TINDAKAN SPIONASE MELALUI PENYADAPAN ANTAR NEGARA SEBAGAI *CYBERCRIME*

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Syarat-Syarat Memperoleh Gelar Kesarjanaan Dalam Ilmu Hukum

Oleh:

ROFI'A ZULKARNAIN

NIM. 105010107111092

KEMENTRIAN PENDIDIKAN DAN KEBUDAYAAN

UNIVERSITAS BRAWIJAYA

FAKULTAS HUKUM

MALANG

2014

DAFTAR ISI

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Saat ini duniadalam kondisi yang lazim disebut globalisasi, dimana hubungan antar subyek seolah-olah tanpa batas (*borderless*).[1] Globalisasi ini didukung oleh kemajuan teknologi dan informasi yang sangat pesat dengan sumber daya manusia (SDM) yang semakin kreatif demi untuk memenuhi kebutuhan yang semakin kompleks. Untuk menghubungi kolega yang jaraknya beribu-ribu kilo meter cukup dengan tekan angka-angka yang ada pada *handphone*, untuk berdagang dengan mitra bisnis yang berbeda Benua juga tidak perlu repot dengan datang ke lokasi yang dimaksud, cukup menggunakan fasilitas perdagangan elektronik (*e-commerce*). Untuk melakukan aktivitas perbankan juga tidak perlu datang ke bank, cukup memanfaatkan kecanggihan teknologi *e-banking* dan banyak hal lain yang terasa sangat mudah untuk dilakukan dibanding sebelumnya.[2]

Jaringan*borderless*merupakan jaringan yang disediakan untuk memudahkan pengguna internet agar dapat mengakses informasi seluas-luasnya.[3] Perpaduan antara teknologi komputer dan teknologi telekomunikasi membentuk sebuah piranti baru dengan nama internet.

---

[1]Tim Dosen Fakultas Hukum Universitas Brawijaya, 2011, **Ketika Hukum Berhadapan Dengan Globalisasi**, UB Press, Malang, hlm. V.

[2]Ibid, hlm. V.

[3]Intan Innayatun Soeparna, **KejahatanTelematikaSebagaiKejahatanTransnasional**, http://www.academia.edu/208360/Kejahatan_Telematika_sebagai_Kejahatan_Transnasional, tertanggal 22 September 2013

Pada intinya, internet merupakan jaringan komputer yang terhubung satu sama lain melalui media komunikasi, seperti kabel telepon, serat optic, satelit atau gelombang frekuensi.[4]

Di dalam jaringan *borderless* bukan hanya ada individu atau perorangan yang menjadi subjek, negara juga termasuk. Sama halnya dengan individu, cara negara berhubungan dengan negara lain kini makin maju dengan internet dan jaringan telekomunikasi lain. Meskipun dalam hal ini kegiatan diwakili oleh orang, namun dilakukan atas nama negara. Menghubungi kepala negara lain, perdana menteri, atau menteri luar negeri hanya perlu menggunakan telepon. Mengirim surat menggunakan surat elektronik atau *e-mail,* lebih mudah dari sebelumnya yang harus mengirim surat menggunakan jasa pengiriman sehingga memakan waktu lama jika letak negara yang dituju jauh. Selain itu, juga bermafaat sebagai media publikasi mengenai konvensi-konvensi baru yang dibuat dan diratifikasi oleh negara-negara dalam hal perjanjian internasional serta peraturan-peraturan baru yang dibuat oleh pemerintah dalam satu negara.

Sejauh ini globalisasi serta kemajuan teknologi memberikan dampak positif maupun negatif. Salah satu dampak positif yangdidapat yaitu menghemat waktu karna berhubungan dengan orang lain dari tempat yang jauh hanya dengan waktu yang sangat singkat. Dampak negatifnya adalah bahwa dalam globalisasi dan kemajuan teknologi komunikasi ini terdapat penyalahgunaan teknologi, terutama dalam teknologi komunikasi. Era globalisasi dan teknologi informasi membawa pengaruh terhadap munculnya berbagai bentuk kejahatan yang sifatnya

---

[4]Agus Raharjo. 2002. ***Cybercrime*, Pemahaman dan Upaya Pencegahan kejahatanBerteknologi.** Bandung: Citra Aditya Bakti. Hal. 59.

baru.[5] Jaringan *borderless* digunakan sebagai alat untuk melakukan perbuatan yang bertentangan hukum. Umumnya kejahatan yang berhubungan dengan teknologi atau *cybercrime* merupakan kejahatan yang menyangkut harta benda dan/atau kekayaan intelektual. Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer.[6]

Dalam kondisi globalisasi dengan jaringan komunikasi yang bersifat *borderless,* dimana hubungan antar negara sudah jauh lebih mudah dari sebelumnya, suatu negara dapat mengalami permasalahan dengan negara lain yang menjadi mitra atau negara sahabatnya. Masalah yang terjadi antara negara bermacam-macam, mulai dari masalah yang biasa hingga masalah yang bisa menimbulkan permusuhan.Salah satu masalah yang sedang terjadi antar negara saat iniadalah masalah penyadapan, yaitupenyadapan intelejen Australia terhadap presiden RI dan beberapa Menteri serta terhadap beberapa negara di Asia lainnya.

Menurut Undang-undang No 36 tahun 1999 tentang Telekomunikasi, penjelasan pasal 40;

> *"Yang dimaksud dengan penyadapan dalam pasal ini adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Pada dasarnya informasi yang dimiliki oleh seseorang adalah hak pribadi yang harus dilindungi sehingga penyadapan harus dilarang."*

Kemudian, definisi penyadapan yang sah secara hukum menurut *European Telecommunications Standards Institute* (ETSI) yaitu kegiatan penyadapan

---

[5]Didik M. Arief Mansur dan Elisatris Gultom, 2005, ***Cyber Law*: Aspek Hukum Teknologi Informasi**, Refka Aditama, Bandung, hlm. 19.

[6]Didik M. Arief Mansur dan Elisatris Gultom, *Ibid*, hlm.7.

dilakukan terhadap *network operator*, akses *provider*, *service provider* dengan tujuan agar informasi yang ada selalu siap digunakan sebagai fasilitas kontrol pelaksanaan hukum.[7] Penyadapan pada dasarnya hanya dibolehkan bagi petugas yang berwenang dalam suatu negara guna meningkatkan pengawasan tingkat tinggi dan dilakukan sepenuhnya untuk kepentingan keamanan negara agar mampu mempertahankan dan meningkatkan kemampuan melawan tindakan teror. Kewenangan penuh untuk menerapkan penyadapan yang sah secara hukum tersebut dikenal dengan istilah lawful interception.[8]

Dari beberapa media informasi, didapatkan bahwa kegiatan penyadapan Australia terhadap beberapa negara di Asia termasuk Indonesia dilakukan dengan bekerjasama dengan Amerika Serikat.Menanggapi kejadian tersebut, Presiden SBY menuntut Perdana Menteri Australia untuk segera meminta maaf dan menjelaskan alasan mengapa melakukan penyadapan. Selain itu Presiden SBY juga mengancam akan mengusir perwakilan diplomatik Australia di Indonesia. Dalam prakteknya tidak mungkin akan dilakukan penjelasan mengapa intelejen Australia melakukan penyadapan karena mencari informasi dengan memata-matai adalah sewajarnya pekerjaan dari intelejen. Yang menjadi masalah adalah spionase dilakukan dalam masa damai, bukan dalam keadaan perang. Spionase dilakukan dengan cara menyadap *handphone* milik Presiden RI, kegiatan ini dipusatkan di kantor kedutaan Australia di Indonesia. Hukum positif Indonesia tidak mengatur secara rinci mengenai tindakan spionase dalam Undang-undang tersendiri, namun hal ini diatur di dalam Undang-undang tentang teknologi dan

[7] Firman Nuro, **Aspek Hukum Mengenai Monitoring Aktivitas Komputer dan Tindak Pidana Penyadapan Data Pribadi Pengguna Internet**, jbptunikompp-gdl-firmannuro-24692-4-babii.pdf, hlm. 22. (Diakses 28 Februari 2014)

[8] Firman Nuro,*Ibid*, hlm 22-23.

informasi.Selain itu, Indonesia juga merupakan negara anti spionase.Dalam Undang-undang tentang teknologi dan informasi spionase merupakan kejahatan dunia maya atau *cybercrime.*

Selain spionase yang dilakukan Australia kepada Indonesia dan beberapa negara di Asia Tenggara, kemarahan dunia internasional atas dugaan spionase yang dilakukan Badan Keamanan Nasional (NSA) Amerika Serikat (AS) memuncak.Jerman dan Brazil, sebagian dari negara yang merasa jadi korban spionase NSA merancang resolusi PBB untuk mengakhiri kegiatan spionase yang berlebihan itu. Di Eropa, selain Jerman, Perancis juga berang atas ulah NSA. Sebuah laporan dari media Perancis, Le Monde,mengungkap, 70 juta lebih komunikasi telepon rakyat Perancis disadap NSA. Belum reda kemarahan Perancis, media itu kembali melansir laporan, komunikasi diplomat Perancis di PBB dan Washington juga disadap.Spanyol, yang belum memiliki bukti telah dimata-matai AS, juga berniat memanggil Duta Besar AS yang berada di Spanyol. Di Amerika Latin, selain Brazil, Meksiko juga jadi korban spionase AS. Pemerintah Meksiko marah setelah laporan NSA memata-matai presiden mereka pada tahun 2010 terbongkar. E-mail Felipe Calderon yang pada 2010 menjabat sebagai Presiden Meksiko, disadap oleh NSA. Seperti itulah yang diberitakan dalam sindonews.com pada Sabtu, 26 Oktober 2013.[9]

Hal ini mudah diputuskan apabila subjek dan objek dari spionase ini merupakan individu atau kelompok dalam satu negara. Yang menjadi pertanyaan adalah jika kegiatan spionase yang dilakukan oleh antar negara terhadap negara

[9] Muhaimin, **FOKUS DUNIA: Kemarahan dunia atas spionase AS memuncak,**http://international.sindonews.com/read/2013/10/26/45/798548/kemarahan-dunia-atas-spionase-as-memuncak, tertanggal 9 Desember 2013.

dengan catatan bahwa spionase merupakan suatu *cybercrime* menurut negara yang menjadi objek spionase, tetapi di sisi lain spionase bukan merupakan merupakan suatu *cybercrime* di negara yang melakukan siponase. Dalam dunia internasional pun belum ada konvensi khusus yang mengatur spionase secara terperinci. Namun beberapa negara anti-spionase telah mengusulkan PBB agar mengeluarkan resolusi anti spionase antar negara atau *Anti-Spying Resolution* dengan harapan tidak ada lagi tindakan spionase melalui cara apapun termasuk melalui penyadapan. Dari permasalahan tersebut maka penulis mengambil judul **TINDAKAN SPIONASE MELALUI PENYADAPAN ANTAR NEGARASEBAGAI *CYBERCRIME*** sebagai penelitian penulisan skripsi.

B. RUMUSAN MASALAH

1. Apakah tindakan spionase memalui penyadapan antar negara termasuk sebagai *cybercrime*?
2. Bagaimana upaya Indonesia dalam mengatasi tindakan spionase melalui penyadapan antar negara seperti yang telah dilakukan Australia?

C. TUJUAN PENELITIAN

1. Untuk mengetahui tindakan spionase santar negara temasuk sebagai *cybercrime*.
2. Untuk mengetahui upaya Indonesia dalam mengatasi tindakan spionase melalui penyadapan antar negara seperti yang telah dilakukan Australia

D. MANFAAT PENELITIAN

1. Manfaat Teoris

Memberikan pengetahuan dan pemahaman atas masalah yang timbul dalam ruang lingkup hukum internasional yaitu hubungan antar negara khususnya dalam hal spionase melalui penyadapan antar negara merupakan salah satu bentuk dari *cybercrime*.

2. Manfaat Praktis

a. Bagi Akademisi

Memberikan pengetahuan serta referensi bagi sesama akademisi mengenai tindakan spionase melaui penyadapan antar negara sebagai *cybercrime*.

b. Bagi Pemerintah

Memberikan masukan kepeada pemerintah RI agar dapat lebih tegas dalam menangani permasalahan Internasional, terutama menyangkut keamanan dan hubungan internasional.

c. Bagi Penulis

Menambah pengetahuan penulis akan permasalahan internasional terutama mengenai kejahatan dunia maya yang dilakukan oleh negara. Selain itu juga Penulisan ini merupakan syarat Penulis untuk mendapat gelar kesarjanaan.

E. SISTEMATIKA PENULISAN

BAB I : PENDAHULUAN

Berisi tentang latar belakang yang mendasari dilakukannya penelitian, perumusan masalah yang enjadi persoalan yang jawabannya ingin diketahui oleh peneliti,

tujuan penelitian yang merupakan maksud dari diadakannya penelitian serta manfaat dan sistematika penulisan yang digunakan.

BAB II : KAJIAN PUSTAKA

Berisi penguraian kajian teori-teori ilmiah yang berhubungan dengan pokok permasalahan yang dipermasalahkan dan yang akan dipakai dalam analisis, hasil-hasil kajian ilmiah lain yang berhubungan dengan apa yang dipermasalahkan, dan rangkuman hasil-hasil kajian teori yang berkaitan dengan permasalahan.

BAB III : METODE PENELITIAN

Berisi tentang metode pendekatan yang digunakan, jenis dan sumber bahan hukum, teknik memperoleh bahan hukum, teknik analisis bahan hukum serta definisi konseptual.

BAB IV : HASIL DAN PEMBAHASAN

Menguraikan hasil penelitian atau pembahasan tentang kegiatan spionase melalui penyadapan sebagai cybercrime yang dilakukan negara kepada negara lain menurut hukum internasional.

BAB V : PENUTUP

Berisi kesimpulan dan saran. Kesimpulan merupakan uraian jawaban dari rumusn masalah yang telah dianalisis di dalam pembahasan. Serta saran yang berisi harapan-harapa mengenai hasil kajian ke arah yang lebih baik untuk masa yang akan datang.

BAB II

KAJIAN PUSTAKA

A. Tinjauan Umum Hukum Internasional

Pengertian Hukum Internasional

Pada umumnya hukum internasional diartikan sebagai himpunan dari peraturan-peraturan dan ketentuan-ketentuan yang mengikat serta mengatur hubungan antar negara-negara dan subjek-subjek hukum internasional lainnya dalam kehidupan masyarakat internasional.[1] Hukum Internasional adalah hukum yang mengatur pelaku-pelakunya secara sejajar, yang pada hakikatnya merupakan pantulan nyata dari struktur masyarakat dunia.[2] Hal ini sesuai dengan fungsi hukum internasional adalah menyediakan dasar hukum bagi manajemen hubungan internasional.[3]

Yang dimaksudkan dengan istilah hukum internasional dalam pembahasan ini adalah hukum internasional publik, yang harus kita bedakan dari hukum perdata internasional. Hukum perdata internasional adalah keseluruhan kaedah-kaedah dan azas hukum yang mengatur hubungan perdata yang melintasi batas-batas negara-negara. Sedangkan hukum internasional publik adalah keseluruhan kaedah-kaedah dan azas hukum yang mengatur hubungan atau persoalan yang melintasi batas-batas negara-negara (hubungan internasional) yang bukan bersifat

[1]Boer Mauna, **Hukum Internasional: Pengertian, Peranan dan Fungsi dalam Era Dinamika Global**, 2011, PT Alumni, Bandung, hlm. 1

[2] Boer Mauna,Ibid, hlm. 3.

[3]Philip C. Jessup, ***A Modern Law of Nations***, 2012, Nuansa, Bnadung, hlm. 32.

perdata.[4] Mengenai uraian pengertian hukum iternasional di atas, kita merumuskannya sebgai berikut:

Hukum internasional adalah keseluruhan kaedah-kaedah dan azas-azas yang mengatur hubungan atau persoalan yang melintasi batas-batas negara-negara antara:

(1) Negara dengan negara;

(2) Negara degan subjek hukum lain bukan negara atau subjek hukum bukan negara satu sama lain.[5]

Singkatnya, hukum internasional publik secara konvensional mengatur hubungan antar negara-negara berdaulat sedangkan hukum perdata internasional mengatur hubungan antara atau diantara orang-orang yang merupakan warga negara dari negara-negara berbeda.[6]

Subjek Hukum Internasional

Dalam arti yang sebenarnya subjek hukum internasional adalah pemegang (segala) hak dan kewajiban menurut hukum internasional. Kalau mau subjek hukum internasional demikian dapat kita sebut subjek hukum internasional penuh. *Negara* merupakan subjek hukum internasional dalam arti ini.[7] Bagi pengamatan secara hukum positip tidak menjadi soal apa yang menjadi sumber hukum dari

[4]Mochtar Kusumaatmadja, **Pengantar Hukum Internasional**, 1982, Binacipta, Jakarta, hlm. 1.
[5] Mochtar Kusumaatmadja,Ibid, hlm. 3-4.
[6]Hata, **Hukum Internasional: Sejarah dan Perkembangan Hingga Pasca Perang Dingin**, 2012, Setara Press, Malang, hlm. 106.
[7] Mochtar Kusumaatmadja , *Op Cit*, hlm.91.

pada hak-hak dan kewajiban itu. Apabila kita melihat persoalan secara demikian maka hukum internasional sevagai tersebut dibawah ini.[8]

(1) Negara

Negara adalah subjek hukum internasional dalam arti yang kalsik, dan telah demikian sejak lahirnya hukum internasional.

(2) Tahta Suci

Tahta Suci atau Vatican merupakan suatu contoh dari pada suatu subjek hukum internasional yang telah ada sejak dahulu di samping negara-negara.

(3) Palang Merah Internasional

Yang dimaksud dengan Palang Merah Internasional adalah *International Committee of the Red Cross* (ICRC) yang berkedudukan di Jenewa.

(4) Organisasi Internasional

Organisasi internasional seperti Perserikatan Bangsa-Bangsa dan Organisasi Buruh Internasional (ILO) mempunyai hak-hak dan kewajiban-kewajiban yang ditetapkan dalam konvensi-konvensi internasional yang merupakan semacam anggaran dasarnya.

(5) Orang perorangan (Individu)

Dalam arti yang terbatas orang perorangan sudah agak lama dapat dianggap sebagai subjek hukum internasional. Lebih penting artinya bagi perkembangan pengertian individu sebagai subjek hukum internasional dari ketentuan-ketentuan yang bertujuan melindungi hak

[8]Mochtar Kusumaatmadja , *Op Cit*, hlmn. 92-97

minoritas, adalah keputusan Mahkama Internasional Permanen (Permanent Court of International Justice).

(6) Pemberontak dan Pihak Dalam Sengketa (*belligerent*)

Menurut hukum perang pemberontak dapat memperoleh kedudukan dan hak sebagai pihak yang bersengketa (*belligerent*) dalam keadaan-keadaan tertentu.[9]

Sumber Hukum Internasional

J.G. Starke menguraikan bahwa sumber-sumber hukum internasional dapat dikategorikan dalam lima bentuk, yaitu:[10]

1. Kebiasaan;
2. Traktat;
3. Keputusan pengadilan atau badan-badan arbritasi;
4. Karya-karya hukum;
5. Keputusan atau ketetapan organ-organ/lembaga internasional.

Sedangkan Pasal 38 ayat (1) Piagam Mahkamah Internasional mengatakan bahwa dalam mengadili perkara-perkara yang diajukan kepadanya, Mahkamah Internasional akan mempergunkan:[11]

1. Perjanjian-perjanjian internasional, baik yang besifat umum maupun khusus, yang mengandung ketentuan-ketentuan hukum yang diakui secara tegas oleh negara-negara yang bersengketa,

---

[9]Oppenheim-Lauterpacth, ***International Law***, 8th Edition, vol II dalam Mochtar Kusumaatmadja, Pengantar Hukum Internasional, 1982, Binacipta, Jakarta.

[10] J.G. Starke, cq, Introduction to International Law, Butterworth & Co., Tenth Edition, 1989, hlm. 429.

[11]Mochtar Kusumaatmadja, Pengantar Hukum Internasional, 1982, Binacipta, Jakarta, hlm. 107-108.

2. Kebiasaan-kebiasaan internasional, sebagai bukti dari pada suatu kebiasaan umum yang telah diterima sebagai hukum,
3. Prinsip-prinsip hukum umum yang diakui oleh bangsa-bangsa yang beradap,
4. Keputusan pengadilan dan ajaran-ajaran sarjana-sarjana yang paling terkemuka dari berbagai negara sebagai sumber tambahan bagi menetapkan kaedah-kaedah hukum.

B. Hubungan Antara Hukum Internasional dan Hukum Nasional

Mengenai hubungan antara perangkat hukum ini terdapat dua teori utama yang dikenal adalah monisme dan dualisme. Menurut teori monisme, hukum internasional dan hukum nasional merupakan dua aspek yang sama dari satu sistem hukum umumnya; menurut teori dualisme, hukum internasional dan ukum nasional merupakan dua sistem hukum yang sama sekali berbeda, hukum internasional mempunyai suatu karakter yang berbeda secara *intrinsik* (*intrinsically*) dari hukum nasional.[12]

Paham monisme didasarkan atas pemikiran kesatuan dari seluruh hukum yang mengatur hidup manusia.Akibat pandangan monisme ini ialah bahwa antara dua perangkat ketentuan hukum ini mungkin ada hubungan hirarki.Persoalan hirarki antara hukum nasional dan hukum internasional inilah yang melahirkan beberapa sudut pandang yang berbeda dalam aliran monisme mengenai masalah hukum nasional dan hukum internasional.Ada pihak yang menganggap bahwa dalam hubungan hukum nasional dan hukum internasional yang utama adalah

[12] J.G. Starke, ***An Introduction to International Law***, Butterworth & Co (Publishers) Ltd. 4th edition 1958, hlmn. 60.

hukum nasional.Paham ini adalah paham monisme dengan primat hukum nasional. Dalam pandangan monisme dengan primat hukum nasional, hukum internasional tidak lain dari merupakan kelanjutan hukum nasional untuk urusan luar negeri.[13]

Kemudian dalam bukunya, Pengantar Hukum Internasional Bagian I, Mochtar Kusumaatmajamenyatakan, menurut paham monisme dengan primat hukum internasional, maka hukum nasional itu bersumber pada hukum internasional yang menurut pandangannya merupakan suatu perangkat ketentuan hukum yang hirarkis lebih tinggi. Menurut paham ini hukum nasional tunduk pada hukum internasional dan pada hakekatnya berkekuatan mengikat berdasarkan suatu "pendelegasian" wewenang dari hukum internasional.

Lain paham monisme, paham dualisme ini yang bersumber pada teori bahwa daya ikat hukum internasional bersumber pada kemauan negara, maka hukum internasional dan hukum nasional merupakan dua sistem atau perangkat hukum yang terpisah satu dari yang lainnya. Dengan perkataan lain, dalam teori dualisme tidak ada tempat bagi persoalan hirarki antara hukum nasional dan hukum internasional karena pada hakekatnya kedua perangkat hukum ini tidak saja berlainan dan tidak tergantung satu sama lainnya tapi juga lepas satu dari yang lainnya.[14]

C. Tinjauan Umum Spionase

Spionase menurut Kamus Besar Bahasa Indonesia adalah penyelidikan secara rahasia terhadap data kemiliteran dan data ekonomi negara lain; segala

---

[13] *Op Cit*, hlm. 43.

[14] Mochtar Kusumaatmaja, **Pengantar Hukum Internasional: Bagian I**, 1999, Binacipta, Jakarta, hlm. 40-41

sesuatu yang berhubungan dengan seluk-beluk spion; pemata-mataan: penangkapan dua orang wakil atase militer itu atas tuduhan.[15] Kemudian dalam Oxford English Dictionari Espionage, siponase atau lebih sering disebut spying diterjemahkan sebagai berikut;

> "Spying" is a colloquial, rather than legal, term. The Oxford English Dictionary defines "to spy" as, among other things, "[t]o watch (a person, etc.) in a secret or stealthy manner; to keep under observation with hostile intent; to act as a spy upon" and "[t]o make stealthy observations in (a country or place) from hostile motives."[16]

Atau jika diterjemahkan dalam bahasa Indonesia adalah "Spionase" adalah bahasa sehari-hari, bukan bahasa hukum, Istilah Oxford English Dictionary mendefinisikan "untuk memata-matai" sebagai, diantaranya, "[untuk] menonton (orang, dan lain-lain) secara rahasia atau diam-diam, Untuk tetap di bawah pengamatan dengan niat bermusuhan, untuk bertindak sebagai mata-mata pada "dan" [untuk] melakukan pengamatan tersembunyi dalam (sebuah negara atau tempat) dari motif bermusuhan".

Aturan mengenai spionase diatur dalam *Hague Convention* IV 1907 tentang *Regulations concerning the Laws and Customs of War on Land*. Terdapat dalam artikel 29-31, berikut adalah artikel 29;

> Artikel 29
> Seseorang hanya dapat dianggap sebagai mata-mata apabila melakukan suatu perbuatan secara diam-diam atau berpura-pura untuk mencari dan memperoleh informasi di daerah operasi dari negera-negara yang berperang dengan maksud untuk memberitahukannya kepada pihak musuh.
> Tentara yang tidak berada dalam penyamaran yang telah menerobos masuk ke daerah operasi pihak musuh untuk

---

[15]Kamus Besar Bahasa Indonesia dalam http://www.artikata.com/arti-351900-spionase.html
[16]Oxford English Dictionary

> memperoleh informasi, tidak dianggap sebagai mata-mata. Demikian pula, golongan berikut tidak dianggap sebagai mata-mata: tentara atau orang sipil yang melaksanakan misinya secara terbuka, yang bertugas untuk menyerahkan berita, baik kepada pasukannya sendiri maupun kepada musuhnya.
> Dalam pengertian ini termasuk juga orang-orang yang dikirimkan dengan menggunakan balon untuk menyampaikan berita dan biasanya untuk memelihara komunikasi diantara satuan-satuan yang berbeda dari suatu pasukan atau suatu wilayah."

Spasal 30 dan 31 mencatumkan mengenai hukum mata-mata yang tertangkap.

Secara teknis, istilah "spionase" dimaknai sebagai mengumpulkan informasi rahasia dari pihak lawan yang akan digunakan untuk kepentingan pihak pengumpul. Namun demikian, istilah spionase pada praktiknya digunakan untuk menyebut kegiatan intelijen secara luas. Perbedaan utama antara spionase dan bentuk pengumpulan intelijen lain adalah bahwa spionase melibatkan akses fisik ke sebuah lokasi di mana informasi rahasia disimpan.Terdapat sejumlah cara untuk mencapai tujuan ini, misalnya, mendapatkan pekerjaan sebagai anggota sah dari suatu organisasi tertentu yang ingin dicuri informasinya.[17] Selain dengan cara melibatkan diri secara langsung pada objek spionase, pengaruh perkembangan teknologi juga berdampak pada spionase yang dilakukan melalui penyadapan.

Secara umum, mengenai penyadapan atau tindakan menyadap menurut Kamus Besar Bahasa Indonesia, penyadapan dapat diartikan sebagai proses dengan sengaja mendengarkan dan/atau merekam informasi orang lain secara diam-diam dan penyadapan itu sendiri berarti suatu proses, suatu cara atau perbuatan menyadap.[18] Selain itu dalam KBBI, penyadapan (menyadap) juga didefinisikan sebagai kegiatan mendengarkan (merekam) informasi (rahasia) atau

---

[17] Apa itu Spionase? Fakta, Sejarah & Informasi Lainnya, http://www.amazine.co/25151/apa-itu-spionase-fakta-sejarah-informasi-lainnya/.

[18] **Kamus Besar Bahasa Indonesia**, Jakarta: Departemen Pendidikan Nasional, 2008, hlm.1337.

pembicaraan orang lain yang dilakukan dengan sengaja tanpa sepengetahuan orang yang bersangkutan.[19] Penjelasan pasal 40 Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi[20] menjelaskan;

> "Yang dimaksud dengan penyadapan dalam pasal iniadalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Pada dasarnya informasi yang dimiliki oleh seseorang adalah hak pribadi yang harus dilindungi sehingga penyadapan harus dilarang.."

Selain pengertian yang diberikan undang-undang, Abdul Hakim Ritonga juga menyatakan bahwa interception atau dalam bahasa Indonesia dapat diterjemahkan sebagai intersepsi atau penyadapan adalah tindakan mendengarkan, merekam, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel.[21]Dalam konteks yang lebih luas tentang praktik penyadapan yang dilakukan oleh lembaga intelijen/aparat penegak hukum suatu negara, penyadapan tidak hanya dilakukan melalui jaringan telekomunikasi maupun secara elektronik. Informasi hasil penyadapan diperoleh melalui berbagai cara dan sumber, baik dengan menggunakan sarana teknologi, maupun dengan cara-cara konvensional. Sarana teknologi misalnya penggunaan *software* atau *hardware*/perangkat khusus intersepsi, baik dengan atau tanpa melalui jaringan telekomunikasi. Sedangkan cara konvensional bisa dilakukan dengan mendengarkan langsung tanpa alat dengan sembunyi-sembunyi, menguping pembicaraan, atau menggunakan peralatan non-elektronis untuk mendengarkan

---

[19] *Ibid*. hlmn.1337.

[20] Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi

[21] Kristian dan Yopi Gunawan, 2013, **Sekelumit Tentang Penyadapan Dalam Hukum Positif Di Indonesia**, Nuansa Aulia, Bandung, hlm.184-185.

percakapan pihak yang disadap.[22]Secara umum, penyadapan sesungguhnya dapat terbagi dalam 5 (lima) bentuk utama berikut ini:[23]

a. Penyadapan Telepon Rumah Analog

Merupakan penyadapan yang dilakukan dengan menggunakan *splitter* (alat sederhana yang digunakan untuk memaralel telepon rumah). Kabel cabang splitter tersebut dipasang pada telelpon target peyadapan (objek peyadapan), kemudian disambungkan langsung ke perekam suara, atau alat perekam lainnya sehingga penyadap dapat mendengar atau mempeoleh informasi dari telepon tersebut.

b. Penyadapan Telepon Rumah Digital

Merupakan penyadapan yang dilakuakn dengan menggunakan alat kecil yang disebut *bug*. Dengan *bug* tersebut data akan dikirimkan dengan menggunakan frekuensi radio ke *reciever* penyadap (penangkap gelombang).

c. *Software* Pengintai

Merupakan penyadapan yang dilakukan dengan cara menanamkan aplikasi penyadap pada telepon seluler target penyadapan (objek penyadapan). Ketika objek yang disadap melakuka sambungan telekomunikasi atau menerima sambungan telekomunikasi maka secara otomatis *software* tersebut akan mengirimkannya pada penyadap.

---

[22] Teguh Arifiyadi, **Langkah Hukum Jika Disadap Negara Tetangga**, http://www.hukumonline.com/klinik/detail/lt5276f8bec3f65/langkah-hukum-jika-disadap-negara-tetangga, (diakses 4 Mei 2014)

[23]Trias Yuliana Dewi, dkk, **Naskah Akademik Rancangan Undang-undang tentang Penyadapan**, 2010, Tim Legistative Drafting, UNPAR, hlm.27-29.

d. Ponsel pengintai

Merupakan penyadapan yang dilakukan dengan menggunakan perangkat khusus yang telah dimodifikasi pada telepon seluler target atau objek penyadapan. Penyadap kemudian melakukan panggilan secara diam-diam kepada tersadap tanpa adanya tanda-tanda panggilan apa pun pada telepon seluler tersebut.

e. Penyadapan dalam Ruangan

Merupakan cara yang paling klasik dalam melakukan penyadapan, namun hingga saat ini masih digunakan. Penyadapan dalam ruangan merupakan tindakan penyadapan yang dilakukan dengan cara meletakkan secara diam-diam alat penyadapan (yang biasanya tidak terlalu besar) di dalam ruangan target penyadapan. Sistem kerjanya adalah alat penyadap tersebut akan menangkap semua pembicaraandari tersadap dan mengirimkannya dalam bentuk sinyal ke alat penangkap sinyal (*reciever*) penyadap.

D. Tinjauan Umum Cybercrime

Pengertian Cybercrime

Dalam beberapa literatur, *cybercrime* sering diidentikkan dengan *computer crime*. The US Department of Justice memberikan pengertian computer crime sebagai "*any illegal act requiring knowledge of computer for its perpetration, investigation, or prosecution.*", artinya setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki, dan menuntutnya". Lain dengan pengertian diatas, Indra Safitri mengemukakan,

kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingjkat keamanan yang tinggi dan kredebilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[24]

Berbeda dengan beberapa pengertian di atas, Andi Hamzah dalam bukunya Aspek-aspek Pidana di Bidang Komputer menyatakan bahwa "kejahatan di bidang komputer secara umaum dapat diartikan sebagai penggunaan komputer secara illegal".Dari beberapa definisi belum ada kesepakatan mengenai definisi tentang *cybercrime* atau kejahatan dunia *cyber*, seperti yang diungkapkan Agus Raharjo, bahwa istilah *cybercrime* sampai saat ini belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cybercrime* dengan *computer crime*.[25]

Karakteristik Cybercrime

Menurut freddy haris, cybercrime merupakan suatu tindak pidana dengan karakteristik-karakteristik sebagai berikut:[26]

1. *Unauthorized acces* (dengan maksud memfasilitasi kejahatan),
2. *Unauthorized alteration or destruction of data*,

[24]Indra Safitri, **Tindak Pidana di Dunia *Cyber***, 1999, *Insider, Legal Journal From Indonesia Capital & Investment Market*, http://business.fortunecity.com./buffett/842/art18099_tindakpidana.htm, tertanggal

[25]Agus Raharjo, ***Cybercrime*, Pemahaman, dan Upaya Pencegahan Kejahatan Teknologi**, 2002, Citra Adtya, Bandung, hlm. 227.

[26] Freddy Haris, ***Cybercrime* dari Perspektif Akademis**, lembaga kajian hukum dan teknologi fakultas hukum universitas indonesia, hlm. 4 dalam <http:www.gipi.or.id> tertanggal 9 Desember 2013.

3. Menggangu/merusak operasi komputer, mencegah atau menghambat akses pada komputer.

Barda[27] dalam bukunya, *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan,* dalam masalah cybercrime merujuk pada "Backgroun Paper" kongres PBB X untuk "Workshop on Crimes Related to The Computer Network", dokumen A/CONF.187/10, hlm 5. Dalam dokumen tersebut ditegaskan bahwa, *cybercrime* meliputi kejahtan yang dilakukan:

1. Dengan menggunakan sarana-sarana dari sistem/jaringan komputer (*by means of a computer system or network*);
2. Di dalam sistem/jaringan komputer (*in a computer system or network*)
3. Terhadap sistem/jaringan komputer (*against a computer system or network*)

Di samping itu berdasarkan beberapa literatur serta praktiknya, *cybercrime* memiliki karakteristik yang khas dibandingkan dengan kejahatan konvensional, yaitu;[28]

- Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.

---

[27]Brada Nawawi Arief, **Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan,** 2001, Citra Aditya Bakti, Bandung, hlm. 249-250.

[28]Ari Juliano Gema, 2013, ***Cybercrime*: Sebuah Fenomena di Dunia Maya**, http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya/89-cybercrime-sebuah-fenomena-di-dunia-maya, (diakses 9 desember 2013)

- Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet .
- Perbuatan tersebut mengakibatkan kerugian material mamupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
- Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
- Perbuatan tersebut sering dilakukan secara transnasional/melintas batas negara.

Jenis-jenis Cybercrime

Meskipun berbeda sama sekali dengan kejahatan konvensional, *cybercrime* memiliki karakteristik tersendiri. Namun pada dasarnya *cybercrime* juga terbagi dalam beberapa jenis seperti halnya kejahatan konvensional.

Jenis jenis kejahatan yang masuk dalam kategori cybercrime diantaranya:[29]

1. *Cyber*-terorism: National Police Agency of Japan (NPA) mendefinisikan *cyber terorism* sebagai *electronic attacks through computer network agains critical infrastructures that have potential critical effects on social and economic activities of nation.*
2. *Cyber-pornography*: penyebarluasan *obscene* materials termasuk *pornography, incident exposure,* dan *child pornography*.[30]

[29] Didik M. Arief Mansur dan Elisatris Gultom, 2005, ***Cyber Law*: Aspek Hukum Teknologi Informasi**, Refka Aditama, Bandung, hlm. 26-27.

[30] Di Amerika Serikat terdapat Undang-undang yang memberikan perlindungan bagi anak-anak terhadap pengaruh pornografi yaitu undang-undang tentang "*chlid online protection*". Undang-

3. *Cyber-harassment*: pelecehan seksual melalui e-mail, websites, atau chat programs.
4. *Cyber-stalking*: *crimes of stalking* melalui penggunaan komputer dan internet.
5. *Hacking*: penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum.
6. *Carding* ("*credit-card fraud*"):[31] melibatkan berbagai macam aktivitas yang melibatkan kartu kredit. *Carding* muncul ketika seorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Kemudian, beberapa bentuk kejahatan yang berhubungan erat dengan penggunaan teknlogi informasi yang berbasis utama komputer dan jaringan telekomunikasi ini, dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:[32]

1. *Unauthorized Acces to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. *Illegal Contents*

---

undang ini mengharuskan para penyedia jasa dan pemilik situs untuk membatasi akses ke situs yang berisi muatan porno bagi anak-anak yang belum dewasa.

[31]Ervina Lerry W. S, Iman, dan Stella K. R, ***The World of Cyber Crimes: Carding***, BhetaVersions, IKI-40000.

[32]Mas Wigrantoro Roes Setyadi dan Mirna Dian Avanti Siregar, **Naskah Akademik Rancangan Undang-undang Tidak Pidana di Bidang Teknologi Informasi**, Global Internet Policy Initiative – Indonesia bekerja sama dengan Indonesia Media Law and Policy Center, November, 2003, hlm. 25-26.

Merupkan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dann dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

3. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* memalui internet.

4. *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network sytem*) pihak sasaran.

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, proggram komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. *Offense Against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain.

7. *Infringements of Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan

terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui orang lain akan dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Selain itu, Ade Maman Suherman (2002: 168-171)[33] menyatakan bahwa menurut NCIS[34] Inggris, manifestasi dari tindak kejahatan *cyber crime* muncul dalam berbagai macam atau varian seperti: *Recreational Hackers, Crackers* atau *criminal minded hackers, Political Hackers, Denial of Service Attack, Insider* atau *Internal Hackers, Viruses, Piracy, Fraud, Gambling, Pornography and Paeddophilia, Cyber-Stalking, Hate Sites* dan *Criminal Communications*.

Dasar Hukum Cybercrime

Undang-undang yang mengatur mengenai cybercrime adalah Undang-undang No 36 tahun 1999 tentang Komunikasi dan Undang-undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Sedangkan dalam lingkup internasional diatur dalam *Convention on Cybercrime* 2000.

[33] Ade Maman Suherman dalam Abdul Wahid dan Mohammad Labib, **Kejahatan Mayantara (*Cybercrime*)**, 2005, Refika Aditama, Bandung, hlm 70-72.

[34] Naval Criminal Investigative Service, The NCIS Cyber Department *utilizes advanced cyber technologies and methodologies to identify and process electronic data of intelligence or evidentiary value*, (http://www.ncis.navy.mil/).

BAB III
METODE PENELITIAN

A. Jenis Penelitian

Jenis penelitian ini adalah yuridis normatif, yaitu metode atau cara yang dipergunakan di dalam penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka yang ada.[1]

B. Pendekatan Penelitian

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan kasus (*case approach*). *Statute approach* dalam penulisan ini adalah pendekatan terhadap undang-undang serta konvensi yang terkait dengan *cyberspace*, *cybercrime*,*interception*,dan*espionage*. Kemudian pendekatan kasus ialah menghubungakan pemasalahan yang terjadi dengan undang-undang dan konvensi yang ada.

C. Jenis dan Sumber Bahan Hukum

Bahan hukum yang digunakan adalah sebagai berikut:

a. Bahan hukum primer, yaitu bahan hukum utama yang bersifat mengikat, seperti:
   1. *Convention on Cybercrime* 2000
   2. Undang-undang No 36 tahun 1999 tentang Komunikasi

---

[1]Soerjono Soekanto dan Sri Mamudji, **Penelitian Hukum Normatif Suatu Tujuan Singkat**, 2009, PT Raja Grafindo, Jakarta, hlm. 13-14.

3. Undang-undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.
4. German *Criminal Code*
5. Australia *Criminal Code Act* 1995
6. *The Espionage Act of* 1917 (USA)

b. Bahan hukum sekunder, merupakan bahan hukum yang menjelaskan dan mendukung bahan hukum primer seperti Buku, Hasil Penelitian Ahli Hukum, dan Jurnal Nasional dan Internasional. Selain itu juga Konvensi dan Undang-undang yang lain yang mendukung Konvensi dan Undang-undang primer juga termasuk dalam bahan hukum sekunder. Undang-undang dan konvensi tersebut adalah;

1. *Hague Convention* 1907
2. Pasal 19 ayat (2) c *United Nations Convention on the Law of the Sea* (UNCLOS)

D. Teknik Memeperoleh Bahan Hukum

Dalam penelitian ini bahan hukum diperoleh dengan menggunakan teknik studi kepustakaan terhadap bahan-bahan hukum yang ada, baik bahan hukum primer maupun sekunder.

E. Teknik Analisis Bahan Hukum

Bahan hukum yang telah diperoleh kemudian dianalisis secara deskriptif kualitatif, yaitu dengn cara mendeskripsikan dan menggambarkan hubungan anatara kegiatan spionase melalui penyadapan dengan *cybercrime*. Selain itu juga menganalisis teori-teori yang ada.

BAB IV

TINDAKAN SPIONASE MELALUI PENYADAPAN ANTARNEGARA SEBAGAI *CYBERCRIME*

A. Spionase dan Cybercrime Secara Umum

Fenomena munculnya *cybercrime*, kejahatan baru dari globalisasi dan teknologi informasi serta telekomunikasi yang semakin canggih membawa dampak yang besar dalam perkembangan di bidang hukum. Kejahatan baru yang tidak biasa ini tidak hanya terjadi dalam lingkup nasional tetapi juga dunia internasional. Dari beberapa kasus yang telah terjadi baik di Indonesia maupun di luar negeri, hukum nasional belum mampu menanggulangi secara penuh kejahatah-kejahatan baru dalam bidang teknologi tersebut.

Hukum nasional belum mampu menanggulangi secara penuh kejahatan ini dikarenakan karakteristik kejahatan teknologi dan informasi ini adalah maya. Kegiatannya dilakukan dalam dunia maya (*cyberspace*) yang bersifat *borderless*. Kegiatan kejahatan dapat dilakukan di mana saja dengan akibat yang dapat terjadi dimana saja lain dari tempat kejahatan dilakukan. Sehingga membutuhkan penanganan tersendiri tidak bisa disamakan dengan kejahatan konvensional.

Dalam lingkup Internasional kejahatan ini juga masih belum mendapat penanggulangan yang maksimal. *Cybercrime* yang identik dengan kejahatan dalam bidang harta benda, dalam dunia internasional

hanya diatur mengenai kejahatan yang dilakukan orang perorangan terhadap individu lain atau terhadap badan hukum tertentu. Sedangkan mengenai *cybercrime* yang memungkinkan dilakukan oleh negara terhadap negara lain belum ada pengaturan khusus. Bertolak belakang dengan banyak permasalahan yang terjadi dewasa ini. Sebagian negara mengaku telah menjadi objek spionase oleh negara lain. Hal ini diketahui bukan dilakukan dengan cara konvensional, melainkan melalui dunia maya dengan memanfaatkan kemajuan teknologi informasi dan media telekomunikasi.

Spionase atau dalam bahasa Inggris *Espionage* diartikan dalam Kamus Besar Bahasa Indonesia adalah penyelidikan secara rahasia terhadap data kemiliteran dan data ekonomi negara lain; segala sesuatu yang berhubungan dengan seluk-beluk spion; pemata-mataan: penangkapan dua orang wakil atase militer itu atas tuduhan.[1] Sedangkan *Black Law Dictionary* mendefinisikan Spionase sebagai: "*...mengumpulkan, mengirimkan, atau menghilangkan...informasi yang berhubungan dengan pertahanan nasional*." Spionase juga dapat didefinisikan dengan melakukan tindakan-tindakan yang bertujuan untuk mengetahui segala aktivitas, tujuan, rencana, kapabilitas dan kelemahan-kelemahan musuh atau negara yang dituju baik melalui cara penyadapan ataupun pengiriman agen-agen intelejen yang berkedok diplomat serta kegiatan-kegiatan lain yang bertentangan dengan hukum internasional.[2]

---

[1] Kamus Besar Bahasa Indonesia dalam http://www.artikata.com/arti-351900-spionase.html

[2] Anonim, **224473933Project.docx**, http://www.scribd.com/doc/224473933/4/F-Spionase, hlm.5-6, (diakses 24 Mei 2014)

Kegiatan spionase atau *spying* yang dilakukan antar negara atau dalam lingkup dunia internasional pada dasarnya tidak diatur secara khusus dalam suatu konvensi atau traktat yang disetujui dan diakui masyarakat internasional. Salah satu konvensi yang mengatur mengenai kegiatan spioase ini adalah *Hague Convention IV 1907* artikel 29 hingga 31. *Hague Convention* mengatur mengenai kegiatan *spying* dan *spies* dalam keadaan perang, dimana kegiatan *spying* yang dimaksud dilakukan secara langsung dengan cara konvensional bukan melalui media yang canggih seperti kasus-kasus yang terjadi dewasa ini. Sedangkan kegiatan spionase yang dilakukan dalam masa damai belum diatur secara langsung dalam suatu Undang-undang, konvensi, traktat serta perjanjain atau peraturan dalam bentuk lain. Namun, jika dilihat dari karakteristik, tujuan dan akibat yang ditimbulkan dari kegiatan spionase melalui *cyberspace* dan media canggih lainnya, Peraturan Perundang-undangan atau konvensi tentang Teknologi dan Informasi serta telekomunikasi yang telah ada dapat digunakan sebagai acuan, selain itu juga dapat dilihat dalam peraturan mengenai kejahatan dunia maya (*cybercrime*).

Geoffrey Demarest mengatakan bahwa, "*The development of international legal principles regarding peacetime espionage has lagged behind changes in international intelligence gathering norms and practices*."[3] Dari pernyataan Demarest tersebut dengan melihat fenomena yang terjadi, memang spionase dalam masa damai telah tertinggal di

[3]Lt. Col. Geoffrey B. Demarest, 1996, ***Espionage in International Law,***24 Denv. J. Int'l L. & Pol'y 321, https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=24+Denv.+J.+Int%27l+L.+%26+Pol%27y+321&key=264b0db644528bcd78ae55fa62fec5f2, (diakses 24 Mei 2014)

belakang perubahan dalam norma-norma dan praktek pengumpulan informasi intelijen internasional. Norma-norma dan praktek pengumpulan informasi intelijen internasional jauh lebih berkembang dibanding norma yang mengatur mengenai spionase itu sendiri. Demarest juga berpendapat "*International law regarding peacetime espionage is virtually unstated, and thus, international law has been an inappropriate and inadequate reference for either condemnation or justification of actions involving intelligence gathering.*"[4]

Seperti yang dijelaskan sebelumnya, dalam lingkup Internasional konvensi yang mengatur mengenai spionase hanya *Hague Convention* IV 1907. Namun jika peraturan mengenai spionase yang dilakukan pada masa perang dalam *Hague Convention* IV 1907 diterapkan dalam permasalah spionase yang terjadi dewasa ini tentu tidak sesuai. Selain kegiatan spionase dilakukan dalam masa perang, spionase juga dilakukan dengan cara yang konvensional. Bukan melalui media teknologi komunikasi dan informasi yang canggih. Berikut adalah artikel dalam *Hague Convention* IV 1907 yang mencantumkan tentang spies dalam masa perang:

> "Artikel 29
> Seseorang hanya dapat dianggap sebagai mata-mata apabila melakukan suatu perbuatan secara diam-diam atau berpura-pura untuk mencari dan memperoleh informasi di daerah operasi dari negera-negara yang berperang dengan maksud untuk memberitahukannya kepada pihak musuh.
> Tentara yang tidak berada dalam penyamaran yang telah menerobos masuk ke daerah operasi pihak musuh untuk memperoleh informasi, tidak dianggap sebagai mata-mata. Demikian pula, golongan berikut tidak dianggap sebagai mata-mata: tentara atau orang sipil yang melaksanakan misinya secara

[4] Ibid.

terbuka, yang bertugas untuk menyerahkan berita, baik kepada pasukannya sendiri maupun kepada musuhnya.
Dalam pengertian ini termasuk juga orang-orang yang dikirimkan dengan menggunakan balon untuk menyampaikan berita dan biasanya untuk memelihara komunikasi diantara satuan-satuan yang berbeda dari suatu pasukan atau suatu wilayah."

Dimuat dalam sindonews.com mengenai kegiatan spionase AS melalui penyadapan terhadap beberapa negara di Eropa dan Amerika lainnya. Sama dengan beberapa negara di Eropa dan Amerika, masyarakat Indonesia juga dikejutkan dengan tindakan spionase Australia melalui penyadapan terhadap Presiden RI dan beberapa menteri. Penyadapan yang dilakukan Australia ini berpusat di kantor kedutaan Australia untuk Indonesia di Jakarta. Dimuat dalam vivanews.co.id pada tanggal 21 November 2013,[5] bahwa "*Akhir Oktober 2013, harian Fairfax mengungkap bahwa gedung Kedutaan Australia di beberapa negara Asia, termasuk Indonesia, digunakan sebagai pos penyadapan.*" Kejadian ini Dianggap mengejutkan publik karena dokumen penyadapan dibeberkan secara luas melalui media dan dilakukan oleh pihak ketiga, sehingga bisa saja dinilai mengurangi kewibawaan pemerintah Indonesia di mata warga negaranya maupun di mata internasional.[6]

[5]Ita Lismawati F. Malau, Nila Chrisna Yulika, **Sadap Indonesia, Australia Langgar Konvensi Wina: Australia melancarkan aksi spionase kepada Indonesia**, http://politik.news.viva.co.id/news/read/460248-sadap-indonesia--australia-langgar-konvensi-wina, (diakses 31 Desember 2013)

[6] Teguh Arifiyadi, **Langkah Hukum Jika Disadap Negara Tetangga**, http://www.hukumonline.com/klinik/detail/lt5276f8bec3f65/langkah-hukum-jika-disadap-negara-tetangga, (diakses 4 Mei 2014)

Penyadapan berdasarkan penjelasan Pasal 40 Undang-undang Telekomunikasi:[7]

> "Penyadapan adalah kegiatan memasang alat atau perangkat tambahan pada jaringan telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah."

Dalam konteks yang lebih luas tentang praktik penyadapan yang dilakukan oleh lembaga intelijen/aparat penegak hukum suatu negara, penyadapan tidak hanya dilakukan melalui jaringan telekomunikasi maupun secara elektronik. Informasi hasil penyadapan diperoleh melalui berbagai cara dan sumber, baik dengan menggunakan sarana teknologi, maupun dengan cara-cara konvensional. Sarana teknologi misalnya penggunaan *software* atau *hardware*/perangkat khusus intersepsi, baik dengan atau tanpa melalui jaringan telekomunikasi. Sedangkan cara konvensional bisa dilakukan dengan mendengarkan langsung tanpa alat dengan sembunyi-sembunyi, menguping pembicaraan, atau menggunakan peralatan non-elektronis untuk mendengarkan percakapan pihak yang disadap.[8]

1. Tindakan Spionase SebagaiCybercrime

Berbeda dengan kejahatan konvensional, *cybercrime* memiliki ciri khusus yang tidak dimiliki oleh kejahatan pada umumnya. Meskipun penjabaran mengenai *cybercrime* berbeda-beda menurut tiap ahli tetapi secara garis besar

[7] Undang-undang Republik Indonesia No.36 tahun 1999 tentang Telekomunikasi, hlm.30.

[8] Teguh Arifiyadi, **Langkah Hukum Jika Disadap Negara Tetangga**, http://www.hukumonline.com/klinik/detail/lt5276f8bec3f65/langkah-hukum-jika-disadap-negara-tetangga, (diakses 4 Mei 2014)

dapat ditarik persamaan. Ciri khusus dari *cybercrime* sendiri Menurut Freddy Haris, adalah sebagai berikut:[9]

1. *Unauthorized access* (dengan maksud memfasilitasi kejahatan),
2. *Unauthorized alteration or destruction of data*,
3. Menggangu/merusak operasi komputer,
4. Mencegah atau menghambat akses pada komputer.

Berbeda dengan Freddy Haris, Tubagus Ronny Rahman Nitibaskara menggambarkan ciri khusus dari *cybercrime* yaitu;[10]

1. *Non-violance* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik (*minimaze of physical contact*)
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global;

Disamping itu berdasarkan beberapa literatur serta praktiknya, ciri khusus *cybercrime* yang berbeda degan kejahatan konvensional, yaitu:[11]

1. Perbuatan yang dilakuakan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.

---

[9] Freddy Haris, ***Cybercrime* dari Perspektif Akademis**, lembaga kajian hukum dan teknologi fakultas hukum universitas indonesia, hlm. 4. (Diakses 9 Desember 2013).

[10] Tubagus Ronny Rahman Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, *Op.Cit.*

[11] Ari Juliano Gema, 2013, ***Cybercrime*: Sebuah Fenomena Di Dunia Maya**, http://www.interpol.go.id/id/kejahatan-transnasional/kejahatan-dunia-maya/89-cybercrime-sebuah-fenomena-di-dunia-maya, (diakses 9 desember 2013)

2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan secara transnasional/melintas batas negara.

Selain dari akibat yang ditimbulkan, ciri-ciri khusus *cybercrime* juga dapat dilihat dari bentuk kegiatan yang dilakukan, motif, serta sasaran dilakukannya *cybercrime*. Sama halnya dengan menjabarkan ciri khusus, para ahli juga berbeda-beda dalam mengelompokkan bentuk cybercrime ini. Naskah Akademik Rancangan Undang-undang Tidak Pidana di Bidang Teknologi Informasi mengelompokkan beberapa bentuk cybercrime, antara lain:[12]

a. *Unauthorized Acces to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

b. *Illegal Contents*

[12]Mas Wigrantoro Roes Setyadi dan Mirna Dian Avanti Siregar, ***Op.Cit***.

Merupkan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dann dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

c. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* memalui internet.

d. *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network sytem*) pihak sasaran.

e. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, proggram komputer atau sistem jaringan komputer yang terhubung dengan internet.

f. *Offense Against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain.

g. Infringements of Privacy

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan

terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui orang lain akan dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Kemudian dalam buku ***Cyber Law*: Aspek Hukum Teknologi Informasi**, penulis menggolongkan cybercrime dalam enam bentuk, seperti;[13]

1. *Cyber*-terorism: National Police Agency of Japan (NPA) mendefinisikan *cyber terorism* sebagai *electronic attacks through computer network agains critical infrastructures that have potential critical effects on social and economic activities of nation*.
2. *Cyber-pornography*: penyebarluasan *obscene* materials termasuk *pornography, incident exposure*, dan *child pornography*.[14]
3. *Cyber-harassment*: pelecehan seksual melalui e-mail, websites, atau chat programs.
4. *Cyber-stalking*: *crimes of stalking* melalui penggunaan komputer dan internet.
5. *Hacking*: penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum.
6. *Carding* ("*credit-card fraud*"):[15] melibatkan bernagai macam aktivitas yang melibatkan kartu kredit. *Carding* muncul ketika seorang yang

[13] Didik M. Arief Mansur dan Elisatris Gultom, 2005, ***Cyber Law*: Aspek Hukum Teknologi Informasi**, Refka Aditama, Bandung, hlm. 26-27.

[14] Di Amerika Serikat terdapat Undang-undang yang memberikan perlindungan bagi anak-anak terhadap pengaruh pornografi yaitu undang-undang tentang "*chlid online protection*". Undang-undang ini mengharuskan para penyedia jasa dan pemilik situs untuk membatasi akses ke situs yang berisi muatan porno bagi anak-anak yang belum dewasa.

bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Dilihat dari ciri khusus atau karakteristik dan jenis dan bentuk cybercrime, kegiatan spionase melalui penyadapan teknologi informasi atau alat telekomunikasi bisa tergolong dalam kategori *cybercrime*. Secara sederhana dapat langsung dimasukkan kedalam jenis *cyber-espionage,* namun jika dipahami secara mendalam dapat masuk ke dalam bentuk dan/atau jenis *cybercrime* yang lain. Bukan hanya karena lain dari kejahatan konvensional tetapi pelaku juga mewakili suatu negara berdasarkan perintah dan merupakan pekerjaan yang semestinya.

Berikut adalah karakteristik atau ciri khusus dari *cybercrime* yang sesuai dengan spionase;

1. Karakteristik yang pertama *Unauthorized acces* atau akses tidak sah.Mengumpulkan informasi baik secara langsung mengambil atau dengan cara tidak langsung secara sembunyi-sembunyai tanpa sepengetahuan dari objek spionase. Pada dasarya keegiatan spionase atau memata-mata dalam bentuk apapun tentu bukan suatu yang sah dalam hukum negara manapun.
2. Kedua, kegiatan spionase merupakan kegiatan yang *Non-violance* (tanpa kekerasan), dimana kegiatan dengan tujuan utama adalah mengumpulkan informasi secara rahasia. Baik pengumpulan informasi secara langsung atau tidak langsungdilakuakn dengan cara yang tidak mengundang perhatian pihak target spionase,

---

[15]Ervina Lerry W. S, Iman, dan Stella K. R, ***The World of Cyber Crimes: Carding***, BhetaVersions, IKI-40000.

3. Sedikit melibatkan kontak fisik (*minimaze of physical contact*), karakteristik yang ketiga ini berhubungan dengan karakteristik kedua. Kegiatan spionase merupakan kegiatan yang *Non-violance* juga dikarenakan sedikit melibatkan kontak fisik. Disamping itu berkaitan dengan tujuan mengumpulkan informasi secara rahasia sediki kontak fisik bisa jadi cara yang aman.
4. Keempat, menggunakan peralatan (*equipment*), teknologi, dan memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global. Tiap intelejen atau pihak yang turun langsung melakukan tindakan spionase membutuhkan alat dan teknologi untuk memfasilitasi kegiatan. Informasi yang didapatkan perlu direkam dan dikirimkan.
5. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional. Karena tindakan ini dilakukan suatu negara kepada negara lain, ditak dapat dikatakan tindakan yang remeh.

2. Tindakan Penyadapan Sebagai *Cybercrime*

Pada dasarnya penyadapan adalah satu cara dari kegiatan spionase. Karena dalam era modern ini spionase yang paling memungkan diakukan dengan sedikit resiko diketahui pihak yang dimata-matai adalah dengan penyadapan. Dimana kegiatan dilakukan tanpa harus dilakuakn langsung dari lokasi subjek atau objek yang akan dimata-matai. Dengan kecanggihan teknologi informasi dan

telekomunikasi, kegiatan dapat dilakuakan dari satu tempat tanpa harus mendengarkan, menguping, atau dengan cara konvensonal lainnya seperti spionase yang dilakukan pada jaman dahulu. Namun, dari segi karakteristik dan jenis mengenai penyadapan dan *cybercrime* jika diartikan masing-masing dapat ditarik satu kesamaan dari keduanya. Berikut adalah kesamaan baik spionase maupun penyadapan yang termasuk dalam *cybercrime* yang dalam hal ini adalah dilakukan antar negara;

1. *Unauthorized acces* atau akses tidak sah. Tindakan penyadapan dengan bantuan teknologi informasi dan alat telekomunikasi canggih, bukan hanya informasi yang diperlukan yang didapatkan. Tidak menutup kemungkinan hal-hal lain yang bersifat pribadi diluar objek sponase juga dapat diketahui oleh pihak penyadap. Hal ini bisa jadi bertentangan dengan hak asasi manusia, mengenai *privacy* seseorang.
2. Kedua, tindakan penyadapan media telekomunikasi dan informasi ini merupakan kegiatan yang *Non-violance* (tanpa kekerasan), dimana kegiatan utama adalah mengumpulkan informasi yang dilakukan dengan cara rahasia. Sehingga pegumpulan informasi yang pada dasarnya berakubat fatal namun dilakukan dengan cara diam-diam tanpa ada kekerasan.
3. Penyadapan juga sedikit melibatkan kontak fisik (*minimaze of physical contact*). Penyadapan dan *cybercrime* sama-sama tindakan yang sedikit nelibatkan kontak fisik, hal ini karena tindakan ini dilakukan di *cyberspace* beserta teknologi telekomunikasi dan informasi canggih tanpa harus bertatap muka dengan objek secara langsung.

4. Keempat, menggunakan peralatan (*equipment*), teknologi, dan memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global.
5. Perbuatan yang dilakuakan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyberspace*).
6. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang berhubungan dengan internet.
7. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
8. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Sesuai dengan tingkat dampak yang ditimbulkan, tindakan juga dilakukan oleh orang-orang khusus. Dalam hal ini adalah intelejen yang mempunyai keahlian khusus.

Kemudian jika penyadapan termasuk dalam*cybercrime*, maka beberapa bentuk *cybercrime* yang ada, penyadapan sesuai dengan beberapa bentuk dibawah ini;

1. *Unauthorized Acces to Computer System and Service*, akses tidak sah tehadapa sistem komputer. Selain pada komputer *unauthorized acces* secara luas dapat diartikan bahwa akses dapat dilakukan terhadap alat informasi dan telekomunikasi lain dengan teknologi yang sama dengan komputer. selain itu penyadapan juga dilakukan pada komputer-komputer perusahaan besar dalam kasus spionase industri dan militer.

2. *Cyber Espionage,* secara umum diartikan sebagai kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network sytem*) pihak sasaran. Namun dalam perkembangannya saat ini *cyber espionage* juga dapat diartikan pada tindakan *espionage* pada media informasi dan komunikasi lain selain komputer, misalnya telepon dan telepon seluler.
3. *Infringements of Privacy*, kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized*, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya. Mengenai permasalahan penyadapan terkait kerahasiaan negara, hal ini selain berkaitan dengan *privacy* suatu negara juga menyangkut *privacy* orang yang menjadi target penyadapan.
4. *Cyber-stalking*,umumnya *cyber-stalkig* diartikan *crimes of stalking*. Stalking dalam bahasa Indonesia adalah menguntit, mengikuti dengan hati-hati. Jika diartikan dengan gabungan kata *cyber* maka *stalking* dilakukan di *cyberspace*.

Dari beberapa karakteristik khusus dan bentuk*cybercrime*, tindakan penyadapan bisa dikategorikan ke dalam *cybercrime*. Dapat masuk ke salah satu atau beberapa dari bentuk yang telah dijelaskan diatas. Meskipun dalam pengertian yang sempit *cybercrime* hanya merujuk pada tindakan kejahatan dunia maya yang dilakukan dengan media komputer. Perkembangan serta pengertian penyadapan sendiri berdasar undang-undang saat ini, *cybercrime* sudah mengarah

pada tindakan yang dilakukan bukan hanya dengan komputer. Tindakan baik penyadapan atau kejahatan lain dilakukan dengan media elektronik yang berhubungan dengan internetserta teknologi lain yang mendukung.

B. Peraturan Mengenai Spionase, Penyadapan dan Cybercrime

1. Peraturan Dunia Internasional

Cybercrime

Meskipun belum terdapat peraturan khusus yang mengatur mengenai spionase dalam masa damai dan penyadapan antar negara, namun beberapa konvensi dan manual internasional mencantumkan mengenai *cybercrime*. Peraturan internasional mengenai *cybercrime* terdapat dalam *Conventiom on Cybercrime* 2000. *Convention on Cybercrime* juga biasa disebut dengan *Budapest Covention*. Konvensi ini mencantumkan tindakan apa saja yang tergolong dalam *cybercrime*. Tujuan dibuatnya konvesi ini tercantum dalam preamble yaitu "*Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks*."Karena pada dasarnya berlakunaya hukum Internasional dalm bentuk konvensi perlu adanya ratifikasi negara maka, dalam setiap artikel pada konvensi ini menyatakan "*Setiap Pihak wajib mengambil tindakan-tindakan legislatif dan lainnya yang dianggap perlu untuk menetapkan sebagai kejahatan pidana berdasarkan hukum nasionalnya*".

Yang termasuk *cybercrime* dalam konvensi ini adalah *Illegal access, Illegal interception, Data interface, System interface, Misuse of devices, Computer-related forgery, dan Computer-related fraud*.Kemudian dibedakan lagi

tentang konten yang terkait pelanggaran dan Pelanggaran yang berkaitan dengan pelanggaran hak cipta dan hak terkait.Brada Nawawi Arief (2003; 242)[16] merumuskan delik-delik cybercrime bedasarkan konvensi ini sebagai berikut;

1. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer yaitu;
   a. Mengakses sistem komputer secara tanpa han (*illegal acces*)
   b. Tanpa hak manangkap/mendengar pengiriman dan pemancaran (*illegal interception*)
   c. Tanpa hak merusak data (*data interface*)
   d. Tanpa hak mengganggu sistem (*system interface*)
   e. Menyalahgunakan perlengkapan (*mesuse of device*)
2. Delik-delik yang berhubungan dengan komputer: pemalsuan dan penipuan (*computer related offences; forgery and fraud*)
3. Delik-delik yang bermuatan pernorafi anak (*content-related offences, child phornograpy*)
4. Delik-delik yang berhubungan dengan hak cipta (*offences-related of infringments of copyright*)

Spionase dan Penyadapan

Belum adanya peraturang mengenai spionase dalam masa damai, penyadapan, serta spionase melaui penyadapan, hal ini juga belum dapat dikatagorikan sebagai *cybercrime*. Tetapi beberapa konvensi internasional yang mengatur mengnai *cybercrime*, kurang lebihnya dapat dijadikan acuan dalam

[16]Barda Nawawi Arief dalam Abdul Wahid dan Mohammad Labib, **Kejahatan Mayantara (*Cybercrime*)**, 2005, Refika Aditama, Bandung, hlm.74

penyelesaian masalah yang ada. Sedangakan mengenai spionase dalam beberapa konvensi juga dapat dijadikan referensi, meskipun hanya sepintas dicantumkan.

Hague Convention IV 1907 mencantumkan beberapa pasal mengenai spionase dan *spies* dalam masa perang. Kemudian dalam UNCLOS 1982 (*United Nations Convention Law Of The Sea*) juga terdapat satu pasal mengenai kegiatan pengumpulan informasi yang merugikan bagi pertahanan atau keamanan negara. Terdapat pada pasal 19 ayat (2) c mengenai Lintas Damai, pasal 19 ayat (2) c menyatakan "*setiap perbuatan yang bertujuan untuk mengumpulkan informasi yang merugikan bagi pertahanan atau keamanan negara pantai*". Jika diartikan sepintas pasal ini hanya diperuntukkan kegiatan kapal asing di perairan negara pantai, namun jika diartikan secara luas, yang dimaksud perbuatan atau kegiatan mengumpulkan informasi yaitu mengumpulkan informasi dalam bentuk apapun teramasuk spionase mealalui penyadapan merupakan kegiatan yang merugikan bagi pertahanan atau keamanan negara. Meskipun tidak ada penjelasan lanjut dalam pasal berikutnya, jika diperhatikan, pada dasarnya kegiatan mengumpulkan informasi atau *spying* adalah perbuatan yang dianggap merugikan bagi negara-negara.

Pada kenyataan setiap negara terlibat dalam spionase. *Central Intelligence Agency* (CIA) menekankan bahwa *cyber* spionase tidak jatuh di bawah payung *cyber-warfare*, kemungkinan karena pemerintah AS seperti banyak lainnya pemerintah-secara rutin melakukan pengintaian melalui jaringan komunikasi.[17]Dari pernyataan tersebut secara langsung CIA mengakui bahwa

[17] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, 2011, ***The Law of Cyber-Attack***,

pemerintah AS terlibat dalam kegiatan spionase serta menyatakan bahwa pada kenyataannya banyak negara juga melakukan kegiaan tersebut. Bertolak belakang dengan beberapa ketentuaan yang dicantumkan dalam beberapa konvensi yang ada.

Pasal 19 ayat (2) c UNCLOS hanya mencantumkan satu pernyataan dalam pasal lintas damai kapal asing, bahwa kegiatan mengumpulka informasi adalah kegiatan yang dianggap membahayakn pertahanan dan keamanan negara. Namun, jika diperhatikan secara mendalam negara-negara yang meratifikasi UNCLOS secara otomatis sepakat bahwa kegiatan spionase melanggar hukum internasional.Selain UNCLOS yang mencantumkan larangan mendapatkan informasi, *Convention on Cybercrime* juga mencantumkan satu artikel mengenai penyadapan atau intersepsi. Berikut adalah artikel 3 *Convention on Cybercrime*;

> *Article 3*
> *Illegal interception*
> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

Beberapa peraturan regional dari negara-negara Eropa dan Afrika yang beberapa diantarananya juga mencantumkan tentang cybercrime dan interception[18] (lihat lampiran 1).

2. Peraturan Negara-Negara

---

http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf, Note 45 hlm. 14. (Diakses 29 November 2013)

[18]***Comprehensive Study on Cybercrime****, Draft,* 2013, *United Nations Officeon Drugsand Crime*, Vienna.

Meskipun setiap negara memiliki sistem hukum yang berbeda namun setiap negara memiliki peraturan khusus mengenai suatu hal. Baik peraturan tersebut digunakan sebagai sumber hukum utama maupun hanya sebagai sumber hukum tambahan. Negara dengan sistem hukum *common law* meskipun menggunakan yurisprudensi sebagai sumber utama dalam pemecahan masalah yang ada, tetap memiliki peraturan yang dijadikan tolak ukur dalam putusannya. Terlebih negara yang mengaut sistem hukum *civil law*, dimana suatu peraturan tertulis atau undang-undang merupakan sumber hukum utama dalam pemecahan dan memutuskan suatu permasalahan. Namun, tiap negara baik sesama penganut sistem hukum *civil law* maupun sistem hukum *common law* tidak selalu memiliki peraturan yang sama dalam hal tertentu.

Seperti halnya peraturan mengenai spionase beserta *spies*, dan *cybercrime*, dimana tidak semua negara memiliki peraturan tentang beberapa hal tersebut. Suatu negara bisa jadi hanya memiliki salah satu dari peraturan tersebut. Indonesia salah satunya, di Indonesia belum memiliki peraturan mengenai spionase dan *spies*, tetapi sudah memiliki peraturan mengenai *cybercrime*. Pengaturan tentang *cybercrime* di Indonesia yaitu Undang-undang No.36 Tahun 1999 tentang Telekomunikasi dan Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut tidak secara khusus mengatur mengenai *cybercrime*, di dalamnya diatur mengenai sebagian besar kegiatan dalam *cyberspace*. Di dalam undang-undang ini juga diatur mengenai penyadapan, dimana penyadapan merupakan suatu kejahatan apabila dilakukan untuk kepentingan pribadai dan bukan oleh pejabat yang berwenang untuk melakukan penyadapan seperti halnya dijelaskan sebelumnya.

German

Lain dengan Indonesia, Jerman yang merupakan sesama negara penganut sistem hukum *civil law seperti* telah memiliki kedua peraturan tersebut. Peraturan mengenai spionase beserta *spies* dan peraturan mengenai *cybercrime*. Peraturan mengenai spionase serta spies atau intelejen diatur dalam *German Criminal Code* atau *German Penal Code* atau dalam bahasa Jerman peraturan ini disebut dengan *Strafgesetzbuches*, dan disingkat menjadi StGB.[19] Peraturan ini dibagi menjadi 2 *part*, yang pertama adalah *General Part* dan yang kedua adalah *Special Part*. Kemudian setiap part dibagi menjadi *chapter* yang setiap *chapter* berisi beberapa *title* kemudian masuk ke dalam *section* atau pasal-pasalnya.

General Part berisi 79 section yaitu mulai dari section pertama hingga section 79, *part* ini berisi mengenai peraturan-peraturan umum seperti berlakunya peraturan dan hal-hal umum. Kedua adalah *Special Part* yang berisi perbuatan-perbuatan yang dianggap sebagai kejahatan di Jerman. *Special Part* ini dimulai dari *section* 80 hingga selesai, *section* 358. Dalam part ini baru dicantumkan mengenai tindak pidana, defininisi, serta hukuman. Mengenai spionase dan intelejen terdapat dalam *special part - chapter two* dengan judul *Treason And Endangering External National Security*.[20] Dicantumkan dalam chapter ini mengenai hal-hal yang menyangakut kemanan nasional, rahasia negara, serta agen hingga ancaman hukuman terhadap agen atau siapa saja yang melakukan hal yang dapat membahayakan keamanan negara.

Spionase terdapat pada section 94, dicantumkan bahwa;

---

[19] http://en.wikipedia.org/wiki/Strafgesetzbuch, (diakses 3 Juni 2014).

[20] **Germa Criminal code**, 1889, Federal Ministry of Justice and Consumer Protection, hlm. 53-57.

(1) Siapa saja
1. mengkomunikasikan rahasia negara kepada kekuatan asing atau salah satu perantara; atau
2. sebaliknya mengijinkan rahasia negara untuk mendatangkan perhatian dari orang yang tidak berhak atau menjadi diketahui oleh publik untuk merugikan Republik Federal Jerman atau menguntungkan kekuatan asing dan dengan demikian menciptakan bahaya prasangka serius terhadap keamanan eksternal dari Federal Republik Jerman, dipidana dengan pidana penjara tidak kurang dari satu tahun

ayat berikutnya berisi tentang lama hukuman bagi yang melakukan tindakan dalam ayat (1). Selanjutnya juga dicantumkan dalam section 96;

Section 96

Pengkhianatan spionase; memata-matai rahasia negara

(1) Barang siapa memperoleh rahasia negara dalam rangka untuk mengungkapkan itu (pasal 94) dapat dikenakan hukuman penjara dari satu sampai sepuluh tahun.
(2) Barang siapa memperoleh rahasia negara yang telah dirahasiakan oleh lembaga resmi atau atas perintah dalam rangka untuk mengungkapkan itu (pasal 95) bertanggung jawab untuk hukuman penjara onment dari enam bulan sampai lima tahun. Upaya tersebut dapat dihukum.

Hukum nasioanal Jerman, mengkatagorikan spionase dalam sebuah kejahatan yang dapat dijatuhi hukuman serius.

German Criminal Code atau *German Penal Code* atau dalam bahasa *Strafgesetzbuches*(StGB) juga mencantumkan mengenai *cybercrime*. *Cybercrime* diatur dalam section 202 hingga 303StGB.

Australia

Australia yang merupakan negara persemakmuran Inggris memiliki peraturan sendiri mengenai spionase. Hukum nasional Australia memasukkan tindakan atau kegiatan spionase ke dalam suatu bentuk kejahatan. Peraturan mengenai spionase terdapat dalam *Crimes Act* 1995 dan *Crimianl Code*

Amendement (Espionage and Relaed Matters) Bill 2002. *Criminal Code Act* 1995 menyebutkan tindakan apa saja yang termasuk dalam spionase dan hukuman yang dapat dijatuhkan pada pelaku. Sedangkan *Criminal Code Amendement Bill 2000* adalah penambahan peraturan dari peraturan *Criminal Code Act* 1995 dan *Crimes Act* 1914.

Menurut *Criminal Code Act* 1995 Division 90 (2)[21], kegiatan Spionase di gambarkan sebagai ekspresi mengacu pada memperoleh, rekaman, menggunakan, memiliki, berkomunikasi atau penahan termasuk memperoleh, rekaman, menggunakan, memiliki, berkomunikasi atau mempertahankan secara keseluruhan atau sebagian, dan baik hal atau informasi itu sendiri, atau hanya substansi, efek atau deskripsi dari hal atau informasi, diperoleh, tercatat, digunakan, dimiliki, dikomunikasikan atau dipertahankan; dan...

Yang dimaksud dengan "informasi" pada artikel tersebut adalah;

> **"*information*** *means information of any kind, whether true or false and whether in a material form or not, and includes:*
> *(a) an opinion; and*
> *(b) a report of a conversation.*"

Yang dalam bahasa Indonesia dapat diartikan segala macam bentuk baik benar atau tidak dan baik dalam bentuk materi tau tidak dan termasuk pendapat dan laporan sebuah percakapan, merupakan sebuah informasi. Selanjutnya *part* (2) (b) *Division* 90 melanjutkan tentang kegiatan spionase selain memperoleh, rekaman, menggunakan, memiliki dan berkomunikasi, yang termasuk dalam kegiatan spionase adalah mengacu ke sebuah sketsa, dokumen atau artikel atau

[21] Australia ***Criminal Code Act 1995***, *Act No. 12 of 1995 as amended*, hlm.87.

informasi yang harus dibaca, termasuk referensi untuk salinan, sebagian atau salinan bagian dari sketsa, dokumen atau artikel atau informasi.

Dalam *division* berikutnya yaitu *Division* 91[22], dicantumkan bahwa siapapun yang melakukan kegiatan seperti yang dijelaskan sebagi kegiatan spionase dalam Division 90 dengan tujuan merugikan keamanan dan pertahanan persemakmuran, memberikan keuntungan terhadap keamanan dan pertahanan negara lain, serta melakukan kegiatan tersebut tanpa kewenangan yang sah dihukum penjara selama 25 tahun. Lama hukuman penjara yang dijatuhkan bagi yang melakukan, menunjukkan bahwa kegiatan spionase merupakan kejahatan yang serius menyangkut keamanan dan pertahanan negara menurut Australia.

United States of America

Negara berikutnya yang mempunyai peraturan mengenai spionase selain German dan Australia adala USA. Peraturan mengenai spionase yang dimiliki USA hanya berisis beberapa *Section*, karena perturannya terpisah dengan yang lain. Berbeda dengan German dan Australia, peraturan mengenai kejahatan dikodifikasi dalam satu *Ciminal Code.* Di USA peraturan mengenai spionase diatur khusus dalam *The Espionage Act of* 1917. Menurut *The Espionage Act of* 1917

Section 1

(a) Siapa saja, untuk tujuan memperoleh informasi menghormati pertahanan nasional dengan maksud atau alasan untuk percaya bahwa informasi yang diperoleh akan digunakan untuk mencederai Amerika Serikat, atau keuntungan dari setiap bangsa asing, berjalan, masuk, terbang, atau memperoleh informasi, tentang ....."

[22]Australia ***Criminal Code Act 1995***, *Act No. 12 of 1995 as amended*, hlm.89-90.

(b) siapa pun untuk tujuan tersebut di atas, dan dengan seperti maksud atau alasan untuk percaya, salinan, mengambil, membuat, atau memperoleh, atau usaha, atau menginduksi atau alat bantu lain untuk menyalin, mengambil, membuat, atau memperoleh, sketsa apapun, foto, fotografi negatif, blue print, rencana, peta, model, instrumen, alat, dokumen, tulisan atau catatan apa pun yang berhubungan dengan pertahanan nasional; atau

section 1 berisi hingga huruf (e) yang mendefinisikan mengenai tindakan apa saja yang termasuk dalam *espionage*. Section berikutnya 2 hingga 9 menjelaskan sangsi pelanggaran serta berlakunya *The Espionage Act of* 1917.

Untuk cybercrime, USA mempunyai banyak peraturan dimana tiap tindakan dikelompokkan, beberapa diantaranya yaitu *Computer Software Privacy and Control Act*, *Department of Justice - Computer Crime and Intellectual Property Section*, *Electronic Communications Privacy Act*, *Electronic Communications Privacy Act*, *Economic Espionage Act (EEA)*, *Communications Assistance for Law Enforcement Act (CALEA)* dan masih banyak lagi. Sedangkan peraturan mengenai intersepsi atau penyadapan terdapat dalam *Communications Assistance for Law Enforcement Act of* 1994 (CALEA).

3. Peraturan di Indoneisa

Terlepas dari pasal mengenai *spies* dalam *Hague Convention IV* 1907, sama halnya dengan dunia Internasional, di Indonesia pengaturan khusus mengenai spionase juga tidak ada. Namun dicantumkan dalam beberapa Undang-undang, pengaturan sekilas mengenai penyadapan yang bisa dikatakan sebagai bentuk baru dari spionase dalam perkembangan teknologi dan informasi sekarang. Undang-undang yang mencantumkan sekilas mengenai penyadapan in adalah Undang-undang No.36 Tahun 1999 tentang Telekomunikasi dan Undang-undang

No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Poin dari kedua Undang-undang tersebut adalah bahwa Penyadapan merupakan kegiatan yang dilarang.

Lain dengan Undang-undang tentang Telekomunikasi dan Undang-undang tentang Informasi dan Transaksi Elektronik, Peraturan Menteri NO: 11/PER/M.KOMINFO/02/2006 tentang Teknis Penyadapan Terhadap Informasi, merupakan salah satu peraturan yang memperbolehkan penyadapan. Dimana peraturan ini berisi tentang teknis dari kegiatan penyadapan. Kemudian terdapat peraturan lain, yaitu Peraturan Kepala Kepolisian No.5 tahun 2010 tentang Tata Cara Penyadapan Pada Pusat Pemantauan Kepolisian Negara Republik Indonesia.

Penyadapan pada dasarnya hanya dibolehkan bagi petugas yang berwenang dalam suatu negara guna meningkatkan pengawasan tingkat tinggi dan dilakukan sepenuhnya untuk kepentingan keamanan negara agar mampu mempertahankan dan meningkatkan kemampuan melawan tindakan teror. Kewenangan penuh untuk menerapkan penyadapan yang sah secara hukum tersebut dikenal denganistilah *lawful interception*.[23]

Penyadapan yang sesuai dengan hukum atau dapat dikatakan dengn penyadapan yang sah (*lawful interception*) bukanlah sesuatu yang baru dalam kehidupan masyarakat internasional.[24] Dikatakan demikian karena dalam 50-60 tahun terakhir pemerintah di seluruh dunia telah dievaluasi dan diperkenankan untuk menggunakan sistem yang mampu melacak informasi dan telekomunikasi,

[23] Firman Nuro, **Aspek Hukum Mengenai Monitoring Aktivitas Komputer dan Tindak Pidana Penyadapan Data Pribadi Pengguna Internet**, jbptunikompp-gdl-firmannuro-24692-4-babii.pdf, hlm. 22. (Diakses 28 Februari 2014).

[24] Kristian dan Yopi Gunawan, 2013, **Sekelumit Tentang Penyadapan Dalam Hukum Positif Di Indonesia**, Nuansa Aulia, Bandung, hlm.182.

yakni penyadapan.[25] Dalam bahasa Indonesia sendiri, istilah *lawful interception*, secara sederhana dapat diartikan sebagai intersepsi yang didasarkan pada hukum atau intersepsi yang dilakukan sesuai dengan hukum atau penyadapan yang sesuai dengan hukum atau prosedur yang berlaku dan dilakukan oleh otoritas yang berwenang untuk itu.[26]

Selanjutnya, Romanidis Evipidis dan Gerald Q. Maguire menjelaskan bahwa lembaga yang berwenang untuk melakukan tindakan penyadapan adalah "*the mediator organizations*" atau dapat disebut dalam bahasa Indonesia sebagai organisasi mediator yang berdiri sebagai lembaga yang ingin melakukan tindakan penyadapan dan operator jaringan.[27]Di Indonesia pihak yang berwenang melakukan penyadapan menurut Undang-undang adalah aparat penegak hukum, yaitu Kepolisian, Kejaksaan, Komisi Pemberantasan Korupsi, Badan Intelejen Nasional, dan Badan Narkotika Nasional.

Dasar hukum mengenai pihak yang berwenang melakukan penyadapan terdapat pada undang-undang yang berbeda sesuai dengan tindak pidana yang dilakukan. Beberapa peraturan yang mencantumkan mengenai pihak berwenang yang melakukan penyadapan adalah Undang-undang No.36 Tahun 1999 tentang Telekomunikasi, Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Menteri NO: 11/PER/M.KOMINFO/02/2006 tentang Teknis Penyadapan Terhadap Informasi dan Peraturan Kepala Kepolisian

---

[25] Kristian dan Yopi Gunawan,*ibid*.
[26]Kristian dan Yopi Gunawan, *ibid*.
[27] Romanidis Evipidis dan Gerald Q. Maguire**,** ***Lawful Interception and Countermeasures***, Master of Science Thesis Stockholm, Sweden, 2008, hlm.4

No.5 tahun 2010 tentang Tata Cara Penyadapan Pada Pusat Pemantauan Kepolisian Negara Republik Indonesia.

C. Upaya Indonesia Dalam Mengatasi Tidakan Spionase Melalui Penyadapan Antar Negara

Pemberitaan media yang merespon paparan informasi dari harian berita Australia, *Australian Broadcasting Corporation* (ABC) dan *Sydney Morning Herald* mengenai dokumen penyadapan pejabat tinggi Indonesia menjadi puncak dari berbagai pemberitaan mengenai negara tetangga di sebelah tenggara tersebut.[28] Di Indonesia, Anggota Komisi I DPR Meutya Hafid meminta agar Pemerintah mengusir Duta Besar Australia Greg Moriarty dari Indonesia. Bukan tanpa alasan, pengusiran itu bisa dilakukan karena Australia telah melanggar Pasal 9 Konvensi Wina tahun 1961 mengenai hubungan diplomatik. Dalam pasal itu disebutkan pengusiran kepada duta besar bisa dilakukan jika wakil diplomatik itu melanggar tiga hal. Pertama, duta besar melakukan kegiatan yang subversif dan merugikan kepentingan nasional. Kedua, kegiatan yang dilakukan oleh wakil diplomatik melanggar hukum atau perundang-undangan negara penerima. Ketiga kegiatan yang digolongkan sebagai kegiatan mata-mata atau spionase yang dapat mengganggu stabilitas keamanan negara penerima.[29]

Menanggapi kejadian tersebut, baik Perdana Menteri Australia Tony Abbott maupun Presiden Indonesia Susilo Bambang Yudhoyono (SBY) telah

---

[28]R. Aj. Rizka F. Prabaningtyas, Indonesia–Australia: Menguji Persahabatan di Tengah Konflik Penyadapan,Institute of International Studies Universitas Gadjah Mada, https://www.iis.fisipol.ugm.ac.id. (Diakses 12 Jui 2014)

[29]Ita Lismawati F. Malau, Nila Chrisna Yulika, Sadap Indonesia, Australia Langgar Konvensi Wina: Australia melancarkan aksi spionase kepada Indonesia, http://politik.news.viva.co.id/news/read/460248-sadap-indonesia--australia-langgar-konvensi-wina, (diakses 31 Desember 2013)

berkomentar tentang skandal tuduhan spionase yang terlihat memanaskan hubungan kedua negara.Tanggal 19 November lalu, Abbott berkata di hadapan parlemen Australia, "Semua pemerintahan mengumpulkan informasi dan ... semua pemerintahan tahu bahwa pemerintahan lain mengumpulkan informasi."Sementara itu, SBY mengatakan dalam sebuah pernyataan yang disiarkan lewat televisi bahwa menurutnya, baik hukum Indonesia, Australia, maupun hukum internasional, tidak memperbolehkan penyadapan pejabat-pejabat negara lain.[30]

Di Indonesia hal-hal mengenai spionase dan penyadapan bisa dikatakan bukan hal yang biasa. Dimana kegiatan ini merupakan hal yang dilarang menurut hukum nasional dengan pengecualian bahwa kegiatan tersebut dilakukan oleh pejabat yang berwenang. Seperti yang telah dibahas sebelumnya, di Indonesia pejabat yang berwenang melakukan penyadapan atau intersepsi adalah aparat penegak hukum yang diberi kewenangan oleh undang-undang. Selain aparat penegak hukum yang diberi kewenangan oleh undang-undang, penyadapan atau intersepsi juga dilakukan pada masalah hukum tertentu yang juga ditentukan oleh undang-undang dengan tujuan utama yakni penegakan hukum. Selain itu di Indonesia juga belum mempunyai peraturan khusus mengenai penyadapan, spionase maupun kegiatan lain yang berhubungan dengan kegiatan mata-mata. Permasalahan yang kini terjadi, kegiatan penyadapan dilakukan oleh negara lain kepada Indonesia. Menurut beberapa surat kabar, bahwa gedung kedutaan Australia digunakan sebagai pusat pemantauan penyadapan.

---

[30]Egidius Patnistik (Ed) - ABC Australia, Langgar Hukumkah bila Australia Sadap Telepon Pejabat Indonesia?, www.kompas.com. (Diakses 31 Desember 2013)

Pada dasarnya perintah penyadapan yang diberikan Australia kepada wakil diplomatiknya yang berada di Indonesia adalah bertentangan dengan hukum nasional Indonesia, meskipun hal tersebut merupakan perintah yang diberikan secara resmi. Baik yang melakukan kegiatan tersebut secara langsung adalah Perdana Menteri, perwakilan diplomatik yang lain atau intelejen negara Australia. Sehingga, apabila terbukti terbukti Australia telah melakukan penyadapan kepada Indonesia dengan tujuan spionase dan menggunakan gedung keduataan Australia sebagai pusat pemantauan, maka pemeritah perlu menanggapi dan menangani hal ini dengan cermat. Pertama, kegiatan penyadapan ini dilakukan di Indonesia. Maka hukum indonesia dapat diberlakukan sesuai aturannya. Sesuai dengan Undang-undang No.36 Tahun 1999 tentang Telekomunikasi serta Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dimana kegiatan penyadapan yang tidak sah atau *unlawfull interception* merupakan pelanggaran hukum di Indonesia. Maka pelaku dapat dikenai sanksi sesuai dengan undang-undang yang berlaku. Apabila tindakan penyadapan dilakukan oleh agen tertentu yang ditugaskan untuk melakukan spionase maka hukum nasional dapat diberlakukan kepada agen tersebut. Kedua, terkait tentang kantor kedutaan Australia di Indonesia yang digunakan sebagai pusat kegiatan spioase melalui penyadapan, hal ini bertentengan dengan pasal 9 *Vienna Convention* 1961 tentang hubungan diplomatik. Pemerintah Indonesia dapat melakukan *persona non-grata* kepada perwakilan diplomatik Australia untuk Indonesia atau dapat dilakukan pemutusan hubungan diplomatik apabila tindakan yang dialakuak adalah kegiatan yang subversif dan merugikan kepentingan nasional seta membahayakan keamanan dan pertahanan Negara Indonesia.

Terlepas dari masalah dalam sisi hubungan diplomatik, tindakan yang dilakukan Australia memang bertentangan dengan hukum nasional Indonesia dan tindakan tersebut dapat dikatakan sebagai pelanggaran kedaulatan dalam hukum internasional. Di dalam beberapa konvensi internasional juga dicantumkan bahwa *illegal interception* merupakan salah satu bagian dari *cybercrime*. Terkait penyadapan dalam hukum nasional Indonesia, kegiata ini secara tegas dilarang kecuali dilakukan oleh pihak yang berwenang. Sesuai dengan bentuk penyadapan dan *cybercrime* di Indonesia tindakan Australia dapat dipastikan melanggar hukum Indonesia.

Namun, dalam permasalahan ini tidak dapat begitu saja memberlakukan hukum nasional meskipun tindakan yang dilakukan Australia adalah melanggar hukum nasional. Selain dengan penyelesaian melalui penyelesaian diplomatik. Persoalan antar negara ini juga dapat diselesaikan melalui Mahkamah Internasional atau International Court of Justice. Dengan begitu Mahkama internsional akan memutuskan masalah tersebut. Dengan catatan bahwa kedua belah pihak setuju dilakukan penyelesaian masalah melalui Mahkama Internasional. Sesuai dengan perkembangan permasalah yang terjadi ini Indonesia telah mengajukan penyelesaian sengketa ini ke Mahkamah Internasional. Bukan hanya Indonesia satu-satunya negara yang mengajukan permasalahan ini ke Mahkamah Internasional, German dan Brasil serta beberapa negara lainnya yang menjadi korban penyadapan juga merancang Resolusi PBB tentang kode etik mengenai *Cyberspace*.[31] Kabar terakhir, bahwa Resolusi yang diajukan negara-

[31]Muhaimin, **FOKUS DUNIA: Kemarahan dunia atas spionase AS memuncak,**http://international.sindonews.com/read/2013/10/26/45/798548/kemarahan-dunia-atas-spionase-as-memuncak, tertanggal 9 Desember 2013.

negara korban penyadapan ini telah disetujui oleh PBB. Namun, resolusi mengenai *Cyberspace* yang juga termasuk *Cybercrime* dan penyadapan ini belum beredar pada masyarakat luas.

Berkaca dari permasalahan yang telah terjadi baik yang dialami Indonesia maupun yang terjadi di luar negeri, Indonesia harus meningkatkan kehati-hatian dalam segala hal yang berhubungan langsung dengan negara lain. Baik hal mengenai perjanjian ataupun sekedar hubungan baik dengan negara lain. Selain itu pemerintah Indonesia juga harus meningkatkan kualiatas keamanan Negara terutama mengenai data dan informasi rahasia negara, baik dalam bentuk manual ataupun data elektronik. Memperbanyak ahli dalam bidang informasi dan telekomunikasi yang berkompeten dan benar-benar menguasai materi dalam bidang informasi dan telekomunikasi serta teknologi.

BAB V

KESIMPULAN DAN SARAN

1. Kesimpulan

Dilihat dari beberapa karakteristik *cybercrime* terhadap spionase dan penyadapan, maka spionase melalui penyadapan dapat dikategorikan sebagai cybercrime. Karakteristik yang pertama *Unauthorized acces* atau akses tidak sah, kegiatan spionase merupakan kegiatan yang *Non-violance* (tanpa kekerasan), Sedikit melibatkan kontak fisik *(minimaze of physical contact*), menggunakan peralatan *(equipment*), teknologi, dan memanfaatkan jaringan telematika (telekomunikasi, media dan informatika) global, Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional. Selain itu berdasarkan bentuk dari cybercrime maka penyadapan dapat masuk di beberapa bentuk seperti;*Unauthorized Acces to Computer System and Service*, *Cyber Espionage*, *Infringements of Privacy*, dan *Cyber-stalking*.

Berdasarkan hukum nasional Indonesia, Undang-undang No.36 Tahun 1999 tentang Telekomunikasi dan Undang-undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tindakan yang dilakukan Australia melanggar hukum nasional Indonesia. Namun, dalam permasalahan ini tidak dapat begitu saja menerapkan hukum nasional meskipun tindakan yang dilakukan Australia adalah melanggar hukum nasional. Selain dengan penyelesaian melalui

penyelesaian diplomatik. Persoalan antar negara ini juga dapat diselesaikan melalui Mahkamah Internasional atau International Court of Justice.

2. Saran

Pemerintah Indonesia lebih meningkatkan kehati-hatian dalam segala hal yang berhubungan dengan negara lain. Baik hal mengenai perjanjian ataupun sekedar hubungan baik dengan negara lain. Selain itu pemerintah Indonesia juga harus meningkatkan kualiatas keamanan Negara terutama mengenai data dan informasi rahasia negara, baik dalam bentuk manual ataupun data elektronik. Memperbanyak ahli dalam bidang informasi dan telekomunikasi yang berkompeten dan benar-benar menguasai materi dalam bidang informasi dan telekomunikasi serta teknologi. Selain itu pemerintah juga harus segera mempunyai Undang-undang yang khusus membahas mengenai *cybercrime* serta spionase atau intersepsi dalam perkembangan teknologi.