

“CYBERCRIME” DAN KAITANNYA DENGAN BEBERAPA KEGIATAN DI LAUT

Etty R. Agoes*

Abstrak

Pada jaman digital dimana komunikasi secara *online* telah menjadi suatu keharusan, pengguna internet dan negara-negara dihadapkan pada ancaman serangan melalui dunia maya. Para penjahat siber terus mengembangkan teknik serangannya, mereka juga mulai mengalihkan targetnya dengan mengurangi pencurian informasi perbankan atau keuangan dan beralih ke spionase business dan mengakses informasi dari situs-situs pemerintah. Untuk melawan *cybercrime* yang berkembang dengan sangat pesat negara-negara harus bekerjasama untuk mengembangkan suatu model yang efektif untuk mengawasi ancaman-ancaman demikian. Ancaman terhadap pelayaran internasional hari ini tidak lagi datang hanya dari para pembajak maupun teroris, tetapi para peretas (*hackers*) melalui komputer, baik yang berada di atas kapal maupun jauh di daratan. Dampak dari kejahatan dunia maya tersebut tidak hanya terasa di bidang pelayaran, tetapi di bidang-idang pemanfaatan laut lainnya seperti kabel dan pipa di dasar laut. Tulisan ini akan mencoba untuk melihat sejumlah kegiatan pemanfaatan laut yang rawan terkena *cybercrime* terutama dikaitkan dengan sejumlah aktivitas dilaut seperti pelayaran, baik oleh kapal niaga, kapal perang, maupun kapal pemerintah yang dioperasikan untuk kepentingan niaga maupun bukan, kapal yang bertenaga nuklir maupun yang mengangkut nuklir atau bahan lain yang karena sifatnya berbahaya atau beracun, yang diatur oleh UNCLOS 1982.

Kata Kunci: *cybercrime*, digital, laut

Abstract

In the digital era where online communication has become a necessity, internet users and the states have to overcome the threat through cyberspace. The cyber criminals simultaneously develop they attack techniques and also began to shift the target from banking or financial information to business espionage and access information from government websites. To overcome the threats from cybercrime, states should work together and develop an effective model for overseeing such threats. Threats to international shipping today no longer come only from the hijackers or terrorists, but also from the hackers through a computer. The hackers can be located on the boat or in the main island. The impact of cyber crime is not only to the shipping, but also in another fields such as cables and pipelines on the seabed. This paper will try to see a number of activities that are vulnerable to the cybercrime in particular related to the a number of activities at sea such as shipping, either by commercial ships, warships, as well as government ship operated for

* Fakultas Hukum Universitas Padjadjaran, anggota Dewan Kelautan Indonesia (DEKIN) dan anggota Dewan Pakar Komunitas Hukum Padjadjaran, email: era@gmail.com

commercial or not, a ship with nuclear-powered or carrying nuclear or other materials that are inherently dangerous or toxic, regulated by UNCLOS 1982.

Keyword: *cybercrime, sea, digital*

Pendahuluan

Pada jaman digital dimana komunikasi secara *online* telah menjadi suatu keharusan, pengguna internet dan negara-negara dihadapkan pada ancaman serangan melalui dunia maya. ketika para penjahat siber terus mengembangkan teknik serangannya, mereka juga mulai mengalihkan targetnya dengan mengurangi pencurian informasi perbankan atau keuangan dan beralih ke spionase business dan mengakses informasi dari situs-situs pemerintah. Untuk melawan *cybercrime* yang berkembang dengan sangat pesat negara-negara harus bekerjasama untuk mengembangkan suatu model yang efektif untuk mengawasi ancaman-ancaman demikian.

Pada awal abad ke 19, pembajakan di laut merupakan ancaman keamanan yang terus berkembang, namun kemudian menurun dan hanya terjadi di sekitar lepas pantai negara-negara dengan pemerintahan yang lemah tanpa kekuatan untuk melawan ancaman demikian, seperti misalnya di lepas pantai Somalia. Namun demikian pembajakan tidak hapus secara keseluruhan, dan berpindah serta berkembang melalui jaringan komputer, yang mengakibatkan kerugian terhadap perusahaan-perusahaan dan para konsumen dalam jumlah milyaran dollar Amerika.

Oleh karena itu dewasa ini, ancaman terhadap pelayaran internasional tidak lagi datang hanya dari para pembajak maupun teroris, tetapi para peretas (*hackers*) melalui komputer, baik yang berada di atas kapal maupun jauh di daratan. Dampak dari

kejahatan dunia maya tersebut tidak hanya terasa di bidang pelayaran, tetapi di bidang-bidang pemanfaatan laut lainnya seperti kabel dan pipa di dasar laut.

Tulisan ini akan mencoba untuk melihat sejumlah kegiatan pemanfaatan laut yang rawan terkena *cybercrime*. Kalau dilihat dari pengaturan Konvensi PBB tentang Hukum Laut (UNCLOS) 1982, di dalamnya diatur berbagai jenis kegiatan yang mengambil tempat di laut, seperti misalnya pelayaran, baik oleh kapal niaga, kapal perang, maupun kapal pemerintah yang dioperasikan untuk kepentingan niaga maupun bukan, kapal yang bertenaga nuklir maupun yang mengangkut nuklir atau bahan lain yang karena sifatnya berbahaya atau beracun. UNCLOS 1982 juga mengatur berbagai hak lintas bagi kapal-kapal asing untuk melalui perairan dari suatu negara (termasuk negara kepulauan), yaitu hak lintas damai (*innocent passage*), hak lintas transit (*transit passage*), dan hak lintas alur-alur laut kepulauan (*archipelagic seallanes passage*).

Disamping itu juga diatur tentang pemanfaatan sumberdaya alam baik hayati maupun non-hayati, survei dan riset ilmiah kelautan, pengembangan dan alih teknologi kelautan. Luasnya berbagai bentuk kegiatan di laut dikaitkan dengan berkembangannya teknologi informasi, yang baik secara langsung maupun tidak langsung akan berpengaruh pada kegiatan-kegiatan tersebut, cukup menarik untuk dijadikan bahan kajian, namun dalam waktu yang sangat terbatas tidak mungkin bagi penulis untuk membahasnya melalui satu

tulisan ini saja.

A. Apakah Cybercrime Itu?

Dari beberapa sumber bacaan, penulis dihadapkan pada berbagai istilah yang mengkaitkan dunia maya atau siber dengan tindakan-tindakan yang dapat menimbulkan ancaman dan kerugian pada pihak lain selain yang dikenal sebagai *cybercrime*, juga *cyberattack* dan *cyberaggression*, yang kemudian disimpulkan tentang perlunya suatu *cybersecurity*. Sulit untuk membuat suatu definisi tentang *cybercrime*. Apabila didefinisikan terlalu luas sebagaimana yang dibahas oleh kelompok bilateral Amerika Serikat dan Rusia *cybercrime* dianggap sebagai "*cyberspace for criminal purposes as defined by national or international law.*"¹ Sebaliknya apabila didefinisikan secara sempit sebagaimana yang pernah dilakukan oleh suatu panel PBB dianggap sebagai "*electronic operations that targets the security of computer systems*" maka akan melewati kejahatan *online* yang bergantung pada tipuan dan bukan pada kemampuan teknis, misalnya tipuan-tipuan dalam bentuk permintaan transfer sejumlah uang ke rekening tertentu dari si penipu.²

Permasalahan menjadi makin rumit disebabkan oleh kenyataan bahwa, pada internet, tidak mudah untuk membedakan seseorang sebagai penjahat, mata-mata atau prajurit pejuang, karena ketiganya

dapat membuat kesalahan yang sama dalam menggunakan *internet explorer* untuk memperoleh akses ke internet, dan ketiganya dapat menggunakan perangkat lunak (*software*) yang sama untuk mencari lubang-lubang peretasan pada jaringan komputer. Apakah hasilnya berupa suatu tindak pidana, spionase atau dokumen intelijen untuk perang, pada akhirnya akan tergantung pada maksud dari orang yang melakukan peretasan tersebut. *Council of Europe* yang telah berhasil menyusun suatu *Convention on Cybercrime*³ bahkan tidak berhasil memberikan definisi tentang *cybercrime* di dalamnya.

Dari penelusuran melalui internet penulis menemukan beragam definisi tentang *Cybercrime*, beberapa contoh, diantaranya adalah:

1. *Cyber crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.*
2. *Any crime that involves a computer and a network is called a "Computer Crime" or "Cyber Crime".*⁵
3. *A crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).*⁶
4. *In a nutshell, it is simply a crime that has some kind of computer or cyber aspect*

¹ Karl Frederick Rauscher and Valery Yaschenko, "Russia-U.S. bilateral on Cybersecurity Critical Terminology Foundations," p. 27, April, 2010, <<http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations>>, diunduh tanggal 1 November 2015.

² Noah Shachtman, "Pirates of the ISPs : Tactics for Turning Online Crooks Into International Pariah," *Brooking Institutions*, Cyber Security #1, July, 2011., p. 5

³ Budapest Convention on Cybercrime, 23 November 2001, European Treaty Series No. 185.

⁴ study.com/academy/.../what-is-cyber-crime-definition-types-examples, diunduh tanggal 7 November 2015.

⁵ bytes-notes.com, diunduh tanggal 7 November 2015.

⁶ <https://www.techopedia.com/definition/2387/cybercrime>, diunduh tanggal 7 November 2015.

*to it. To go into more detail is not as straightforward, as it takes shape in a variety of different formats.*⁷

Situs Hukumonline memberikan hasil kajian tentang definisi cybercrime berdasarkan dua sumber pendapat yaitu dari Susan Brenner dan Nicholson, sebagai berikut:⁸

“Menurut Sussan Brenner (2011) membagi cybercrimes menjadi tiga kategori:

1. *crimes in which the computer is the target of the criminal activity,*
2. *crimes in which the computer is a tool used to commit the crime, and*
3. *crimes in which the use of the computer is an incidental aspect of the commission of the crime.*

Sedangkan, Nicholson menggunakan terminology *computer crimes* dan mengkategorikan *computer crimes* (*cybercrimes*) menjadi objek maupun subjek tindak pidana serta instrumen tindak pidana.

[first, a computer may be the ‘object’ of a crime: the offender targets the computer itself. This encompasses theft of computer processor time and computerized services. Second, a computer may be the ‘subject’ of a crime: a computer is the physical site of the crime, or the source of, or reason for, unique forms of asset loss. This includes the use of ‘viruses’, ‘worms’, ‘Trojan horses’, ‘logic bombs’, and ‘sniffers.’ Third, a computer may be an ‘instrument’ used to commit traditional crimes in a more complex manner. For example, a computer might be used to collect credit card information to make fraudulent purchases.

Lebih jauh dalam situs yang sama dijelaskan bahwa dalam instrumen yang dikeluarkan oleh PBB melalui *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10-17 April 2000, *cybercrime* dapat dilihat secara sempit maupun secara luas, yaitu:

- (a) *Cybercrime in a narrow sense (“computer crime”): any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them;*
- (b) *Cyber crime in a broader sense (“computer-related crime”): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.*

Oleh karena tidak ada keseragaman dalam definisi *cybercrime*, dalam makalah ini penulis mengartikan *cybercrime* sebagai tindakan dimana komputer, jaringan (*network*) dan perangkat lunak (*software*) digunakan untuk suatu tindak pidana, dimana korban ditargetkan melalui penggunaan sarana dan prasarana elektronik tersebut. Sebagai contoh, berbagai macam kegiatan ilegal tersebut, antara lain jaringan situs-situs palsu yang dimaksudkan untuk menipu orang-orang, misalnya untuk memberikan nomor rekening bank-nya, yang biasa dikenal sebagai kegiatan “*phishing*”. Ada juga yang disebut “*malware*” (*malicious software*)” yang biasanya digunakan untuk menguasai komputer dan mencuri informasi atau data yang ada didalamnya. Ada juga yang memasuki jaringan suatu perusahaan untuk mencuri rahasia perusahaan tersebut.

⁷ us.norton.com, diunduh tanggal 7 November 2015.

⁸ hukumonline.com, diunduh tanggal 8 November 2015.

Menurut Shachtman,¹⁰ berbeda dengan senjata nuklir yang hanya dapat dimiliki oleh beberapa negara saja, senjata peretas digital dapat dimiliki oleh siapa saja, mulai dari para penjahat biasa sampai negara adidaya. Para peretas dapat meloncat melintasi batas negara dengan kecepatan yang dapat mengalahkan kecepatan di darat, udara maupun laut. Lebih jauh lagi mereka dapat menyembunyikan identitasnya, meskipun mereka meloncat dari satu tempat ke tempat lain.

B. Cybercrime dan Beberapa Kegiatan di Laut

Ajang permainan para *hacker* di laut khususnya di laut lepas, misalnya dirasakan oleh tanker pengangkut minyak dan kapal kargo yang mengangkut kurang lebih 90 persen dari barang-barang yang diangkut ke seluruh dunia. Pada era teknologi informasi dewasa ini, dimana berbagai bentuk produk teknologi digunakan secara *online*, akan menjadi makin rawan terhadap serangan dari luar. Ketika industri maritim dan energi menghubungkan kapal-kapal (termasuk kapal tanki), *containers* dan anjungan minyak lepas pantai melalui jaringan komputer, maka mereka makin terbuka dan rawan akan ancaman dari para peretas (*hackers*).

Beberapa waktu yang lalu para peretas telah berhasil memiringkan suatu anjungan minyak terapung (*floating oil rig*), dan diperlukan kurang lebih satu minggu untuk mencari penyebab dan mereparasinya karena tidak ada ahli cybersecurity di atas anjungan tersebut. Anjungan lain komputernya diretas

dan memerlukan kurang lebih 19 hari untuk memperbaikinya sehingga sistemnya dapat berjalan kembali. Dalam pada itu para pembajak Somalia memilih targetnya dengan membaca data-data navigasi yang dapat diperoleh secara *online*.

Untuk menghindari hal demikian banyak kapal-kapal yang mematikan alat-alat navigasinya atau dengan memasukkan data-data palsu untuk memberi gambaran kapalnya sedang berada di tempat lain. Para peretas ini juga pernah berhasil memasuki jaringan komputer yang terhubung dengan pelabuhan Antwerpen di Belgia, dan berhasil mendeteksi sejumlah *containers* dan menyelundupkan kargonya sambil menghapus data-data terkait pada jaringan komputer tersebut.¹¹

Diperkirakan bahwa secara global kerugian yang diakibatkan oleh kejahatan dunia maya terhadap sarana industri minyak dan gas akan mencapai US \$ 1,9 milyar hingga tahun 2018. Pemerintah Inggris bahkan telah mengestimasi kerugian sekitar US \$ 672 juta per tahun.¹²

Dengan makin berkurangnya penggunaan awak kapal dan kapal-kapal dibuat makin besar, perusahaan pelayaran sangat bergantung pada otomatisasi dan pengawasan jarak jauh melalui komputer, yang berarti bahwa komponen-komponen kunci termasuk sistem navigasi melalui komputer dengan mudah terbuka untuk dapat diretas.

Dewasa ini kapal-kapal yang berlayar di laut banyak menggunakan teknologi digital sebagai standar yang didukung oleh

⁹ *Ibid.*

¹⁰ *Id, supra*, n.3.

¹¹ Jeremy Wagstaff, "All at sea: global shipping fleet exposed to hacking threat", <http://www.reuters.com/news/picture/all-at-sea-global-shipping-fleet-exposed?>, diunduh tanggal 29 Oktober 2015.

¹² *Ibid.*

International Maritime Organisation (IMO), dan telah mewajibkan penggunaannya bagi kapal-kapal niaga dan kapal angkut (*passenger ships*) dengan ukuran besar, seperti *Global Positioning System (GPS)*, *Automatic Identification System (AIS)* dan sistem untuk membaca peta pelayaran (*navigational chart*) yang dikenal sebagai *Electronic Chart Display and Information System (ECDIS)*. Namun, untuk menghindari para pembajak banyak kapal-kapal yang menutup penggunaan AIS.

Selain dari itu, untuk meningkatkan produksi, biaya dan jadwal pengiriman barang, industri maritim dan sektor energi berpaling pada penggunaan teknologi. Perubahan dengan menggunakan teknologi elektronik telah membuka peluang masuknya berbagai ancaman baru karena teknologi tersebut juga tersedia secara bebas bagi pihak luar.

Menurut Wagstaff, suatu perusahaan Israel, *Winward*, yang mengumpulkan dan menganalisis data AIS, menemukan 100 kapal yang mengirimkan lokasi yang salah melalui AIS dalam satu hari sebagian besar tujuannya adalah untuk alasan keamanan atau finansial-misalnya kapal-kapal penangkap ikan yang beroperasi di luar wilayah penangkapan yang telah ditetapkan atau dalam hal penyelundupan.¹³ Menurut sumber yang sama, dalam suatu laporan PBB tentang tuduhan adanya usaha Korea Utara untuk memperoleh senjata nuklir, para penyidik melaporkan adanya satu kapal yang mengangkut kargo yang disembunyikan telah mematikan sinyal AIS untuk menyamarkan dan menyembunyikan pelayarannya ke Cuba.¹⁴

Dalam pada itu, *Convention on the Safety of Life at Sea (SOLAS)* yang disusun oleh *International Maritime Organization (IMO)* telah menetapkan kewajiban bahwa semua kapal harus memiliki peta elektronik ECDIS, paling lambat tahun 2018. Akan tetapi, apabila sistem ECDIS tersebut dipasang secara tidak benar atau sempurna-misalnya apabila sistem tersebut tidak dipisahkan dari sistem informasi telekomunikasi kapal secara keseluruhan, misalnya dengan memasang *firewall*, maka sistem tersebut akan sangat terbuka untuk diretas, dan memungkinkan kapal untuk diarahkan ke rute yang bukan sebenarnya.

Dalam suatu makalah yang ditulis oleh Rabkin dan Rabkin, *cybercrime* atau *cyber attacks* bahkan diarahkan kepada hukum tentang konflik bersenjata di laut lepas, dengan menyatakan bahwa¹⁵:

"The historic practice of naval war is a much better guide to reasonable tactics and necessary limits for conflicts in cyberspace. Cyber conflict should be open-as naval war has been-to hostile measures short of war, to attacks on enemy commerce, to contribution from private auxiliaries. To keep such measures within safe bounds, we should consider special legal constraints, analogous to those traditionally enforced by prize courts."

Di kawasan yang berbatasan dengan Indonesia yaitu Laut Tiongkok Selatan, keamanan dunia maya (*cybersecurity*) erat kaitannya dengan masalah keamanan maritim di kawasan ini. Kawasan ini merupakan tempat

¹³ Jeremy Wagstaff, "All at sea: global shipping fleet exposed to hacking threat", *Reuters*, Singapore, Apr 23, 2014.

¹⁴ *Ibid.*

¹⁵ Jeremy Rabkin and Ariel Rabkin, "Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea", *Chicago Journal of International Law*, Vol. 14, No. 1, Article 7, June 1, 2013.

peletakkan kabel dan pipa dasar laut yang sangat penting. Khususnya kabel-kabel di dasar laut merupakan alat komunikasi yang sangat penting. Situasi di jazirah Korea dapat meningkatkan kemungkinan terjadinya perang di dunia maya.

Pada bulan Mei 2010, *East West Institute (EWI)* menyelenggarakan pertemuan tingkat tinggi yang disebut *Worldwide Cybersecurity Summit* di Dallas, Texas. Pada pertemuan tersebut kabel-kabel komunikasi di dasar laut di kawasan ini telah diidentifikasi sebagai komponen jaringan siber yang sangat penting dan keamanannya dianggap krusial, dan bahwa "*... satellites cannot handle the volume of traffic -- the available capacity is not even close, without cables, markets would freeze.*" Lebih jauh dilaporkan bahwa:¹⁶

"... the impact of such a failure on international security and economic stability could be devastating...There is no sufficient alternative back-up in the case of a catastrophic loss of regional or global connectivity. A single disaster in such an area could cause catastrophic loss of regional and global connectivity."

Menurut Konvensi PBB tentang Hukum Laut (UNCLOS) 1982, peletakkan kabel dan pipa di dasar laut manapun merupakan hak bagi semua negara di dunia, termasuk untuk memeliharanya dan bilamana perlu menggantinya.¹⁷ Di kawasan Laut Tiongkok Selatan yang masih menjadi obyek sengketa kewilayahan dan melibatkan sejumlah negara yang berbatasan dengannya, penggantian

atau pemeliharaan kabel-kabel tersebut sangat sukar dilaksanakan. Kondisi seperti itu dapat menimbulkan dampak global terhadap berbagai pelayanan, antara lain, finansial, media, transportasi, industri energi, disamping pelayanan pemerintah dan kemanan dari negara-negara terkait. Dalam era digital seperti ini, dalam hubungan internasional di bidang maritim, diplomasi maritim untuk menjamin keamanan dunia maya tampaknya sangat jauh untuk dapat dilaksanakan.

Meningkatnya manuver maritim dan reklamasi pantai di kepulauan Spratlys akhir-akhir ini, telah meningkatkan kekhawatiran akan timbulnya insiden di laut yang akan meningkatkan ketegangan bahkan mungkin menimbulkan konflik di Laut Tiongkok Selatan. Pada tanggal 27 Oktober 2015, *destroyer* Amerika Serikat, USS Larsen, memasuki wilayah perairan 12 mil dari Subi Reef yang merupakan batu karang yang diklaim oleh Tiongkok. Kapal-kapal angkatan laut Tiongkok membayang-bayangi *destroyer* tersebut sampai keluar dari wilayah perairan Subi Reef dan Mischief Reef. Tindakan provokatif Tiongkok dengan melakukan reklamasi di Subi Reef, dan dengan membangun helipad, dermaga, stasiun pengamat cuaca dan bangunan empat tingkat di bagian yang telah direklamasi. Dikabarkan bahwa Tiongkok juga sedang melakukan reklamasi untuk membangun landasan pacu pesawat terbang yang mampu memenuhi kebutuhan pesawat terbang militer.¹⁸

¹⁶ Fred Teng, "Maritime Diplomacy Necessary for Cyber Security", *The Huffington Post*, November 9, 2015.

¹⁷ Pasal 51 ayat (2).

¹⁸ Barry Desker, "South China Sea Tensions: Unlikely to Lead to War," *RISIS Commentary* No. 233/2015, 3 November 2015, publications@rsis.edu.sg, diunduh tanggal 4 November 2015.

C. Pengaturan Tentang *Cybercrime* dan Konvensi Pbb Tentang Hukum Laut (UNCLOS) 1982

Sebagaimana telah diketahui, berbeda dengan pengaturan atas kegiatan di laut, sampai saat ini belum ada suatu kerangka perjanjian internasional yang mengatur *cybercrime* atau *cyber security* secara komprehensif. Usaha negara-negara untuk menangani masalah tersebut lingkupnya tidak luas, utamanya hanya membahas pengaturan data privasi dan hak asasi manusia,¹⁹ dengan menyempitkan fokus yang lebih luas untuk mendefinisikan dan membedakan berbagai tingkat *cyberaggression* dan mengkodifikasikannya dengan pendekatan hukum internasional untuk menjawab berbagai tantangan tersebut.²⁰ Tanpa pengaturan tentang pengertian yang komprehensif dari *cybercrime*, *cyberattack* atau *cyberaggression*, negara-negara akan terus dihadapkan pada masalah apakah langkah yang diambil untuk menghadapi tindakan-tindakan tersebut dapat dianggap sah secara hukum.

Sampai saat ini belum ada suatu badan atau organisasi internasional yang memiliki kewenangan untuk menangani *cybercrime*, *cyberattack* atau *cyberaggression*, dimana pun hal tersebut dilaksanakan. Dengan demikian untuk menghadapi serangan demikian, negara-negara mendasarkan kewenangan tersebut pada yurisdiksi teritorial. Menurut teori yurisdiksi teritorial, suatu negara dapat menerapkan hukum nasionalnya terhadap

suatu tindak pidana berdasarkan pada lokasi secara fisik dari asal dan target serangan.²¹ Dalam *cybercrime* mudah untuk menentukan lokasi target, akan tetapi tidak demikian untuk menentukan lokasi asal serangan.

Di samping itu, sampai saat ini hukum internasional belum meletakkan kewajiban bagi negara-negara untuk membantu negara lain dalam melakukan penyelidikan terhadap tindakan-tindakan tersebut, kecuali apabila telah ada persetujuan untuk itu, misalnya melalui mekanisme *mutual legal assistance* (MLA).

Budapest Convention on Cybercrime, 2001 yang dihasilkan oleh *Council of Europe* merupakan satu-satunya perjanjian multilateral yang mengikat secara hukum, dan mengatur tentang kegiatan tindak pidana di dunia maya. Konvensi ini memiliki lima tujuan yaitu (1) harmonisasi tentang substansi hukum pidana tentang *cybercrime*, (2) harmonisasi hukum acara pidana, (3) memfasilitasi *mutual legal assistance* (MLA), (4) mengkodifikasikan hukum internasional, dengan penekanan pada ketentuan-ketentuan hukum berdasarkan yurisdiksi teritorial, dan (5) menyediakan kerangka pengaturan untuk pengembangan dan pemahaman isu-isu terkait dengan *cybercrime*.²²

Konvensi ini dimaksudkan untuk memberikan perlindungan kepada masyarakat dari *cybercrime* dan memfokuskan pada tindak pidana seperti "*copyright infringement*,

¹⁹ Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law," 88 Tex. L. Rev. p. 1571, 1581 (2010), sebagaimana dikutip oleh William J. Stahl, "The Uncharted Waters of Cyberspace : Applying the Principles of International Maritime Law to the Problems of Cybersecurity," digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024...gjicl

²⁰ *Id.*, p. 1571.

²¹ Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," 43 *Vand. J. Transnat'l L.* 57, 67-69 (2010), sebagaimana dikutip oleh Stahl, *supra*, n. 20.

²² Sharon R. Stevens, "Internet War Crimes Tribunals and Security in an Interconnected World," 18 *Transnat'l L. & Contemp. Probs.* at 685-686 (2009), sebagaimana dikutip oleh Stahl, *supra*, n. 20.

computer-related fraud, child pornography, and offenses related to breaches of network security."²³ Meskipun Konvensi mengidentifikasi tindakan-tindakan khusus yang dilarang, negara-negara pihak pada Konvensi tersebut secara unilateral dapat menetapkan unsur-unsur dari tindakan yang dilarang dan metode penegakan hukum yang terbaik sesuai dengan hukum nasionalnya.²⁴

Upaya ke arah pengaturan tentang *cybercrime* dilakukan juga oleh kelompok 8 negara yang dikenal sebagai Group of 8 (G8), yang terdiri dari Kanada, Perancis, Jerman, Italia, Jepang, Russia, Inggris dan Amerika Serikat.²⁵ Kelompok ini berhasil menyusun suatu *G8 Recommendations on Transnational Crime*.²⁶ Kelompok ini merekomendasikan kerjasama internasional dalam penyelidikan *cybercrime*, meninjau substansi dan hukum acara dari hukum nasional untuk menjamin keberadaan sanksi, serta mengadopsi *Budapest Convention on Cybercrime*. Sayangnya rekomendasi tersebut tidak disertai dengan pedoman implementasinya, serta tidak memiliki kekuatan mengikat secara hukum.

Dalam pada itu PBB juga telah berusaha untuk mengembangkan suatu pendekatan yang komprehensif untuk memberantas *cybercrime*.²⁷ Pada tahun 1995 PBB telah menerbitkan *United Nations Manual on the Prevention and Control of Computer-Related Crime* yang meninjau

pengaturan tentang *cybercrime* dan perlunya kerjasama internasional dalam penyelidikan tentang *cybercrime*.²⁸ Pada tahun 2000 Majelis Umum PBB mengadopsi *GA Resolution 55/59* yang meminta negara-negara anggota PBB untuk mengembangkan lebih jauh satu kebijaksanaan nasional (*national policy*) tentang tindak pidana yang berkaitan dengan komputer.²⁹ Rekomendasi ini hanya berupa rekomendasi untuk menyusun suatu kebijaksanaan secara luas dan tidak secara khusus menganjurkan harmonisasi antar berbagai hukum nasional.

Konvensi PBB tentang Hukum Laut (UNCLOS) 1982, disusun sejak tahun 1970-an yaitu sejak dimulainya sidang-sidang *United Nations Sea-bed Committee* yang kemudian dalam perkembangannya menjadi Panitia Persiapan Konferensi PBB tentang Hukum Laut ke-III. Pada waktu itu meskipun penggunaan komputer telah cukup berkembang, masalah *cybercrime* belum masuk ke dalam agenda persidangan Konferensi. Satu-satunya masalah yang berkaitan dengan teknologi adalah masalah alih teknologi, yang sama sekali tidak menyinggung teknologi komunikasi. Oleh karena itu istilah *cyber* tidak ditemukan dalam naskah Konvensi.

Namun demikian, sebagaimana telah diuraikan melalui beberapa contoh di atas, dalam pelaksanaan berbagai kegiatan di laut ancaman *cybercrime*, *cyberattack* bahkan

²³ Jon P. Jurich, "Cyberwar and Customary International Law: The Potential of a "Bottom-Up" Approach to an International Law of Information Operations," 9 *Chi. J. Int'l L.*, p. 283 (2008), sebagaimana dikutip oleh Stahl, *supra*, n. 20.

²⁴ *Id.*, p. 283-84.

²⁵ G8 Research Group: About Us, G8LIVE.ORG, <http://g8live.org/about/>

²⁶ Group of 8, *G8 Recommendations on Transnational Crime* (2002), http://www.canadainternational.gc.ca/g8/ministerials-ministerielles/2002/transnational_crime-criminalite_transnationale.aspx?lang=eng&view=d, diunduh tanggal 11 November 2015.

²⁷ Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 *J. MARSHALL J. COMPUTER & INFO. L.* 347, 363 (2002), sebagaimana dikutip oleh Stahl, *supra*, n. 20.

²⁸ United Nations, *United Nations Manual on the Prevention and Control of Computer-Related Crime* (1995).

²⁹ *Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century*, G.A. Res. 55/59, U.N. Doc. A/RES/55/59 (Jan. 17, 2001).

cyberaggression bukan tidak mungkin timbul. Para penyusun Konvensi PBB tentang Hukum Laut (UNCLOS) 1982, telah menyadari kemungkinan adanya kaitan antara Konvensi tersebut dengan perjanjian-perjanjian internasional yang berkaitan. Hal ini terbukti dengan dicantumkannya dalam Pasal 311 ketentuan tentang hubungan antara UNCLOS 1982 dengan konvensi-konvensi dan perjanjian-perjanjian internasional yang lain. Dengan demikian, sepanjang berkaitan dengan masalah *cybercrime* maka UNCLOS 1982 dapat berpedoman pada perjanjian-perjanjian internasional terkait. Sayang sekali bahwa sampai saat ini belum ada perjanjian multilateral yang mengatur tentang *cybercrime*.

Penutup

Dunia maya dapat dikatakan masih baru, sehingga tantangan terhadap pengaturannya bukan suatu hal yang mudah diselesaikan. Sebagian besar dari dunia maya masih belum tereksplorasi. Karena sifatnya yang unik, berbagai masalah di dunia maya dapat melewati yurisdiksi teritorial dari suatu negara.

Meskipun terdapat berbagai macam usulan ke arah pembentukan pengaturan secara global, tidak banyak kesepakatan pengaturan secara universal yang telah dicapai. Dalam waktu yang bersamaan kebutuhan akan pengaturan secara efektif makin mendesak karena dunia maya memiliki kedudukan penting dan strategis. Misalnya saja, dunia maya sangat penting dan strategis untuk komunikasi, bisnis, lembaga-lembaga pemerintah maupun bukan pemerintah, bahkan kepentingannya di bidang militer menunjukkan peningkatan. Dengan

demikian, diperlukan suatu pengaturan yang efektif, dan untuk itu sifat khusus dan unik dari dunia maya harus difahami sedemikian rupa dan dimasukkan ke dalam kerangka pengaturan yang lebih luas, dan kalau perlu berbeda-beda.

Cybercrime merupakan tindak pidana yang melewati batas negara, timbul dalam bentuk kegiatan ilegal yang tidak mudah untuk ditangani hanya dengan menggunakan hukum nasional yang penerapannya dibatasi oleh batas-batas kewilayahan. *Cybercrime* merupakan akibat negatif dari globalisasi teknologi informasi, yang telah membantu para pelaku tindak pidana untuk melakukan berbagai kegiatan ilegal melalui dunia maya.

Sejumlah bukti nyata telah menunjukkan bahwa *cybercrime* juga telah memasuki kegiatan pemanfaatan laut, yang tidak hanya terpusat di bidang pelayaran, bahkan dapat diakibatkan oleh sengketa kewilayahan. Konvensi PBB tentang Hukum Laut (UNCLOS) 1982 yang selama ini dianggap sebagai "*a constitution of the oceans*" tidak memiliki ketentuan khusus tentang *cybercrime*. Namun demikian, dari pengamatan terhadap sejumlah kegiatan di laut, *cybercrime* telah dan mungkin memasuki berbagai kegiatan tersebut. Kemungkinan Konvensi tersebut mempunyai keterikatan dengan konvensi atau perjanjian internasional lainnya telah disadari oleh para penyusun. Dalam hal penanggulangan *cybercrime*, mungkin ketentuan Pasal 311 tersebut dapat digunakan, apabila dikemudian hari ada konvensi atau perjanjian internasional yang berkaitan dengan hal ini.

Daftar Pustaka**Jurnal**

Jeremy Rabkin and Ariel Rabkin, "Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea", *Chicago Journal of International Law*, Vol. 14, No. 1, Article 7, June 1, 2013.

Konvensi dan Perundang-Undangan

Budapest Convention on Cybercrime, 23 November 2001, European Treaty Series No. 185.

United Nations Manual on the Prevention and Control of Computer-Related Crime (1995).

Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, G.A. Res. 55/59, U.N. Doc. A/RES/55/59 (Jan. 17, 2001).

Sumber Lain

Barry Desker, "South China Sea Tensions: Unlikely to Lead to War," *RISIS Commentary* No. 233/2015, 3 November 2015, publications@rsis.edu.sg.

Fred Teng, "Maritime Diplomacy Necessary for Cyber Security", *The Huffington Post*, November 9, 2015.

G8 Research Group: About Us, G8LIVE.ORG, <http://g8live.org/about/>

Group of 8, *G8 Recommendations on Transnational Crime* (2002), http://www.canadainternational.gc.ca/g8/ministerials-ministerielles/2002/transnational_crime-criminalite_transnationale.aspx?lang=eng&view=d

Jeremy Wagstaff, "All at sea: global shipping fleet exposed to hacking threat", <http://www.reuters.com/news/picture/all-at-sea-global-shipping-fleet-exposed>.

Karl Frederick Rauscher and Valery Yaschenko, "Russia-U.S. bilateral on Cybersecurity Critical Terminology Foundations," p. 27, April, 2010, <http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations>

Noah Shachtman, "Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariah," *Brooking Institutions*, Cyber Security #1, July, 2011.

study.com/academy/.../what-is-cyber-crime-definition-types-examples.

William J. Stahl, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problems of Cybersecurity," digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024...gjicl

bytes-notes.com.

<http://www.techopedia.com/definition/2387/cybercrime>.

us.norton.com

hukumonline.com