, mari belajar dari ini" sangat sedikit. Itu adalah kesempatan yang hilang bagi perusahaan dan pihak lain. Ini merupakan kemenangan ganda bagi para peretas: keberhasilan penetrasi dan kegagalan perusahaan untuk saling belajar. Meskipun setiap perusahaan memiliki kepentingan untuk dilindungi, ada cukup banyak kesamaan dan nilai-nilai umum yang akan memudahkan—dan menyambut—pembagian informasi mengenai keberhasilan atau percobaan penetrasi.

Namun, kenyataannya adalah bahwa sebagian besar perusahaan sangat ragu untuk melapor dan mengakui bahwa mereka telah diretas. Untuk itu, mereka tidak terbuka kepada pelanggan, pemegang saham, dan penegak hukum. Selain itu, mereka menghambat atau mencegah perusahaan lain untuk melindungi diri mereka sendiri. Mungkin ada unsur rasa malu bahwa meskipun pengeluaran besar untuk firewall dan tim TI, kerentanan masih ada. Namun, mengingat kejahatan para penyerang siber, dan kerusakan yang ditimbulkan, perusahaan harus mengesampingkan faktor rasa malu itu dan bersikap lebih terbuka.

Mari kita pertimbangkan pelanggan: Sebagai pelanggan perusahaan yang telah diretas, Anda ingin segera tahu bahwa privasi Anda terancam. Anda berhak mengetahui bahwa seseorang yang tidak Anda beri wewenang memiliki nomor jaminan sosial, informasi kesehatan, dan informasi lain yang sangat pribadi. Perusahaan harus memiliki kewajiban langsung untuk memberi tahu pelanggan mereka.

Mari kita pertimbangkan pemegang saham: Pemegang saham memiliki kepentingan finansial yang signifikan yang dipertaruhkan. Meskipun demikian, ada pertimbangan finansial yang signifikan dalam menentukan kapan—dan bagaimana—memberi tahu pemegang saham tentang upaya atau keberhasilan serangan siber. Jelas, perusahaan mempertimbangkan dengan cermat dampak dari respons negatif. Meskipun demikian, perusahaan harus memiliki tanggung jawab mutlak untuk bersikap terbuka kepada pemegang saham sebisa mungkin dan segera.

Mari kita pertimbangkan penegakan hukum: Semakin cepat informasi diberikan kepada penegak hukum mengenai serangan siber, semakin efektif penegak hukum dapat memulai proses mengidentifikasi siapa yang bertanggung jawab. Perusahaan yang diserang, seolah-olah, memiliki kepentingan pribadi dalam membantu penegakan hukum; namun penundaan berulang kali dalam pelaporan menunjukkan adanya konflik dalam perusahaan, terlepas dari manfaat nyata yang diperoleh dari pelaporan langsung dan pembagian informasi.

Bayangkan skenario berikut: Anda dan keluarga baru-baru ini menghabiskan akhir pekan di Austin, Texas, menginap di jaringan hotel populer yang terletak di pusat kota dekat Lady Bird Lake. Selama di sana, Anda menikmati pemandangan indah dari kamar hotel dan pengalaman menginap yang menyenangkan. Anda membayar dengan kartu kredit, tanpa ragu-

ragu, dan meninggalkan ulasan bagus di situs web hotel. Kemudian pada minggu itu, sistem komputer hotel diretas, dan informasi kartu kredit Anda kini berada di tangan penyerang siber.

Bayangkan Anda adalah pelanggannya. Seberapa cepat Anda ingin mengetahui bahwa sistem hotel telah diretas, yang mengakibatkan informasi kartu kredit Anda berada di tangan penyerang siber? Apakah Anda memiliki hak hukum untuk mengetahuinya? Jika hotel menunda memberi tahu Anda, apakah Anda akan menderita kerugian tambahan di tangan penyerang siber? Pemulihan apa yang tidak lagi tersedia karena keterlambatan hotel dalam memberi tahu Anda tentang serangan siber?

Pada akhirnya, Anda, sebagai pelanggan, tentu ingin segera mengetahuinya. Bukan hanya agar dapat menanggapi situasi tersebut secara efektif, tetapi juga agar Anda merasa tenang karena mengetahui bahwa informasi Anda hanya berada di tangan orang-orang yang telah Anda percayai. Dalam skenario ini, mudah dipahami mengapa perusahaan, seperti sistem perhotelan, harus memiliki kewajiban untuk segera memberi tahu konsumen tentang pelanggaran tersebut, khususnya jika hal itu mengakibatkan hilangnya informasi pribadi mereka.

Sekarang, bayangkan Anda adalah pemegang saham jaringan hotel. Apakah Anda ingin tahu bahwa sistem hotel tersebut mengalami serangan siber? Dengan tidak memberi tahu Anda sebagai pemegang saham, apakah Anda merasa lebih percaya pada perusahaan tersebut? Tampaknya, kurangnya pemberitahuan kepada pemegang saham akan mengakibatkan meningkatnya ketidakpercayaan dan permusuhan antara pemegang saham dan perusahaan, bukan sebaliknya. Di dunia saat ini, di mana serangan siber begitu canggih, dan pencegahan 100% hampir mustahil, tampaknya pemegang saham akan lebih memahami sistem hotel yang mengalami serangan siber dan segera memberi tahu mereka, dibandingkan dengan sistem hotel yang mengalami serangan siber dan mencoba menutupinya.

Terakhir, mari kita pertimbangkan penegakan hukum. Jika kita menginginkan bantuan penegakan hukum dalam menangani perlindungan siber, atau mengharapkan keterlibatan mereka, kita tidak dapat menuntut kehadiran tersebut sementara memberikan mereka informasi yang sangat kurang. Penegakan hukum tidak akan efektif jika mereka tidak memiliki alat yang diperlukan. Tanpa segera memberi tahu penegak hukum tentang serangan siber, mereka tidak dapat menyelidiki tempat kejadian perkara dan mengembangkan pola—pola yang dapat mereka gunakan untuk memperingatkan dan memberi tahu sistem hotel lain, atau perusahaan, agar waspada. Pada akhirnya, pemberitahuan kepada konsumen, pemegang saham, dan penegak hukum sangat penting.

Untuk memfasilitasi proses pelaporan yang dilembagakan, kami mengalihkan perhatian kami ke peningkatan kerja sama di antara pihak-pihak yang secara langsung terkena dampak serangan siber terhadap suatu perusahaan.

6.7 KONSEKUENSI DARI KEGAGALAN BEKERJA SAMA

Diskusi dengan para pemimpin bisnis dari berbagai perusahaan menyoroti keraguan intrinsik untuk berbagi informasi dengan perusahaan lain. Di satu sisi, hal ini dapat dimengerti. Pertimbangan bisnis, kepentingan finansial, persaingan, dan rahasia dagang ditawarkan

sebagai alasan utama untuk pendekatan semacam itu. Di sisi lain, pemikiran strategis jangka panjang menunjukkan bahwa pendekatan yang berbeda sangat penting untuk berhasil melawan serangan siber.

Pendekatan jangka panjang yang lebih strategis ini terutama didasarkan pada pengakuan musuh bersama, dan menggabungkan kekuatan akan secara signifikan meningkatkan pengembangan tindakan pencegahan yang lebih efektif. Model kerja sama menunjukkan kerja sama antara perusahaan dan antara perusahaan dan penegak hukum.

Wawancara telepon yang ekstensif dengan pejabat penegak hukum di Florida menyoroti kurangnya kerja sama pada tiga tingkat berbeda terkait keamanan siber: perusahaan ke perusahaan, perusahaan ke penegak hukum, dan penegak hukum ke penegak hukum. Ini adalah waktu yang tepat untuk kembali ke pembahasan kita sebelumnya tentang Sony. Ketika Sony diretas, yang konon dilakukan oleh Korea Utara, itu merupakan indikasi adanya perusahaan besar yang diretas.

Apa yang dapat dilakukan Sony secara proaktif dan reaktif? Saya ingin menekankan pentingnya ancaman, kerentanan, dan waktu. Jadi jawaban mudah dalam hal tindakan proaktif oleh Sony adalah menginvestasikan sumber daya, personel, pengalaman, dan upaya tambahan dalam menciptakan firewall yang mungkin lebih canggih untuk melindungi diri mereka sendiri dengan lebih baik.

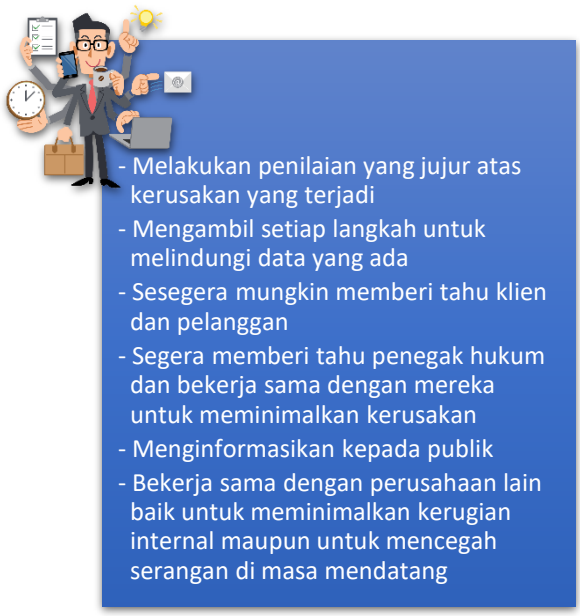
Mungkin, Sony tidak sepenuhnya menghargai kerentanan mereka sendiri sesuai dengan model kerentanan 12 poin; mungkin, pejabat Sony menyadari kerentanan mereka tetapi memilih pendekatan menutup mata. Atau, mungkin, Sony meremehkan dampak film tersebut dari perspektif Korea Utara dan gagal mengenali kemampuan siber rezim tersebut. Kegagalan tersebut mencakup banyak vektor, termasuk (1) kurangnya proaktivitas, (2) kurangnya pengakuan atas kemampuan orang lain, dan (3) kurangnya pengakuan kerentanan.

Di sini saya ingin menyela dengan catatan pribadi dari pengalaman saya sendiri: meremehkan kemampuan, kecanggihan, dan keinginan penyerang, baik itu teroris tradisional atau negara-bangsa atau dunia maya, adalah kesalahan yang luar biasa. Korporasi, individu, atau negara-bangsa, dari waktu ke waktu, secara konsisten meremehkan kemampuan penyerang potensial.

Kita meremehkan; menganggap sistem kita lebih baik atau lebih efektif atau efisien. Serangan yang berhasil terhadap korporasi menunjukkan dan menunjukkan, dari waktu ke waktu, bagaimana kepemimpinan telah gagal menerapkan tindakan pencegahan proaktif. Kurangnya kerja sama yang dilembagakan merupakan manifestasi dan kontributor terhadap realitas yang mengganggu ini. Jadi, itu adalah pada sisi proaktif (Gambar 6.4). Apa yang harus dilakukan korporasi setelah menemukan penetrasi telah terjadi?

Melakukan tindakan ini memerlukan kecanggihan, kerja sama tim, dan kemampuan—dan kemauan—untuk menganalisis kerentanan internal. Reaksi yang cepat meminimalkan kerugian di masa mendatang. Namun, hasil utama dari pemeriksaan bagaimana perusahaan bereaksi terhadap peretasan yang berhasil adalah kegagalan untuk merespons dengan cepat. Apakah kegagalan untuk merespons dengan cepat disengaja atau tidak masih menjadi pertanyaan terbuka; meskipun demikian, hal itu menunjukkan kecanggungan karena tidak

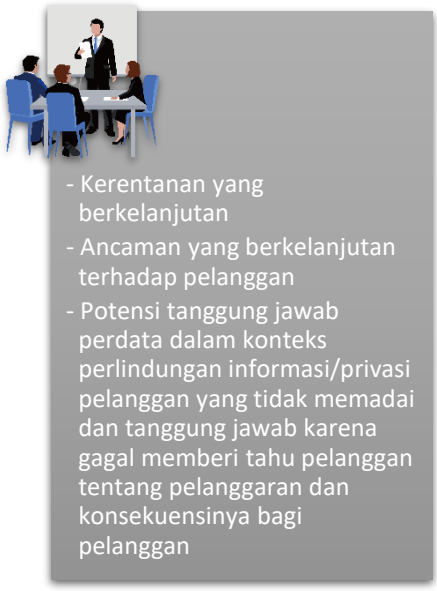
dapat mengidentifikasi penetrasi dengan cepat, dan kegagalan untuk memberi tahu pelanggan.



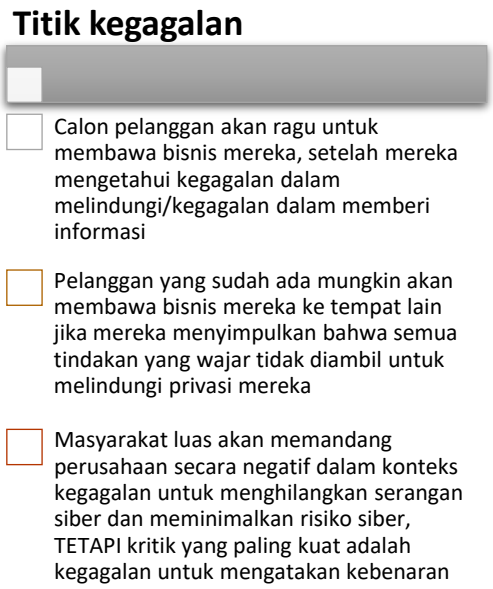
Gambar 6.4 Respons korporasi.

Konsekuensinya signifikan yang diberikan pada Gambar 6.5.

Meskipun fokus pada kemungkinan tuntutan hukum dapat dipahami, masalah yang lebih penting adalah kegagalan untuk melindungi dan kegagalan untuk memberi tahu. Alasannya jelas dan diberikan pada Gambar 6.6.

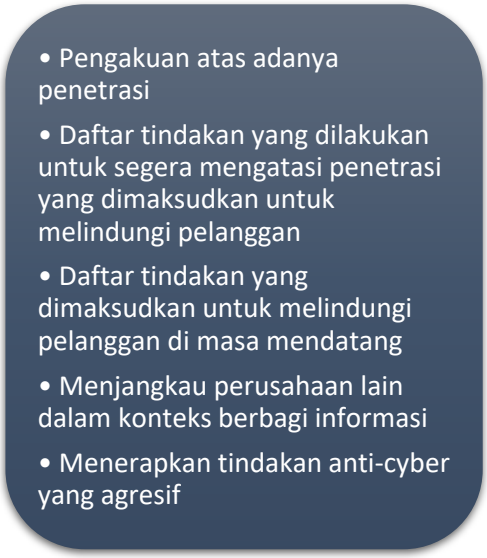


Gambar 6.5 Konsekuensi bagi korporasi.



Gambar 6.6 Titik kegagalan.

Lalu, apa artinya itu bagi perusahaan? Secara gamblang, perusahaan harus lebih terbuka. Saya pikir ada manfaat yang jelas diperoleh perusahaan dalam membahas secara publik ketika mereka telah dilanggar. Meskipun masyarakat akan menyatakan kekhawatiran setelah serangan yang dilaporkan, reaksi jangka panjang akan berupa penghargaan karena telah mengatakan kebenaran. Selain itu, pengetahuan tentang bagaimana pelanggaran terjadi, jika dibagikan kepada masyarakat, dapat mencegah pelanggaran di masa mendatang di perusahaan lain dengan cara yang sama. Perubahan perilaku ini dapat memberikan dampak positif yang besar yang berpotensi memengaruhi jutaan konsumen. Kebenaran itu perlu dibahas sebagaimana diberikan dalam Gambar 6.7.



Gambar 6.7 Kebenaran korporasi.

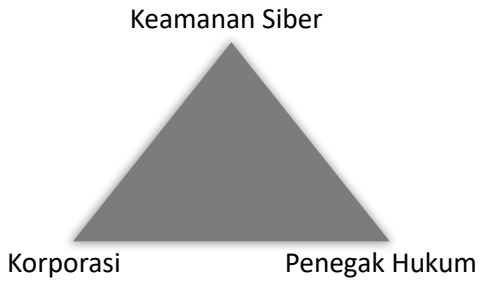
Ada risiko dalam pendekatan terbuka ini; namun, dari perspektif biaya-manfaat, sisi positifnya pada akhirnya lebih besar daripada sisi negatifnya. Meskipun elemen kerentanan muncul dari keterbukaan dan keterusterangan, pendekatan yang menekankan penerapan langkah-langkah untuk mencegah serangan di masa mendatang, kejujuran dengan pelanggan dan publik mencerminkan hal-hal berikut: (1) perlindungan pelanggan yang lebih baik, (2) perlindungan infrastruktur penting yang lebih baik; dan (3) perlindungan yang lebih baik terhadap kepentingan yang lebih besar.

Mitigasi risiko yang didasarkan pada kejujuran dan tindakan agresif yang proaktif adalah sama-sama menguntungkan. Dari perspektif hukum, dalam hal meminimalkan dampak potensial dari gugatan perdata, kebijakan keterusterangan dan kejujuran yang didasarkan pada "kami mengambil langkah-langkah untuk meminimalkan paparan informasi pribadi dan belajar darinya serta bekerja sama dengan pelanggan," akan mengurangi kemungkinan tuntutan hukum terhadap perusahaan. Pendekatan semacam itu menunjukkan, dari perspektif perusahaan, kemauan untuk melibatkan audiens yang berbeda, khususnya pelanggan dan penegak hukum.

6.8 PENEGAKAN HUKUM

Tidak diragukan lagi bahwa serangan siber menimbulkan tantangan baru yang sangat sulit bagi penegakan hukum. Percakapan dengan pejabat penegak hukum menekankan bahwa kejahatan siber sangat berbeda dari polisi dan perampok tradisional maupun terorisme konvensional. Bagi penegakan hukum, kejahatan siber merupakan model kejahatan yang sangat berbeda yang menimbulkan tantangan yang kompleks dan rumit. Interaksi dengan pejabat penegak hukum menunjukkan keinginan yang sangat besar untuk bekerja sama dengan perusahaan baik secara proaktif maupun reaktif.

Motivasi utamanya adalah mengurangi ancaman dan meminimalkan dampak serangan yang sebenarnya. Segitiga keamanan siber, perusahaan, dan penegakan hukum menuntut kemampuan operasional yang, secara harfiah, berkembang seiring berjalannya waktu (Gambar 6.8).

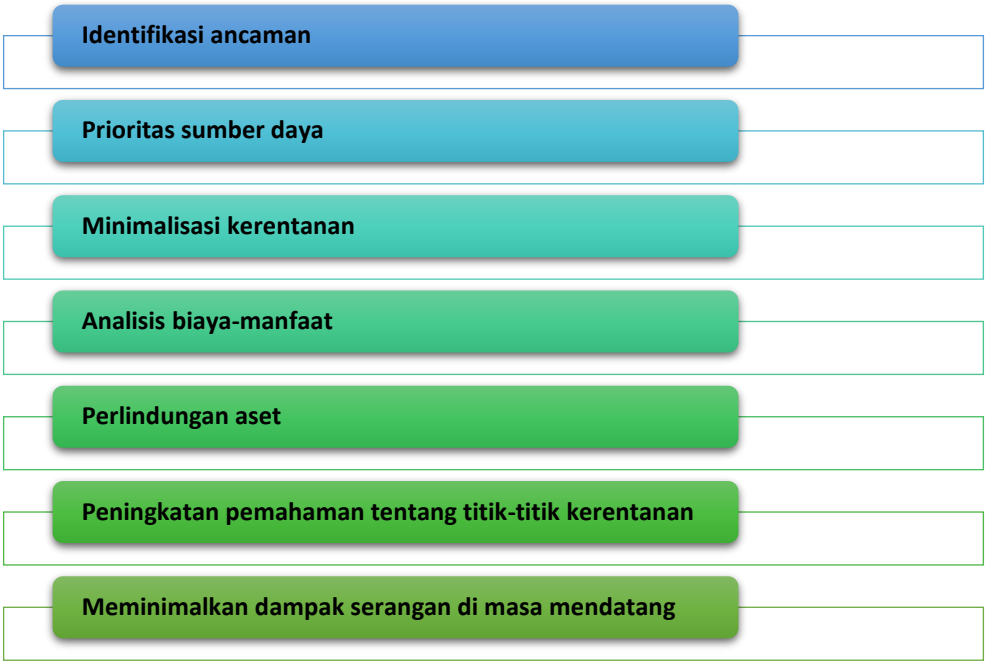


Gambar 6.8 Segitiga keamanan siber.

Agar penegakan hukum dapat melindungi perusahaan secara efektif, diperlukan perubahan mendasar dalam konteks dan konsep kerja sama. Agar penegakan hukum dapat melindungi perusahaan secara lebih efektif, perusahaan harus lebih terbuka kepada penegak

hukum. Kerja sama ini akan memudahkan penegak hukum memahami di mana peretasan itu terjadi, di mana kerentanan spesifiknya, dan akan meningkatkan penanganan 12 titik kerentanan.

Ini hanya dapat terjadi jika perusahaan lebih terbuka. Dalam hal itu, beban ada pada mereka. Kegagalan untuk bekerja sama dengan penegak hukum mencegah pengembangan—apalagi implementasi—model kerja sama penegakan hukum-perusahaan yang canggih. Karena kerentanan terhadap individu yang diakibatkan oleh serangan siber yang berhasil, ada kebutuhan mendesak untuk pendekatan yang tidak biasa terhadap penegakan hukum.



Gambar 6.9 Model penegakan hukum.

Namun, syarat untuk pendekatan tersebut adalah kemauan perusahaan untuk memandang penegakan hukum sebagai mitra penuh, baik secara preemptif maupun reaktif. Untuk tujuan tersebut, diperlukan model tata kelola perusahaan untuk keamanan siber; meskipun saat ini belum dimanfaatkan, beban pengembangannya berada di tangan perusahaan. Pejabat penegak hukum berulang kali menyatakan kemauan untuk bekerja sama erat dengan perusahaan dalam pengembangan dan penerapannya. Model tersebut akan menekankan item yang tercantum dalam Gambar 6.9.

6.9 INVESTASI

Serangan baru-baru ini menunjukkan bahwa diperlukan waktu hingga 243 hari bagi perusahaan untuk memahami, mengenali, dan menemukan bahwa perusahaan telah diretas. Salah satu alasan penundaan yang mencengangkan—dan sangat meresahkan—ini adalah bahwa pencegahan siber memerlukan investasi yang signifikan. Investasi tersebut tidak hanya bersifat finansial, tetapi juga memerlukan investasi dalam personel yang memerlukan perubahan penting dalam budaya perusahaan yang memerlukan kepemimpinan untuk

mengenali dan mengartikulasikan kerentanan siber.

Dalam konteks kerentanan, 12 langkah produksi—kadang-kadang disebut sebagai bean to cup—mengharuskan perusahaan, besar, menengah, dan kecil, untuk bertanya kepada diri mereka sendiri kepada siapa mereka berutang tugas utama. Jawaban yang jelas adalah pemegang saham dan pelanggan.

Konsekuensinya signifikan dan mahal. Tugas itu membebankan kewajiban kepada perusahaan untuk membuat firewall canggih yang meningkatkan perlindungan yang diberikan kepada kedua audiens. Namun, dalam konteks memprioritaskan tugas, saya sarankan tugas yang paling utama adalah kepada pelanggan: konsekuensi dari pelanggaran privasi begitu menakutkan dan signifikan sehingga tugas ini membebankan kewajiban yang luar biasa kepada pimpinan perusahaan.

Tentu saja pertanyaan tentang biaya akan muncul; para pemimpin perusahaan, yang telah saya temui berulang kali, dengan tegas menyampaikan kekhawatiran itu. Dari sudut pandang mereka, itu adalah kekhawatiran yang dapat dibenarkan. Dari sudut pandang yang lebih luas dan lebih strategis, sudut pandang ini tidak dapat dibenarkan. Mengingat ancaman yang ditimbulkan oleh dunia maya, perusahaan perlu mengakui keutamaan tugas yang harus diemban kepada pelanggan daripada kepada pemegang saham. Model prioritas yang diartikulasikan ulang itu memaksakan kepada para pemimpin perusahaan persyaratan untuk lebih terbuka, jujur, dan terbuka meskipun hal itu menimbulkan kekhawatiran di antara para pemegang saham. Pendekatan ini didasarkan pada pengakuan bahwa tugas utama perusahaan adalah melindungi—dan memberi tahu—pelanggan, meskipun tugas itu membebani perusahaan.

Jika tidak, pelanggan dapat dengan sah bertanya—Apakah perusahaan cukup melindungi saya? Jika jawabannya tidak, maka itu sangat mengkhawatirkan dalam konteks bagaimana perusahaan menanggapi keamanan dunia maya. Demikian pula, dan yang tidak kalah pentingnya, langkah-langkah kerja sama yang canggih antara perusahaan dan penegak hukum harus dilaksanakan. Meskipun dapat dimengerti bahwa hal ini bermasalah dan mungkin menjadi sumber ketidaknyamanan, kewajiban kepada pelanggan menjamin, jika tidak menuntut, pendekatan semacam itu. Meskipun beberapa perusahaan memang telah memulai proses pengeluaran sumber daya yang signifikan untuk perlindungan siber, ini hanyalah segelintir perusahaan.

Sampai semua perusahaan—besar, menengah, dan kecil—sepenuhnya memahami ancaman serius yang ditimbulkan oleh peretas, tindakan penanggulangan siber tidak akan berhasil, sehingga menimbulkan risiko yang signifikan bagi ratusan juta pelanggan. Hal ini dengan sendirinya membenarkan pengembangan kebijakan siber yang didasarkan pada pemberian informasi kepada publik, terlepas dari biayanya, baik langsung maupun tidak langsung.

Biaya langsung mencakup perekrutan pakar siber yang mahal; biaya tidak langsung mencakup kemungkinan kehilangan bisnis. Biaya tambahan mencakup hilangnya pendapatan, sementara serangan siber ditanggapi. Dan ada biaya keempat: Bagaimana Anda mempertahankan loyalitas pelanggan ketika perusahaan tidak hanya gagal melindungi

pelanggan tetapi—mungkin yang lebih penting—gagal memberi tahu/memberi tahu pelanggan tentang serangan siber?

Cara terbaik untuk memastikan kesetiaan saya adalah dengan menunjukkan kepada saya bahwa Anda telah menerapkan langkah-langkah perlindungan siber yang memadai, memuaskan, dan canggih secara proaktif yang akan melindungi saya. Jika setelah peretasan berhasil, ternyata Anda tidak cukup proaktif melindungi saya, maka wajar untuk berasumsi bahwa Anda akan kehilangan saya sebagai pelanggan.

Sebaliknya, jika Anda sebagai perusahaan menerapkan firewall canggih semacam ini dan terjadi peretasan, asumsi saya adalah Anda tidak akan mudah kehilangan kesetiaan saya, karena dari sudut pandang saya, Anda telah melakukan langkah-langkah untuk melindungi saya dan saya sepenuhnya tahu bahwa Anda tidak dapat melindungi saya 100% sepanjang waktu.

Jadi, meskipun loyalitas pelanggan disebutkan sebagai biaya, menurut saya kebenarannya berkaitan dengan kebijakan dan perusahaan; kegagalan untuk menyusun rencana merupakan cara pasti untuk kehilangan loyalitas pelanggan daripada tidak menyusun rencana.

Apa artinya itu dalam konteks geopolitik? Perusahaan besar, yang berorientasi internasional, di mana pun kantor pusatnya berada, memiliki cabang di seluruh dunia. Jelas, ada hubungan yang kuat antara geopolitik dan perusahaan, khususnya perusahaan yang berfokus pada pasar internasional. Hal ini mengharuskan perusahaan, yang memiliki kehadiran internasional, untuk sepenuhnya menyadari hukum terkait kewajiban keamanan siber.

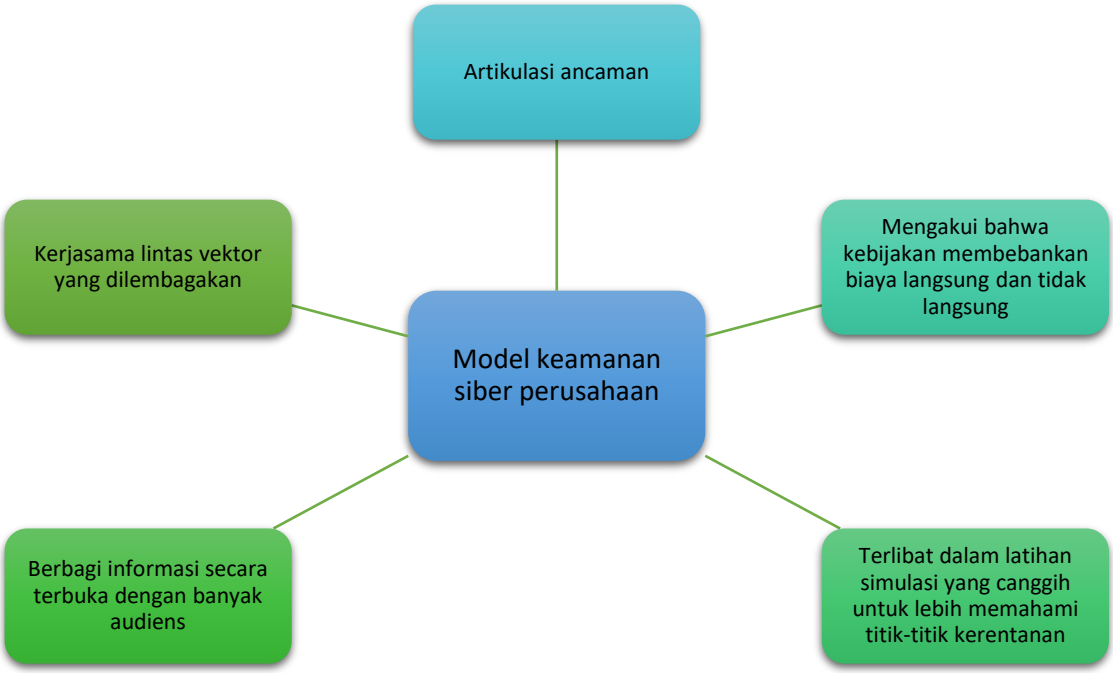
Perusahaan yang mempertimbangkan untuk mendirikan kantor di negara lain harus sepenuhnya memahami hukum keamanan siber untuk memastikan bahwa tindakan yang memadai telah diambil terkait kepatuhan. Selain itu, perusahaan harus mengerahkan energi yang signifikan untuk memahami budaya yang berbeda. Implikasinya jelas: Jika negara tuan rumah sangat sensitif terhadap serangan siber, baik dari segi hukum maupun budaya, maka perusahaan (eksternal) yang berinvestasi tidak hanya perlu memastikan kepatuhan terhadap hukum tetapi juga berkenaan dengan budaya siber dan budaya perlindungan siber negara tersebut.

Saya ingin menceritakan kepada Anda satu atau beberapa percakapan yang pernah saya lakukan dengan wakil presiden untuk keamanan perusahaan yang khawatir bahwa level C tidak cukup fokus pada siber, tetapi yang saya sarankan adalah kita memeriksa sensitivitas perusahaan yang ingin berinvestasi di luar negeri; maka persyaratan, persyaratan kepatuhan, dalam hal hukum, kebijakan, dan budaya pada perusahaan menjadi signifikan. Saya akan menyarankan dalam konteks itu untuk meminimalkan kemungkinan ancaman yang ditimbulkan oleh serangan siber; pada akhirnya, minimalisasi itu akan menjadi hal yang negatif dari perspektif perusahaan itu dalam hal klien masa depan dan juga dalam konteks pemegang saham.

Jadi, apa yang perlu dilakukan perusahaan? Para pemimpin perusahaan dapat duduk bersama dan berdiskusi tanpa henti tentang titik-titik kerentanan, tetapi satu-satunya mekanisme yang paling efektif untuk benar-benar memahami titik-titik kerentanan tersebut

adalah dengan melakukan latihan simulasi yang canggih baik secara internal maupun dengan para ahli untuk mengidentifikasi di mana perusahaan tersebut rentan.

Saya akan sangat menyarankan penegak hukum untuk duduk bersama dengan perusahaan lain dan pejabat pemerintah. Jika tidak, latihan tersebut akan mirip dengan ruang gema, yang sebagian besar tidak efektif dalam hal mengartikulasikan dan menerapkan kebijakan keamanan siber yang efektif. Saya sepenuhnya memahami dan menghargai bahwa bagi banyak pemimpin perusahaan, gagasan kerja sama yang dilembagakan dengan penegak hukum, badan pemerintah, perusahaan lain, dan pesaing menimbulkan tanda bahaya.



Gambar 6.10 Model keamanan siber perusahaan.

Namun, mengingat biaya, dampak, dan kejahatan peretas keamanan perusahaan, saya tidak yakin bahwa ada alternatif lain selain mengartikulasikan ulang model keamanan siber perusahaan (Gambar 6.10). Pertanyaan yang perlu dipertimbangkan dalam meninjau Bab 6 diberikan pada Gambar 6.11.

Latihan Soal

1. Haruskah korporasi bertanggung jawab atas keamanan siber mereka sendiri?
2. Haruskah pemerintah memaksa korporasi untuk memiliki kebijakan keamanan siber?
3. Haruskah korporasi diwajibkan untuk berbagi informasi keamanan siber yang relevan dengan korporasi lain, termasuk pesaing?
4. Haruskah korporasi diwajibkan untuk melaporkan ketika mereka diserang kepada penegak hukum?
5. Haruskah korporasi memiliki kewajiban untuk melaporkan serangan siber kepada pemegang saham?

Gambar 6.11 Pertanyaan tinjauan.

BAB 7
INDIVIDU DALAM MENGURANGI RISIKO KEAMANAN SIBER

7.1 PENDAHULUAN

Beralih dari korporasi, selanjutnya kita dapat mempertimbangkan siapa saja yang membentuk korporasi. Individu dapat mengurangi risiko, bahaya, dan kerentanan yang ditimbulkan oleh keamanan siber. Masing-masing dari kita, secara individu, berperan dalam konteks keamanan siber. Berikut ini adalah contoh kecil. Banyak dari kita yang pernah diretas, baik kartu kredit kita dibobol atau email kita diretas. Jadi, kita masing-masing memiliki pengalaman pribadi. Keamanan siber dapat dilihat baik pada tingkat pribadi maupun umum.

7.2 SIBER PADA TINGKAT PRIBADI

Dalam pengalaman pribadi kita, reaksi awal adalah kekesalan. Namun, kekesalan biasanya merupakan kerugian terbesar yang kita derita. Dalam kasus pelanggaran kartu kredit, bank biasanya mendapatkan kembali uangnya, dan kerugiannya tidak terlalu signifikan. Secara keseluruhan, ini adalah kerugian finansial jangka pendek yang dikompensasikan, setelah dana dikembalikan. Secara individu, pelanggaran kartu kredit sekali saja bukanlah tanda bahaya yang mencolok. Pelanggaran kartu kredit kedua, atau bahkan ketiga, seharusnya menjadi peringatan tentang perlunya melindungi diri kita sendiri dengan lebih baik.

Sebagian besar dari kita tidak mengambil perlindungan yang memadai, atau memenuhi standar keamanan minimum, untuk melindungi kartu kredit dan kata sandi kita dengan lebih baik. Mengapa demikian? Alasannya adalah bahwa sering kali pelanggaran kartu kredit tidak terlalu berbahaya, hanya sekadar ketidaknyamanan, sehingga ancaman pelanggaran tidak terlalu menakutkan. Pertanyaan utamanya adalah apakah meminimalkan ketidaknyamanan merupakan respons individu yang tepat terhadap serangan siber dan mempertimbangkan apakah kebocoran kartu kredit atau kata sandi lebih dari sekadar gangguan.

Gagasan di balik meminimalkan ketidaknyamanan tampaknya merupakan respons yang salah. Seorang peretas, yang mencoba membobol kartu kredit dan kata sandi, lebih suka kita masing-masing meminimalkan ketidaknyamanan daripada mengatasi ancaman. Pertanyaan penting yang harus ditanyakan setiap individu diberikan dalam Gambar 7.1.

Dalam mempertimbangkan titik-titik kerentanan, pertanyaannya adalah, haruskah kita memiliki harapan atau tuntutan yang lebih besar dari perusahaan kartu kredit kita untuk melindungi kita dengan lebih baik? Sebagai individu, kita tampaknya memiliki tanggung jawab untuk melindungi diri kita sendiri dengan lebih baik karena ancaman peretasan siber itu signifikan. Seperti yang disebutkan sebelumnya, peretasan siber tidak selalu mengakibatkan kematian. Namun, catatan pribadi kita akan terekspos, dan itu mengakibatkan ancaman. Banyak kejadian di masa lalu menunjukkan kerugian yang melampaui pelanggaran kartu kredit dan hilangnya dolar.

Seperti disebutkan di atas, sangat penting untuk mempertimbangkan titik-titik kerentanan dalam menentukan cara terbaik untuk melindungi diri kita dari pelanggaran kartu

kredit. Analisis titik-titik kerentanan mengakibatkan Anda, sebagai individu, memeriksa aspek-aspek kehidupan Anda untuk menentukan titik-titik penetrasi termudah bagi penyerang dunia maya.

Pertama, serangan dunia maya sering terjadi melalui email. Secara khusus, penyerang dunia maya memperoleh akses ke akun email pribadi kita, dan dengan demikian, mengakses sejumlah besar informasi pribadi yang Anda, sebagai individu, ingin rahasiakan. Mengapa ini terjadi? Pertanyaan itu menyangkut kata sandi. Seberapa sering kita mengubah kata sandi kita? Seberapa berbeda kata sandi email kita dari kata sandi kita dengan hal-hal lainnya? Ketika kita menerima pengingat untuk memperbarui kata sandi kita, apakah kita benar-benar melakukannya? Apakah kata sandi kita sesuatu yang dapat dengan mudah ditebak, baik nama gadis kita atau kota tempat kita tinggal? Semua pertimbangan ini menciptakan titik kerentanan.

Kedua, serangan siber sering terjadi saat penyerang mengakses informasi kartu kredit kita. Hal ini dapat terjadi karena kita memasukkan PIN debit dan peretas memperoleh informasi tersebut. Seperti kata sandi email kita, apakah kita sudah cukup melindungi kata sandi ATM kita? Pom bensin yang sering saya kunjungi selalu mengingatkan setiap kali saya memasukkan PIN untuk memastikan bahwa saya melindungi PIN saya. Metode yang dianjurkan adalah meletakkan tangan saya di atas tangan saya yang lain saat memasukkan PIN, sehingga menghambat kemampuan untuk melihat PIN. Apakah saya melakukan ini setiap saat? Biasanya tidak. Saya cenderung teralihkan atau lupa, meskipun sudah diperingatkan sebelumnya. Hal ini menciptakan titik kerentanan.

Ketiga, serangan siber dapat terjadi terhadap kita sebagai individu, saat kita ceroboh dengan nomor jaminan sosial kita. Ada dua cara kita bisa ceroboh dengan nomor jaminan sosial kita, baik karena perbuatan kita sendiri maupun karena perbuatan orang lain. Kita bisa ceroboh, karena perbuatan kita sendiri, dengan memasukkan nomor jaminan sosial kita ke situs web yang tidak dilindungi dengan baik. Salah satu contoh yang secara khusus memengaruhi seorang pembaca adalah saat dia mencari apartemen di CraigsList. Satu postingan mengharuskan orang tersebut untuk mengisi informasi untuk pemeriksaan latar belakang yang diperlukan, yang mencakup memasukkan nomor jaminan sosialnya.

Tanpa berpikir dua kali, orang ini memasukkan nomor jaminan sosialnya dan mengirimkan informasi tersebut ke situs web yang tidak dikenal. Trik ini sering digunakan oleh penyerang dunia maya dan merupakan cara mudah bagi mereka untuk memangsa orang yang tidak tahu apa-apa dalam mengakses nomor jaminan sosial mereka. Ini adalah hasil langsung dari orang tersebut yang memasukkan nomor jaminan sosialnya secara proaktif.

Kita bisa ceroboh dengan nomor jaminan sosial kita dan secara langsung terpengaruh oleh tindakan orang lain. Orang lain sering mengunjungi taman anjing setempat. Di sekitar taman anjing ini, ada tanda-tanda yang dengan jelas mengatakan, "Ambil barang-barang Anda, sembunyikan kunci Anda, dan kunci mobil Anda." Meskipun ada peringatan, orang ini meninggalkan dompetnya di kursi depan.

Tidak hanya itu, orang ini meninggalkan kartu jaminan sosialnya di dompet yang sama yang ada di kursi depan. Setelah selesai di taman anjing, orang ini kembali ke kendaraannya

untuk menemukan jendela depan yang pecah dan dompet serta nomor jaminan sosial yang sekarang hilang. Agar dapat lebih melindungi individu terhadap serangan keamanan siber, penting untuk mengenali banyak titik kerentanan dalam kehidupan kita dan menentukan cara terbaik untuk meminimalkan risiko yang ditimbulkan oleh setiap titik kerentanan.

7.3 PELANGGARAN CATATAN KESEHATAN

Pertimbangkan pelanggaran catatan kesehatan, pertimbangkan catatan Anda, atau catatan anggota keluarga Anda, yang terekspos dan tersedia untuk orang lain. Pelanggaran ini akan menimbulkan konsekuensi yang mengerikan. Jika catatan Anda terekspos dan disebarkan di Internet, ada potensi untuk mempermalukan. Kita masing-masing memiliki hal-hal dalam catatan medis kita yang tidak ingin diketahui orang lain. Jadi, pelanggaran status seperti itu mengakibatkan rasa malu karena penyebaran informasi yang seharusnya bersifat rahasia.

Selain pelanggaran tersebut memengaruhi kehidupan pribadi kita, pelanggaran catatan medis dapat memengaruhi kemungkinan peluang kerja. Calon pemberi kerja dapat, bahkan melalui metode yang jahat, menanyakan dan memperoleh catatan kesehatan seseorang dan mengajukan pertanyaan tambahan dalam menentukan peluang kerja. Tidak hanya calon pemberi kerja, terekspos nya catatan kesehatan rahasia dapat memengaruhi pemberi kerja Anda saat ini.

Mari kita tinjau kembali dan pertimbangkan, misalnya, jika pada pekerjaan Anda saat ini, catatan medis tertentu terungkap, hal itu dapat memengaruhi kemungkinan promosi, persepsi rekan kerja, dan kemampuan Anda untuk terus menjadi karyawan yang efektif. Selain hubungan pribadi dan pekerjaan, pelanggaran tersebut dapat memengaruhi hubungan Anda dengan perusahaan asuransi. Seperti yang kita semua ketahui, saat Anda mencari asuransi kesehatan, mungkin ada hal-hal yang tidak ingin Anda ketahui oleh perusahaan asuransi. Namun, setelah catatan tersebut dilanggar dan disebarkan, informasi tersebut dapat dilihat oleh semua orang, termasuk perusahaan asuransi.

Keempat, selain hubungan pribadi, bisnis, dan asuransi, pelanggaran catatan kesehatan dapat mengakibatkan penyebaran informasi di media sosial, khususnya Facebook atau Twitter. Dengan demikian, informasi yang dilanggar kini telah memengaruhi kontur luas kehidupan Anda sehari-hari.

Pertimbangkan contoh kehidupan nyata berikut. Seorang individu saat ini sedang menjalani perawatan untuk kanker esofagus stadium IV. Ia terdaftar dalam uji klinis, yang mengakibatkan ia harus menjalani pemeriksaan laboratorium dan perawatan setiap dua minggu sekali. Individu ini saat ini tidak bekerja, begitu pula suaminya. Namun, pada perawatan terakhirnya, sistem komputernya mati. Jadi, hari kerja enam jam yang sudah panjang berubah menjadi hari kerja sembilan jam yang lebih panjang karena tim medis mencoba mendapatkan hasil tes darah yang diperlukan tanpa akses ke komputer.

Penundaan ini mengakibatkan penyakit tambahan bagi individu tersebut, karena tubuhnya saat ini tidak dapat menangani terlalu banyak aktivitas berat, mengingat ia saat ini sedang berjuang melawan kanker stadium akhir. Namun, penundaan tersebut tidak hanya mengakibatkan penyakit tambahan, tetapi juga mengakibatkan rasa takut untuk melanjutkan

perawatan. Pada saat sistem komputer mati pada hari perawatan, tidak seorang pun menyadari bahwa sistem tersebut sedang diretas.

Sebaliknya, mereka percaya itu adalah suatu bentuk kerusakan. Namun, lima hari kemudian, sistem masih mati, dan sangat jelas bahwa mereka telah menjadi korban serangan siber. Orang ini tidak takut catatan medisnya terekspos ke pemberi kerja saat ini atau di masa mendatang, dia juga tidak takut catatannya diunggah di media sosial. Sebaliknya, dia paling takut tidak dapat mengakses perawatan uji klinis yang diperlukan karena serangan siber tersebut. Ini jelas menunjukkan bahwa pelanggaran sistem rumah sakit memiliki banyak konsekuensi negatif; dengan demikian kebutuhan akan pencegahan dan perlindungan menjadi jelas.

7.4 KUNCI PERLINDUNGAN

Ancaman telah terbukti. Kerugian telah terbukti. Oleh karena itu, pertanyaannya adalah, apa yang harus dilakukan? Kunci pertama untuk perlindungan adalah pendidikan bagi individu. Sangat penting untuk mendidik individu tentang bahaya yang ditimbulkan oleh peretas dunia maya. Kunci kedua untuk perlindungan adalah mendidik individu dalam langkah-langkah untuk menekan bank mereka, penyedia layanan kesehatan mereka, perusahaan asuransi mereka, dan pemegang informasi rahasia lainnya untuk terlibat dalam perlindungan individu yang lebih canggih dan efektif.

Dua kunci perlindungan, pendidikan individu tentang perlindungan dan individu yang menuntut perlindungan, menciptakan jalan dua arah. Ketika kita, sebagai individu, mendaftar dengan penyedia layanan kesehatan, banyak dari kita tidak cukup menuntut perusahaan asuransi untuk menunjukkan bagaimana mereka akan melindungi catatan kita. Ini adalah kesalahan. Adalah wajar, sebagai individu, untuk menuntut perusahaan asuransi kesehatan untuk bersikap proaktif dalam hal meminimalkan kerentanan setiap individu terhadap serangan dunia maya.

Hal ini dapat dilihat sebagai bentuk kebersihan siber, mekanisme, atau infrastruktur untuk secara konsisten menangani perlindungan yang memadai. Beban ini dibebankan pada dua kelompok, seperti yang ditunjukkan pada gambar di atas. Beban pertama dibebankan pada individu dalam hal bagaimana saya, sebagai individu, melindungi diri saya sendiri. Perlindungan ini semudah mengubah kata sandi secara berkala. Selain itu, individu dapat, dan boleh dibilang harus, mengambil langkah berikutnya untuk menuntut, tidak hanya lebih banyak dari dirinya sendiri tetapi juga dari layanan yang diberikan kepada mereka. Berikut adalah contoh kunci kedua untuk perlindungan. Jika individu membeli sesuatu dari industri kesehatan, mereka dapat memberikan daftar tuntutan.

Dalam hal perlindungan siber, tuntutannya adalah untuk melihat rencana permainan, semacam daftar periksa, tentang bagaimana perusahaan akan melindungi catatan kesehatan rahasia yang dipercayakan kepada mereka. Ini termasuk meminimalkan ancaman peretasan dengan mengidentifikasi titik-titik kerentanan. Ini terkait kembali dengan bab sebelumnya yang melibatkan bagaimana perusahaan menanggapi keamanan siber.

Dalam bab itu, kita membahas argumen bahwa perusahaan harus lebih terbuka ketika

mereka mengalami serangan siber. Sifat yang akan datang ini tidak hanya berlaku untuk penegakan hukum, untuk tujuan meningkatkan perlindungan siber, tetapi juga untuk konsumen individu, untuk tujuan menyampaikan tingkat dan tingkat keparahan peretasan. Ada hubungan langsung antara tanggung jawab dan harapan yang kita miliki dengan perusahaan dengan tanggung jawab dan harapan yang kita miliki dengan perusahaan asuransi kesehatan, karena keduanya adalah pemegang informasi rahasia individu.

Melanjutkan contoh sebelumnya tentang penyerang siber yang berfokus pada sistem komputer uji klinis, mari kita terapkan diagram jalan dua arah untuk melihat bagaimana perlindungan dapat dicapai, baik melalui pendidikan individu tentang perlindungan maupun individu yang menuntut perlindungan. Pendidikan individu tentang perlindungan berfokus pada hal-hal kecil yang dapat dilakukan individu untuk memastikan perlindungan. Individu yang menuntut perlindungan berfokus pada tuntutan yang harus dibuat individu kepada mereka yang menyimpan informasi individu tersebut.

Dengan contoh sebelumnya, seorang individu saat ini sedang menjalani perawatan di uji klinis lokal. Suatu hari, sistem komputer diserang, yang mengakibatkan perawatan hari itu diperpanjang secara signifikan, serta ancaman nyata bahwa perawatan tidak dapat dilanjutkan karena kurangnya kontrol atas sistem komputer.

Dalam mempertimbangkan aspek pertama, pendidikan individu tentang perlindungan, penting untuk menentukan dengan cara apa individu benar-benar dapat mendidik diri mereka sendiri. Hal ini sulit dalam skenario khusus ini, karena tidak banyak yang dapat dikontrol individu dengan sistem komputer uji klinis. Mereka tidak menggunakan login; oleh karena itu, sistem ini tidak menangani kebutuhan untuk mengubah kata sandi. Selain itu, mereka tidak gegabah dalam memberikan informasi; sebaliknya, mereka mempercayakannya kepada penyelenggara uji klinis, dengan pengertian bahwa informasi tersebut akan dilindungi. Jadi, dalam skenario ini, jalan dua arah lebih berfokus pada kebutuhan individu untuk menuntut perlindungan.

Pertanyaannya kemudian adalah bagaimana seseorang dapat menuntut operator uji klinis untuk melindungi informasi penting mereka. Ketika pertama kali berkonsultasi dengan uji klinis, apakah individu tersebut menanyakan perlindungan apa yang saat ini berlaku untuk informasi pribadi mereka? Apakah mereka menuntut adanya mekanisme apa pun sebelum mereka membagikan informasi pribadi? Apakah mereka mengharapkan organisasi untuk bereaksi dengan cara tertentu jika terjadi serangan?

Sayangnya, dalam situasi seperti ini, ketika individu tersebut berjuang melawan kanker esofagus stadium IV yang telah dianggap terminal, individu tersebut tidak memiliki banyak pilihan untuk pengobatan. Jadi, uji klinis ini, meskipun berpotensi tidak melindungi informasi pribadinya, mungkin masih menjadi satu-satunya pilihannya. Oleh karena itu, kemampuannya untuk menuntut perlindungan tersebut secara memadai mungkin terbatas karena sifatnya yang wajib.

Apa pun itu, penting bagi individu untuk mengenali jalan dua arah. Jadi, tidak hanya ada kebutuhan bagi individu untuk mendidik diri mereka sendiri tentang perlindungan, tetapi juga ada kebutuhan yang sebanding bagi individu untuk menuntut perlindungan tersebut.

Seperti yang terlihat dalam bab korporasi sebelumnya, korporasi dapat ragu untuk memberikan perlindungan yang memadai atau melaporkan kejadian serangan yang sebenarnya. Jadi, tanpa mekanisme jalan dua arah dan individu yang mengambil inisiatif untuk menuntut perlindungan dan pendidikan tersebut, banyak bisnis atau organisasi akan jauh dari standar yang seharusnya mereka capai saat menyimpan informasi pribadi.

7.5 PERLINDUNGAN INDIVIDU DIMINTA DARI ASURANSI KESEHATAN

Mari kita bahas sebuah contoh. Pada suatu ketika, saya mengalami cedera dan pergi ke dokter. Setelah kunjungan itu, saya memberi mereka kartu kredit untuk membayar layanan yang diberikan. Saya memberikan semua informasi yang ditanyakan tentang catatan kesehatan dan catatan sosial saya. Saya menjawab setiap pertanyaan dengan itikad baik karena saya berasumsi pertanyaan itu diajukan dengan itikad baik.

Penting bagi dokter untuk mengakses informasi tersebut, sehingga ia dapat merawat saya dengan lebih baik. Jadi, menjawab pertanyaan dengan itikad baik bukan hanya demi kepentingan terbaik saya, tetapi juga demi kepentingan terbaiknya untuk mengajukan pertanyaan dengan itikad baik. Ini akan memungkinkan kunjungan menjadi lebih efektif dan lebih bermanfaat bagi kesehatan saya.

Saat saya menjawab pertanyaan, dokter memasukkan semua informasi secara elektronik, baik di komputer desktop, tablet, atau laptop. Pertanyaannya kemudian menjadi—ke mana informasi ini disimpan? Apakah riwayat medis pribadi dan rahasia saya dilindungi? Apakah informasi ini disimpan dalam brankas yang hanya dapat diakses dengan kata sandi? Atau, apakah catatan tersebut tidak sepenuhnya dilindungi? Apakah informasi itu sekarang tersedia bagi siapa saja yang memiliki komputer dan memiliki kemampuan untuk meretas?

Pertimbangkan, ketika kita menjawab pertanyaan dokter dengan itikad baik, kita berasumsi bahwa mereka bertanya karena mereka membutuhkan jawaban. Kita berasumsi bahwa informasi itu penting untuk kemampuan mengobati kita dengan sukses. Jarang sekali terpikir oleh kita untuk mempertimbangkan di mana informasi itu akan berakhir. Catatan medis rahasia berpotensi menjadi hal yang mudah, karena produksi catatan itu penting dalam bidang medis dan menjadi peluang untuk peretasan.

Namun, mari kita berhenti sejenak dan mengevaluasi apa yang akan terjadi jika saya tidak menjawab pertanyaan itu dengan itikad baik. Jika saya berhenti sejenak dan menolak untuk menjawab, dokter akan semakin sulit untuk merawat saya secara efektif. Pada saat itu, dokter akan memiliki riwayat yang tidak lengkap, yang secara signifikan menghambat kemampuan profesionalnya untuk memberikan bantuan medis yang diperlukan.

Jadi, ada kerumitan dalam tidak menjawab pertanyaan. Dengan tidak menjawab pertanyaan, untuk menghindari catatan dipublikasikan, hal itu berpotensi menyebabkan kerugian dalam masalah medis saat ini. Di satu sisi, ada ekspektasi masyarakat bahwa ketika kita pergi ke dokter untuk meminta bantuan, pertanyaan-pertanyaan tertentu akan diajukan, dan kita harus menjawabnya agar mereka dapat menangani kita dengan lebih efisien dan efektif.

Informasi ini, mau tidak mau, dimasukkan ke dalam perangkat elektronik dan disimpan

seperti itu. Jadi, bagaimana jika Anda menyembunyikan sesuatu? Bagaimana jika ada sesuatu dalam riwayat pribadi Anda yang tidak ingin Anda bagikan dengan orang lain? Bagaimana jika Anda yakin bahwa informasi yang diberikan dalam pertanyaan dokter akan menjadi korban peretasan dunia maya? Apakah itu berarti, sebagai individu yang takut akan potensi serangan dunia maya, Anda tidak boleh menuruti pertanyaan dokter? Jawabannya mungkin ya.

Namun, itu tidak terlalu realistis. Dalam konteks cara kita berbagi informasi, kenyataannya adalah kita cukup sering membuat diri kita rentan. Dan dengan melakukan itu, kita berharap informasi kita dilindungi.

Kenyataannya adalah bahwa informasi kemungkinan besar tidak akan pernah sepenuhnya dilindungi. Informasi yang kita anggap pribadi dan rahasia kemungkinan besar tidak dilindungi sejauh yang kita inginkan. Pertanyaannya kemudian adalah, bagaimana kita dapat melindungi diri kita sendiri sebagai individu secara lebih efektif? Dan dengan demikian, apa saja solusi yang dapat diambil jika terjadi serangan siber?

Seperti yang terlihat dalam pembahasan di atas, sering kali kita diwajibkan untuk menanggapi pertanyaan pribadi, untuk meningkatkan kesehatan fisik kita, dan dengan demikian, kita menempatkan informasi kita pada risiko serangan siber. Namun, seperti yang disebutkan di atas, kebutuhan untuk mengungkapkan informasi penting kepada penyedia layanan kesehatan kita sering kali lebih besar daripada rasa takut informasi kita akan terekspos. Namun, pertimbangkan hal berikut, bagaimana jika informasi pribadi Anda terekspos ke atasan Anda saat ini? Bayangkan Anda bekerja di posisi buruh kasar.

Posisi ini mengharuskan Anda untuk sering mengangkat barang dengan berat lebih dari 75 pon atau lebih. Jadi, ada persyaratan tinggi, berat, dan kebugaran yang tepat untuk memenuhi syarat untuk pekerjaan tersebut. Anda telah dengan mudah memenuhi persyaratan ini. Anda memiliki tinggi dan berat yang dibutuhkan dan menjaga diri Anda dalam kondisi fisik yang sangat baik. Oleh karena itu, Anda telah mendapatkan pekerjaan tersebut, dan Anda adalah karyawan yang luar biasa.

Sekarang, bayangkan, meskipun Anda saat ini mampu memenuhi persyaratan tinggi, berat, dan kebugaran, ada saat di masa lalu Anda tidak mampu. Bayangkan Anda berhadapan dengan penyakit yang menghambat kemampuan kebugaran Anda dan ada sesuatu yang mengancam untuk kambuh lagi. Jika pemberi kerja Anda mengetahui informasi ini, Anda mungkin akan didiskualifikasi dari pekerjaan Anda, hanya karena pemberi kerja takut Anda akan potensi kambuh.

Oleh karena itu, Anda telah memilih, karena itu adalah hak Anda, untuk merahasiakan informasi pribadi Anda. Dan, karena Anda lulus tes tinggi, berat, dan kebugaran dengan nilai yang memuaskan, Anda sekarang bekerja dengan senang hati di posisi pekerja kasar ini.

Namun, pada hari ini, kantor dokter kesehatan Anda sebelumnya diretas. Seorang penyerang siber, yang kemudian mengakses semua catatan medis pribadi yang ada di arsip, menembus sistem komputer. Penyerang ini menerbitkan informasi medis di situs yang mudah diakses, yang memungkinkan semua orang untuk melihat catatan medis pribadi. Informasi medis tidak hanya diunggah, tetapi juga secara langsung dikaitkan dengan individu yang bersangkutan, sehingga sangat spesifik mengenai catatan milik siapa.

Pada titik ini, pemberi kerja menyadari pelanggaran tersebut dan catatan publik yang terlihat, dan melanjutkan untuk menentukan apakah ada karyawannya yang terkena dampak serangan siber. Pemberi kerja individu dalam posisi pekerja kasar sekarang menyadari bahwa karyawannya, meskipun lulus persyaratan tinggi, berat, dan kebugaran dengan nilai yang memuaskan, telah berhadapan dengan penyakit yang mungkin kambuh, dan penyakit yang dapat dipicu oleh mengangkat barang berat. Oleh karena itu, untuk menghindari cedera atau tanggung jawab di masa mendatang bagi karyawan, pemberi kerja segera memecat karyawan tersebut.

Sekarang, mengingat bahwa karyawan tersebut tidak melakukan kesalahan dan seharusnya memenuhi syarat untuk posisi tersebut, bagaimana karyawan tersebut dapat bertindak berbeda untuk menghindari hasil ini? Jika karyawan tersebut tidak berterus terang kepada dokternya sejak awal, ia mungkin tidak akan pernah pulih dari penyakitnya. Apakah ia menyembunyikan informasi karena takut dipecat dari pemberi kerja di masa mendatang? Kemungkinan besar penyakitnya saat ini akan berlanjut untuk waktu yang lebih lama. Oleh karena itu, tampaknya jelas bahwa menyembunyikan informasi bukanlah jawabannya.

Pertanyaannya kemudian beralih ke apakah pemberi kerja dapat secara hukum memecat individu tersebut karena ia mengetahui informasi dari catatan yang dilanggar. Tampaknya tidak adil jika pemberi kerja dapat mengakses informasi tersebut, meskipun mereka bukanlah orang yang awalnya melakukan serangan siber dan memposting dokumen tersebut. Pembahasan ini muncul di lain waktu dalam menentukan tanggung jawab bagi mereka yang mengakses informasi yang secara tidak sah diambil dari organisasi yang sah.

7.6 REAKSI DAN UPAYA HUKUM TERHADAP SERANGAN SIBER

Pertimbangkan hal berikut: Jika rekening bank pribadi Anda diretas, hal pertama yang Anda lakukan adalah menghubungi bank dan mengklarifikasi pembelian mana yang menjadi milik Anda, mana yang bukan, dan uang yang dicuri akan dikembalikan kepada Anda. Jarang sekali kita bertanya, apakah ada orang yang dapat saya tuntut? Ini menimbulkan pertanyaan yang menarik. Siapa yang akan Anda tuntut? Bank? Perusahaan kartu kredit? Bagi keduanya, jawabannya tampaknya tidak. Baik bank maupun perusahaan kartu kredit telah memasang perlindungan untuk melindungi diri mereka dari individu tersebut.

Jadi, dapatkah Anda menuntut individu yang menyebabkan pelanggaran? Apakah ada hukuman terhadap peretas siber? Secara potensial, jika penegak hukum dan perusahaan bekerja sama, dapat ada hukuman. Ini terkait kembali dengan bab-bab sebelumnya di mana kita mempertimbangkan tanggung jawab dan kompleksitas penegakan hukum dan serangan siber, serta perusahaan dan serangan siber. Sangat penting bagi keduanya untuk berinteraksi. Dengan demikian, identifikasi peretas siber menjadi lebih mudah. Namun, kemungkinan besar tidak ada yang akan dituntut, karena identitas peretas dilindungi melalui berbagai firewall. Jadi, solusinya bukan gugatan hukum, melainkan sekadar mengganti kerugian kita.

Sekarang, ambil contoh, informasi Anda diretas, dan orang lain menyebarkan informasi itu. Dapatkah penyebar dituntut dalam gugatan perdata? Argumennya adalah ya; jika Anda dapat mengidentifikasi siapa yang benar-benar telah menyebabkan kerugian bagi Anda, hal itu

layak secara hukum. Namun, apakah hal itu layak secara realistis? Saat ini, jawabannya kemungkinan besar tidak. Energi yang dibutuhkan untuk mengidentifikasi peretas, atau penyebar, adalah sesuatu yang tidak dapat dilakukan oleh rata-rata individu dengan sumber daya, waktu, atau pengetahuan.

Untuk menekankan, penyebar informasi yang diretas sama jahatnya dengan individu yang meretas. Keduanya menyebabkan kerugian bagi individu. Sangat penting untuk tidak meremehkan kerugian, khususnya dalam konteks yang telah kita bicarakan, dari catatan kesehatan.

Perlindungan Individu

Apa insentif untuk perlindungan? Bagaimana kita mengembangkan perlindungan yang lebih efektif? Beberapa panduan diberikan pada Gambar 7.2.

- *Buat kata sandi baru dan inovatif secara berkala*
- *Ubah kata sandi Anda sesering mungkin*
- *Jangan bagikan kata sandi Anda dengan orang lain*
- *Jika ditulis atau direkam, hancurkan kertas yang digunakan untuk mencatatnya atau simpan di tempat yang aman*
- *Lebih tegas terhadap perusahaan atau bisnis yang Anda beri informasi tertentu*
- *Cerdaslah dalam cara Anda membagikan informasi*

Gambar 7.2 Pedoman individu.

Terkait dengan poin terakhir, saat membeli barang secara daring, jangan berikan informasi jaminan sosial Anda. Berikan nomor jaminan sosial Anda hanya melalui telepon. Pahami bahwa setelah Anda mencantumkan nomor jaminan sosial secara daring, nomor tersebut akan segera tersedia. Selain itu, sadari kerentanannya. Dalam melakukannya, tegaskan cara untuk melindungi kerentanan tersebut. Dalam mengenali kerentanan, cara terbaik adalah dengan menjadikan masalah tersebut sebagai tindakan diskusi harian dengan teman, keluarga, dan rekan kerja. Pahami kenyataan bahwa kerentanan itu ada. Ancaman dunia maya paling pedih, bukan dalam hal kerugian fisik, tetapi dalam hal kerugian finansial, rasa malu, atau rasa sakit pada barang yang dipublikasikan.

Dalam menjadi lebih sadar dan tanggap, penting bagi individu untuk menyadari bahwa kita semua rentan terhadap serangan dalam banyak hal yang tidak sering dibahas. Lebih jauh, aset prioritas apa pun yang tidak diberi perlindungan yang memadai dapat dianggap rentan. Kuncinya adalah mengenali bahwa informasi rahasia dapat disebarluaskan. Jika Anda ingin menghindari penyebaran, penting untuk memikul tanggung jawab demi perlindungan yang lebih efektif. Seperti yang dinyatakan dalam bab sebelumnya, tanggung jawab berada di tangan perusahaan. Selain itu, individu harus memikul tanggung jawab dan menuntut perlindungan tambahan.

Ada banyak contoh, yang terjadi di dunia ini, mengasumsikan akuntabilitas dan menuntut perlindungan tambahan bukanlah pilihan yang tepat. Banyak pemberi kerja

meminta informasi spesifik saat memulai pekerjaan. Informasi ini dapat berupa nomor jaminan sosial, catatan kesehatan, catatan kriminal, dan dokumen penting lainnya. Seseorang tidak memiliki kemampuan untuk begitu saja menolak akses pemberi kerja ke formulir ini. Dengan begitu, individu tersebut akan kehilangan kesempatan untuk bekerja bagi pemberi kerja.

Pertanyaannya adalah, jika saya ingin bekerja untuk perusahaan tertentu, tetapi saya takut akan kemampuan mereka untuk menjaga kerahasiaan catatan saya, bagaimana saya menuntut perlindungan yang memadai? Apakah menuntut perlindungan tersebut akan membuat saya kehilangan pekerjaan? Bahkan jika perlindungan tersebut dituntut, apakah perusahaan akan menanggapi dan menyediakan perlindungan tersebut? Apakah perlindungan yang mutlak dan memadai seperti itu memang ada?

Secara keseluruhan, semakin sulit bagi seseorang untuk bertanggung jawab secara pribadi. Seperti yang disebutkan sebelumnya dalam perselisihan Apple/FBI, FBI ingin mengakses telepon untuk mendapatkan akses ke informasi pribadi. Informasi ini juga disimpan di Cloud. Ada banyak sekali dokumen yang disimpan di Cloud yang ingin dirahasiakan oleh individu. Dengan demikian, individu tersebut menuntut pertanggungjawaban oleh perusahaan untuk menjaga privasi mereka. Namun, banyak penyerang dunia maya dapat menerobos firewall meskipun mereka telah berusaha sekuat tenaga. Dengan demikian, kesulitan bagi seorang individu muncul karena biaya menuntut perlindungan yang memadai dari perusahaan, ditambah dengan kesadaran bahwa perlindungan yang memadai mungkin tidak ada.

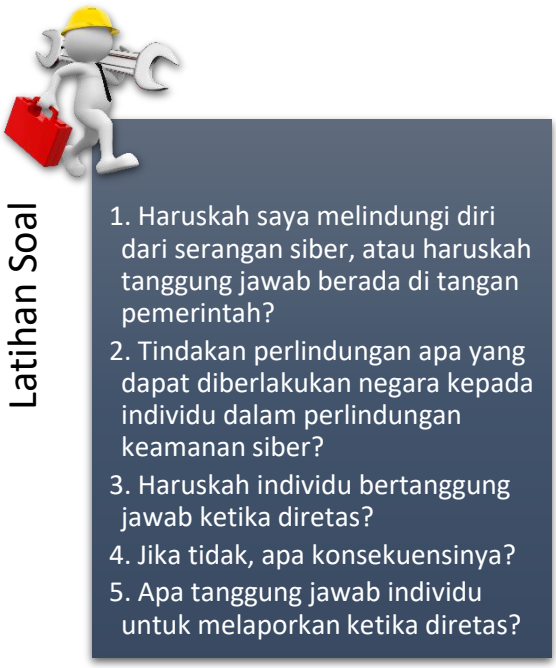
Dengan akuntabilitas pribadi, individu harus berhenti sejenak dan mempertimbangkan situs web tempat mereka mengunduh informasi, atau tempat mereka memberikan informasi. Sangat penting untuk sangat berhati-hati dalam hal informasi yang kita berikan ke Internet. Peretas dunia maya lebih canggih daripada kita, rata-rata individu. Mereka mampu menembus rahasia kita yang kita simpan rapat, sehingga membuat kita rentan. Dalam konteks itu, akan bermanfaat untuk lebih siap melindungi diri kita dari serangan di masa mendatang.

Kita tidak bisa hidup di dunia yang penuh ketakutan untuk menaruh apa pun di Internet. Itu tidak berarti harus 100% curiga sepanjang waktu. Itu hanya membutuhkan kesadaran tambahan tentang serangan di masa mendatang. Dengan demikian, pertanyaan yang diajukan adalah, apa yang akan saya lakukan setelah saya diretas? Responsnya bisa beragam, mulai dari memberikan informasi pribadi lebih sedikit atau memberikan informasi pribadi dengan cara yang berbeda.

Meskipun kita sudah berusaha untuk berhati-hati, banyak orang menjadi korban phishing dan penipuan. Dari orang-orang tersebut, mayoritas adalah orang lanjut usia. Dengan demikian, generasi muda memiliki kewajiban untuk mendidik diri sendiri, anggota keluarga, dan tetangga mereka agar cerdas dalam berinternet. Dengan demikian, pembahasan tentang individu disertai dengan kewajiban untuk berbagi informasi dengan pemahaman bahwa dengan berbagi, kita dapat, baik secara individu maupun kolektif, meminimalkan ancaman yang ditimbulkan oleh peretas dunia maya.

Berikut ini adalah pertanyaan-pertanyaan yang perlu dipertimbangkan dalam meninjau

Bab 7 (Gambar 7.3).



Gambar 7.3 Pertanyaan tinjauan.

BAB 8
PENEGAKAN HUKUM DALAM MENGURANGI KEAMANAN SIBER

8.1 PENDAHULUAN

Bab ini membahas hubungan antara penegakan hukum dan keamanan siber, khususnya bagaimana penegakan hukum dapat bekerja lebih efektif dengan perusahaan, individu, dan negara untuk membantu mereka melindungi diri dari serangan siber. Penekanannya adalah pada apa yang dapat dilakukan penegakan hukum untuk mengurangi keamanan siber atau ancaman siber.

Sebelum membahas pembahasan penegakan hukum, mari kita pertimbangkan terlebih dahulu peran penegakan hukum dalam kaitannya dengan entitas sebelumnya yang telah kita bahas. Dengan perusahaan dan penegakan hukum, ada hubungan yang hidup berdampingan, di mana masing-masing pihak saling bergantung dan membutuhkan kerja sama serta bantuan mereka agar paling efektif. Untuk penegakan hukum, mereka membutuhkan kerja sama perusahaan dalam melaporkan peristiwa siber dan mendokumentasikannya dengan benar.

Selama bertahun-tahun, pertimbangkan bagaimana penegakan hukum dapat ditingkatkan. Dalam memecahkan masalah rumit, seperti serangan siber, terorisme, atau penculikan, mereka dipaksa untuk mengembangkan teknik pemecahan masalah. Hal ini dapat berupa dukungan masyarakat, kemajuan teknologi, atau survei dari pintu ke pintu. Apa pun itu, penegakan hukum telah meningkatkan kemampuan mereka saat mereka mengembangkan pola dan tren tentang cara terbaik untuk menanggapi situasi sulit. Hal yang sama berlaku di ranah siber. Agar penegakan hukum dapat meningkatkan respons mereka terhadap siber, diperlukan kerja sama korporasi untuk membantu mengembangkan respons dan pola guna memerangi serangan siber secara efektif.

Serupa dengan itu, sebelumnya kita telah membahas dampak individu. Penegakan hukum tidak hanya bergantung pada korporasi dalam menggagalkan dan menanggapi serangan siber, tetapi juga pada individu. Sebelum kemajuan teknologi terkini, penegakan hukum semata-mata bergantung pada kecerdasan dan pengamatan manusia untuk memecahkan kejahatan. Diperlukan pembicaraan dengan banyak orang, kerja sama banyak orang, dan ingatan banyak orang. Demikian pula, serangan siber, meskipun mungkin tidak memerlukan kerja sama banyak orang atau ingatan banyak orang, memerlukan kerja sama setidaknya beberapa individu.

Dengan demikian, penegakan hukum merupakan cabang atau langkah terakhir dalam respons serangan siber. Penegakan hukum adalah aspek yang bertindak terakhir, yang pada akhirnya menanggapi situasi yang ada dan mengembangkan mekanisme untuk menghindarinya di masa mendatang. Tidak seperti perusahaan, personel penegak hukum memiliki kewajiban untuk bertindak dengan cara tertentu atau melaporkan kejadian tertentu. Selain itu, tidak diragukan lagi merupakan fakta yang valid bahwa tanpa kerja sama perusahaan, individu, atau entitas lain, penegakan hukum tidak akan seefektif yang seharusnya. Pemahaman ini akan melanjutkan analisis kita di bab selanjutnya, saat kita

menguraikan tanggung jawab penegak hukum.

8.2 KEWAJIBAN DAN TANGGUNG JAWAB PENEGAKAN HUKUM

Pertanyaan pertama yang harus diajukan adalah kewajiban dan tanggung jawab apa yang dimiliki penegak hukum terhadap individu, negara, dan perusahaan? Ini semua berbicara dalam konteks dunia maya. Ini adalah pertanyaan praktis, sekaligus titik penyelidikan filosofis yang luas. Ada banyak cara untuk menjawab pertanyaan ini. Secara historis sebagai sebuah masyarakat, kita mendorong penegak hukum untuk mendidik anak-anak kita tentang kejahatan pengedar narkoba atau tidak masuk ke mobil bersama orang asing. Kita mendorong penegak hukum untuk memperingatkan kita tentang bahaya yang ditimbulkan oleh berbagai penjahat. Mengapa? Karena, kita ingin penegak hukum melindungi kita sebagai individu.

Dengan demikian, pertanyaan tentang kewajiban dan tanggung jawab penegak hukum kemudian menjadi: Apakah penegak hukum memiliki tugas yang sama terhadap ancaman dunia maya yang terus berkembang? Bahkan ketika ancaman dunia maya tidak didefinisikan, tidak jelas dari mana asalnya, bahaya apa yang dapat ditimbulkannya, dan siapa yang pada akhirnya bertanggung jawab? Ini adalah pertanyaan yang rumit dan kontroversial. Namun, ini adalah pertanyaan yang harus didiskusikan, dan diskusi itu akan mendorong langkah ke arah yang benar.

Mengingat ancaman yang ditimbulkan oleh serangan siber, baik itu serangan terhadap perusahaan, negara, atau individu, penegak hukum memang berkewajiban untuk melibatkan ketiga entitas tersebut secara proaktif. Meskipun serangan siber mungkin merupakan ancaman, penegak hukum juga menangani perampokan, pemerkosa berantai, dan ancaman praktis lainnya yang memerlukan perhatian dan sumber daya mereka. Jadi, argumen yang menentang perlindungan terhadap serangan siber adalah bahwa ada banyak masalah praktis tambahan yang harus ditangani terlebih dahulu.

Secara keseluruhan, ada kebutuhan untuk memprioritaskan. Penegakan hukum beroperasi berdasarkan analisis biaya-manfaat dalam menentukan cara menanggapi berbagai kejahatan. Jadi, dengan siber sebagai masalah utama, hal itu mengakibatkan pengalihan perhatian dan uang dari ancaman nyata dan langsung. Pada akhirnya, seperti yang dikatakan banyak orang, hal itu akan mengakibatkan minimnya perlindungan yang diberikan kepada individu dari ancaman nyata dan praktis, sebagai ganti potensi ancaman siber.

Bayangkan Anda sedang berjalan di taman, saat itu sudah larut malam dan hanya ada sedikit orang di sekitar, lalu tiga orang mendatangi dan mengepung Anda. Mereka meminta dompet, kartu identitas, dan barang berharga lainnya yang Anda miliki. Mereka menegaskan bahwa mereka akan melakukan apa pun untuk mendapatkan apa yang mereka inginkan, jadi, Anda akhirnya menuruti permintaan mereka.

Pada saat itu, setelah ketiga orang ini kabur membawa dompet, kartu identitas, dan barang berharga lainnya yang mungkin Anda bawa, apa langkah pertama yang akan Anda ambil? Pada saat itu, kemungkinan besar Anda akan meminta bantuan. Baik polisi yang pertama datang, atau orang terdekat yang pertama datang, biasanya Anda akan menelepon polisi. Alasannya adalah karena polisi terlatih untuk menangani situasi seperti ini dan dapat

beroperasi sedemikian rupa untuk melindungi Anda, mungkin bukan dari pengalaman itu, tetapi dari pengalaman di masa mendatang. Selain itu, polisi mungkin memiliki kemampuan untuk mengambil kembali barang-barang yang dicuri.

Bayangkan sekarang, Anda adalah seorang karyawan perusahaan yang belum berinvestasi dalam perlindungan siber yang memadai. Dalam hal itu, pada dasarnya Anda sedang berjalan di taman, larut malam, sendirian. Selanjutnya, perangkat lunak perusak diterapkan dalam sistem perusahaan Anda, dan informasi tersebut dicuri. Informasi ini melibatkan catatan karyawan, informasi identifikasi, dan informasi rahasia lainnya. Akhirnya, karena kurangnya perlindungan siber yang memadai di perusahaan, mereka secara metaforis menuruti tuntutan pencuri dan kehilangan informasi karyawan Anda.

Pada saat itu, setelah penyerang siber ini melarikan diri dengan catatan karyawan, informasi identifikasi, dan informasi rahasia lainnya, apa langkah pertama yang harus dilakukan? Langkah pertama yang harus dilakukan adalah meminta bantuan. Namun, masalah kritisnya adalah, siapa yang harus Anda hubungi? Apakah polisi diperlengkapi untuk menangani keadaan ini? Apakah pelatihannya memadai? Apakah mereka memiliki kemampuan untuk memulihkan barang-barang yang dicuri? Jika bukan polisi, siapa yang dapat membantu dalam situasi ini? Apakah ada peluang untuk pulih ketika Anda menjadi korban serangan siber? Ini adalah pertanyaan penting yang perlu dipertimbangkan.

8.3 ANCAMAN SIBER

Mari kita telaah pertanyaan kritis lebih lanjut, yaitu, apakah penegak hukum memiliki kewajiban terhadap negara, perusahaan, dan individu dari ancaman nyata yang tidak jelas yang disebut siber? Untuk menjawab pertanyaan tersebut, kita harus mundur sejenak dan mempertimbangkan apakah serangan siber benar-benar menimbulkan ancaman yang kredibel, atau apakah ancaman tersebut dibesar-besarkan? Lebih jauh, apakah ancaman tersebut dibesar-besarkan karena berbagai alasan, baik itu pendanaan untuk lembaga atau isu yang sedang hangat dibicarakan saat ini?

Ada bukti yang jelas tentang serangan siber yang signifikan terhadap perusahaan, yang menunjukkan ancaman nyata dan sah yang ditimbulkan oleh para penyerang siber. Apakah ancaman tersebut akan segera terjadi, seperti seseorang yang bersiap merampok rumah? Ada ancaman yang jelas yang ditimbulkan oleh peretas siber. Pertanyaan selanjutnya, apakah mereka menimbulkan ancaman fisik dalam konteks kerusakan fisik? Jawabannya tampaknya tidak.

Mari kita luangkan waktu sejenak untuk meninjau pertanyaan sebelumnya. Pertanyaannya adalah apakah ancaman siber menimbulkan ancaman fisik dalam konteks kerusakan fisik? Jawaban yang mudah, dan jawaban yang diasumsikan kebanyakan orang, tampaknya tidak. Siber, tidak seperti terorisme tradisional, tidak melibatkan individu yang mencoba menimbulkan rasa sakit fisik. Namun, penting untuk diingat bahwa meskipun ada pemahaman ini, bukan berarti rasa sakit fisik tidak dapat ditimbulkan, sebagai akibat dari serangan siber.

Serangan siber sangat sulit untuk diketahui. Sering kali, perusahaan yang telah

ditembus tidak mendeteksi penetrasi selama berminggu-minggu. Selain itu, serangan siber sangat sulit untuk dilawan, dan sering kali perlindungan siber tidak memadai. Dengan demikian, sentimen takut akan serangan ini, yang mengakibatkan kelemahan yang tampak, atau ketidakmampuan untuk menghentikan penetrasi, meskipun telah mengambil tindakan proaktif, adalah sentimen yang mirip dengan serangan fisik.

Dengan demikian, banyak yang berpendapat bahwa serangan siber tidak memiliki peran fisik dan tidak sama dengan ancaman fisik dalam konteks kerusakan fisik; dapat dikatakan bahwa pembedaan tersebut tidak ada gunanya. Kedua peristiwa tersebut, baik invasi fisik ke rumah seseorang atau invasi siber ke komputer pribadi seseorang, melanggar privasi individu. Kedua peristiwa tersebut mengakibatkan perasaan dilanggar dan rentan, dan keduanya harus dikategorikan dengan cara yang sama.

Namun, ini adalah perbedaan yang penting; potensi kerugian ekonomi yang signifikan sebagai akibat dari serangan siber tidak dapat diminimalkan. Kerentanan individu terhadap peretasan catatan medis pribadi mereka, seperti yang dibahas dalam Bab 6, ada sebagai ancaman nyata dan sah. Kemungkinan serangan terhadap infrastruktur pemerintah merupakan serangan. Apakah mereka menimbulkan ancaman fisik langsung? Kemungkinan tidak. Namun, apakah itu berarti ancaman serangan harus diminimalkan? Sama sekali tidak.

Serangan siber yang berhasil berpotensi menyebabkan kerusakan signifikan pada berbagai sumber: sistem air kota, bandara, dan kontrol lalu lintas udara, atau jaringan elektronik. Semua ini berpotensi menyebabkan kerugian ekonomi yang besar. Ancaman ini tidak dapat diminimalkan. Pertanyaannya selanjutnya adalah, apakah merupakan tanggung jawab penegak hukum untuk secara proaktif menghadapi ancaman siber? Mengingat kecanggihan penyerang siber, mekanisme perlindungan yang ada saat ini berpotensi tidak cukup untuk meminimalkan ancaman.

Menolak ancaman siber tidaklah realistis. Rekomendasi yang diusulkan bagi penegak hukum untuk terlibat secara proaktif sangatlah penting. Akan tetapi, yang lebih penting lagi adalah menemukan jalan tengah. Jalan tengah memerlukan hal-hal berikut. Jalan tengah mengharuskan tiga calon korban—negara, perusahaan, dan individu—untuk terlibat dengan penegak hukum dalam sebuah percakapan. Percakapan ini rumit tetapi akan memaksa penegak hukum untuk memprioritaskan ancaman dan kerentanan, termasuk dunia maya sebagai salah satu ancaman tersebut.

Di atas tercantum tiga calon korban: negara, perusahaan, dan individu. Masing-masing memiliki kemampuan untuk menyimpan dan mengakses informasi penting yang kemungkinan akan ditembus dalam serangan dunia maya. Apakah setiap korban memiliki kewajiban untuk melapor kepada penegak hukum? Apakah penegak hukum memiliki kewajiban untuk menanggapi dan bereaksi terhadap serangan dunia maya dengan cara tertentu kepada setiap korban? Lebih jauh, apakah respons penegak hukum bervariasi tergantung pada korban—khususnya, apakah negara merupakan perusahaan dan individu? Kami akan menggunakan skenario untuk membantu kami menjawab pertanyaan-pertanyaan ini.

Tidak hanya ada kebutuhan untuk memprioritaskan, tetapi juga ada percakapan analisis biaya-manfaat tentang cara terbaik untuk menggunakan sumber daya yang terbatas

dalam hal pendidikan. Pendidikan tersebut melibatkan penanganan dengan pemerintah, perusahaan, dan individu serta bekerja sama dengan penegak hukum untuk secara proaktif mewaspadai ancaman siber.

Hal pertama yang perlu dipertimbangkan, dalam memahami tiga kelompok korban yang terpisah, adalah apakah setiap kelompok memiliki kewajiban yang lebih tinggi untuk melapor kepada penegak hukum dibandingkan dengan kelompok lain. Apakah negara, atau pemerintah, memiliki kewajiban yang lebih tinggi untuk bekerja sama dengan penegak hukum? Argumen ini terdiri dari kewajiban negara untuk melindungi warga negaranya sebagaimana warga negaranya sendiri. Jadi, apakah persyaratan perlindungan tambahan tersebut mengharuskannya untuk melapor lebih cepat, dibandingkan dengan perusahaan atau individu?

Pertimbangkan korban berikut, yaitu perusahaan. Apakah mereka memiliki tanggung jawab yang lebih tinggi untuk melapor kepada penegak hukum? Tanggung jawab yang lebih tinggi ini akan muncul karena kesediaan individu untuk menyimpan informasi di perusahaan. Perusahaan, tidak seperti negara, tidak ada secara keseluruhan untuk melayani individu. Sebaliknya, perusahaan biasanya didirikan dengan tanggung jawab minimum dan tujuan untuk menghasilkan uang.

Namun, dengan pemahaman tersebut, korporasi juga mengakui bahwa individu yang berbisnis dengannya memilih untuk melakukannya. Dan, dengan pilihan tersebut, korporasi berkewajiban untuk melindungi pelanggan mereka. Jadi, apakah mereka, seperti negara, memiliki kewajiban yang lebih tinggi, sebagai korban, untuk melaporkan lebih cepat kepada penegak hukum? Pertimbangkan alternatifnya. Apakah penegak hukum memiliki kewajiban yang lebih rendah kepada korporasi—karena tujuan utamanya bukanlah untuk melindungi konsumennya? Apakah penegak hukum memiliki kewajiban yang lebih tinggi kepada negara karena alasan yang sama—karena tujuan utamanya adalah untuk melayani warganya?

Terakhir, mari kita pertimbangkan korban ketiga, individu. Rekomendasi bagi penegak hukum untuk terlibat secara proaktif mencakup varians paling banyak saat berurusan dengan individu. Tidak seperti korporasi atau negara, individu tidak diturunkan untuk mengikuti kode tertentu. Selain itu, individu biasanya tidak memiliki parameter atau persyaratan tertentu yang harus mereka penuhi agar dapat terus menjadi individu. Sebaliknya, individu membuat keputusan khusus yang dapat, baik atau buruk, memengaruhi keamanan siber mereka.

Dengan demikian, pertanyaan keseluruhannya adalah, bahkan ketika menemukan jalan tengah dengan masing-masing calon korban, apakah ada pendekatan yang dapat diterapkan untuk masing-masing, meskipun ada perbedaan yang sangat besar? Selain itu, apakah kewajiban dari penegak hukum bervariasi tergantung pada entitas? Dan jika demikian, apakah itu tepat? Atau haruskah penegakan hukum berlaku sama untuk setiap entitas, terlepas dari parameter atau tolok ukur yang dipatuhi entitas? Pertanyaan-pertanyaan sulit ini terus tidak terjawab hingga saat ini.

Poin-poin penting yang perlu ditindaklanjuti dalam diskusi dengan penegak hukum diberikan dalam Gambar 8.1.

Untuk menetapkan poin-poin di atas, sangat penting bagi penegak hukum untuk secara

proaktif memberikan edukasi. Petugas penegak hukum harus melatih diri mereka sendiri dalam ranah siber untuk lebih memahami risiko yang ditimbulkan oleh hal tersebut.

1. Prioritaskan sumber daya kita

2. Lakukan diskusi tentang biaya-manfaat mengenai pelatihan publik yang efektif

3. Ungkapkan dan definisikan apa yang efektif dan apa yang tidak efektif dalam hal pelatihan

Gambar 8.1 Poin-poin penegakan hukum.

8.4 PENDIDIKAN PENEGAKAN HUKUM

Berikut ini adalah diskusi yang saya lakukan baru-baru ini dengan seorang pejabat senior penegak hukum yang bertugas melacak pencucian uang canggih melalui dunia maya. Pejabat ini bermaksud sangat baik, karena ia memahami betapa pentingnya baginya untuk terlibat dalam pelacakan pencucian uang untuk tujuan memerangi industri narkoba. Namun, ia juga menegaskan bahwa ia memiliki banyak kewajiban lain. Kewajiban lain ini terdiri dari poin-poin yang tercantum dalam Gambar 8.2.

Jadi, ia tidak memiliki sumber daya untuk terlibat dalam jenis pelacakan yang diperlukan untuk meminimalkan ancaman yang ditimbulkan oleh dunia maya.

Meskipun niat pejabat ini tidak lain adalah yang terbaik, rasa frustrasinya nyata dan didasarkan pada hal berikut. Ada beberapa alasan yang membuat penegak hukum kesulitan dalam menghadapi realitas perlindungan dunia maya, yang diberikan dalam Gambar 8.3.

Secara keseluruhan, pendidikan proaktif dalam pelatihan sangat penting. Selain itu, ada kebutuhan bagi lembaga penegak hukum untuk bekerja sama satu sama lain. Kerja sama ini harus terjadi di tingkat lokal, negara bagian, dan nasional. Penegakan hukum harus terlibat dalam rencana kerja sama yang canggih untuk menanggapi ancaman yang ada dengan lebih memadai.

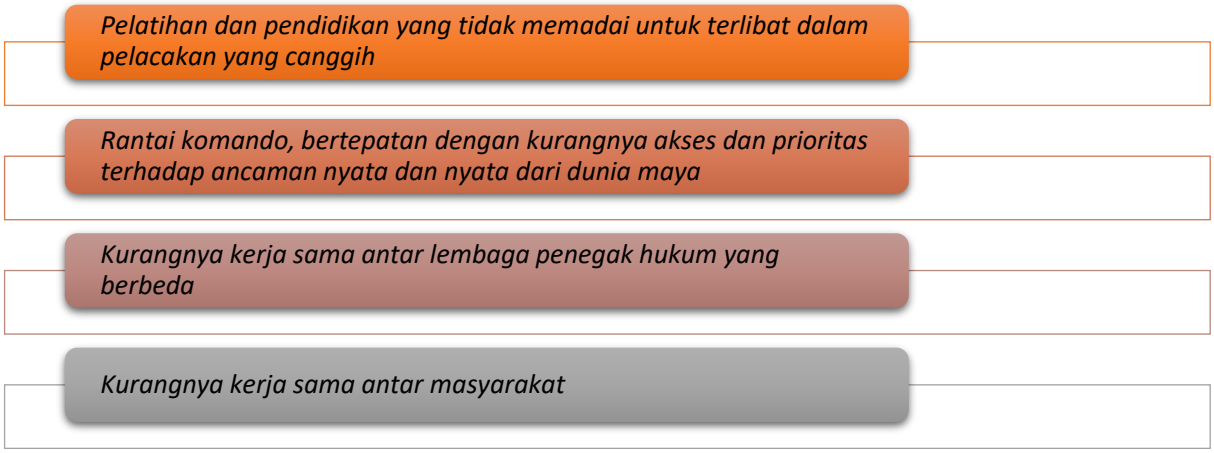
Perlunya kerja sama

Latar belakang saya, khususnya pekerjaan saya dalam operasi kontraterorisme, menunjukkan perlunya kerja sama tersebut. Namun, kerja sama itu tidak selalu menjadi kenyataan. Kenyataannya, kerja sama itu sulit.

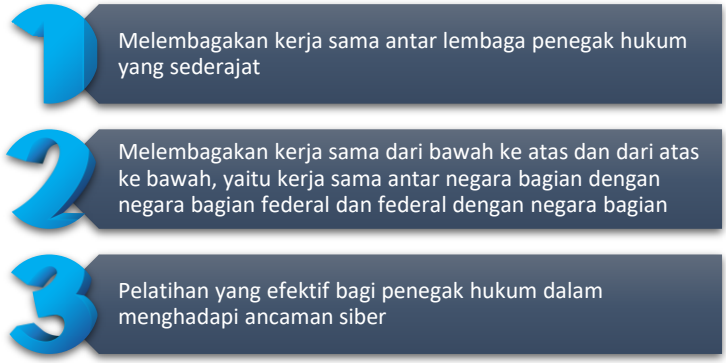
Kewajiban penegakan hukum.

- Menangani pelaku tindak pidana yang saat ini sedang melakukan tindak pidana
- Bekerjasama dengan perbankan
- Membuat metode kerjasama dengan lembaga keuangan lain
- Memberikan edukasi kepada masyarakat tentang potensi ancaman

Gambar 8.2 Kewajiban penegakan hukum.



Gambar 8.3 Realitas penegakan hukum.



Gambar 8.4 Langkah-langkah kerja sama.

Langkah-langkah yang harus diambil untuk kerja sama diberikan pada Gambar 8.4.

Mari kita perhatikan contoh berikut. Beberapa tahun yang lalu, saya mengadakan rapat makan siang dengan lembaga-lembaga negara bagian, lokal, dan federal. Inti dari rapat tersebut adalah untuk berdiskusi tentang berbagi informasi. Bahasa tubuh di ruangan ini jelas. Lembaga-lembaga federal akan sangat ragu untuk berbagi informasi sensitif dengan lembaga-lembaga lokal. Model keraguan ini menunjukkan sesuatu yang berpotensi, yaitu adanya rasa cemburu institusional.

Kurangnya kerja sama sehubungan dengan berbagi intelijen akan menjamin bahwa peretas siber akan terus-menerus berada di atas angin, karena mereka mendapatkan keuntungan dari kurangnya kerja sama. Mendidik masyarakat sangatlah penting. Mendidik masyarakat akan mendorong kerja sama antara lembaga-lembaga lokal, negara bagian, dan federal. Tanpa itu, mustahil untuk menyusun jenis model serangan balik canggih yang diperlukan untuk meminimalkan ancaman yang ditimbulkan oleh siber. Namun, tidak tepat untuk berpendapat bahwa model kerja sama ini menjamin bahwa tidak akan ada lagi serangan siber.

Itu adalah kekeliruan. Namun, untuk meminimalkan ancaman dan kerentanan

serangan siber, kerja sama ini penting. Sebelumnya, saya pernah bersaksi di Kongres tentang isu serupa, yang melibatkan model berbasis kerja sama beberapa tahun lalu. Dalam kesaksian ini, saya melanjutkan argumen bahwa tanpa kerja sama di antara berbagai lembaga, mustahil untuk mengembangkan kontraterorisme yang canggih.

Tingkat kecanggihan ini hanya terjadi jika ada kerja sama menyeluruh di antara tingkat lokal, negara bagian, dan federal. Dalam membicarakan kerja sama dan pendidikan, poin ketiga adalah pelatihan. Penegakan hukum harus melatih dirinya sendiri sehubungan dengan keamanan siber, ancaman yang ditimbulkannya, dan tindakan yang paling efektif untuk menanggapi keamanan siber. Untuk terlibat dalam pelatihan semacam itu, penegak hukum harus berpikir di luar kotak. Ini mengharuskan kita semua, masyarakat dan penegak hukum, untuk mengenakan topi kreatif dan berpikir seperti yang mungkin dipikirkan oleh para penyerang siber.

Seperti yang dibahas di atas, harus ada penekanan pada pembagian informasi intelijen di antara lembaga lokal, negara bagian, dan federal. Tanpa pembagian dan kerja sama tersebut, peretas siber akan terus-menerus mengakali dan menggagalkan perlindungan siber, khususnya karena mereka yang berusaha mencegahnya tidak akan memiliki keterampilan dan keahlian yang dibutuhkan. Pertimbangkan analogi berikut untuk membantu menggambarkan kelemahan yang muncul sebagai akibat dari kurangnya kerja sama.

Bayangkan sebuah sekolah dasar. Agar sekolah dasar dapat berhasil, agar setiap siswa memperoleh kualitas pendidikan yang mereka butuhkan, beberapa lapisan terlibat. Lapisan terbawah, yang bekerja paling dekat dengan siswa, adalah guru. Lapisan ini bertanggung jawab untuk memantau kesulitan di kelas, atau saat-saat penetrasi bagi penyerang dunia maya. Jika satu individu tertentu kesulitan memahami suatu konsep, tugas mereka adalah memastikan mereka mencapai tingkat yang setara dengan teman sebayanya. Selain itu, langkah-langkah tambahan mungkin diperlukan untuk memberi tahu mereka yang lebih tinggi tentang siswa tersebut.

Hal ini mirip dengan titik penetrasi bagi penyerang dunia maya. Selain itu, organisasi atau perusahaan seperti guru. Tugas mereka adalah memantau perusahaan mereka dan memastikan titik penetrasi, siswa yang kesulitan memahami suatu konsep, mendapat perhatian tambahan.

Selain itu, merupakan kewajiban mereka untuk melaporkan titik penetrasi tersebut kepada yang lebih tinggi, yang berarti lembaga lokal, negara bagian, atau federal, atau penegak hukum. Tanpa ketekunan dan pelaporan perusahaan, lembaga atau penegak hukum tidak akan memiliki cara untuk mengetahui titik penetrasi tertentu tersebut. Selain itu, tanpa guru yang merekomendasikan bantuan tambahan untuk siswa tertentu, akan sangat sulit bagi kepala sekolah untuk menyadari siapa yang membutuhkan bantuan tambahan.

Di luar guru, Anda memiliki sistem administrasi sekolah, khususnya kepala sekolah dan wakil kepala sekolah. Peran ini setara dengan lembaga, baik di tingkat lokal, negara bagian, maupun federal. Administrasi, kepala sekolah, dan wakil kepala sekolah memiliki tugas untuk memantau sekolah, memastikan perawatan terbaik bagi siswa, dan menjaga lingkungan yang aman.

Demikian pula, lembaga memiliki kewajiban kepada perusahaan yang ada di dalamnya, di tingkat lokal, negara bagian, dan federal, untuk melakukan hal yang sama. Mereka harus memantau perusahaan atau organisasi, memastikan mereka bertindak dengan cara terbaik, dan menjaga lingkungan kerja sama tempat mereka dapat menjalankan bisnis mereka. Jika seorang guru tidak melapor kepada administrasi, mereka tidak dapat melayani seefektif mungkin. Selain itu, jika administrasi tidak bersedia mendukung guru ketika kebutuhannya diketahui, guru akan cenderung tidak bekerja sama atau bergantung pada layanan administrasi.

Hal ini serupa dengan serangan siber. Jika sebuah perusahaan atau organisasi melaporkan titik-titik penetrasi ke lembaga lokal, negara bagian, dan federal, mereka melakukannya dengan pemahaman bahwa lembaga-lembaga tersebut akan bekerja sama dan membantu melindungi dari penyerang siber. Selain itu, lembaga-lembaga tersebut mengandalkan perusahaan atau organisasi untuk melaporkan titik-titik penetrasi tersebut, sehingga mereka dapat memenuhi kebutuhan mereka dengan lebih baik. Tingkat terakhir yang perlu dipertimbangkan adalah konselor bimbingan di sekolah dasar. Peran konselor bimbingan mencakup banyak tugas. Secara khusus, seorang konselor bimbingan dimaksudkan untuk membantu para guru dalam kemampuan mereka untuk memastikan kualitas perawatan tertinggi bagi siswa.

Selain itu, konselor bimbingan membantu administrasi, khususnya kepala sekolah dan wakil kepala sekolah, dalam memastikan bahwa tindakan yang mereka ambil tepat dan efektif. Konselor bimbingan berfungsi sebagai jembatan antara keduanya, dengan tujuan akhir untuk mengembangkan cara yang paling efektif untuk melayani anak-anak. Penegakan hukum menjalankan peran konselor bimbingan. Secara khusus, penegakan hukum dimaksudkan untuk menjadi jembatan antara perusahaan dan organisasi serta lembaga lokal, negara bagian, dan federal, dan membantu semua pihak untuk mengembangkan cara yang paling efektif untuk melawan penyerang dunia maya.

Penegakan hukum membantu perusahaan dalam kemampuan mereka untuk menggagalkan serangan di masa mendatang dengan mengembangkan pelatihan untuk mengenali titik penetrasi yang umum di antara perusahaan dan mengembangkan cara untuk melawannya. Selain itu, penegakan hukum membantu lembaga dalam memastikan bahwa mereka menanggapi secara khusus kebutuhan perusahaan dan menghabiskan waktu dan uang untuk hal-hal yang benar-benar penting.

Secara keseluruhan, setiap peran di sekolah dasar memainkan peran penting. Guru, yang paling dekat dengan individu, memainkan peran untuk mengenali kebutuhan dan menanggapinya. Demikian pula, perusahaan atau organisasi yang paling dekat dengan titik penetrasi memainkan peran untuk mengisi lubang saat menemukannya.

Pemerintah, atau lembaga lokal, negara bagian, dan federal, memainkan peran penting dalam mendukung guru dalam pencegahan mereka terhadap titik penetrasi. Tugas mereka adalah bekerja sama dan membantu sebaik mungkin, memanfaatkan keahlian para guru atau perusahaan. Terakhir, konselor pembimbing menjembatani kesenjangan tersebut. Secara khusus, konselor membantu mengembangkan dan menerapkan mekanisme yang paling efektif

untuk melayani anak-anak.

Demikian pula, penegak hukum mengembangkan pelatihan dan mekanisme yang diperlukan untuk menggagalkan serangan siber di masa mendatang. Selain itu, penegak hukum membuat dokumentasi serangan siber di masa lalu, dengan harapan dapat mengenali titik penetrasi sebelumnya dan mencegah kesamaan di masa mendatang di antara perusahaan dan organisasi.

8.5 PELATIHAN PENEGAKAN HUKUM

Penegak hukum harus secara proaktif terlibat dalam kerja sama yang canggih, konsisten, dan terlembaga dengan lembaga-lembaga di seluruh dunia. Individu yang melakukan serangan siber berada di suatu tempat di dunia dan menimbulkan ancaman.

Jadi, kerja sama semacam itu harus meluas ke luar negara kita. Akan keliru jika mengatakan hal ini sudah terjadi atau belum terjadi. Kerja sama ini tidak terjadi sejauh yang diperlukan karena jenis ancaman yang harus dilindungi bersifat internasional. Pikirkan kembali mantan pejabat penegak hukum yang menangani pencucian uang. Agar pejabat tersebut dapat lebih efektif terlibat dalam menanggapi dan meminimalkan ancaman yang ditimbulkan, mereka perlu memperluas cakupan, karena ini jelas merupakan masalah internasional.

Berpegang pada pejabat penegak hukum yang menangani pencucian uang, individu tersebut tidak hanya ditolak kerja samanya dari lembaga-lembaga di atasnya, dalam hal tingkat federal dan negara bagian, ia juga tidak memiliki kerja sama penuh secara internasional. Agar individu tersebut dapat meminimalkan ancaman secara efektif, diperlukan kerja sama antara pejabat internasional, pelatihan, dan pendidikan. Secara keseluruhan, dunia maya menimbulkan ancaman yang sangat besar sehingga jika kita tidak terlibat dalam kerja sama tiga bagian ini, lokal, negara bagian, dan federal, serta pelatihan dan pendidikan, maka penegakan hukum akan sangat terhambat.

Pikirkan sejenak, Anda menerima surat melalui pos yang menyatakan bahwa Anda menunggak beberapa kartu kredit, dan Anda harus membayar dalam waktu 90 hari. Hal pertama yang perlu dipertimbangkan adalah, apa saja kartu kredit ini? Untuk contoh ini, asumsikan semua kartu kredit dibuka tanpa sepengetahuan Anda karena pelanggaran dunia maya yang mengakibatkan nomor jaminan sosial Anda dicuri. Anda sekarang menjadi korban pencurian identitas. Namun, kepada siapa Anda melapor ketika Anda menjadi korban pencurian identitas? Anda dapat menghubungi polisi setempat.

Namun, bagaimana jika pencurian terjadi? Ini menjadikannya masalah lintas yurisdiksi. Apakah keragaman yurisdiksi mengubah masalah ini menjadi masalah federal? Secara keseluruhan, apakah pelanggaran yang mengakibatkan pencurian identitas merupakan pelanggaran yang sedang ditangani? Selain itu, jika pelanggaran tersebut ditangani oleh satu lembaga penegak hukum, apakah ada pelaporan yang diperlukan antar lembaga untuk memperbaiki masalah tersebut dengan sebaik-baiknya? Selain itu, apakah lembaga tersebut telah mendapatkan pelatihan yang memadai tentang cara menanggapi ancaman siber? Apakah lembaga tersebut telah mendapatkan pelatihan yang memadai tentang cara mengatasi ancaman siber? Tanpa pelatihan tersebut, beralih ke penegak hukum jika terjadi serangan siber

akan tampak sia-sia.

8.6 PENTINGNYA PENEGAKAN HUKUM DENGAN SIBER

Seperti yang telah dikatakan di awal, kita telah mengajarkan anak-anak kita, dan mendorong penegak hukum untuk mengajarkan anak-anak kita, untuk tidak naik mobil bersama orang asing. Mengapa? Karena kita tahu bahwa ketika beberapa anak naik mobil bersama orang asing, kengerian yang tak terbayangkan telah menimpa anak-anak tersebut. Sama seperti kita telah melatih anak-anak kita untuk tidak naik mobil bersama orang asing, penting untuk melatih individu untuk menjaga keamanan informasi pribadi mereka. Saat kita daring, jika seseorang meminta informasi jaminan sosial Anda, jangan berikan kepada mereka. Tanggung jawab pendidikan ini dimulai dengan pelatihan penegakan hukum kepada masyarakat.

Tanggung jawab ini berlaku dua arah: penegak hukum harus mendidik, dan perusahaan harus maju dengan contoh-contoh serangan siber. Dalam Bab 7, pembahasan berkisar seputar perusahaan. Di dalamnya, kita membahas tanggung jawab perusahaan untuk maju dan memberi tahu penegak hukum setelah diretas.

Perusahaan harus maju ke penegak hukum untuk mengidentifikasi di mana mereka rentan dan tindakan apa yang dapat diambil untuk meminimalkan ancaman di masa mendatang. Tanpa langkah ini, tanpa perusahaan maju dan berbagi informasi tersebut, tidak mungkin penegak hukum dapat secara efektif memulai proses pembuatan tindakan anti-keamanan siber yang efektif. Dengan demikian, beban berada di pundak perusahaan untuk maju dan maju.

CONTOH PERUSAHAAN

Mari kita pertimbangkan sebuah contoh. Katakanlah Perusahaan X telah diretas. Setelah diretas, Perusahaan X mendatangi kepala polisi setempat, atau departemen luar negeri, atau Departemen Keamanan Dalam Negeri dan melaporkan insiden tersebut.

Agar percakapan itu efektif, penegak hukum harus memiliki keterampilan yang memadai untuk menangani insiden tersebut. Dalam menangani insiden tersebut, penegak hukum perlu bekerja sama dengan tim TI Korporasi X untuk memahami di mana serangan terjadi, berbagai titik kerentanan, dan langkah terbaik untuk meminimalkan ancaman.

Korporasi ragu untuk maju, karena akan memengaruhi model ekonomi, persepsi pemegang saham, dan persepsi konsumen mereka. Namun, korporasi yang menutup mata bukanlah solusi. Korporasi memiliki kewajiban untuk melapor kepada penegak hukum. Ada undang-undang yang diusulkan yang mewajibkan korporasi untuk melaporkan peretasan, dan itu adalah langkah ke arah yang benar. Korporasi tidak perlu takut akan ancaman dampak ekonomi atau kekecewaan pemegang saham. Dampak jangka panjang dari tidak melaporkan, tidak memahami titik kerentanan, dan tidak memahami cara meminimalkan ancaman di masa mendatang jauh lebih besar daripada kekecewaan ekonomi atau pemegang saham jangka pendek.

Namun, agar percakapan ini dapat dilakukan, penegak hukum harus memiliki keterampilan, pelatihan, dan sumber daya. Ada titik kerentanan dalam korporasi, dan penegak

hukum harus memahami korporasi sebelum mereka dapat memahami titik-titik tersebut. Untuk menentukan titik-titik tersebut, penegak hukum harus bekerja sama dengan tim IT perusahaan untuk menentukan titik-titik tersebut. Ini adalah satu-satunya cara agar penegak hukum dapat secara efektif meminimalkan ancaman yang akan datang.

Kembali ke contoh kita, setelah Korporasi X datang ke penegak hukum, penegak hukum dapat mulai mengenali pola serangan siber. Penegak hukum dapat mengenali, tidak hanya pola terhadap Korporasi X, tetapi mungkin pola pada korporasi dengan ukuran yang sama di lokasi berbeda yang diserang dengan cara yang sama. Ini memulai proses pembuatan pola. Dalam mengembangkan pola tersebut, dapat ditentukan apakah serangan tersebut disebabkan oleh peretas yang sama. Satu-satunya cara untuk melakukannya adalah ketika Korporasi X memberi tahu penegak hukum setempat. Dengan demikian, model kerja sama adalah antara korporasi dan penegak hukum, serta penegak hukum terhadap korporasi.

Kesimpulan

Secara keseluruhan, serangan siber merupakan bentuk terorisme nonkonvensional yang benar-benar memerlukan tindakan nonkonvensional, yang memerlukan perlunya kerja sama. Poin kedua adalah persyaratan untuk pelatihan. Poin ketiga bertumpu pada tanggung jawab untuk melatih dan mendidik. Dengan demikian, ini adalah pendekatan tiga kali lipat: kerja sama, pelatihan, dan pendidikan. Dapat sepenuhnya diakui bahwa pendekatan ini tidak murah. Hal ini menguras sumber daya yang ada dan memerlukan diskusi tentang memprioritaskan kembali sumber daya.

Jika memang ancaman siber menimbulkan bahaya yang disarankan, maka perlu dipertimbangkan seberapa rentannya kita terhadap serangan siber agar dapat memiliki model yang lebih canggih dan kreatif. Secara keseluruhan, penegak hukum perlu mendatangi perusahaan, pemimpin negara, dan individu, serta menawarkan bantuan. Penegak hukum perlu mengartikulasikan kembali model penegakan hukum yang ada.

Pertanyaan yang perlu dipertimbangkan dalam meninjau Bab 8 diberikan dalam Gambar 8.5.

Latihan Soal

1. Apakah penegak hukum memiliki kewajiban untuk mendidik masyarakat?
2. Apakah penegak hukum memiliki kewajiban untuk menghabiskan sumber daya yang signifikan untuk keamanan siber?
3. Apa kewajiban penegak hukum untuk bekerja sama dengan lembaga penegak hukum lainnya?
4. Apa kewajiban lembaga penegak hukum federal, negara bagian, dan lokal untuk bekerja sama satu sama lain?
5. Apa kewajiban penegak hukum untuk memberi tahu masyarakat tentang serangan siber atau potensi serangan siber?

Gambar 8.5 Pertanyaan tinjauan.

BAB 9
KEAMANAN SIBER DI MASA DEPAN

9.1 PENDAHULUAN

Bab ini menekankan keamanan siber di masa depan, besarnya risiko, dan langkah-langkah yang harus diambil untuk mengurangi risiko tersebut. Penggunaan berbagai skenario akan membuat percakapan lebih realistis dan tidak terlalu teoritis. Hal ini dilakukan untuk membantu pembaca memahami keamanan siber pada tingkat yang paling praktis.

SKENARIO A

Individu A menerima panggilan telepon. Di ujung telepon yang lain, seseorang mengaku dari sebuah lembaga yang meminta Anda untuk memberikan konfirmasi identitas, alamat, atau nama belakang. Orang di telepon yang lain ini mengaku dari lembaga kartu kredit atau lembaga keuangan yang perlu melakukan pemeriksaan latar belakang terhadap Anda.

Tahun lalu, saya menerima telepon dari seseorang di Internal Revenue Service (IRS) yang mengklaim bahwa saya memiliki tunggakan pajak. Orang ini mengancam bahwa jika saya tidak membayar tunggakan pajak ini pada tanggal tertentu, saya akan melanggar hukum. Untuk membayar tunggakan pajak tersebut, orang tersebut meminta informasi kartu kredit saya. Saya paham bahwa panggilan itu penipuan dan segera menutup telepon. Namun, itu mungkin bukan reaksi pertama orang lain. Sebagian orang mungkin langsung mengambil kesimpulan dan berasumsi bahwa mereka telah melakukan kesalahan.

Biasanya, setelah orang tersebut menjauh dari situasi tersebut, mereka dapat mengenalinya sebagai penipuan. Namun, tidak semua orang dapat memiliki pandangan ke depan seperti itu. Statistik dengan jelas menunjukkan bahwa banyak sekali orang Amerika yang menjadi korban penipuan seperti skenario di atas. Untuk mengatasi situasi tersebut, dibutuhkan biaya yang sangat besar.

Ini berarti para peretas tidak hanya berhasil, mereka juga membebankan biaya yang sangat besar pada masyarakat kita. Para penyerang dunia maya dapat meretas sistem kita, menerima nomor telepon, dan membebankan biaya yang sangat besar pada masyarakat kita.

Mari kita kembali ke Skenario A. Hal pertama yang harus dilakukan orang tersebut adalah memutus panggilan. Atau bahkan mengambil langkah lebih jauh, dan tidak menjawab panggilan. Namun jika Anda menjawab, jangan berikan nomor jaminan sosial Anda atau informasi apa pun, dan cukup akhiri panggilan.

SKENARIO B

Individu B menerima panggilan telepon. Penelepon mengaku dari kantor polisi. Orang ini mengatakan jika Individu B tidak membayar sejumlah uang tertentu, mereka akan ditangkap atau rumahnya akan digeledah. Hal pertama yang harus dilakukan setelah panggilan selesai adalah memberi tahu lembaga penegak hukum setempat bahwa penyerang siber tersebut mengaku sebagai pelaku. Anda harus melaporkan percakapan yang merupakan penipuan.

Selain itu, jika nomor telepon yang digunakan adalah nomor kantor polisi yang

sebenarnya, bukan hanya nama yang digunakan, tetapi sistem mereka juga telah diretas. Jadi, Anda harus memberi tahu kantor polisi terkait. Kemudian, tanggung jawab jatuh kepada penegak hukum. Pertanyaannya adalah, apa yang harus dilakukan penegak hukum dengan informasi tersebut?

Penting bagi penegak hukum untuk melakukan hal berikut. Pertama, buat mekanisme yang memungkinkan mereka memberi tahu publik. Informasi ini dapat diperoleh melalui stasiun radio, stasiun televisi, posting di beranda mereka, atau cara lain. Kedua, beri tahu lembaga lain bahwa nomor mereka telah diretas. Ketiga, beri tahu FBI bahwa nomor mereka telah diretas.

Upaya ini kembali ke Bab 7, yang melibatkan penentuan prioritas sumber daya dan analisis biaya-manfaat. Terkait dengan Skenario B, dengan penipuan polisi, mari kita melangkah lebih jauh dalam langkah-langkah yang harus diambil. Bayangkan, setelah Anda menerima panggilan, Anda melaporkannya ke kantor polisi setempat. Anda menelepon operator, dan respons sederhana operator adalah, "terima kasih banyak, kami mengetahui situasinya, terima kasih." Itu adalah respons yang tidak memadai.

Respons yang lebih tepat adalah operator mendapatkan informasi sebanyak mungkin dari individu tersebut dalam upaya membuat gabungan jenis panggilan yang dilakukan, informasi yang diminta sehingga mereka dapat membuat profil. Dalam membuat profil peretas secara aktif, penegak hukum mengambil langkah-langkah awal yang penting untuk mengatasi situasi tersebut.

Mari kita kembali ke Skenario A. Individu A menerima panggilan telepon dari IRS. Asumsi atau reaksi awal, yaitu bahwa mereka telah melakukan kesalahan, tidaklah tepat. Penting untuk mengubah pola pikir dari rasa takut melakukan kesalahan menjadi asumsi bahwa penelepon adalah orang jahat, orang yang melanggar hak Individu A untuk mengumpulkan informasi. Respons individu tersebut harus jauh lebih agresif. Responsnya harus segera, yaitu memutus panggilan, memberi tahu aparat penegak hukum, dan memercayai mereka untuk secara proaktif bekerja sama dengan aparat penegak hukum lainnya.

SKENARIO C

Skenario berikutnya akan membahas berbagai kelompok yang terkena dampak siber, termasuk perusahaan dan pemerintah. Untuk skenario ini, pertimbangkan sebuah maskapai penerbangan yang telah diretas. Kemungkinan konsekuensi dari peretasan pesawat terbang, atau menara kontrol udara, sangat besar. Ini adalah skenario serupa yang ditemukan dalam film populer yang dibintangi Bruce Willis, Live Free or Die Hard. Jika sebuah maskapai penerbangan telah diretas, ada cara untuk memanipulasi maskapai penerbangan, pesawat, atau sistem kontrol udara. Dengan peretasan itu, ada dua kelompok berbeda yang terkena dampak negatif.

Kelompok yang terkena dampak pertama adalah perusahaan, khususnya maskapai penerbangan. Kelompok yang terkena dampak kedua adalah pemerintah, khususnya Asosiasi Penerbangan Federal dan menara kontrol lalu lintas udara. Dengan demikian, analisis ini memerlukan diskusi dari berbagai perspektif. Dalam analisis tersebut, penekanannya kembali

ke kerja sama. Sangat penting bahwa kedua kelompok yang terkena dampak, maskapai penerbangan dan pemerintah, bekerja sama.

Dengan demikian, kita kembali ke reaksi yang seharusnya ada setelah setiap skenario. Pertama, harus ada pemberitahuan segera tentang peretasan tersebut. Namun, seperti yang disebutkan dalam bab-bab sebelumnya, terdapat perbedaan besar antara perusahaan yang melaporkan serangan dengan perusahaan yang benar-benar diserang. Jika sebuah maskapai penerbangan khawatir telah menjadi korban serangan siber, meskipun mungkin ada dampak negatif atau kekhawatiran konsumen, kenyataannya kekhawatiran tersebut sangat minim dibandingkan dengan persyaratan untuk melindungi mereka yang berada di udara dan melaporkan serangan tersebut.

Agar maskapai penerbangan dapat melaporkan secara efektif, penting untuk melembagakan mekanisme pelaporan yang efisien antara maskapai penerbangan dan menara pengawas udara. Selain hubungan antara maskapai penerbangan dan menara pengawas udara, harus ada hubungan antara maskapai penerbangan lain, termasuk pesaing. Agar kita dapat meminimalkan dampak negatif yang ditimbulkan oleh peretas, perusahaan perlu bekerja sama satu sama lain, meskipun ada ancaman persaingan. Secara keseluruhan, prioritas nomor satu haruslah keselamatan penumpang, bukan ketakutan akan pembalasan ekonomi atau kekecewaan pemegang saham.

Ambil contoh, seseorang yang sering terbang, bahkan setiap minggu. Orang ini sangat mengenal maskapai penerbangan tersebut, serta instruksi keselamatan penumpang yang diberikan di awal setiap penerbangan. Dalam instruksi tersebut, maskapai penerbangan tersebut menekankan keselamatan penumpang, menjadikannya prioritas utama maskapai penerbangan tersebut. Jadi, jika maskapai penerbangan tersebut merasa atau khawatir akan diretas, persyaratan mutlaknya adalah mekanisme pelaporan ganda, satu ke pemerintah dan satu ke maskapai penerbangan lain.

Pertanyaannya adalah, apa yang harus dilakukan pemerintah, yaitu Administrasi Penerbangan Federal atau Departemen Keamanan Dalam Negeri? Sebagai penumpang yang peduli, saya sarankan untuk membuat daftar periksa dalam hal menanggapi dan meminimalkan ancaman tersebut. Pertama, jika sebuah pesawat telah diretas dan pesawat tersebut sedang mengudara, rencana darurat yang relevan harus diterapkan. Ancaman memanipulasi pesawat di udara ada sebagai serangan teroris. Serangan ini dapat mengakibatkan hilangnya nyawa dengan cara yang sama persis seperti serangan teroris konvensional.

Karena serangan siber memiliki tingkat ancaman yang setara dengan serangan teroris konvensional, harus ada rencana darurat, dalam skenario ini, untuk mendaratkan pesawat dalam keadaan darurat. Meskipun ini dapat menjadi ketidaknyamanan bagi penumpang dan biaya yang mahal, merupakan kewajiban bagi badan pemerintah yang terlibat dalam industri penerbangan untuk membuat rencana darurat. Diperlukan program intensif untuk mengidentifikasi bagaimana maskapai penerbangan diserang. Ini kembali ke pembahasan tentang titik-titik kerentanan.

9.2 TITIK-TITIK KERENTANAN

Semua industri memiliki titik-titik kerentanan. Maskapai penerbangan yang mengalami peretasan siber mengharuskan maskapai penerbangan untuk mempertimbangkan titik-titik kerentanan tersebut dan mengidentifikasi di mana peretasan terjadi. Ini harus dilakukan dengan cepat karena maskapai penerbangan harus tetap terbang. Jutaan orang setiap hari perlu terbang; oleh karena itu, maskapai penerbangan harus tetap beroperasi.

Namun, respons cerdas terhadap serangan siber terhadap maskapai penerbangan adalah menghentikan penerbangan untuk terlibat dan menentukan di mana peretasan terjadi. Maskapai penerbangan harus membuat respons balasan siber yang canggih, dan cara terbaik untuk melakukannya adalah dengan menerapkan analisis titik kerentanan. Secara keseluruhan, kita tidak dapat melihat serangan siber terhadap maskapai penerbangan sebagai sesuatu yang terjadi hari ini dan hilang besok; tidak akan berhasil seperti itu.

Tanggapan terhadap situasi seperti ini memerlukan kerja sama antara perusahaan dan pemerintah. Pemerintah harus memberlakukan batasan pada perusahaan, yang berpotensi menjadi periode larangan terbang. Pemerintah mungkin harus mengenakan biaya tambahan kepada maskapai penerbangan untuk membuat firewall yang canggih dan canggih. Membuat firewall ini membutuhkan waktu. Namun, dalam menelusuri titik-titik kerentanan tersebut, kebutuhan akan firewall menjadi lebih jelas.

Dalam perbincangan kritis tentang keamanan siber di masa depan ini, ancamannya signifikan. Ancaman oleh peretas baik pada tingkat individu maupun perusahaan harus dilihat sebagai tindakan perang. Jika serangan itu berasal dari aktor non-negara, maka secara teknis itu bukan tindakan perang, mengingat aktor non-negara tidak dapat menyatakan perang terhadap negara. Namun, itu adalah tindakan agresi yang signifikan. Tindakan agresi ini mengharuskan negara-bangsa, perusahaan, dan individu untuk memahami bahwa ancaman siber dan serangan siber itu nyata dan signifikan.

Dalam konteks itu, serangan siber mungkin memiliki kemungkinan untuk merugikan kita. Jenis-jenis serangan berikut pada infrastruktur mungkin memiliki kemungkinan untuk merugikan kita. Ambil contoh, serangan terhadap hal-hal berikut: sistem air kota, sistem transportasi kota, sistem rumah sakit, dan sistem komputer maskapai penerbangan.

Hal-hal di atas adalah contoh serangan siber yang jauh melampaui peretasan kartu kredit Anda. Skenario di atas menunjukkan poin-poin yang diberikan pada Gambar 9.1.

Karena alasan tersebut, sangat penting bagi kita untuk menganggap serangan siber sebagai ancaman yang patut direnungkan secara serius. Jadi, pertanyaannya adalah, apa yang dapat kita, sebagai individu, lakukan untuk melindungi diri kita sendiri dengan lebih baik? Atau, bahkan untuk melindungi perusahaan, kota, negara bagian, atau negara dari penyerang siber? Serangan siber berpotensi berbahaya dan merupakan serangan yang sangat tidak stabil dengan konsekuensi dan konsekuensi yang sangat besar. Konsekuensi tersebut mencerminkan maksud sebenarnya dari peretasan siber yang jahat yang jauh melampaui penipuan kartu kredit.

Gambar 9.1 Efek peretasan.

Ancaman ini mengharuskan perlunya mendidik masyarakat, melatih individu kita, dan bekerja sama secara lebih efektif di tingkat lokal, negara bagian, dan federal untuk mengatasi masalah kritis ini.

9.3 PEMBAHASAN LEBIH LANJUT

Dalam bab-bab sebelumnya, banyak masalah keamanan siber yang berkaitan dengan geopolitik dan hukum internasional dibahas, termasuk seluk-beluk yang terjadi dalam menangani siber dalam skala global. Pengembangan kebijakan keamanan siber dibahas secara menyeluruh dalam Bab 4, khususnya dengan konsekuensi penerapan kebijakan tersebut.

Bab-bab awal difokuskan pada reaksi, bagaimana perusahaan menanggapi kejahatan siber, dan mungkin bagaimana mereka harus menanggapi kejahatan siber. Setelah pembahasan tersebut, bab-bab berikutnya menekankan bagaimana individu dapat mengurangi dampak keamanan siber, dan kemungkinan bagaimana penegakan hukum harus mengurangi keamanan siber. Bab 8 menekankan berbagai skenario yang dimaksudkan untuk mengatasi ancaman keamanan siber di masa mendatang.

Bab ini melanjutkan pembahasan, membahas berbagai skenario keamanan siber dan merinci langkah-langkah yang mungkin diambil, langkah-langkah yang mungkin harus diambil, dan langkah-langkah yang harus dihindari. Setiap skenario akan menjadi salah satu yang Anda, sebagai pembaca, mungkin dapat hubungkan baik melalui pengalaman pribadi atau melihatnya terjadi pada perusahaan atau individu di sekitar Anda.

Pesan keseluruhan yang harus diterima adalah bahwa dunia keamanan siber itu luas dan menyentuh semua sudut kehidupan kita. Semakin cepat kita, sebagai individu, mempersiapkan diri dan melindungi diri dari serangan siber, semakin cepat pula perusahaan, penegak hukum, dan lembaga pemerintah akan melakukan hal yang sama.

SKENARIO D

Bayangkan Anda sedang duduk di rumah, menikmati acara televisi favorit, dan telepon berdering, panggilan dari nomor yang tidak Anda kenal. Banyak dari kita, jika tidak mengenali nomor telepon tersebut, tidak menjawab panggilan tersebut. Kita dengan cepat mencari nomor tersebut di Google dan memastikan bahwa nomor tersebut berasal dari agen penagihan, dan tujuan panggilan mereka adalah untuk memberi tahu Anda tentang akun yang belum dibayar atas nama Anda. Ini sering kali merupakan tanda pertama bahwa identitas seseorang telah dicuri.

Mudah untuk menyimpulkan bahwa panggilan penagihan itu bukan untuk Anda, jika akun yang dimaksud menggunakan nama yang berbeda dari akun Anda, meskipun sangat mirip (misalnya, Ms. Right Investments versus Ms. Wright Investments). Selain itu, jika akun ini

ada di Florida, dan Anda belum pernah ke Florida, itu adalah pemicu lain identitas Anda dicuri.

Pemicu lain dalam mempertimbangkan apakah identitas Anda telah dicuri adalah menentukan apakah ada orang yang tidak berwenang memiliki akses ke informasi aman Anda. Salah satu cara terjadinya hal ini adalah dengan membiarkan kartu jaminan sosial Anda di tempat umum. Namun, hal ini tidak mungkin terjadi karena mayoritas dari kita memiliki akal sehat yang lebih baik. Salah satu kemungkinan cara orang yang tidak berwenang dapat mengakses informasi aman Anda adalah melalui pelanggaran data. Seperti yang disebutkan dalam Bab 2, pelanggaran di Target berdampak pada 70 juta orang. Hal ini kemungkinan memengaruhi informasi kartu kredit.

Pelanggaran di agen asuransi dan sekolah dapat memengaruhi nomor jaminan sosial seseorang. Pertimbangkan, saat mendaftar ke sekolah, dalam aplikasi tersebut kemungkinan Anda menyertakan nomor jaminan sosial dan alamat rumah Anda. Jadi, jika sebuah lembaga pendidikan rentan terhadap serangan siber dan diretas, nomor jaminan sosial Anda dapat diakses. Ini sering kali menjadi jalur yang ditempuh untuk pencurian identitas.

Jadi, pada titik ini, Anda menghadapi situasi yang sangat sulit untuk ditangani. Ini adalah situasi yang tidak akan hilang dengan mengabaikannya dan memerlukan beberapa jenis tindakan. Langkah selanjutnya dalam skenario ini adalah mempertimbangkan berbagai jalur yang dapat Anda ambil dalam menangani situasi tersebut (Gambar 9.2).

Jalur A	Jangan lakukan apa pun. Berharap agen penagihan melupakannya, atau orang lain membayar tagihan yang belum dibayar, dan terus mengabaikan panggilan tersebut.
Jalur B	Hubungi agen penagihan dan lawan, dengan menyatakan bahwa akun yang belum dibayar bukan masalah Anda. Ancam penegak hukum dan akhirnya sadari bahwa akun tersebut menggunakan nomor jaminan sosial Anda dan terkait dengan kredit Anda. Lalu, jangan lakukan apa pun.
Jalur C	Teliti berbagai metode, tentukan respons terbaik, dan bertindaklah sesuai dengan itu. Ini dapat mencakup pelaporan nomor jaminan sosial yang disalahgunakan, menutup semua akun baru atas nama Anda, atau mengoreksi laporan kredit Anda. Ini harus selalu mencakup pelaporan pencurian identitas ke Komisi Perdagangan Federal.
Jalur D	Minimalkan dampaknya. Selain langkah-langkah dalam Rencana C, minimalkan dampaknya dengan mengajukan ke Equifax (atau perusahaan terkait serupa) dan mengambil langkah-langkah tambahan seperti yang diinstruksikan oleh Komisi Perdagangan Federal.

Gambar 9.2 Jalur potensial

Identitas Anda dicuri adalah cobaan yang berat. Ini memengaruhi banyak aspek kehidupan Anda, termasuk beberapa hal yang mungkin tidak Anda pertimbangkan pada awalnya. Ini memengaruhi kemampuan Anda untuk membuka rekening bank, mengambil pinjaman, membeli rumah, atau membuka bisnis baru. Pada dasarnya, identitas Anda dicuri memberi tanda A merah pada nomor jaminan sosial Anda. Jadi, pertanyaannya kemudian

menjadi, apa yang bisa menjadi kompensasi?

Ketika bertanya kepada seorang individu yang menjadi korban pencurian identitas apakah mereka diberi kompensasi setelah identitas mereka dicuri, mereka dengan tegas menekankan bahwa mereka tidak diberi kompensasi. Selain itu, mereka butuh waktu beberapa tahun untuk mengetahui besarnya dampak yang terjadi akibat pencurian identitas mereka. Implikasi tambahan tersebut terdiri dari orang lain yang mengajukan pajak untuk mereka, dan dengan demikian mengumpulkan pengembalian pajak penghasilan mereka. Saran mereka untuk kompensasi adalah bahwa kompensasi tersebut harus berasal dari pemerintah federal. Atau, jika tidak ada kompensasi yang dapat ditawarkan, setidaknya harus ada tindakan untuk mengubah nomor jaminan sosial seseorang.

Seperti yang terlihat pada kartu kredit, jika informasi tersebut dilanggar, perusahaan kartu kredit akan menerbitkan kartu baru untuk Anda. Jadi, pertanyaannya adalah, dapatkah pemerintah federal menerbitkan nomor jaminan sosial baru ketika identitas seseorang dicuri? Ini adalah pertanyaan penting untuk dipertimbangkan. Secara keseluruhan, ada beberapa jalur yang dapat diambil seseorang untuk bereaksi terhadap pelanggaran nomor jaminan sosial mereka, yang berarti identitas mereka dicuri, dan jalur yang dipilih secara signifikan memengaruhi konsekuensi yang dirasakan oleh pelanggaran tersebut.

SKENARIO E

Meskipun skenario individu yang dirinci di atas mungkin beresonansi dengan lebih banyak individu, skenario perusahaan yang dibahas berikutnya adalah skenario dengan potensi dampak yang lebih dahsyat. Pertama, dalam menyajikan skenario ini, penting untuk mempertimbangkan empat perusahaan yang berbeda, masing-masing dengan perbedaan yang jelas. Perusahaan A adalah salah satu perusahaan terbesar di Amerika.

Dari situ, Perusahaan A memikul tanggung jawab besar dalam jumlah informasi yang diaksesnya. Oleh karena itu, Perusahaan A menginvestasikan banyak uang dan waktu dalam perlindungan siber. Perusahaan ini bekerja sama erat dengan penegak hukum, terlibat dalam pelatihan karyawan, dan secara aktif mempekerjakan beberapa pakar data untuk melindungi perusahaan mereka dari serangan siber.

Sekarang, terlepas dari semua upaya terbaik mereka, Perusahaan A telah diretas. Mirip dengan Target atau eBay, lebih dari 100 juta pelanggan kini telah terpengaruh oleh pelanggaran tersebut. Pertanyaannya kemudian adalah, apa langkah selanjutnya, dan siapa yang bertanggung jawab setelah serangan tersebut? Seperti yang terlihat pada contoh-contoh sebelumnya, pemerintah telah mengambil tindakan sendiri untuk terlibat ketika perusahaan-perusahaan berukuran tertentu ada.

Namun pertanyaannya adalah, karena Perusahaan A mengambil tindakan signifikan untuk melindungi diri mereka dari serangan siber, dan tetap menjadi korban, apakah kompensasi atau pembalasan harus lebih besar karena mereka mengambil tindakan untuk mencoba mencegah kejadian tersebut?

Apa pun itu, hal pertama yang harus terjadi ketika sebuah perusahaan menjadi korban serangan siber adalah pemberitahuan kepada penegak hukum. Meskipun perusahaan mungkin tidak ingin melaporkan, karena takut akan keraguan atau akibat buruk dari

pelanggan, ini harus menjadi kewajiban hukum. Tanpa pemberitahuan kepada penegak hukum, penegak hukum tidak dapat membuat pola atau algoritme yang dapat mencegah serangan di masa mendatang.

Hal berikutnya yang perlu dipertimbangkan adalah apakah Korporasi A telah terbebas dari tanggung jawab, karena mereka telah mengambil tindakan pencegahan yang diperlukan dan, bukan karena kesalahan mereka sendiri, tetap menjadi korban serangan siber. Hal ini sulit dijawab dan mungkin tidak akan terjawab sepenuhnya hingga undang-undang tambahan diberlakukan.

Sekarang kita akan mempertimbangkan Korporasi B. Korporasi B, seperti Korporasi A, adalah salah satu korporasi terbesar di Amerika. Dari situ, Korporasi B memikul tanggung jawab besar dalam jumlah informasi yang diaksesnya. Namun, Korporasi B belum menginvestasikan banyak uang atau waktu dalam perlindungan siber. Sebaliknya, dewan direksi mereka, yang secara aktif menyadari ancaman keamanan siber, memilih untuk menunda investasi finansial atau personel apa pun dalam upaya perlindungan siber karena hal itu mahal, dan korporasi tersebut menjalankan bisnis untuk menghasilkan uang. Masalah ini adalah puncak dari perdebatan perlindungan versus laba.

Sekarang, bayangkan Korporasi B telah diretas. Mirip dengan Target atau eBay, lebih dari 100 juta pelanggan kini telah terpengaruh oleh pelanggaran tersebut. Pertanyaannya kemudian adalah, apa langkah selanjutnya, dan siapa yang bertanggung jawab setelah serangan tersebut? Seperti yang disebutkan sebelumnya, pemerintah AS dapat mengambil tindakan sendiri untuk terlibat ketika ada perusahaan dengan ukuran tertentu, seperti yang telah mereka lakukan sebelumnya.

Namun pertanyaannya adalah, karena Perusahaan B tidak mengambil tindakan signifikan untuk melindungi diri mereka dari serangan siber, dan menjadi korban, apakah kompensasi atau pembalasan harus dikurangi karena mereka tidak mengambil tindakan untuk mencegah kejadian tersebut? Seperti yang disebutkan sebelumnya, bagaimanapun juga, hal pertama yang perlu dilakukan ketika sebuah perusahaan menjadi korban serangan siber adalah pemberitahuan serangan tersebut kepada penegak hukum. Biasanya, sebagian besar perusahaan tidak ingin melapor, apakah itu karena takut akan keraguan pelanggan atau persepsi pemegang saham, atau akibat lainnya, itu harus menjadi kewajiban hukum. Hal berikutnya yang perlu dipertimbangkan adalah apakah Perusahaan B semakin bertanggung jawab atas kelalaiannya.

Tidak seperti Korporasi A, tanggung jawab mereka tidak dapat dibebaskan dengan cara apa pun karena mereka tidak mengambil tindakan pencegahan yang diperlukan. Meskipun ada rekomendasi dari kepala intelijen (CIO) atau karyawan lain di korporasi tersebut, Korporasi B memilih keuntungan daripada perlindungan dan menjadi sasaran empuk. Pertanyaannya kemudian adalah, karena kelalaian mereka, apakah kompensasi atau perlindungan pascaserangan harus dikurangi? Itu adalah pertanyaan yang perlu ditentukan oleh undang-undang mendatang.

Sekarang kita akan mempertimbangkan Korporasi C. Korporasi C, tidak seperti Korporasi A dan B, adalah salah satu korporasi kecil di Amerika, bisnis kota kecil yang dipegang

erat oleh beberapa anggota keluarga. Dari situ, Korporasi C memikul tanggung jawab yang jauh lebih sedikit dalam jumlah informasi yang diaksesnya.

Namun, seperti Korporasi A, Korporasi C telah menginvestasikan banyak uang dan waktu dalam perlindungan siber. Mereka bekerja sama erat dengan penegak hukum, terlibat dalam pelatihan karyawan, dan secara aktif mempekerjakan pakar data untuk melindungi korporasi mereka dari serangan siber.

Meskipun Korporasi C telah berupaya sebaik mungkin, mereka telah dilanggar. Namun, tidak seperti Korporasi A dan B, pelanggaran tersebut tidak memengaruhi lebih dari 100 juta pelanggan. Sebaliknya, pelanggaran tersebut hanya memengaruhi 5000 orang. Pertanyaannya adalah, apa langkah selanjutnya, dan siapa yang bertanggung jawab setelah serangan tersebut? Dapat diasumsikan bahwa pemerintah cenderung tidak terlibat jika pelanggarannya sangat minimal, dibandingkan dengan Korporasi A dan B.

Namun, pertanyaan yang harus diajukan adalah, karena Korporasi C mengambil tindakan signifikan untuk melindungi diri mereka dari serangan siber, dan tetap menjadi korban, haruskah mereka diberi kompensasi atau dukungan dengan cara tertentu lebih dari perusahaan yang tidak berupaya melindungi diri dari serangan siber?

Korporasi C, meskipun ukurannya kecil dibandingkan dengan Korporasi A dan B, tetap harus memiliki kewajiban hukum untuk melaporkan kepada penegak hukum sebagai korban serangan siber. Setelah itu, pertanyaan berikutnya yang perlu dipertimbangkan adalah apakah Korporasi C terbebas dari tanggung jawab, karena mereka mengambil tindakan pencegahan yang diperlukan dan, bukan karena kesalahan mereka sendiri, tetap menjadi mangsa serangan siber.

Korporasi terakhir adalah Korporasi D. Korporasi D, tidak seperti Korporasi A dan B, tetapi mirip dengan Korporasi C, adalah salah satu korporasi kecil di Amerika, bisnis kota kecil yang dipegang erat oleh beberapa anggota keluarga. Dari situ, Korporasi D memikul tanggung jawab yang jauh lebih sedikit dalam jumlah informasi yang diaksesnya. Namun, seperti Korporasi B, Korporasi D tidak menginvestasikan uang atau waktu yang signifikan dalam perlindungan siber.

Sebaliknya, korporasi memutuskan untuk menunda investasi finansial atau personel apa pun dalam upaya perlindungan siber karena mahal, dan korporasi berfokus pada menghasilkan uang. Masalah ini, seperti yang ditunjukkan dengan Korporasi B juga, adalah puncak dari perdebatan perlindungan versus keuntungan.

Karena kurangnya upaya Korporasi D, mereka telah dilanggar. Namun, tidak seperti Korporasi A dan B, pelanggaran tersebut tidak memengaruhi lebih dari 100 juta pelanggan. Sebaliknya, pelanggaran tersebut hanya memengaruhi 5000 orang. Alasan dan pertimbangannya kini menjadi sangat mirip dengan pertanyaan yang muncul terkait pelanggaran di Korporasi C. Pertanyaannya tetap, apa langkah selanjutnya, dan siapa yang bertanggung jawab setelah serangan tersebut?

Dapat diasumsikan bahwa pemerintah cenderung tidak akan terlibat jika pelanggarannya sangat minimal, dibandingkan dengan Korporasi A dan B. Namun, pertanyaannya adalah, karena Korporasi D tidak mengambil tindakan signifikan untuk

melindungi diri dari serangan siber, dan menjadi korban, apakah kompensasi atau pembalasan harus dikurangi karena mereka tidak mengambil tindakan untuk mencegah kejadian tersebut?

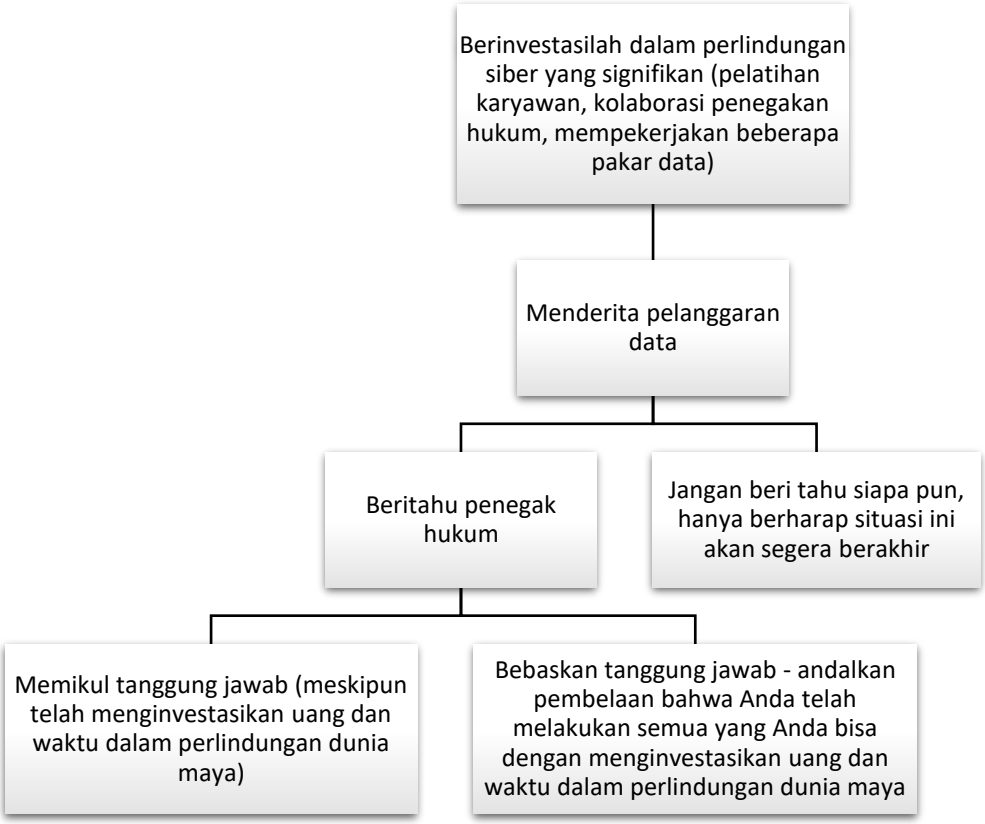
Korporasi D, meskipun ukurannya kecil dibandingkan dengan Korporasi A dan B, tetap harus memiliki kewajiban hukum untuk melaporkan diri sebagai korban serangan siber. Pertanyaan berikutnya yang perlu dipertimbangkan adalah tanggung jawab. Tidak seperti Korporasi A dan C, tanggung jawab mereka tidak dapat dibebaskan dengan cara apa pun, karena mereka tidak mengambil tindakan pencegahan yang diperlukan.

Meskipun ada rekomendasi dari CIO, atau karyawan lain di korporasi tersebut, Korporasi D memilih keuntungan daripada perlindungan dan menjadi sasaran empuk. Pertanyaannya kemudian adalah, karena kelalaian mereka, apakah kompensasi atau perlindungan pascaserangan harus dikurangi? Itu adalah pertanyaan yang perlu ditentukan oleh undang-undang mendatang.

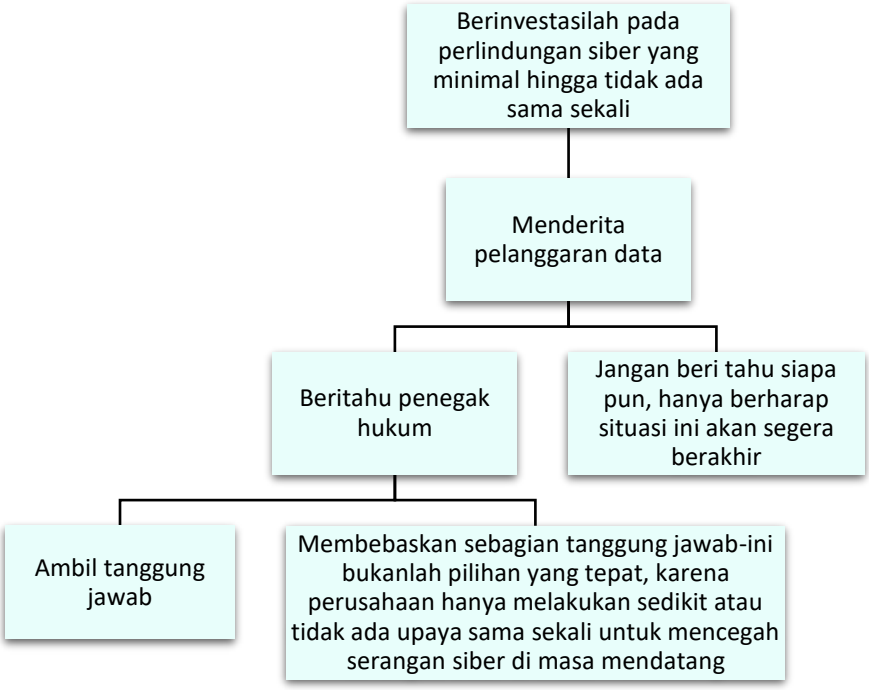
Secara keseluruhan, ada banyak faktor yang berperan ketika sebuah korporasi diretas. Persyaratan untuk menerapkan perlindungan keamanan siber yang memadai adalah masalah yang saat ini sedang diperdebatkan. Hal ini menimbulkan pertanyaan, apakah korporasi dengan ukuran tertentu, dengan akses ke catatan tertentu, harus diwajibkan untuk menerapkan tingkat perlindungan keamanan siber tertentu sebagai imbalan atas akses ke informasi penting?

Selain itu, persyaratan, atau persyaratan potensial, untuk memberi tahu penegak hukum merupakan masalah yang terus berlanjut. Haruskah pelanggaran dengan ukuran tertentu memiliki persyaratan tanggung jawab ketat yang memaksa perusahaan untuk segera melaporkan pelanggaran tersebut?

Sebaliknya, kendala bahasa ini terjadi antara orang-orang dari departemen yang berbeda dengan tujuan yang sangat berbeda. Orang-orang dari departemen TI berbicara dalam bahasa operasi dan perlindungan teknologi—dan itulah satu-satunya fokus mereka. Orang-orang dari departemen keuangan berbicara dalam bahasa keuntungan dan biaya riil—dan itulah satu-satunya fokus mereka. Jadi, sangat penting dalam perusahaan mana pun untuk memiliki karyawan atau orang yang dapat berbicara dalam kedua bahasa, menekankan pentingnya setiap tujuan, dan menemukan cara untuk membuat keduanya dapat diakses (Gambar 9.3 dan 9.4).



Gambar 9.3 Pelanggaran data di perusahaan dengan perlindungan signifikan.



Gambar 9.4 Pelanggaran data di perusahaan tanpa perlindungan yang signifikan.

Kesulitan lain yang harus ditemukan adalah kendala bahasa. Kendala bahasa ini bukanlah yang biasa Anda pikirkan saat mendengar frasa kendala bahasa. Kendala ini tidak

melibatkan satu orang yang berbicara bahasa Spanyol dan yang lainnya berbicara bahasa Prancis.

9.4 SERANGAN SIBER YANG DIGUNAKAN UNTUK KEBAIKAN

Satu hal terakhir yang perlu dipertimbangkan adalah contoh-contoh di mana aktivitas siber dapat digunakan untuk mencapai tujuan akhir yang tidak jahat atau buruk, melainkan untuk mencoba mencapai tujuan yang diinginkan banyak orang. Misalnya, Anonymous, yang merupakan sekelompok peretas yang berafiliasi secara longgar yang mencoba mencapai tujuan akhir melalui cara siber, telah mempromosikan beberapa contoh seperti itu.

Para peretas ini sangat berpengalaman dalam bidang keamanan siber dan memiliki kekuatan untuk menggunakan keterampilan itu baik untuk kebaikan maupun keburukan. Anonymous terkadang dipandang rendah, karena mereka mencoba untuk membobol rahasia negara atau membuat frustrasi tim keamanan siber perusahaan tertentu. Namun, di lain waktu mereka berada di pihak yang baik, pihak yang dapat didukung banyak orang.

Dalam beberapa bulan terakhir, Anonymous telah menyatakan perang terhadap Negara Islam Irak dan Suriah (ISIS). Dalam sebuah video yang dipublikasikan setelah serangan teroris di Paris pada bulan November, Anonymous menyatakan bahwa "serangan teroris ini tidak dapat dibiarkan begitu saja tanpa hukuman." Secara khusus, Anonymous menyatakan bahwa akan ada banyak serangan siber dan perang telah terjadi.

Selain itu, Anonymous mengancam akan mengambil tindakan terhadap mereka yang bertanggung jawab atas krisis air di Flint, Michigan. Sehari setelah ancaman tindakan oleh Anonymous, Hurley Medical Center mengonfirmasi bahwa mereka menjadi korban serangan siber. Hurley Medical Center mempekerjakan dokter yang awalnya menyuarakan keprihatinan mengenai tingginya kadar timbal pada anak-anak yang tinggal di Flint, Michigan.

Selain itu, situs web Michigan.gov diserang keesokan harinya, dua hari setelah Anonymous mengunggah video yang mengancam akan mengambil tindakan terhadap mereka yang bertanggung jawab atas krisis air. Karena sifatnya yang tepat waktu, mudah untuk menyimpulkan bahwa Anonymous bertanggung jawab atas kedua kejadian tersebut. Dengan adanya krisis air di Flint, dan serangan teroris di Paris, serta deklarasi perang terhadap ISIS oleh Anonymous, hal ini memunculkan percakapan dan penekanan yang berbeda di balik gagasan keamanan siber.

Contoh-contoh ini menunjukkan contoh-contoh di mana metode siber digunakan sebagai katalisator untuk rasa kebaikan, sebagai cara untuk mengakui ketidakadilan atau melawan mereka yang mempromosikan ketidakadilan. Apa pun itu, hal terpenting yang harus dikenali adalah berbagai dampak yang ditimbulkan oleh keamanan siber tidak hanya dalam bentuk serangan siber, tetapi juga dalam bentuk upaya menyatukan individu dan mempromosikan tujuan bersama. Seiring kita melangkah maju ke dunia siber yang semakin berkembang, dampak ini akan terus meningkat.

Pertanyaan yang perlu dipertimbangkan dalam meninjau Bab 9 diberikan dalam Gambar 9.5.

Latihan Soal

1. Seberapa besar ancaman keamanan siber?
2. Apakah ancaman serangan siber dibesar-besarkan?
3. Tugas atau kewajiban apa yang kita miliki sebagai individu dalam mengatasi ancaman tersebut?
4. Apa tugas pemerintah terhadap individu terkait siber?
5. Apakah tugas yang dimiliki sama terhadap setiap negara dan setiap individu?

Gambar 9.5 Pertanyaan tinjauan.

BAB 10
KATA PENUTUP

Dari sekian banyak poin yang diangkat dalam buku ini, ada tiga, khususnya, yang saya harap akan sangat diperhatikan publik. Saya berharap buku ini akan memfasilitasi diskusi mengenai poin-poin berikut yang diberikan dalam Gambar 10.1.

Saya yakin, ketiga isu ini adalah inti dari aspek hukum dan kebijakan dunia maya; secara individual dan kolektif, ketiganya merupakan titik awal. Hingga kita memiliki diskusi yang diperlukan, hingga para pemimpin nasional dan pejabat perusahaan benar-benar menghadapi ancaman luar biasa yang ditimbulkan oleh kejahatan dunia maya dan terorisme dunia maya, kita, secara individu dan kolektif, akan terus rentan dan berisiko.

Dalam banyak hal, ketiga isu tersebut memiliki tema yang menyatukan: Kepada siapa kewajiban dibebankan dan siapa yang berutang kewajiban itu?

Pada halaman-halaman sebelumnya, sejumlah isu yang relevan dengan keamanan dunia maya telah diangkat dengan fokus khusus pada pertanyaan hukum dan kebijakan. Meskipun pertanyaan teknis merupakan yang paling penting, pertanyaan tersebut bukanlah fokusnya. Pertanyaan yang lebih besar, oleh karena itu judulnya menjadi kata penutup, adalah ke mana kita akan pergi dari sini? Mungkin, lebih dari apa pun, ini adalah titik kritis pertanyaan bagi pembaca dan penulis.

Sepanjang buku, serangkaian cerita pendek dimasukkan untuk menghadapkan pembaca dengan keadaan dan masalah yang sulit, banyak di antaranya adalah contoh kehidupan nyata. Tujuan dari cerita pendek tersebut adalah untuk menyoroti kompleksitas masalah, memfasilitasi diskusi yang lebih besar, dan mudah-mudahan mengarah pada penyelesaian banyak masalah yang tidak memiliki akhir. Dalam buku semacam ini, cerita pendek sangat penting, mengingat berbagai dan cakupan dilema yang disajikan. Dalam banyak kasus, tidak ada jawaban yang sempurna atau jelas untuk pertanyaan-pertanyaan tersebut. Ini seharusnya tidak mengejutkan, mengingat kompleksitas keamanan siber.

1. *Kerjasama antar lembaga penegak hukum*
2. *Meningkatnya kemauan para pemimpin perusahaan untuk secara langsung menangani ancaman siber*
3. *Mengartikulasikan dan menerapkan batasan tanggung jawab negara terkait kejahatan siber dan terorisme siber*

Gambar 10.1 Poin-poin pembahasan.

Misalnya, pertanyaan penting seperti "apakah serangan terhadap perusahaan besar merupakan serangan terhadap negara-bangsa?" menimbulkan respons yang sangat meyakinkan dan saling bertentangan. Ketika saya mengajukan pertanyaan ini kepada

akademisi, pejabat penegak hukum, dan profesional dunia maya, jawaban mereka beragam, sering kali bertentangan satu sama lain. Yang menarik untuk dicatat adalah respons naluriah mayoritas adalah ya. Ini berubah, terkadang, menjadi mungkin ketika pertanyaan tersebut perlu diurai. Satu percakapan khususnya menonjol.

Orang yang dimaksud adalah wakil presiden keamanan perusahaan untuk perusahaan besar Amerika yang memiliki aset internasional. Perusahaan ini telah menjadi sasaran serangan selama bertahun-tahun. Serangan tersebut merupakan akibat langsung dari produk mereka. Oleh karena itu, ada rasa kewaspadaan dan kerentanan yang meningkat di antara para eksekutif tingkat C.

Ketika saya mengajukan pertanyaan kepadanya, respons langsungnya adalah "ya, tentu saja." Asumsi saya adalah jawabannya mencerminkan kenyataan yang menyadarkan dari serangan sebelumnya. Namun, ada peringatan menarik dalam tanggapannya: "Jawaban 'ya' bergantung pada ukuran perusahaan." Saya tidak yakin apa maksudnya dan meminta dia menjelaskan jawabannya. Dia dengan ramah menjelaskannya.

Menurut pendapatnya, jawaban ya didasarkan secara eksklusif pada serangan terhadap perusahaan besar. Serangan terhadap perusahaan menengah dan kecil, menurut orang ini, tidak dapat ditafsirkan sebagai hal yang memerlukan tanggapan dari pemerintah AS. Ketika saya bertanya kepadanya apakah serangan teroris tradisional terhadap perusahaan menengah atau kecil akan membenarkan tindakan pemerintah, jawabannya adalah ya dengan tegas.

Saya telah mengenal orang ini selama bertahun-tahun dan sangat menghormati wawasan dan pengalaman profesionalnya dalam penegakan hukum Amerika. Ketidaksesuaian tanggapannya antara terorisme tradisional dan terorisme siber sangat membantu dalam upaya saya untuk memahami perbedaan antara keduanya. Konsekuensi dari yang pertama jelas, tidak seperti yang terakhir. Lebih jauh, kerusakan jiwa dan harta benda menjadi visual yang kuat yang dapat berfungsi untuk mendorong masyarakat dan para pembuat keputusan.

Media memainkan peran penting dalam menyoroti kerugian yang ditimbulkan. Drama yang menyertai setelah serangan yang berhasil yang mengakibatkan kematian tidak dapat ditangkap, ketika akun klien diretas dalam serangan siber. Pepatah, "satu gambar bernilai seribu kata," tidak berlaku ketika peretasan telah terjadi. Ini bukan untuk meminimalkan dampaknya, tetapi berfungsi untuk menjelaskan, setidaknya sebagian, jawaban yang diberikan untuk pertanyaan saya. Bersatu di sekitar bendera dapat dimengerti setelah serangan teroris tradisional; respons yang mendalam itu sulit untuk dimunculkan setelah target diretas. Hal yang sama berlaku untuk Sony dan sejumlah besar perusahaan lainnya.

Pertanyaannya adalah apakah respons yang terbagi itu melayani kepentingan keamanan nasional. Diartikulasikan ulang: Apa batasan keterlibatan pemerintah dalam keamanan siber? Jawaban yang mudah adalah bahwa keamanan siber merupakan prioritas bagi pemerintah daerah, negara bagian, dan nasional. Pertanyaan yang lebih sulit adalah apa artinya itu dan apakah itu dapat diterapkan secara konsisten? Implementasi, lebih dari sekadar retorika, memerlukan analisis prioritas yang canggih, penerapan model analisis biaya-manfaat, dan pengakuan terhadap tingkat dan sifat ancaman.

Bagaimanapun, mustahil bagi pemerintah (terlepas dari tingkat mana) untuk bertindak—secara proaktif atau reaktif—terhadap semua ancaman. Inilah sebabnya mengapa prioritas mengenai alokasi sumber daya menjadi sangat penting. Namun, yang lebih penting adalah artikulasi dan implementasi kebijakan keamanan siber nasional. Namun, di sini juga kebijakan tersebut tidak memadai; ujiannya adalah seberapa realistis implementasinya. Ini membutuhkan pilihan yang sulit oleh pemerintah, penegak hukum, pemimpin perusahaan, dan masyarakat.

Ini membawa saya kembali ke percakapan dengan wakil presiden untuk keamanan perusahaan: penggambarannya antara perusahaan besar dan perusahaan menengah-kecil, mungkin, mencerminkan kenyataan yang tidak mengenakkan. Kenyataan ini menjangkau audiens yang berbeda, semuanya relevan dengan diskusi ini. Namun, selain kenyataan tentang "seberapa banyak yang dapat dilakukan pemerintah", ada sisi lain yang paling baik diartikulasikan sebagai kerja sama yang luas dan terlembagakan dalam menanggapi ancaman yang ditimbulkan oleh keamanan siber.

Bentuk kerja sama tersebut penting untuk mengembangkan—dan menerapkan—kontra keamanan siber yang efektif. Contoh dan cerita pendek yang disisipkan di seluruh buku ini dimaksudkan untuk memudahkan pemahaman pembaca tentang perlunya mengembangkan kerja sama yang dilembagakan dan, bersamaan dengan itu, mengenali kesulitan dalam upaya tersebut.

Alasannya beragam; rasionalisasinya ditawarkan. Apakah itu didorong oleh faktor finansial seperti halnya dengan perusahaan atau wilayah dan anggaran seperti yang dijelaskan kepada saya oleh pejabat penegak hukum, konsekuensinya jelas dapat diprediksi. Penerima manfaat dari kurangnya kerja sama yang konsisten adalah pelaku kesalahan; korbannya banyak sekali.

Ada baiknya mengingat kembali percakapan saya dengan seorang eksekutif perusahaan yang dirujuk dalam Bab 1. Intinya, perusahaan menanggung risiko ketika secara sengaja kurang berinvestasi dalam perlindungan siber. Keputusan ini, tampaknya, mencerminkan apatisme klien mengenai kemungkinan konsekuensi dari serangan siber. Konsekuensi finansial bagi perusahaan—menurut eksekutif yang bertugas menangani dampaknya—menurutnya, sangat signifikan. Dampak negatif bagi klien juga signifikan.

Keputusan yang tampaknya penuh perhitungan itu bermasalah. Keputusan itu mencerminkan kegagalan untuk menghadapi ancaman secara langsung. Keputusan itu juga tidak menyelesaikan pertanyaan tentang sejauh mana keterlibatan pemerintah, baik secara proaktif maupun retroaktif.

Hal ini sangat kontras dengan pertemuan yang saya adakan di Israel dengan seorang pakar dunia maya terkemuka. Percakapan itu sangat mendalam, menyoroti hubungan antara keamanan nasional dan keamanan dunia maya. Yang lebih penting, percakapan itu menyoroti peran penting yang dapat—dan seharusnya—dimainkan pemerintah dalam kaitannya dengan dunia maya.

Percakapan ini difokuskan pada pertanyaan tentang hukum dan kebijakan; masalah teknis, meskipun tidak diragukan lagi penting, bukanlah yang terpenting dalam apa yang kami

bahas. Yang paling mengesankan bagi saya—dalam konteks kerja sama—adalah manfaat besar yang diperoleh, ketika sektor publik dan swasta bergabung dan bekerja sama.

Itu tidak dimaksudkan sebagai penutup ketegangan, kecemburuan, dan persaingan yang tak terelakkan antara keduanya. Akan tetapi, itu sangat kontras dengan diskusi yang saya lakukan dengan pejabat penegak hukum. Perbedaan antara kedua pendekatan itu sangat mencolok. Konsekuensinya jelas. Karena alasan itulah tema kerja sama menempati posisi yang sangat penting dalam buku ini.

Dalam Bab 1, penulis menggunakan istilah new frontier. Saya mengurangi sisi positif yang umumnya dikaitkan dengan istilah itu dengan mencatat manfaat yang sepadan adalah penggunaan dunia maya yang jahat dan tak terelakkan. Tak perlu dikatakan, hal itu berbahaya dan merugikan dan sering kali disadari terlambat. Seperti yang telah kita pelajari, ada banyak kerugian yang secara langsung berasal dari dunia maya. Contoh-contohnya berlimpah setiap hari.

Banyak dari kita telah menjadi korban kerugian, baik secara pribadi, profesional, maupun komunitas. Kerentanan kita terhadap kejahatan dunia maya telah terdokumentasi dengan baik; tidak perlu mengulang-ulang serangkaian insiden, mulai dari yang menjengkelkan hingga yang benar-benar membawa bencana.

Jelas bahwa individu dalam kelompok, di seluruh dunia, berdedikasi untuk terus mencari cara menggunakan dunia maya untuk keuntungan mereka dan kerugian kita. Benar-benar ada hubungan antara kami dan mereka dalam hal dunia maya. Kerugian yang ditimbulkan oleh penjahat dunia maya dan teroris dunia maya sangat signifikan; kerugian di masa mendatang yang tidak diragukan lagi akan mereka timpakan kepada masyarakat adalah hal yang lebih memprihatinkan. Saya tidak meragukan hal itu.

Selain pentingnya kerja sama dan manfaat yang diperoleh darinya, buku ini juga membahas sejumlah isu relevan lainnya. Kami juga telah mengeksplorasi pertanyaan-pertanyaan penting mengenai perlindungan; yaitu, bagaimana perusahaan harus melindungi diri mereka sendiri dan apa peran negara-bangsa dalam menanggapi serangan terhadap entitas perusahaan. Dalam melakukannya, kami telah berfokus pada pertimbangan hukum dan kebijakan yang penting dengan fokus khusus pada penerapan—dan batasan—pembelaan diri. Seperti disebutkan di atas, terdapat kurangnya konsensus yang mendalam mengenai pertanyaan tentang keterlibatan pemerintah.

Mungkin sebagai cerminan langsung dari latar belakang saya di Pasukan Pertahanan Israel, saya terus terang bingung dengan keraguan yang berulang kali diungkapkan kepada saya mengenai peran pemerintah dalam perlindungan dunia maya. Saya percaya bahwa serangan siber perlu dianggap serupa dengan serangan fisik.

Konsekuensinya, bagi saya, jelas: Serangan terhadap perusahaan Amerika memerlukan respons pemerintah. Meskipun hal itu memerlukan kerja sama yang dibahas di atas, manfaatnya—baik jangka pendek maupun jangka panjang—jauh lebih besar daripada konsekuensi negatif apa pun terkait keterlibatan pemerintah.

Terus terang, taruhannya terlalu tinggi untuk menggunakan klise yang sudah usang dan mantra yang tidak relevan terkait masalah privasi, yaitu, bukan untuk mengecilkan masalah

privasi—kebocoran NSA secara mengganggu menyoroti realitas intrusi pemerintah—tetapi untuk menunjukkan bahwa ancaman dunia maya memerlukan pendekatan yang seimbang dan bernuansa.

Menyangkal keterlibatan pemerintah secara ringkas adalah tindakan yang picik dan pada akhirnya kontraproduktif. Prinsip itu sangat jelas bagi saya saat bertugas di Pasukan Pertahanan Israel dan telah diperkuat dengan kuat saat meneliti dan menulis buku ini. Bersamaan dengan keterlibatan pemerintah adalah masalah pembelaan diri. Kenyataannya, keduanya terkait langsung dan tidak dapat dipisahkan satu sama lain.

Pembelaan diri merupakan pertanyaan penting dalam diskusi siber. Pertanyaannya adalah apakah negara-bangsa memiliki kewajiban terhadap korporasi dan individu, yang telah menjadi korban serangan siber. Ini bukanlah pertanyaan abstrak, melainkan pertanyaan yang dimaksudkan sebagai pertanyaan konkret. Jawabannya, seperti yang disoroti dalam percakapan saya dengan berbagai individu, tidak jelas.

Meskipun jawaban yang mudah adalah ya, jawabannya jauh lebih rumit dari itu. Demikian pula, tidak merupakan respons yang tidak dapat diterima, karena kepentingan nasional memang membenarkan keterlibatan negara dalam keamanan siber bahkan ketika target negara tidak diserang secara langsung.
Oleh karena itu, jawabannya terletak di antara keduanya.

Di kelas saya, baik Perspektif Global tentang kontraterorisme atau Prosedur Pidana, saya menekankan kepada siswa bahwa kata terpenting dalam membahas ketegangan antara hak kebebasan individu yang sah dan hak keamanan nasional serta ketertiban umum yang sama-sama sah adalah keseimbangan. Saya menyebutnya sebagai kata B.

Keseimbangan sulit didefinisikan dan tidak diragukan lagi sulit diterapkan. Dalam konteks kewajiban negara terhadap korporasi dan individu, akan menjadi hal yang tidak praktis untuk memaksakan kewajiban kepada pemerintah untuk menanggapi setiap serangan siber. Saran ini tidak akan berhasil sejak awal. Sebaliknya, menyarankan bahwa pemerintah tidak memiliki kewajiban berarti melanggar kontrak sosial yang menjadi dasar masyarakat sipil. Ini juga tidak akan berhasil.

Ada risiko besar dalam memaksakan beban respons pada negara-bangsa setelah serangan siber. Jika serangan tersebut dapat ditelusuri kembali ke agen negara lain, maka muncul pertanyaan yang sah mengenai batas kedaulatan, pembelaan diri, dan konflik. Ini adalah pertanyaan yang sangat penting dengan konsekuensi yang kuat, terlepas dari bagaimana pembaca menyarankan penyelesaiannya.

Kita berkewajiban untuk mendorong diskusi ini terlepas dari betapa sulit dan tidak nyamannya diskusi ini. Ego yang terluka harus dikutuk: ancaman yang ditimbulkan terlalu besar.

DAFTAR PUSTAKA

Alfi, Muhammad; Yundari, Ni Putu; & Tsaqif, Ahnaf. (2023). "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional*, Vol. 6(2).

Arquilla, John; & Ronfeldt, David F., eds. (1996). The Advent of Netwar. RAND Corporation.

Buchanan, Ben. (2016). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford University Press.

Clarke, Richard A., & Knake, Robert K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Deibert, Ronald J., et al. (2008). Access Denied: The Practice and Policy of Global Internet Filtering. MIT Press.

Dunn Cavelty, Myriam. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.

Friedman, George. (2009). The Battle for Cyber Supremacy: China, America, and the Struggle for Technological Dominance. Routledge.

Goldsmith, Jack; & Wu, Tim. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.

Greenwald, Glenn. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S Surveillance State*. Metropolitan Books.

Healey, Jason eds., et al..(2011) "Strategi Penanganan Keamanan Siber." Universitas Pahlawan

Hukum Perlindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity. (2024). *Library Pusperkim*.

Kello, Lucas. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Kissinger, Henry. (2014). *World Order: Reflections on the Character of Nations and the Course of History*. Penguin Books.

Libicki, Martin C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Nye, Joseph S. Jr. (2010). Cyber Power. Harvard Kennedy School Belfer Center for Science and International Affairs.

Pagliery, Jose. (2014). *Bitcoin and the Future of Money in Cyberspace*. Triumph Books.

Putri, Kristiani Virgi Kusuma. (2021). "Kerja Sama Indonesia dengan ASEAN Mengenai Cyber Security dan Cyber Resilience dalam Mengatasi Cyber Crime." Rewang Rencang: Jurnal Hukum Lex Generalis, Vol. 2(7), 542-548.

Ramadhan, Iqbal. (2021). "Implikasi Ruang Siber terhadap Geopolitik Negara." *Politicon*, Vol. 3(2), 161-172.

Rid, Thomas. (2013). *Cyber War Will Not Take Place*. Oxford University Press.

Schneier, Bruce. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Singer, P.W., & Friedman, Allan. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Situmeang, Sahat Maruli T. (2020). *Cyber Law*. Penerbit Cakra.

Westby, Jody R., eds. (2003). *International Guide to Cybersecurity*. American Bar Association.

Yehizkia, B.R.M., & Wibisono, I.W. (2024). "Ancaman Siber dan Penguatan Kedaulatan Digital Indonesia dari Perspektif Geopolitik Digital." *Jurnal JUKIM*, Vol. 3(2), 83-93.

Zetter, Kim. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown Publishing Group.

HUKUM CYBERSECURITY DAN GEOPOLITIK

Dr. Agus Wibowo, M.Kom, M.Si, MM.

BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen dan ilmu sosiologi. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik).

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-97-7 (PDF)
9 786238 642977