BAB II

PENGATURAN TINDAK PIDANA *CYBER ESPIONAGE* BERDASARKAN HUKUM POSITIF DI INDONESIA

2.1. Sejarah *Cyber Espionage*

"Spionase berasal dari bahasa Perancis yakni *espionnage* yang merupakan suatu praktik untuk mengumpulkan informasi mengenai sebuah organisasi atau lembaga yang dianggap rahasia tanpa mendapatkan izin yang sah dari pemilik informasi tersebut".[26] Sejarah mengenai spionase ini sendiri pun terdokumentasi dengan baik dimulai dari sejak jaman-jaman kekaisaran hingga jaman modern sekarang ini di berbagai belahan dunia. Salah satu cerita mengenai spionase berawal dari kisah Chandragupta Maurya seorang pendiri kekaisaran Maurya di India yang memanfatkan pembunuhan, mata-mata sebagai bagian dari upaya spionase dan agen rahasia yang dijelaskan secara gamblang pada Chanakya Arthasastra.

Beranjak dari kisah tersebut, pada saat perang dingin berlangsung, kegiatan spionase telah dilakukan oleh Amerika Serikat, Uni Soviet, dan *People's Republic of China* dan sekutu mereka khususnya yang berkaiatan dengan aktivitas kepemilikan senjata nuklir rahasia. "Tidak seperti bentuk lain dari pengumpulan data intelejen, spionase biasanya melibatkan pengaksesan tempat penyimpanan informasi yang diinginkan, atau mengakses orang-orang yang mengetahui

[26] Wikipedia, *Spionase*, diakses melalui: www.Wikipedia/spionase.com, diakses pada tanggal 1 Mei 2025.

mengenai informasi tersebut dan akan membocorkannya melalui berbagai dalih".[27]

> *The US* mendefinisikan spionase sebagai "Tindakan memperoleh, memberikan, mengirimkan, berkomunikasi, atau menerima informasi mengenai pertahanan nasional dengan tujuan atau alasan untuk percaya, bahwa informasi dapat digunakan untuk mencederai Amerika atau bangsa asing. Sedangkan *Black's Law Dictionary* (1990) mendefinisikan spionase *"The practice of using spies to collect information abaout what another government or company is doing or plans to do.*[28]

Salah Satu kasus mengenai spionase yang sangat fenomenal terjadi ketika Perang Dunia I. Saat itu seorang wanita Belanda bernama Margareth Getruide Zelle yang lebih terkenal dengan nama Mata Hari merupakan penari orientalis dan spion politik untuk pemerintah Jerman. Ketika berusia 19 tahun dia dinikahi oleh Rudolp McLeod yang merupakan Perwira Tinggi Militer Belanda yang bertugas di Indonesia sehingga kemudian tinggal berpindah-pindah di berbagai kota di Indonesia, salah satunya adalah kota Malang dan Semarang.

Sebelum terjun di dunia spionase, wanita yang memilki kode rahasia H21 ini mengawali karirnya sebagai penari erotis di Paris. Berbekal keahlian *erotic temple dance* yang dipelajari di India serta tarian-tarian daerah selama tinggal di Indonesia dan daya pikatnya yang tinggi, dia menjadi terkenal dimana-mana. Tak heran bila kemudian tawaran menari banyak berdatangan dari kota-kota besar di Eropa bahkan Mesir. Kondisi inilah yang kemudian menyeretnya dalam dunia spionase. Saat menjadi *stripper* di Berlin, agen rahasia Jerman merekrutnya. Mata hari kemudian sering berkelana baik antar kota maupun antar negeri. Karena

---

[27] *Ibid.*

[28] Shelly Nicco, *Tindak Pidana Cyber Espionage*, Skripsi, Fakultas Hukum Universitas Airlangga, Surabaya, 2010, h. 20.

sering bepergian, maka dia tidak punya kesulitan untuk menyusup, termasuk dalam masa Perang Dunia Pertama.

Agen rahasia Inggris yang mempunyai kode M15 mulai curiga dengan aktivitas yang dilakukan oleh Mata Hari. Agen rahasia Inggris tersebut lalu mengintrogasinya, namun mereka tidak bisa memaksa Mata Hari untuk membuka mulut. Bekali-kali interogasi dilakukan namun hasilnya tetap nihil. Sampai akhirnya Agen rahasia Perancis berhasil menangkap dan mengintrogasinya saat dia menyebrangi Perancis untuk mengunjungi salah satu *affair*nya. "Agen rahasia Perancis menangkap Mata Hari karena diyakini dialah "*The Greatest Woman Spy*" yang harus bertanggung jawab atas kematian beribu-ribu tentara akibat informasi yang diberikannya. Dia lalu diadili di pengadilan perang dan dieksekusi dihadapan regu tembak pada tanggal 15 September 1917".[29]

"Perkembangan spionase, yang awalnya hanya digunakan atau dianggap sebagai upaya institusional dengan cara memata-matai musuh potensial atau aktual, terutama untuk tujuan militer, kini telah berkembang untuk memata-matai perusahaan, yang kini dikenal secara spesifik sebagai Spionase Industrial".[30] Dalam perjalanan spionase industrial ini, satu kasus besar yang pernah terjadi adalah kasus spionase yang melibatkan dua perusahaan otomotif dunia terbesar peserta Formula 1 yakni McLarren Mercedes dengan Ferrari.

---

[29] Wikipedia, *Matahari*, diakases melalui: http://wikipeda.org/wiki/Mata_Hari.com, diakses pada tanggal 1 Mei 2025.

[30] Wikipedia, *Sejarah Espionase*, diakses melalui: www.wikipedia/spionase/sejarah.com, diakses pada tangal 1 Mei 2025.

2.2. Modus Operandi *Cyber Espionage*

Modus operandi merupakan cara-cara yang digunakan sebagai sarana untuk melakukan *cyber espionage*. *Cyber Espionage* lazimnya disebut tindakan mata-mata atau pengintaian terhadap suatu data pihak lain. Mengingat internet merupakan media lintas informasi yang berdampak luas, maka akses data yang menyangkut pihak lain patut menjadi perhatian dan dapat menjadi kejahatan yang serius. Aksi pengintaian ini dilakukan dengan motif yang beragam. Diantaranya politik, ekonomi, ilmu pengetahuan, perdagangan, dan lain sebagainya.

Dalam sistem hukum dan kehidupan sehari-hari, keberadaan suatu arsip berupa data dan/atau informasi elektronik adalah dimaksudkan sebagai suatu alat bukti yang merekam/menerangkan keberadaan suatu informasi tertentu, atau dalam bahasa hukum ini dinyatakan sebagai pembuktian terhadap telah terjadinya suatu peristiwa hukum yang tentunya mempunyai akibat hukum tertentu bagi hak dan kewajiban para pihak yang tersangkut daripadanya. "Demikian juga adanya dengan arsip elektronik".[31] "Ada tiga macam data dan/atau informasi elektronik yang terdapat di internet yang dapat diakses secara bebas. Pertama adalah yang tersedia dalam bentuk basis data (*database*) *online*; kedua yang diperoleh dalam suatu transaksi *online;* dan ketiga yaitu basis data yang dimiliki oleh negara atau pemerintah yang terdapat dalam situs-situs pemerintah tersebut".[32]

Sedangkan Data dan/atau informasi yang umumnya dijadikan target atau sasaran dalam tindak pidana *cyber espionage* ini umumnya bukan merupakan

---

[31] Edmon Makarim, *Kompilasi Hukum Telematika,* PT Raja Grafindo Persada, Jakarta, 2004, h. 207.

[32] Susan E.Gindin, *Lost and Found in Cyberspace: Informational Privacy in The Age of The Internet*, Jurnal San Diego Law Review 1153, 1997.

informasi elektronik sembarangan maupun yang dapat diakses secara bebas, hal tersebut dapat dilihat dari nilai kualitas informasi itu sendiri yang tergantung pada 3 (tiga) hal yaitu informasi tersebut haruslah akurasi, ketepatan waktu, dan relevansi. Akurasi berarti informasi tersebut harus bebas dari kesalahan dan tidak bias. Akurat juga berarti bahwa informasi tersebut harus jelas maksud dan tujuan. "Ketepatan waktu berarti informasi tersebut bukan sesuatu yang sudah usang. Relevansi berarti informasi tersebut memiliki manfaat bagi pemakai atau pihak lain yang membutuhkan".[33]

Cara-cara yang dilakukan dalam proses pengintaian ini terjadi bila terjadi suatu akses ke dalam suatu sistem yang dituju mencapai suatu keberhasilan. Proses penyusupan hingga terjadi pengintaian secara sistematis melalui tahapan sebagai berikut :

1) *Footprinting* (Pencarian Data)

   Hacker baru mencari-cari sistem yang dapat disusupi. *Footprinting* merupakan kegiatan pencarian data berupa:

   a. Menentukan ruang lingkup (*scope*) aktivitas atau serangan;
   b. *Network enumeration* (menyeleksi jaringan);
   c. Introgasi jaringan;
   d. Mengintai jaringan

   Semua kegiatan ini dapat dilakukan dengan *tools* dan informasi yang tersedia bebas di internet. Kegiatan *footprinting* ini diibaratkan mencari

[33] Jogiyanto H.M, *Pengenalan Komputer*, Cetakan Pertama, Andi Ofset, Jogyakarta, 2005, h. 5.

informasi yang tersedia umum melalui buku telepon. *Tools* yang tersedia untuk ini diantaranya :

a) *Teleprot Pro*: Dalam menentukan ruang lingkup, *hacker* dapat men-*download* keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon, *contact person*, dan lain sebagainya.

b) *Whois for* 95/9/NT: Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (*domain hijack*).

c) *NSLookup*: Mencari hubungan antara *domain name* dengan IP *address*

d) *Traceroute* 0.2: Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

2) *Scanning* (Pemilihan Sasaran)

Lebih bersifat aktif terhadap sasaran. Di sisni diibaratkan *hacker* sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya. Kegiatan *scanning* dengan demikian dari segi jaringan sangat “berisik” dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali menggunakan *stealth scanning*. *Scanning tool* yang paling legendaris adalah nmap (yang kini sudah tersedia pula untuk *windows* 9x/ME maupun DOS), selain *SuperScan* dan *UltraScan* yang juga banyak digunakan dalam sistem *windows*. Untuk melindungi diri dari kegiatan *scanning* adalah memasang *firewall* seperti misalnya Zone Alarm, atau bila

keseluruhan *network*, dengan menggunakan IDS (*Instrusion Detection Sistem*) seperti misalnya *Snort.*

3) *Enumerasi* (Pencarian Data Mengenai Sasaran)

   Sudah bersifat intrusif (mengganggu) terhadap suatu sistem. Di sini penyusup mencari *account name* yang absah, serta *share resources* yang ada. Pada tahap ini, khusus untuk sistem *windows*, terdapat port 139 (NetBIOS *session service*) yang terbuka untuk *resoursce sharing* antar pemakai dalam jaringan. Anda mungkin berpikir bahwa *hard disk* yang di-*share* itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannnya tidak demikian. NetBIOS *session service* dapat dilihat oleh siapapun yang terhubung lewat internet di seluruh dunia! *Tools* seperti *Legion*, SMB *Scanner,* atau *Shares Finder* membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka *resource share tanpa password*).

4) *Gaining Access* (Akses *Illegal* telah didapatkan)

   Adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai *user* biasa. Ini adalah kelanjutan dari kegiata *unemerasi*, sehingga biasanya di sini *hacker* sudah mempunyai paling tidak *user account*

5) *Escalating Privilage* (Menaikkan atau Mengamankan Posisi)

   Mengasumsikan bahwa penyerang sudah mendapatkan *logon access* pada sistem sebagai *user* biasa. Penyerang kini berusaha naik kelas menjadi admin (pada *sistem windows)* atau menjadi *root* (pada unit *Unix/Linux*). Teknik yang digunakan sudah tidak lagi *dictionary attack* atau *brute force*

attack yang memakan waktu, melainkan mencuri *password file* yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem windows 9x/ME *password* disimpan dalam file. PWL sedangkan pada Windows NT/2000 dalam *file*.SAM. Bahaya pada tahap ini bukan hanya penyerang diluar sistem, melainkan lebih besar lagi bahayanya adalah orang dalam yaitu *user* absah dalam jaringan itu sendiri yang berusaha "naik kelas" menjadi admin atau *root.*

6) Memata-matai data

   Pada tahap ini *hacker* mulai melakukan aksinya yaitu *cyber espionage*.

7) Membuat *backdoor* dan menghilangkan jejak

   Setelah *hacker* melakukan aksinya, biasanya mereka akan menghilangkan jejak. Seorang *hacker* akan memperkecil kemungkinan terdeteksi oleh orang lain. Cara ini biasanya dengan memanfaatkan *trojan* atau *finger*. "Seorang *hacker* yang berpengalaman, biasanya suatu hari ia akan kembali ke sistem tersebut dan terlalu lama jika prosedurnya atau proses *hacking* diulang dari awal. Berkaitan dengan hal itu biasanya *hacker* membuat *backdoor* atau pintu belakang yang pada dasarnya adalah jalan tembus".[34]

Modus lain dari *cyber espionage* dilakukan dengan metode acak atau tidak sistematis, salah satunya datang dari berita yang menghebohkan dunia dari pusat studi di Kanada, *Munk Center For International Studies*, yang mengemukakan peneliatiannya bahwa adanya sistem komputer mata-mata yang berasal dari Cina yang dapat menyusup kedalam sistem komputer pemerintahan negara di seluruh

[34] Edmon Makarim, *Kompilasi Hukum Telematika*, Cet.2, PT Raja Grafindo Persada, Jakarta, 2004, h. 402.

dunia dan juga instansi data untuk memata-matai data atau informasi untuk kemudian dicuri. Hingga saat ini sedikitnya 103 (seratus tiga) negara yang disusupi dengna jumlah total komputer sebanyak 1295 (seribu dua ratus sembilan puluh lima) unit, kelompok peneliti ini menamakannya *GhostNet*. Cara yang dilakukan pengintai pada kasus ini adalah dengan menyusupkan virus Trojan dan sejumlah *software* jahat yang telah menyusup kedalam sistem komputer dan mengambil dokumen-dokumen yang sifatnya sensitif dari komputer. Laporan riset menyebutkan bahwa sistem komputer mata-mata ini memiliki kemampuan yang luar biasa yang disebut dengan istilah *Big Brother Style*. Selain dapat mencuri data juga dapat membuat komputer yang telah disusupi untuk secara otomatis menyalakan kamera dan menjalankan fungsi rekaman suara untuk tujuan melakukan pengintaian jarak jauh.

Selanjutnya adalah dengan menyusupkan *Spyware*. Istilah *spyware* atau peranti lunak yang memata-matai pengguna komputer telah lama menjadi kosa kata dunia informasi teknologi. *Spyware* merupakan aplikasi yang bertugas untuk melacak aktivitas *surfing* seorang *netter*, *netter* merupakan sebutan untuk orang-orang yang memanfaatkan jaringan internet secara diam-diam. Lalu secara diam-diam pula mengirim informasi-informasi hasil lacakan tersebut ke *server* komputer tertentu yang dirancang oleh si pembuat aplikasi *spyware*. *Spyware* juga dikenal dengan istilah *adware* adalah semacam program tersembunyi yang berfungsi untuk mengirim informasi mengenai komputer yang terinfeksi melalui internet ke si pembuat *spyware.*

Biasanya *spyware* otomatis terinstal baik akibat men*download* sesuatu secara tidak sengaja maupun disususpi secara sengaja oleh orang lain. *Spyware* menjadi berbahaya karena saat ini *spyware* tidak hanya sebagai pengirim info tersembunyi saja, tapi menginstal semacam program khusus yang akhirnya si pemilik *spyware* bisa memata-matai segala aktivitas korban di internet. "Data yang diperoleh dari hasil memata-matai tersebut dikumpulkan dan digunakan untuk kepentingan komersial bahkan kriminal. Tentu saja tanpa seijin dan pengetahuan si *netter*."[35] Hal yang membahayakan lainnya adalah bahwa program pengintai yang bisa mencuri *username* dan *password*, sehingga *spyware* bisa disebut "*species*" baru yang mengancam keamanan komputer setelah virus.

2.3. Perbedaan *Cyber Crime, Cyber Warfare,* dan *Cyber Espionage*

Di dalam dunia maya, banyak jenis operasi siber yang terjadi. Beberapa jenis operasi siber yang paling dikenal adalah *cyber crime, cyber warfare*, dan *cyber espionage*. Masing-masing dari operasi tersebut memiliki unsur berbeda, dan memiliki hukum yang berbeda pula. Maka dari itu, penting untuk mengidentifikasi perbedaan antara operasi-operasi siber sebelum berbicara tentang hukum yang mengaturnya.

> *Cyber crime* atau kejahatan siber diatur dalam *Budapest Convention on Cyber crime*, sebuah konvensi internasional yang dibuka untuk tanda tangan di Budapest, Hongaria pada November 2001, dan berlaku sejak 1 Juli 2004. Konvensi ini dinegosiasikan antara negara anggota Majelis Eropa beserta Kanada, Jepang, Afrika Selatan dan Amerika Serikat, namun terbuka untuk diaksesi negara manapun.[36]

---

[35] Boytra, *Cerita Sedikit Tentang Spyware*, diakses melalui: www.boytra.blogspot.com/ 2007/08/cerita-sedikit-tentang-spyware.html, diakse pada tanggal 1 Mei 2025.

[36] Hollis, Duncan B., *A Brief Primer on International Law and Cyberspace*, Carnegie Endowment for International Peace, 2021, h. 2.

Konvensi ini mengatur "(i) kriminalisasi perilaku mulai dari akses ilegal, gangguan data dan sistem hingga penipuan terkait komputer dan pornografi anak; (ii) perangkat hukum acara untuk menyelidiki kejahatan dunia maya dan mengamankan bukti elektronik terkait dengan kejahatan apapun; dan (iii) kerjasama internasional yang efisien".[37] Menurut Pasal 13 ayat (1). Konvensi ini mengharuskan setiap Pihak untuk menerapkan Undang-Undang yang mengkriminalisasi pelanggaran-pelanggaran melalui komputer yang diatur dalam Pasal 2 hingga Pasal 11. Pelanggaran yang tertulis dalam Pasal-Pasal tersebut antara lain:

1) Akses ilegal;
2) Penyadapan ilegal;
3) Gangguan data;
4) Gangguan sistem;
5) Penyalahgunaan perangkat;
6) Pemalsuan yang berhubungan dengan komputer;
7) Penipuan yang berhubungan dengan komputer;
8) Pelanggaran yang berkaitan dengan pornografi anak;
9) Pelanggaran yang berkaitan dengan hak cipta dan hak-hak lainnya;
10) Mencoba dan menolong atau bersekongkol; dan
11) Pertanggungjawaban perusahaan.

Cyber crime tidak memiliki satu definisi hukum yang pasti, namun dapat disimpulkan dari unsur-unsur yang ada di dalam konvensi yang mengaturnya. Jika

[37] Majelis Eropa, *The Budapest Convention on Cyber Crime: Benefits and Impact in Practice Strasbourg Prancis 2020*, diakses melalui: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, diakse pada tanggal 1 Mei 2025.

mengacu pada jenis-jenis pelanggaran yang diatur dalam *Budapest Convention on Cyber crime*, dapat dilihat bahwa masing-masing pelanggaran tersebut merupakan pelanggaran yang dilakukan melalui dunia maya. Menurut Pasal 14 ayat (2), selain dari pelanggaran yang tertulis dalam Pasal 2 hingga Pasal 11, langkah-langkah legislatif juga dapat diterapkan pada tindak pidana lain yang dilakukan melalui sistem komputer. Maka dari itu, dapat disimpulkan bahwa definisi *cyber crime* atau kejahatan siber adalah kejahatan yang berkaitan dengan sistem komputer atau dilakukan di dunia maya.

> Di dalam pembukaan *Budapest Convention on Cyber crime*, perancang konvensi mengingat kembali konvensi lain serta rekomendasi mengenai perlindungan data pribadi, salah satunya *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (disebut juga *Convention ETS* (*European Treaty Series*) 108) yang juga dirancang oleh Majelis Eropa. Data pribadi dalam konteks *Budapest Convention on Cyber Crime* dibahas dalam salah satu laporan Majelis Eropa, *Cyber Crime Investigation and the Protection of Personal Data and Privacy*. Menurut dokumen tersebut, *Budapest Convention on Cyber Crime* mengacu pada *Convention* ETS 108 tentang data pribadi, walaupun di dalam *Cyber Crime Convention* sendiri tidak tertulis definisi data pribadi.[38]

Jika melihat dari tujuan dokumen dan filosofi yang tertuang di pembukaan *Cyber Crime Convention*, serta konvensi dan rekomendasi yang dijadikan acuan, dapat ditarik kesimpulan bahwa data yang menjadi target dalam *cyber crime* lebih merujuk kepada data pribadi. Selain *cyber crime*, jenis operasi siber lain adalah *cyber warfare*. "Istilah *cyber warfare* atau perang dunia maya mengacu pada cara dan metode peperangan yang terdiri dari operasi siber yang berujung pada, atau

[38] Majelis Eropa, ***C****ybercrime Investigation and The Protection of Personal Data and Privacy Strasbourg Prancis 2020*, diakses melalui: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, diakses pada tanggal 1 Mei 2025.

dilakukan dalam, konteks konflik bersenjata sesuai dengan pengertian di dalam Hukum Humaniter Internasional (HHI)".[39]

Selain *Budapest Convention on Cyber Crime* dan *African Union Convention on Cyber Security and Personal Data Protection* yang belum berlaku, belum ada aturan khusus yang mengatur aktivitas di *cyber space*. *Cyber warfare* tidak diatur di dalam perjanjian internasional khusus, namun tetap diatur di bawah hukum humaniter internasional, karena dilakukan di dalam konteks konflik bersenjata. Serangan siber yang dilakukan dalam *cyber warfare* berpotensi untuk memiliki dampak humaniter. Ketika komputer atau jaringan suatu Negara diserang, disusupi, atau diblokir, mungkin ada risiko warga sipil kehilangan kebutuhan dasar seperti listrik, air minum, dan perawatan medis. "Menurut ICRC, aturan dan batasan perang berlaku pada *cyber warfare* seperti halnya dengan penggunaan senapan, artileri, dan misil".[40]

Operasi siber selanjutnya adalah *cyber espionage*, yang telah dibahas di bagian kedua kajian pustaka. Seperti kebanyakan aktivitas yang dilakukan di dunia maya, *cyber espionage* belum diatur oleh perjanjian khusus dalam hukum internasional, sehingga belum memiliki satu definisi yang pasti. Jika merujuk pada definisi tindakan illegal interception dalam *Budapest Convention on Cyber Crime*, dapat dibuat argumentasi bahwa *cyber espionage* merupakan bagian dari *cyber crime*.

> Menurut para ahli Tallinn Manual 2.0, *cyber espionage* dapat didefinisikan sebagai, "*any act undertaken clandestinely or under false pretences that*

[39] ICRC (*International Committee of the Red Cross*), *Cyber Warfare and International Humanitarian Law: The ICRC's Position*, diakses melalui: https://www.icrc.org/en/doc/assets/files /2013/130621-cyberwarfare-q-and-a-eng.pdf, diakses pada tanggal 1 Mei 2025.

[40] *Ibid.*

> *uses cyber capabilities to gather, or attempt to gather, information,"* yang berarti setiap tindakan yang dilakukan secara sembunyi-sembunyi atau dengan alasan palsu menggunakan kemampuan dunia maya untuk mengumpulkan (atau berusaha mengumpulkan) informasi.[41]

Definisi tersebut memiliki unsur-unsur yang sama dengan definisi spionase yang tertulis dalam Deklarasi Brussels 1874, serta Konvensi Den Haag 1899 dan 1907, di mana selalu tertulis kriteria "*acting clandestinely or on false pretences, he obtains or endeavours to obtain information.*" Satu-satunya hal yang membedakan definisi spionase biasa dengan *cyber espionage* adalah unsur pengambilan informasi melalui dunia maya.

"*Cyber espionage* sering kali dibedakan menjadi dua kategori, yaitu *political* dan *economic cyber espionage*, berdasarkan informasi yang diambil".[42] Dalam konteks ini, informasi yang diambil merupakan milik negara lain, dilakukan untuk mendapat keuntungan politik atau ekonomi. Hal ini yang mungkin membedakan *cyber espionage* dengan *cyber crime* seperti dimaksud dalam *Budapest Convention on Cyber Crime*; di mana *cyber crime* cenderung berhubungan dengan data pribadi, *cyber espionage* berhubungan dengan informasi rahasia atau sensitif milik suatu negara.

2.4. Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Kitab Undang-Undang Hukum Pidana

Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia telah mengatur hubungan-hubungan hukum tentang kejahatan yang berkaitan dengan komputer (*komputer crime*) yang kemudian berkembang menjadi *cyber crime.* Dasar pokok

---

[41] International Groups of Experts at the Invitation of the NATO CCDCOE, *Tallinn Manual 2.0*, Cambridge University Press, Cambridge, 2017, h. 168.

[42] Herrmann, Dominik, *Cyber Espionage and Cyber Defence***,** *Information Technology for Peace and Security,* Springer Vieweg, Wiesbaden, 2019, h. 84.

dalam menjatuhkan pidana atas pelaku *cyber espionage* di Indonesia, harus memenuhi kualifikasi perbuatan pidana. Mengingat *cyber espionage* merupakan salah satu aktvitas *cyber crime* yang dilakukan oleh *hacker*, yang merupakan kejahatan terhadap informasi seseorang, instansi ataupun lembaga yang bersifat pribadi dan rahasia sehingga penerapan Pasal-Pasal pidana haruslah tepat baik berdasarkan yang ada dalam KUHP maupun diluar KUHP karena kegiatan mata-mata ini melalui proses yang runtut.

> Moeljatno dalam bukunya tentang "Asas-asas Hukum Pidana Di Indonesia" dikatakan bahwa, untuk dapat digolongkan menjadi suatu perbuatan pidana, maka suatu perbuatan itu harus terlebih dulu dilarang dan diancam dengan pidana dalam suatu perundang-undangan yang berlaku. Persyaratan pemidanaan ini dikenal dengan sebutan asas legalitas (*principle of legality*). Dalam bahasa Latin dikenal dengan "*Nullum Delictum nulla poen sine preaviaa lege*" dan dalam bahasa Indonesia diterjemahkan sebagai tiada delik, tiada pidana tanpa peraturan lebih dahulu atau dengan kalimat sederhana "tiada suatu perbuatan yang dapat dipidana selain telah ada ketentuan-ketentuan perundang-undangan pidana yang mendahuluinya".[43]

Lebih lanjut Moeljatno menambahkan bahwa penerapan asas legalitas dalam hukum pidana Indonesia mengandung 3 (tiga) pengertian yaitu:[44]

a. Suatu perbuatan tidak dapat dipidana kalau terhadap perbuatan itu tidak ada ketentuan perundang-undangan yang mengaturnya. Hal ini nampak jelas dalam ketentuan Pasal 1 ayat (1) Kitab Undang-Undang Hukum Pidana yang berbunyi: "Tiada suatu perbuatan dapat dipidana kecuali atas kekuatan aturan pidana dalam perundang-undangan yang telah ada sebelum perbutan dilakukan".
b. Tidak boleh menggunakan analogi dalam menentukan adanya suatu perbuatan pidana. Suatu analogi terhadap aturan hukum pidana dilarang karena analogi bersifat subjektif, tidak berpegang pada aturan yang ada tetapi menggunakan ratio terhadap maksud dan inti dari aturan yang ada sehingga dapat berakibat pada ketidakadilan dalam suatu putusan pengadilan.
c. Tidak berlakunya asas retroaktif (berlaku surut) terhadap aturan-aturan hukum pidana. Namun dalam perkembangan akhir-akhir ini, telah

[43] Moeljatno, *Asas-Asas Hukum Pidana*, Cet.VII, Rineka Cipta, Jakarta, 2002, h. 23.
[44] *Ibid*, h. 25.

> diperbolehkan berlakunya asas retroaktif ini dalam batas-batas tertentu seperti terhadap pelaku kejahatan/pelanggaran Hak Asasi Manusia berat.

Berdasarkan persyaratan asas legalitas ini maka pemidanaan terhadap pelaku *cyber espionage* tentunya harus didasarkan pada sumber hukum yang berlaku saat ini yakni Kitab Undang-Undang Hukum Pidana maupun peraturan perundang-undangan lain diluar Kitab Undang-Undang Hukum Pidana yang berkaitan dengan *cyber espionage.*

Dalam hukum pidana terdapat pendekatan dalam menerapkan suatu ketentuan pidana, yang biasa dikenal dengan istilah interpretasi atau penafsiran. Tidak akan diuraikan secara menyeluruh mengenai penafsiran, namun secara lebih khusus akan akan dibahas mengenai penafsiran ekstensif. Penafsiran ekstensif adalah memperluas pengertian dari suatu istilah berbeda dengan pengertiannya yang digunakan dalam istilah sehari-hari. Mengenai penggunaan cara penafsiran ini sering terjadi perbedaan pendapat diantara para sarjana karena sukar memberi batas bagi perluasan tersebut. Hal ini menjadi perhatian karena analogi juga dikatakan sebagai perluasan pengertian atau perluasan cakupan ketentuan suatu peraturan, padahal pada umumnya analogi tidak diperbolehkan dalam hukum pidana.

Menggunakan analogi berarti menganggap sesuatu sebagai termasuk dalam pengertian dari suatu ketentuan Undang-Undang hukum pidana, karena sesuatu itu banyak sekali kemiripannya atas kesamaannya dengan ketentuan tersebut. Contoh terkenal mengenai penerapan analogi adalah kasus pencurian aliran listrik. Yang menjadi persoalan adalah, apakah aliran listrik dianggap sebagai “barang” dan apakah terjadi terjadi tindakan “mengambil”. Hooge Raad (Mahkamah Agung

negara Belanda) telah memutuskan bahwa aliran listrik termasuk dalam pengertian barang dan dengan demikian terjadi pengambilan sesuai denagan istilah yang digunakan Pasal 362 Kitab Undang-Undang Hukum Pidana, walaupun pada kenyataannya yang terjadi adalah penyalurannya. "Pertimbangan Hoge Raad adalah, bahwa maksud dari Pasal 362 adalah untuk melindungi harta orang lain, tanpa merumuskan apa yang dimaksud dengan barang. (Arrest HR tanggal 23 Mei 1921 W.10728)".[45]

Penafsiran ekstensif berbeda dengan analogi, menurut Wirjono perbedaan antara penafsiran ekstensif dengan analogi adalah : Orang masih ada di bidang penafsiran ekstensif apabila dari kata-kata suatu peraturan hukum tidak terlihat, tetapi dengan suatu cara pikiran itu disimpulkan, bahwa suatu kejadian atau peristiwa tertentu dimaksudkan turut teratur juga. "Sedangkan analogi terjadi apabila suatu penafsiran disimpulkan bahwa suatu kejadian atau peristiwa tertentu tidak turut diatur dalam suatu peraturan hukum, namun tetap saja dianggap diliputi oleh peraturan itu".[46]

Penerapan Kitab Undang-Undang Hukum Pidana terhadap tindak pidana *cyber espionage* memerlukan pemilah-milahan, perbuatan yang mana substansinya hampir sama dengan rumusan tindak pidana biasa dalam Kitab Undang-Undang Hukum Pidana, rumusan perbuatan *cyber espionage* adalah merupakan kejahatan yang menggunakan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain. Dengan memasuki jaringan komputer

---

[45] E.Y. Kanter dan S.R Sianturi, *Asas-Asas Hukum Pidana di Indonesia dan Penerapannya*, Alumni AHM-PTHM, Jakarta, 1982, h. 76.

[46] Wirjono Prodjodikoro, *Asas-Asas Hukum Pidana Indonesia*, PT Eresco, Jakarta, 1969, h. 68.

(*komputer network sistem)* pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen maupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*. Mengingat *cyber espionage* melalui proses yang runtut, maka penjatuhan pidana didasarkan pada relevansi tindak pidana yang dilakukan dari awal hingga akhir, sehingga Pasal yang dijerat pun bisa lebih dari 1 (satu).

Berdasarkana penjelasan mengenai modus operandi *cyber espionage* pada bab sebelumnya, maka ada beberapa ketentuan dalam Kitab Undang-Undang Hukum Pidana yang dapat dikenakan terhadap pelaku, diantaranya adalah aturan yang mengatur perihal ketentuan yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain yaitu dalam Pasal 167 Kitab Undang-Undang Hukum Pidana, yang rumusannya sebagai berikut:

Pasal 167

1) Barang siapa memaksa masuk ke dalam rumah, ruangan atau pekarangan tertutup dipakai orang lain dengan melawan hukum atau berada di situ dengan melawan hukum, dan atas permintaan yang berhak atau suruhannya tidak pergi dengan segera, diancam dengan pidana penjara paling lama Sembilan bulan atau paling banyak empat ribu lima ratus rupiah.
2) Barang siapa masuk dengan merusak atau memanjat, dengan menggunakan anak kunci palsu, perintah palsu, atau pakaian jabatan palsu atau barang siapa tidak setahu yang berhak lebih dulu bukan karna kekhilafan masuk dan kedapatandi situ pada waktu malam, dianggap memaksa masuk.
3) Jika mengeluarkan ancaman atau menggunakan sarana yang dapat menakutkan orang, diancam dengan pidana penjara paling lama satu tahun empat bulan.
4) Pidana tersebut dalam ayat (1) dan ayat (3) ditambah sepertiga jika yang melakukan kejahatan dua orang atau lebih dengan bersekutu.

Sebagaimana kita ketahui bahwa konvergensi teknologi (komputer, komunikasi dan informasi), yang terwujud dalam bentuk internet, dimana isu privasi merupakan suatu hal yang tidak bisa ditawar lagi. Jika terjadi suatu

penuyusupan terhadap suatu sistem komputer dan disaat yang bersamaan tindakan tersebut telah terdeteksi oleh pemilik sistem, tindakan tersebut dapat dikategorikan sebagai suat kejahatan jika dampak yang ditimbulkan menimbulkan kerugian pada orang lain. Unsur-unsur yang dapat ditemukan dalam Pasal 167 Kitab Undang-Undang Hukum Pidana sebagai berikut:

1) Unsur Subjektif

   Unsur subjektif yang dimaksud dengan Pasal 167 Kitab Undang-Undang Hukum Pidana adalah tiada kekhilafan atau ringkasnya adanya suatu kesengajaan dalam melakukan perbuatan tersebut. Jika kita kembali melihat Kitab Undang-Undang Hukum Pidana (R.Sesilo), perbuatan tersebut dilakukan dengan kesengajaan, dimana pelaku terdeteksi (diketahui) dan setelah diperingati tidak dihindarkan oleh yang bersangkutan. Dari rumusan tersebut kiranya dapat ditarik kesimpulan bahwa adanya suatu kesengajaan dalam tindakan tersebut. Jika Kitab Undang-Undang Hukum Pidana diterapkan dalam *cyber espionage* ini, maka sifat kesengajaan dari perbuatan tersebut perlu dibuktikan di siding pengadilan, dan jika terbukti maka pelaku (*hacker*) baru dapat dipidana. Kesengajaan menurut doktin dalam hukum pidana terbagi atas:[47]

   a. Kesengajaan sebagai maksud atau tujuan. Yakni terjadinya suatu tindakan atau maksud atau akibat tertentu (sesuai dengan perumusan Undang-Undang Hukum Pidana) kesengajaan dengan kesadaran kepastian atau keharusan
   b. Seberapa jauh pengetahun atau kesadarn pelaku tentang tindakan dan akibat yang merupakan salah satu unsur dari pelaku delik. Disini termasuk tindakan atau akibat tersebut harus pasti terjadi.

[47] Edmon Makarim, *Kompilasi Hukum Telematika*, Cet.2, PT Raja Grafindo Persada, Jakarta, 2004, h. 409.

c. Kesengajaan dengan kesadaran kemungkinan, yakni kesengajaan dengan gradasi terendah, bahkan sering sukar untuk membedakan dengan culpa, yang menjadi sandaran adalah sejauh mana pengetahuan atau pelaku, tentang akibat dan tindakan yang dilarang beserta tindakan lainnya yang mungkin akan terjadi.

2) Unsur Objektif

Memasuki wilayah dalam hal ini wilayah fisik (rumah, ruangan, pekarangan tertutup). Sifat fisik ini yang membatasi aturan pidana Kitab Undang-Undang Hukum Pidana dapat diterapkan, *cyber space* bukanlah wilayah fisik seperti yang kita bayangkan. Oleh sebab itu perlu adanya perubahan makna, jangan lagi sifat fisik dari *cyber space* diajdikan perdebatan, tetapi pada "tindakan atau perbuatan masuk melawan hukumnya." Dunia maya (*cyber space*) yang bersifat tidak nyata ini menjadikan tindakan yang bersifat fisik tidak lagi dijadikan sandaran bahwa pelaku telah melakukan tindak pidana. Unsur barangsiapa tetap dijadikan patokan, hanya cara yang dilakukantidak lagi langsung pada objek fisik, tindakan yang dimaksud disini berupa suatu jejak elektronik (*electronic path*) yang berisikan *log file*, angka atau data matematis yang mengindikasikan telah berlangsung aktivitas elektronik.

Pasal lain yang berkaitan dengan perbuatan memasuki atau melintasi wilayah orang lain adalah Pasal 551 Kitab Undang-Undang Hukum Pidana, yang berbunyi: Barang siapa tanpa wewenang berjalan atau berkendaraan dia atas tanah yang oleh pemiliknya dengan cara jelas dilarang memasukinya, diancam dengan pidana denda paling banyak dua ratus dua puluh lima rupiah.

Jika dilihat dari susunan kata perkatanya saja, kesimpulan yang dapat ditarik dari Pasal ini adalah bahwa Pasal ini melarang orang yang berjalan atau berkendaraan di atas tanah orang lain yang nyata-nyata sudah diberi tanda larangan bahwa tanah itu tidak boleh dilalui. Namun demikian, apabila dilakukan kajian perluasan konsepsi, tanah identik dengan ruang atau fasilitas sistem komputer karena memiliki kesamaan sifat yaitu properti. Berjalan atau berkendara di atas tanah tanpa ijin meski sudah ada larangan dapat disamakan sebagai akses kepada fasilitas komputer tanpa ijin. Penggunaan *user-id*, *password* dan alat verifikasi lainnya dapat disamakan sebagai alat masuk tanpa ijin.

Berkaitan dengan Pasal diatas, ada beberapa hal yang tidak sesuai lagi untuk diterapkan dalam upaya penanganan hukum siber jenis *cyber espionage* yang sangat ringan (dapat mengganti pidaan kurungan) padahal *cyber espionage* yang umumnya terjadi dapat merugikan financial yang tidak sedikit.

Apabila berhubungan dengan kaamanan negara, Kitab Undang-Undang Hukum Pidana hannya mengatur spionase terhadap negara yang cenderung dilakukan secara konvensional pada saat perang, yakni terdapat dalam Pasal 124 ayat (2) dan 126 Kitab Undang-Undang Hukum Pidana. Pada Pasal 124 ayat (2) Kitab Undang-Undang Hukum Pidana dirumuskan bahwa:

Pasal 124 ayat (2)

> Diancam dengan pidana penjara seumur hidup atau selama waktu tertentu atau paling lama dua puluh tahun jika si pembuat:
> 1. Memberitahukan atau memberikan kepada musuh peta, rencana, gambar, atau penulisan mengenai bangunan-bangunan tentara;
> 2. menjadi mata-mata musuh, atau memberikan pondokan kepadanya.

Ketentuan lain yang berkaitan dengan tindak pidana *cyber espionage* apabila perbuatan seseorang itu menyangkut bocornya data keluar terutama

mengenai data yang harus dirahasiakan (*data leakage*) maka ketentuan yang dapat diterapkan adalah ketentuan yang berkaitan dengan perbuatan membocorkan suatu rahasia. Ketentuan yang berkaita dengan membcorkan suatu rahasia negara (termasuk di dalamnya perbuatan dengan menggunakan sarana internet) diatur dalam Pasal 112, Pasal 113 dan Pasal 114 Kitab Undang-Undang Hukum Pidana serta perbuatan yang membocorkan rahasia perusahaan yang diatur dalam Pasal 322 dan Pasal 323 Kitab Undang-Undang Hukum Pidana.

Pasal 112

> Barang siapa dengan sengaja mengumumkan surat-surat, berita-berita atau keterangan- keterangan yang diketahuinya bahwa harus dirahasiakan untuk kepentingan negara, atau dengan sengaja memberitahukan atau memberikannya kepada negara asing, diancam dengan pidana penjara paling lama tujuh tahun.

Pasal 113

1) Barang siapa dengan sengaja, untuk seluruhnya atau sebagian mengumumkan, atau memberitahukan maupun menyerahkan kepada orang yang tidak berwenang mengetahui, surat-surat, peta-peta, rencana-rencana, gambar-gambar atau benda benda yang bersifat rahasia yang bersangkutan dengan pertahanan atau keamanan Indonesia terhadap serangan dari luar, yang ada padanya atau yang isinya, bentuknya atau susunanya benda- benda itu diketahui olehnya, diancam dengan pidana penjara paling lama empat tahun.
2) Jika surat-surat atau benda-benda ada pada yang bersalah, atau pengetahuannya tentang itu karena pencariannya, pidananya dapat ditambah sepertiga.

Pasal 114

> Barang siapa karena kesalahannya (kealpaannya) menyebabkan surat-surat atau benda- benda rahasia sebagaimana yang dimaksudkan dalam Pasal 113 harus menjadi tugasnya untuk menyimpan atau menaruhnya, bentuk atau susunannya atau seluruh atau sebagian diketahui oleh umum atau dikuasai atau diketahui oleh orang lain (atau) tidak berwenang mengetahui, diancam dengan pidana penjara paling lama satu tahun enam bulan atau pidana kurungan paling lama satu tahun atau pidana denda paling tinggi empat ribu lima ratus rupiah.

Pasal ini merupakan ketentuan yang berkaitan dengan perbuatan pembocoran rahasia negara yang sering kali bersinggunangan dengan masalah spionase. Kaitannya dengan kejahatan siber khususnya dengan *cyber espionage* adalah pembukaan rahasia negara dapat dilakukan kepada pihak yang tidak berwenang untuk menerima rahasia tersebut. Untuk masuk dalam suatu terminal yang berisikan rahasia negara memang dibutuhkan suatu keahlian khusus tetapi bukan berarti hal yang tidak mungkin dapat dilakukan karena basis data pemerintah saat ini banyak yang menggunakan kecanggihan teknologi *e-government*. Unsur kesengajaan pada Pasal 1 ini diancam pidana paling lama 7 (tujuh) tahun.

Sedangkan membocorkan rahasia perusahaan dapat dikaterorikan sebagai kejahatan membuka rahasia, sehingga si pelaku dapat diancam dengan pidana berdasarkan Pasal 322 dan Pasal 323 Kitab Undang-Undang Hukum Pidana.

Pasal 322
1) Barang siapa dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya, baik yang sekarang maupun yang dahulu, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah.
2) Jika kejahatan dilakukan terhadap seorang tertentu, maka perbuatan itu hanya dapat dituntut atas pengaduan orang itu.

Pasal 323
1) Barang siapa dengan sengaja memberitahukan hal-hal khusus tentang suatu perusahaan dagang, kerajinan atau pertanian, di mana ia bekerja atau dahulu bekerja, yang harus dirahasiakannya, diancam dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak sembilan ribu rupiah.
2) Kejahatan ini hanya dituntut atas pengaduan pengurus perusahaan itu.

Perkembangan teknologi informasi bagi kegiatan suatu negara ataupun perusahaan seperti menyimpan surat-surat atau menyimpan benda-benda rahasia ke dalam *data base* atau *storage* yang berupa data merupakan suatu sisi positif

dari dari kehadiran teknologi informasi itu sendiri. Suatu data dapat juga mengenai organisasi kenegaraan atau produksi mengenai metode dan bahan baku serta angka produksi perusahaan dan sebagainya. Tetapi manakala data ini jatuh ke pihak ketiga yang tidak berwenang untuk menerima, mengetahui atau mendapatkannya maka hal tersebut dapat merugikan dan membahayakan bagi kelangsungan dari perusahaan yang bersangkutan.

Selain sanksi pidana yang dikenakan untuk delik atau tindak pidana yang telah selesai dilakukan, Kitab Undang-Undang Hukum Pidana juga mengatur mengenai percobaan kejahatan tindak pidana sebagaimana yang tertulis pada Pasal 53 (1) Kitab Undang-Undang Hukum Pidana yang berbunyi: " Mencoba melakukan kejahatan dipidana, jika niat untuk itu telah ternyata dari adanya permulaan pelaksanaan, dan tidak selesainya pelaksanaan itu, bukan semata-mata disebabkan karena kehendaknya sendiri". Unsur-unsur yang pada Pasal tersebut adalah : 1) adanya niat; 2) adanya permulaan pelaksanaan; 3) tidak selesainya tindak kejahatan tersebut bukan karena kehendaknya sendiri

Pasal tersebut apabila dikatkan dengan tindak pidana di bidang teknologi informasi khususnya tindak pidana *cyber espionage*, maka relevansinya adalah apabila pelaku atau *hacker* berdasarkan modus operandi sebagaimana telah dijelaskan pada bab sebelumnya telah berhasil memasuki akses jaringan internet atau komputer milik pihak lain dengan niat untuk memata-matai data dengan didahului kegiatan pencariaan data (*footprinting*), pemilihan sasaran (*scanning*) dan/atau pencarian data mengenai sasaran (*enumerasi*), namun belum sampai pada tahap *cyber espionage* atau memata-matai data bukan karena kehendaknya

sendiri, maka pelaku dapat dikenakan Pasal ini karena spionase sendiri merupakan tindak pidana kejahatan bukan pelanggaran.

2.5. Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik

Tindak pidana *cyber espionage* ini merupakan Tindak Pidana khusus yang artinya dari segi hukum materiilnya menyimpangi Kitab Undang-Undang Hukum Pidana (KUHP), sedangkan dari sisi hukum formilnya masih mengikuti ketentuan yang ada dalam Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Sebelum disahkannya Undang-Undang Informasi dan Transaksi Elektronik, penanganan atas tindak pidana *cyber espionage* belum mendapat payung hukum yang jelas. Hal ini disebabkan belum ada satupun Undang-Undang yang mengatur tentang tindak pidana *cyber espionage* secara eksplisit. Kitab Undang-Undang Hukum Pidana hanya mengatur tentang tindak pidana spionase konvensional dan tindak pidana-tindak pidana yang dapat ditafsirkan secara ektensif sebagai tindak pidana *cyber espionage*.

Penggunaan Pasal-Pasal yang sudah tidak sesuai lagi atau dapat dikatakan kurang tepat dapat menyulitkan aparat dalam menjerat pelaku, tidak saja dikarenakan hukum materiilnya yang tidak mengakomodir bentuk baru dari kejahatan spionase atau mata-mata ini, tetapi juga hukum formil yang bersumber dari Kitab Undang-Undang Hukum Acara Pidana belum mengenal adanya alat bukti digital. Padahal sebagian besar barang bukti yang didapat dari penyidikan tindak pidana *cyber espionage* berbentuk digital. Secara yuridis kegiatan *cyber space* tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional

saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum.

Setelah disahkannya Undang-Undang informasi dan transaksi elektronik ini maka terbentuklah payung hukum para aparat penegak hukum untuk menangkap dan menjerat pelaku kejahatan ini. Manfaat yang dapat diambil dengan adanya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik adalah: 1) Menjamin kepastian hukum bagi masyarakat; 2) Mendorong pertumbuhan ekonomi; 3) Sebagai salah satu upaya untuk mencegah terjadinya kejahatan berbasis teknologi informasi; dan 4) Melindungi masyarakat pengguna jasa dengan memanfaatkan teknologi informasi.

Di dalam Undang-Undang Informasi dan Transaksi Elektronik, *cyber espionage* diatur dalam Pasal 30 ayat (2) yang berbunyi: Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen Elektronik dikenai sanksi pidana berdasarkan Pasal 46 ayat (2) yang berbunyi: Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).

Hacker yang melakukan aksi mata-mata atau *cyber espionage* untuk mendapatkan informasi dari hasil mengakses komputer secara *illegal* memenuhi unsur-unsur yang ada dalam rumusan Pasal 30 ayat (2) Undang-Undang ini. Sedangkan untuk orang (*hacker*) yang dengan sengaja memfasilitasi orang lain

agar bisa mengetahui ataupun mengakses informasi yang bukan haknya sebagaimana yang terjadi pada kasus pembuat *Spyware* jenis *Lover Spy*, maka dapat dikenakan Pasal 32 ayat (2) dan Pasal 34 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yakni: Setiap orang dengan sengaja dan tanpa hak atau melawan hukumdengan cara apa pun memindahkan atau mentrasfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik orang lain yang tidak berhak.

Pasal 34 ayat (1):

> Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untukm digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :
>
> a. Perangkat keras atau perangkat lunak computer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;
> b. Sandi lewat computer, kode akses, atau hal yang sejenis dengan ituyang ditujukan agar system Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Undang-Undang Informasi dan Transaksi Elektronik selain mengatur mengenai tindak pidana terhadap perbuatan *cyber espionage* itu sendiri, juga mengatur mengenai subjek yang melakukan tindak pidana tersebut, yankni yang dilakukan oleh perorangan maupun oleh korporasi. Adanya pengaturan tersebut berimplikasi pada pidana yang akan dijatuhkan, sebagaimana yang tercantum pada Pasal 52 ayat (4) yakni : “Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua per tiga”.

Mengenai percobaan, Undang-Undang Informasi dan Transaksi Elektronik tidak mengatur secara tersendiri, oleh sebab itulah maka secara otomatis berlaku

ketentuan Pasal 86 Kitab Undang-Undang Hukum Pidana. Berdasarkan Pasal 86 Kitab Undang-Undang Hukum Pidana, maka jika di dalam suatu Undang-Undang diatur tentang tindak pidana kejahatan didalamnya termasuk ketentuan tentang percobaan. Dengan dmikian, meskipun Undang-Undang Informasi dan Transaksi Elektronik tidak mengatur tentang percobaan, maka siapapun yang mencoba melakukan tindak pidana di bidang Informasi dan Transaksi Elektronik, akan tetap dijatuhi pidana dengan ancaman maksimum pidana pokok dikurangi sepertiga. Hal ini sesuai dengan Pasal 53 dan Pasal 56 Kitab Undang-Undang Hukum Pidana.

Berbeda dengan Percobaan yang masih menggunakan ketentuan yang ada dalam Kitab UndangUndang Hukum Pidana, hal lain yang diatur secara khusus pada Undang-Undang Informasi dan Transaksi Elektronik adalah mengenai hukum acara formil atas tindak pidana siber (*cyber crime*). Terutama mengenai alat bukti yang digunakan dalam tindak pidana siber ini. Hal ini berdasarkan Pasal 44 yang berbunyi :

Pasal 44

Alat bukti penyidikan, penuntutan, dan pemerikasaan di siding pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. Alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
b. Alat bukti berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angkan 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

2.6. Pengaturan Tindak Pidana *Cyber Espionage* Berdasarkan Undang-Undang Telekomunikasi

Di bidang komunikasi yang merupakan bagian dari teknologi komunikasi, ketentuan yang mengatur tentang tindak pidana kejahatan telekomunikasi sudah

diatur dalam Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang berbunyi: “Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atua memanipulasi: a) Akses ke jaringan telekomunikasi; dan atau b) Akses ke jasa telekomunikasi; dan atau c) Akses atau jaringan ke telekomunikasi khusus”.

Unsur-unsur dalan Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi antara lain: a) Setiap orang; b) Dilarang; c) Melakukan perbuatan tanpa hak; d) Tidak sah; e) Memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi dan atau akses ke jaringan telekomuniksi khusus. Pada Pasal ini tidak tidak secara langsung menggunakan kata cyber espionage dalam rumusan Pasalnya, tetapi mengatur mengenai akses tidak sah ,sehingga aksi *hacker* yang melakukan spionase untuk mengintai atau memata-matai data melanggar ketentuan Pasal ini.

Penekanan dari Pasal ini adalah larangan terhadap akses tidak sah kepada jaringan dan jasa telekomunikasi. Pada kenyataannya dan sesuai dengan definisi telekomunikasi (Pasal 1 Undang-Undang Nomor 36 Tahun 1999) tidak ada perbedaan lagi antara jaringan dan jasa telekomunikasi dengan jaringan dan jasa teknologi informasi, karena di dalamnya juga selalu ada jaringan komputer. Oleh karena itu tindakan mengakses sistem komputer dengan tidak sah dapat dikenai tuntutan pidana sebagaimana dimaksud dalam Pasal 50 yang berbunyi: “Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda peling banyak Rp.600.000.000,- (enam ratus juta rupiah)”.

Penekanan sanksi pidana pada pelanggar akses tidak sah, dengan tuntutan pidana penjara serta denda sesuai dengan Pasal 50, menguatkan pentingnya jaminan keamanan terhadap data-data yang secara *computerized* patut untuk dilindungi, sehingga tindakan apapun yang dilakukan *hacker* pada sebuah jaringan komputer khusunya internet tanpa kewenangan patut ditindak secara tegas.

2.7. Pengaturan Kejahatan *Cyber Espionage* Berdasarkan Hukum Positif di Indonesia

Pengaturan kejahatan *cyber espionage* berdasarkan hukum positif yang ada di Indonesia menunjukkan bahwa regulasi yang tersedia masih bersifat umum dan belum secara spesifik mengatur jenis kejahatan ini. *Cyber espionage*, atau spionase siber, adalah tindakan memperoleh data rahasia melalui jaringan komputer tanpa izin, biasanya untuk kepentingan politik, militer, atau ekonomi.

> Menurut Prof. Barda Nawawi Arief menyatakan bahwa *cyber* atau siber merupakan suatu istilah untuk menjelaskannya dengan istilah "mayantara". *Cyber* juga dapat diartikan dari bahasa Inggris sebagai suatu istilah "maya, tidak nyata, tidak terlihat, terawang, terawang, tidak ada bentuk". Dengan mengartikan *cyber espionage* dalam penjelasan yang lebih komprehensif, perlu juga di maknai apa itu spionase dan elemen-elemen yang menjadi parameter dalam tindakan spionase.[48]

Di Indonesia, pengaturan terkait kejahatan ini secara tidak langsung dapat ditemukan dalam beberapa peraturan, namun belum mencakup secara komprehensif. Diantaranya sebagai berikut:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, menjadi dasar hukum utama dalam menindak kejahatan

[48] Aldo Rahmandana, *Tinjauan Yuridis Cyber Espionage Berdasarkan Hukum Internasional*, Jurnal Jurist-Diction, Vol.4, No.6, 2021, h. 2143.

berbasis teknologi informasi. Namun, Undang-Undang Informasi dan Transaksi Elektronik lebih fokus pada akses ilegal, penyadapan, perusakan sistem elektronik, dan pencurian data, tanpa secara eksplisit mengatur tindakan *cyber espionage* yang melibatkan spionase terhadap negara atau perusahaan.

2. Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara memuat larangan terhadap tindakan yang mengancam keamanan negara, termasuk kegiatan spionase, tetapi tidak memberikan rincian mengenai bentuk kejahatan siber sebagai salah satu modus spionase.
3. Kitab Undang-Undang Hukum Pidana sendiri belum secara memadai mengatur kejahatan siber, karena merupakan produk hukum yang lahir sebelum era digital. Beberapa Pasal tentang pengkhianatan atau pencurian informasi negara memang ada, namun tidak relevan dengan karakteristik *cyber espionage* modern yang sering dilakukan secara anonim dan melintasi batas negara.
4. Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme pun belum menyentuh ranah spionase siber, meskipun dapat terkait secara tidak langsung bila *cyber espionage* digunakan untuk kepentingan aksi terorisme.

Dengan demikian, analisa terhadap hukum positif yang ada menunjukkan adanya kekosongan normatif dan belum adanya regulasi khusus yang secara tegas dan terperinci mengatur *cyber espionage* sebagai tindak pidana tersendiri. Untuk menjamin kepastian hukum dan efektivitas penegakan hukum terhadap kejahatan

ini, dibutuhkan pembaruan hukum, baik melalui revisi Undang-Undang yang ada maupun pembentukan instrumen hukum baru yang spesifik mengatur kejahatan siber lintas negara dan berdimensi intelijen seperti *cyber espionage*.