



DR. MASKUN S.H., L.L.M DR. NASWAR, S.H., M.H. ACHMAD, S.H., M.H. HASBI ASSIDIQ, S.H. ARMELIA SAFIRA SITI NURHALIMA LUBIS

Sanksi Pelanggaran Hak Cipta

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 28 TAHUN 2014 TENTANG HAK CIPTA

Ketentuan Pidana Pasal 113

- Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
- 2) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hamk Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
- 3) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- 4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).



Korelasi Kejahatan Siber dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional

Dr. Maskun S.H, L.LM Achmad S.H, M.H Dr. Naswar S.H, M. H Hasbi Assidiq Armelia Safira Siti Nurhalima Lubis

- Makassar : © 2020

Copyright © Maskun dkk 2020 All right reserved

Layout : **Rizaldi Salam**Design Cover : **Tim Penulis**

Cetakan Pertama, November 2020 viii + 190 hlm; 14.5 x 20,5 cm ISBN 978-623-6714-73-7

Diterbitkan oleh Penerbit Nas Media Pustaka

CV. Nas Media Pustaka Anggota IKAPI No. 018/SSL/2018

Jl. Batua Raya No. 550 Makassar 90233
Telp. 0812-1313-3800
redaksi@nasmediapustaka.id
www.nasmediapustaka.co.id
nasmedia.id

Instagram : @nasmedia.id

Fanspage: Penerbit Nas Media Pustaka

Dicetak oleh Percetakan CV. Nas Media Pustaka, Makassar Isi di luar tanggung jawab percetakan

KATA PENGANTAR

Hal terpenting dan utama dalam kejahatan siber dan kejahatan agresi adalah Kejahatan agresi telah memiliki sejarah panjang dalam perkembangan hukum internasional, sementara itu kejahatan siber merupakan bentuk kejahatan baru yang perkembangannya beriringan dengan perkembangan teknologi. Dalam konteks ini haruslah dipahami bahwa terdapat relasi yang sangat erat antara perkembangan kejahatan agresi yang saat ini telah menggunakan teknologi siber dalam aktivitasnya.

Buku referensi ini merupakan bagian dari hasil penelitian terkait dengan artikulasi hubungan kejahatan siber dan kejahatan agresi yang memberikan bukti bahwa perkembangan kejahatan agresi telah menggunakan teknologi sebagai alat dalam melakukan aktivitas agresi terhadap suatu negara. Tentunya, buku referensi ini diharapkan akan bermanfaat dalam menyediakan informasi baik dalam bentuk teks maupun konteks dalam memahami kejahatan agresi dan kejahatan siber. Di samping itu, buku referensi ini diharapkan berkontribusi bagi pengajaran Hukum Kejahatan Internasional dan Hukum Telematika untuk diajarkan pada mahasiswa program sarjana dan pascasarjana.

Akhirnya, disadari bahwa buku referensi ini jauh dari kesempurnaan. Kritik dan saran akan sangat bermanfaat dalam penyempurnaan bahan ajar ini, sekaligus menghasilkan gagasan baru bagi penelitian sejenis di masa yang akan datang.

Makassar, Agustus 2020

DAFTAR ISI

KATA PENGANTAR	V
BAB I PENDAHULUAN	1
BAB II KEJAHATAN SIBER	18
A. Sejarah Singkat Perkembangan <i>Cyberspace</i>	18
B. Istilah	20
C. Pengertian	22
D. Jenis Kejahatan Siber	26
 Akses Pelayanan dan Sistem Komputer yang 	
tidak sah (unauthorized access to computer	
system and service)	26
Data atau Informasi yang Tidak Sah	
(Illegal Contents);	27
3. Pemalsuan Data (Data Forgery);	27
4. Siber Espionase (<i>Cyber Espionage</i>);	27
5. Siber Sabotase (Cyber Sabotage and Extortion);.	28
Pelanggaran Terhadap Kekayaan Intelektual	
(Offence Against Intellectual Property);	29
Kejahatan Terhadap Privasi Seseorang	
(Infringments of Privacy);	29
E. Media Komputer dalam Kejahatan Siber	32
1. Komputer Sebagai Sasaran	32
Komputer Sebagai Ketidak-sengajaan atas	
suatu Kejahatan	33
Komputer Sebagai Sarana untuk Melakukan	
tindak kejahatan	34
F. Kejahatan Siber Sebagai Salah Satu Kejahatan	
Internasional	. 34

G. Yurisdiksi Cyberspace	45
1. Yurisdiksi Pidana	
2. Yurisdiksi Perdata	46
BAB III KEJAHATAN AGRESI	49
A. Sejarah Pengertian Kejahatan Agresi	
B. Elemen Agresi	
1. Elemen Objektif	
Elemen Subjektif	
BAB IV ARTIKULASI ANTARA KEJAHATAN SIBER	
DAN KEJAHATAN AGRESI	62
A. Konsep Hukum Internasional Kontemporer	
B. Teori yang Relevan dengan Korelasi Kejahatan	
Siber dan Kejahatan Agresi	67
1. eori Kualifikasi Kejahatan oleh Bassiouni	
2. Teori Kedaulatan Negara (<i>State Sovereignty</i>)	
3. Teori Jurisdiksi (<i>Theory of Jurisdiction</i>)	
4. Teori Hukum Kosmopolitan	
5. Hermeneutika Hukum	
BAB V RINTANGAN DAN TANTANGAN PEMBUKTIAN	
SERANGAN SIBER SEBAGAI SUATU KEJAHATAN	
INTERNASIONAL	. 132
A. Kejahatan Internasional	
B. Serangan siber	
C. Contoh Kasus Serangan Siber	
D. Serangan Siber Sebagai Kejahatan Internasional	
E. Analisis Kasus Pembuktian Serangan siber	

BAB VI FORMULA KERJASAMA INTERNASIONAL	
TERKAIT SERANGAN SIBER	158
A. Pengantar	158
B. Formula Kerjasama Internasional	160
C. Asean Menghadapi Tantangan Serangan Siber	165
DAFTAR PUSTAKA	173

BAB I

PENDAHULUAN

Kejahatan bukanlah konsep baru dalam sejarah peradaban manusia. Sejak manusia diciptakan yang di mulai dengan tindakan pembangkangan iblis terhadap perintah Allah untuk memberi penghormatan terhadap makhluk ciptaan Allah lainnya yang disebut manusia. Pembangkangan ini kemudian diteruskan dengan janji Iblis untuk selalu menggoda manusia hingga akhir zaman. Konflik kepentingan antara manusia dan iblis dipandang sebagai embrio kejahatan yang bermula dari perasaan iri, sombong, dan dengki.

Pada tahapan perkembangannya, modus operasi kejahatan bergerak maju seiring perkembangan peradaban manusia. Kejahatan dan eksistensi masyarakat menjadi "dua sisi mata uang" yang saling terkait. Sehingga Lacassagne² mengatakan bahwa masyarakat mempunyai sisi penjahat sesuai dengan jasanya.

Perkembangan teori-teori kejahatan juga berkembang signifikan, akan tetapi tidak berarti kejahatan akan musnah dari permukaan bumi. Hal ini disebabkan kejahatan merupakan salah satu sifat fitrah manusia yang ada pada diri manusia

¹ Lihat Al-Qur'an.

² Agus Raharjo, Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi, Bandung: Citra Aditya, 2002, hlm. 29-30.

dan terus mengalami perkembangan signifikan dengan perkembangan masyarakat itu sendiri. Hal ini hampir sejalan dengan apa yang dikemukan oleh Freud³ yang mengatakan bahwa hasrat manusia untuk merusak sama kuatnya dengan hasrat untuk mencintai.

Pendapat Freud mungkin benar adanya, akan tetapi argumentasi yang muncul kemudian adalah keseimbangan hasrat untuk merusak dan mencintai dapat dipengaruhi oleh lingkungan sekitarnya (faktor luar). Lorenz⁴ dalam argumentasinya mengatakan bahwa keagresifan manusia merupakan insting yang digerakkan oleh sumber energi yang selalu mengalir, dan tidak selalu akibat rangsangan dari luar. Jadi, dapat dikatakan bahwa destruktivitas kejahatan selalu ada pada diri setiap manusia, hanya bagaimana meminimalisasikan potensi yang secara kefitrahan ada pada setiap individu. Dalam hal ini, sifat destruktivitas dimaksud juga akan dipengaruhi oleh keadaan disekitarnya.⁵

Menyadari konsep psikologi yang ada pada setiap manusia, bagaimanapun perkembangan teknologi informasi maka akan semakin mutakhir pula bentuk dan modus individu melakukan kejahatan. Hal tersebut tidaklah mengherankan jika berangkat pada konsepsi bahwa tidak ada kejahatan tanpa masyarakat. Komunitas atau masyarakat yang peduli terhadap teknologi informasi seperti internet disebut dengan *netizen*.

³ Erich Frommm, Akar Kekerasan, Jakarta: Pustaka Pelajar, 2000, hlm. 15.

⁴ Ibid, hlm. 8

⁵ Lihat David B. Henry, et.al., *A Return Potential Measure of Setting Norms for Aggression*, American Journal of Community Psychology, 33, (June 2004), hlm. 131. Dalam hal ini, David B. Henry, dkk., mengatakan bahwa konteks sosial memainkan peranan yang sangat penting dalam perkembangan sifat agresi dan kekerasan.

Ini berarti dengan komunitas masyarakat tersendiri, kejahatan akan tercipta seiring timbul dan berkembangnya *netizen* itu sendiri.

Kejahatan berteknologi, dalam konteks ini diistilahkan sebagai kejahatan siber, mengalami perkembangan yang sangat pesat dengan modus yang beragam.⁶ Ragam dan varian modus kejahatan siber yang semakin kompleks, tidaklah diikuti dengan pengaturan atau instrumen hukum yang memadai, khususnya dalam konteks hukum internasional.⁷ Oleh karena itu, kebutuhan akan kerangka hukum dalam konteks kejahatan siber merupakan suatu tantangan baru dalam dunia hukum itu sendiri. Ketersediaan dan keterbatasan aturan-aturan hukum yang ada selama ini, "mengharuskan" aparat penegak hukum dan pengambil kebijakan untuk melakukan penemuan hukum di bidang ini (*emerging norms/laws*) sehingga putusan-putusan yang berkaitan dengan masalah-masalah kejahatan siber dapat memenuhi aspek keadilan, kemanfaatan, dan kepastian hukum.⁸

Kedudukan hukum dalam kejahatan siber, jika ditelaah lebih jauh ternyata juga membawa implikasi bagi perubahan yang terjadi dalam masyarakat. Perkembangan teknologi informatika telah melahirkan bias-bias bagi lingkungan sekitarnya termasuk

⁶ Agus Raharjo, op.cit, hlm. 29.

⁷ Katherine C. Hinkle, *Countermeasures in the Cyber Context : One More Thing to Worry About*, YJIL Online, Vol. 17 (Fall 2011), hlm. 12.

⁸ Lihat beberapa kasus yang berhubungan dengan kejahatan syber seperti pembobolan karu kredit BCA, pembobolan situs Komisi Pemilihan Umum (KPU) tahun 2004, kasus Prita Mulya Sari, kasus perjudian (*game foker*), dan beberapa kasus lainnya. Lihat juga Dedy Nurhidayat, *Eksaminasi Terhadap Perkara Pidana Terkait Pembobolan Situs Komisi Pemilihan Umum*, Jurnal Hukum Teknologi, Vol 2. Nomor 1 (Agustus 2006), hlm. 29. Lihat juga Abdul Wahid dan Mohammad Labib, Kejahatan Mayantara (Cyber Crime), (Bandung: Refika Aditama, 2005), hlm. 125.

didalamnya masyarakat. Perubahan sosial yang timbul sebagai implikasi berkembangannya ranah telematika haruslah menempatkan hukum sebagai payung (un umbrella of law) untuk mendukung usaha-usaha perubahan yang terjadi dalam masyarakat. Mochtar Kusumaatmadja⁹ menyebutkan bahwa perubahan ketertiban dan keteraturan merupakan tujuan dari masyarakat yang sedang berubah (membangun). Oleh karena itu, jika perubahan hendak dilakukan dengan tertib dan teratur, maka hukum adalah sarana yang tidak dapat diabaikan.

Perubahan karakter sosial dan budaya masyarakat sebagai akibat perkembangan telematika tentunya merupakan fakta yang tidak dapat dihindarkan. Perubahan karakter tersebut mengantarkan masyarakat pada pola "pengingkaran hakikat kemanusiaan manusia" sebagai makhluk Tuhan yang berakal. Dampaknya dapat diprediksi bahwa masyarakat semakin tak terkendali hingga menyentuh titik kriminalisasi dari apa yang diperoleh dari perkembangan telematika tersebut. Oleh karena itu, hukum yang diharapkan lahir, apapun bentuknya, haruslah memiliki kekuatan mengikat bagi para pihak di dalamnya (*legally binding*) yang tentunya dilengkapi dengan mekanisme sanksi sebagai alat pemaksa.

Menurut Grolier¹⁰, hukum dapat didefinisikan secara luas sebagai suatu standar sistem dan aturan yang ada dalam masyarakat. Standar tersebut akan menjadi acuan bagi setiap individu yang akan melahirkan hak dan kewajiban. Sementara aturan-aturan akan menjadi pertimbangan dalam memperoleh, menciptakan, memodifikasi, dan menegakkan hak dan

⁹ Mochtar Kusumaatmadja, Masyarakat dan Pembinaan Hukum Nasional: Suatu Uraian tentang Landasan Pikiran, Pola, dan Mekanisme Pembangunan Hukum di Indonesia, (Bandung: Binacipta, 1976), hlm. 13.

¹⁰ Grolier dikutip dalam Edmon Makarim, op.cit., hlm. 13

kewajiban yang dilakukan oleh setiap individu. Tentunya, hukum sebagai suatu kesatuan sistem yang diakui oleh masyarakat haruslah berada dalam lingkup kewenangan negara atau pemerintah yang menentukan apa yang boleh dan yang tidak.

Pendapat Grolier tidak sepenuhnya benar dalam mendeskripsikan hukum khususnya dalam melihat peran pemerintah. Diskursus tentang peran pemerintah dalam mengatur apa yang boleh dan tidak oleh warga negaranya khususnya di bidang telematika, mengantarkan pada suatu perdebatan tersendiri. Ada yang berpandangan bahwa pemerintah perlu dilibatkan, akan tetapi disisi lain ada yang berpendapat sebaliknya.

Boele-Woelki¹¹ berpandangan bahwa keterlibatan langsung pemerintah dan undang-undang dalam masalah *cyberspace* merupakan sesuatu yang dibutuhkan khususnya dalam menyelesaikan sengketa-sengketa yang timbul dibidang telematika. Pandangan senada juga dikemukakan oleh Tom Maddox¹² yang pada prinsipnya sepakat dengan Boele-Woelki, hanya saja berbeda dalam kaitan dengan sumber pengendalian seperti fungsi pengendaliannya.

Pandangan lain tentunya menghendaki agar pemerintah sama sekali tidak terlibat dalam urusan hukum, khususnya permasalahan *cyber*. Pandangan ini dikonstruksi dari paham *delegalization*¹³ yang menjadi sebuah trend baru dalam

¹¹ Boele-Woelki, dkk., *Internet: Which Court Decides? Which Law Applies?*, (the Haque/London/Boston: Kluwer Law International, 1998), hlm. *preface*.

¹² ibid

¹³ Konstruksi paham delegalisation dalam hal ini berbeda dengan konstruksi teori delegasi yang dikembangkan dalam praktek-praktek hukum internasional. Teori delegasi lahir sebagai jawaban terhadap Teori Transformasi dan *Specific Adoption*. Teori delegasi dianggap sebagai *variant* dari teori atau

pemikiran hukum. Paham ini berpandangan bahwa privatisasi kehidupan manusia harus dikembalikan oleh negara yang diawali oleh konsep the welfare state modern itu, sedikit demi sedikit harus semakin dibatasi. Keterlibatan hukum formal dalam aspek tertentu kehidupan manusia sering malah lebih menimbulkan keruwetan dan ketidak-adilan. Hukum semakin terbatas kemampuannya untuk mewujudkan solusi dalam berbagai conflict of interest warga masyarakatnya.

Argumentasi dibutuhkannya instrumen hukum sebagai sarana pencapaian tujuan hukum menunjukkan bahwa pengabungan telekomunikasi dan informatika yang telah dilakukan telah melahirkan suatu fenomena yang telah mengubah konfigurasi model komunikasi konvensional¹⁴ dalam dimensi ketiga,¹⁵ yang berimplikasi pada keterbatasan aturanaturan hukum yang ada dalam mengejar perubahan yang begitu cepat.¹⁶ Oleh karena itu, berbagai diskusi dan debat

kaidah-kaidah fungsional dari hukum internasional terhadap primat hukum internasional. Teori delegasi beranggapan bahwa: kaidah-kaidah fungsional dari hukum internasional mendelegasikan kepada setiap konstitusi negara (hukum nasional) hak-hak untuk menentukan *kapan* ketentuan-ketentuan traktat atau konvensi akan berlaku dan cara-cara memasukkannya ke dalam hukum nasional.prosedur dan metode yang digunakan untuk maksud-maksud tersebut merupakan *kelanjutan dari proses penutupan* atau berakhirnya suatu traktat atau konvensi.Oleh karena itu, menurut teori delegasi tidak ada transformasi dan tidak ada pembentukan hukum nasional baru melalui *specific adoption*.

- ¹⁴ Dikdik M. Arief Mansur dan Alitaris Gultom, Cyber Law: Aspek Hukum Teknologi Informasi, (Bandung: Refika Aditama, 2005), hlm. 2.
- ¹⁵ Dimensi pertama adalah kenyataan keras dalam kehidupan empiris. Dimensi kedua adalah kehidupan simbolik dan nilai-nilai yang dibentuk, dan Dimensi ketiga adalah kenyataan maya (*virtual reality*) yang melahirkan suatu format masyarakat lahirnya. Lihat juga Ashadi Siregar, 2001, Negara, masyarakat, dan Teknologi Informasi, Makalah, Yogyakarta.
- ¹⁶ Pameo sebagaimana dicantumkan juga telah dikemukakan oleh Immanuel Kant seorang ilmuwan hukum yang berasal dari Belanda.

ilmiah dilakukan dalam rangka mendudukan pola hubungan kejahatan siber sebagai salah satu kejahatan yang merupakan lingkup hukum internasional atau apakah kejahatan siber dapat dikategorikan sebagai suatu penggunaan kekuatan bersenjata atau tindakan perang di ruang siber.¹⁷

Berbagai analisis telah dikemukakan berbagai pakar (scholars/expertise) untuk menjelaskan pola hubungan dimaksud, dimana kejahatan siber merupakan salah satu kejahatan internasional dengan memberi label pada yurisdiksi yang melekat padanya. Hal tersebut merupakan sesuatu yang "sah-sah saja". Akan tetapi, dalam perspektif berbeda, sesungguhnya kejahatan siber dapat didekatkan dengan kejahatan agresi yang merupakan salah satu dari 4 (empat) kejahatan dalam yurisdiksi *International Criminal Court* (selanjutnya disingkat ICC)¹⁸.

Secara Umum kejahatan agresi tidak disebutkan dalam ketentuan piagam Perserikatan Bangsa-Bangsa (PBB). Berdasarkan catatan sejarah, mulai dari zaman kuno, abad

Lihat pandangan Bassiouni yang menyebutkan bahwa suatu kejahatan mempunyai elemen internasional jika kejahatan dimaksud inkonsisten dengan norma-norma dasar hukum internasional dan melanggar norma-norma *lus Cogen.* Lihat juga Neil Boister, *Transnational Criminal Law*, EJIL Vol. 14 No. 5, (2003), hlm. 965. Lihat juga Major Graham H. Todd, *Armed Attack in Cyberspace Deterring Asymmetric Warfare With an Asymmetric Definition*, the Air Force Law Review, Vol. 64 (2009), phlm. 66-67. Lihat juga Michael N. Schmitt, *Compute Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum J. of Transnat'l Law, 885 (1999).

¹⁸ ICC lahir melalui konferensi internasional diplomatik di Italia, pada tanggal 17 Juli 1998 yang disetujui oleh 120 negara anggota PBB, 21 negara abstain, dan 7 menyatakan sikap menentang ICC. Negara-negara yang menentang antara lain Amerika Serikat, Cina, Jepang, India, Irak, Qatar dan Israel. Lihat Hamid Awaluddin, HAM Politik, Hukum, dan Kemunafikan Internasional, (Jakarta: Kompas, 2012), hlm. 157.

pertengahan dan zaman modern itu kejahatan agresi sering terjadi¹⁹, pelaku-pelaku dari kejahatan agresi tersebut belum dapat diberikan sanksi yang pasti dikarenakan pengaturan agresi masih sangat krusial dan kompleks serta mengundang banyak penafsiran yang berbeda-beda, namun selama ini instrumen hukum yang sering digunakan dalam menindak pelaku-pelaku kejahatan internasional, negara-negara anggota PBB mengacu pada Pasal 2 ayat (4) Piagam PBB yakni²⁰

"All members shall refrain in their international relation from the threat or use of force against the teritorial integrity or political independence of any state, or in any other manner inconsistent with the purpose of the United Nations."

Pasal 2 ayat (4) tersebut mengemukakan segenap anggota, dalam perhubungan internasional akan menghindarkan dirinya dari ancaman atau penggunaan kekerasan terhadap keutuhan wilayahnya atau kemerdekaan politik suatu negara, atau dengan cara apapun yang bertentangan dengan tujuantujuan PBB. Isi dari pasal tersebut merupakan suatu langkah

¹⁹ Karakteristik kejahatan agresi selalu dikonotasikan pada peristiwa kejahatan yang terjadi di Nuremberg, dimana menjadi sumber referensi dalam berbagai pustaka hukum kejahatan/pidana internasional. Suatu bukti ilmiah dikemukakan oleh Donald M. Ferenz yang menyebutkan bahwa seorang ahli hukum berkebangsaan Swiss, Emmerich de Vattel, dalam bukunya the Law of Nations pada tahun 1758 menyatakan bahwa karakteristik kejahatan agresi menyebabkan horror, pertumpahan darah tindak perampokan, pemerkosaan dan berbagai kejahatan lainnya. Akhirnya, pelakunya dianggap bersalah karena melanggar hak-hak manusia secara umum dan merusak/mengancam perdamaian. Lihat Donald M. Ferenz, *The Crime of Aggression: Some Personal Reflections on Kampala*, Leiden Journal of International Law, Vol. 23 (2010), hlm. 905-908.

²⁰ Lihat: *United Nations Convention*, Pasal 2 ayat (4) Piagam PBB. Lihat juga Katharine C. Hinkle, op. cit, hlm. 12

dari negara-negara anggota PBB untuk mengkualifikasikan negara tersebut ketika telah melakukan kejahatan agresi.

Lebih lanjut, Resolusi Majelis Umum PBB Nomor 3314 (XXIX), 14 Desember 1974 menekankan bahwa definisi agresi melingkupi bombardier (serangan) yang dilakukan oleh armada bersenjata (*the armed forces of a state*) terhadap wilayah negara lain atau penggunaan berbagai senjata oleh suatu negara terhadap wilayah negara lainnya.²¹ Pertanyaan yang menarik kemudian untuk diketengahkan apakah *cyber weapon* dapat dikategorikan sebagai ...*any weapons*...menurut Resolusi Majelis Umum PBB Tahun 1974? Pertanyaan elaborasi ini dimaksudkan untuk menguraikan ketertautan suatu negara atas kejahatan agresi yang fokusnya diletakkan pada aktivitas negara (*committed by a state concerned*).²²

Menengok penerapan hukum di dalam Liga Bangsa-Bangsa (LBB) terhadap pelaku-pelaku kejahatan agresi di masa lalu, pada saat itu (LBB) hanya menganggap bahwa untuk menjamin perdamaian dan keamanan, para anggota menerima kewajiban untuk tidak memilih perang, bahkan bukan hanya itu dalam piagam LBB tersebut menentukan bahwa negaranegara peserta sepakat apabila ada kemungkinan timbulnya

²¹ Lihat James P. Farwell and Rafal Rohonzinski, *Stuxnet and the Future of Cyber War*, Survival, Vol. 53 (February-March 2011), phlm.23-40. Lihat pula definisi *attack* dalam Pasal 49 Protokol Tambahan I Konvensi Jenewa yang menyebutnya sebagai "*acts of violence against the adversary*". Lihat pula Pasal 2 Konvensi Jenewa 4 yang menyatakan bahwa '*the Conventions shall apply during "any armed conflict" yet that terms is not well defined in the Conventions*. Dalam konteks ini, kedua pengertian atau definisi *attack* memberikan pemaknaan yang luas (*broad application*) terhadap pengertian konflik bersenjata (*armed conflict*), termasuk didalamnya cyber weapons.

²² Lihat Roger S. Clark, *Rethinking Aggression as a Crime and Formulating Its Elements : The Final Work-Product of the Preparatory Commission fo International Criminal Court*, 15 LJIL, (2002), hlm. 872.

perselisihan, mereka akan mengusahakan penyelesaiannya dengan jalan arbitrase, *judicial settlement* (penyelesaian secara hukum), serta tidak akan memulai perang sebelum lewat tiga bulan sesudah putusan arbiter atau keputusan hukum diterima.

Penerapan hukum terhadap pelaku agresi sebagaimana tercantum dalam LBB, tidaklah memberikan rasa keadilan bagi negara yang diagresi. Padahal persoalan agresi merupakan persoalan mendasar yang melanggar kedaulatan negara suatu negara yang seharusnya dilindungi. Oleh karena itu, PBB memberikan perhatian yang besar kepada negara-negara anggota PBB untuk menghindari tindakan agresi terhadap kedaulatan wilayah negara lain.

Dalam hal ini, Pasal 2 ayat (4) Piagam PBB sebagaimana disebutkan di atas, memiliki keterkaitan dengan BAB VII Pasal 39 Piagam PBB, yakni²³

"Dewan Keamanan akan menentukan adanya sesuatu ancaman terhadap perdamaian, atau tindakan agresi dan akan memajukan anjuran-anjuran atau memutuskan tindakan apa akan diambil sesuai dengan Pasal 41 dan 42, untuk memelihara atau memulihkan perdamaian dan keamanan internasional".

Pasal 39 piagam PBB ini, merupakan acuan dari Pasal 2 ayat (4) yang digunakan oleh pihak PBB dalam menerapkan hukum terhadap pelaku kejahatan agresi, dikarenakan isi dari Pasal 2 ayat (4) piagam PBB belum terlalu jelas sehingga ketika terjadi pelanggaran hukum kejahatan agresi maka di samping Pasal 2 ayat (4), juga diterapkan BAB VII Pasal 39 piagam PBB yang merupakan penafsiran oleh PBB dalam menerapkan sanksi pelanggaran terhadap kejahatan agresi.

²³ Lihat: *United Nations Convention*, BAB VII Pasal 39 Piagam PBB

Statuta Roma (International Criminal Court selanjutnya disingkat ICC) merupakan salah satu instrumen hukum yang dapat menjadi dasar dalam penerapan sanksi terhadap pelanggaran kejahatan internasional. Statuta Roma diadopsi dalam Konferensi Diplomatik di Roma pada bulan Juli tahun 1998 dan telah dijadikan acuan oleh PBB dalam menuntut dan mengadili pelanggar kejahatan yang serius dan telah keprihatinan masyarakat internasional (serious menjadi crimes of international concern) di depan Mahkamah Pidana Internasional (selanjutnya disingkat MPI). Kejahatan yang telah menjadi perhatian serius masyarakat internasional salah satu diantaranya yaitu kejahatan agresi.²⁴ Oleh karena itu, Statuta Roma merupakan salah satu instrumen yang sering digunakan oleh masyarakat internasional dalam menyelesaikan masalah terutama terkait dengan masalah kejahatan internasional, terkait dengan kejahatan agresi instrumen hukum yang digunakan yaitu Pasal 5 Statuta Roma menyebutkan bahwa:25

- 1. Yurisdiksi dari Mahkamah harus dibatasi hanya terhadap tindak pidana yang oleh keseluruhan masyarakat internasional dianggap paling serius. mahkamah memiliki yurisdiksi dalam kaitannya dengan statuta ini dalam hal kejahatan sebagai berikut:
 - a) Tindak Pidana Genocide (pembunuhan massal);
 - b) Kejahatan terhadap kemanusiaan;

²⁴ Sumaryo Suryokusumo, Studi Kasus Hukum internasional, (Jakarta: Tatanusa, 2007), hlm 26.

²⁵ Lihat: Statuta Roma, Pasal 5 ayat 1. Lihat juga David Luban, Fairness to Rightness: Jurisdiction, Legality, and Legitimacy of International Law, in Samantha Besson and John Tasioulas, the Philosophy of International Law, (Oxford: Oxford University Press, 2010). hlm. 579. lihat juga Roger S. Clark, op.cit., hlm. 860-861.

- c) Kejahatan Perang;
- d) Kejahatan agresi
- 2. Mahkamah melaksanakan yurisdiksi atas kejahatan agresi setelah ketentuan disahkan sesuai dengan Pasal 121 dan 123 yang mendefinisikan kejahatan dan menetapkan kondisi-kondisi dimana mahkamah menjalankan yurisdiksi berkenaan dengan kejahatan ini. Ketentuan semacam itu haruslah sesuai dengan ketentuan terkait dari Piagam Perserikatan Bangsa-Bangsa.

Penerapan hukum terhadap pelaku kejahatan agresi, sering terjadi pertentangan antara negara-negara peserta dikarenakan masing-masing negara memiliki persepsi masing-masing terhadap definisi kejahatan agresi. Oleh karena itu, ketika terjadi pelanggaran terhadap kejahatan agresi itu sangat susah dalam menjatuhkan sanksi, Namun terkadang pihak PBB mengeluarkan Resolusi Dewan Keamanan untuk menyelesaikan kasus tersebut walaupun itu masih kurang maksimal misalnya pada kasus agresi Korea Utara melawan Korea Selatan tahun 1950.

Ketidaksepakatan atas pengertian kejahatan agresi sebagaimana diuraikan sejak Nuremberg hingga ICC, telah melahirkan upaya untuk sesegera mungkin menemukan formula baku atas definisi dimaksud. Dibentuklah komite khusus yang diberi mandate untuk merumuskannya. Komite tersebut dikenal dengan *Special Working Group on the Crime of Aggression (Special Working Group – SWGCA).*²⁶ Perjuangan panjang *SWGCA*, akhirnya menghasilkan suatu konsensus yang komprehensif yang dijadikan sebagai amandemen atas

²⁶ Stefan Barriga and Leena Grover, *A Historic Breakthrough on the Crime of Aggression*, AJIL, Vol 105:477 (2011), hlm. 518-519)

kejahatan agresi sebagaimana disebutkan dalam Pasal 5 ayat 2 ICC.²⁷ Dalam Review Konferensi (*SWGCA*) disebutkan bahwa "...untuk tujuan Statuta, kejahatan agresi bermakna perencanaan, persiapan, inisiasi atau pelaksanaan yang dilakukan oleh seseorang (individu) dalam kedudukannya untuk mengendalikan secara efektif atau langsung tindakan militer atau politik suatu negara atas suatu tindakan agresi..."²⁸

Dalam konteks ini, SWGCA menyatakan bahwa terdapat 3 (tiga) unsur utama dalam mendefinisikan kejahatan agresi, yaitu:

- 1. Dilakukan oleh individu;
- 2. Tindakan negara dalam melakukan agresi;
- 3. Suatu kejahatan yang berbasis pemimpin (*a leadership crime*).²⁹

Ketiga unsur utama sebagaimana disebutkan di atas, tidaklah lantas menyelesaikan "no emerging norms", khususnya berhubungan dengan kejahatan siber. Pertanyaan mendasar : Apakah "serangan siber atau cyber war" dapat dikualifikasikan sebagai "armed attack"? Pertanyaan ini harus dapat terjawab dalam rangka mengantar pada pertanyaan berikut ; Apakah dengan terpenuhinya ketiga unsur utama sebagaimana disebutkan dalam kasus serangan siber maka dapatlah dikualifikasikan bahwa cyber crime adalah crime of aggression?

²⁷ Peristiwa bersejarah tersebut terjadi di Kampala Uganda pada tanggal 10 Juni 2010, tepatnya Sabtu Pagi pukul 12.20.

²⁸ The Review Conference provides "For purpose of the Statute, crime of aggression means the planning, preparation, initiation or execution, by a person in position effectively to exercise control over or to direct the political or military action of the State, of an act of aggression.." Lihat lebih lanjut dalam Stefan Barriga and Leena Grover, op..cit., hlm.517-521.

²⁹ Lihat the Coalition for the International Criminal Court, *the ICC and the Crime of Aggression*, Factsheet, http://www.iccnow.org. hlm. 2.

Pertanyaan-pertanyaan sederhana di atas sesungguhnya berangkat dari fakta-fakta yang menunjukkan bahwa serangan siber telah berlangsung dalam beberapa tahun terakhir, yang dilakukan oleh suatu negara terhadap wilayah negara lain. Beberapa peristiwa dimaksud dapat dilihat pada tahun 2005 ketika pemerintah Cina menggunakan outsourcing untuk melakukan pembajakan (cyber piracy) terhadap Amerika Serikat.³⁰ Pada tahun 2007, Estonia mendapat serangan (serangan siber) yang diduga dilakukan oleh Russia³¹ yang melumpuhkan jaringan-jaringan (networks) pemerintah dan perdagangan milik pemerintah Estonia. Kurang lebih satu juta komputer Pemerintah terinfeksi yang didistribusikan dalam bentuk Distributed Denial-of-Service (DDoS) attacks.32 Kejadian serupa juga terjadi pada tahun 2008 ketika terjadi perang antara Georgia dan Rusia yang menempatkan Moscow sebagai sebuah strategi multiple untuk kampanye angkatan bersenjata Rusia, yang juga dilakukan melalui Distributed Denial-of-Service (DDoS).33

Peristiwa yang terjadi di Estonia dan Georgia dipandang sebagai peristiwa yang melibatkan atau merupakan bagian dari kebijakan pemerintah Rusia. Dalam konteks ini modus yang dilakukan dengan menyerang dokumen-dokumen milik pemerintah yang berakibat fatal dan dapat mengancam keberadaan dan kenyamanan warga negara kedua Negara.

³⁰ James P.. Farwell and Rafal Rohonzinski, op.cit., hlm. 26.

³¹ Katherina C. Hinkle, op.cit, hlm. 13.

³² Ibid.

James P. Farwell and Rafal Rohonzinski, ohlm cit., hlm. 26. Lihat juga http://www.un.org/apps/news/story.asp?NewsID=23977&Cr=general&Cr1=debate&Kw1=general+assembly&Kw2=&Kw3=, Estonia Urges UN Member States to Cooperate Against Cyber Crimes, Posting 27 Sepetember 2007, accessed 05 October 2012.

Fatal yang dimaksudkan karena melanggar kedaulatan negara dan infrastruktur Estonia dan Georgia.³⁴

Serangan siber yang terakhir menimpa Iran terjadi pada bulan Juni 2010. Serangan tersebut menyerang fasilitas nuklir Iran di Natanz. Kurang lebih 60.000 komputer terinfeksi oleh virus yang disebut dengan Stuxnet.³⁵ Target terhadap infrastruktur pengayaan uranium di Iran tentunya sangat berbahaya. Bukan saja melanggar kedaulatan Negara Iran akan tetapi dampak yang ditimbulkannya berbahaya bagi keselamatan peradaban umat manusia.

Menurut Kevin Hogan, Senior Direktur Symantec bahwa 60% dari komputer yang terinfeksi di seluruh dunia berada di Iran dan target utamanya instalasi nuklir milik pemerintah Iran.³⁶ Pernyataan perusahaan keamanan komputer Rusia Kaspersky Lab menyimpulkan bahwa serangan canggih tersebut bisa

³⁴ Lihat Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 Int'l L. STUD, 99 (2002), hlm.102-103.

³⁵ James HLM. Farwell and Rafal Rohonzinski, ohlm.cit., hlm. 23-26. Stuxnet merupakan cacing komputer yang diketahui keberadaannya di bulan Juli 2010. Perangkat perusak ini memiliki sasaran peranti lunak Siemens dan perangkat yang berjalan dalam sistem operasi Microsoft Windows. Ini bukan pertama kalinya cracker menargetkan sistem industri. Namun, ini adalah perangkat perusak pertama yang ditemukan mengintai dan mengganggu sistem industri, dan yang pertama menyertakan rootkit *programmable logic controller (PLC)*. Cacing ini awalnya menyebar secara membabi buta, namun memuat muatan perangkat perusak yang sangat khusus yang dirancang hanya mengincar sistem Kontrol Pengawas Dan Akuisisi Data Siemens (SCADA, *Siemens Supervisory Control And Data Acquisition*) yang diatur untuk mengendalikan dan memantau proses industri tertentu. Stuxnet menginfeksi PLC dengan mengubah aplikasi perangkat lunak Step-7 yang digunakan untuk memprogram ulang perangkat tersebut.

³⁶ Reuters, 2-Serangan siber Appears to target Iran-tech Firms, http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE-68N1OI20100924.

dilakukan "dengan dukungan negara" dan diduga bahwa Israel dan Amerika Serikat mungkin telah terlibat.³⁷

Tidak seperti Stuxnet yang menyerang dan atau menginfeksi komputer dan jaringan. Di akhir Bulan Mei 2012, ditemukan adanya pengembangan virus jenis baru yang disebut "Flame" yang berfungsi sebagai alat spionase atau mata-mata dengan cara melakukan infiltrasi ke dalam komputer dan jaringan dan eksfiltrasi informasi yang terdapat (posting) dalam komputer dan jaringan. Pengembangan Flame ini dilakukan oleh negara-negara untuk memata-matai aktifitas negara lain.³⁸

Sepintas, beberapa serangan siber ³⁹ yang terjadi dalam kurun waktu 2005-2012 telah memenuhi kualifikasi yang disebutkan dalam definisi yang dikemukakan SWGCA. Akan tetapi, hal ini akan menimbulkan perdebatan khususnya dugaan bahwa tindakan kejahatan tersebut dilakukan oleh negara, sebagaimana disebutkan dalam Resolusi Majelis Umum Nomor 3314 (XXIX) 14 Desember 1974 yang menyatakan bahwa tindak agresi yang ditentukan telah dilakukan oleh negara.

Oleh karena itu, dalam menjembatani fakta dan teori tentang kejahatan siber dan kejahatan agresi maka diperlukan

³⁷ Ibid.

³⁸ David P. Fiddler, *Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law*, ASIL, Vol.16. Issue 22 (20 June 2012), hlm. 1. Lihat juga Thomas Erdbrink, *Iran Confirms Attack by Virus That Collects Information*, N.Y. Times, May 29, 2012, at A4. Lihat juga Kim Zeiter, *Researchers Connect Flame to US-Israel Stuxnet Attack*, Wired.com (June 11, 2012), *available at*http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet/?utm_source=June+11%2C+2012-AoH&utm_campaign=BNT+06112012&utm_medium=email.

³⁹ Lihat http://www.un.org/News/Press/docs/2010/soccp349.doc.htm, Delegates Consider Best Response to Cybercrime as Congress Committee: Takes Up Dark Side of Advances in Information Technology, posting 13 April 2010, accessed by 05 October 2012.

solusi tepat untuk mendudukan keduanya sebagai suatu fakta yuridis dalam literatur hukum internasional kontemporer. Tentunya solusi tersebut membutuhkan media dan dalam hal ini metode penafsiran sangat tepat untuk digunakan, sebagaimana yang dilakukan PBB. Akan tetapi dalam konteks ini, pendekatan yang akan digunakan adalah hermeneutika hukum. Pendekatan ini dipandang memiliki daya jangkau yang lebih luas dibandingkan penafsiran dan atau interpretasi. Hal ini dilakukan untuk memberikan ruang yang lebih bebas agar dapat memecahkan persoalan kejahatan siber dan kejahatan agresi dalam studi hukum internasional kontemporer.

⁴⁰ Gregory Leyh, Hermeneutika Hukum: Sejarah, Teori, dan Praktik, diterjemahkan oleh M. Khozim, (Bandung: Nusamedia, 2011), hlm. 1. Lihat juga Adian Husaini dan Abdurrahman Al-Bahgdadi, Hermeneutika dan Tafsir Al-Qur'an, (Jakarta: Gema Insani, 2007), hlm.7.

⁴¹ Fred Dallmayr, Hermeneutika dan Rule of Law, dalam Gregory Leyh, Hermeneutika Hukum: Sejarah, Teori, dan Praktik, diterjemahkan oleh M. Khozim, (Bandung: Nusamedia, 2011), hlm. 15.

BAB II

KEJAHATAN SIBER

A. Sejarah Singkat Perkembangan Cyberspace

Komputer pertama kali ditemukan sekitar tahun 1940 dan pada tahun 1950 komputer difungsikan untuk meningkatkan kemampuan militer. Komputer dalam perkembangan berikutnya menjadi sesuatu yang sangat penting dan sangat dibutuhkan khususnya untuk tujuan penelitian dan komunikasi bagi institusi akademi (universitas), organisasi militer, dan institusi keuangan. Keingintahuan mahasiswa perguruan tinggi yang begitu besar terhadap kebutuhan penggunaan komputer sehingga mereka berupaya untuk mengembangkannya karena mereka yakin bahwa komputer dapat menyelesaikan berbagai masalah yang timbul.⁴²

Perkembangan komputer yang digunakan untuk peruntukkan militer dan universitas dikembangkan dengan menggunakan sistem jaringan komputer (computer network system) yang terdapat dalam suatu rangkaian terminal komputer. Rangkaian jaringan komputer ini kemudian membentuk LAN (local area network) dan rangkaian beberapa LAN kemudian membentuk WAN (wide area network). Dalam

⁴² Samuel C. McQuade, Encyclopedia Cyber Crime, (Westport: Greenwood Press, 2009), hlm. ix-x.

⁴³ Abdul Wahid dan Mohammad Labib, op.cit, hlm. 33-34.

konteks yang lebih luas, WAN ini kemudian dikenal dengan sebutan internet (*cyberspace*).⁴⁴

Dalam perkembangan selanjutnya, Selama tahun 1960, dengan penemuan dan pengembangaan internet oleh ARPANET (*US Defense Advanced Research Project Agency*), pengembangan komputer yang berlokasi di universitas dapat dihubungkan dengan aktifitas-aktifitas pemerintah dan bisnis. Hal ini dimaksudkan untuk menghindarkan akses penyalahgunaan komputer yang rawan untuk menimbulkan *chaos*.⁴⁵

Kontribusi positif dalam kurun waktu dua atau tiga dekade, perlahan mulai bergeser ke arah penyalahgunaan komputer (computer abuse). Hal tersebut terjadi di pertengahan tahun 1970. Ini dikarenakan aktifitas-aktifitas yang menyalahgunakan komputer tidak dilarang menurut hukum kejahatan komputer.

Pada tahun 1980, Pemerintah dan Pemerintah Federal mulai menerapkan hukum kejahatan komputer yang tentunya berangkat dari semakin berkembangannya industri komputer dengan koneksi internet. Awalnya, aturan ini memfokuskan pada fenomena pembajakan komputer. Akan tetapi, kemudian fokusnya diperluas hingga menyoal pada perilaku kejahatan.

Keberadaan aturan atau regulasi yang dibuat tidaklah menghambat penemuan dan inovasi komputer dan telekomunikasi. Justru sebaliknya pengembangan komputer dan telekomunikasi terus berlangsung, meskipun dengan resiko

⁴⁴ Al Wisnubroto, Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer, (Yogyakarta: Penerbitan Universitas Atmajaya, 1999), hlm. 35.

⁴⁵ Agus Raharjo, op.cit, hlm. 61.

bahwa jumlah penyalahgunaan komputer juga mengalami peningkatan signifikan.

B. Istilah

Istilah siber menjadi istilah yang sering digunakan oleh seluruh lapisan masyarakat sekarang ini. Kata siber telah ditambahkan pada berbagai istilah untuk menggambarkan bentuk masyarakat atau jenis kejahatan baru yang berbasis siber, seperti *cyber society*⁴⁶, *cyber attacks*⁴⁷, *cyber crime*, *cyber terrorism*, dan lain sebagainya.⁴⁸ Dalam konteks ini, yang menjadi penekanan dalam tulisan ini yaitu *cyber crime*.

Sebelum menjelaskan lebih jauh tentang pengertian kejahatan siber, dipandang perlu untuk menyatukan pendapat tentang apa yang dimaksud dengan kejahatan siber. Apakah kejahatan telematika dapat disamakan dengan kejahatan komputer (computer crime) atau kejahatan siber (cyber crimes) atau ketiganya adalah jenis kejahatan baru yang dikenal dalam kepustakaan teknologi dan informasi.⁴⁹

Pada beberapa literatur disebutkan bahwa apa yang disebut dengan kejahatan telematika (konvergensi), itu pula

⁴⁶ Lihat P. Lorents, R. Ottis, and R. Rikk, *Cyber Society and Cooperative Cyber Defence. In Internationalization, design and Global Development.* Lecture Notes in Computer Science, Vol. 5623 (2009), hlm. 180-186.

⁴⁷ Lihat juga R. Ottis, Analysis of the 2007 Serangan siber s Against Estonia from the Information Warfare Perspective, in Proceeding of the 7th European Conference on Information warfare and Security, (Plymouth: Academic Publishing Limited, 2008), hlm. 163-168.

⁴⁸ R. Ottis and HLM. Lorents, Cyberspace: Definitions and Implications, (Estonia: Cooperative Cyber Defence Centre of Excellence, 2009), hlm. 267.

⁴⁹ Maskun, Kejahatan Cyber Crime, (Makassar: Pustaka Pena Press, 2011), hlm. 51.

yang disebut dengan kejahatan siber.⁵⁰ Hal ini didasari pada argumentasi bahwa *cyber crimes* merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi baik itu *dial up system,* menggunakan jalur telepon, ataukah *wireless system* yang menggunakan antena khusus yang nirkabel.⁵¹ Konvergensi antara komputer dan sistem telekomunikasi sebagaimana diataslah yang disebut dengan telematika. Sehingga jika menyebutkan kejahatan telematika maka yang dimaksud juga adalah *cyber crimes*.

Akan tetapi disisi lain, beberapa pakar tetap berpendapat bahwa baik kejahatan komputer, kejahatan siber, maupun kejahatan telematika adalah kejahatan yang sama dengan penamaan berbeda. Argumentasi yang melatarbelakanginya bahwa meskipun pada awalnya komputer hanyalah sebagai alat pengumpul dan penyimpan data yang dapat digunakan untuk melakukan kejahatan konvensional, akan tetapi dalam perkembangan selanjutnya kejahatan komputer juga telah dilakukan dengan basis internet seperti trojan horse hacking, dan data leakage.

Kontroversi pengistilahan di atas, tidaklah menciptakan perdebatan mengenai penggunaan istilah yang digunakan. Oleh karena itu, dengan alasan konsistensi penulis maka istilah yang digunakan kejahatan siber (*cyber crimes*).

⁵⁰ Istilah lain yang dikenal untuk menggambarkan kejahatan *cyber* antara lain kejahatan maya antara dan kejahatan internet.

⁵¹ Judhariksawan, Pengantar Hukum Telekomunikasi, (Jakarta: Rajawali Press, 2005), hlm. 12-13.

C. Pengertian

Sebelum menguraikan pengertian *cyber crimes* secara terinci, terlebih dahulu akan dijelaskan "induk" *cybercrimes* yaitu *cyber space*. Konsep ini dipandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini *cyberspace* dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam bahasa sehari-hari dikenal dengan internet.

Realitas baru ini dalam kenyataanya terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis protokol *transmission control protocol/internet protocol.* Hal ini berarti, dalam sistem kerjanya dapatlah dikatakan bahwa *cyberspace* telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.⁵²

Dalam perkembangan selanjutnya kehadiran teknologi canggih komputer dengan jaringan internet telah membawa manfaat besar bagi manusia. Pemanfaatannya tidak saja dalam pemerintahan, dunia swasta/perusahaan, akan tetapi sudah menjangkau pada seluruh sektor kehidupan termasuk segala keperluan rumah tangga dan pribadi. Komputer dengan jaringan internet telah mampu membuka cakrawala baru dalam kehidupan manusia baik dalam konteks sarana komunikasi dan informasi yang menjanjikan menembus batas-batas negara

⁵² Kenny Wiston, The Internet: Issues of Jurisdiction and Controversies Surrounding Domain Names, (Bandung: Citra Aditya,2002), hlm. Vii.

maupun penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuwan di seluruh dunia.⁵³

Akan tetapi, kemajuan teknologi informasi (internet) dan segala bentuk manfaat didalamnya membawa konsekuensi negatif tersendiri dimana semakin mudahnya para penjahat untuk melakukan aksinya yang semakin meresahkan masyarakat. Penyalahgunaan yang terjadi dalam *cyberspace* inilah yang kemudian dikenal dengan *cyber crime* atau dalam literatur lain digunakan istilah *computer crime*.

Dalam beberapa kepustakaan, *cyber crime* sering diidentikkan sebagai *computer crime*. Menurut the U.S. Department of Justice, *computer crime* sebagai "any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution"⁵⁴. Pendapat lain dikemukakan oleh *Organization for Economic Cooperation Development* (OECD) yang menggunakan istilah *computer related crime* yang berarti any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data.⁵⁵

Dari berbagai pengertian computer crime di atas, dapat dirumuskan bahwa computer crime merupakan perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai obyek, baik untuk memperoleh keuntungan maupun tidak, dengan merugikan pihak lain.

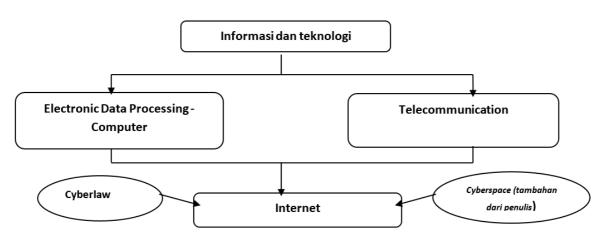
⁵³ Widyopramono Hadi Widjojo, *Cybercrimes dan Pencegahannya*, Jurnal Hukum Teknologi, Fakultas Hukum Universitas Indonesia, Vol 2 (Agustus 2005), hlm. 7.

⁵⁴ www.usdoj.gov/criminal/cybercrimes.

⁵⁵ Lihat Obsatar Sinaga, Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia, Makalah, IPB Bogor, 5 Desember 2010., hlm. 10.

Cyber crime di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer akan tetapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya. Hal ini dapat dilihat pada pandangan Indra Safitri yang mengemukakan bahwa 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 tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.

Untuk lebih jelasnya posisi *cyberspace* dapat dilihat pada bagan evolusi hukum siber (*cyberlaw*) yang merupakan aturan main dalam *cyberspace*.⁵⁸



Komposisi bagan sebagaimana di atas dapatlah diilustrasikan dengan memaknai dan memahami sistem kerja komputer dan telekomunikasi yang menghasilkan internet yang kemudian disebut *cyberspace* (*kolom cyberspace pada bagian*

⁵⁶ Ari Juliano Gema, Cybercrime: Sebuah Fenomena di Dunia Maya, 2000, diakses pada www.theceli.com.

⁵⁷ Indra Safitri, Tindak Pidana di Dunia Cyber, Insider, Legal Journal From Indonesian Capital and Investment Market, 1999, diakses http://business.fortunecity.com.

⁵⁸ Agus Raharjo, op.cit. hlm. 222

kanan adalah tambahan penulis) yang membutuhkan aturan yang disebut dengan cyberlaw.

Merujuk pada komposisi bagan di atas, dapat dikatakan bahwa *cybercrime* dan *computer crime* adalah dua hal yang berbeda. Perbedaan tersebut dapat dilihat pada pandangan yang dikemukan oleh Nazura Abdul Manaf⁵⁹ yang membedakan *cybercrime* dan *computer crime*, sebagai berikut:

"Defined broadly, computer crime could reasonably include a wide variety of criminal offences, activities or issues. It is also known as a crime committed using a computer as a tool and it involves direct contact between the criminal and the computer. For instance, a dishonest bank clerk who unauthorizedly transfers a customer's money o a dormant account for his own interest or a person without permission has obtained access to other person's computer directly to download information, which in the first place, are confidential. These situations require direct access by the hacker to the victim's computer. There is no internet line involved, or only limited networking used such as the Local Area Network (LAN). Whereas, cyber crimes are committed virtually through internet online. This means that the crimes could extend to other countries, which is beyond the Malaysian jurisdiction. Anyway, it causes no harm to refer computer crimes as cyber crimes or vice versa, since they have same impact in law".

Perbedaan mendasar cyber crime dan computer crime sebagaimana yang dikemukakan oleh Nazura Abdul Manaf adalah adanya unsur komputer yang terkoneksi melalui perangkat telekomunikasi dalam bentuk internet online yang

⁵⁹ ibid, hlm. 227

menjadi media bagi seseorang atau kelompok untuk melakukan pelanggaran dan atau kejahatan.

D. Jenis Kejahatan Siber

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk antara lain:⁶⁰

1. Akses pelayanan dan sistem komputer yang tidak sah (unauthorized access to computer system and service);

Kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet. Beberapa contoh yang berhubungan dengan hal tersebut, antara lain:

a) Pada tahun 1999, ketika masalah Timor Timur sedang hangat dibicarakan di level internasional,

⁶⁰ Ari Juliano Gema, loc.cit. Lihat juga Maskun,ohlm.cit, hlm. 58-63 (diekstraksi). Lihat juga Dikdik M. Arief Mansur dan Alitaris Gultom, ohlm. cit., hlm. 9-10. Lihat juga Budi Suhariyanto,Tindak Pidana Teknologi Informasi (*Cybercrime*), (Jakarta: PT. RajaGrafindo, Persada, 2012), hlm. 14-16.

- beberapa website milik pemerintah Republik Indonesia dirusak oleh *hacker*.⁶¹
- b) Pada tahun 2000, hacker berhasil menembus masuk ke dalam *data base* sebuah perusahaan Amerika Serikat yang bergerak di bidang *e-commerce* yang memiliki tingkat kerahasiaan yang tinggi.
- c) Pada tahun 2004, situs Komisi Pemilihan Umum (KPU) dibobol hacker yang notabene memiliki tingkat keamanan yang sangat tinggi.
- 2. Data atau Informasi yang Tidak Sah (Illegal Contents);

Kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah:

- a) Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
- b) Pemuatan hal-hal yang berhubungan dengan pornografi.
- c) Pemuatan suatu informasi yang merupakan rahasia negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.
- 3. Pemalsuan Data (Data Forgery);

Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

⁶¹ Lihat Kompas 11 Agustus 1999.

4. Siber Espionase (Cyber Espionage);

Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.

5. Siber Sabotase (Cyber Sabotage and Extortion);

Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*,62 virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase, tentunya dengan bayaran tertentu.

Sebagai contoh, pada April 1997, Kementerian Energi Amerika Serikat Unit *Computer Incident Advisory Capability* mengumumkan adanya suatu program *Trojan Horse* yang sangat berbahaya yang dapat menghapus

⁶² *Logic bomb* adalah suatu program yang dibuat dan dapat digunakan oleh pelakunya sewaktu-waktu atau tergantung dari keinginan dari si pelaku, dari situ terlihat bahwa informasi yang ada di dalam komputer tersebut dapat terganggu, rusak, atau bahkan hilang.

semua file dalam hard disk yang bersirkulasi di internet.63

6. Pelanggaran Terhadap Kekayaan Intelektual (Offence Against Intellectual Property);

Kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seorang di internet. Sebagai contoh adalah peniruan tampilan web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. Kejahatan Terhadap Privasi Seseorang (Infringements of Privacy);

Kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain maka dapat merugikan orang tersebut baik secara materiil maupun immateriil, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi dan sebagainya.

a) Pelecehan atau Gangguan dengan Media Siber (Cyberstalking);

Kejahatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan email yang dilakukan secara berulang-ulang seperti teror di dunia siber. Pada umumnya perempuan

⁶³ Gabriola Zeviar-Geese, The State of the Law on Cyberjurisdiction and Cybercrime on the Internet, (California Pacific School of Law), hlm. 3.

menjadi target *cyberstalkers*. Sebagai contoh, seorang perempuan di Carolina Selatan telah diganggu dalam beberapa tahun melalui email oleh seseorang yang tidak dikenal yang mengancam kehidupannya.⁶⁴

b) Penipuan (Fraud);

Kejahatan yang dilakukan melalui modus penipuan dengan target informasi kartu kredit dan informasi pribadi serta keuangan. Pada April 1997, Komisi Perdagangan Federal dan Asosiasi Administrator Keamanan Amerika Utara melakukan penyelidikan atas dugaan *fraud* di internet.⁶⁵

c) Siber Teroris (Cyberterrorism);

Kejahatan yang berbasis politik, ideologi dan agama yang dilakukan dengan memanfaatkan perangkat teknologi yang ada. Akibat yang ditimbulkannya berdampak pada manusia dan infrastruktur.⁶⁶

Uraian berbagai jenis kejahatan siber sebagaimana disebutkan di atas, dikemukan pula oleh Richard Power,⁶⁷ dimana beliau menyebutkan jenis tindak kejahatan

⁶⁴ Gabriola Zeviar-Geese, ohlm.cit., hlm. 5. Lihat juga Barbara Jenson, Cybertalking: Crime, Enforcement and personal Responsibility in the On-Line World, (May, 1996), hlm.10.

⁶⁵ Lihat juga Jonathan Rosenoer and Kimberly Smigel, Notable Legal Development Reported in April 1997, Cyberlex.

⁶⁶ Jonathan Clough, Principle of Cybercrime, (Cambridge: Cambridge University Press, 2010), hlm. . 11-12. Lihat juga C. Walker, *Cyber-terrorism: Legal principle and law in the United Kingdom*, Pennsylvania State Law Review 625 (2006), hlm. 635–42.

⁶⁷ Richard Power, dalam Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace, QUE Division of Macmillan, USA., 2000. Lihat juga Dikdik M. Arief Mansur dan Alitaris Gultom, op.cit., hlm.26.

komputer (cyber crime) sebagai berikut "There is a broad spectrum of cyber crimes, including:

- Unauthorized access by insiders (such as employees);
- System penetration by outsiders (such as hackers);
- 3. Theft of proprietary information (whether a simple user ID and password or a trade secret worth tens of millions of dollars);
- 4. Financial fraud using computers;68
- 5. Sabotage of data or networks;
- 6. Disruption of network traffic, for example denial of service attacks;
- 7. Creation and distribution of computer viruses, Trojan horses, and other type of malicious code;
- 8. Software piracy;
- 9. Identity theft; and
- 10. Hardware theft, for example laptop theft".

Hal lain yang penting untuk digaris bawahi bahwa tidak semua tindak kejahatan yang dilakukan dengan komputer merupakan kejahatan komputer (*cyber crimes*). Misalnya,

⁶⁸ Financial fraud using computers dapat pula disebut sebagai internet fraud. Menurut US Department of Justice, jenis-jenis internet fraud antara lain:

Skema lelang dan retail online. Skema ini berisi penawaran item-item bernilai tinggi yang memungkinkan menarik perhatian konsumen.

Skema peluang bisnis. Skema ini menggunakan internet untuk mempromosikan peluang bisnis yang memungkinkan seseorang memperoleh ribuan dollar dalam sebulan dengan work at home.

Pencurian identitas dan fraud. Skema ini melibatkan pencurian identitas, yaitu memperoleh dan menggunakan data personal orang lain untuk melakukan fraud demi kepentingan ekonomis.

Skema investasi. Skema investasi online ini umumnya berupa skema manipulasi pasar.

apabila seseorang mencuri satu kode akses tertentu seperti nomor kartu untuk sambungan telepon jarak jauh dan mempergunakannya untuk melakukan telepon jarak jauh, nomor tersebut diperiksa oleh komputer sebelum sambungan telepon itu diproses. ⁶⁹ Meskipun dalam hal ini tetap juga menggunakan media komputer, akan tetapi tindak kejahatan seperti ini tidak dikategorikan kejahatan komputer melainkan lebih kepada "penipuan bea". ⁷⁰

E. Media Komputer dalam Kejahatan Siber

Bertitik tolak pada gambaran singkat kasus di atas, dalam konteks media yang digunakan oleh pelaku adalah komputer maka dalam hal ini tindak kejahatan tersebut dapat dianalisis berupa:⁷¹

1. Komputer sebagai sasaran

Ketika komputer merupakan sasaran dari tindak kejahatan, tujuan si penjahat adalah untuk mencuri informasi dari, atau menyebabkan kerusakan pada komputer, suatu sistem komputer, atau jaringan komputer. Bentuk kejahatan semacam ini menjadikan sistem komputer sebagai sasarannya baik untuk mendapatkan informasi yang disimpan pada sistem komputer maupun untuk menguasai sistem itu tanpa otorisasi contohnya penghentian *yahoo!* akibat *overload*.⁷²

⁶⁹ Maskun, op.cit., hlm. 64.

William Wiebe, Tindak Kejahatan Melalui Komputer, Seminar, Makassar, 2000. hlm. 4

⁷¹ ibid, hlm. 5-8

⁷² Overload artinya kelebihan beban yang diakibatkan oleh membanjirnya pesan-pesan yang masuk melalui e-mail.

Bentuk kejahatan seperti ini pada umumnya melibatkan *hacker*⁷³ yang melakukan pencantolan pada sistem komputer untuk mendapatkan akses secara tidak sah (*access illegal*). Pencurian informasi dapat dilakukan dalam berbagai cara seperti:

- a. Pencurian informasi tentang keamanan (militer) suatu negara yang menggoda bagi para teroris.
- b. Pembobolan nomor-nomor kartu kredit.
- c. Pencurian rahasia dagang.
- d. Penggandaan bahan cetakan yang memiliki hak cetak, seperti program-program *software*.
- e. Pencurian informasi pribadi orang lain dengan tujuan untuk melakukan pemerasan uang atau untuk alasan-alasan bisnis.

Dalam kasus dimana *hackers* memperoleh akses yang tidak sah ke suatu komputer untuk masuk kedalam suatu sistem jaringan hubungan telepon jarak jauh. Pada kasus ini, tindakan para *hackers* disebut dengan *phreaking*.

2. Komputer sebagai ketidak-sengajaan atas suatu kejahatan.

Komputer dalam hal ini digunakan sebagai penyimpan informasi. Misalnya para pengedar narkotika yang menyimpan informasi tentang penjualan dan para langganannya atau juga dapat berupa tindakan para hackers yang menyimpan password atau nomor-nomor

⁷³ Hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengamanan lainnya, tetapi tidak melakukan tindakan perusakan apapun, tidak mencuri uang atau informasi. Dalam hal seseorang (illegal hacker) melakukan perusakan dan pencurian informasi maka pelakunya disebut dengan *cracker*.

kartu kredit yang telah dicurinya dalam komputer. Oleh karena itu, dapat dikatakan bahwa pada cara kedua ini komputer berisikan bukti-bukti pelanggaran hukum yang dilakukan oleh para *hackers*.

3. Komputer sebagai sarana untuk melakukan tindak kejahatan.

Komputer pada cara ini dipergunakan untuk kejahatan dengan sistem elektronik sebagai sarana untuk melakukan kejahatan. Pada umumnya kejahatan semacam ini merupakan tindak kejahatan tradisional yang dilakukan dengan komputer. Akan tetapi, modus tersebut telah berkembang, dimana kejahatan elektronik tersebut telah menghubungkan komputer dan internet sebagai sarana untuk melakukan atau mempermudah kejahatan-kejahatan yang bersifat tradisional/konvensional.

Pada bulan April 1999 misalnya, seorang bekas satpam yang berumur 50 tahun dinyatakan bersalah di California atas tuduhan pelecehan seksual melalui internet terhadap seorang wanita. Si satpam akhirnya dinyatakan bersalah dengan hukum enam tahun penjara.

F. Kejahatan Siber Sebagai Salah Satu Kejahatan Internasional

Penggunaan istilah hukum kejahatan internasional merupakan istilah yang relatif baru dalam studi literatur di Indonesia.⁷⁴ Meskipun dalam studi literatur pada umumnya, istilah ini bukanlah suatu studi ilmu hukum yang baru. Hal

⁷⁴ I Wayan Parthiana, Hukum Pidana Internasional, (Bandung: Yrama Widya, 2006), hlm. 27.

ini dapat dilihat pada uraian sejarah perkembangan hukum kejahatan internasional yang menunjukkan aktivitas tindak pidana internasional seperti pembajakan di laut (*piracy*) hampir memiliki usia yang sama dengan sejarah perkembangan peradaban manusia.⁷⁵ Oleh karena itu, sebagai suatu kajian ilmu hukum maka menurut penulis istilah yang digunakan adalah hukum kejahatan internasional.

istilah Penggunaan ini dipertimbangkan dengan argumentasi bahwa lingkup atau cakupan kejahatan internasional bersifat lebih luas. Keluasan makna hukum kejahatan internasional dikarenakan kejahatan yang sudah ditetapkan sebagai tindak pidana juga meliputi kejahatan yang belum ditetapkan sebagai tindak pidana dalam hukum pidana nasional negara-negara.⁷⁶

Argumentasi lain yang digunakan untuk menunjukkan kejahatan sebagai ilmu, urgensi hukum sebagaimana oleh Bassiouni⁷⁷ bahwa hukum kejahatan dikemukakan berkembang internasional sedang dan sesuai kondisi dunia dewasa ini. Argumentasi lain yang digunakan untuk menunjukkan urgensi hukum kejahatan sebagai ilmu, sebagaimana dikemukakan oleh Bassiouni⁷⁸ bahwa hukum kejahatan internasional sedang berkembang dan sesuai dengan kondisi dunia dewasa ini.

Meskipun telah diuraikan di atas bahwa istilah yang digunakan dalam tulisan ini adalah hukum kejahatan

⁷⁵ Romli Atmasasmita, Pengantar Hukum Pidana Internasional, (Bandung: Eresco, 1995), hlm. 2-3

⁷⁶ I Wayan Parthiana, loc.cit..

⁷⁷ M. Cherif Bassiouni, *International Criminal Law, Vol III Enforcement*, (New York: Transnational Publishers, Inc, 1987), hlm. xiii.

⁷⁸ Ibid.

internasional. Akan tetapi pada dasarnya penggunaan istilah tindak pidana internasional atau *international crimes*, baik menurut perjanjian-perjanjian internasional maupun di dalam hukum kebiasaan internasional, masih terus diperdebatkan karena belum terdapat ketentuan yang jelas hingga saat ini. Hal tersebut disebabkan adanya perdebatan seputar penetapan peristilahannya yang dapat berdampak luas, dalam hal substansi dan subjeknya⁷⁹.

Sudah sejak abad ke-18, masyarakat bangsa-bangsa mengenal dan mengakui kejahatan perompak di laut sebagai kejahatan internasional yang dikenal sebagai *piracy de jure gentium*⁸⁰. Kejahatan tersebut dianggap sangat merugikan kesejahteraan bangsa-bangsa pada saat itu dan dianggap sebagai musuh bangsa-bangsa. *Piracy de jure gentium* kemudian ditetapkan sebagai kejahatan internasional karena merupakan satu-satunya tindak kriminal murni.

Definisi tentang tindak pidana internasional atau kejahatan internasional (*international crimes*) menurut Bassiouni⁸¹ sebagai berikut:

"Tindak pidana internasional adalah setiap tindakan yang telah ditetapkan di dalam konvensi-konvensi multilateral dan yang telah diratifikasi oleh negara-negara peserta, sekalipun di

⁷⁹ Romli Atmasasmita, Pengantar Hukum Pidana Internasional, (Bandung: Refika Aditama, 2003), hlm.35

⁸⁰ Istilah *Piracy de jure gentium* merupakan istilah yang dipergunakan pada Zaman Romawi Kuno terhadap para pembajak laut yang dianggap sebagai pelaku kejahatan, mengancam bangsa Romawi yang saat itu menggunakan hukum yang disebut dengan *Jure Gentium* atau hukum nasional terhadap negara kekuasaan Romawi. Lihat, Eddy O.S. Hiariej, Pengantar Hukum Pidana Internasional (Jakarta: Airlangga, 2009), hlm. 49.

⁸¹ Romli Atmasasmita, op.cit, hlm. 37.

dalamnya terkandung salah satu dari kesepuluh karakteristik pidana"

Bassiouni lebih lanjut menjelaskan kesepuluh karakteristik yang dimaksudkan, sebagai berikut:

- Explicit recognition of proscribed conduct as constituting an international crime or a crime under international law. (Pengakuan secara eksplisit atas tindakan-tindakan yang dipandang sebagai kejahatan berdasarkan hukum internasional).
- 2. Implicit recognition of the penal nature of the act by establishing a duty to prohibit, prevent, prosecute, punish or the like (pengakuan secara implisit atas sifat-sifat pidana dari tindakan-tindakan tertentu dengan menetapkan suatu kewajiban untuk menghukum, mencegah, menuntut, menjatuhi hukuman atau pidananya).
- 3. Criminalization of the proscribed conduct (kriminalisasi atas tindakan-tindakan tertentu).
- 4. Duty or right to prosecute (kewajiban atau hak untuk menuntut).
- 5. Duty or right to punish the proscribed conduct. (kewajiban atau hak untuk memidana tindakan tertentu).
- 6. Duty or right to extradite (kewajiban atau hak untuk mengekstradisi).
- 7. Duty or right to cooperate in prosecution, punishment, including judicial assistance in penal proceeding. (kewajiban atau hak untuk bekerjasama di dalam proses pemidanaan).
- 8. Establishment of a criminal jurisdiction basis (penetapan suatu dasar-dasar yurisdiksi kriminal).
- 9. Reference to the establishment of an international court (referensi pembentukan suatu pengadilan internasional).

10. Elimination of the defense of superiors orders (penghapusan alasan-alasan perintah atasan).

Dilihat dari perkembangan dan asal-usul tindak pidana internasional ini, eksistensi tindak pidana internasional dapat dibedakan dalam:82

- 1. Tindak pidana internasional yang berasal dari kebiasaan yang berkembang di dalam praktik hukum internasional.
- 2. Tindak pidana internasional yang berasal dari konvensikonvensi internasional.
- 3. Tindak pidana internasional yang lahir dari sejarah perkembangan konvensi mengenai hak asasi manusia.

Tindak pidana internasional yang berasal dari kebiasaan hukum internasional adalah tindak pidana pembajakan atau piracy, kejahatan perang atau war crimes, dan tindak pidana perbudakan atau Slavery. Tindak pidana internasional yang berasal dari konvensi-konvensi internasional ini secara historis dibedakan antara tindak pidana internasional yang ditetapkan di dalam satu konvensi saja dan tindak pidana internasional yang ditetapkan oleh banyak konvensi.

Tindak pidana internasional yang lahir dari sejarah perkembangan konvensi mengenai hak asasi manusia merupakan konsekuensi logis akibat Perang Dunia II yang meliputi bukan hanya korban-korban perang mereka yang termasuk *combatant*, melainkan juga korban penduduk sipil (non-combatant) yang seharusnya dilindungi dalam suatu peperangan. Salah satu tindak pidana internasional ini adalah *crimes of genocide* sesuai dengan Deklarasi Perserikatan Bangsa-Bangsa (PBB) Tanggal 11 Desember yang menetapkan genosida sebagai kejahatan menurut hukum internasional⁸³.

⁸² *Ibid.*hlm. 40.

⁸³ Ibid

Penetapan tindak pidana internasional atau *International crimes* itu diperkuat dalam Piagam Mahkamah Militer Internasional di Nuremberg atau *the International Military Tribunal* yang dibentuk segera setelah Perang Dunia II terakhir (1946). Mahkamah ini ditetapkan oleh negara pemenang Perang Dunia II yakni Amerika Serikat, Inggris, Prancis, dan Rusia. The *International Military Tribunal* memiliki yurisdiksi atas tiga golongan kejahatan:

- Crimes against peace atau kejahatan atas perdamaian, yang diartikan termasuk persiapan-persiapan atau pernyataan perang agresi.
- 2. War crimes atau kejahatan perang atau pelanggaran atas hukum-hukum tradisional dan kebiasaan dalam peperangan.
- 3. Crimes against humanity yakni segala bentuk kekejaman terhadap penduduk sipil selama peperangan berlangsung.

Dalam naskah rancangan ketiga Undang-Undang Pidana Internasional atau the International Criminal Code Tahun 1954, telah ditetapkan 13 kejahatan yang dapat dijatuhi pidana berdasarkan hukum internasional sebagai kejahatan terhadap perdamaian dan keamanan seluruh umat manusia. Ketiga belas tindak pidana ini adalah sebagai berikut:

- 1. Tindakan persiapan untuk agresi dan tindakan agresi.
- 2. Persiapan penggunaan kekuatan bersenjata terhadap negara lain.
- 3. Mengorganisasi atau memberikan dukungan persenjataan yang ditujukan untuk memasuki wilayah suatu negara.
- 4. Memberikan dukungan untuk dilakukan tindakan terorisme di negara asing.
- 5. Setiap pelanggaran atas perjanjian pembatasan senjata yang telah disetujui.

- 6. Aneksasi wilayah asing.
- 7. Genocide (genosida).
- 8. Pelanggaran atas kebiasaan dan hukum perang.
- 9. Setiap pemufakatan, pembujukan, dan percobaan untuk melakukan tindak pidana tersebut pada butir 8 di atas.
- 10. Piracy (Pembajakan).
- 11. Slavery (Perbudakan).
- 12. Apartheid.
- 13. Threat and use of force against internationally protected persons.

Dalam naskah rancangan Undang-Undang Pidana Internasional atau *The International Criminal Code* Tahun 1979 yang disusun oleh *The International Association of Penal Law*, telah dimasukkan jenis tindak pidana lainnya, seperti: lalu lintas perdagangan narkotika ilegal (*illicit drug trafficking*), pemalsuan mata uang (*counterfeiting*), keikutsertaan di dalam perdagangan budak, penyuapan (*bribery*), dan pengambilan harta karun negara tanpa izin.

Berdasarkan internasionalisasi kejahatan dan karakteristik kejahatan internasional, dalam konteks hukum kejahatan internasional, kejahatan internasional memiliki hirarki atau tingkatan. Sampai dengan tahun 2003 atas dasar 281 konvensi internasional sejak tahun 1812, ada 28 kategori kejahatan internasional. Kategori tersebut yakni⁸⁴:

- 1. Aggression.
- 2. Genocide.
- 3. Crimes against humanity.
- 4. War crimes.
- 5. Unlawful possession or use or emplacement of weapons.

⁸⁴ Eddy O.S. Hiariej, op.cit. hlm. 55.

- 6. Theft of nuclear materials.
- 7. Mercenaries.
- 8. Apartheid.
- 9. Slavery and slave-related practices.
- 10. Torture and other forms of cruel, inhuman, or degrading treatment.
- 11. Unlawful human experimentation.
- 12. Piracy.
- 13. Aircraft hijacking and unlawful acts against international air safety.
- 14. Unlawful acts against the safety of maritime navigation and the safety of platforms on high seas.
- 15. Threat and use of force against internationally protected persons.
- 16. Crimes against United Nations and associated personnel.
- 17. Taking of civilian hostages.
- 18. Unlawful use of the mail.
- 19. Attacks with explosives.
- 20. Financing of terrorism.
- 21. Unlawful traffic in drugs and related drug offenses.
- 22. Organized crime.
- 23. Destruction and/or theft of national treasures.
- 24. Unlawful acts against certain internationally protected elements of the environment.
- 25. International traffic in obscene materials.
- 26. Falsification and counterfeiting.
- 27. Unlawful interference with submarine cables.
- 28. Bribery of foreign public officials.

Berdasarkan 28 kategori kejahatan internasional tersebut, M. Cherif Bassiouni⁸⁵ membagi tingkatan kejahatan internasional menjadi tiga. **Pertama**, kejahatan internasional yang disebut sebagai *international crimes* adalah bagian dari *jus cogens*⁸⁶. Tipikal dan karakter dari *international crimes* berkaitan dengan perdamaian dan keamanan manusia serta nilai-nilai kemanusiaan yang fundamental. Terdapat sebelas kejahatan yang menempati hirarki teratas sebagai *international crime*, yakni:

- 1. Aggression.
- 2. Genocide.
- 3. Crimes against humanity.
- 4. War crimes
- 5. Unlawful possession or use or emplacement of weapons.
- 6. Theft of nuclear materials.
- 7. Mercenaries.
- 8. Apartheid.
- 9. Slavery and slave-related practices.
- 10. Torture and other forms of cruel, inhuman, or degrading treatment.
- 11. Unlawful human experimentation.

Kedua, kejahatan internasional yang disebut sebagai *international delicts*. Tipikal dan karakter *international delicts* berkaitan dengan kepentingan internasional yang dilindungi meliputi lebih dari satu negara atau korban dan kerugian yang timbul berasal dari satu negara. Ada tiga belas kejahatan internasional yang termasuk dalam *international delicts*, yaitu:

⁸⁵ *Ibid*,hlm. 56

⁸⁶ *Jus Cogens* adalah hukum pemaksa yang tertinggi dan harus ditaati oleh bangsa-bangsa beradab di dunia sebagai prinsip dasar umum dalam hukum internasional yang berkaitan dengan moral. Lihat, Eddy O.S. Hiariej, *ibid*,hlm. 50.

- 1. Piracy.
- 2. Aircraft hijacking and unlawful acts against international air safety.
- 3. Unlawful acts against the safety of maritime navigation and safety of platforms on the high seas.
- 4. Threat and use of force against internationally protected person.
- 5. Crimes against United Nations and associated personnel.
- 6. Taking of civilian hostages.
- 7. Unlawful use of the mail.
- 8. Attacks with explosives.
- 9. Financing of terrorism.
- 10. Unlawful traffic in drugs and related drug offenses.
- 11. Organized crime
- 12. Destruction and/or theft of national treasures.
- 13. Unlawful acts against certain internationally protected elements of the environment.

Ketiga, kejahatan internasional yang disebut dengan istilah *international infraction*. Dalam hukum pidana internasional secara normatif, *international infraction* tidak termasuk dalam kategori *international crime* dan *international delicts*. Kejahatan yang tercakup dalam *international Infraction* hanya ada empat, yaitu:

- 1. International traffic in obscene materials.
- 2. Falsification and counterfeiting.
- 3. Unlawful interference with submarine cable.
- 4. Bribery of foreign public officials.

Uraian penggunaan istilah dan batasan pengertian kejahatan internasional, semakin memperjelas posisi kejahatan siber yang secara implisit belum dikategorikan. Oleh karena

itu, pengkualifikasian kejahatan siber harus didasarkan pada penguraian unsur-unsur kejahatan internasional agar dapat dikategorikan sebagai kejahatan internasional. Menurut Bassiouni terdapat 3 (tiga) unsur yang harus dipenuhi agar dapat dikatakan sebagai kejahatan internasional.

Unsur tersebut adalah:87

- 1. Unsur internasional termasuk didalamnya ancaman secara langsung dan tidak langsung atas perdamaian dunia dan menggoyah perasaan kemanusiaan.
- Unsur transnasional termasuk didalamnya bahwa dampak yang ditimbulkan memiliki dampak terhadap lebih dari satu negara, terhadap warga negara dari lebih satu negara, dan sarana dan prasarana serta metode yang dipergunakan melampaui batas-batas teritorial suatu negara.
- 3. Unsur kebutuhan termasuk didalamnya kebutuhan akan kerjasama antara negara-negara untuk melakukan penanggulangan.

Bertitik tolak pada uraian unsur kejahatan internasional sebagaimana yang diungkapkan oleh Bassiouni maka secara sederhana (*simple way*) kejahatan siber memenuhi keseluruhan unsur untuk dikatakan sebagai kejahatan baru dalam literatur kejahatan internasional dewasa ini.

⁸⁷ Romli Atmasasmita, Op.Cit, hlm. 58.

G. Yurisdiksi Cyberspace

Yurisdiksi cyberspace dibedakan atas:88

1. Yurisdiksi Pidana

Yurisdiksi pidana umumnya diuraikan dari segi tempat kejadian (*locus delicti*), yang berarti bahwa terdakwa melakukan seluruh atau sebagian kejahatan di lokasi geografis (terkadang disebut "forum") tempat terletaknya pengadilan. Dalam konteks ini, prinsip teritorial dapat diterapkan dengan mempertimbangkan bahwa setiap tempat dimana suatu kejahatan dilakukan dapat menjadi objek penerapan prinsip teritorial.⁸⁹

Seringkali, tempat kejadian dapat ada di forum yang berlainan. Misalnya, jika seseorang mencuri orang di Hong Kong, dan membawanya ke Bali, tempat kejadian berada di Hong Kong dan Bali karena bagian-bagian yang signifikan dari kejahatan itu dilakukan di kedua tempat. Artinya bagi kejahatan siber adalah bahwa seorang terdakwa tentu dapat dikenai sanksi pidana di hampir semua yurisdiksi dimana ada sambungan internet. Suatu pemerintah dapat memiliki kelonggaran yang luas untuk memutuskan dimana untuk menuntut pelaku kejahatan *online* karena kejahatan dapat dilakukan dimana terdakwa berada, dimana korban berada, dan semua yurisdiksi yang secara elektronik telah terkena tindakan terdakwa.

Dengan kata lain, dalam kejahatan siber, terdakwa seringkali berada di lokasi fisik yang sama dengan korban. Itu membuat tempat kejadian (dari yurisdiksi pidana) relatif mudah ditentukan. Tetapi di ruang maya, seorang pelaku

⁸⁸ Diekstraksi dari Maskun, op.cit., hlm. 107-113.

⁸⁹ Henrik W.K. Kaspersen, Cybercrime and Internet Jurisdiction (Discussion Paper), (Netherland: Council of Europe, 2009), hlm. 9.

kejahatan tidak lagi perlu berada di tempat kejadian perkara yang sebenarnya. Sebuah server komputer di Thailand dapat mengelola sebuah halaman website yang menipu masyarakat dan korbannya mungkin tersebar di seluruh dunia. Seorang penyedia pornografi anak-anak dapat mendistribusikan fotofoto melalui *e-mail* yang berjalan melewati jaringan-jaringan komunikasi di berbagai negara sebelum mencapai si penerima ponografi tersebut. Seorang pengintip syber (*cyberstalker*) di Denpasar dapat mengirimkan *email* ke seseorang di Jakarta.

Meskipun demikian, pada kenyataannya, prinsip-prinsip hukum tradisional dapat diterapkan di internet. Sekalipun sambungannya berdurasi singkat, secara fisik komputer tetap terletak di tempat tertentu, terdakwa memulai kejahatan dari tempat tertentu, dan korban berada di tempat tertentu. Tentunya, yang menjadi tantangan adalah mengidentifikasi lokasi tersebut.

Disampingpenerapanprinsipteritorial, prinsipperlindungan juga diterapkan dengan mempertimbangkan bahwa prinsip teritorial tidak menyiapkan basis yurisdiksi dimana secara utuh bahwa tindak pidana dilakukan di luar wilayah teritorial negara pelaku. Fokus penerapan prinsip perlindungan adalah aktivitas pelaku yang mengancam secara serius kepentingan nasional. Meskipun dalam konteks ini, prinsip perlindungan belum menentukan secara pasti suatu interpretasi atas apa yang dimaksud dengan kepentingan nasional. Sehingga dapat disimpulkan bahwa prinsip perlindungan ini hanya diterapkan untuk jenis kejahatan khusus.

2. Yurisdiksi Perdata

Pemikiran-pemikiran tradisional atas yurisdiksi didasarkan pada geografi dan kontak fisik yang dimiliki terdakwa dengan

forum (baik secara langsung atau dengan jalan mengirimkan produk). Tetapi internet memungkinkan adanya peluang untuk "kontak virtual". Mengingat sifat kontak di internet, kontak seorang terdakwa dengan forum mungkin seluruhnya bersifat online, dan kontak fisiknya dengan forum mungkin tidak ada. Yurisdiksi diri atas seorang pengguna internet yang hanya memiliki kontak online dengan forum akan didasarkan pada sifat kontak tersebut.

Berdasarkan uji kontak minimum tradisional, perolehan keuangan menunjukkan bahwa seorang terdakwa telah mendapatkan manfaat dari forum. Jika seorang pengguna internet menghasilkan uang di forum, ini mungkin merupakan indikasi bahwa pengguna hendaknya dikenai tuntutan di forum tersebut. Tetapi perbuatan di internet seringkali tidak terarah ke forum. Terutama jika produk tersebut di-download langsung, misalnya perangkat lunak atau musik, si penjual tidak mengetahui lokasi fisik pembeli. Jasa-jasa informasi lainnya dapat ditawarkan sepenuhnya online, misalnya pemantauan sistem, pendidikan, pengolahan data dan konsultasi. Pembayaran lewat kartu kredit dapat mengungkapkan identitas seorang pelanggan, tetapi bukan lokasinya. Pembayaran dengan "uang tunai digital" bahkan lebih sulit lagi dilacak.

Demikian pula, perbuatan lain yang tidak diarahkan untuk menghasilkan uang dapat dikenai gugatan, sebagai contoh komunikasi pribadi dan kelompok diskusi dapat memunculkan gugatan kerugian, misalnya pencemaran nama baik atau fitnah. Sesuatu yang sulit pula melihat bagaimana pemakaian tertentu internet dipandang sebagai "pemanfaatan keuntungan dari forum", sebagai contoh, meskipun seorang pemakai mungkin meminta informasi dari sebuah komputer induk di forum, si pemakai biasanya tidak tahu dan tidak peduli dimana komputer

induk tersebut berada. Demikian pula, bila suatu usaha internet tidak mengetahui lokasi pembeli produk download-annya. Sulit menyimpulkan bahwa bisnis itu hendaknya mengantisipasi diseret di pengadilan di forum si pembeli.

Beberapa prinsip sudah jelas. Pada umumnya, pengadilan akan menengok halaman website tersebut dan kontaknya dengan forum. Jika halaman website itu sekedar mencantumkan informasi, kecil kemungkinan bahwa yurisdiksi akan ada dalam suatu forum (kecuali dimana si pembuat halaman Web tinggal). Di lain pihak, penawaran usaha yang berulang-ulang dari forum dapat menerapkan yurisdiksi, seperti halnya transmisi informasi iklan. Intinya adalah, jika sebuah perusahaan membuat situs yang mengandung lebih dari informasi pasif mengenai produk atau jasa-jasanya, perusahaan tersebut mengandung resiko terkena yurisdiksi forum dimana produk-produknya dikirim.

BAB III

KEJAHATAN AGRESI

A. Sejarah Pengertian Kejahatan Agresi

Pengertian mengenai agresi memang sangat krusial dan kompleks serta banyak mengundang penafsiran yang berbedabeda dari banyak negara khususnya dari para ahli hukum internasional. Pada dasarnya dugaan tindakan agresi telah terjadi dalam konflik bersenjata sejak beberapa abad yang lalu. Pakan tetapi hukum internasional tidak secara tegas melarang negara-negara untuk melakukan agresi hingga kesimpulan dari *Kellogg-Briand Peace Pact* tahun 1928. Meskipun demikian dalam *Pact* sendiri belum memberikan definisi secara tegas. Suatu proposal definisi kejahatan agresi pernah diajukan pada tahun 1933, oleh Uni Soviet ketika *Conference Disarmament (Konferensi Pelucutan senjata)*.

⁹⁰ Lihat Robert L. O'Connell, Of Arms and Men: A History of War, Weapons, and Aggression, (1989) in Michael J. Glennon, *the Blank-Prose crime of Aggression*, the Yale J. of Int'l Law, Vol. 35:71, (2010), hlm.72.

⁹¹ Lihat General Treaty for Renunciation of Wars as an Instruments of National Policy Art. I Aug 27, 1928, 46 Stat.2343, 94 L.N.T.S. 57 (hereinafter Treaty for Renunciation of War).

⁹² Michael J. Glennon, *the Blank-Prose crime of Aggression*, the Yale J. of Int'l Law, Vol. 35:71, (2010), hlm.73.

⁹³ Lihat Mattias Schuster, the Rome Statute and the Crime of Aggression: A Gordian Knot in Search of a Sword, 14 Crim. L.F. 1, 4 (2003).

Konvensi yang dibuat atas prakarsa Uni Soviet merumuskan laporannya kepada Komite Keamanan pada tanggal 24 Mei 1933 termasuk sebuah rancangan konvensi beserta protokolnya, dimana Uni Soviet pada waktu itu merekomendasikan kepada negara-negara tetangganya dan mereka telah menandatanganinya pada tanggal 3 Juli 1933.94 Rancangan definisi yang diajukan Uni Soviet dapat dilihat rumusannya pada antara lain bagi negara yang pertama akan melibatkan tindakan-tindakan seperti:

- a) Pernyataan perang terhadap negara lain;
- b) Melakukan invasi dengan kekuatan senjata, bahkan sekalipun tanpa adanya perang terhadap wilayah suatu negara;
- c) serangan melalui darat, laut dan udara terhadap wilayah, kapal laut dan kapal terbang negara lain;
- d) Melakukan *blockade* laut di pantai atau pelabuhan negara lain;
- e) Pemberian bantuan kepada gerombolan bersenjata yang dibentuk di wilayah suatu negara dan menduduki wilayah negara lain.

Usai konferensi yang digagas Uni Soviet, upaya pendefinisian agresi yang baku terus dilakukan oleh para ahli, termasuk didalamnya merumuskan definisi kejahatan agresi seusai Perang Dunia II ketika Pengadilan Tribunal Nuremberg merumuskan kejahatan agresi, ketika itu dikenal dengan sebutan kejahatan terhadap perdamaian, sebagai "planning, preparation, initiation or waging of a war of aggression, or a war in violation of international treaties, agreement or assurances,

⁹⁴ Sumaryo Suryokusumo, Organisasi Internasional, (Jakarta: Penerbit Universitas Indonesia, 1987), hlm 26.

or participation in a common plan or conspiracy for the accomplishment of any foregoing".95

Rumusan kejahatan agresi yang dihasilkan dalam Pengadilan Tribunal Nuremberg telah menjadi acuan bagi negara-negara. Tentunya definisi dimaksud membutuhkan penyempurnaan. Selanjutnya, PBB melalui Komite Khusus yang dibentuk merumuskan definisi agresi dan telah menyampaikan rancangan definisi tersebut yang terdiri dari 8 Pasal kepada Majelis Umum PBB pada bulan April 1974. Dalam hal ini, mengeluarkan Resolusi Majelis Umum PBB Nomor 3314 (XXIX) 14 Desember 1974 yang dipandang sebagai keputusan hukum dalam konteks hukum yang tidak perlu diragukan lagi. Se

Berdasarkan Pasal 1 Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974, disebutkan bahwa:

"Agresi adalah penggunaan pasukan bersenjata oleh suatu negara terhadap kedaulatan, keutuhan wilayah atau kemerdekaan politik dari negara lain atau dengan cara-cara lain apa pun yang bertentangan dengan piagam PBB seperti tersebut dalam definisi ini".

Perumusan istilah ini, tidak lagi mempersoalkan masalah pengakuan atau apakah negara itu merupakan anggota PBB atau tidak. Di samping itu, negara diartikan termasuk pula sebagai konsep "kelompok negara", sedangkan ketiga unsur

⁹⁵ Michael J. Glennon, op.cit., hlm. 74.

⁹⁶ Antonio Cassese, *On Some Problematical Aspects of the Crime of Aggression*, Leiden JIL, 20, (2007), hlm. 842.

⁹⁷ Sumaryo Suryokusumo, op.cit., hlm.26.

⁹⁸ M. Cherif Bassiouni, Historical development of Prosecuting Crimes Against Peace, in M. Cherif Bassiouni, International Criminal Law, Vol. III Enforcement, (New York: Transnational Publishers Inc, 1987), hlm. 27.

yang digunakan seperti kedaulatan, keutuhan wilayah dan kemerdekaan ketiganya merupakan atribut pokok (*an essential attribute*) dari suatu negara sebagai subjek hukum internasional yang merupakan kesatuan yang bersifat integratif.⁹⁹

Pasal 2 Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974 mengenai penggunaan pasukan bersenjata yang pertama oleh sesuatu negara, yang tidak sesuai dengan piagam PBB, akan merupakan bukti dari suatu tindak agresi, meskipun Dewan Keamanan PBB menurut Piagam PBB dapat menentukan bahwa sesuatu tindak agresi yang telah dilakukan tidak akan dibenarkan.¹⁰⁰

Sebagaimana yang dinyatakan dalam Pasal 3 Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974, tindakan-tindakan yang harus dianggap sebagai tindak agresi tanpa memandang adanya pernyataan perang, adalah tindakan-tindakan sebagai berikut:¹⁰¹

- Invasi atau serangan yang dilakukan oleh pasukan bersenjata dari suatu negara terhadap wilayah negara lainnya atau sebagian dari wilayah itu;
- 2. Pemboman oleh pasukan bersenjata dari suatu negara terhadap wilayah negara lain atau penggunaan senjata apapun oleh suatu negara terhadap wilayah negara lain;
- 3. Blokade di pelabuhan atau pantai dari sesuatu negara oleh pasukan bersenjata dari negara lain;

⁹⁹ Sumaryo Suryokusumo, op.cit., hlm. 26.

¹⁰⁰ Ibid

¹⁰¹ Lihat: Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974

- 4. Suatu serangan oleh pasukan bersenjata dari suatu negara dengan angkatan darat, laut, dan udara di lapangan terbang dari negara lain;
- 5. Penggunaan pasukan bersenjata dari suatu negara yang berada di wilayah negara lain, dengan persetujuan dari negara penerima, yang tidak sesuai dengan kondisi yang dinyatakan dalam persetujuan tersebut atau setiap perluasan dari kehadirannya di wilayah itu yang tidak sesuai dengan persetujuan tersebut;
- 6. Tindakan dari suatu negara untuk mengizinkan di wilayahnya atas perintah dari negara lain, digunakan oleh negara lainnya untuk melakukan suatu tindak agresi terhadap negara ketiga;
- 7. Pengiriman oleh atau atas nama suatu negara, kelompok gerombolan bersenjata, pasukan sewaan yang melakukan tindakan-tindakan dengan kekuatan senjata terhadap negara lain dengan suatu gravitasi agar dapat memperkuat tindakan-tindakan seperti tersebut di atas atau keterlibatannya secara substansial di dalamnya.

Pasal 4 Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974 menyatakan bahwa "Tindakan-tindakan yang telah diuraikan di atas belum berarti mencakup keseluruhannya dan Dewan Keamanan PBB dapat saja menentukan bahwa tindakan-tindakan lainnya sesuai dengan ketentuan Piagam PBB". Adapun pasal 5 Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974 menyatakan bahwa:

"Tidak ada pertimbangan mengenai sifat apapun baik politik, ekonomi, militer atau lainnya yang dapat dijadikan sebagai pembenaran mengenai agresi. Perang agresi

merupakan kejahatan terhadap perdamaian dunia. Agresi tersebut mengakibatkan tanggung jawab internasional dan tidak ada perolehan wilayah atau keuntungan khusus sebagai hasil dari agresi itu akan diakui secara sah".

Pasal 7 Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974 mengatur tentang:

"Tidak ada dalam definisi ini, khususnya pasal 13 bagaimanapun juga yang dapat merugikan hak penentuan nasib sendiri, kebebasan dan kemerdekaan, sebagaimana tersebut dalam piagam PBB, menghilangkan hak bangsabangsa tersebut dengan paksa sebagaimana tersebut juga dalam deklarasi mengenai prinsip-prinsip hukum internasional yang mengatur hubungan bersahabat dan kerja sama antara bangsa-bangsa sesuai dengan Piagam PBB, khususnya bangsa-bangsa yang berada dibawah penjajahan dan rezim rasis ataupun bentuk-bentuk dominasi asing lainnya, ataupun hak dari bangsa-bangsa tersebut untuk mencari dan menerima bantuan sesuai dengan prinsip-prinsip piagam dan Deklarasi tersebut".

Rumusan agresi pada akhirnya dapat disetujui dengan aklamasi oleh Majelis Umum PBB dalam sidangnya tertanggal 14 Desember 1974 yang menghasilkan Resolusi 3314 (XXIX) Majelis Umum PBB 14 Desember 1974, walaupun masih ada anggapan bahwa definisi itu tidak sempurna dan kurang lengkap sehingga dapat menimbulkan banyak penafsiran. Hal terpenting adalah bagaimana PBB dapat menjamin bahwa tindak agresi itu tidak akan dilakukan terhadap suatu negara atau bangsa; dan bagaimana PBB dapat menjamin hukuman

dari negara yang telah melanggar perdamaian, mengancam perdamaian dan melakukan tindak agresi. 102

Pertanyaan lain yang timbul dari definisi agresi dalam Resolusi Majelis Umum PBB 3314, yang menimbulkan keraguan akan definisi dimaksud adalah tidak disebutkannya secara tegas pertanggungjawaban individu dan negara dalam kejahatan agresi. Hal ini dikarenakan Resolusi Majelis Umum PBB 3314 membedakan tindakan agresi yang menciptakan tanggung jawab internasional dan agresi perang yang ditujukan sebagai kejahatan melawan perdamaian. Dalam hal ini Resolusi Majelis Umum PBB 3314 mengabaikan lahirnya pertanggungjawaban individu dalam *act of aggression*. 104

Hal lain yang dipersoalkan oleh para ahli bahwa rumusan agresi yang ternyata hanya ditetapkan dengan Resolusi Majelis Umum PBB 3314 sehingga kekuatan hukumnya sangat disangsikan karena keputusan Majelis Umum hanya bersifat *externa corporis*, suatu keputusan yang hanya bersifat rekomendatif dan kurang mempunyai kekuatan hukum yang mengikat tidak sebagaimana keputusan Dewan Keamanan.

Kritikan yang muncul terhadap Resolusi Majelis Umum PBB 3314, memunculkan upaya dari Komisi Hukum Internasional PBB untuk merumuskan definisi kejahatan agresi dengan memformulasi prinsip-prinsip Nuremberg ke dalam bentuk Kode Draf Kejahatan Melawan Perdamaian pada tahun 1996. Dalam hal ini Komisi Hukum Internasional mengutip prinsip Nuremberg

¹⁰² Quency Right, The Preventive Of Aggressions, AJIL, Vol.50, (1956), hlm 514.

¹⁰³ Antonio Cassese, op.cit. hlm. 862.

¹⁰⁴ Major Karl M. Fletcher, *Defining the Crime of Aggression : Is There an Answer to the International Criminal Court's Dilemma*, Air Force Law Review, 65, (2010), hlm. 238.

dan Piagam PBB yang dasar pijakan atas pertanggungjawaban individu, akan tetapi bukan definisi Resolusi Majelis Umum PBB 3314.¹⁰⁵ Upaya pendefinisian kejahatan agresi dalam Draf Kejahatan Melawan Perdamaian pada tahun 1996, juga belum menemukan rumusan baku karena seusai Perang Dunia II tidak ada suatu peradilan yang dilakukan untuk mengadili suatu negara atas dugaan kejahatan agresi. Dewan Keamanan PBB lebih memilih menciptakan Tribunal untuk menyelesaikan kejahatan-kejahatan yang terjadi di Rwanda dan Yugoslavia. Tribunal yang dibentuk tidak memasukkan kejahatan agresi sebagai salah satu kejahatan mandat dimana dugaan kejahatan agresi terjadi di Rwanda dan Yugoslavia.¹⁰⁶

Harapan untuk menyempurnakan definisi kejahatan agresi terus diupayakan melalui *International Criminal Court* (ICC) yang disahkan pada tahun 1998 dimana salah satu yurisdiksi ICC adalah kejahatan agresi. Pasal 5 ICC menyebutkan bahwa "Yurisdiksi dari Mahkamah harus dibatasi hanya terhadap tindak pidana yang oleh keseluruhan masyarakat internasional dianggap paling serius. Mahkamah memiliki yurisdiksi dalam kaitannya dengan statuta ini dalam hal kejahatan sebagai berikut:

- a. Tindak Pidana Genocide (pembunuhan massal);
- b. Kejahatan terhadap kemanusiaan;
- c. Kejahatan Perang;
- d. Kejahatan agresi

lbid. hlm. 239. Lihat juga Antonio Cassese, op.cit. hlm. 862. Pasal 16 Kode Draf Kejahatan Melawan Perdamaian menyebutkan bahwa "an individual who as leader or organizer actively participates in orders the planning, preparation, initiation or waging of aggression committed by a state, shall be responsible for a crime of aggression". (UN Doc.A/51/332). Lihat juga M. Cherif Bassiouni and Benjamen Ferencz, *the Crime Against Peace in International Criminal Law*, 313, 316, (1999).

¹⁰⁶ Major Karl M. Fletcher, op.cit. hlm. 240.

Pasal 5 ayat (2) lebih lanjut menyatakan bahwa "Mahkamah melaksanakan yurisdiksi atas kejahatan agresi setelah ketentuan disahkan sesuai dengan pasal 121 dan 123 yang mendefinisikan kejahatan dan menetapkan kondisi-kondisi di mana Mahkamah menjalankan yurisdiksi berkenaan dengan kejahatan ini. Ketentuan semacam itu haruslah sesuai dengan ketentuan terkait dari Piagam Perserikatan Bangsa-Bangsa".

Definisi yang sebagaimana dalam Pasal 5 ICC, sangat sulit untuk diwujudkan. Hal kemudian memunculkan upaya untuk melakukan amandemen terhadap Pasal 5 ayat (2) ICC. Untuk memuluskan hal tersebut, dibentuklah *Special Working Group on the Crime of Aggression* (SWGCA) yang diberikan mandat untuk menyiapkan proposal tentang kejahatan agresi. Upaya yang panjang dan berliku akhirnya membuahkan hasil, *SWGCA Review Conference*, sejak 2002-2010, dengan dirumuskannya suaru definisi kejahatan agresi. Rumusan definisi tersebut adalah "planning, preparation, initiation or execution, by a person in position actively to exercise control over or to direct the political or military action of a state, of act of aggression."

Sekilas definisi dihasilkan dalam SWGCA yang Conference telah mengakomodasi seluruh keinginan berbagai pihak yang telah bergulir selama ini tentang definisi kejahatan agresi. Meskipun demikian perdebatan masih terus bergulir khususnya berkenaan dengan yurisdiksi pengadilan. Pasal 121 ayat 5 ICC menyebutkan bahwa amandemen terhadap Pasal 5, 6, 7, dan 8 ICC diberlakukan terhadap negara-negara anggota setelah amandemen tersebut diterima oleh negara-negara tersebut satu tahun setelah didepositkan baik dalam bentuk ratifikasi atau penerimaan. Dalam hal negara-negara belum atau tidak menerima amandemen dimaksud maka pengadilan

tidak dapat menggunakan yurisdiksinya terhadap kejahatan yang menjadi lingkup yurisdiksinya.¹⁰⁷

B. Elemen Agresi

Pada dasarnya elemen agresi terbagi atas:

1. Elemen Objektif

Pada umumnya, hukum kebiasaan internasional pada dasarnya melarang segala bentuk tindakan agresi baik dalam konteks tindakan internasional yang salah (*international wrongful acts*) maupun tindakan kriminal (*criminal acts*) ataupun kombinasi keduanya. Tindakan agresi dimaksud merujuk pada definisi Resolusi Majelis Umum PBB 3314 tahun 1974. Dalam hal ini, elemen objektif yang dimaksud didasarkan pada definisi Resolusi Majelis Umum PBB 3314, sebagai berikut:

- a. Invasi atau serangan yang dilakukan oleh pasukan bersenjata dari suatu negara terhadap wilayah negara lainnya atau sebagian dari wilayah itu;
- b. Pemboman oleh pasukan bersenjata dari suatu negara terhadap wilayah negara lain atau penggunaan senjata apapun oleh suatu negara terhadap wilayah negara lain;
- c. Blokade di pelabuhan atau pantai dari sesuatu negara oleh pasukan bersenjata dari negara lain;

¹⁰⁷ Kriangsak Kittichaisaree, International Criminal Law, (New York: Oxford University Press, 2002), hlm. 420.

¹⁰⁸ Antonio Cassese, op.cit., hlm.847.

- d. Suatu serangan oleh pasukan bersenjata dari suatu negara dengan angkatan darat, laut, dan udara, di lapangan terbang dari negara lain;
- e. Penggunaan pasukan bersenjata dari suatu negara yang berada di wilayah negara lain, dengan persetujuan dari negara penerima, yang tidak sesuai dengan kondisi yang dinyatakan dalam persetujuan tersebut atau setiap perluasan dari kehadirannya di wilayah itu yang tidak sesuai dengan persetujuan tersebut.
- f. Tindakan dari suatu negara untuk mengizinkan di wilayahnya atas perintah dari negara lain, digunakan oleh negara lainnya untuk melakukan suatu tindak agresi terhadap negara ketiga;
- g. Pengiriman oleh atau atas nama suatu negara, kelompok gerombolan bersenjata, pasukan sewaan yang melakukan tindakan-tindakan dengan kekuatan senjata terhadap negara lain dengan suatu gravitasi agar dapat memperkuat tindakan-tindakan seperti tersebut di atas atau keterlibatannya secara substansial di dalamnya.

Hukum kebiasaan internasional tampak mempertimbangkan agresi sebagai kejahatan internasional dalam artian adanya perencanaan atau organisasi, atau persiapan, atau partisipasi dalam penggunaan pertama kekuatan bersenjata yang dilakukan oleh suatu negara atau organisasi non-negara atau entitas lain yang melanggar kedaulatan dan kemerdekaan politik negara lain serta bertentangan dengan Piagam PBB, yang dilakukan dalam skala besar dan berdampak serius.¹⁰⁹

109 Ibid.

Hukum kebiasaan internasional meletakkan pertanggungjawaban tindakan agresi dimaksud pada negara. Contoh agresi dimaksud yakni agresi Israel ke Irak pada tahun 1981 yang merupakan suatu pelanggaran penggunaan kekuatan bersenjata. Dalam hal ini, pertanggungjawaban tidak diletakkan pada individu meskipun faktanya bahwa tindakan agresi yang dilakukan merupakan tindakan kolektif individuindividu.

2. Elemen Subjektif

Elemen subjektif dalam kejahatan agresi diletakkan pada maksud dari kejahatan (*criminal intent*). *Intent* harus ditunjukkan pelaku dalam bentuk partisipasi dalam perencanaan dan peperangan. *Intent* harus didasarkan pada kesadaran mengenai lingkup kejahatan, signifikansi dan konsekuensi dari tindakan agresi yang diambil. Dalam hal ini, pertanggungjawaban yang dapat timbul bukan hanya diletakkan pada negara, akan tetapi dapat pula melibatkan seorang pimpinan militer atau petugas resmi negara atau bahkan seorang individu jika mereka mengetahui (*knowledge*) rencana dilaksanakan suatu kejahatan agresi. Dalam konteks ini, dapat dilihat pada pengadilan kejahatan perang sebelum Tribunal Militer Internasional, Nuremberg.

Sehingga dapat dikatakan bahwa suatu kejahatan agresi harus memiliki maksud khusus (*special intent*) untuk mencapai keuntungan teritorial dan atau untuk memperoleh keuntungan ekonomi atau secara langsung melakukan intervensi terhadap urusan dalam negeri negara lain. Penerapan *special intent* dapat dilihat pada perjanjian Paris tentang Penolakan Perang 27 Agustus 1928 (*the General Treaty of Paris for the Renunciation*

¹¹⁰ Ibid, hlm. 848

of War - called Kellogg-Briand Pact). 111

Dalam hubungannya dengan ICC, Pasal 30 ICC mengenal pula elemen subjektif dengan sebutan "Elemen Mental". Elemen Mental yang dimaksudkan dalam pasal ini bahwa seseorang harus bertanggung jawab atas kejahatan dalam yurisdiksi pengadilan jika elemen material dilakukan dengan *intent* dan *knowledge. Intent* disini diartikan dalam hubungan dengan melakukan (*conduct*), dan konsekuensi (pelaku mengetahui sebab yang ditimbulkan). Di sini *knowledge* diartikan sebagai sebuah kesadaran bahwa kejahatan tersebut dalam kondisi yang ada atau suatu konsekuensi akan timbul dari dilakukannya kejahatan tersebut.¹¹²

Conduct pada dasarnya merujuk pada tindakan kejahatan dan consequence merupakan hasil dari conduct. Akan tetapi pada kenyataanya kedua unsur pada elemen subjektif atau elemen material sering tumpang-tindih. Apabila conduct dan consequence dapat diartikan dengan jelas maka tidak halnya dengan circumstances. Dalam hal ini, circumstances agak sulit untuk didefinisikan, termasuk bagi mereka yang terlibat dalam draf Pasal 30 ICC ketika pembuatan ICC. Circumstances disini lebih dikonotasikan "know it when we see it". Artinya diketahui ketika kejahatan agresi terjadi. 113

Circumstances merupakan faktor hukum yang penting dalam lingkungan dimana pelaku melakukan tindak kejahatan termasuk didalamnya kejahatan agresi. Sehingga dalam pengembangan circumstances dalam Pasal 30 ICC merupakan contextual circumstances (keadaan yang kontekstual).

¹¹¹ Ibid.

¹¹² Roger S. Clark, op.cit. hlm. 863.

¹¹³ Ibid, hlm. 867

BABIV

ARTIKULASI ANTARA KEJAHATAN SIBER DAN KEJAHATAN AGRESI

A. Konsep Hukum Internasional Kontemporer

Hukum internasional adalah bidang hukum yang merupakan integrasi antara sistem hukum yang berbeda dari berbagai negara. Integrasi dimaksud menunjukkan perspektif bahwa hukum internasional secara esensial merupakan kerjasama antara negara. Dalam pendekatan hukum (*legal approaches*), aturan hukum internasional tidak dapat dilindungi dan dipromosikan secara individu, akan tetapi harus diupayakan secara bersama-sama.

Perkembangan hukum internasional yang terjadi dewasa ini telah dipengaruhi berbagai varian isu seperti perdagangan internasional, hak asasi manusia, demokrasi, kemiskinan, konservasi lingkungan, dan ancaman terhadap perdamaian dan keamanan. Perkembangan selanjutnya menunjukkan bahwa ragam isu-isu tersebut mengalami interaksi satu sama lainnya.

¹¹⁴ Magdalena Petronella Ferreira-Synman, the Erosion of State Sovereignty in Public International Law: Towards a World Law?, (Doctor Legum, University of Johannesburg, 2009), hlm. 1.

Interaksiantaraberbagai varian isu-isu hukum internasional yang telah mengalami perkembangan yang begitu pesat seiring dengan perkembangan zaman, melahirkan pengistilahan hukum internasional kontemporer. Frasa kontemporer yang digunakan menunjukkan kekinian, kemutakhiran, atau modern. Dalam hal ini, hukum internasional kontemporer yang dikenal saat ini sesungguhnya telah menyatu dengan kehidupan bangsa-bangsa di dunia yang dalam prakteknya cakupan dan kedalaman maknanya belum pernah terjadi sebelumnya.

Perkembangan dimaksud tentunya tidak dapat dipisahkan dengan peristiwa yang terjadi di masa lampau, sebagai contoh pelanggaran terhadap perdamaian, pembajakan, perompakan di laut, perang, dan hak asasi manusia. Dalam konteks ini, proses transformasi hukum internasional saat ini dan yang akan datang tentunya harus dimulai dengan memahami hukum internasional tradisional (*the old-fashion of international law*) secara menyeluruh termasuk didalamnya kompleksitas yang melatarbelakangi hukum internasional tradisional tersebut.¹¹⁵

Kelas kapitalis transnasional misalnya merupakan fraksi transnasional dari kelas kapitalis nasional yang berusaha untuk menyatukan pasar dunia melalui instrumen internasional law. Para kapitalis transnasional memandang bahwa produksi merupakan unifikasi ruang ekonomi global yang dalam konteks sejarah sangat banyak terjadi. Contoh konkrit dari

¹¹⁵ B.S. Chimni, *the past, Present and Future of International Law : a Critical Third world Approach,* Melbourne of International Law Journal, Vol. 8 (2007), hlm. 500.

¹¹⁶ William Robinson and Jerry Harris, *Towards a Global Ruling Class? Globalization and the Transnational Capitalist Class*, Science and Society, Vol. 64 (2000), hlm 11; Leslie Sklair, *The Transnational Capitalist Class* (2001); B S Chimni, *An Outline of a Marxist Course on Public International Law*, Leiden Journal of International Law, Vol. 17 (2004), hlm. 1.

praktek tersebut dapat dilihat pada kaum borjuis di Eropa yang melakukan proses produksi ekonomi nasional negara-negara Eropa pada abad 18 dan 19.¹¹⁷ Dalam mewujudkan tujuan dimaksud, kapitalis transnasional memanfaatkan bantuan hukum internasional, dengan cara memproduksi sebuah kaidah dan norma hukum internasional baru yang tetap berlaku bagi mereka.

Praktek-praktek kapitalis transnasional sebagaimana dijelaskan di atas, sesungguhnya mengungkapkan ketidakmampuan untuk menangani penyebaran globalisasi yang sementara terjadi, yang dalam sudut pandang mereka dipandang sebagai bentuk keterasingan; dan efek dari hubungan sosial yang tidak manusiawi yang sesungguhnya mendasari hubungan internasional kontemporer. Dalam Manuskrip Ekonomi dan Filosofis Karl Marx, ia menyebutkan empat jenis keterasingan, yaitu:

- 1. keterasingan manusia dari alam;
- 2. keterasingan manusia dari kegiatan produktivitas mereka sendiri;
- 3. keterasingan manusia dari kebiasaan yang mereka miliki; dan
- 4. keterasingan manusia dari manusia lainnya

Bentuk keterasingan sebagaimana disebutkan Karl Marx menggambarkan ketidakadilan yang menandai lahirnya badanbadan atau institusi-institusi hukum internasional modern, yang

¹¹⁷ Gary Teeple, *Globalization as the Triumph of Capitalism: Private Property, Economic Justice and the New World Order* in Ted Schrecker (ed), Surviving Globalism: The Social and Environmental Challenges (1997) 15, hlm. 15–16.

¹¹⁸ Lihat Karl Marx, *Economic and Philosophic Manuscripts of 1844* (1959).

berefek pada lahir isu-isu lingkungan global, hak asasi manusia, dan informasi-teknologi.

Lingkungan merupakan salah satu permasalahan yang mendera dunia saat ini. Sejak berkembangnya industri sampai dengan saat ini, berbagai permasalahan lingkungan seakan tidak pernah surut. Lebih jauh, selain disebabkan oleh faktor alam, pembangunan yang dilakukan oleh manusia juga telah memberikan kontribusi negatif bagi kemerosotan lingkungan hidup. Terlepas dari itu manusia sebagai makhluk yang paling mempunyai kemampuan mempengaruhi lingkungan, dengan akal pikiran yang dimiliki, manusia mampu membuat lingkungan disekitarnya menjadi tempat yang sehat dan nyaman untuk melangsungkan hidup, ataupun sebaliknya dengan akal pikiran yang dimiliki hanya dengan hitungan detik manusia dapat menghancurkan semuanya. Perspektif konvensional, yang memposisikan pola pikir manusia sebagai makhluk yang paling mempunyai hak terhadap alam, menyebabkan manusia terus mengeksploitasi lingkungan tanpa batas demi menunjang kebutuhan hidupnya. Sehingga, disadari atau tidak perbuatan manusia tersebut menyebabkan komponen-komponen penting bagi ekosistem menjadi hilang, dan stabilitas dari lingkungan menjadi terganggu.

Kondisi objektif sebagaimana diuraikan di atas. menunjukkan disfungsional antara alam dan manusia. manusia dan alam saling berhadap-hadapan yang tentunya membawa efek bagi keduanya. Alam semakin rusak dan rusaknya alam tersebut mengakibatkan ancaman bagi eksistensi manusia dipermukaan bumi. Sebagai contoh, pencemaran perusakan lingkungan yang telah terjadi secara global. Secara periodik pencemaran dan perusakan lingkungan dimaksud

telah mengancam kelestarian dan keanekaragaman hayati yang ada di dunia.

Dampak yang ditimbulkannya pun menyebabkan makhluk yang ada di ekosistem baik darat maupun laut menjadi berkurang ataupun punah. Hal ini memicu ketidakseimbangan alam dalam menjaga daya dukung lingkungan bagi keberlanjutan kehidupan manusia dan makhluk lainnya. Penyebab dari terancamnya kelestarian dan keanekaragaman hayati tentunya tidak terlepas dari tindakan manusia, seperti adanya perburuan liar, perusakan hutan, penggunaan pestisida dan pupuk secara berlebihan, pembuangan bahan berbahaya beracun langsung ke alam dan masih banyak perbuatan manusia yang tidak bertanggung jawab lainnya yang secara langsung maupun tidak langsung berkontribusi terhadap kerusakan keanekaragaman hayati.

Informasi dan teknologi merupakan isu lain, selain isu perdagangan dan lingkungan, yang berkembang pesat saat ini yang membutuhkan pengaturan yang lebih detail.Kehadiran teknologi canggih komputer dengan jaringan internet disadari telah membawa manfaat besar bagi manusia. Pemanfaatannya tidak saja dalam pemerintahan, dunia swasta/perusahaan, akan tetapi sudah menjangkau pada seluruh sektor kehidupan termasuk segala keperluan rumah tangga (pribadi). Komputer (internet) telah mampu membuka cakrawala baru dalam kehidupan manusia baik dalam konteks sarana komunikasi dan informasi yang menjanjikan menembus batas-batas negara maupun penyebaran dan pertukaran ilmu pengetahuan dan gagasan di kalangan ilmuwan di seluruh dunia.¹¹⁹

Akan tetapi, kemajuan teknologi informasi (internet) dan segala bentuk manfaat didalamnya membawa konsekuensi

¹¹⁹ Widyopramono Hadi Widjojo, op.cit., hlm. 7.

negatif tersendiri dimana semakin mudahnya para pelaku kejahatan untuk melakukan aksinya yang semakin meresahkan masyarakat. Penyalahgunaan yang terjadi dalam *cyberspace* inilah yang kemudian dikenal dengan kejahatan siber (*cyber crime*) atau dalam literatur lain digunakan istilah kejahatan komputer (*computer crime*).

Interaksi kejahatan siber dan hukum internasional telah menempatkan kejahatan siber sebagai salah satu varian hukum internasional kontemporer. Makna kekinian yang melekat pada kejahatan siber sebagai konsekuensi perkembangan hukum internasional, khususnya hukum kejahatan internasional juga telah memperluas cakupan (*expand*) dan lingkup hukum kejahatan internasional. Hal ini dapat dibuktikan dengan melihat pada jenis kejahatan internasional yang dalam konteks sejarah belum mengkualifikasi kejahatan siber sebagai salah satu jenis kejahatan internasional.

Konsekuensi lain yang ditimbulkan dari perkembangan hukum internasional mengharuskan dirumuskannya instrumen hukum internasional baru, termasuk didalamnya dalam konteks antara dunia maya dan agresi. Kedua varian inipun dalam perkembangannya telah berintegrasi dan menjadi ancaman serius bagi perdamaian dan keamanan jika kemudian perkembangan varian ini salah diterapkan. Contoh pembuatan dan pengembangan virus stuxnet yang menyerang instalasi fasilitas nuklir Iran adalah bukti yang tak dapat dielakkan.

B. Teori yang Relevan dengan Korelasi Kejahatan Siber dan Kejahatan Agresi

Dalam rangka menghubungkan mayantara dan agresi dalam koridor kejahatan maka dibutuhkan landasan teori yang berbasis pada teori, prinsip, dan asas-asas hukum internasional. Secara garis besarnya teori, prinsip, dan asasasas hukum internasional yang relevan untuk dipergunakan dalam menggambarkan hubungan kejahatan siber dan kejahatan agresi, yaitu:

1. Teori Kualifikasi Kejahatan oleh Bassiouni

Teori kualifikasi kejahatan menjelaskan pengkualifikasian suatu kejahatan ke dalam suatu kejahatan baru. Menurut Bassiouni bahwa kualifikasi ini dimaksudkan untuk menunjukkan terpenuhinya elemen atau unsur suatu kejahatan untuk dikatakan sebagai suatu kejahatan dalam bingkai hukum kejahatan internasional.

Menurut Bassiouni terdapat tiga unsur yang harus dipenuhi agar suatu kejahatan dapat dikatakan sebagai kejahatan internasional. Unsur tersebut adalah: 120

- 1. Unsur internasional termasuk didalamnya ancaman secara langsung dan tidak langsung atas perdamaian dunia dan menggoyah perasaan kemanusiaan.
- 2. Unsur transnasional termasuk didalamnya bahwa dampak yang ditimbulkan memiliki dampak terhadap lebih dari satu negara, terhadap warga negara dari lebih satu negara, dan sarana dan prasarana serta metode yang dipergunakan melampaui batas-batas teritorial suatu negara.
- 3. Unsur kebutuhan termasuk didalamnya kebutuhan akan kerjasama antara negara-negara untuk melakukan penanggulangan.

Bertitik tolak pada uraian unsur kejahatan internasional sebagaimana yang diungkapkan oleh Bassiouni maka secara implisit kejahatan siber dapat memenuhi keseluruhan unsur

¹²⁰ Romli Atmasasmita, op.cit, hlm. 58.

untuk dikatakan sebagai kejahatan baru dalam literatur kejahatan internasional dewasa ini. Adapun uraian unsur dimaksud dapat dikonstruksi sebagai berikut:

- 1. Unsur internasional, yakni adanya ancaman terhadap perdamaian dunia baik langsung maupun tidak langsung. Dalam konteks ini, kejahatan siber berpotensi untuk memberikan ancaman terhadap perdamaian dunia. Kasus stuxnet (2010) dan flame (2012) sebagaimana telah disebutkan pada bagian sebelumnya sangat berbahaya karena kontrol terhadap aktivitas nuklir dapat dilakukan oleh seseorang dan atau negara dengan secara mudah. Menurut Ralph Langner¹²¹ bahwa stuxnet digambarkan sebagai senjata siber yang digunakan untuk menyerang seluruh program nuklir Iran.¹²² Penggunaan senjata siber seperti ini akan sangat mudah digunakan saat ini dengan pertimbangan perkembangan massif informasi dan teknologi yang tak dapat dielakkan lagi.
- 2. Unsur transnasional, artinya cakupan atau lingkup kejahatan siber yang lintas antar negara. Menurut Hata bahwa kejahatan siber yang terjadi menunjukkan kedaulatan tradisional negara sangat mudah untuk ditembus, yang sekaligus melemahkan fungsi-fungsi kekuasaan tradisional suatu negara. Pendapat Hata ini kemudian dengan sangat mudah untuk dibuktikan dengan melihat beberapa kasus mulai dari kasus pencurian kartu kredit, judi online, akses tidak

¹²¹ Ralph Langner adalah seorang ahli dibidang telematika yang berkebangsaan Jerman.

¹²² James P.. Farwell and Rafal Rohonzinski, op.cit. hlm. 23.

¹²³ Hata, Hukum Internasional : Sejarah dan Perkembangan hingga Pasca Perang Dingin, (Malang: Setara Press, 2012), hlm. 110.

- sah, spionase, hingga siber terrorism yang mulai dikembangkan dalam beberapa tahun terakhir.
- 3. Unsur kebutuhan, artinya dibutuhkan kerjasama secara internasional antar negara-negara untuk menghadapi dan mengadili pelaku kejahatan siber dalam suatu bingkai pengadilan internasional. Dalam konteks ini, dibutuhkan satu aspek *interpenetration* (hubungan saling mempengaruhi antara hukum nasional dan internasional) untuk menggambarkan urgensi kerjasama dimaksud dengan formula hukum perjanjian internasional.¹²⁴

Secara teori, M. Cherif Bassiouni¹²⁵ membagi tingkatan kejahatan internasional menjadi tiga. **Pertama**, kejahatan internasional yang disebut sebagai *international crimes* adalah bagian dari *jus cogens*¹²⁶. Tipikal dan karakter dari international crimes berkaitan dengan perdamaian dan keamanan manusia serta nilai-nilai kemanusiaan yang fundamental. Terdapat sebelas kejahatan yang menempati hirarki teratas sebagai kejahatan internasional (*international crime*), yakni: *Aggression; Genocide; Crimes against humanity; War crimes; Unlawful possession or use or emplacement of weapons; Theft of nuclear materials; Mercenaries; Apartheid; Slavery and slaverelated practices; Torture and other forms of cruel, inhuman, or degrading treatment; dan Unlawful human experimentation.*

Kedua, kejahatan internasional yang disebut sebagai international delicts. Tipikal dan karakter international delicts

¹²⁴ Ibid.

¹²⁵ Eddy O.S. Hiariej, op.cit, hlm. 56.

¹²⁶ *Jus Cogens* adalah hukum pemaksa yang tertinggi dan harus ditaati oleh bangsa-bangsa beradab di dunia sebagai prinsip dasar umum dalam hukum internasional yang berkaitan dengan moral. Lihat, Eddy O.S. Hiariej, op.cit,hlm. 50.

berkaitan dengan kepentingan internasional yang dilindungi meliputi lebih dari satu negara atau korban dan kerugian yang timbul berasal dari satu negara. Ada tiga belas kejahatan internasional yang termasuk dalam international delicts, yaitu: Piracy; Aircraft hijacking and unlawful acts against international air safety; Unlawful acts against the safety of maritime navigation and safety of platforms on the high seas; Threat and use of force against internationally protected person; Crimes against United Nations and associated personnel; Taking of civilian hostages; Unlawful use of the mail; Attacks with explosive; Financing of terrorism; Unlawful traffic in drugs and related drug offenses; Organized crime; Destruction and/or theft of national treasures; Unlawful acts against certain internationally protected elements of the environment.

Ketiga, kejahatan internasional yang disebut dengan istilah international infraction. Dalam hukum pidana internasional secara normatif, international infraction tidak termasuk dalam kategori international crime dan international delicts. Kejahatan yang tercakup dalam international Infraction hanya ada empat, yaitu: International traffic in obscene materials; Falsification and counterfeiting; Unlawful interference with submarine cable; Bribery of foreign public official.

Untuk mendukung teori kualifikasi kejahatan sebagaimana dikemukakan oleh Bassiouni, hukum kejahatan internasional pada dasarnya menganut tiga prinsip fundamental yang harus terpenuhi dalam suatu kejahatan internasional. Ketiga prinsip fundamental dimaksud adalah sebagai berikut:

Pertama, prinsip kesalahan pribadi (*personal culpability principle*) yaitu bahwa setiap orang hanya bertanggung jawab atas perbuatan yang mereka lakukan sendiri. Hukum kejahatan internasional mengakui prinsip ini sebagai dasar (pondasi)

pertanggungjawaban pidana dimana tidak ada seorangpun yang bertanggung jawab secara pidana untuk tindakan atau perbuatan yang tidak dilakukannya. Prinsip ini dalam penerapannya harus ditunjang dengan pengetahuan dan maksud pelaku terhadap kejahatan yang dilakukannya. 127

Kedua, prinsip legalitas (*nullum crimen sine lege – no crime without law, nulla poena sine lege – no penalty without law, nullum crimen, nulla poena sine lege – no crime may be committed nor punishment imposed without a preexisting penal law) yakni prinsip yang mensyaratkan bahwa pendefinisian tidak digunakan secara retroaktif¹²⁸ dan pendefinisian dilakukan dengan mendefinisikannya secara ketat (<i>in dubio pro reo, rule of lenity*) dalam rangka memberikan keadilan kepada pelaku dan sekaligus untuk membatasi kesewenang-wenangan kekuasaan koersif. Dengan kata lain, perbuatan yang disangkakan kepada pelaku merupakan kejahatan yang telah tercantum dalam peraturan perundang-undangan. Sehingga seseorang tidak dapat disangkakan atas suatu kejahatan dimana kejahatan tersebut belum diatur.¹²⁹

Ketiga, prinsip pelabelan (tuduhan) yang adil (*fair labelling principle*) yaitu prinsip yang mensyaratkan bahwa tuduhan yang dialamatkan kepada pelaku merupakan tuduhan yang

¹²⁷ H. Jescheck, 'The General Principles of International Criminal Law Set Out in Nuremberg, as Mirrored in the ICC Statute', Journal of International Criminal Justice, 38 (2004), hlm.44.

¹²⁸ Lihat Universal Declaration of Human Rights Pasal 11 ayat (2) yang menyebutkan "no one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time it was committed".

¹²⁹ CC Statute, Art. 22; Celebci supra note 5, paras. 415–418; B. Broomhall, 'Article 22, Nullum crimen Sine Lege, in O. Triffterer (ed.), Commentary on the Rome Statute of the International Criminal Court (1999), hlm. 450–451.

benar dan menunjukkan jenis kejahatan yang dilakukan oleh tersangka. Hal ini dimaksudkan untuk menghindari "peradilan yang sesat".

Uraian ketiga prinsip dasar yang diakui hukum kejahatan internasional sebagaimana dijelaskan di atas tentunya seharusnya melahirkan sinergitas dengan elemen kualifikasi kejahatan internasional sebagaimana dikemukakan oleh Bassiouni. Dalam prakteknya khususnya beberapa kejahatan genosida dan kejahatan terhadap kemanusiaan yang terjadi Yugoslavia dan Rwanda menimbulkan kompleksitas untuk mengadilinya karena beberapa perbuatan pelaku secara kualifikasi dapat dikatakan sebagai kejahatan internasional tapi secara prinsip ditemukan permasalahan dimana perbuatan tersebut tidak diatur secara detail dalam rumusan Konvensi. 130

2. Teori Kedaulatan Negara (State Sovereignty)

Kedaulatan negara memegang peranan yang sangat penting bagi eksistensi suatu negara dipanggung masyarakat internasional. Kedaulatan negara dimaksud meliputi lingkup proses penciptaan hukum dan aplikasinya dalam konstruksi kedaulatan negara itu sendiri. Negara yang merdeka tentunya memiliki kedaulatan dan atas kedaulatan tersebut maka negara memiliki personalitas internasional (international personality) untuk bertindak dalam international community. 132

Untuk lebih rinci dan detail, kedaulatan negara dielaborasi sebagai berikut:

¹³⁰ Lihat Pasal 22 ICC.

¹³¹ Carlos Fernandez de Casadevante Romani, Sovereignty and Interpretasi of International Norms, (New York: Springer, 2007), hlm. 1.

¹³² Shabtai Rosenne, the Perplexities of Modern International Law, (Netherlands: Martinus Nihjoff Publishers, 2004), hlm. 236.

a) Pengertian Kedaulatan

Gagasan kedaulatan negara yang pada awalnya merupakan unsur penting, telah mengalami erosi. Tren kemerdekaan dan kerjasama antar negara-negara menjadi tren baru dalam beberapa dekade terakhir. Kedaulatan negara yang dipandang merupakan prinsip utama hukum internasional, akan tetapi makna dan artinya belum didefinisikan secara detail. Sebuah definisi yang mungkin ditawarkan tentang kedaulatan, yaitu"

"Sovereignty is the most extensive form of jurisdiction under international law. In general terms, it denotes full and unchallengeable power over a piece of territory and all the persons from time to time therein". (Kedaulatan merupakan bentuk yurisdiksi yang luas menurut hukum internasional. Dalam konteks yang umum, kedaulatan menunjukkan kekuasaan yang penuh dan tak terkalahkan atas wilayah dan orang-orang yang ada diatasnya).

Menurut Krasner¹³⁴, ada empat cara dimana definisi kedaulatan biasanya digunakan:

- Kedaulatan domestik, yang merujuk pada kewenangan politik antara negara dan tingkatan pengawasan yang dilakukan oleh negara;
- 2. Kedaulatan yang saling bergantung, yang merujuk pada fungsi pengawasan suatu negara atas wilayahnya;
- 3. Kedaulatan hukum internasional, yang merujuk pada penciptaan status suatu entitas politik dalam sistem

¹³³ Magdalena Petronella Ferreira-Synman, ohlm.cit., hlm.32. Lihat juga, Oppenheim L., International Law: a Treatise, edited by Arnold Mcnair (1928), hlm. `137.

¹³⁴ Krasner S., Sovereignty: Organized Hypocrisy in Steiner HJ, Alston P., and Goodman R., International Human Rights in Context: Law, Politics, Moral, 3rd ed., (2008), hlm. 690-692.

- internasional. Negara dalam tingkatan internasional diperlakukan sama dengan individu dalam tingkatan nasional;
- 4. Kedaulatan Westphalia, yang dipahami sebagai suatu pengaturan institusi untuk mengatur kehidupan politik dan didasarkan pada 2 (dua) prinsip dasar teritorial dan pengesampingan faktor-faktor eksternal dari kewenangan struktur domestik. Kedaulatan Westphalia dilanggar ketika faktor-faktor eksternal mempengaruhi atau menentukan kewenangan struktur domestik. Dalam konteks ini, bentuk kedaulatan dapat dikompromikan melalui intervensi ketika negara secara sukarela menjadi subjek dari kewenangan struktur domestik.

Identifikasi Krasner atas definisi dan klasifikasi kedaulatan sebagaimana diuraikan di atas masih dirasa membingungkan. Akan tetapi terdapat dua hal penting yang perlu digaris bawahi ketika mendefinisikan kedaulatan negara. *Pertama*, kedaulatan merupakan kekuasaan mutlak yang dimiliki oleh suatu negara dan merupakan unsur penting dan utama dari prinsip hukum internasional. *Kedua*, kedaulatan merupakan subjek yang sangat penting dalam hukum internasional dimana negara tidak dapat mengklaim bahwa negara berada di atas hukum internasional atau bahwa hukum internasional tidak mengikatnya secara hukum.¹³⁵

b) Aspek Eksternal, Internal dan Teritorial Kedaulatan

Pasal 1 Konvensi Montevideo 1933 menempatkan "... kemampuan untuk melakukan hukum dengan negara lain..." sebagai salah satu unsur untuk menunjukkan bahwa suatu negara merupakan entitas subjek hukum internasional. Penempatan unsur "...kemampuan untuk melakukan

¹³⁵ Magdalena Petronella Ferreira-Synman, op.cit., hlm. 35.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

hukum dengan negara lain..." dalam perkembangan hukum internasional perlahan digantikan dengan konsep kedaulatan mengingat sifat dan lingkupnya yang lebih luas.¹³⁶

Kedaulatan merupakan kekuasaan mutlak yang dimiliki oleh suatu negara untuk mengatur negara (wilayahnya) termasuk orang-orang didalamnya (warga negaranya), asal tidak bertentangan dengan hukum internasional. Menurut Nkambo Mugerwa, kedaulatan memiliki 3 (tiga) aspek utama, yaitu: 138

- 1. Aspek eksternal kedaulatan adalah hak bagi negara untuk melakukan perhubungan dengan negara lain tanpa adanya tekanan, kekangan dan pengawasan dari negara lain.¹³⁹
- 2. Aspek internal kedaulatan adalah hak atau wewenang eksklusif suatu negara untuk menentukan lembagalembaganya, cara kerja lembaga-lembaga tersebut dan hak untuk membuat undang-undang serta tindakan untuk mematuhinya;¹⁴⁰
- Aspek teritorial kedaulatan adalah kekuasaan penuh dan eksklusif yang dimiliki negara atas individu-individu dan benda-benda yang terdapat di wilayah tersebut.

Dalam hubungannya dengan kedaulatan eksternal, para

Lihat Boer Mauna, Hukum Internasioal: Pengertian, Peranan, dan Fungsi Dalam Era Dinamika Global, (Bandung: PT Alumni, 2005), hlm 24.
 137 Ibid.

¹³⁸ Nkambo Mugerwa, Subject of International Law, edited by Max Sorensen (New York: MacMillan, 1968), hlm. 253.

Lihat Magdalena Petronella Ferreira-Synman, op.cit., hlm. 36. Lihat juga Fassbender in SimmaB., Ed., the charter of the United Nations: A Commentary, Volume 1 (2002), hlm. 70. Lihat juga Perrez FX, Cooperative Sovereignty from Independence to Interdependence in the Structure of International Environmental law, (2003), hlm. 13.

¹⁴⁰ Lihat Magdalena Petronella Ferreira-Synman, op.cit., hlm. 36

ahli klasik, lebih lanjut, mendefinisikan kedaulatan eksternal sebagai kemerdekaan. Salah satunya diberikan oleh Max Huber yang menggambarkannya dalam *the Island of Palmas Case* (1928). Max Huber mendefinisikan kedaulatan sebagai berikut: "Sovereignty in the relation between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to exclusion of any other states, the functions of a state" 141

Pandangan Max Huber dapat pula ditemukan dalam kedaulatan tradisional. Dalam pandangan pandangan kedaulatan tradisional. kedaulatan dipahami sebagai kemerdekaan dan kekuasaan tertinggi. Jean Bodin di abad yang mendefinisikan kedaulatan sebagai kekuasaan mutlak dan terus menerus. Menurutnya, konsep kedaulatan merupakan kekuasaan mutlak dan kompetensi untuk membuat hukum dalam batas-batas wilayah teritorialnya dan tidak akan mentolerir agen-agen lain (negara lain) untuk menciptakan hukum melanggar wilayah teritorialnya. 142

Jean Bodin lebih lanjut menyebutkan bahwa kedaulatan adalah kekuasaan tertinggi negara yang tidak dapat dibatasi kecuali dengan hukum Tuhan dan hukum alam. Tidak satupun konstitusi yang dapat membatasi kedaulatan dan oleh karenanya kedaulatan dipertimbangkan sebagai hukum positif. Oleh karena itu, dapat dikatakan bahwa dalam pandangan penganut kedaulatan tradisional, kedaulatan merupakan konsep mutlak dimana negara-negara harus secara utuh merdeka dari negara lain.¹⁴³

¹⁴¹ Ibid. hlm. 37.

¹⁴² Ibid. Lihat juga Van der Vyver JD, the Concept of Political Sovereignty, in Visser C.,Ed., Essay in honor of Ellison Kahn, (1989), hlm. 290.

¹⁴³ Magdalena Petronella Ferreira-Synman, op.cit., hlm.42.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

Konseptual kedaulatan yang didasarkan pada ide atau cita kemerdekaan dapat pula ditemukan dalam the Peace of Westphalia. Akan tetapi pada umumnya penerimaan akan paham kedaulatan yang aslinya merujuk pada perjanjian the Peace of Westphalia ini telah mengalami perkembangan khususnya di akhir abad ke-18 dan 19 dimana kedaulatan diartikan pula sebagai konsep kesamaan negara sebagai unsur utama dari kedaulatan. Dalam kontes ini, konsep kedaulatan telah melahirkan suatu konsep baru dalam hukum internasional yang biasa disebut dengan "Prinsip non-Intervensi". Prinsip ini meniadakan campur tangan negara lain dalam urusan dalam negeri negara bersangkutan.

Penerapan "Prinsip non-Intervensi" dapat ditemukan dalam Pasal 2 ayat (7) Piagam PBB, yang menyatakan sebagai berikut:

"Tidak ada suatu ketentuan pun dalam Piagam ini yang memberi kuasa kepada PBB untuk mencampuri urusan-urusan yang pada hakikatnya termasuk urusan negeri sesuatu negara atau mewajibkan anggota-anggotanya untuk menyelesaikan urusan-urusan demikian menurut ketentuan Piagam ini; akan tetapi prinsip ini tidak mengurangi ketentuan mengenai penggunaan tindakan-tindakan mengenai penggunaan tindakan-tindakan pemaksaan seperti tercantum dalam Bab VII".

Doktrin kedaulatan dalam perkembangannya khususnya di abad 19 atau sebagian 20 menganut pandangan bahwa ide negara hanya terikat pada aturan-aturan hukum internasional yang mereka sepakati baik yang diperoleh melalui perjanjian maupun kebiasaan internasional. Hal tersebut dapat dilihat pada pertimbangan the Permanent Court of International Justice

(PCIJ) pada kasus Lotus tahun 1927. Dalam pertimbangannya, PCIJ mengatakan bahwa :

"International law governs relations between independent states. The rules of law binding upon states therefore emanate from their own free will as expressed in conventions or by usage generally accepted as expressing principles of law..." 144

Kedudukan hukum internasional yang mengatur hubungan negara-negara yang merdeka lantas tidak menurunkan nilai kedaulatan yang dimiliki oleh negara-negara tersebut. Sifat mutlak kedaulatan negara yang dalam beberapa abad dipahami dan dianut oleh negara-negara, telah mengalami perkembangan dengan memberi batasan pada penggunaan makna kedaulatan untuk menghindari "anarchy sovereignty".

Sifat mutlak kedaulatan yang dipahami di abad 20 dan 21, lebih ditekankan pada aspek-aspek internal, eksternal dan teritorial kedaulatan. Tentunya, pemanfaatan kedaulatan sebagai sesuatu yang fundamental sifatnya bagi suatu negara harus diberi batasan untuk menghindari penyalahgunaan kegiatan-kegiatan kedaulatan untuk yang mengancam dan keamanan internasional. Konsekuensi perdamaian pelaksanaan kegiatan-kegiatan yang mengancam perdamaian dan keamanan internasional akan mengancam pula status kemerdekaan suatu negara.

Dalam konteks di atas, kedaulatan mutlak perlahan digantikan posisinya oleh suatu konsep kedaulatan relatif (*relative sovereignty*), dimana kebebasan/kedaulatan suatu negara dibatasi oleh kebebasan/kedaulatan negara lain dan

¹⁴⁴ Fassbender, op.cit., hlm. 11

kemerdekaan suatu negara menjadi unsur utama dan penting dalam hukum internasional.

3. Teori Yurisdiksi (*Theory of Jurisdiction*)

seiring dengan Dewasa ini, berkembangnya pengetahuan, politik, ekonomi, kebudayaan, dan teknologi informasi dalam kehidupan manusia, seolah telah mengikis secara perlahan batas-batas antar negara yang satu dengan negara lainnya. Pola-pola kerjasama internasional terusmenerus dikembangkan guna mencapai titik kemakmuran dalam negeri yang menjadi tujuan utama dilakukannya kegiatan-kegiatan tersebut. Namun, seiring dengan berjalannya globalisasi tersebut, permasalahan-permasalahan yang kemudian timbul pun semakin beragam dan kompleks. Di saat kepentingan negara yang satu berbenturan dengan kepentingan negara lainnya maka pada saat itulah conflict of interest berkembang dan semakin runyam, tiap-tiap negara tentu ingin pihaknya tidak dirugikan. Terkait hal tersebut maka pemahaman mengenai konsep yurisdiksi menjadi sangat penting sebab ketika suatu persoalan muncul ke permukaan biasanya pihak-pihak terkait akan berlomba-lomba 'menjual' konsep kedaulatan yang dimilikinya agar kepentingan mereka tetap terjaga.

a) Definisi Yurisdiksi

Yurisdiksi merupakan refleksi dari prinsip dasar kedaulatan negara di mana kedaulatan negara tidak akan diakui apabila negara tersebut tidak memiliki yurisdiksi. Negara lain dalam hal ini juga tidak diperkenankan oleh Hukum Internasional untuk memaksakan yurisdiksi atas wilayah teritorial negara berdaulat

¹⁴⁵ Mirza Satria Buana, Hukum Internasional Teori dan Praktik, (Bandung: Nusamedia, 2007), hlm 56.

lainnya, kecuali dalam derajat yang lebih rendah, misalnya negara protektorat. Inilah yang kemudian dikenal dengan prinsip *Par in Parem Non Habet Imperium*. 146

Yurisdiksi dapat diartikan sebagai kekuasaan dan dalam kaitannya dengan negara kekuasaan itu merupakan cara atau tindakan yang diambil oleh suatu negara untuk melakukan kekuasaannya, baik dalam menentukan peraturan perundangundangan nasionalnya sendiri maupun untuk memberlakukan peraturan tersebut. Berdasarkan pengertian di atas, dapat diketahui bahwa terdapat setidaknya tiga tipologi yurisdiksi nasional suatu negara yaitu 'bersifat menentukan' atau *prescriptive*; 'bersifat melaksanakan' atau *enforcement*; serta 'bersifat mengadili' atau *adjudicative*. Pandangan senada juga disampaikan oleh Masaki Hamano yang secara spesifik membagi 3 (tiga) jenis yurisdiksi tradisional, sebagai berikut: 148

1. Yurisdiksi Legislatif ("Jurisdiction to Prescribe"); Yurisdiksi legislatif adalah wewenang negara untuk membuat hukum sesuai dengan masyarakat dan keadaan yang ada;

¹⁴⁶ Prinsip ini mengandung beberapa pengertian, *pertama*, suatu negara tidak dapat melaksanakan yurisdiksi melalui pengadilannya terhadap tindakan-tindakan negara lain, kecuali negara tersebut menyetujuinya; *kedua*, suatu pengadilan yang dibentuk berdasarkan perjanjian internasional tidak dapat mengadili tindakan suatu negara yang bukan merupakan anggota atau peserta perjanjian; *ketiga*, pengadilan suatu negara tidak berhak mempersoalkan keabsahan tindakan negara lain yang dilaksanakan di dalam wilayah negara lain tersebut.

¹⁴⁷ Sumaryo Suryokusumo, op.cit., hlm 239.

¹⁴⁸ Ayu Putriyanti, *Yurisdiksi di Internet*, Media Hukum, Vol IX, No.2 (April-Juni/2009), hlm 2. Bandingkan juga dalam Barda Nawawi Arief, Sari Kuliah Perbandingan Hukum, Materi Kuliah Program Pascasarjana Ilmu Hukum Universitas Diponegoro (2001), hlm 259.

- 2. Yurisdiksi untuk Mengadili ("Jurisdiction to Adjudicate"); Yurisdiksi untuk mengadili didefinisikan sebagai wewenang negara terhadap seseorang yang kepadanya dilakukan proses pemeriksaan pengadilan terkait masalah kriminal;
- 3. Yurisdiksi untuk Melaksanakan (*"Jurisdiction to Enforce"*).

Yurisdiksi untuk melaksanakan berhubungan dengan wewenang suatu negara untuk melakukan penghukuman terhadap terdakwa sesuai hukum yang berlaku, baik melalui pengadilan maupun melalui tindakan non-yuridis lainnya, misalnya sanksi administratif.

Dame Rosalyn Higgins, Presiden *International Court of Justice* (selanjutnya disingkat ICJ) periode 1995-2009, lebih lanjut berpendapat bahwa yurisdiksi dapat diartikan sebagai alokasi kewenangan kepada negara, yang mana hal itu penting untuk menghindari terjadinya konflik kewenangan di kemudian hari. 149 Jadi, yurisdiksi dalam Hukum Internasional pada dasarnya digunakan untuk memberi kewenangan kepada suatu negara untuk menjalankan kewenangan hukum yang sah atas orang, wilayah, bahkan peristiwa-peristiwa yang terjadi di wilayah hukumnya. Kemudian, definisi lain juga terdapat dalam *Black's Law Dictionary*, yang menyatakan bahwa yurisdiksi:

 memiliki makna yang luas dan komprehensif serta mencakup setiap jenis tindakan-tindakan pengadilan;

Sebagaimana tertuang dalam Report of The Commission on The use of The Principle of Universal Jurisdiction by Some Non-African States as Recommended by The Conference of Ministers of Justice or Attorneys General, EX.CL/411(XIII) Tahun 2008 oleh African Union, hlm 1. Lihat juga dalam Rosalyn Higgins, Problems and Process: International Law and How We Use it, (New York: Oxford University Press, 1994), hlm. 56.

- 2. merupakan sumber otoritas pengadilan dan pekerjapekerja yudisial untuk mengambil tanggung jawab dan memutuskan kasus-kasus;
- 3. merupakan suatu hak hukum yang dimiliki hakim untuk melaksanakan otoritas mereka;
- 4. dinyatakan ada pada saat pengadilan memiliki tanggung jawab untuk mengklasifikasikan kasus-kasus, pihak-pihak yang terlibat, serta memutuskannya sesuai dengan kewenangan pengadilan; serta
- 5. kewenangan atau kekuasaan pengadilan terhadap hal-hal pokok (*"subject matter"*) dalam kasus tersebut.¹⁵⁰

Selanjutnya, menurut *Encyclopedia International Law* dikatakan bahwa terdapat lima prinsip umum yurisdiksi, yaitu prinsip teritorial; prinsip nasionalitas; prinsip personalitas pasif; prinsip perlindungan; dan prinsip universal. Prinsip teritorial dan nasionalitas berlaku sama pada yurisdiksi sipil dan kriminal, sementara tiga prinsip lainnya hanya berlaku untuk yurisdiksi kriminal.¹⁵¹

Secara konseptual, istilah yurisdiksi seringkali diformulasikan dalam korelasinya di antara negara-negara, kedaulatan ("sovereignty"), dan teritorial ("territory"). 152 Sesungguhnya kedua terminologi (sovereignty dan jurisdiction) sangat erat kaitannya satu sama lain dan merupakan atribut esensial dari negara namun memiliki perbedaan cakupan

¹⁵⁰ Henry Campbell Black, Black's Law Dictionary Fifth Edition, (West Publishing Co, 1994), hlm. 766.

¹⁵¹ Supra 2, hlm 2.

¹⁵² Shaunnagh Dorsett dan Shaun McVeigh, Questions of Jurisdiction, in Shaun McVeigh, Jurisprudence of Jurisdiction, (Routledge-Cavendish, 2007), hlm. 8.

yang menonjol. Istilah kedaulatan menunjuk pada kekuasaan mutlak dan abadi dari negara yang tidak terbatas dan tidak dibagi-bagi. 153 Berdasarkan dapat pandangan tersebut dapat diketahui bahwa kedaulatan mencakup kekuasaan ("power") negara atas semua bidang kehidupan yang ada di negaranya, baik itu politik, ekonomi, hukum, sosial, maupun budaya. Sedangkan yurisdiksi berbicara mengenai kekuasaan negara dalam bidang hukum saja. Dengan demikian, jelas terlihat perbedaan sekaligus keterkaitan antara yurisdiksi dan kedaulatan negara yaitu bahwa yurisdiksi merupakan bagian dari kedaulatan negara. Kedaulatan negara mencakup hak dan kekuasaan untuk menjalankan segala tindakan, sedangkan yurisdiksi menunjuk pada kewenangan yuridis saja. 154

Oleh karena itu, disinilah letak dan peran yang harus dimainkan Hukum Internasional dalam mengatur kapan suatu negara dapat melaksanakan yurisdiksinya dan dalam keadaan-keadaan di mana negara itu tidak bisa melaksanakan yurisdiksinya tersebut, hal ini dalam rangka mengurangi benihbenih pertikaian yang bisa timbul antar negara. Hingga saat ini, persoalan yurisdiksi negara masih menjadi isu hangat, baik dalam sengketa politik maupun sipil.

b) Jenis-Jenis Yurisdiksi

Hukum Internasional mengatur beberapa jenis pelaksanaan yurisdiksi, antara lain yurisdiksi teritorial, yurisdiksi

¹⁵³ Pandangan ini menurut Jean Bodin, pencetus bentuk ilmiah konsep kedaulatan. Menurut beliau, kedaulatan mengandung satu-satunya kekuasaan sebagai yang asli, tertinggi, abadi, kekal, dan tidak dapat dibagibagi. Lihat dalam Adji Samekto, Negara dalam Dimensi Hukum Internasional, (Bandung: PT Citra Aditya Bakti, ,2009), hlm 49.

¹⁵⁴ *Ibid*, hlm 61.

¹⁵⁵ Supra 1, hlm 139.

perlindungan, yurisdiksi universal, dan yurisdiksi personal.¹⁵⁶ Semua jenis yurisdiksi tersebut dapat digunakan sesuai dengan persyaratan yang telah diatur dalam hukum internasional dan juga memiliki dampak hukum yang berbeda-beda pula.

I. Yurisdiksi Teritorial

Konsep

Pada umumnya, yurisdiksi ini dipandang sebagai yurisdiksi utama, tidak terbatas, dan paling mapan. Hal ini dapat dipahami bila mengingat bahwa yurisdiksi ini merupakan satu-satunya jenis yurisdiksi yang mencerminkan konsep kedaulatan negara, dimana suatu negara memiliki kedaulatan penuh atas wilayah teritorialnya, baik itu meliputi orang-orang, hal-hal, maupun peristiwa-peristiwa tertentu. Menurut Georg Schwarzenberger, adalah suatu otoritas atas suatu bagian permukaan bumi serta ruang di atas dan tanah di bawahnya yang ditentukan secara geografis dan diklaim sebagai teritorial kedaulatannya, termasuk semua orang dan benda di atasnya. Di samping itu, pelaksanaan yurisdiksi oleh suatu negara atas wilayah teritorialnya juga diakui oleh masyarakat internasional. Prinsip ini telah dikemukakan dengan tepat oleh Lord Macmillan, yang menyatakan:

"Adalah suatu ciri pokok dari kedaulatan dalam batasbatas ini, seperti negara merdeka yang berdaulat, bahwa negara harus memiliki yurisdiksi terhadap semua orang dan benda di dalam batas-batas teritorialnya dan dalam semua perkara perdata dan pidana timbul di dalam batasbatas teritorial ini".

¹⁵⁶ Supra 2, hlm 1.

¹⁵⁷ Adji Samekto, op.cit., hlm 63.

Selain itu, Hukum Internasional juga mengenal Prinsip Yurisdiksi Sementara atau *Transient Jurisdiction*, sebagaimana yang berlaku di Inggris dan Amerika Serikat. Menurut praktek Inggris, keberadaan fisik dari seseorang atau benda di dalam wilayah negara ini saja sudah cukup untuk menarik yurisdiksi tanpa perlu berdomisili di negara ini. Lebih lanjut, suatu negara hanya mempunyai yurisdiksi absolut terhadap penduduknya yang tinggal di wilayahnya. Dalam hal mereka berada di wilayah negara lain maka negara asal tetap berkewajiban untuk memberikan perlindungan pada warganya tersebut tetapi warga tersebut juga terikat pada yurisdiksi negara yang ditujunya tersebut.

Dalam kaitannya dengan orang asing, hukum internasional menegaskan bahwa perlakuan yang sama harus diberikan oleh suatu negara seperti perlakuan yang diberikannya kepada warga negaranya sendiri. Hal ini ditegaskan oleh J. B. Moore dalam *Lotus Case*, bahwa tidak ada anggapan imunitas yang muncul dari fakta bahwa orang yang dikenai perkara itu adalah orang asing. Orang asing itu tidak dapat menuntut pembebasan dari pelaksanaan yurisdiksi kecuali ia mampu menunjukkan bahwa (1) ia memiliki imunitas khusus sehingga tidak tunduk pada hukum negara setempat; dan (2) hukum lokal tersebut tidak sesuai dengan hukum internasionalnya. Kemudian, bagaimana dengan warga asing yang terbukti melakukan kejahatan di negara penerima? Apakah ia tunduk pada hukum negara setempat ataukah pada hukum negara asalnya?

Sebagaimana yang telah dijelaskan sebelumnya, untuk setiap tindakan kriminal yang dilakukan oleh warga asing sudah seharusnya tunduk pada yurisdiksi negara penerima. Kondisi ini

¹⁵⁸ Soemaryo Suryokusumo, op.cit, hlm 277.

biasa disebut pula dengan Yurisdiksi Kriminal Teritorial. Pada dasarnya penerapan tipe yurisdiksi seperti ini dapat dipahami oleh beragam prinsip. Justifikasi normalnya adalah bahwa negara penerima merupakan pihak yang paling dirugikan keamanan nasionalnya akibat kejahatan yang telah dilakukan oleh warga asing tersebut di wilayahnya.

Selain itu. pertimbangan penting lainnya adalah kepentingan negara penerima paling kuat, dalam arti negara tersebut memiliki fasilitas paling baik dan memiliki perangkat paling kuat untuk menumpas kejahatan-kejahatan, baik yang dilakukan oleh warga negaranya sendiri maupun oleh orangorang asing yang berdomisili di dalam wilayahnya. 160 Namun, sekalipun negara penerima memiliki yurisdiksi atas warga asing yang melakukan kejahatan di wilayahnya, akan tetapi harus diingat pula bahwa negara asal warga asing tersebut juga tetap memiliki yurisdiksi atas warga negaranya tersebut, yaitu dalam hal memberikan perlindungan terhadap warganya, biasanya melalui perwakilan diplomatik maupun perwakilan konsuler. Inilah esensi yang dimaksud dengan Hak Dasar, yaitu hak-hak yang dimiliki seseorang sebagai konsekuensi ia adalah warga suatu negara. Oleh karena itu, prinsip saling menghormati antar negara sangat diperlukan untuk menghindari terjadinya konflik yurisdiksi sekaligus konflik kepentingan di antara mereka.

Lebih lanjut, setiap negara mempunyai yurisdiksi secara eksklusif di lingkungan wilayahnya sendiri, tetapi yurisdiksi semacam itu bukanlah merupakan yurisdiksi yang bersifat absolut karena akan tergantung dari pembatasan-pembatasan tertentu yang diatur oleh hukum internasional. Oleh karena

¹⁵⁹ J. G. Starke, Pengantar Hukum Internasional *(Edisi Kesepuluh)*, (Jakarta: Sinar Grafika, 2010), hlm 277.

¹⁶⁰ *Ibid*.

itu, dalam praktik negara tidak selalu dapat melakukan caracara atau tindakan yang diambilnya untuk melaksanakan yurisdiksi di wilayahnya. Namun, di lain pihak, suatu negara dalam hal-hal tertentu dapat melaksanakan yurisdiksinya di luar wilayahnya. Hal ini menjadi penting dalam rangka mengantisipasi perkembangan-perkembangan kejahatan yang bersifat lintas batas. Inilah yang kemudian kita kenal dengan Yurisdiksi dengan Asas Teritorial Objektif dan Yurisdiksi dengan Asas Teritorial Subjektif.

Klasifikasi

Sejalan dengan perkembangan sarana komunikasi dan transportasi internasional yang demikian pesat, masyarakat internasional memandang perlu dilakukannya perluasan teknis yurisdiksi teritorial. Hal ini diperlukan untuk meminimalisir bebasnya pelaku kejahatan hanya karena telah keluar dari wilayah tempatnya melakukan tindak kejahatan. Dalam Hukum Internasional, dikenal 2 (dua) jenis perluasan yurisdiksi teritorial, yaitu:

a. Yurisdiksi dengan Asas Teritorial Subjektif

Istilah lain jenis ini adalah Prinsip Teritorial Subjektif ("Subjective Territorial Principle"). Yurisdiksi ini merupakan yurisdiksi negara yang diterapkan terhadap pelaku kejahatan yang dimulai dari negara setempat dan diakhiri atau menimbulkan akibat di negara lain. 162 Inti dari asas ini dapat dilihat pada aspek akibat yang ditimbulkan oleh kejahatan tersebut. Menurut prinsip ini, tindak kejahatan di lakukan di dalam negeri akan tetapi akibat perbuatan tersebut dirasakan dampaknya di luar negeri. Walaupun prinsip ini belum diterapkan

¹⁶¹ *Ibid*, hlm 240.

¹⁶² Adji Samekto, op.cit., hlm 64.

secara umum oleh negara-negara setara dengan suatu kaidah umum hukum bangsa-bangsa tetapi penerapannya secara khusus telah menjadi bagian dari hukum internasional sebagai akibat ketentuan dua konvensi internasional, yaitu *Geneva Convention for Suppression of Counterfeiting Currency* (Konvensi Jenewa untuk Memberantas Pemalsuan Mata Uang) tahun 1929 dan *Geneva Convention for Suppression of the Illicit Traffic Drug* (Konvensi Jenewa untuk Memberantas Perdagangan Obat Bius) tahun 1936. Kedua konvensi inilah yang melatarbelakangi lahirnya jenis yurisdiksi ini.

b. Yurisdiksi dengan Asas Teritorial Objektif

Jenis yurisdiksi ini juga dikenal sebagai Prinsip Teritorial Territorial Principle"). Yurisdiksi Objektif ("Objective merupakan kebalikan dari jenis Prinsip Teritorial Subjektif. Yurisdiksi ini merupakan yurisdiksi yang diterapkan terhadap pelaku kejahatan yang dimulai di negara lain dan diakhiri atau memberi akibat di negara setempat. Berdasarkan ketentuan prinsip ini negara-negara tertentu menerapkan yurisdiksi teritorial mereka terhadap perbuatan-perbuatan pidana atau perbuatan-perbuatan yang dilakukan di negara lain tetapi (1) dilaksanakan atau diselesaikan di dalam wilayah mereka; atau (2) menimbulkan akibat yang sangat berbahaya terhadap ketertiban sosial dan ekonomi di dalam wilayah mereka. 164 Inti utama jenis yurisdiksi ini menekankan pada akibat kejahatan yang dirasakan negara setempat sekalipun kejahatannya dimulai di negara lain.

Ilustrasi mengenai teori ini diberikan oleh sebuah laporan resmi LBB mengenai yurisdiksi kriminal negara-negara terhadap perbuatan-perbuatan pidana yang dilakukan di luar wilayah

¹⁶³ Soemaryo Suryokusumo, op.cit., hlm 273.

¹⁶⁴ J. G. Satrke, op.cit., hlm 274.

mereka, misalnya seseorang menembakkan senapan di seberang perbatasan dan menewaskan orang lain yang berada di negara tetangga. Pada kasus ini pelaku melakukan tindakan penembakan di negara lain tetapi dampaknya dirasakan di dalam negeri, yaitu tewasnya warga negara setempat. Berdasarkan uraian di atas, terlihat jelas bahwa perluasan teknis yurisdiksi teritorial ini ditujukan untuk mengantisipasi kejahatan-kejahatan transboundaries atau lintas batas negara.

Pembatasan Penerapan Yurisdiksi Teritorial

Ketentuan Hukum Internasional mengenai pelaksanaan yurisdiksi teritorial ini tidak terbatas. Akan tetapi terdapat golongan-golongan tertentu yang memiliki hak imunitas (hak kekebalan hukum) yang padanya tidak berlaku yurisdiksi teritorial negara setempat, yaitu:

a. Kepala Negara atau Kepala Pemerintahan Asing

Kekebalan yang dimiliki oleh kepala negara atau kepala pemerintahan asing juga berlaku dalam hubungan diplomatik dan konsuler. Sebagaimana tercantum pada Pembukaan Konvensi Wina 1961 tentang Hubungan-hubungan Diplomatik dinyatakan bahwa "peoples of all nations from ancient time have recognized the status of diplomatic agents", jadi sejak zaman dahulu masyarakat internasional telah mengenal status perwakilan-perwakilan diplomatik.

Kedudukan kepala negara maupun kepala pemerintahan di dalam hubungan internasional tidak berdasarkan atas kepribadiannya akan tetapi sebagai berlandaskan dari negaranya anggota

¹⁶⁵ *Ibid*, hlm 274.

masyarakat internasional. Kedudukannya di luar negeri tidak diukur dari sifat orangnya sebagai individu melainkan status negaranya di dunia internasional. Singkatnya, kepala negara dan/atau kepala pemerintahan dianggap sebagai lambang negara dengan segala kehormatan dan kewibawaan yang melekat padanya. Menurut J. L. Brierly, mengenai kekebalan kepala negara dan/atau kepala pemerintahan mempunyai dua kaidah, yakni: 167

- Bahwa seorang kepala negara asing tidak dapat dituntut di depan pengadilan, baik terhadap dirinya pribadi maupun untuk mendapatkan kembali sesuatu barang atau meminta ganti rugi;
- Bahwa terhadap harta benda yang menjadi miliknya atau yang di bawah pengawasannya tidak dapat dilakukan penyitaan atau ditahan atas nama pengadilan, baik kepala negara itu merupakan pihak dalam perkara atau bukan.

Pertanyaannya kemudian adalah: mengapa kepala negara dan/atau kepala pemerintahan ini memperoleh kekebalan dan hak-hak istimewa sehingga tidak harus tunduk pada yurisdiksi negara penerima? Jika menilik pada teoriteori Hukum Internasional dalam bidang Hukum Diplomatik, setidaknya terdapat tiga teori yang melatarbelakangi pemberian kekebalan tersebut, yaitu:

¹⁶⁶ Edy Suryono dan Moenir Arisoendha, Hukum Diplomatik: Kekebalan dan Keistimewaannya, (Bandung: PT Angkasa, Bandung, 1991), hlm 9.

¹⁶⁷ *Ibid*, hlm 10. Lihat juga dalam J. L. Brierly, Hukum Bangsa-Bangsa, (Jakarta: Bhratara, 1963), hlm 195.

1. Teori Exterritoriality atau Ekstrateritorial

Teori ini menyatakan bahwa seorang wakil diplomatik itu karena *exterritorialiteit* dianggap tidak berada di wilayah negara penerima tetapi berada di wilayah negara pengirim meskipun pada kenyataannya ia berada di wilayah negara penerima. Oleh karena itu, dengan sendirinya seorang wakil diplomatik itu tidak takluk kepada hukum negara penerima. Seorang wakil diplomatik tersebut menurut teori ini dikuasai oleh hukum negara pengirim. Pandangan ini dilandasi pada teori yurisdiksi ekstrateritorial.¹⁶⁸

Namun pada prakteknya, konsekuensi diterimanya pandangan demikian juga sukar diterima. Teori exterritorialiteit tidak bisa ditetapkan sebagai dasar yang memadai karena sejumlah pembebasan-pembebasan ataupun kekebalan-kekebalan yang berasal dari teori ini tidak pernah diterima dalam praktiknya, misalnya untuk maksud-maksud tertentu kediaman diplomatik dapat masuk yurisdiksi negara penerima (*"receiving state"*).¹⁶⁹

2. Teori *Representative Character*¹⁷⁰

Teori ini menyatakan bahwa kekebalan diberikan kepada kepala negara dan/atau kepala pemerintahan sebab mereka merupakan wakil negara mereka sehingga dalam hal ini kembali berlaku adegium klasik "Par im Parem non Habet Imperium", yang dapat diartikan bahwa suatu negara berdaulat tidak dapat melaksanakan yurisdiksinya atas negara berdaulat lainnya,

¹⁶⁸ Yurisdiksi ekstrateritorial diartikan sebagai kepanjangan secara semu (*quasi extentio*) dari yurisdiksi sesuatu negara di wilayah yurisdiksi negara lain.

¹⁶⁹ *Ibid*, hlm 33.

¹⁷⁰ *Ibid*, hlm 36.

kecuali terhadap yang lebih rendah. Dengan demikian, maka negara penerima berkewajiban untuk memperlakukan seorang diplomat di dalam tindakan-tindakan yang sesuai dengan sifat perwalikannya ("consequently the receiving state is obliged to treat envoy in a manner befitting his representative character").

3. Teori Functional Necessity¹⁷¹

Teori Kebutuhan Fungsional menegaskan bahwa dasar pemberian kekebalan dan hak-hak istimewa kepada seorang wakil diplomatik agar mereka dapat melaksanakan tugasnya dengan memuaskan dan tanpa tekanan.¹⁷² Oleh karena itu, beberapa pembatasan-pembatasan yang dibebankan atau ditetapkan oleh peraturan-peraturan hukum setempat dibebaskan atas mereka.¹⁷³ Teori ini juga didukung oleh Konvensi Wina 1961 yang menyatakan bahwa "tujuan hak-hak istimewa dan kekebalan tersebut bukan untuk menguntungkan orang-perorangan tetapi untuk membantu pelaksanaan yang efisien fungsi-fungsi misi diplomatik sebagai wakil dari negara".¹⁷⁴

Di samping kekebalan atas yurisdiksi yang dimiliki oleh kepala negara dan/atau kepala pemerintahan tersebut, mereka juga tetap harus tunduk pada beberapa pengecualian dari kaidah imunitas tersebut, yang meliputi:¹⁷⁵

 Perkara-perkara yang berkenaan dengan alas hak terhadap tanah di dalam jurisdiksi teritorial, yang bukan tanah di mana bangunan-bangunan kedutaan didirikan. Prinsip yang diberlakukan di

¹⁷¹ *Ibid*, hlm 36.

¹⁷² Edy Suryono dan Moenir Arisoendha, op.cit.,, hlm 118.

¹⁷³ *Ibid*, hlm 39.

¹⁷⁴ Boer Mauna, op.cit. hlm 548.

¹⁷⁵ J. G. Starke, op.cit., hlm 281-282.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

sini adalah bahwa negara lokal mempunyai suatu kepentingan yang sangat vital di tanahnya, yang tidak memungkinkan adanya penghapusan dari jurisdiksinya untuk menuntut hak-hak atas tanah tersebut.

- Suatu dana di pengadilan (dana perwalian) yang diuruskan yang mana menyangkut kepentingan negara asing atau Pemegang kedaulatan asing, tetapi tidak demikian apabila pihak yang diuruskan perwalian dananya itu merupakan pemerintah negara asing yang berdaulat.
- 3. Tindakan-tindakan perwalian, seperti tindakan pemegang surat utang ("debenture"), apabila negara asing atau pemegang kedaulatan asing itu adalah pemegang surat utang.
- 4. Berakhirnya suatu perusahaan yang dalam asetasetnya negara asing atau Pemegang kedaulatan asing mengklaim suatu kepentingan.

b. Perwakilan Diplomatik dan Konsul Negara Asing

Imunitas terhadap agen-agen diplomatik diatur dalam Pasal 31-32 Konvensi Wina 1961. Kekebalan yurisdiksional seorang perwakilan diplomatik berhubungan dalam bidang kriminal, sipil, dan administratif negara penerima, kecuali dalam tiga hal khusus yang telah ditentukan secara limitatif oleh Pasal 31, yaitu: 176

¹⁷⁶ Lihat Pasal 31 Geneva Convention on Diplomatic Relations 1961.

- Tindakan-tindakan untuk mendapatkan kembali harta benda tidak bergerak yang semata-mata pribadi;
- 2. Tindakan-tindakan yang berkaitan dengan suksesi di mana mereka terlibat dalam kapasitas yang benar-benar pribadi; dan
- 3. Tindakan-tindakan yang berkaitan dengan suatu aktivitas profesi atau komersial pribadi yang dilakukan oleh mereka.

Namun, adanya kekebalan yang dimiliki perwakilan diplomatik ini tidak serta merta membebaskannya dari kekuasaan hukum negaranya sendiri atau negara pengirim ("sending state"). Bila perbuatan dilakukan oleh seorang diplomat maka negara penerima dapat melaporkan peristiwanya kepada pemerintah negara pengirim dan dalam kasus-kasus yang serius dapat memintanya kembali pulang dan selanjutnya diadili sesuai dengan peraturan perundang-undangan negara pengirim. Terhadap pelanggaran yang sangat serius, misalnya ikut serta berkomplot untuk menggulingkan pemerintahan yang sah maka negara penerima dapat menahan dan mengusirnya.177 Kendati pun seorang perwakilan diplomatik kebal terhadap hukum negara penerima tetapi mereka juga tetap harus mematuhi undang-undang dan peraturan negara setempat serta tidak melakukan kegiatan-kegiatan yang menjurus pada peraturan-peraturan setempat. pelanggaran itu, perlu diingat bahwa kekebalan yang dimiliki agen diplomatik bukan hanya meliputi diri mereka pribadi saja, akan tetapi juga mencakup pengiring mereka serta

¹⁷⁷ Boer Mauna, op.cit., hlm 551.

anggota-anggota keluarganya yang menjadi bagian dari rumah tangganya, tentunya dengan pengertian bahwa bagian dari rumah tangga tersebut bukan warganegara negara penerima.

Sementara, konsul-konsul asing tidak sama dengan perwakilan diplomatik. Golongan ini tidak kebal dari yurisdiksi negara penerima, kecuali imunitas itu secara khusus diberikan melalui traktat. Pembenaran atas imunitas konsuler tersebut dengan pertimbangan bahwa konsul tersebut ditugaskan untuk melaksanakan tugastugas konsuler sehingga untuk mencapai kinerja yang maksimal ia memerlukan imunitas dari yurisdiksi nasional setempat. Pengaturan spesifik mengenai hubungan konsuler diatur dalam Konvensi Jenewa 1963.

c. Kapal Milik Asing

Kapal milik asing dalam hal ini dapat dibedakan atas 2 (dua), yaitu kapal perang dan kapal negara. Guna membedakan manakah kapal perang¹⁷⁸ dan manakah kapal negara¹⁷⁹ maka dapat dilihat pada bendera kapalnya dan juga dokumen-dokumen kapal terkait, misalnya surat pelayaran yang dikeluarkan dan dan ditandatangani oleh otoritas negara pemilik kapal.

¹⁷⁸ Menurut Pasal 29 Konvensi Hukum Laut 1982, dinyatakan bahwa "kapal perang adalah suatu kapal yang dimiliki angkatan bersenjata suatu negara yang memakai tanda luar yang menunjukkan ciri khusus kebangsaan kapal tersebut, di bawah komando seorang perwira yang diangkat untuk itu oleh pemerintah negaranya dan yang namanya terdapat di dalam dinas militer atau daftar yang serupa itu dan yang diawaki oleh awak kapal yang tunduk kepada disiplin angkatan bersenjata regular".

¹⁷⁹ Kapal negara adalah suatu kapal swasta yang disewa oleh suatu negara untuk tujuan-tujuan publik, misalnya untuk mengangkut tentara atau pengangkutan peralatan perang.

Kapal perang dan kapal negara yang dioperasikan untuk tujuan non-komersial hanya tunduk pada yurisdiksi legislatif ("legislative jurisdiction") negara pantai, di mana memiliki konsekuensi bahwa kapal-kapal itu harus tunduk pada kewajiban untuk menghormati perundang-undangan negara pantai dan hukum kebiasaan internasional. Hal ini didasarkan bahwa pelabuhan adalah satu bagian dari perairan pedalaman dan oleh karenanya di perairan pedalaman ini suatu negara pantai memiliki kedaulatan penuh sehingga berhak menegakkan hukumnya. Akan tetapi harus dipahami bahwa yurisdiksi negara dalam hal ini terbatas. Setidaknya terdapat dua teori mengenai yurisdiksi terhadap kapal negara milik asing, yaitu: 180

- 1. Teori "Pulau Terapung" atau *The Floating Island Theory.* Teori menyatakan bahwa kapal negara harus dianggap sebagai bagian dari wilayah negara yang memilikinya. Menurut teori ini, yurisdiksi dari pengadilan teritorial negara lain dikesampingkan untuk semua tujuan apabila suatu tindakan dilakukan di atas kapal, atau terhadap pihak yang bersalah yang berada di atas kapal itu.
- 2. Pengadilan teritorial suatu negara memberikan kepada kapal dan awak kapal serta isi kapal tersebut imunitasimunitas tertentu yang tidak bergantung atas suatu teori objektif yang menyatakan bahwa kapal negara merupakan wilayah negara asing tetapi atas suatu implikasi yang diberikan oleh hukum teritorial lokal. Imunitas-imunitas lokal ini merupakan pengecualian dan sebaliknya dapat dihapuskan oleh negara pemilik kapal negara yang terkait.

¹⁸⁰ J. G. Starke, op.cit., hlm 293.

Sekalipun mempunyai kekebalan, akan tetapi kapal-kapal tersebut tetap diwajibkan untuk menghormati dan menaati peraturan perundang-undangan yang lazim berlaku di pelabuhan, seperti peraturan tentang karantina, saniter, dan bea cukai. Adapun apabila kapal-kapal itu lalai dalam menjalankan kewajibannya, protes diplomatik bahkan pengusiran menjadi sah dilakukan oleh negara pantai. Dalam konteks ini, pertanyaan lebih lanjut adalah yurisdiksi manakah yang berlaku atas tindak kejahatan yang terjadi di atas kapal milik asing namun sedang berada di pelabuhan negara pantai?

Persoalan kejahatan yang terjadi di atas kapal milik asing sekalipun berada di wilayah teritorial negara pantai, tetaplah menjadi yurisdiksi negara asing tersebut, dengan catatan bahwa korban kejahatan bukanlah warga negara pantai. Lain halnya bila awak kapal tersebut melakukan kejahatan di wilayah darat negara pantai, kemudian setelah melakukan kejahatannya ia kembali naik ke atas kapal. Bila hal itu terjadi maka mereka tidak lagi mendapat imunitas dari negara kapal, melainkan negara pantai.

d. Angkatan Bersenjata Negara Asing

Pada dasarnya, angkatan bersenjata negara asing yang sedang bertugas di negara penerima menikmati imunitas terbatas dari yurisdiksi teritorial negara tersebut. Besarnya imunitas yang diberikan kepada angkatan bersenjata negara asing tersebut ditentukan oleh perjanjian tegas antara negara tuan rumah dan negara pengirim yang mengatur syarat-syarat mengenai masuknya angkatan bersenjata di wilayah itu. Menurut perkembangan Hukum Internasional, terdapat dua

cakupan penerimaan atau izin negara teritorial terhadap angkatan bersenjata asing, yaitu: 181

- 1. Komandan angkatan bersenjata yang ditempatkan itu dan mahkamah militernya memiliki yurisdiksi eksklusif terhadap tindak pelanggaran yang dilakukan oleh anggota-anggotanya di dalam wilayah di mana angkatan bersenjata tersebut ditempatkan, atau dalam hubungannya dengan masalah-masalah disiplin, atau terhadap tindakan pelanggaran yang dilakukan di luar wilayah penempatannya, dengan ketentuan anggota yang bersangkutan sedang dalam tugas.
- 2. Angkatan bersenjata yang ditempatkan dan anggotaanggotanya kebal dari yurisdiksi lokal, baik perdata pidana, berkenaan dengan maupun masalah administrasi intern angkatan bersenjata itu, atau yang perlu dimasukkan dalam pelaksanaan angkatan bersenjata tugas-tugas itu (seperti menggunakan membawa senjata, kendaraan bermotor, dan sebagainya). Di lain pihak, apabila anggota angkatan bersenjata itu melakukan tindakan pelanggaran di luar kawasan penempatannya dan terlibat dalam kegiatan non-militer, maka pada saat itu mereka tunduk pada yurisdiksi negara setempat.

Berdasarkan pemaparan diatas, terlihat bahwa dalam struktur angkatan bersenjata terdapat komando yang jelas, dimana komandan diberi kewenangan khusus untuk mengatur dan mengendalikan anggota-anggotanya selama menjalankan tugas. Jadi, bila terjadi suatu

¹⁸¹ *Ibid*, hlm 299.

pelanggaran yang dilakukan anggota angkatan bersenjata selama menjalan tugasnya, maka pertanggungjawaban dapat dimintakan kepada komandannya. Akan tetapi hal ini tidak berlaku bila pelanggaran anggota terjadi tidak sedang dalam kapasitasnya sebagai anggota bersenjata.

e. Organisasi-Organisasi Internasional di Suatu Negara

Lembaga atau organisasi internasional memperoleh imunitas dari yurisdiksi teritorial negara penerima. Pada umumnya status organisasi tersebut beserta wakil-wakilnya telah ditetapkan dalam konvensi mengenai hak-hak istimewa dan kekebalan atau dalam khusus kesepakatan-kesepakatan yang mempunyai beberapa kesamaan dengan status para diplomatik. Namun, fungsi mereka jauh berbeda dari para pejabat diplomatik biasa karena dibatasi oleh prinsip spesialitas yang walaupun dalam praktiknya sering dianggap sebagai duta besar seperti duta besar lainnya. 182

- 1. Yurisdiksi Negara di Wilayah Laut dan Ruang Udara
- a. Wilayah Laut

Wilayah laut dapat dikatakan sebagai wilayah kontroversial sebab sejarah mencatat banyak sekali sengketa-sengketa internasional yang berasal dari konflik wilayah laut, baik itu terkait batas-batas wilayah maupun pemanfaatan kekayaan alam yang terkandung di dalamnya. Persoalan-persoalan tersebut timbul karena ketidakjelasan batas-batas yurisdiksi wilayah laut suatu negara. Wilayah laut sendiri secara kasat mata memang tidak dapat dibagi-bagi karena merupakan karya alamiah llahi yang saling bersambung melintasi negara-negara.

¹⁸² Boer Mauna, op.cit., hlm 572.

Laut juga merupakan jalan raya yang menghubungkan seluruh pelosok dunia. Melalui laut, masyarakat dari berbagai bangsa mengadakan segala macam pertukaran dari komoditi perdagangan hingga ilmu pengetahuan. Di samping mempunyai arti komersial dan strategis, laut juga merupakan sumber makanan bagi umat manusia. Laut menjadi semakin penting bila mengingat hasil riset yang menunjukkan bahwa ²/₃ permukaan bumi terdiri atas wilayah laut. ¹⁸³

Menyadari urgensi tersebut, masyarakat internasional secara perlahan mulai membangun konsepsi Hukum Laut yang bertujuan untuk mengatur kegunaan rangkap dari laut, yaitu sebagai jalan raya dan sebagai sumber kekayaan serta sebagai sumber tenaga. Setelah melalui perjuangan pembentukan suatu konsep yang bersifat universal, maka akhirnya pada tanggal 30 April 1982 diterimalah Konvensi PBB tentang Hukum Laut, yang juga lazim dikenal dengan nama *United Nations Convention on Law of the Sea* (selanjutnya disingkat UNCLOS) 1982.

Wilayah laut menurut UNCLOS 1982 dapat dibedakan atas beberapa wilayah, yaitu Laut Teritorial, Zona Tambahan, Zona Ekonomi Eksklusif, dan Laut Lepas.

1. Laut Teritorial dan Zona Tambahan

Kedaulatan negara pantai selain di wilayah daratan dan perairan pedalamannya, juga meliputi laut teritorial beserta ruang udara diatasnya dan dasar laut serta lapisan tanah di bawahnya. Laut wilayah sendiri dapat diartikan sebagai bagian yang paling dekat dari pantai yang pada umumnya dianggap sebagai lanjutan dari daratannya dan di atas mana

¹⁸³ *Ibid*, hlm 306.

¹⁸⁴ Alma Manuputty, dkk, Hukum Internasional, (Depok: Rech-ta, 2008), hlm 93.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

negara pantai tersebut mempunyai kedaulatan. 185 Jadi, terlihat dengan jelas bahwa hanya pada laut teritorial inilah suatu negara memiliki Hak Kedaulatan Penuh, dengan kata lain di wilayah ini negara memiliki yurisdiksi penuh.

Pada mulanya, doktrin yang digunakan untuk menunjukkan penguasaan atas wilayah laut teritorial ini adalah Doktrin Hak Milik. Namun, konsep ini dirasa terlalu mengeksklusifkan negara pantai karena berdasarkan terminologi ini, negara pantai dimungkinkan membuka dan menutup jalur laut wilayah sesukanya dan melakukan monopoli pemanfaatan hasil laut. Hal ini dipandang akan menimbulkan kesenjangan bagi negaranegara yang kurang beruntung, yaitu negara hanya sedikit bahkan tidak memiliki wilayah laut, seperti Laos. Oleh karena itu, maka disusunlah konsep Hak Kedaulatan, yang tetap membuka akses bagi negara lain untuk melintasi wilayah laut teritorial negara pantai pada jalur-jalur yang telah ditentukan oleh negara pantai. Di Indonesia, kita mengenal ALKI (Alur Laut Kepulauan Indonesia) yang terdiri atas tiga lintasan, yaitu ALKI I, ALKI II, dan ALKI III.

Berdasarkan Pasal 2 ayat (2) UNCLOS 1982, dinyatakan bahwa "kedaulatan suatu negara pantai meliputi ruang udara di atas laut wilayah serta dasar laut dan lapisan tanah di bawahnya". Berdasarkan ketentuan tersebut, pada pembahasan selanjutnya akan Penulis paparkan mengenai yurisdiksi di wilayah udara negara pantai. Setiap negara pantai memiliki kewenangan dalam melaksanakan kedaulatannya, sebagai berikut: 186

¹⁸⁵ Boer Mauna, op.cit., hlm 365.

¹⁸⁶ Lihat Pasal 25 UNCLOS 1982. Lihat dalam Boer Mauna, *Ohlm.cit*, hlm 374-375.

- Mengambil langkah-langkah yang diperlukan dalam laut wilayahnya untuk mencegah lintas yang tidak damai;
- Mempunyai hak untuk mengambil langkah-langkah yang diperlukan untuk mencegah pelanggaran apapun terhadap persyaratan yang telah ditentukan bagi masuknya kapal ke perairan pedalaman atau untuk melakukan persinggahan di pelabuhan;
- c. Menangguhkan sementara bagian tertentu laut teritorialnya bagi lintas damai kapal asing apabila penangguhan demikian untuk perlindungan keamanannya.

Berdasarkan ketentuan UNCLOS 1982, batas laut teritorial suatu negara pantai tidak lebih dari 12 mil yang diukur dari garis pangkal normal. Selain mengenai Laut Teritorial, pada Pasal 33 ayat (2) UNCLOS 1982 juga diatur ketentuan mengenai Zona Tambahan. Zona ini tidak boleh melebihi 24 mil laut dari garis pangkal dari mana lebar laut wilayah diukur. Bila disimak dengan seksama, total dari garis pangkal hingga zona tambahan sepanjang 24 mil, dikurangi 12 mil panjang laut teritorial, maka panjang zona tambahan juga tidak bisa lebih dari 12 mil.

1) Zona Ekonomi Eksklusif (ZEE)

ZEE merupakan suatu zona yang berdampingan dengan laut teritorial. Berdasarkan Pasal 57 UNCLOS 1982, lebar ZEE tidak boleh melebihi 200 mil laut dari garis pangkal dari mana lebar laut wilayah diukur. Jadi, sebenarnya lebar ZEE ini hanya sekitar 188 mil setelah dikurangi 12

¹⁸⁷ Alma Manuputty dkk, op.cit., hlm 94.

mil lebar laut teritorial. Pada ZEE tidak lagi berlaku hak kedaulatan penuh negara pantai sebagaimana pada laut teritorial, akan tetapi berlaku Hak Berdaulat. Pasal 56 UNCLOS menyatakan bahwa negara pantai diberikan hak juga keperluan eksplorasi, eksploitasi, konservasi, dan pengelolaan sumber kekayaan alam laut. Namun, UNCLOS juga menegaskan bahwa semua negara, baik berpantai atau tidak, tetap dapat mempergunakan bagian laut tersebut sebagai laut lepas dengan kebebasan-kebebasan yang telah diatur secara limitatif dalam Pasal 87 UNCLOS 1982.

2) Laut Lepas

Prinsip hukum yang berlaku di wilayah laut lepas adalah prinsip kebebasan, dalam artian laut lepas dapat digunakan oleh negara manapun, baik itu meliputi kebebasan berlayar; kebebasan penerbangan; kebebasan untuk memasang kabel dan pipa bawah laut dengan mematuhi ketentuan Bab VI Konvensi; kebebasan untuk membangun pulau buatan dan instalasi-instalasi lainnya; kebebasan untuk menangkap ikan dengan tunduk pada persyaratan yang tercantum dalam Bab II; serta kebebasan riset ilmiah. Selain itu, patut diingat pula bahwa laut lepas hanya dapat digunakan untuk tujuan-tujuan damai.

¹⁸⁸ Lihat Pasal 87 UNCLOS 1982. Bandingkan dalam Boer Mauna, op.cit., hlm 313-314.

b. Wilayah Udara

Selain wilayah darat dan laut, negara juga memiliki yurisdiksi atas wilayah udaranya. Menurut ketentuan Pasal 1 Konvensi Chicago 1944, yang merupakan penyempurna Konvensi Paris 1919, dikatakan bahwa "the contracting parties recognize that every state has complete and exclusive sovereignty over the airspace above its territory", yang dapat diartikan "negara-negara pihak mengakui bahwa tiap-tiap negara mempunyai kedaulatan penuh dan eksklusif atas ruang udara yang terdapat di atas wilayahnya".

Penerimaan konsep ini diakui oleh masyarakat internasional, yang mana pengakuan kedaulatan di udara tidak terbatas pada negara anggota melainkan juga berlaku terhadap bukan negara anggota Konvensi Chicago 1944. Hal ini jelas dengan adanya istilah *every state* pada pasal di atas. Lebih lanjut walaupun tidak secara tegas disebutkan, akan tetapi semua negara mengakui bahwa tidak ada negara mana pun yang berdaulat di atas laut lepas (*"high seas"*).

Konvensi Chicago 1944 lebih lanjut tidak mengatur batasan ruang udara, akan tetapi definisi ruang udara menurut penafsiran *Permanent Court of International Justice* diartikan sebagai *the natural meaning of the term is its geographical meaning* atau ruang dimana terdapat udara atau air. Selain itu, ada juga yang mendefinisikan batas wilayah udara sampai sejauh pesawat sipil biasa dapat terbang dengan menggunakan kekuatan aerodinamis atau gaya gesek partikel udara. 190 Lingkup yurisdiksi teritorial suatu negara diakui dan diterima

¹⁸⁹ Martono, Pengantar Hukum Udara Nasional dan Internasional, (Jakarta: PT RajaGrafindo Persada, 2007), hlm 19.

¹⁹⁰ *Ibid*, hlm 19.

oleh negara anggota Konvensi Chicago 1944 terus ke atas sampai tidak terbatas dan ke bawah pusat bumi sepanjang dapat dieksploitasi. Adapun konsekuensi dari kedaulatan penuh yang dimiliki negara kolong adalah negara tersebut dapat melakukan pengawasan penuh atas wilayah udaranya, termasuk memerintahkan pesawat asing yang dicurigai mengancam keamanan dalam negeri untuk segera mendarat. Selain itu, setiap pesawat yang hendak memasuki wilayah udara teritorial negara kolong juga harus meminta izin terlebih dahulu.

Konsekuensi terbesar dengan meningkatnya volume, jangkauan, dan frekuensi lalu lintas udara internasional di mana jumlah pesawat udara semakin membengkak, adalah semakin meningkatnya pula persoalan-persoalan yurisdiksi pelik terkait dengan tindak pidana yang dilakukan di dalam pesawat udara dalam penerbangan., misalnya pembajakan pesawat udara ("hijacking") dan tindakan terorisme melalui media pesawat udara. Menyadari hal tersebut, maka masyarakat internasional mulai melakukan berbagai upaya, salah satunya dengan membentuk regulasi-regulasi agar pelaku kejahatan bisa segera diadili sebab jangan sampai karena benturan yurisdiksional pelaku tersebut bisa lepas dari jeratan hukum.

Konvensi pertama yang lahir terkait tindak pidana yang dilakukan di dalam pesawat udara adalah Konvensi Tokyo 1963 di bawah naungan *International Civil Aviation Organisation* (biasa disingkat ICAO). Adapun tujuan utama Konvensi Tokyo 1963 adalah melindungi pesawat udara, orang, dan barang yang diangkut untuk menjamin keselamatan penerbangan. Persoalan yurisdiksi ini diatur dalam Bab II Pasal 3 dan 4 Konvensi Tokyo 1963. Dikatakan yurisdiksi yang berlaku terhadap tindak pidana pelanggaran dan kejahatan adalah

negara pendaftar pesawat udara. Jadi, Konvensi Tokyo 1963 telah melakukan unifikasi yurisdiksi yang dapat mencegah conflict of jurisdiction, mengingat transportasi udara mempunyai karakteristik internasional yang tidak mengenal secara pasti batas yurisdiksi suatu negara. Kemudian, 7 (tujuh) tahun kemudian, lahirlah Convention for the Suppression of Unlawful Seizure of Aircraft atau yang lazim dikenal sebagai Konvensi The Hague 1970. Konvensi ini bertujuan untuk melengkapi kekurangan Konvensi Tokyo 1963. Intinya dari konvensi-konvensi tersebut menegaskan bahwa yurisdiksi yang berlaku pada saat terjadinya kejahatan dengan pesawat udara adalah negara pendaftar pesawat udara ("registered state").

II. Yurisdiksi Kuasi Teritorial

Yurisdiksi Kuasi Teritorial adalah yurisdiksi yang diterapkan bukan pada wilayah teritorial, melainkan pada wilayah yang bersambungan atau berbatasan dengan wilayah teritorial tersebut. 192 Prinsip ini berlaku untuk wilayah-wilayah di mana tidak terdapat hak kedaulatan negara, seperti pada laut lepas dan ruang angkasa. Sebagaimana yang telah dijelaskan sebelumnya, pada laut lepas berlaku prinsip kebebasan yang artinya setiap negara memiliki hak yang sama untuk memanfaatkan wilayah tersebut. Akan tetapi, negara bendera kapal dipandang memiliki yurisdiksi atas kapalnya tersebut, misalnya saja di sebuah kapal berbendera Indonesia sedang berlayar di Samudera Pasifik, yang merupakan laut lepas. Menurut ketentuan Hukum Internasional, kapal itu tetap tunduk pada yurisdiksi nasional negara Indonesia sehingga apapun

¹⁹¹ *Ibid*, hlm 50.

¹⁹² Adji Samekto, op.cit., hlm 65.

yang terjadi pada kapal itu maupun yang terjadi pada awakawak kapal atau barang-barang muatannya menjadi tanggung jawab penuh Indonesia selaku negara bendera kapal.

Demikian pula halnya dengan pesawat ruang angkasa, di mana negara peluncur (*"launching state"*)¹⁹³ memiliki tanggung jawab mutlak untuk membayar kompensasi atas kerugian yang disebabkan oleh benda-benda angkasa yang diluncurkannya, sebagaimana yang diatur dalam Pasal 2 *Liability Convention* 1972.¹⁹⁴ Persoalan yurisdiksi di laut lepas dan ruang angkasa akan dijelaskan secara lebih rinci pada mata kuliah Hukum Laut Internasional dan Hukum Ruang Angkasa.

III. Yurisdiksi Personal atau Individu

Bila yurisdiksi teritorial menekankan fokusnya pada wilayah, lain halnya dengan yurisdiksi personal yang menekankan fokusnya pada individu. Yurisdiksi personal merupakan istilah yang menunjuk pada yurisdiksi yang berlaku atas orang ataupun benda yang ditundukkan oleh hukum nasional yang bersangkutan. Dengan kata lain, yurisdiksi personal merupakan otoritas yang ditimbulkan oleh kedaulatan negara atas individu-individu berdasarkan proteksi atau perlindungan. Paham yurisdiksi ini ditekankan pada pendapat bahwa kedaulatan negara tetap akan membawahi subjek yang

peluncur bukan saja negara yang meluncurkan benda-benda angkasa itu akan tetapi juga dapat dikategorikan sebagai negara peluncur, yaitu negara yang mendapat kesempatan ikut meluncurkan objek ruang angkasa, negara yang wilayahnya atau yang memberikan fasilitas dari mana objek ruang angkasa tersebut diluncurkan, turut bertanggung jawab atas kerugian yang disebabkan oleh peluncuran itu. *Infra note* 51, hlm 41.

¹⁹⁴ Juajir Sumardi, Hukum Ruang Angkasa (Suatu Pengantar), (Jakarta: PT Pradnya Paramita, 1996), hlm 41.

ditundukkannya ke mana pun subjek hukum itu berada. 195 Kualitas ini dapat membenarkan suatu negara atau negara negara menjalankan jurisdiksinya apabila orang itu berada dalam kekuasaan negara, dan proses peradilah dapat di laksanakan terhadapnya.

Perkembangan praktik hukum internasional membagi lagi tipe yurisdiksi ini ke dalam dua teori, yaitu:

1. Yurisdiksi Personal Aktif (Prinsip Nasionalitas Aktif)

Prinsip ini menekankan bahwa semua negara memiliki hak untuk memberlakukan yurisdiksinya atas setiap warga negaranya dimanapun ia pergi. Adapun sistem hukum pidana Indonesia menganut prinsip ini sehingga setiap orang yang melakukan kejahatan di wilayah hukum RI dan kemudian melarikan diri ke luar negeri, dapat ditangkap dengan dasar yurisdiksi personal aktif. 196

Apabila diperhatikan dengan seksama, pola pemulangan dengan dasar yurisdiksi personalitas aktif sedikit mirip dengan yurisdiksi teritorial subjektif. Letak perbedaan kedua jenis yurisdiksi tersebut adalah pada sudut pandangnya. Pada yurisdiksi personalitas yang dilihat sebagai faktor utama berlakunya yurisdiksi negara asal didasari pada faktor individunya, yang merupakan warga negara asal sedangkan pada yurisdiksi teritorial subjektif, alasan utama dimintakan pemulangan tersangka karena ia melakukan kejahatan di wilayah teritorial

¹⁹⁵ Adji Samekto, op.cit., hlm 62.

¹⁹⁶ *Ibid*, hlm 62.

negara asal, terlepas dari atributnya sebagai seorang warga negara.

Selain itu, hal yang perlu diingat pula bahwa negara tidak wajib menyerahkan warga negaranya yang telah melakukan tindak pidana di luar negeri. Diberikannya hak tersebut pada negara karena adanya pertimbangan bahwa setiap negara mempunyai kewajiban untuk melindungi warga negaranya dimanapun ia berada. Hal ini juga merupakan salah satu asas ekstradisi yaitu Asas Tidak Menyerahkan Warga Negara Sendiri.

2. Yurisdiksi Personal Pasif (Prinsip Nasionalitas Pasif)

Yurisdiksi Personal Pasif merupakan tipe yurisdiksi yang mencerminkan dengan bagaimana suatu negara berkewajiban melindungi negaranya kapanpun dan dimanapun warga berada. Prinsip ini membenarkan negara untuk menjalankan yurisdiksi apabila seorang warga kerugian negaranya menderita oleh tindakan pihak asing. Adapun dasar pembenar prinsip nasionalitas pasif ini adalah bahwa setiap negara berhak melindungi warga negaranya di luar negeri, dan apabila negara teritorial di mana tindak pidana itu terjadi tidak menghukum orang yang menyebabkan kerugian tersebut maka negara asal korban berwenang menghukum tindak pidana itu apabila orang itu berada di wilayahnya. 197 Mengapa negara asal hanya bisa mengadili pelaku bila ia

¹⁹⁷ J. G. Starke, op.cit., hlm 303.

berada di wilayah negara asal? Kembali lagi harus diingat bahwa berdasarkan ketentuan Hukum Internasional, tidak dimungkinkan suatu negara memberikan warga negaranya kepada negara lain untuk diadili. Jadi, kesempatan untuk mengadili warga negara lain oleh negara asal hanya dapat terjadi bila kebetulan pelaku kejahatan itu berada di wilayah negara asal.

Akan tetapi, pada prakteknya seringkali negara asal pelaku kejahatan keberatan bila negara asal korban ingin terlibat untuk mengadili kasus yang sedang terjadi, biasanya mereka menyatakan bahwa ketertiban umum negara asal korban tidak terganggu hanya karena satu warganya itu dirugikan.

IV. Yurisdiksi Perlindungan

Berdasarkan prinsip yurisdiksi perlindungan, dibenarkan untuk melaksanakan yurisdiksinya negara terhadap warga negara asing bilamana warga tersebut melakukan kejahatan di luar negeri yang dipandang dapat mengancam kepentingan keamanan, integritas, kemerdekaan, atau kepentingan ekonomi yang vital. Adapun latar belakang lahirnya prinsip ini didasari oleh adanya kekhawatiran negara korban mengenai mekanisme yurisdiksi yang mungkin saja tidak diatur di negara tempat kejahatan itu dilakukan atau bahkan bisa saja perbuatan merugikan itu tidak digolongkan sebagai kejahatan di negara setempat. Menyadari hal itu, maka ketentuan Hukum Internasional mencoba mengakomodasi kemungkinan-kemungkinan terburuk melalui lahirnya prinsip yurisdiksi perlindungan ini.

Setidaknya terdapat dua alasan yurisdiksi perlindungan ini dibenarkan oleh ketentuan hukum internasional, yaitu:¹⁹⁸

- 1. Akibat tindak pidana itu sangat besar bagi negara terhadap mana pidana itu dituju.
- 2. Apabila yurisdiksi tidak dilaksanakan terhadap tindak pidana tersebut maka dikhawatirkan pelaku tindak pidana itu dapat lolos dari penghukuman karena di negara di mana tindak pidana itu dilakukan ("lex loci delicti") perbuatan itu bukanlah pelanggaran terhadap hukum setempat atau karena ekstradisi akan ditolak dengan alasan tindak pidana itu bersifat politis.

Namun, pada prakteknya, prinsip ini juga tidak sepenuhnya dapat diterima semua negara. Negara-negara pada umumnya menyatakan keberatan dengan argumen bahwa setiap negara pasti memiliki kepentingan-kepentingan tersendiri sehingga sangat sulit memutuskan tindakan mana yang membahayakan keamanan nasional atau keadaan finansial negara tersebut. Sebagian besar negara mempunyai ketakutan bahwa prinsip hanya akan digunakan sebagai tameng untuk mengadili warga negara lain sewenang-wenang.

V. Yurisdiksi Universal

Sesungguhnya hingga saat ini belum terdapat suatu konsep yurisdiksi universal yang dapat diterima secara universal. Namun, bagaimanapun juga hal tersebut tidak menghalangi masyarakat internasional untuk membuat definisi yurisdiksi universal. Salah satunya seperti yang diungkapkan oleh Reydams di bawah ini:

¹⁹⁸ *Ibid*, hlm 304.

"Universal jurisdiction means that there is no links of territory or nationality between the State and the conduct or offender, nor is the State seeking to protect its security or credit". 199

Jadi, menurut beliau, yurisdiksi universal dapat diartikan bahwa tidak ada hubungan wilayah maupun kewarganegaraan antara negara dan pelaku kejahatan, dan tidak terdapat satupun negara yang ingin memberikan perlindungan keamanan kepada pelaku tersebut. Senada dengan Reydams, Meron mendefinisikan yurisdiksi universal sebagai suatu keadaan di mana negara tidak memiliki keterkaitan wilayah, nasionalitas (baik aktif maupun pasif), maupun prinsip perlindungan yang diizinkan oleh Hukum Internasional, sehingga negara tersebut dapat menuntut siapa saja yang melakukan pelanggaran tertentu di wilayahnya.²⁰⁰ Sementara, Paragraf 404 Restatement (Third) of the Foreign Relations Law of the United States juga menyediakan pandangan sejalan. Tipe yurisdiksi ini menyatakan "that any state or every state is permitted to criminalize the conduct on question", yang kurang lebih dapat diartikan bahwa yurisdiksi ini mengizinkan semua atau setiap negara untuk mengadili setiap tindakan kriminal, tentu saja sesuai dengan ketentuan internasional.

Intinya, menurut prinsip ini setiap negara mempunyai yurisdiksi untuk menerapkan hukum nasionalnya sekalipun tindak kejahatan itu terjadi di luar wilayahnya, dilakukan bukan oleh warga negaranya, bahkan ketika negara itu tidak dirugikan melalui tindakan tersebut.²⁰¹ Menurut *Princeton Principles*

¹⁹⁹ Roger O'Keefe, Universal Jurisdiction: Clarifying the Basic Concept, (New York: Oxford University Press, 2004), hlm. 745.

²⁰⁰ *Ibid*.

²⁰¹ Supra note 5, hlm 1.

on Universal Jurisdiction, yurisdiksi universal berkaitan luas dengan kewenangan yang dimiliki negara untuk menghukum kejahatan-kejahatan terlepas di mana kejahatan dilakukan dan siapa yang melakukan kejahatan tersebut. Jadi, yurisdiksi ini lahir tanpa melihat dimana dan siapa pelaku kejahatan.

a. Ruang Lingkup

Pada awalnya, prinsip yurisdiksi universal lahir disebabkan karena tidak adanya badan peradilan internasional yang khusus mengadili kejahatan yang dilakukan orang-perorangan (individu). Namun, seperti yang kita ketahui bersama bahwa saat ini telah hadir *International Criminal Court* (biasa disingkat ICC) yang memiliki yurisdiksi terhadap individuindividu yang melakukan kejahatan.

Ruang lingkup atau cakupan yurisdiksi universal ini juga tidak memiliki batasan yang jelas, bahkan oleh PBB sekalipun. Namun, terdapat karakteristik untuk menentukan apakah kejahatan itu masuk batasan yurisdiksi universal atau tidak yaitu apakah kejahatan itu termasuk delik jure gentium atau tidak, serta merupakan norma erga omnes atau tidak. Namun, tetap harus diingat bahwa kategorisasi kejahatan internasional sesuai jus cogens maupun erga omnes tidak berarti bahwa negara langsung dapat menerapkan yurisdiksi universal begitu saja, tetapi juga harus berdasarkan kesepakatan atau konsensus negara-negara.

Kejahatan dengan kategori jure gentium dapat diartikan sebagai tindak pidana yang bertentangan dengan hukum dunia atau tidak pidana yang dikutuk oleh seluruh umat manusia (demikian dikenal istilah "Hostis Humanis Generis" atau musuh bersama umat manusia). Sedangkan, obligatio erga omnes dalam Hukum Internasional digunakan sebagai istilah yang menunjukkan sebuah kewajiban hukum yang dimiliki oleh

negara terhadap masyarakat internasional secara keseluruhan.

Menurut M. Cherif Bassiouni, prinsip *erga omnes* adalah prinsip yang bersifat *inderogable* atau tidak dapat dikurangi atau dihapuskan oleh siapapun juga. Konsep *erga omnes* dan *jus cogens* sering beliau ibaratkan sebagai dua sisi mata uang, karena kewajiban *erga omnes* mengalir dari *jus cogens*.²⁰² Kriteria utama hingga lahirnya kewajiban ini adalah *"the obligations of a state towards the international community as a whole"*. Perihal kapankah suatu norma bisa menjadi *jus cogens* atau mengapa dan kapan bisa menjadi *erga omnes* tidak pernah dijelaskan secara tegas, baik oleh PCIJ maupun ICJ, tidak juga oleh yurisprudensi-yurisprudensi pengadilan.²⁰³ Namun, satu hal yang jelas bahwa tujuan pemberian yurisdiksi universal adalah untuk menjamin bahwa tidak ada tindak pidana yang lepas dari jangkauan hukum.

Kontroversi seputar kejahatan mana sajakah yang masuk ke dalam kompetensi yurisdiksi kriminal masih terus diperbincangkan hingga kini. Apakah semua kejahatan internasional ("international crimes") padanya dapat berlaku yurisdiksi universal? Jawabannya, "universal jurisdiction doesn't apply to all international crimes, but rather to a very limited category of offences", artinya tidak semua kejahatan internasional masuk yurisdiksi universal melainkan hanya beberapa pelanggaran terbatas saja. 204 Oleh karena itu, harus pula dipahami bahwa kejahatan yang secara moral patut dicela tidak dapat dipersamakan dengan yurisdiksi universal.

²⁰² Cherif Bassiouni, op.cit., hlm. 270.

²⁰³ Ibid, hlm 271.

²⁰⁴ Supra note 5, hlm 2.

Pertanyaannya yang timbul kemudian adalah jenis kejahatan apa sajakah yang masuk yurisdiksi universal ini? Menurut J.G. Starke, saat ini hanya ada dua kasus yang masuk yurisdiksi universal, yaitu pembajakan ("piracy") dan kejahatan perang ("war crimes").²⁰⁵ Berikut akan diuraikan satu persatu:

A. Kejahatan Pembajakan di Laut ("Piracy")

Pembajakan di laut adalah kejahatan internasional tertua di dunia.²⁰⁶ Bahkan pembajakan di laut merupakan satu-satunya tindak kriminal murni yang ditetapkan sebagai kejahatan internasional. Buktinya pada tanggal 14 September 1937 telah berhasil lahir Perjanjian Nyon yang secara eksplisit menyatakan bahwa *piracy* sebagai salah satu terorisme. Namun, tidak terdapat satu ketentuan pun yang menegaskan pelaku tindakan *piracy* sebagai subjek hukum pidana internasional.²⁰⁷

Kemudian, seiring berjalannya waktu pembajakan menjadi contoh yang representatif di dalam hukum pidana internasional yang telah mempertemukan dan sekaligus membuktikan relevansi interelasi antara hukum (pidana) nasional dan hukum internasional. Hal lain yang juga harus bisa dibedakan adalah antara pembajakan laut ("piracy") dan perompakan di laut ("sea robbery"). Kedua istilah tersebut dapat dikatakan sama hakikatnya, dan kadang secara bersamaan digunakan untuk menyebutkan suatu peristiwa tindak kekerasan di laut, tetapi sebenarnya mempunyai perbedaan mengenai wilayah yurisdiksi tempat terjadinya (locus delicti) tindak kekerasan di laut tersebut. Pembajakan di laut mempunyai dimensi internasional karena biasanya digunakan untuk menyebutkan tindak kekerasan

²⁰⁵ J. G. Starke, op.cit., hlm 304.

²⁰⁶ Eddy O. S. Hiariej, op.cit., hlm 63.

²⁰⁷ Romli Atmasasmita, op.cit.., hlm 10.

yang dilakukan di laut lepas sedangkan perompakan di laut lebih berdimensi nasional karena merupakan tindak kekerasan di laut yang dilakukan di bawah yurisdiksi suatu negara, dengan tujuan yang berbeda pula, meskipun juga dapat mencakup lingkup transnasional.²⁰⁸ Dengan demikian penanganan kedua jenis kejahatan tersebut juga tentu berbeda.

Setelah memahami perbedaan antara pembajakan dan perompakan, maka dengan mudah akan diketahui bahwa ketentuan mengenai kejahatan pembajakan masuk ke dalam rezim Hukum Laut Internasional. Pengaturan tersebut terdapat dalam Pasal 100 hingga Pasal 107 UNCLOS 1982. Penegasan status yurisdiksi universal terhadap kejahatan pembajakan di laut tertuang dalam Pasal 105, yang menyatakan:²⁰⁹

"On the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board. The courts of the State which carried out the seizure may decide upon the penalties to be imposed, and may also determine the action to be taken with regard to the ships, aircraft or property subject to the rights of third parties acting in good faith."

Berdasarkan ketentuan di atas, terlihat jelas bahwa wilayah kejahatan pembajakan di laut haruslah berada di laut lepas ("high seas") atau paling tidak diluar batas yurisdiksi teritorial negara pantai itu. Ketentuan pasal 105 di atas juga menegaskan kewenangan setiap negara ("every state") untuk

²⁰⁸ Tri Setyawanta, *Pengaturan Hukum Penanggulangan Pembajakan dan Perompakan Laut di Wilayah Indonesia*, Jurnal Media Hukum, Vol. V. No.1 (Januari-Maret, 2005).

²⁰⁹ Lihat Pasal 105 UNCLOS 1982.

menangkap kapal pembajak atau pesawat terbang pembajak, atau sebuah kapal laut atau pesawat terbang yang dibajak di bawah kekuasaan pembajak, serta menahan penumpang dan menahan harta benda di atas kapal.²¹⁰ Pengadilan negara yang menangkap pelaku kejahatan pembajakan itu dapat menetapkan pidana sesuai hukum nasionalnya.

Di sisi lain, apabila tindakan-tindakan pembajakan di laut dilakukan oleh suatu negara yang berdaulat maka tindakan tersebut bukan termasuk dalam kejahatan internasional yang pelakunya harus ditangkap, melainkan dimasukkan dalam kategori *international torts* (kesalahan internasional) dan menimbulkan pertanggungjawaban negara. Sedangkan apabila pembajakan itu dilakukan oleh organ negara, tanpa otorisasi negaranya, maka negara asal bajak laut, baik dengan kapal maupun pesawat udara tidak berhak melakukan perlindungan dari tindakan negara lain yang akan menerapkan yurisdiksi universal terhadap warga negaranya yang menjadi bajak laut.²¹¹

Sejak dahulu kala, pembajakan di laut ini telah menjadi musuh banyak negara sehingga dikenal istilah *piracy jure gentium*. Keberadaan Pasal 105 UNCLOS 1982 ini (dahulu dimuat dalam Pasal 19 UNCLOS 1958) semakin memperkuat kedudukan *piracy* sebagai *hostis humanis generis* sehingga negara mana pun yang berhasil menangkap pelaku kejahatan tersebut dapat menerapkan pidana nasionalnya. Hal ini dilakukan untuk memberi perlindungan kepentingan masyarakat dunia.

²¹⁰ Romli Atmasasmita, op.cit., hlm 37.

²¹¹ Adji Samekto, op.cit., hlm 65-66.

B. Kejahatan Perang ("War Crimes")

Pada awalnya, terhadap pelaku kejahatan perang juga diterapkan prinsip universalitas. Namun, sejak berjalannya fungsi Mahkamah Pidana Internasional (ICC) pada tahun 2002, yurisdiksi atas pelaku pelanggaran kejahatan perang mengalami pergeseran. Menurut ketentuan Hukum Humaniter, pada prinsipnya setiap kombatan yang telah jatuh ke tangan musuh ("hors de combat") memiliki hak untuk mendapat perlindungan dari negara asalnya. Akan tetapi, apabila mereka terbukti telah melakukan kejahatan perang selama masa perang maka pihak penguasa musuh dapat mengadili mereka dan memberlakukan hukuman kepadanya, sama halnya pada pembajakan di laut. 213

Sebagaimana yang telah disebutkan sebelumnya, sejak kehadiran ICC, maka sistem pengadilan terhadap kejahatan perang semakin komprehensif. Berbeda dengan ICJ, ICC memainkan perannya dalam menuntut dan mengadili individuindividu yang bertanggung jawab atas kejahatan-kejahatan berat terhadap kemanusiaan yang menjadi keprihatinan masyarakat internasional. Lantas, yurisdiksi manakah yang berlaku? Apakah yurisdiksi negara penguasa atau ICC?

Guna menjawab pertanyaan di atas, maka harus melihat prinsip apa yang berlaku dalam tubuh ICC. Salah satu prinsip utama ICC adalah Prinsip Komplementer ("complementary principle"). Menurut prinsip ini, ICC berperan sebagai pelengkap dari yurisdiksi pidana nasional, yang artinya ICC hanya bisa menangani perkara tersebut apabila negara penguasa dinilai

²¹² Berdasarkan Pasal 5 Statuta ICC, yurisdiksi ICC meliputi tindak pidana genosida; kejahatan terhadap kemanusiaan; kejahatan perang; dan agresi.

²¹³ Adji Samekto, *Loc.cit*.

tidak mau ("unwillingness") dan/atau tidak mampu ("unable") menangani perkara tersebut.

Lebih lanjut, mengenai kejahatan-kejahatan jure gentium selain pembajakan di laut dan kejahatan perang, tunduk pada asas khusus dan pertama di dalam hukum pidana internasional yang berasal dari Hugo Grotius, yaitu asas au dedere au punere yang berarti terhadap pelaku tindak pidana internasional dapat dipidana oleh negara tempat locus delicti terjadi dalam batas teritorial negara tersebut atau diserahkan atau diekstradisi kepada negara peminta yang memiliki yurisdiksi untuk mengadili pelaku tersebut. Di samping asas di atas, juga dikenal asas au dedere au judicare yang dicetuskan oleh Bassiouni, yang berarti setiap negara berkewajiban untuk menuntut dan mengadili pelaku tindak pidana internasional dan berkewajiban untuk melakukan kerja sama dengan negara lain di dalam menangkap, menahan, dan menuntut, serta mengadili pelaku tindak pidana internasional.

4. Teori Hukum Kosmopolitan

Karakter dasar hak kosmopolitan secara eksplisit disebutkan dalam the metaphysical elements of justice dimana Kant berpendapat bahwa hak publik harus mencakup tiga bentuk: hak politik, hak internasional dan kosmopolitan yang tepat membentuk suatu sistem yang saling bergantung satu dengan yang lain. Hak kosmopolitan ini pun tampak dalam Perpetual Peace sebagai salah satu dari tiga artikel definitif dari konstitusi negara-negara liga Pasifik. Dalam konteks ini hak kosmopolitan diabadikan dalam setiap konstitusi domestik negara-negara yang mensyaratkan bahwa setiap negara memperlakukan setiap individu (termasuk non warga negara) seolah-olah mereka adalah warga dunia. Dalam hal ini, hak kosmopolitan mungkin berlaku bagi semua orang untuk memiliki

hak-hak dasar meskipun tanpa keberadaan nyata dari negara dunia.²¹⁴

Dalam hubungannya dengan ilmu hukum, hukum kosmopolitan mengubah kekuatan politik hukum dari prinsip kedaulatan populer negara-negara dengan prinsip-prinsip warga negara dunia. Dasar filosofis ini menjelaskan konseptualisasi hak-hak dasar manusia sebagai hak yang melebihi yurisdiksi negara-negara dan bukan hanya menyangkut persoalan moral. Hal ini didasarkan pada konsepsi hak asasi manusia yang menjelaskan bahwa hukum kosmopolitan bisa mengadili genosida dan kejahatan terhadap kemanusiaan. Secara praktis, ini berarti membangun sistem hukum transnasional dan lembaga yang didasarkan pada kebutuhan politik warga dunia dapat secara hukum dimediasi dan termasuk cabang eksekutif yang dapat melaksanakan sanksi yang sesuai.

Salah satu perbedaan penting antara hukum kosmopolitan dan kontemporer hukum internasional berkaitan dengan kedaulatan negara-negara bahwa konsepsi kedaulatan dalam hukum internasional klasik menyatakan larangan adanya campur tangan dalam urusan internal suatu negara yang diakui secara internasional. Larangan terhadap adanya intervensi dimaksud ditegaskan kembali dalam Piagam PBB.

Habermas berpendapat bahwa hukum internasional harus beralih ke hukum kosmopolitan dalam rangka mencapai yurisprudensi yang berlaku secara global terhadap berbagai isu hak asasi manusia, termasuk didalamnya beberapa jenis kejahatan dalam lingkup kejahatan internasional seperti

²¹⁴ Lihat Sharon Anderson-Gold, the Cosmopolitan Foundation of the (Kantian) State, Rensselaer Polytechnic Institute.

²¹⁵ E. Eriksen and J. Weigard, Understanding Habermas, Communicative action and Deliberative Democracy, (London, NY: Continuum Press, 2005).

genosida dan kejahatan terhadap kemanusiaan. Lebih lanjut, Habermas menyebutkan bahwa seluruh sistem hukum internasional harus beralih ke hukum kosmopolitan.

Menurut Kant bahwa *freedom* (kemerdekaan) sejauh dapat hidup berdampingan dengan kebebasan orang lain yang sesuai dengan hukum yang bersifat universal merupakan sesuatu yang asasi sifatnya. *Freedom* tersebut dapat dipandang sebagai satu-satunya hak asasi yang dimiliki setiap orang yang menunjukkan sisi kebajikan manusia tersebut yang sesungguhnya.²¹⁶

Hak asasi manusia yang pengaturannya dicantumkan dalam konstitusi suatu negara yang merupakan bentuk penghargaan terhadap hak bagi seluruh umat manusia (*qua human*), tentu saja bukan hanya bagian dari budaya tertentu suatu bangsa, sejarah kehidupan, atau dalam konteks perspektif moral. Akan tetapi, pada dasarnya hak asasi manusia tersebut harus dihormati dalam bentuk penuangan norma hukum positif suatu negara berdasarkan kondisi negara-negara tersebut. Dalam hal ini, hak asasi manusia memiliki karakter ganda, yakni hak asasi manusia sebagai validitas positif yang tertuang dalam hukum positif yang merupakan norma konstitusi dan validitas supra positif yang tertuang dalam hukum alam sebagai hak yang dimiliki oleh setiap orang (*qua human*).²¹⁷ Hal ini tidak selalu bisa diterjemahkan ke dalam praktek yang memenuhi rasa keadilan, seperti dalam kasus pemerkosaan.

Dalam konteks validitas supra positif, hak asasi manusia secara intuitif menunjukkan bahwa hak asasi manusia

²¹⁶ J. Habermas, The Inclusion of the Other: Studies in Political Theory, (Cambridge, MA: MIT Press, 1998), hlm. 147.

²¹⁷ Ibid, hlm. 189

merupakan hak setiap warga negara dalam segala tingkatan dan spesies di dunia ini. Menurut Habermas, pengertian hak asasi manusia seperti ini dapat dipandang sebagai hak asasi manusia trans-subjektif dan dapat dilindungi melalui; (1) transformasi moral yang bersifat demokratis ke dalam sistem hukum positif dengan cara yang prosedural dalam aplikasi dan implementasinya; atau (2) transformasi kosmopolitan yang secara alamiah antara negara-negara yang dituangkan dalam bentuk perintah hukum (*legal order*) dan toleransi terhadap perbedaan.²¹⁸

Hukum kosmopolitan menjamin setiap warga negara baik dalam konteks hukum dan politik. Dalam hal ini, titik fokus hukum kosmopolitan, lebih tepatnya, ia melewati subjek hukum internasional secara kolektif sebagai negara dan secara langsung menetapkan status hukum dari subjek individu yang bebas dan sama sebagai warga dunia. Hal ini berarti, individu menikmati kedudukannya baik sebagai warga negara suatu negara maupun sebagai warga dunia tanpa ketergantungan satu dengan yang lainnya.²¹⁹

Konsepsi Habermas tentang hukum kosmopolitan mencerminkan kritik atas komitmen yang memungkinkan untuk membangun keadilan internasional hak asasi manusia yang bukan hanya terdapat berbagai pandangan tentang hak asasi manusia yang berbeda, akan tetapi manfaat yang diperoleh dari pandangan-pandangan yang berbeda tersebut. Dalam konteks masyarakat yang kompleks, hukum adalah satu-satunya media yang dimungkinkan untuk membangun hubungan moral yang secara timbal balik saling menghormati bahkan di antara

²¹⁸ Ibid, hlm. 201.

²¹⁹ Ibid, hlm 181.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

orang asing.²²⁰ Sebagai contoh kasus genosida dan kejahatan terhadap kemanusiaan yang memiliki pertautan dengan isu hak asasi manusia. Genosida dan kejahatan terhadap kemanusiaan dimaksud secara filosofis merupakan *judicial in nature* yang secara *de facto* menunjukkan bahwa kedua kejahatan tersebut secara faktual telah melanggar hak asasi manusia. Dalam konteks ini, peradilan Nuremberg yang mengadili kejahatan terhadap kemanusiaan misalnya tidak harus secara formal berada di ranah hukum untuk menjadi alasan yang cukup untuk mendakwa dan menahan pelaku dengan asumsi bahwa manusia memiliki hak diuji dengan mendalilkan validitas universal.

Fundamental yuridis, trans-subjektif, dan supra positif hak asasi manusia adalah pembenaran filosofis yang utama untuk hukum kosmopolitan dan secara bersamaan membutuhkan pembenaran praktis. Secara filosofis, negara-negara tidak memberikan manusia hak melalui status warga negara dalam negara-negara tersebut, akan tetapi, hak-hak ini ada sejak manusia lahir dan secara yuridis hak-hak tersebut diakui. Kemudian, dalam tataran praktis, hak asasi manusia tersebut harus tetap dijamin secara hukum meskipun berada di luar batasbatas negara-negara. Dengan kata lain, hak asasi manusia tersebut bersifat validitas universal (*universal validity*).²²¹

²²⁰ J. Habermas, Between Facts and Norms, Translated by William Rehg (Cambridge, MA: MIT Press, 1996), hlm. 460.

²²¹ Barbara Korth, *Establishing Universal Human Rights Through War Crimes Trials And The Need For Cosmopolitan Law In An Age Of Diversity*, Liverpool Law Review, Vol. 27 (2006), hlm. 104.

5. Hermenutika Hukum

Sejarah dan Pengertian Hermeneutika Hukum

Hermeneutika merupakan derivasi dari kata Hermes, seorang dewa dalam mitologi Yunani, yang berfungsi sebagai penghubung Sang Maha Dewa di langit dengan para manusia di bumi.²²² Dalam konteks ini peran Hermes sesungguhnya tak ubahnya dari peran nabi utusan Tuhan yang bertugas sebagai juru penerang dan penghubung untuk menyampaikan pesan dan ajaran Tuhan kepada manusia.²²³ Hal ini pula yang dikenal dalam tafsir Injil (bible).²²⁴

Peri Hermeneias mendefinisikan hermeneutika dalam konteks yang sangat sempit dalam menentukan kebenaran dan kepalsuan pernyataan. Kata hermêneuein, hermêneia, dan sanak mereka banyak digunakan pada zaman Yunani kuno yang merupakan interpretasi dalam beberapa pengertian: pertama, penafsiran lisan Homer dan teks-klasik lainnya. penafsir Homer disebut "hermeneuts". Kedua, terjemahan dari satu bahasa ke lain adalah proses hermeneutis, dan ketiga, penafsiran teks.²²⁵

Penafsiran ini membawa keluar makna, kadang-kadang artinya menjadi tersembunyi. Hermeneutika bukan hanya penafsiran teks yang berkaitan dengan retorika di zaman kuno, yang memiliki lingkup yang lebih luas, akan tetapi juga diterapkan untuk memberi penjelasan mimpi, nubuat, dan teks-teks sulit lainnya termasuk didalamnya teks hukum dan

²²² Komaruddin Hidayat, Memahami Bahasa Agama: Sebuah Kajian Hermeneutik, (Jakarta: Paramidana, 1996), hlm. 13.

²²³ Ibid.

²²⁴ Adian Husaini dan Abdurrahman Al-Baghdadi, op.cit. hlm. 8.

²²⁵ Richard E. Palmer, the Relevance of Gadamer's Philosophy Hermeneutics to Thirty Topic or Field of Human Activity, (Carbondale: Southern Illinois University, 1999).

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

preseden, dan teks sastra dan agama.²²⁶ Tradisi penafsiran aturan dalam konteks menafsirkan sastra, teks hukum, dan agama telah turun dari zaman kuno, dan ini memberikan subjek hermeneutika luas didefinisikan sebagai terkait dengan penafsiran teks.

Selanjutnya, hermeneutika mengalami faseperkembangan yang lebih spesifik hingga kemudian dipergunakan dalam ranah hukum, yang kemudian melahirkan hermeneutika hukum. Dalam konteks ini, hermeneutika sebagai metode tafsir dan interpretasi dipergunakan dalam menjelaskan teks hukum.²²⁷ Tafsir dimaksudkan bukan hanya secara formal menjelaskan pembacaan terhadap teks hukum, akan tetapi juga menjelaskan berbagai model tekstual yang muncul dalam argumen-argumen terkini mengenai apa itu hukum dan bagaimana hukum harus dipahami.²²⁸ Hal ini diartikan bahwa hukum diterjemahkan dengan menggambarkan hubungan antara norma hukum dan keadaan yang sebelumnya ada dan menjajaki secara terbuka bagaimana hubungan tersebut terus berlanjut hingga saat ini. Dalam konteks ini maka teks hukum sebelum dan setelah (futuristic model) mengalami perkembangan yang saling berhubungan satu dengan lainnya.²²⁹

²²⁶ Ibid.

Menurut Hans-Georg Gadamer bahwa hermeneutika hukum berkembang antara lain di bawah pengaruh inspirasi ilmu hukum. Lihat Jazim Hamidi, Hermeneutika Hukum: Sejarah-Filsafat & Metode Tafsir, (Malang: UB Press, 2011), hlm. 89. Lihat Juga Hans-Georg Gadamer, Truth and Method, (New York: The Seabury Press, 1975).

²²⁸ Gerald L. Bruns, Hukum dan Bahasa: Hermeneutika Teks Hukum, dalam Gregory Leyh, Hermeneutika Hukum: Sejarah, Teori, dan Praktik, diterjemahkan oleh M. Khozim, (Bandung: Nusamedia, 2011), hlm. 41. Lihat Juga Humberto Avila, Theory of Legal Principles, (the Netherlands: Springer, 2007), hlm. 83-85

²²⁹ Jurgen Habermas, Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy, translated by William Rehg,

Hermeneutika hukum pada dasarnya hendak meletakkan metode memahami atau metode interpretasi terhadap teks secara holistik yang melingkupi hubungan antara teks, konteks, dan kontekstualisasi.²³⁰ Dalam konteks ini maka interpretasi tidak hanya diletakkan pada teks yuridis saja akan tetapi juga diarahkan pada kenyataan yang menyebabkan munculnya masalah hukum itu sendiri.²³¹

Proses dan cara menginterpretasikan sesuatu dalam perspektif hermeneutika hukum memberikan ruang baru bagi penginterpretasi untuk memberikan interpretasi yang lebih luas dari sekedar menginterpretasi makna teks sebagaimana dalam interpretasi pada umumnya. Hal ini dikarenakan lingkup hermeneutika hukum yang luas.

Hermeneutika hukum pada dasarnya tidak menolak aturan-aturan yang ada akan tetapi hermeneutika hukum melakukan adaptasi terhadap aturan-aturan tersebut dan reproduksi aturan-aturan tersebut ke arah yang lebih baik. Dalam beberapa studi literatur, penggunaan hermeneutika hukum dalam menyelesaikan sengketa hukum, di Eropa misalnya, pada umumnya digunakan untuk menyelesaikan sengketa hukum tata negara dan hukum hak asasi manusia.²³²

⁽Massachusetts: the MIT Press, 1996), hlm. 199-200.

²³⁰ Jimly Asshiddiqie, Pengantar Ilmu Hukum Tata Negara, (Jakarta: Sekjen dan Kepaniteraan Mahkamah Konstitusi, 2006), hlm. 306. Lihat juga Alicja Ornowska, Introducing Hermeneutic Methods in Criminal Law Interpretation in Europe, in Joanna Jemielniak and Przemysław Mikłaszewicz, Interpretation of law in the Global world: From Particularism to a universal Approach, (London: Springer, 2010), hlm. 251.

²³¹ Ibid.

²³² Alicja Ornowska, ohlm.cit, hlm. 258.

Hermeneutika Hukum dan Interpretasi

Secara etimologis hermeneutika hukum memiliki persamaan sekaligus perbedaan dengan tafsir atau interpretasi hukum, khususnya interpretasi perjanjian sebagaimana dikemukakan oleh Fitzmaurice. Akan tetapi perbedaan dimaksud tidak hendak meletakkan keduanya dalam posisi superioritas yang satu terhadap yang lainnya. Hal ini dikarenakan bahwa dalam konteks penafsiran teks yang digunakan dalam koridor hermeneutika hukum, interpretasi dalam konteks hukum (perjanjian) internasional tetaplah menjadi patron yang harus dirujuk.

Menurut Fitzmaurice, terdapat tiga hal penting dalam interpretasi suatu perjanjian yakni maksud para pihak (*intention*), teks perjanjian (makna kata kata), dan tujuan dan objek perjanjian.²³³ Dalam konteks maksud perjanjian maka dalam beberapa sistem hukum yang khusus, maksud perjanjian dapat dipengaruhi atau ditentukan oleh praktek hukum yang merujuk pada kasus yang dihadapinya.²³⁴ Uraian atas maksud perjanjian yang dilakukan sebagaimana disebutkan di atas dapat diterapkan pada kasus yang sama pada waktu yang berbeda, yang kemudian dikenal sebagai "konsep maksud perjanjian yang direpresentasikan".²³⁵

²³³ D.J. Harris, *Case and Materials on International Law*, 5th ed.,(London: Sweet & Maxwell, 1998), hlm. 810. Lihat juga Ian Brownlie, *Principles of Public International Law*, 5th ed., (Oxford: Clarendon Press, 1998), hlm. 631-633. Lihat juga M. N. Shaw, *International Law*, 6th ed., (Cambridge: Cambridge University Press, 2008), hlm. 932-938. Lihat Juga Aharon Barak, *Purposive Interpretation in Law*, (New York: Princeton University Press, 2005), hlm. 307-309.

²³⁴ Andrei Marmor, Interpretation and Legal Theory, 2nd Ed. (revised), (Oxford: Hart Publishing, 2005), hlm. 121.

²³⁵ Ibid. hlm. 122.

Selain maksud perjanjian, teks suatu perjanjian memainkan peranan yang sangat penting dalam menguraikan maksud perjanjian itu sendiri. Teks perjanjian seharusnya diuraikan dengan jelas tanpa harus menimbulkan makna ganda (ambiguity) dan ketidakjelasan makna (vagueness). Akan tetapi dalam praktek, hal tersebut sulit untuk dihindari. Ambiguitas menjadi sesuatu yang lumrah yang ditemui dalam peraturan perundang-undangan nasional dan internasional.

Solusi dibutuhkan untuk menyelesaikan yang permasalahan ambiguitas, menurut Elmer Driedger yaitu dengan "pendekatan interpretasi pragmatis".236 Interpretasi ini bermakna bahwa kata-kata yang digunakan dan termaktub dalam suatu peraturan perundang-undangan harus dibaca utuh (keseluruhan) dan makna sesungguhnya secara dan gramatikal peraturan perundang-undangan diharmonisasikan dengan skema menyeluruh dari peraturan perundang-undangan tersebut termaktub di dalamnya tujuan dan maksud peraturan perundang-undangan dibuat.²³⁷ Uraian maksud dan makna perjanjian berlaku pula untuk menguraikan tujuan dari perjanjian tersebut dibuat. Meskipun tujuan yang termuat dalam suatu teks belum tentu merupakan bagian dari teks itu sendiri. Dalam hal ini tujuan dirumuskan berdasarkan maksud dari pembuat teks (subjective purpose) dan maksud dari suatu sistem hukum (objective purpose).²³⁸

Dengan kata lain, dalam konteks suatu perjanjian maka tujuan suatu perjanjian dimaksudkan untuk menunjukkan apa

 $^{^{236}}$ Elmer Driedger, Construction of Statues, 2^{nd} ed. (Toronto: Butterworths, 1983), hlm. 87.

²³⁷ Moshe Azar, Transforming Ambiguity into Vagueness in Legal Interpretation, in Anne Wagner, et.al., Interpretation, Law and the Construction of Meaning, (Netherlands: Springer, 2007), hlm. 121.

²³⁸ Aharon Barak, op.cit., hlm. 110.

yang hendak diraih dan dicapai dari perjanjian tersebut dibuat. Tujuan yang dimaksud tentunya dinterpretasikan dalam konteks tujuan yang bersifat objektif dan subjektif.²³⁹

Harmonisasi ketiganya dalam studi hukum internasional khususnya dapat ditemukan dalam Pasal 31-33 Konvensi Wina 1969. Pasal 31 mengatur tentang aturan umum interpretasi; Pasal 32 mengatur tentang komplementari makna interpretasi; dan Pasal 33 mengatur bahwa interpretasi secara otentik disajikan dalam 2 (dua) bahasa atau lebih. Penekanan interpretasi dilakukan dalam bentuk tertulis merupakan suatu keharusan. Hal ini dilakukan karena penuangan interpretasi dalam bentuk bahasa telah menjadi elemen penting, sebagaimana dikemukakan oleh As. Focsaneanu bahwa:

"setiap aturan hukum perlu dikemukakan dalam suatu bahasa yang menjadi unsur penting. Interpretasi dan aplikasi hukumnya meminta suatu kritik berdasarkan makna linguistik, yang dapat dikaji dari sudut pandang leksikal, morfologi, sintatik, dan aspek logika modern".²⁴¹

Tujuan dilakukannya interpretasi untuk mempelajari arti sebenarnya dan isi dari peraturan-peraturan hukum yang berlaku.²⁴² Disamping itu, interpretasi juga harus ditekankan dapat digunakan oleh *International Court of Justice* (ICJ) secara independen dalam menyelesaikan kasus-kasus yang menjadi yurisdiksi ICJ.²⁴³ Dalam konteks hermeneutika hukum maka

²³⁹ Ibid.

²⁴⁰ Carlos Fernandez de Casadevante Romani, op.cit., hlm. 37.

²⁴¹ As Focsaneau, Les langues Comme Moyen D'expression du droit International, in Carlos Fernandez de Casadevante Romani, Sovereignty and Interpretasi of International Norms, (New York: Springer, 2007), hlm. 40.

²⁴² Lihat Boer Mauna, op.cit., hlm. 141.

²⁴³ Lihat the Arbitral Award of 31 July 1989, ICJ, Reports, 1991.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

interpretasi tetap memainkan peran yang sangat vital dalam melakukan penafsiran. Tentunya dalam konteks ini, perluasan teknik atau metode penafsiran memberikan keleluasaan untuk memahami maksud dari lahirnya suatu ketentuan hukum internasional. Sehingga kesan bahwa interpretasi tidak mendapatkan "tempat" dalam hermeneutika hukum dengan sendirinya terbantahkan.

BAB V

RINTANGAN DAN TANTANGAN PEMBUKTIAN SERANGAN SIBER SEBAGAI SUATU KEJAHATAN INTERNASIONAL

Globalisasi mendorong perkembangan teknologi informasi di dunia. Perkembangan ini membuat tatanan dunia baru yang bertumpu pada modernisasi di segala aspek kehidupan. Jika dibandingkan dengan masa sebelum globalisasi, aktivitas manusia masih bersifat konvensional dimana aktivitas tersebut terbatas dengan jarak, waktu dan teknologi, sedangkan dunia dewasa ini batasan tersebut bukan menjadi persoalan. Perkembangan teknologi informasi mayoritas berhubungan erat dengan penggunaan internet, *Internet of Thing* (IoT). Mayoritas aktivitas manusia baik secara individu, perusahaan bahkan kegiatan pemerintahan telah ditransformasikan dalam ruang maya atau yang disebut *cyberspace*.

Istilah *cyberspace* pertama kali muncul di tahun 1984, digunakan oleh William Gibson pada 1984.²⁴⁴ William Gibson menggambarkan karakternya bergerak di dalam internet, menghasilkan lanskap yang stabil, ada penduduknya, mudah dinavigasikan, seukuran negara atau bahkan lebih besar.²⁴⁵

²⁴⁴ Murray Andrew D, *The Regulation of Cyberspace, Control in the Online Environment*, London: Routledge-Cavendish, 2007, hlm., 5.

²⁴⁵ Murray Andrew D, *Ibid*.

Dalam *cyberspace*, para pengguna dapat berkomunikasi dengan menyamarkan identitasnya (*anonymous*), tanpa dibatasi oleh batas wilayah (*borderless*), dan bahkan lintas negara (transnasional).²⁴⁶

Teknologi mendorong terciptanya informasi global dan jaringan komunikasi yang sekarang menjadi bagian integral dari cara pemerintahan modern, bisnis, pendidikan, dan ekonomi beroperasi.²⁴⁷ Namun, perkembangan ini tidak hanya membawa dampak positif tetapi juga memunculkan dampak negatif. Dewasa ini, kejahatan juga mulai bertransformasi ke ranah cyberspace. Serangan siber merupakan dampak negatif dari perkembangan teknologi informasi pada era modernisasi. memanfaatkan perkembangan Serangan ini komputer khususnya internet sebagai alat untuk menyerang jaringan telekomunikasi bahkan sampai sistem pertahanan suatu negara. Bahkan dapat dianggap sebagai sinyal awal dari kejahatan internasional lainnya.

Serangan siber yang terjadi di Estonia pada 2007 lalu, mengakibatkan terganggunya layanan publik dan kerugian materi. Serangan yang diduga dilakukan oleh Rusia²⁴⁸ ini melumpuhkan jaringan-jaringan pemerintahan dan perdagangan milik Pemerintah Estonia. Kurang lebih satu juta komputer Pemerintah terinfeksi yang didistribusikan dalam bentuk *Distributed Denial of Service (DDoS) attacks*.²⁴⁹ Kasus

²⁴⁶ Murray Andrew D, *Ibid*, hlm.. 25.

²⁴⁷ Purna Cita Nugraha, *Konsepsi Kedaulatan Negara dalam Borderless Space*, Jurnal Opinio Juris, Volume 13, 2013, hlm. 26.

²⁴⁸ Katherina C. Hinkle, *Counter measures in the Cyber Context: One More Thing to Worry About*, The Yale Journal of International Law Online, Volume. 17, No.4, 2011, hlm.. 13.

²⁴⁹ Katherina C. Hinkle, *Ibid*.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

terbaru terjadi di Iran pada awal tahun 2020. Konflik senjata antara Iran dengan Amerika Serikat salah satunya dipicu oleh adanya dugaan *serangan siber* yang terjadi sebelumnya. Serangan terbaru berupa serangan yang menggunakan Drone MQ Reaper 9, sebuah pesawat tak berawak yang dioperasikan oleh militer AS, dengan kemampuan jelajah 14 jam saat terisi penuh dengan amunisi, dengan berbagai senjata, sensor visual yang kuat untuk mencapai sasaran, sehingga sangat akurat dan mematikan.²⁵⁰ Serangan ini terjadi di Bandara Baghdad dan berhasil menewaskan delapan orang termasuk seorang Jenderal Qassem Soleimani.

Pada tahun 2010 Iran juga telah mengalamI serangan siber yang menyerang fasilitas nuklir Iran di Natanz, kurang lebih 60.000 komputer fasilitas nuklir terinfeksi oleh virus yang disebut dengan Stuxnet.²⁵¹ Target terhadap infrastruktur pengayaan uranium di Iran tentunya sangat berbahaya, bukan saja melanggar kedaulatan negara Iran akan tetapi dampak yang ditimbulkannya berbahaya bagi keselamatan peradaban umat manusia.²⁵² Serangan siber mampu mematikan sentrifugal nuklir, sistem pertahanan udara, dan jaringan listrik, serangan dunia maya menjadi ancaman serius bagi keamanan nasional.²⁵³ Serangan siber dapat dikategorikan sebagai suatu kejahatan

²⁵⁰ Erwin Prima and Khory Alfarizi, *Bunuh Soleimani, Drone MQ-9 Reaper AS Paling Ditakuti di Dunia*, Tempo.Co, https://tekno.tempo.co/read/1294958/bunuh-soleimani-drone-mq-9-reaper-as-paling-ditakuti-didunia/full&view=ok, 14 January 2020.

²⁵¹ James P. Farwell and Rafal Rohonzmskl, *Stuxnet and the Future of Cyber War*, Journal Survial, Volume 53, 2011, hlm. 23-26.

²⁵² Maskun; Alma Manuputty; S.M. Noor; Juajir Sumardi, *Kedudukan Hukum Cyber Crime dalam Perkembangan Hukum Internasional Kontemporer*, Jurnal Masalah-Masalah Hukum, Volume 42 No. 4, 2013, hlm. 512.

²⁵³ Oona A. Hathaway; Rebecca Crootof; Philip Levitz; Haley Nix; Aileen Nowlan; William Perdue and Julia Spiegel, *The Law of Cyber-Attack, California Law Review*, Volume 100, No. 4, 2012, hlm.. 817-885.

internasional. Sayangnya, pembuktian dari praktik serangan siber masih menjadi polemik dalam dunia internasional. Terdapat beberapa kendala pembuktian serangan siber seperti kekuatan politik, sifat serangan borderless and anonym, variasi teknik serangan serta sukarnya menentukan tempat dan waktu serangan. Sampai saat ini, pembuktian praktik serangan siber masih menjadi polemik dalam dunia internasional, ini disebabkan tidak terdapat instrumen hukum internasional mengatur pembuktian praktik serangan siber secara universal.

A. Kejahatan Internasional

Dunia internasional melalui konsensus tujuan pendirian Perserikatan Bangsa-Bangsa (PBB) sepakat untuk menjunjung tinggi perdamaian dan keamanan dunia.²⁵⁴ Namun dalam praktik perkembangan zaman, terdapat tindakan masyarakat internasional yang dapat menghancurkan dan melanggar kesepakatan tersebut, salah satunya dengan melakukan kejahatan internasional. Kejahatan internasional merupakan objek kajian dari hukum pidana internasional. Hukum Pidana Internasional adalah cabang ilmu hukum yang semula diperkenalkan dan dikembangkan oleh pakar-pakar hukum internasional dari Eropa seperti: Friedrich Meili pada tahun 1910 (Swiss), Georg Schwarzenberger pada tahun 1950 (Jerman), Gerhard Mueller pada tahun 1965 (Jerman), J.P Francois pada tahun 1967, Rolling pada tahun 1979 (Belanda), Van Bemmelen pada tahun 1979 (Belanda), kemudian diikuti oleh pakar hukum dari Amerika serikat seperti: Edmund Wise pada tahun 1965 dan Cherif Bassiouni pada tahun 1986 (Amerika Serikat).²⁵⁵

²⁵⁴ United Nations, Charter of the United Nations, Article 1.

²⁵⁵ Hukum Pidana Internasional, Mochtar Kusumaatmadja, Op.Cit,hal 68-80

Pengembangan Hukum Pidana Internasional sebagai salah satu cabang ilmu hukum dimulai dari pekerjaan oleh Gerhard O.W. Muelller dan Edmund M. Wise (1965) dalam rangka proyek dibawah judul, *Comparative Law Project* dari University New York. Pekerjaan ini kemudian dilanjutkan oleh M. Cherif Bassiouni dan Van. Nanda (1986), yang telah menulis sebuah karya tulis *A Treatise on International Criminal Law* (1973).

Pada bab sebelumnya telah dibahas terkait pengkategorian kejahatan internasional. Berdasarkan teori, M. Cherif Bassiouni²⁵⁶ membagi tingkatan kejahatan internasional menjadi tiga. *Pertama*, kejahatan internasional yang disebut sebagai *international crimes* adalah bagian dari *jus cogens*.²⁵⁷ Tipikal dan karakter dari *international crimes* berkaitan dengan perdamaian dan keamanan manusia serta nilai-nilai kemanusiaan yang fundamental.

Terdapat sebelas kejahatan yang menempati hirarki teratas sebagai kejahatan internasional (*international crime*), yakni:

- a. Aggression.
- b. Genocide.
- c. Crimes against humanity.
- d. War Crimes
- e. Unlawful possession or use or emplacement of weapons.
- f. Theft of nuclear materials.
- g. Mercenaries.

²⁵⁶ Eddy O.S. Hlanej, *Pengantar Hukum Pidana internasional*, Jakarta; Airlangga, 2009, hlm.. 56.

²⁵⁷ Jus Cogens adalah hukum pemaksa yang tertinggi dan harus ditaati oleh bangsa-bangsa beradab d1 dunla sebagai prinsip dasar umum dalam hukum intemasionaJ yang berkaltan dengan moral. Lihat: Eddy O.S. tflariej, ibid.hlm.. 50

- h. Apartheid.
- i. Slavery and slaverelated practices.
- j. Torture and other forms of cruel, inhuman, or degrading treatment.
- k. Unlawful human experimentation.

Kedua, kejahatan internasional yang disebut sebagai international delicts. Tipikal dan karakter international delicts berkaitan dengan kepentingan internasional yang dilindungi meliputi lebih dari satu negara atau korban dan kerugian yang timbul berasal dari satu negara. Ada tiga belas kejahatan internasional yang termasuk dalam international delicts, yaitu:

- a. Piracy.
- b. Aircraft hijacking and unlawful acts against international air safety.
- c. Unlawful acts against the safety of maritime navigation and safety of platforms on the high seas.
- d. Threat and use of force against internationally protected person.
- e. Crimes against United Nations and associated personnel.
- f. Taking of civilian hostages.
- g. Unlawful use of the mail.
- h. Attacks with explosive.
- i. Financing of terrorism.
- j. Unlawful traffic in drugs and related d rug offenses.
- k. Organized crime
- I. Destruction and/or theft of national treasures.
- m. Unlawful acts against certain internationally protected elements of the environment.

Ketiga, kejahatan internasional yang disebut dengan istilah international infraction. Dalam hukum pidana internasional secara normatif, international infraction tidak termasuk dalam kategori international crime dan international delicts. Kejahatan yang tercakup dalam international Infraction hanya ada empat, yaitu:

- a. International traffic in obscene materials.
- b. Falsification and counterfeiting.
- c. Unlawful interference with submarine cable.
- d. Bribery of foreign public official.

Selanjutnya, menurut Bassiouni terdapat tiga unsur yang harus dipenuhi agar dapat dikatakan sebagai kejahatan internasional. Unsur tersebut adalah:²⁵⁸

- a. Unsur internasional termasuk didalamnya ancaman secara langsung dan tidak langsung atas perdamaian dunia dan menggoyah perasaan kemanusiaan.
- b. Unsur transnasional termasuk didalamnya bahwa dampak yang ditimbulkan memiliki dampak terhadap lebih dari satu negara, terhadap warga negara dari lebih satu negara, dan sarana dan prasarana serta metode yang dipergunakan melampaui batas-batas teritorial suatu negara.
- Unsur kebutuhan termasuk didalamnya kebutuhan akan kerjasama antara negaranegara untuk melakukan penanggulangan.

٠

²⁵⁸ Romli Atmasasmita, *Pengantar Hukum Pidana internasional*, Bandung; Refika Aditama, 2003, hlm.. 58.

B. Serangan siber

Sebelum membahas lebih lanjut terkait *serangan siber*, terlebih dahulu harus diketahui terkait penjelasan umum terkait kejahatan siber. Kejahatan siber (*cyber crime*) merupakan kejahatan di dunia maya (*cyberspace*), secara umum didefinisikan sebagai "*any activity in which computers or networks are a tool, a target or a place of criminal activity*".²⁵⁹ Dalam *Convention on Cybercrime* tindakan *cybercrime* dapat dikategorikan sebagai berikut: *The criminalisation of conduct – ranging from illegal access, data and systems interference to computer-related fraud and child pornography*.²⁶⁰

Kejahatan siber akan terus berkembang secara signifikan yang menjadi suatu ancaman yang potensial dalam bidang keamanan dan menjadi tantangan paling serius pada abad ke-21.²⁶¹ Kini kejahatan ini merambah ke ranah militarian dan ketahanan suatu negara, seperti contohnya perkembangan kejahatan militarian di luar angkasa, penggunaan senjata luar angkasa dan penggunaan senjata antariksa non-kinetik di atas tanah, platform maritim, atau udara dan digunakan untuk mempengaruhi operasi satelit atau sensor tanpa melakukan kontak fisik.²⁶²

²⁵⁹ Marco Gercke, *Understanding Cybercrime :Phenomena, Challenges and Legal Response of Telecommunication Development Sector,* Telecommunication Development Sector; International Telecommunication Union (ITU), 2012, hlm. 11.

Nyman Gibson Miralis, *The Budapest Convention on Cybercrime : International Criminal Law and use the Theaties*, Lexology https://www.lexology.com/library/detail.aspx?g=4220b287-ac07-4a33-a711-bee235721d9f, 29 July 2019.

²⁶¹ Paul Meyer, *Norms of Responsible State Behaviour in Cyberspace*, The International Library of Ethics, Law and Technology, Volume 21, 2020, hlm. 349.

²⁶² Todd Harrison, *International Perspectives on Space Weapon*, The

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

Pertemuan antara kejahatan siber dan militarian dapat dapat dilihat sebagai suatu kejahatan siber kontemporer. Makna kontemporer disini ialah sifat kekinian yang terjadi karena perkembangan zaman. Penggunaan senjata atau tools dalam melakukan kejahatan siber ini juga merupakan tindakan militarian. Kejahatan ini menitikberatkan pada adanya suatu serangan dengan menggunakan bantuan teknologi siber dalam mengoperasikannya atau dikenal dengan istilah serangan siber (serangan siber). Serangan ini sejenis manuver ofensif yang digunakan oleh negara, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer, dan/atau perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya berasal dari sumber anonim yang mencuri, mengubah, atau menghancurkan target yang ditentukan dengan cara meretas sistem yang rentan.²⁶³ Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Rule 92 mendefinisikan serangan siber sebagai berikut: "A serangan siber is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."264

Suatu serangan akan selalu dihubungkan dengan kehancuran (*destroy*) atau kerusakan (*damage*), dalam hal siber attack belum ada definisi yang formal mengenai kehancuran maupun kerusakan di dalam hukum humaniter internasional.²⁶⁵ Dalam suatu pertempuran atau peperangan,

Center for Strategic and International Studies (CSIS), 2020, hlm.. 5-6.

²⁶³ Financial Weapon of War, 100 Minnesota Law Review 1377, 2016.

²⁶⁴ Schmitt, M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,

Cambridge: Cambridge University Press, 2017, Rule 92.

²⁶⁵ Hayashi, Nobuo, Requirement of Military Necessity in International

hancurnya suatu benda pasti dikarenakan adanya suatu serangan, namun hal tersebut kini banyak diragukan karena serangan tidak selalu identik dengan kehancuran yang dapat dilihat secara fisik dan kasat mata. Dalam melakukan serangan siber contohnya, penggunaan cyber weapon tidak serta merta dapat menimbulkan kerusakan dan kehancuran saat itu juga, namun tetap dapat menimbulkan kerugian, kerusakan dan kehancuran yang menyangkut hajat hidup manusia.

Merujuk pada Tallinn Manual Rule 103, *Cyber Weapon* didefinisikan sebagai: "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operations as an attack,"²⁶⁶

Beberapa ahli sependapat bahwa serangan bila dihadapkan dengan hukum humaniter menjadi serangan bersenjata. Menurut Jean Pictet, serangan bersenjata terkait dengan durasi dan intensitas yang memadai. Namun, tidak sedikit ahli yang menanggapi bahwa, durasi dan intensitas sebagai patokan terhadap suatu serangan dirasa masih belum cukup, Michael N. Schmitt mengemukakan terdapat enam kriteria untuk dapat memenuhi sebagai suatu serangan;²⁶⁷

1. Severity, dilihat dari ruang lingkup dan intensitas serangan tersebut, seperti banyaknya korban jiwa yang diakibatkan, luas area yang terkena dampaknya

Humanitarian Law and International Criminal Law, Boston University International Law Journal, Volume 28, 2010, hlm.. 110.

²⁶⁶ Schmitt, M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,

Cambridge: Cambridge University Press, 2017, Rule 103.

²⁶⁷ Carr, Jeffrey, *Inside Cyber Warfare*, California : O'Reilly Media, Inc., 2010, hlm.. 60.

- dan banyaknya benda-benda yang rusak karena serangan tersebut
- 2. Immediacy, melihat pada durasi dari serangan tersebut, seperti berapa banyak waktu yang dibutuhkan agar efek dari serangan tersebut dapat dirasakan, dan berapa lama efek dari serangan tersebut terjadi,
- **3. Directness**, melihat pada luka atau kerusakan yang di timbulkan oleh adanya serangan tersebut,
- **4. Invasiveness**, melihat pada locus dari serangan tersebut, maksudnya bagaimana serangan tersebut melintasi batas-batas Negara,
- **5. Measurability**, yaitu akibat dari serangan tersebut dengan melakukan penafsiran dan pengukuran,
- 6. Presumptive Legitimacy, melihat pada penilaian serta legitimasi dari serangan tersebut yang didasarkan pada praktik Negara-Negara, dan normanorma yang ada di dalam komunitas internasional, suatu tindakan dapat memperoleh legitimasi berdasarkan hukum ketika hal tersebut diterima oleh komunitas internasional.

Terdapat beberapa jenis *cyber attack* yang biasa digunakan diantaranya adalah :²⁶⁸

1. **DoS** (**Denial of Service**), serangan siber jenis ini bertujuan untuk menghambat kerja sebuah layanan (service) atau mematikannya, sehingga user yang berhak atau yang berkepentingan tidak

²⁶⁸ Mitra Teleinformatika Perkasa, *7 Jenis Cyber Attack yang Mengancam IT Perusahaan dan Solusinya*, Mitra Teleinformatika Perkasa, https://mtp.co.id/project/7-jenis-cyber-attack-yang-mengancam-it-perusahaan-dan-solusinya/, 2018.

dapat menggunakan layanan tersebut, serangan DoS mentargetkan bandwidth dan koneksi sebuah jaringan untuk dapat mencapai misinya.²⁶⁹ Serangan yang bertubi-tubi tersebut dilakukan agar situs menjadi *down*, kemudian semakin gencar serangannya maka bisa menyebabkan website menjadi lumpuh total.

- 2. *Malware*, bentuk dari serangan ini sendiri merupakan perangkat lunak yang memiliki kadar bahaya tingkat tinggi. Saat perangkat lunak itu sudah berhasil ke perangkat yang digunakan, *Malware* bisa dengan cepat merusak apa saja yang ada di dalamnya. Dari merusak sistem hingga mencuri data penting, semua bisa dilakukan oleh *Malware*. Biasanya serangan berbahaya ini masuk ke perangkat saat mengunduh suatu *file* hingga di-*install*. Hal inilah yang membuat *Malware* merupakan salah satu bentuk *serangan siber* paling berbahaya. Terdapat beberapa jenis malware yang umum dikenal dan sering menyerang sistem komputer seperti Virus, Worm, Trojan Horse, Backdoors, Keystroke Logger, rootkit atau Spyware.
- 3. **Phishing,** merupakan bentuk serangan yang berhubungan dengan menyerang perangkat yang kemudian berhubungan dengan pencurian data. Biasanya, data-data yang dicuri merupakan data penting seperti *PIN*, *password* hingga *username*.

²⁶⁹ Chad Nelson, *Cyber Warfare: The Newest Battle Field*, Washington University in St. Louis, https://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar.pdf, 2011, hlm. 2-3.

- 4. **Credential Reuse**, jenis serangan siber ini jika memiliki username, password, dan PIN yang mirip atau sama di beberapa akun, maka itu menjadi sasaran empuk serangan ini. Konsep dari serangan ini yaitu dengan menggunakan ulang beragam informasi penting yang sudah mereka dapatkan sebelumnya.
- 5. **SQL Injection**, SQL Injection dalam praktiknya secara manual, hacker biasanya memasukkan kode berupa tanda seperti titik, petik tunggal, dan strip. Ketika kode tersebut berhasil, maka seluruh data dalam sebuah database akan terhapus dan data tersebut digunakan oleh hacker untuk melakukan tindakan lainnya yang merugikan sebuah perusahaan.
- 6. Cross-Site Scripting (XSS), jenis serangan ini berusaha merusak atau mengambil alih suatu website tertentu, terutama di instansi pemerintahan atau perusahaan di sektor perbankan dan keuangan. Informasi semacam username, password, dan PIN bisa didapatkan oleh hacker dengan cara memasukkan kode HTML atau client script code ke sebuah situs.
- 7. *Man in the Middle*, serangan jenis ini menempatkan *hacker* di tengah-tengah komunikasi antara dua orang. Ketika mereka sedang berkomunikasi, maka berbagai informasi penting yang dibagikan di antara keduanya bisa dicuri oleh *hacker*.

C. Contoh Kasus Serangan Siber

Estonia - Russia

Estonia sebagai salah satu negara pecahan Uni Soviet memiliki latar belakang historis yang sangat erat dengan Rusia. Pada 2007 Pemerintah Estonia mengumumkan akan memindahkan patung *Bronze of Soldier* yang dibangun sebagai simbol pembebasan wilayah Soviet Liberation of Estonia dari Nazi Jerman. Sehingga patung ini memiliki hubungan historis dengan Rusia dan Estonia sebagai suatu kesatuan dalam Uni Soviet. Kebijakan ini menjadi pemicu kerusuhan parah yang dilakukan oleh etnis Rusia di Estonia pada wilayah tersebut yang tidak terima dengan kebijakan tersebut.²⁷⁰

Konflik yang terjadi ini pun akhirnya merambah ke serangan siber selama 22 hari mulai dari 27 April hingga 18 Mei 2007 menyerang berbagai server fasilitas publik milik pemerintah, parlemen, polisi, bank, penyedia layanan internet, media online, dan banyak usaha kecil, dan pemerintah daerah. Serangan siber dilakukan melalui komputer di berbagai lokasi negara yakni Mesir, Rusia dan Amerika Serikat dan digunakan untuk melawan server dan router di Estonia dengan spam email dan ping serta serangan datagram yang membanjiri protokol pengguna.

Serangan siber dilakukan dalam bentuk *Distributed Denial of Service* (DDoS). Situs web yang biasanya menangani 1000 hit per hari mengalami crash dengan menerima 2000 hit per detik, transaksi perbankan, kartu kredit, dan ATM online terhenti, sementara situs pemerintah kesulitan untuk diakses,

²⁷⁰ Mohan B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, Cybersecurity Interdisciplinary Systems Laboratory (CISL), Cambridge: Massachusetts Institute of Technology, 2017, hlm. 68.

atau bahkan telah rusak, media online tidak mampu untuk mengunggah berita. Hal ini diperparah dengan dengan tingkat penggunaan internet di Estonia yang sangat tinggi, 60 % dari penduduk Estonia merupakan pengguna internet setiap hari, dan 97 % transaksi perbankan sudah menggunakan media elektronik. ²⁷¹ Serangan siber tersebut menyebabkan berbagai layanan publik tidak berjalan maksimal dan terganggunya kelangsungan hidup manusia di sana.

Iran- Amerika Serikat

Sejarah konflik antara Iran dan Amerika Serikat (AS) terjadi pada pra dan pasca revolusi Islam Iran 1978. Di ujung rezim pemerintah Shah Reza Pahlevi di Iran pada 1978, presiden melarikan diri dengan dibantu oleh pemerintah AS. Pemerintah terpilih kemudian menahan warga negara AS di kedutaan besar AS di Teheran. Hubungan ini semakin memburuk pasca pada tahun 1988 AS menembak jatuh pesawat Iran. Pada tahun 2002 AS mengecam Iran sebagai poros kejahatan dunia, dan menuduh Iran sedang mengembangkan program senjata nuklir secara rahasia.272 Demi memastikan Iran tidak melakukan pengembangan senjata nuklir, AS melakukan berbagai upaya, baik itu secara diplomatik, melalui perundingan maupun melalui operasi intelijen. Program Olympic Games atau biasa disebut juga dengan Stuxnet adalah bagian dari upaya untuk mengacaukan program pengembangan nuklir yang dilakukan oleh Iran.

²⁷¹ Stephen Herzog, *Country in Focus Ten Years after the Estonian Cyber Attacks Defense and Adaptation in the Age of Digital Insecurity ,* Georgetown Journal Of International Affairs Fall 2017, Volume Xviii, Number III, hlm. 68-69

²⁷² Mohan B. Gazula, *op. cit.*, hlm. 30.

Stuxnet merupakan virus yang menyerang Infrastruktur nuklir Iran di Natanz. Menurut Stefano Mele, Stuxnet dapat dikategorikan sebagai Cyber Weapon, jika merujuk pada konteks penggunaanya yang digunakan pada situasi konflik antara negara yakni Iran dan AS. Penggunaan Stuxnet bertujuan secara khusus untuk menyerang infrastruktur Nuklir Iran yang termasuk kedalam infrastruktur penting Iran. Operasi siber dilakukan dengan menggunakan virus yang dikembangkan dengan kecanggihan teknologi informasi dan komunikasi.²⁷³ Stuxnet dirancang untuk mengubah gerak sentrifugal ini secara diam-diam hingga meningkat dengan sangat cepat kemudian, secara perlahan-lahan kemudian melambat. Akibat dari serangan virus ini menimbulkan getaran yang berlebihan hingga sudah cukup untuk merusak sentrifugalnya. Hal ini dinilai serangan siber tersebut telah menimbulkan kerugian material terhadap Iran.²⁷⁴

Kasus Qassim Solaimani

Pada 3 Januari 2020, AS kembali melakukan manuver dengan memutuskan tindakan penting untuk membantai Komandan Islamic Revolutionary Guard Corps- Quds Force (IRGC-QF), Jenderal Qassem Soleimani, salah satu Jenderal paling berpengaruh di Iran. Rencana ini dilakukan AS dengan sebuah serangan siber yang menggunakan drone tanpa awak. Berdasarkan keterangan resmi dari Departemen Pertahanan AS, tindakan ini dinilai diambil sebagai "Defensif Action", Qasem Soleimani dinilai bertanggung jawab terhadap kematian ratusan orang AS dan anggota pasukan koalisi, dan persetujuan blokade terhadap kedutaan AS di Baghdad, dan secara aktif

²⁷³ Stephen Herzog, *loc. cit*.

²⁷⁴ Gary Lilienthal and Nehaluddin Ahmad, *Cyber attack as Invitable Kinetic War*, The *Computer Law and Security Review* XXXI. 3, 2015, hlm. 7.

mengembangkan rencana untuk menyerang diplomat AS dan anggota tentara di Irak dan seluruh kawasan Timur Tengah.²⁷⁵

Serangan ini berupa serangan yang menggunakan Drone MQ Reaper 9, sebuah pesawat tak berawak yang dioperasikan oleh militer AS, dengan kemampuan jelajah 14 jam saat terisi penuh dengan amunisi, dengan berbagai senjata, sensor visual yang kuat untuk mencapai sasaran, sehingga sangat akurat dan mematikan.²⁷⁶ Serangan ini terjadi di Bandara Baghdad dan berhasil menewaskan delapan orang termasuk seorang Jenderal Qassem Soleimani. Dengan dilakukannya serangan ini membuat tensi antara AS-Iran semakin memanas, keadaan ini juga membuat dunia internasional mulai menakar terancamnya keamanan dunia.

D. Serangan Siber Sebagai Kejahatan Internasional

Berdasarkan uraian penjelasan dan unsur kejahatan internasional, maka dapat dikonstruksi bahwa *serangan siber* sebagai kejahatan internasional. Adapun uraian unsur dimaksud dapat dikonstruksi sebagai berikut:

a. Unsur internasional, yakni adanya ancaman terhadap perdamaian dunia baik langsung maupun tidak langsung. Dalam konteks ini, cyberattack berpotensi untuk memberikan ancaman terhadap perdamaian dunia. Kasus cyber attack yang terjadi di Estonia dan Iran menunjukkan bahwa cyber attack dapat mengganggu jalannya suatu sistem pelayanan publik suatu negara

²⁷⁵ Clayton Thomas et.al, *U.S Killing of Qasem Soleimani : Frequently Asked Questions*, Congressional Research Service, 2020, hlm. 1.

²⁷⁶ Erwin Prima and Khory Alfarizi, *Bunuh Soleimani, Drone MQ-9 Reaper AS Paling Ditakuti di Dunia*, Tempo.Co, https://tekno.tempo.co/read/1294958/bunuh-soleimani-drone-mq-9-reaper-as-paling-ditakuti-didunia/full&view=ok, 14 January 2020.

yang dimana merupakan fasilitas vital yang diperuntukkan lebih dari satu negara seperti fasilitas perbankan dan perdagangan lintas negara. Pada kasus Stuxnet (2010), *cyberattack* menjadi sangat berbahaya karena dengan serangan ini seseorang dan/atau negara dapat secara mudah mengontrol aktifitas. Menurut Ralph Langner²⁷⁷ bahwa stuxnet digambarkan sebagai senjata siber yang digunakan untuk menyerang seluruh program nuklir Iran.²⁷⁸ Penggunaan senjata siber seperti ini akan sangat mudah digunakan saat ini dengan pertimbangan perkembangan massif informasi dan teknologi yang tak dapat dielakkan lagi. Sehingga terjadinya cyber attack secara langsung maupun tidak langsung dapat berpotensi mengancam perdamaian dan keamanan dunia.

b. Unsur transnasional, artinya cakupan atau lingkup *cyber attack* yang lintas antarnegara. Seperti yang sudah dijelaskan sebelumnya, serangan siber memanfaatkan *cyberspace* sebagai ranah untuk melancarkan serangan, sehingga serangan siber dapat bersifat *borderless*. Menurut Hata bahwa kejahatan cyber yang terjadi menunjukkan kedaulatan tradisional negara sangat mudah untuk ditembus, yang sekaligus melemahkan fungsi-fungsi kekuasaan tradisional suatu negara.²⁷⁹ Selain itu jika merujuk *Convention Against Transnational Organized Crime*, maka dapat dikategorikan bahwa cyber attack merupakan kejahatan transnasional.

²⁷⁷ Ralph Langner adalah seorang ahli di bidang telematika yang berkebangsaan Jerman.

²⁷⁸ James P. Farwell and Rafal Rohonzmskl, *Op. cit.,* hlm. 23

²⁷⁹ Hata, *Hukum internasional: Sejarah dan Perkembangan hingga Pasca Perang Dingin*, Malang; Setara Press, 2012, page, 110.

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

Pasal 3 konvensi tersebut mengkategorikan suatu kejahtan yang bersifat transnasional sebagai berikut: *For the purpose of paragraph 1 of this article, an offence is transnational in nature if:*²⁸⁰

- i. It is committed in more than one State
- ii. It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
- iii. It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
- iv. It is committed in one State but has substantial effects in another State.
- c. Unsur kebutuhan, artinya dibutuhkan kerjasama secara internasional antar negara-negara untuk menghadapi dan mengadili pelaku kejahatan siber termasuk cyber attack dalam suatu bingkai pengadilan internasional. Dalam konteks ini, dibutuhkan satu aspek interpenetration untuk menggambarkan urgensi kerjasama dimaksud dengan formula hukum perjanjian internasional. Solusi alternatif dalampenegakan hukum tersebutterhadap kejahatan yang bersifat transnasional dilandasi oleh keyakinan seluruh negara peserta konvensi bahwa, penegakan hukum terhadap kejahatan tersebut tidak dapat dilaksanakan secara optimal dan berhasil jika hanya dilakukan satu negara saja. Solusi alternatif penegakan hukum tersebut merupakan strategi baru dengan penerapan prinsip, "No

²⁸⁰ United Nation, Convention Against Transnational Organized Crime and The Protocol Thereto, Article 3.

Safe Haven" ditujukan untuk mempersempit ruang gerak aktivitas pelaku-pelaku kejahatan transnasional.²⁸¹

E. Analisis Kasus Pembuktian Serangan siber

Sejak perkembangan Information and Communication Technology (ICT), manusia mengenal cyberspace sebagai ruang dimensi terbaru. There is also a fifth one available for international conflicts.²⁸² Dimensi spasial kelima ini sangat berbeda dibandingkan dengan contoh-contoh yang disebutkan di atas. Memiliki jangkauan global, yang mengaburkan batasbatas fisik antar negara (tanpa batas), dan memungkinkan untuk beroperasi terlepas dari sistem politiknya, dengan aktor yang sangat beragam - dari individu, melalui berbagai pengelompokan, hingga negara.²⁸³

Serangan siber termasuk dalam kejahatan kontemporer yang menggunakan teknologi sebagai alat dalam mewujudkan kejahatan melalui cyber space. Sampai saat ini belum terdapat instrumen hukum internasional yang bersifat universal terkait pengaturan pembuktian serangan siber yang berkorelasi dengan pertanggungjawaban serangan tersebut. Pasal 14²⁸⁴ dan 21²⁸⁵ Convention on Cybercrime hanya memungkinkan

²⁸¹ Pengakuan atas prinsip tersebut telah dicantumkan dalam berbagai Konvensi Internasional tentang Pemberantasan Terorisme sejak tahun 1937 sampai dengan tahun 1999; Konvensi Internasional Menentang Korupsi tahun 2003(Konvensi Merida); Konvensi Menentang Kejahatan Transnasional Terorganisasi tahun 2000(Konvensi Palermo) beserta Protokol Tambahannya; dan Statuta ICC tahun 1998 /2002 (Statuta Roma) https://pusham.uii.ac.id/upl/article/id Hukum%20Pidana%20Internasional.pdf

²⁸² Ibid.

²⁸³ Cf. Michaela Melková and Tomáš Sokol, *Cyber Space as the New Dimension of the National Security*,

Banska Bystrica: Belianum, 2015, hlm.. 55-56.

²⁸⁴ European Union, *The Convention on Cybercrime*, Article 14

²⁸⁵ European Union, *Ibid*, Article 21.

adanya pembuatan peraturan prosedural dan kerjasama internasional terkait investigasi dan pengumpulan barang bukti kasus cyber crime. Penjelasan terkait kemungkinan kerjasama internasional diatur pada

Pasal 23 konvensi ini, yakni:

"General principles relating to international co-operation The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence".

Secara umum konvensi ini memberikan kewenangan kepada hukum domestic negara untuk membuat instrumen hukumnya baik berupa hukum domestic maupun perjanjian kerjasama dalam mengatasi kejahatan siber, termasuk variasi teknik serangan siber . Inilah yang menjadi dasar upaya pembuktian terhadap serangan siber yang terjadi di lingkup regional Uni Eropa, contohnya pada kasus Estonia 2007. Kerjasama ini dapat terjalin hanya kita telah mencapai konsensus dari para pihak yang terlibat. Sedangkan, untuk pembuatan peraturan prosedur dan peraturan domestic suatu negara berdasarkan pada kepentingan dan kehendak dari negar tersebut.

Pembuktian dibutuhkan pada tahap penyelidikan atau investigasi. Dalam membuktikan serangan siber , terdapat kendala dan tantangan tersendiri. *Pertama,* sifat serangan

borderless and anonym. Serangan siber dilakukan melalui dimensi cyberspace tanpa batasan luas dan wilayah, sehingga serangan siber bersifat borderless. Sifat ini menimbulkan tantangan dalam membuktikan tempat asal serangan. Pada kasus Estonia sebanyak 1-2 juta 'bot' yang telah terinfeksi sebelumnya di 175 yurisdiksi telah diatur untuk melancarkan serangan terkoordinasi terhadap target Estonia dengan membanjiri situs web dengan data.²⁸⁶ Namun pada tahap penyelidikan, Estonia hanya dapat membuktikan seorang siswa Estonia asal Rusia, Dmitri Galushkevic, ditangkap, didakwa, dan dihukum karena menargetkan situs web partai politik²⁸⁷ skalanya menunjukkan bahwa banyak orang kemungkinan besar terlibat dalam perencanaan dan pelaksanaan namun tidak dapat dibuktikan. Dmitri dapat dibuktikan sebagai penyerang karena dia melakukannya di dalam Estonia²⁸⁸, sehingga pelacakannya lebih mudah. Sifat anonim dimungkinkan dalam serangan siber , hal tersebut juga dilakukan oleh penyerang sebagai taktik agar tidak mudah dilacak untuk hal pembuktian.

Kedua, sukarnya menentukan tempat dan waktu serangan. Sukarnya menentukan tempat dan waktu serangan juga berhubungan dengan sifat serangan yang borderless dan anonym. Penggunaan teknologi dalam serangan siber membuat serangan ini menjadi lebih canggih. Perkembangan

²⁸⁶ Nations Involved: Estonia, Russian Federation, 2007 Serangan siber s on Estonia, halaman 53.

²⁸⁷ Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," International Affairs Review, 4 April 2009, http://www.iar-gwu.org/node/65

²⁸⁸ Rain Ottis, *Analysis of the 2007 Cyber Attack Against Estonia from the Information Warfare Perspective*, Published in Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth in 2008, Reading: Academic Publishing Limited, 2018.

teknologi dapat menyamarkan tempat dan waktu .²⁸⁹ Tantangan ini terjadi pada kasus Estonia, dari jumlah seluruh serangan yang diterima Estonia, hanya satu serangan yang dapat dibuktikan oleh Pengadilan Estonia terkait tempat dan waktunya. Hal ini dikarenakan sebagian besar data lalu lintas jaringan berbahaya tidak dapat diperoleh, sehingga tidak memungkinkan penyidik untuk mengejar banyak orang yang melakukan penyerangan.²⁹⁰

Ketiga, variasi teknik serangan. Pada pembahasan sebelumnya telah dijelaskan beberapa jenis teknik serangan yang bisa dilakukan, yakni meliputi DoS (Denial of Service), Malware, Phishing attacks devices and steals the relevant information on the system. Credential Reuse, SQL Injection, Cross-Site Scripting (XSS) dan Man in the Middle. Namun didorong perkembangan teknologi, saat ini serangan dapat memiliki hubungan dengan kegiatan militarian bersenjata yang berindikasi sebagai kejahatan agresi. Variasi teknik serangan ini dapat dilihat pada kasus Iran-Amerika Serikat. Penggunaan siber sebagai senjata dapat dilihat dari penggunaan teknologi drone untuk menyerang pangkalan udara Baghdad. Berdasarkan, Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations Rule 68291 terkait dengan Larangan ancaman atau penggunaan kekuatan, yang menyatakan bahwa "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations, is unlawful."

²⁸⁹ Joseph Migga Kizza, (2017) Guide to Computer Network Security, Computer Communications and Networks, Springer International Publishing AG, hlm. 535.

²⁹⁰ Rain Ottis, Op.Cit. Hlm. 6, diakses 8 Agustus 2020.

²⁹¹ Schmitt, M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, 2017, Rule 68.

Dalam Amandemen Kampala Pasal 8 bis paragraf 1 Statuta Roma mendefinisikan kejahatan agresi sebagai "the planning, preparation, initiation or execution, by a person in a position that can effectively exercise control on the political or military action of a State, and from an act of aggression, its character, gravity, and scale, constitutes a manifest violation on the Charter of the United Nations."."²⁹² Semetara itu, tindakan agresi ialah "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another, or in any other manner inconsistent with the Charter of the United Nations".

Berdasarkan uraian di atas, potensi serangan siber yang mengancam kedaulatan teritorial dan kemerdekaan politik PBB dapat dikategorikan sebagai tindakan melawan hukum. Tallinn Manual Rule 69 lebih lanjut menjelaskan penggunaan definisi kekuatan sebagai "A cyber activity which constitutes a use of force when its scale and effects are comparable to non-cyber operations.". Variasi teknik serangan baru ini kini juga merupakan tantangan individual bagi para pihak yang ingin membuktikan serangan siber, diperlukan tinjauan hukum humaniter di dalamnya.

Kempat, kekuatan politik. kekuatan politik. Kedua kasus yang coba dianalisis pada penelitian ini merupakan kasus yang berdasar pada konflik politik. Konflik ini juga menjadi tantangan dalam hal pembuktian serangan siber . Adanya tendensi menghalangi pembuktian, seperti yang dilakukan Rusia dengan tidak menerima permohonan "a formal investigation assistance request" to the Russian Supreme Procuratore in May of 2007,

²⁹² United Nation, *Rome Statute of the International Criminal Court*, Article 8 bis paragraph 1.

yang diajukan oleh Estonia²⁹³ menjadi dapat dianggap bukti penggunaan kekuatan politik untuk melindungi diri. Unsur kekuatan politik juga terdapat pada kasus Iran-Amerika Serikat. Menurut Miko Ardiyanto, serangan siber pada infrastruktur nuklir Iran oleh AS dapat dikategorikan sebagai intervensi terhadap kedaulatan negara Iran. Dalih Amerika bahwa tindakan ini dilihat sebagai bentuk pertahanan diri menggunakan pelajaran dari serangan militer pre-emptive untuk melindungi dari ancaman kemungkinan serangan nuklir dari Iran tidak dapat dibenarkan. Hal tersebut didasari tidak adanya aktivitas serangan bersenjata yang dilakukan oleh Iran terhadap AS. Oleh karena itu, unsur "When an Armed Attack Occurs" sebagaimana diatur dalam Pasal 51 Piagam PBB tidak terpenuhi. Pakar PBB Agnes Callamard menilai, hasil investigasi pembunuhan Qasem Soleimani oleh Amerika Serikat dengan drone adalah ilegal dan bertentangan dengan hukum internasional terkait Conduct of Hostilities.

Selain itu, pada kasus penggunaan tindakan serangan drone hanya dibenarkan sebagai tanggapan terhadap ancaman nyata. Informasi untuk menghindari ancaman ini dianggap sangat kabur jika dinilai dari konteks AS tidak menunjukkan bukti yang mengharuskan dilakukannya pembunuhan terhadap Soleimani.²⁹⁴ Adanya korban jiwa dalam serangan siber dikategorikan sebagai kejahatan agresif. Hal ini berdasarkan pemenuhan unsur aksi secara resmi oleh AS menyusul pernyataan Presiden Trump²⁹⁵ yang melakukan serangan

²⁹³ Rain Ottis, Op.Cit. Hlm. 3, diakses 8 Agustus 2020.

Nick Cumming- Bruce, *The Killing of Qassim Suleimani Was Unlawful, Say U.N Expert*, The New York Times, https://www.nytimes.com/2020/07/09/world/middleeast/qassim-suleimani-killing-unlawful.html , 9 July 2020.

²⁹⁵ The New York Times, *The Killing of Gen. Qassim Suleimani: What*

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI DALAM PERKEMBANGAN HUKUM INTERNASIONAL

siber menggunakan Drone MQ-9 Reaper, dikendalikan dari jarak jauh, dan digunakan untuk membunuh Panglima militer IRGC-QF Iran, Jenderal Qasem Soleimani, dan rombongan. Pembunuhan seorang Jenderal militer ini melanggar kedaulatan Iran. Sulitnya pembuktian serangan siber terkait kasus Iran-AS kali ini karena kendala dalam memberikan kesaksian tentang tanggung jawab negara dan unsur-unsur langkah perlindungan. Ini tidak lepas dari kekuatan politik kedua negara.

We Know Since the U.S. Airstrike, The New York Times https://www.nytimes.com/2020/01/03/world/middleeast/iranian-general-qassem-soleimani-killed.html, 3 January 2020.

BAB VI

FORMULA KERJASAMA INTERNASIONAL TERKAIT SERANGAN SIBER

A. Pengantar

Dalam dinamika masyarakat internasional tidak mudah untuk menetapkan suatu pengaturan terkait dengan suatu masalah internasional. Perbedaan kepentingan suatu negara sangat mempengaruhi proses pembentukan suatu hukum internasional. Perjanjian internasional merupakan salah satu sumber hukum internasional modern ini yang sangat signifikan. Keberadaan perjanjian internasional dalam prosesnya dapat sangat cair, hingga mengakomodir kehendak dan persetujuan negara atau secara umum subjek hukum internasional untuk mencapai tujuan bersama.²⁹⁶

Umumnya dalam suatu perjanjian internasional terdapat tiga tahapan yang mesti dilalui yakni Perundingan, Penandatanganan dan Pengesahan suatu perjanjian internasional. Sebelum melangkah ke tahap yang formal, biasanya terlebih dahulu dilaksanakan pendekatan-pendekatan informal untuk mendiskusikan suatu masalah internasional. Jika perjanjian yang hendak didorong dalam bentuk bilateral,

²⁹⁶ Boer Mauna, *op.cit.*, hlm. 82.

maka langkah yang dilakukan pun cukup sederhana dengan mempertemukan kedua belah pihak yang ingin membuat perjanjian. Lain halnya dengan perjanjian multilateral umum yang bersifat terbuka, maka dibutuhkan dorongan bersama dari beberapa negara untuk bersepakat melakukan pertemuan informal terlebih dahulu untuk mendiskusikan suatu masalah internasional. Terkait dengan serangan siber, maka dimensi multilateral dari perjanjian ini lebih terlihat. Meskipun bisa saja, langkah awal dapat terlebih dahulu dilakukan perjanjian bilateral antara dua negara yang memiliki kepentingan yang sama.²⁹⁷

Berbeda dengan ruang yang lain, ruang siber memiliki ciri khusus dengan kesulitan untuk menentukan waktu dan tempat kejadian. Sehingga dalam menentukan norma dalam ruang ini, minimal terdapat tiga hal menurut Lessig, sebagaimana yang diuraikan oleh Edi Atmaja, yang mesti diperhatikan yakni: (a) Siapa yang diatur; (b) Dimana mereka; (c) Apa yang mereka lakukan. Menurut Lessig jika negara tidak dapat mengetahui secara pasti siapa yang diatur, dimana mereka, dan apa yang mereka lakukan, maka negara tidak bisa mengatur norma dalam ruang siber secara sewenang-wenang.²⁹⁸ Untuk mengetahui individu yang diatur, lokasi serta perbuatan mereka, tentu dibutuhkan infrastruktur yang mumpuni sehingga bisa secara tepat mengatur dan menjaga hubungan dalam ruang siber tetap aman dan lancar.

²⁹⁷ I Wayan Parthiana. Hukum Perjanjian Internasional Bagian I. Bandung: Mandar Maju. 2002. Hal. 93.

²⁹⁸ Ap Edi Atmaja. Kedaulatan Negara di Ruang Maya Kritik UU ITE dalam Pemikiran Satcipto Rahardjo. Gema Keadilan Volume 1 No 1 tahun 2014. Hal 100

B. Formula Kerjasama Internasional

Hingga saat ini belum ada, instrumen hukum internasional khusus yang mengatur terkait dengan serangan siber yang terindikasi sebagai kejahatan agresi. Ketiadaan konvensi ini, bukan berarti menihilkan norma hukum internasional terkait dengan tantangan dunia modern saat. Namun secara umum terdapat beberapa norma yang telah didorong oleh berbagai kelompok atau negara yang memiliki perhatian khusus terhadap perkembangan penggunaan siber dan ancamannya sebagai suatu kejahatan agresi. Wibisono seperti yang dikutip dari Iskandar menguraikan lima norma siber yang didorong menjadi hukum internasional itu yakni : (a) Tallinn Manual oleh NATO; (b) Microsoft Norm Paper oleh Microsoft Corp; (c) Code of Conduct oleh China, Rusia dan beberapa kelompok negara lain yang berada dalam porosnya; (d) U.S Government Policy oleh Amerika Serikat; dan (e) 11 Norma siber oleh United Nations Group of Governmental Expert on Information Security (UN GGE)²⁹⁹. Namun hanya empat dari norma yang diatas yang relevan hanya 4 terkecuali Government Policy dari AS. Kami menilai keempat norma sudah mengakomodir perkembangan hukum internasional dalam bidang siber. Berikut merupakan uraiannya:

a. Tallinn Manual

Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, merupakan salah satu langkah organisasi internasional dalam hal ini NATO yang mendorong suatu norma internasional terkait dengan serangan siber. Keberadaan panduan ini dinilai sebagai langkah untuk mengatur dan

²⁹⁹ Hamonangan, I., & Assegaff, Z. Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. *Padjadjaran Journal of International Relations Vol. 1 No. 4, Februari 2020*, 342-363. hlm 354

memastikan keamanan dan stabilitas ruang siber global dalam kondisi damai, maupun dalam insiden tertentu yang dapat memicu penggunaan kekerasan atau konflik bersenjata. Tallinn Manual awalnya ditetapkan oleh *Cooperative Cyber Defense Center of Excellence* (CCD COE) NATO pada 2013. Lalu panduan ini diperbaharui pada tahun 2017 dengan *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations.*

b. Microsoft Norm Paper

Pada tahun 2014, Microsoft Corporation, salah satu perusahaan teknologi raksasa di AS, mendorong suatu norma keamanan siber Internasional. Tidak jauh berbeda dengan beberapa norma internasional yang lain, fokus norma ini pada tanggung jawab negara untuk menghindari atau mencegah serangan siber yang diluncurkan dari wilayah. Norma keamanan siber ini penting untuk mengurangi konflik internasional yang berbasis pada siber.³⁰¹

c. Code of Conduct

Pada tahun 2011, Shanghai Cooperation Organization (SCO) yang terdiri dari China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, dan Uzbekistan, mengajukan Kode etik internasional untuk Keamanan informasi pada sesi 66 Majelis Umum PBB. Di tahun 2015 melalui resolusi majelis umum no (A/66/359) berbagai komentar dan saran dari berbagai pihak pun dipertimbangkan lalu dilakukan revisi terhadap dokumen kode etik ini.

Kode etik ini dinilai bertujuan untuk mengidentifikasi hak dan tanggung jawab negara di ruang informasi, mempromosikan

³⁰⁰ Ibid,

³⁰¹ Ibid, hlm. 355.

secara konstruktif dan perilaku yang bertanggung jawab dalam menangani ancaman dan tantangan di ruang siber, serta membangun lingkungan informasi yang damai, aman, terbuka yang didirikan atas dasar kerjasama dan untuk memastikan penggunaan siber dan jaringannya yang komprehensif untuk pembangunan sosial dan kesejahteraan masyarakat, yang tidak bertentangan dengan tujuan untuk memastikan perdamaian dan keamanan internasional.³⁰²

Terdapat 13 poin norma yang termuat dalam kode etik ini. Kepatuhan terhadap kode etik ini bersifat sukarela dan terbuka untuk semua negara. Gagasan utama dari kode etik ini terletak pada tanggung jawab negara dalam meningkatkan sistem keamanan informasi dan sistem dalam wilayah mereka. Menurut McKune norma dalam kode etik ini menimbulkan keprihatinan serius terhadap HAM, hal ini tidak terlepas dari penekanan kode etik pada kedaulatan negara dan teritorial dalam ruang digital di atas segalanya, yang didominasi oleh intelijen, keamanan nasional, dan imperative untuk stabilitas rezim. 303

d. United Nations Group of Governmental Expert on Information Security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE ICT's) yang merupakan suatu lembaga para ahli yang dibentuk oleh PBB sebagai menjawab tantangan perkembangan dalam dunia siber. Grup ini dibentuk berdasarkan Resolusi Majelis Umum 68/243 yang bertujuan untuk mendorong pemahaman bersama dan mengidentifikasi

³⁰² United Nations General Assembly, Developments in the field of information and telecommunications in the context of international security, UN Document A/69/723, 13 Januari 2015

³⁰³ Hamonangan, I., & Assegaff, Z, Loc.cit

potensi ancaman dalam bidang siber, serta kemungkinan tindakan bersama untuk mengatasinya, termasuk norma, aturan, atau prinsip tanggung jawab perilaku negara, dan langkah-langkah membangun kepercayaan dengan tujuan untuk memperkuat keamanan internasional dalam bidang siber. Dalam Laporannya di tahun 2015, GGE bersepakat dan menetapkan 11 norma yang bersifat sukarela, tidak mengikat, merupakan prinsip perilaku yang bertanggung jawab dari negara yang bertujuan untuk mendorong lingkungan ICT yang terbuka, aman, stabil dapat diakses dan damai. Sebelas norma itu yakni:

- 1. Menjaga Perdamaian dan Keamanan Internasional sebagaimana tujuan PBB;
- 2. Mempertimbangkan semua Informasi yang relevan, termasuk konteks, tantangan serta konsekuensi dari insiden kasus ICT;
- 3. Tidak menggunakan wilayah mereka untuk suatu aktivitas yang salah secara internasional;
- 4. Mempertimbangkan cara terbaik dalam mengatasi ancaman penggunaan ICT untuk tindakan kejahatan;
- Memastikan penggunaan ICT yang aman, menghormati HAM, termasuk hak privasi, serta kebebasan berekspresi;
- 6. Menghindari melalakukan tindakan atau mendukung aktvitas ICT yang bertentangan dengan kewajibannya berdasarkan hukum internasional;
- 7. Mengambil tindakan tepat untuk melindungi infrastruktur kritis mereka dari ancaman ICT;
- 8. Menanggapi permintaan bantuan negara lain terkait dengan perlindungan infrastruktur kritis dari ancaman ICT;

- 9. Mengambil langkah yang wajar dalam memastikan keamanan produk ICT, serta mencegah penyebaran alat dan teknik ICT yang berbahaya;
- 10. Mendorong pelaporan yang bertanggung jawab atas kerentanan ICT dan berbagi informasi atas solusi yang terbaik dalam membatasi ataupun menghilangkan potensi ancaman ICT;
- 11. Larangan untuk mendukung aktivitas untuk merusak sistem informasi dari tim tanggap darurat resmi negara lain. Serta menghindari keterlibatan tim tanggap darurat resmi negaranya untuk terlibat dalam aktivitas internasional yang berbahaya.³⁰⁴

Jika melihat beberapa norma yang terdapat satu semangat yang sama untuk meningkatkan keamanan dalam dunia siber, menghindari penggunaan praktek penggunaan kekuatan dalam melakukan balasan terhadap serangan siber yang tetap dalam koridor mewujudkan tujuan PBB. Secara historis proses pembentukan norma hukum internasional ini, berangkat dari pandangan Nato dengan Tallinn Manualnya pada tahun 2013. Lalu di respon oleh kelompok Shanghai Cooperation Organization, dengan Code of Conduct mereka pada tahun 2015. Keseluruhan norma ini kemudian diakomodir dalam 11 norma yang diajukan oleh GGE ICT's pada tahun 2015. Meskipun demikian karena tidak menyepakati pertemuan selanjutnya, maka langkah GGE ICT untuk meningkatkan keamanan siber cukup terhambat. Hingga akhirnya PBB kembali membentuk GGE yang baru yang dikenal dengan *Open-Ended*

³⁰⁴ United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Document A/70/174, 22 July 2015.

Working Group (OEWG) guna melanjutkan pembahasan dalam periode sidang 2019-2020 dan 2020-2021.³⁰⁵

C. Asean Menghadapi Tantangan Serangan Siber

Secara regional di ASEAN, sendiri telah melakukan berbagai upaya untuk mendorong kesadaran dan komitmen bersama dalam meningkatkan keamanan siber. Beberapa upaya ASEAN ini dapat kita identifikasi dari berbagai dokumen kerja sama seperti dalam ASEAN Leaders' Statement on Cybersecurity Cooperation pada KTT ASEAN ke 32 di Singapura pada tahun 2018. Selain itu di tahun sebelumnya, di Manila, disepakati ASEAN Declaration to Prevent and Combat Cybercrime. Pada tahun 2016, di Brunei Darussalam, negaranegara ASEAN telah sadar akan pentingnya perlindungan data pribadi melalui ASEAN Framework on Personal Data Protection. Selain itu jauh sebelumnya di Tahun 2012, dalam Asean Regional Forum (ARF) ke 19 di Kamboja, para menteri luar negeri di ASEAN telah bersepakat dalam meningkatkan kerjasama dalam menjamin keamanan siber melalui ARF Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security. 306

Pada tahun 2017, ASEAN menyelenggarakan 2nd *International Security Cyber Workshop Series* yang bertujuan untuk melestarikan dan memperkaya stabilitas siber di kawasan regional ASEAN. Workshop ini secara umum mendiskusikan peluang dan tantangan dalam konteks perdamaian dan keamanan dalam Cyberspace. Terdapat 4 tema utama yang didiskusikan dalam workshop ini yakni : (a) The 2017 GGE

³⁰⁵ Hamonangan, I., & Assegaff, Z, *Op.cit.* hlm. 356.

³⁰⁶ Muhammad Aris Yunandar, Laporan Utama Kerja Sama Keamanan Siber di ASEAN dalam Menyambut Industri 4.0, Masyarakat ASEAN edisi 22 September 2019, hlm. 13-14.

and Issues for International Agreement; (b) Kedaulatan dan perspektif global dalam hukum internasional terkait ruang siber; (c) Perspektif regional dalam norma dan tindakan membangun kepercayaan; (d) Langkah selanjutnya untuk kerja sama internasional. Berikut merupakan uraiannya 307:

a. The 2017 GGE dan Isu kerja sama internasional

Tidak tercapainya kesepakatan pada sidang GGE's 2017, bukan berarti bahwa laporan dan rekomendasi ke Majelis Umum PBB yang sebelumnya ada harus diabaikan. Kegagalan GGE's dalam mencapai kesepakatan dikarenakan lingkungan geopolitik pasca kesuksesan GGE's ditahun 2015 yang menetapkan 11 norma dalam pengaturan informasi, komunikasi dan teknologi. Para ahli dalam forum tersebut menilai bahwa sulitnya mencapai kesepakatan dalam beberapa hal seperti analisis ancaman, kekuatan mengikat dari perjanjian, dan peningkatan kapasitas serta peningkatan kepercayaan bersama. Alasan utama mereka tidak bersepakat adalah penerapan hukum internasional yang ada terhadap ICT's dan bagaimana norma-norma yang tidak mengikat dapat melahirkan pertanggungjawaban negara. 308

Kesebelas norma tersebut, tidak dapat mencegah konflik dan kesulitan negara dalam menegakkan norma-norma tersebut dalam praktik. Hal ini dapat dilihat pada beberapa pertanyaan mendasar yang masih menyoal pendefinisian *use of force* dalam konteks siber. Beberapa pendapat mengatakan bahwa mereka tidak mampu mendefinisikan *use of force*. Dalam hal ini negara-negara cenderung mengambil tindakan defensive

³⁰⁷ UNIDIR.. Preserving and Enhancing International Cyber Stability : Regional Realities and Approaches in ASEAN. Singapore: UNIDIR. 2017, hlm. 3.

³⁰⁸ Ibid.

dalam merespon penggunaan *use of force* dalam konteks siber. 309

Hal lain yang dibutuhkan oleh negara, adalah terciptanya berbagai perjanjian baik yang bersifat bilateral, regional maupun internasional untuk membantu tiap negara dalam meningkatkan kepercayaan diantara mereka. Pendekatan berbagai pihak secara terbuka dibutuhkan untuk meningkatkan persatuan regional dalam mendorong kearah proses multilateral. Para pembicara dalam forum itu juga memberikan perhatian khusus pada asimetri informasi diantara 25 anggota dan mereka yang tergabung dalam perumusannya. Sebagai upaya untuk mendorong ruang ICT's yang terbuka, stabil dan aman, banyak negara perlu merasa dilibatkan dan didengar dalam berbagai diskusi ICT's dalam hubungannya dengan isu keamanan internasional.³¹⁰

b. Kedaulatan dan perspektif global hukum internasional mengenai ruang siber.

Dalam konteks kedaulatan, dititik beratkan pada urgensi partisipasi negara-negara secara lebih luas di tingkat regional dalam rangka menciptakan ruang yang lebih luas, bagi keterlibatan negara-negara secara internasional. Dalam prakteknya, hukum humaniter internasional (HHI) tidak secara eksplisit menyebutkan tentang serangan siber, namun dalam prinsipnya HHI telah mengatur terkait dengan *Distinction, Proportionality,* dan *Military Necessity* dan berbagai pengaturan terkait dengan tindakan jahat (*hostility act*) suatu negara dalam sebuah konflik yang terjadi pada ruang siber.³¹¹

³⁰⁹ Ibid.

³¹⁰ Ibid, hlm. 4.

³¹¹ Ibid.

Hal yang sangat berbahaya dalam operasi siber bagi negara adalah menjamin, apakah operasi siber tetap sejalan dengan doktrin dan hukum internasional. Dalam konteks ini penggunaan ICT untuk tujuan militer harus tetap sejalan dengan prinsip kedaulatan negara. Dalam praktiknya beberapa negara dengan peralatan siber yang canggih tidak menempatkan prinsip kedaulatan negara sebagai suatu hal yang harus dijunjung tinggi, dalam kerangka norma dan hukum internasional. Peningkatan transparansi, kemampuan siber tiap negara, merupakan tahap awal dalam membangun kepercayaan, dan stabilitas di ruang siber dalam kehidupan internasional.³¹²

Secara umum, para ahli dalam workshop ini juga bersepakat, bahwa tidak ada kekosongan hukum dalam mengatur terkait dengan tindakan jahat dalam perilaku di ruang siber. Sehingga tidak terdapat urgensi untuk membuat suatu perjanjian internasional atau konvensi baru terkait hal ini. Mereka juga mengingatkan agar tidak menerapkan standar norma yang lebih tinggi dalam ruang siber dibanding dengan ruang yang lain. Yang menjadi tantangan utama bagi masyarakat internasional adalah mengatur aktivitas yang menjadi batasan terhadap use of force serta aktivitas di masa damai, seperti misalnya yang dilakukan oleh proxy, jaringan kejahatan ruang siber yang terorganisir.³¹³

Dalam konteks global, terdapat keraguan terkait dengan satu lembaga permanen khusus terkait dengan ICT's, hal ini didasarkan pada banyak negara masih dalam tahap awal mengembangkan kelembagaan dan struktur hukum untuk isu siber yang bersifat lintas batas. Kondisi geopolitik internasional saat ini juga berimbas pada menurunnya kepercayaan diantara

³¹² Ibid.

³¹³ Ibid hlm. 5.

negara yang menjadi tantangan dalam pembentukan lembaga permanen internasional terkait dengan ICT.³¹⁴

c. Perspektif regional atas norma dan Confidence Building Measures (CBM's)

Kondisi Asia Pasifik secara regional sangat beragam, meliputi latar belakang ekonomi yang berbeda. Sebagai rumah dari 55% total pengguna internet di seluruh dunia, masih terdapat kesenjangan yang sangat nyata antara negara. Lebih dari separuh rumah tangga di wilayah ini belum memiliki akses terhadap internet. Beberapa negara telah melakukan pengembangan untuk menjembatani kesenjangan ini, dengan peningkatan konektivitas masing-masing warga negara. Upaya ini pun berdampak pada lemahnya keamanan siber yang tidak terlalu diprioritaskan. Selain itu perbedaan nilai-nilai nasional, struktur pemerintahan, ditambah pandangan yang kuat dan beragam terkait dengan isu-isu khusus seperti, kedaulatan, HAM, dan kontrol konten, menjadi aspek penting yang tidak boleh diabaikan. ³¹⁵

Laporan GGE's sebelumnya dinilai telah memberikan peta jalan dengan menawarkan komitmen tingkat tinggi negaranegara ASEAN yang menetapkan ekspektasi atas perilaku negara yang bertanggung jawab. Bahkan dengan prinsip tingkat tinggi yang ada, asimetri yang ada dalam keahlian teknis siber, hukum dan politik serta kemampuan siber yang menjadi hambatan dalam meningkatkan kepercayaan antara negara.³¹⁶

³¹⁴ Ibid.

³¹⁵ Ibid, hlm. 6.

³¹⁶ Ibid.

d. Perspektif regional dan langkah selanjutnya dalam mendorong kerja sama internasional.

Pada tahun 2017, setidak nya telah terdapat delapan puluh hingga sembilan puluh negara sedang melakukan revisi terkait dengan hukum keamanan siber. selain itu terdapat tiga puluh negara yang secara aktif menginvestasikan pengembangan keamanan siber secara ofensif. Terdapat kecenderungan peningkatan keterlibatan dan kerja sama internasional diantara negara-negara khususnya dalam hal penggunaan domain siber yang ditujukan untuk membangun ketahanan arsitektur siber, baik pada masa damai maupun pada saat konflik.³¹⁷

Jeda pada tahapan GGE's juga memberikan kesempatan untuk meningkatkan partisipasi dari berbagai negara lainnya. Dengan melibatkan berbagai Non Governmental Organisation (NGO), sebagaimana yang terjadi pada proses *Tallinn Manual* dan *Hague Process* untuk memungkinkan partisipasi yang lebih luas. Meskipun disadari bahwa boleh jadi masing-masing negara tidak selalu setuju dengan kesepakatan yang diambil, namun hal ini mengarah pada diskursus hukum internasional dan tata kelola ruang siber. ³¹⁸

Pada akhir sesi, para peserta diminta untuk mempertimbangan enam format potensial dengan beragam karakteristik untuk memajukan diskusi internasional dengan preferensi regional. Enam format tersebut yakni : (a) Lanjutan Kelompok Ahli Pemerintah (Another GGE's) ; (b) Kelompok Kerja Terbatas; (c) Kelompok Kerja Terbuka; (d) Conference on Disarmament; (e) UN Disarmament Commission; (f) Conference of States.³¹⁹

³¹⁷ Ibid, hlm. 7.

³¹⁸ Ibid, hlm. 7.

³¹⁹ Ibid.

Pada tahun 2019 di Thailand, berlangsung ASEAN Defence Ministers' Meeting Plus (ADMM-plus), bersepakat untuk menetapkan Joint Statement by the ADMM-Plus Defence Ministers on Advancing Partnership for Sustainable Security. Pernyataan bersama ini merupakan suatu langkah positif dalam mengembangkan norma hukum internasional dalam bidang siber³²⁰. Indonesia secara khusus juga terlibat aktif dalam merumuskan norma hukum internasional di bidang siber dalam kerangka Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (OEWG ICT's). Indonesia juga merupakan salah satu anggota khusus dari UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE ICT's) periode 2019-2021.321 Bukan hal yang mustahil, jika kedepannya Indonesia dapat berperan signifikan dalam menentukan pengaturan dalam hukum internasional terkait dengan siber.

³²⁰ Muhammad Aris, Op.cit. hlm. 14.

³²¹ Anonym, *Indonesia Suarakan Stabilitas Siber di PBB*, dapat diakses secara daring melalui https://kemlu.go.id/portal/id/read/1327/view/indonesia-suarakan-stabilitas-siber-di-pbb, diakses pada 6 Oktober 2020

KORELASI KEJAHATAN SIBER DAN KEJAHATAN AGRESI	
DALAM PERKEMBANGAN HIIKUM INTERNASIONAL	

DAFTAR PUSTAKA

- Anne Wagner, e. (2007). *Interpretation, Law and the Construction of Meaning.* Netherlands: Springer.
- Arief, B. N. (2001). *Sari Kuliah Perbandingan Hukum.* Semarang: Materi Kuliah Program Pascasarjana Ilmu Hukum Universitas Diponegoro.
- Asshiddiqie, J. (2006). *Pengantar Ilmu Hukum Tata Negara.* Jakarta: Sekjen dan Kepaniteraan Mahkamah Konstitusi.
- Atmasasmita, R. (1995). *Pengantar Hukum Pidana Internasional.*Bandung: Eresco.
- Atmasasmita, R. (2003). *Pengantar Hukum Pidana Internasional*. Bandung: Refika Aditama.
- Anonym, 2020, *Indonesia Suarakan Stabilitas Siber di PBB,* dapat diakses secara daring melalui https://kemlu.go.id/portal/id/read/1327/view/indonesia-suarakan-stabilitas-siber-di-pbb, diakses pada 6 Oktober 2020
- Avila, H. (2007). *Theory of Legal Principle*. Netherlands: Springer.
- Awaluddin, H. (2012). *HAM Politik, Hukum, dan Kemunafikan Internasional.* Jakarta: Kompas.
- B. Broomhall. (1999). Article 22, Nullum crimen Sine Lege, in O. Triffterer (ed.), Commentary on the Rome Statute of the International Criminal Court. 450-451.
- Barak, A. (2005). *Purposive Interpretation in Law.* New York: Princeton University Press.

- Barriga, S., & Grover, L. (2011). A Historic Breakthrough on the Crime of Aggression. *AJIL Volume 105*, 518-519.
- Bassiouni, M. C. (1987). *International Criminal Law Vol III Enforcement.* New York: Transnational Publishers, Inc.
- Bassiouni, M. C. (1987). *International Criminal Law, Vol. III Enforcement.* New York: Transnational Publishers Inc.
- Black, H. C. (1994). *Black's Law Dictionary Fifth Edition*. West Publishing Co.
- Boele-Woelki, e. a. (1998). *Internet: Which Court Decides? Which Law Applies?* The Hague/London/Boston: Kluwer Law International.
- Boister, N. (2003). Transnational Criminal Law. *EJIL Volume 14 No. 5*, 965.
- Brierly, J. (1963). *Hukum Bangsa-Bangsa*. Jakarta: Bharatara.
- Brownlie, I. (1998). *Principles of Public International Law, 5th ed.* Oxford: Clarendon Press.
- Buana, M. S. (2007). *Hukum Internasional Teori dan Praktik,*. Bandung: Nusamedia.
- Cassese, A. (2007). On Some Problematical Aspects of the Crime of Aggression. *Leiden Journal International Law, Volume 20*, 842.
- Chimni, B. (2007). The Past, Present and Future of International Law: a Critical Third World Approach,. *Melbourne of International Law Journal, Volume* 8, 500.

- Clark, R. S. (2002). Rethinking Aggression as a Crime and Formulating Its Elements: The Final Work-Product of the Preparatory Commission for International Criminal Court. *Leiden Journal of International Law, Volume 15*, 859-890.
- Clough, J. (2010). *Principle of Cybercrime*. Cambridge: Cambridge University Press.
- Convention, U. N. (1948). Nations Charter.
- Court, T. C. (n.d.). *The ICC and The Crime of Aggression.* Factsheet.
- David B Henry, e. a. (Juni 2004). A Return Potential Measure of Setting Norms For Aggression. *American Journal of Community Psychology Volume* 33, 131.
- Dinstein, Y. (2002). Computer Network Attacks and Self-Defense. 76 Int'l L. STUD, 99, 102-103.
- Driedger, E. (1983). *Construction of Statutes, 2nd ed.* Toronto: Butterworths.
- Erdbrink, T. (May 2012). Iran Confirms Attack by Virus That Collects Information. *New York Times*.
- Eriksen., E., & Weigard, J. (2005). *Understanding Habermas, Communicative action and Deliberative Democracy.*London: NY Continuum Press.
- Farwell, J. P., & Rohonzinski, R. (February-March 2011). Stuxnet and the Future of Cyber War. *Survival Volume 53*.
- Ferenz, D. M. (2010). The Crime of Aggression: Some Personal Reflections on Kampala. *Leiden Journal of International Law, Volume* 23, 905-908.

- Ferreira-Synman, M. P. (2009). *The Erosion of State Sovereignty in Public International Law : Towards a World Law?* Doctor Legum: University of Johannesburg.
- Fiddler, D. P. (June 2012). Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law. *ASIL Volume 16 Issue* 22.
- Fletcher, M. K. (2010). Defining the Crime of Aggression: Is There an Answer to the International Criminal Court's Dilemma. *Air Force Law Review, Volume 65*, 238.
- Fromm, E. (2000). Akar Kekerasan. Jakarta: Pustaka Pelajar.
- Gadamer, H. G. (1975). *Truth and Method.* New York: The Seabury Press.
- Gema, A. J. (2000). Cybercrime: Sebuah Fenomena di Dunia Maya. www.theceli.com.
- General Treaty for Renunciation of Wars as an Instruments of National Policy Art. (n.d.). 60.Aug 27, 1928, 46 Stat.2343, 94 L.N.T.S. 57 (hereinafter Treaty for Renunciation of War).
- Glennon, M. J. (2010). The Blank-Prose Crime of Aggression. *The Yale J. of Int'l Law, Vol. 35:71*, 72.
- Gold, S. A. (n.d.). The Cosmopolitan Foundation of the (Kantian) State. *Rensselaer Polytechnic Institute*.
- Habermas, J. (1996). Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy.

 Massachusetts: The MIT Press.

- Habermas, J. (1998). *The Inclusion of the Other: Studies in Political Theory.* Massachusetts: The MIT Press.
- Hamidi, J. (2011). *Hermeneutika Hukum: Sejarah-Filsafat & Metode Tafsir.* Malang: UB Press.
- Hamonangan, I., & Assegaff, Z. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. *Padjadjaran Journal of International Relations Vol.* 1 No. 4, Februari 2020, 342-363.
- Harris, D. (1998). Case and Materials on International Law, 5th ed. London: Sweet & Maxwell.
- Hata. (2012). Hukum Internasional: Sejarah dan Perkembangan hingga Pasca Perang Dingin, . Malang: Setara Press.
- Hiariej, E. O. (2009). *Pengantar Hukum Pidana Internasional.* Jakarta: Airlangga.
- Hidayat, K. (1996). *Memahami Bahasa Agama: Sebuah Kajian Hermeneutik*. Jakarta: Paramadina.
- Higgins, R. (1994). *Problems and Process: International Law and How We Use it.* New York: Oxford University.
- Hinkle, K. C. (2011). Countermeasures in the Cyber Context:
 One More Thing to Worry About. *YJIL Online Volume 17*,
 12.
- Husaini, A., & Al-Baghdadi, A. (2007). *Hermeneutika dan Tafsir Al-Qur'an*. Jakarta: Gema Insani.
- Jemielniak, J., & Miklaszewicz, P. (2010). *Interpretation of law in the Global world: From Particularism to a universal Approach*. London: Springer.

- Jenson, B. (1996). Cybertalking: Crime, Enforcement and Personal Responsibility in the On-Line World. 10.
- Jescheck, H. (2004). The General Principles of International Criminal Law Set Out in Nuremberg, as Mirrored in the ICC Statute. *Journal of International Criminal Justice, Volume* 38, 44.
- Judhariksawan. (2005). *Pengantar Hukum Telekomunikasi.* Jakarta: Rajawali Press.
- Kaspersen, H. W. (2009). *Cybercrime and Internet Jurisdiction* (*Discussion Paper*). Netherland: Council of Europe.
- Kittichaisaree, K. (2002). *International Criminal Law.* New York : Oxford University Press.
- Korth, B. (2006). Establishing Universal Human Rights Through War Crimes Trials And The Need For Cosmopolitan Law In An Age Of Diversity. *Liverpool Law Review Volume 27*, 104.
- Kusumaatmadja, M. (1976). Masyarakat dan Pembinaan Hukum Nasional: Suatu Uraian tentang Landasan Pikiran, Pola, dan Mekanisme Pembangunan Hukum di Indonesia. Bandung: Bina Cipta.
- Leyh, G. (2011). Hermeneutika Hukum: Sejarah, Teori, dan Praktik. Bandung: Nusamedia.
- Lorents, P., Ottis, R., & Rikk, R. (2009). Cyber Society and Cooperative Cyber Defence In Internationalization, design and Global Development. *Lecture Notes in Computer Science Volume 5623*, 180-186.

- Luban, D. (2010). Fairness to Rightness: Jurisidiction, Legality, and Legitimacy of International Law,. Oxford: Oxford University Press.
- M. Cherif Bassiouni and Benjamen Ferencz. (1999). The Crime Against Peace in International Criminal Law.
- Mansur, D. M., & Gultom, E. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi.* Bandung: Refika Aditama.
- Manuputty, A. d. (2008). *Hukum Internasional*. Depok: Rech-ta.
- Marmor, A. (2005). *Interpretation and Legal Theory, 2nd Ed. (revised).* Oxford: Hart Publishing.
- Martono. (2007). *Pengantar Hukum Udara Nasional dan Internasional.* Jakarta: PT. Raja Grafindo Persada.
- Marx, K. (1959). Economic and Philosophic Manuscripts of 1844.
- Maskun. (2011). *Kejahatan Cyber Crime*. Makassar: Pustaka Pena Press.
- Mauna, B. (2005). *Hukum Internasional: Pengertian, Peranan,* dan Fungsi Dalam Era Dinamika Global. Bandung: PT.Alumni.
- Michael N. Schmitt. (1999). Compute Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. 37 Colum J. of Transnat'l Law, 885.
- Mugerwa, N. (1968). Subject of International Law. New York: Mac Millan.

- Muhammad Aris Yunandar, 2019, Laporan Utama Kerja Sama Keamanan Siber di ASEAN dalam Menyambut Industri 4.0, Masyarakat ASEAN edisi 22 September 2019, hlm 13-14
- Nations, U. (n.d.). *Universal Declaration of Human Rights.*
- Nations, United. General Assembly, Developments in the field of information and telecommunications in the context of international security, UN Document A/69/723, 13 Januari 2015
- Nations, United. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Document A/70/174, 22 July 2015.
- Nations, United. UNIDIR. 2017. Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN. Singapore: UNIDIR
- Nurhidayat, D. (Agustus 2006). Eksaminasi Terhadap Perkara Pidana Terkait Pembobolan Situs Komisi Pemilihan Umum. *Jurnal Hukum Teknologi Volume 2 Nomor 1*, 29.
- O'Keefe, R. (2004). *Universal Jurisdiction : Clarifying the Basic Concept.* New York: Oxford University Press.
- Oppenheim, L. (1928). International Law: a Treatise.
- Ottis, R. (2008). Analysis of the 2007 Serangan siber s Against Estonia from the Information Warfare Perspective. Proceeding of the 7th European Conference on Information warfare and Security (pp. 163-168). Plymouth: Academic Publishing Limited.

- Palmer, R. E. (1999). The Relevance of Gadamer's Philosophy Hermeneutics to Thirty Topic or Field of Human Activity. Carbondale: Southern Illinois University.
- Parthiana, I. W. (2006). *Hukum Pidana Internasional.* Bandung: Yrama Widya.
- Perrez, F. X. (2000). Cooperative Sovereignty from Independence to Interdependence in the Structure of International Environmental law. The Hague: Kluwer Law International.
- Power, R. (2020). *Tales of Digital Crime from the Shadows of Cyberspace*. USA: QUE Division of Macmillan.
- Putriyanti, A. (2009). Yurisdiksi di Internet. *Media Hukum Volume IX No.2*, 2.
- Quade, S. C. (2009). *Encyclopedia Cyber Crime*. Westport: Greenwood Press,.
- Raharjo, A. (2002). Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung : Citra Aditya.
- Report of The Commission on The use of The Principle of Universal Jurisdiction by Some Non-African States as Recommended by The Conference of Ministers of Justice or Attorneys General, EX.CL/411(XIII). (2008). African Union.
- Right, Q. (1956). The Prevention of Aggressions. *AJIL, Volume* 50, 514.
- Robinson, W., & Harris, J. (2000). Towards a Global Ruling Class? Globalization and the Transnational Capitalist Class,. *Science and Society, Volume 64*, 11.

- Romani, C. F. (2007). Sovereignty and Interpretasi of International Norms. New York: Springer.
- Romani, C. F. (2007). Sovereignty and Interpretation of International Norms. New York: Springer.
- Rosenne, S. (2004). *The Perplexities of Modern International Law.* Netherlands: Martinus Nijhoff Publishers.
- Rosenoer, J., & Smigel, K. (1997). Notable Legal Development . *Cyberlex*.
- Safitri, I. (1999). Tindak Pidana di Dunia Cyber. *Insider Legal Journal From Indonesian Capital and Investment Market*.
- Samekto, A. (2009). *Negara dalam Dimensi Hukum Internasional.* Bandung: PT Citra Aditya Bakti.
- Schuster, M. (2003). The Rome Statute and The Crime of Aggression: A Gordian Knot in Search of a Sword,. 14 Crim. L.F. 1, 4.
- Setyawanta, T. (2005). Pengaturan Hukum Penanggulangan Pembajakan dan Perompakan Laut di Wilayah Indonesia. Jurnal Media Hukum, Volume V. No.1.
- Shaw, M. (2008). *International Law, 6th ed.,.* Cambridge: Cambridge University Press.
- Simmab, F. i. (2002). the charter of the United Nations: A Commentary, Volume 1.
- Sinaga, O. (2010). Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia. *Makalah IPB Bogor*, 10.
- Siregar, A. (2001). *Negara, Masyarakat, dan Teknologi Informasi.* Yogyakarta: Makalah.

- Sklair, L. (2004). The Transnational Capitalist Class (2001); B S Chimni, An Outline of a Marxist Course on Public International Law. *Leiden Journal of International Law Volume 17*, 1.
- Starke, J. G. (2010). *Pengantar Hukum Internasional (Edisi Kesepuluh)*. Jakarta: Sinar Grafika.
- Steiner, H. J., Alston, P., & Goodman, R. (2008). *International Human Rights in Context: Law, Politics, Moral, 3rd.* New York: Oxford University Press.
- Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime)*. Jakarta: PT. Raja Grafindo Persada.
- Sumardi, J. (1996). *Hukum Ruang Angkasa (Suatu Pengantar).*Jakarta: PT. Pradnya Paramitha.
- Suryokusumo, S. (1987). *Organisasi Internasional.* Jakarta: Penerbit Universitas Indonesia.
- Suryokusumo, S. (2007). *Studi Kasus Hukum Internasional.* Jakarta: Tata Nusa.
- Suryono, E., & Arisoendha, M. (1991). *Hukum Diplomatik: Kekebalan dan Keistimewaannya.* Bandung: PT. Angkasa.
- Teeple, G. (1997). Globalization as the Triumph of Capitalism: Private Property, Economic Justice and the New World Order in Ted Schrecker. *Surviving Globalism: The Social and Environmental Challenges*, 15-16.
- Todd, M. G. (2009). Armed Attack in Cyberspace Deterring Asymmetric Warfare With an Asymmetric Definition. *The Air Force Law Review, Volume 64*.

- Veigh, S. M. (2007). *Jurisprudence of Jurisdiction*. Routledge: Cavendish.
- Vyver, J. D. (1989). *The Concept of Political Sovereignty.* Visser C.,Ed., Essay in honor of Ellison Kahn,.
- Walker, C. (2006). Cyber-terrorism: Legal principle and law in the United Kingdom. *Pennsylvania State Law Review* 625, 635.
- Widjojo, W. H. (2005). Cybercrimes dan Pencegahannya. *Jurnal Hukum Teknolog iFakultas Hukum Universitas Indonesia, Volume* 2, 7.
- Wiebe, W. (2000). *Tindak Kejahatan Melalui Komputer.*Makassar: Seminar.
- Wisnubroto, A. (1999). *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer.* Yogyakarta: Penerbitan Universitas Atmajaya.
- Wiston, K. (Citra Aditya). *The Internet: Issues of Jurisdiction and Controversies Surrounding Domain Names.* Bandung: 2002.
- Zeviar-Geese, G. (n.d.). The State of the Law on Cyberjurisdiction and Cybercrime on the Internet. *California Pacific School of Law*.

BIODATA SINGKAT



Maskun. Menyelesaikan Program Sarjana pada Fakultas Hukum Unhas, Magister pada Fakultas Program Hukum University of New South Wales, Sydney Australia, dan Program Doktor pada Fakultas Hukum Universitas Selain Hasanuddin. mengajar, penulis juga aktif pada penelitian dan pertemuan di bidang Hukum Lingkungan baik dalam maupun luar negeri. Beberapa karya di bidang Hukum Lingkungan adalah Kontributor Hukum Lingkungan: Teori, Kasus, dan

Legislasi (Penerbit Kemitraan Partnership dan AUSAID); dan Editor pada Hukum Lingkungan dan Hukum Penataan Ruang Karya Prof. Dr. A. Muh. Yunus Wahid, S.H.,M.Si (Penerbit Prenada Kencana). Saat ini, aktif dalam IUCN Academy yang merupakan perhimpunan pengajar hukum lingkungan. Penulis dapat dihubungi melalui e-mail: maskunmaskun31@gmail.com



Naswar, Menyelesaikan Program pada Fakultas Sarjana Hukum Unhas, Program Magister pada Fakultas Hukum Universitas Padjadjaran, dan saat ini sementara menyelesaikan Program Doktor pada Fakultas Hukum Universitas Selain Hasanuddin. mengajar, penulis juga aktif pada penelitian dan pertemuan di bidang Hukum Tata Negara dan Hukum Keuangan. Berbagai penelitian di bidang Hukum Tata Negara dan Hukum Keuangan telah dilakukan baik dalam skema

penelitian RistekDikti maupun skema Internal Universitas Hasanuddin.



Achmad, Menyelesaikan Program pada Fakultas Sarjana Hukum Program Magister pada Unhas. Hukum Fakultas Universitas Selain Airlangga. mengajar, penulis juga aktif pada penelitian dan pertemuan di bidang Hukum Ekonomi Islam. Berbagai penelitian di bidang Hukum (Ekonomi) Islam telah dilakukan baik dalam skema penelitian RistekDikti maupun skema Internal Universitas Hasanuddin.



Hasbi Assidiq, lahir di Bantaeng, Menyelesaikan 28 Maret 1997. Program Sarjana pada Fakultas Hukum. Universitas Hasanuddin dengan konsentrasi pada Hukum Lingkungan Internasional pada 2020. Penulis merupakan editor atas buku: Memahami Transformasi Hukum Tidak Tertulis Menuju Hukum Tertulis: Upaya Nyata Penyelamatan Mangrove di Sulawesi Selatan Karya Dr. Maskun yang diterbitkan Nasmedia et.al Pustaka di tahun 2018. Sewaktu

mahasiswa penulis aktif berorganisasi pada Lembaga Pers Mahasiswa Hukum-Universitas Hasanuddin (LPMH-UH). Saat ini aktif pada Environment Law Forum (ELF), lembaga kajian dan advokasi lingkungan hidup yang berdomisili di Kota Makassar. Penulis dapat dihubungi melalui e-mail: assidiqhasbi97@gmail. com



Siti Nurhalima Lubis, lahir di Gorontalo Mei 1998. Penulis merupakan mahasiswa Sarjana Program Universitas pada Fakultas Hukum. Hasanuddin. Penulis merupakan mahasiswa yang aktif pada organisasi Lembaga Pers Mahasiswa Hukum Universitas Hasanuddin (LPMH-UH). Saat ini penulis berdomisili di Makassar dan dapat dihubungi melalui email: halimalubis06@gmail.com

Armelia Safira, Penulis merupakan mahasiswa Program Sarjana pada Fakultas Hukum, Universitas Hasanuddin dengan konsentrasi Hukum Perdagangan Internasional. Penulis merupakan mahasiswa yang aktif pada organisasi Lembaga Pers Mahasiswa Hukum Universitas Hasanuddin (LPMH-UH), International Law Students Association (ILSA) Chapter Universitas Hasanuddin dan berapa komunitas di Kota Makassar. Penulis dapat dihubungi melalui e-mail: Syafiraarmee@gmail.com.

6 Alasan Memilih Nasmedia



Garansi 100%

Tidak puas dengan kualitas cetak Nasmedia? Kami menyediakan garansi 100% buku baru. Gratis!



Anggota IKAPI

Tidak mudah menjadi anggota Ikatan Penerbit Indonesia (IKAPI). Nasmedia telah tergabung sejak 2018



Harga Termurah

Nggak percaya layanan Nasmedia termurah di Timur Indonesia? Banding aja dengan penerbit sebelah



Perpusnas RI

Lebih dari 3 tahun Nasmedia telah terverifikasi dengan terbitan lebih dari 350 Judul buku ber-ISBN



Pelayanan Terbaik

Lebih dari 1300+ penulis dan 30+ mitra cetak Nasmedia adalah bukti dari pelayanan terbaik kami



Support 24/7

Admin Nasmedia Support 24 jam. So, konsultasi orderan anda diterima kapan saja. kami selalu untuk anda



Garansi 30 Hari Uang Kembali

Tidak puas dengan layanan Nasmedia? Kami menyediakan garansi uang kembali yang berlaku 30 hari sejak tanggal buku di terima

BOOK'S PUBLISHED

3 TAHUN NASMEDIA TELAH BERHASIL

MENERBITKAN BUKU

LEBIH DARI

1300+ PENULIS

DENGAN TOTAL PRODUKSI LEBIH DARI

93.000 EKSEMPLAR BUKU

