KEDUDUKAN HUKUM CYBER CRIME DALAM PERKEMBANGAN HUKUM INTERNASIONAL KONTEMPORER

Maskun; Alma Manuputty; S.M. Noor; Juajir Sumardi

Universitas Hasanuddin Makassar
Jl. Perintis Kemerdekaan Km. 10 Tamalanrea, Makassar 90245 Sulawesi Selatan
email : maskunlawschool@yahoo.co.id, maskunmaskun31@gmail.com

Abstract

Cybercrime is anewrange ofinternational law, particularlyinternationalcriminallaw. The existence ofcybercrimeis now afactthatshouldbe taken seriouslybythe international community.Immediateresponseformto do is to regulate the cybercrime internationallybecausethe fact shows that no one convention has foundcybercrime internationally. The existed Convention of CyberC?ime enacts only regionally like European Convention of Cyber Crimeand locally (like in Indonesia), the Law number 11/2008 concerning Information and Electronic Transaction.

Keywords : Cyber Crime, Current International Law

Abstrak

Cybercrime merupakan ragam baru dalam hukum internasional, khususnya hukum kejahatan internasional.Eksistensi cybercrime saat ini merupakan fakta yang harus ditanggapi secara serius oleh dunia internasional.Bentuk respon yang segera harus dilakukan adalah melahirkan produk perundang-undangan yang berlaku secara internasional karena hingga kini belum ditemukan konvensi tentang cybercrime yang berlaku secara internasional.Konvensi atau pengaturan cybercrime yang ada masih bersifat regional dan lokal negara-negara.

Kata Kunci: Cyber Crime, Hukum Internasional Kontemporer

A. Pendahuluan

Cybercrime merupakan salahsatu jenis kejahatan internasional kontemporer. Frasa kontemporer yang digunakan menunjukkan kekinian *cybercrime* sebagai salahsatu jenis kejahatan internasionalyang berkembang pesat, yang berawal di periode 1970-an dan terus berkembang hingga saat ini. Dalam perkembangannya, *cybercrime* mengalami perkembangan yang sangat pesat dengan modus yang beragam. Ragam dimaksud bukan hanya melibatkan pelaku dalam konteks individu, akan tetapi pelaku yang diduga melibatkan negara sebagai aktor intelektual.

Beberapa jenis *cybercrime* dengan ragam dan varian mutakhir dapat dilihat misalnya pada tahun 2005 ketika pemerintah Cina menggunakan *outsourcing* untuk melakukan pembajakan (*cyber-piracy*) terhadap Amerika Serikat.[1] Pada tahun 2007, Estonia mendapat serangan (*cyber-attack*) yang diduga dilakukan oleh Russia[2] 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-Servise (DDoS) attacks*.[3] Kejadian serupa juga terjadi pada tahun 2008 ketika terjadi perang antara Georgia dan Russia yang menempatkan Moscow sebagai sebuah strategi *multiple* untuk kampanye angkatan bersenjata Rusia, yang juga dilakukan melalui *Distributed Denial-of-Servise (DDoS)*.[4]

Peristiwa yang terjadi di Estonia dan Georgia

1 James P. Farwell and Rafal Rohonzinski, *Stuxnet and the Future of Cyber War*,**Survial**, Vol. 53, No. 1, (February-March 2011), hlm. 26.
2 Katherina C. Hinkle, *Countermeasures in the Cyber Context : One More Thing to Worry About*, **YJIL Online,** Vol. 17, No. 4, (Fall 2011), hlm. 13.
3 *Ibid.*
4 James P. Farwell and Rafal Rohonzinski, op.cit., p. 26. Lihat juga http://www.un.org/ apps/news/story.asp?NewsID=23977&Cr=general&Cr1=debate&Kw1=

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. Fatal yang dimaksudkan karena melanggar kedaulatan negara dan infrastruktur Estonia dan Georgia.[5]

Serangan siber (*cyber-attack)* juga menimpa Iran pada bulan Juni 2010. Serangan tersebut menyerang fasilitas nuklir Iran di Natanz. Kurang lebih 60.000 komputer terinfeksi oleh virus yang disebut dengan Stuxnet.[6] 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.[7] Penyataan perusahaan keamanan komputer RusiaKaspersky Lab menyimpulkan bahwa serangan canggih tersebut bisa dilakukan "dengan dukungan negara" dan diduga bahwa Israel dan Amerika Serikat mungkin telah terlibat.[8]

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 (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.[9] Contoh terkini terjadi pada Februari 2013, ketika Perusahaan keamanan internet Amerika Serikat, Mandiant, merilis sebuah laporan yang menunjukkan bahwa Cina telah melakukan peretasan terhadap perusahaan-perusahaan barat.[10]

Kompleksitas ragam dan varian modus *cybercrime*, dalam praktek sebagaimana disebutkan di atas, tidaklah diikuti dengan pengaturan atau instrumen hukum yang memadai, khususnya dalam konteks hukum internasional.[11] Hukum internasional secara faktual dapat dikatakan belum siap untuk menformulasikan instrumen hukum internasional yang menjadi payung hukum bagi negara-negara. Eksistensi beberapa ketentuan tentang *cybercrime* seperti *Cybercrime Convention* yang berlaku di Eropa masih bersifat regional dan undang-undang tentang *cybercrime* yang berlaku di masing-masing negara, yang tentunya bersifat domestik.[12] Oleh karena itu, kebutuhan akan kerangka hukum dalam konteks *cyber crime* merupakan suatu tantangan baru dalam dunia hukum itu sendiri. Ketersediaan dan keterbatasan aturan-aturan hukum yang ada selama ini, "*memaksa*" aparat penegak hukum dan pengambil kebijakan untuk melakukan penemuan hukum di bidang ini (*emerging norms/laws)* sehingga putusan-putusan yang berkaitan dengan masalah-masalah *cybercrime*[13] dapat memenuhi aspek

---

general+assembly&Kw2=&Kw3=, *Estonia Urges UN Member States to Cooperate Against Cyber Crimes*, Posting 27 Sepetember 2007, diakses 05 Oktober 2012.

5 Lihat Yoram Dinstein, *Computer Network Attacks and Self-Defense*, **76 Int'l L. STUD**, Vol. 99, No.2, (2002), hlm.102-103.

6 James P. Farwell and Rafal Rohonzinski, op.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.

7 Reuters, *2-Cyber Attack Appears to target Iran-tech Firms*, **http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE68N1OI20100924.**

8 Ibid.

9 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. 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.

10 Lihat Kompas, 21 Februari 2013, hlm.8.

11 Katherine C. Hinkle, *op.cit.*hlm. 12.

12 Maskun, 2013, *Cybercrime: Suatu Pengantar*, Jakarta, Prenada Kencana, hlm. 141-198.

13 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, 2005, *Kejahatan Mayaantara (Cyber Crime)*, Bandung, Refika Aditama, hlm. 125.

keadilan, kemanfaatan, dan kepastian hukum.

Memahami diskursus *cybercrime*sebagaimana diuraikan di atas maka dalam tulisan ini *cybercrime*akan difokuskan pada kedudukan hukumnya dalam perkembangan hukum internasional kontemporer.

B. Pembahasan

1. Arti dan Makna Cyber Crime

Sebelum menguraikan pergertian *cybercrime* secara terinci, terlebih dahulu dijelaskan bahwa "induk" *cybercrime* yaitu *cyberspace*. *Cyberspace* dipandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini *cyberspace* di anggap 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* (internet) 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.[14]

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 (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.[15]

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

Dalam beberapa kepustakaan, *cybercrime* 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*".[16] Pendapat lain dikemukan oleh *Organization for Economic Cooperation Development* (OECD) yang menggunakan istiah *computer related crime* yang berarti *any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data.*[17]

Cyber crime di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer akan tetapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya.[18] Hal ini dapat dilihat pada pandangan Indra Safitri yang mengemukakan bahwa *cyber crime* 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.[19]

Oleh karena itu, dapat dikatakan bahwa *cyber crime*dan kejahatan komputer adalah dua hal yang berbeda. Perbedaan tersebut dapat dilihat pada pandangan yang dikemukan oleh Nazura Abdul Manaf[20] yang membedakan *cyber crime*dan kejahatan komputer, sebagai berikut:

> *"Defined broadly, computer crime could reasonably include a wide variety of criminal offences, activities or issues. It also knows as a*

14 Kenny Wiston, 2002, *The Internet: Issues of Jurisdiction and Controversies Surrounding Domain Names*, Bandung, Citra Aditya, hlm. vii.
15 Widyopramono Hadi Widjojo, *Cybercrimes dan Pencegahannya*, **Jurnal Hukum Teknologi**, Fakultas Hukum Universitas Indonesia, Vol 2 (Agustus 2005), hlm. 7.
16 www.usdoj.gov/criminal/cybercrimes.
17 Lihat Obsatar Sinaga, *Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia*, Makalah, IPB Bogor, 5 Desember 2010., hlm. 10.
18 Ari Juliano Gema, 2000, *Cybercrime: Sebuah Fenomena di Dunia Maya*, diakses pada www.theceli.com.
19 Indra Safitri, *Tindak Pidana di Dunia Siber*, Insider, Legal Journal From Indonesian Capital and Investment Market, 1999, diakses http://business.fortunecity.com.

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 to 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, cybercrimes 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 cybercrimes or vice versa, since they have same impact in law".

Perbedaan mendasar *cyber crime*dan kejahatan komputer sebagaimana yang dikemukan oleh Nazura Abdul Manaf adalah adanya unsur komputer yang terkoneksi melalui perangkat telekomunikasi dalam bentuk *internet online* yang menjadi media bagi seseorang atau kelompok untuk melakukan pelanggaran dan atau *cybercrime*.Sedangkan kejahatan komputer dilakukan oleh seseorang dengan menjadikan komputer sebagai media untuk melakukan kejahatan tanpa penglibatan jaringan internet.

2. Kedudukan Hukum *CyberCrime* Dalam Perkembangan Hukum Internasional Kontemporer

Hukum internasional adalah bidang hukum yang merupakan integrasi antara sistem hukum yang berbeda dari berbagai negara.Integrasi dimaksud menunjukkan suatu perspektif bahwa hukum internasional secara esensial merupakan kerjasama antara negara.[21] 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 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. Interaksi ini dipengaruhi oleh perkembangan informasi dan teknologi yang menciptakan varian baru sebagai konsekuensi dari sifat internasional yang melekat pada bentuk dan modus varian-varian tersebut.

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

Secara teori, M. Cherif Bassiouni[22] membagi tingkatan kejahatan internasional menjadi tiga. **Pertama**, kejahatan internasional yang disebut sebagai *international crimes* adalah bagian dari *jus cogens*.[23] 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.*

---

20 Agus Raharjo, 2002, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung, Citra Aditya, hlm. 227

21 Magdalena Petronella Ferreira-Synman, 2009,*The Erosion of State Sovereignty in Public International Law : Towards a World Law?*, Afrika Selatan, University of Johannesburg, hlm. 1.

22 Eddy O.S. Hiariej, 2009, *Pengantar Hukum Pidana Internasional*, Jakarta, Airlangga, hlm. 56.

23 *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*,hal. 50.

h. *Apartheid.*
i. *Slavery and slave-related 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 drug offenses.*
k. *Organized crime*
l. *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 obsence materials.*
b. *Falsification and counterfeiting.*
c. *Unlawful interference with submarine cable.*
d. *Bribery of foreign public official.*

Uraian kualifikasi kejahatan internasional sebagaimana diuraikan oleh Bassiouni, semakin memperjelas posisi *cyber crime* yang secara implisit belum dikategorikan sebagai salahsatu jenis kejahatan internasional. Oleh karena itu, dalam rangka pengkualifikasian *cyber crime* sebagai varian baru kejahatan internasional maka pengkualifikasiaan dimaksud harus didasarkan pada penguraian unsur-unsur kejahatan internasional. Menurut Bassiouni terdapat 3 (tiga) unsur yang harus dipenuhi agar dapat dikatakan sebagai kejahatan internasional. Unsur tersebut adalah:[24]

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.
c. 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 *cyber crime*secara implisit dapat memenuhi keseluruhan unsur untuk dikatakan sebagai kejahatan baru dalam literatur kejahatan internasional dewasa ini. 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, *cyber crime* berpotensi untuk memberikan ancaman terhadap perdamaian dunia. Kasus *stuxnet* (2010) dan *flame* (2012) sebagaimana telah disebutkan pada bagian sebelumnya sangat berbahaya karena kontrol terhadap aktifitas nuklir dapat dilakukan oleh seseorang dan atau negara dengan secara mudah. Menurut Ralph Lagner[25] bahwa *stuxnet* digambarkan sebagai senjata siber yang digunakan untuk menyerang seluruh program nuklir Iran.[26] Penggunaan senjata siber seperti ini akan sangat mudah

24 Romli Atmasasmita,2003,*Pengantar Hukum Pidana Internasional*, Bandung, Refika Aditama,hlm. 58.
25 Ralph Lagner adalah seorang ahli dibidang telematika yang berkebangsaan Jerman.
26 James P. Farwell and Rafal Rohonzinski, op.cit.hlm. 23.

digunakan saat ini dengan pertimbangan perkembangan massif informasi dan teknologi yang tak dapat dielakkan lagi.

b) Unsur transnasional, artinya cakupan atau lingkup *cyber crime* yang lintas antar negara. Menurut Hata bahwa *cyber crime* yang terjadi menunjukkan kedaulatan tradisional negara sangat mudah untuk ditembus, yang sekaligus melemahkan fungsi-fungsi kekuasaan tradisional suatu negara.[27] Pendapat Hata ini kemudian dengan sangat mudah untuk dibuktikan dengan melihat beberapa kasus mulai dari kasus pencurian kartu kredit, judi online, akses illegal, spionase, hingga *cyber terorism* yang mulai dikembangkan dalam beberapa tahun terakhir.

c) Unsur kebutuhan, artinya dibutuhkan kerjasama secara internasional antar negara-negara untuk menghadapi dan mengadili pelaku cyber crime 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.[28]

Terpenuhinya uraian elemen kejahatan internasional sebagaimana dikemukan oleh Bassiouni menempatkan *cybercrime*sebagai kejahatan internasional mutakhir yang memiliki kedudukan hukum tersendiri.Internet sebagai media (*tools of crime*) telah memfasilitasi hukum internasional baik privat maupun publik untuk digejewantahkan dalam bentuk produk hukum internasional. Lahirnya produk hukum internasional yang mengatur secara khusus *cybercrime*akan memperkaya khasanah literatur dan praktik hukum internasional itu sendiri. Apalagi fakta terkini menunjukkan bahwa belum adanya instrumen hukum internasional yang berlaku secara universal untuk mengatur dan mengadili *cybercrime* yang terjadi.

Kebutuhan akan pengaturan hukum internasional merupakan suatu keharusan mengingat ragam *cybercrime* yang terus berevolusi untuk melahirkan varian baru. Pengaturan ini pun dapat dianggap sebagai bagian dari sistem keamanan siber untuk melindungi setiap individu baik pengguna aktif maupun pasif.[29]

Secara faktual hingga saat ini belum dirumuskan suatu perjanjian internasional yang khusus mengatur tentang kejahatan siber.Dalam konteks ini, secara kelembagaan PBB memberikan mandat pada organ-organ khusus PBB untuk merumuskan aturan-aturan yang dapat dipandang sebagai upaya untuk menangani permasalahan*cybercrime*.Organ-organ PBB dimaksud adalah:

a. *United Nations Office on Drug and Crime* (UNODC)

UNODC merupakan badan atau organ PBB yang dibentuk untuk memerangi peredaran obat-obat terlarang dan kejahatan internasional lainnya, termasuk didalamnya beberapa jenis *emerges crimes* seperti pembajakan (*piracy*), penyeludupan benda-benda budaya yang bermakna kekayaan intelektual (*trafficking in cultural property*), kejahatan lingkungan (*environmental crime*), dan *cybercrime*. UNODC berkantor pusat di Vienna-Austria.[30]

Dalam konteks *cybercrime*, merujuk pada Konferensi ke-5 *the United Nations Convention on Transnational Organized Crime* pada tahun 2010, telah diidentifikasi bahwa *kejahatan siber* salahsatu jenis kejahatan yang dapat dikategorikan sebagai kejahatan transnasional yang terorganisir, disamping kejahatan penyeludupan benda-benda budaya yang bermakna kekayaan intelektual (*trafficking in cultural property*), dan kejahatan lingkungan (*environmental crime*).

Para pihak peserta Konferensi memandang bahwa kejahatan-kejahatan tersebut telah berkembang sangat pesat dan membutuhkan *legal response* dalam penegekan hukum. Gambaran kondisi tersebut, oleh para pihak peserta Konferensi dianggap sebagai *emerges crimes* yang membutuhkan *emerges norms*.*Cybercrime*menurut UNODC lebih lanjut digambarkan sebagai suatu jenis kejahatan dengan tingkat kerumitan tersendiri dimana sifat kejahatan yang lintas batas dengan

27 Hata, 2012, *Hukum Internasional : Sejarah dan Perkembangan hingga Pasca Perang Dingin*, Malang, Setara Press, hlm. 110.
28 Ibid.
29 Maskun, *Cyber Security: Rule of Use Internet Safely?*,**Journal of Law, Policy and Globalization**, Vol. 15, No. 1 (Juli 2013), hlm. 20-21.
30 Lihat http://www.unodc.org/unodc/organized-crime/emerging-crimes.html, *Emerging* Crimes, diposting 25 Februari 2013 , diunduh 8 Nopember 2013.

media *cyberspace*. Pelaku kejahatanpun semakin bervariasi mulai dari individu, organisasi, dan negara.[31] Adapun korbannya dapat saja berlokasi di beberap tempat untuk suatu periode kejahatan.Oleh karena sifat yang melekat padanya baik dalam konteks pelaku maupun korban maka dibutuhkan respon secara internasional sebagai bentuk solusi atas kondisi saat ini dimana penanganan atas kejahatan siber menjadi sesuatu yang urgen dan dinamis untuk dilakukan, salahsatunya oleh UNODC.

Respon konkrit yang dilakukan oleh UNODC secara kelembagaan yaitu mempromosikan suatu kerja jangka panjang dan pengembangan kemampuan SDM secara berkelanjutan dalam rangka memerangi *cybercrime*melalui dukungan struktur dan tindakan pada level nasional (domestik). Dalam konteks ini, UNODC menyediakan pakar dibidang *criminal justice systems* untuk menyediakan dan menyiapkan bantuan teknis dalam pelaksanaan pengembangan SDM dimaksud, kerjasama internasional, pengumpulan data, penelitian dan analisis mengenai *cybercrime*.

Bentuk konkrit sebagaimana disebutkan di atas oleh UNODC dilaksanakanlah *open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime*, di Vienna pada tanggal 17 hingga 21 Januari 2011. Pertemuan ini mengundang *the Commission on Crime Prevention and Criminal Justice*untuk memberikan respon atas permasalahan *cybercrime*secara komprehensif. Rekomendasi ini kemudian diadopsi oleh *the Commission on Crime Prevention and Criminal Justice* dalam resolusi 2010/18 dan oleh ECOSOC dalam *the General Assembly resolution 65/230*.

Tindak lanjut pertemuan 2011, UNODC kembali *open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime* di Vienna pada tanggal 25 hingga 28 Februari 2013.[323] Pertemuan ini merupakan tindak lanjut dari pertemuan sebelumnya (2011), termasuk didalamnya melakukan evaluasi atas resolusi yang telah dihasilkan sebelumnya.Salahsatu rekomedasi yang dihasilkan berupa *Comprehensive Study on Cyber Crime* 2013 yang dibuat oleh *the Commission on Crime Prevention and Criminal Justice*.

Kedua pertemuan sebagaimana telah disebutkan di atas merupakan langkah konkrit yang dilakukan oleh UNODC sebagai salahsatu agen khusus PBB yang diberi mandat oleh PBB untuk menangani persoalan *cybercrime*. Tentunya ini masih awal, akan tetapi ini adalah sebuah langkah progresif yang dilakukan PBB untuk merespon kondisi saat ini dimana *cybercrime*adalah suatu jenis kejahatan yang dikategorikan sebagai *a new threat of humankind*.

b. International Telecommunication Union (ITU)

ITU adalah agen khusus PBB yang memainkan peranan yang sangat penting dalam menetapkan standardisasi, pengembangan telekomunikasi dan isu-isu keamanan siber.[33] Diantara sekian banyak kegiatan-kegiatan ITU, ITU adalah agen utama dalam *theOrganization of the World Summit on the* Information *Society (*WSIS*)* yang telah melakukan pertemuan di Jenewa (2003) dan di Tunisia (2005). Kedua pertemuan tersebut dihadiri oleh perwakilan negara-negara, para pengambil kebijakan, dan para ahli di seluruh dunia yang berbicara tentang isu-isu terkini yang berhubungan dengan pengembangan informasi global termasuk didalamnya standardisasi kebijakan dan hukum.Hasil yang diperoleh dari kedua pertemuan tersebut, khususnya *the Tunis Agenda* adalah kebutuhan diperlukannya kerjasama internasional dalam penanganan *cybercrime* dan pendekatan legislatif seperti resolusi Majelis Umum PBB dan *European Cybercrime Convention*.

Bentuk konkrit kegiatan yang dilakukan ITU adalah menyelenggarakan *the sole fasilitator for action line C5 on building confidence and security in the use of information and communication technology*, pada tahun 2007.Pada pertemuan tersebut diluncurkan sebuah agenda baru yang disebut dengan ITU *Global Cybersecurity Agenda* (GCA).[34] GCA memiliki 7 (tujuh) tujuan yang dikembangkan dari 5 (lima) pillar termasuk didalamnya strategis elaborasi untuk

31 Ibid.
32 Lihat http://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html. Diposting 22 Februari 2013, diunduh 8 Nopember 2013.
33 Lihat ITU, 2009, *Understanding Cybercrime: A Guide for Developing Countries*, Jenewa, ITU Development, hlm. 93.
34 Lihat www.itu.int/osg/csd/cybersecurity/gca/pillar-goals/index.html, *Global Cybersecurity Agenda*, Diposting Januri 2007, diunduh 8 Nopember 2013.

pengembangan model legislasi *cybercrime*.

Dalam rangka mewujudkan tujuan yang telah ditetapkan, Sekretaris Jenderal ITU telah membentuk *high-level expert group* (HLEG). Pada tahun 2008, HLEG telah mempublikasikan suatu laporan tentang stategis global dalam memberantas *cybercrime* dan pada tahun 2009, WSIS ITU telah mempublikasi suatu *Understanding Cybercrime: a Guide of Developing Countries*.Upaya yang dilakukan ITU sebagaimana telah disebutkan, juga merupakan upaya terstruktur dan tersistematis untuk memerangi dan memberantas *cybercrime* yang mulai terasa sangat meresahkan masyarakat dunia.

C. Simpulan

Cybercrime merupakan suatu fakta dan fenomena baru dalam koridor hukum internasional.Respon hukum internasional menempatkan *cybercrime*sebagai suatu jenis baru kejahatan internasional yang hingga kini belum diatur secara internasional. Kebutuhan akan instrumen hukum internasional sangat medesak untuk diwujudkan, mengingat bahwa ragam *cybercrime* yang sangat bervariasi yang harus diatur dengan produk hukum internasional yang bersifat universal. Dengan sifat pengaturan yang universal dan memberikan *cybercrime* suatu kedudukan hukum dalam hukum internasional(kontemporer).

DAFTAR PUSTAKA

Atmasasmita, Romli,2003,*Pengantar Hukum Pidana Internasional*, Bandung: Refika Aditama.

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

Ferreira-Synman,Magdalena Petronella, 2009, *The Erosion of State Sovereignty in Public Internaional Law: Towards a World Law?*, Afrika Selatan:University of Johannesburg.

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

Hata, 2012, *Hukum Internasional : Sejarah dan Perkembangan hingga Pasca Perang Dingin,* Malang: Setara Press.

ITU, 2009, *Understanding Cybercrime: A Guide for Developing Countries*, Jenewa: ITU Development.

Maskun, 2013, *Cybercrime: Suatu Pengantar*, Jakarta: Prenada Kencana.

Maskun, *Cyber Security: Rule of Use Internet Safely?*,**Journal of Law, Policy and Globalization**, Vol. 15. No. 1 (Juli 2013).

Nurhidayat, Dedy,*Eksaminasi Terhadap Perkara Pidana Terkait Pembobolan Situs Komisi Pemilihan Umum*, **Jurnal Hukum Teknologi**, Vol 2. Nomor 1 (Agustus 2006).

O.S. Hiariej, Eddy, 2009, *Pengantar Hukum Pidana Internasional,* Jakarta: Airlangga.

P. Fiddler,David,***Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law*, ASIL, Vol.16. Issue 22 (20 June 2012).**

P. Farwell, James, and Rohonzinski, Rafael,*Stuxnet and the Future of Cyber War*, **Survial**, Vol. 53 (February-March 2011).

Raharjo, Agus, 2002, *Cyber Crime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya.

Sinaga, Obsatar, *Penanggulangan Kejahatan Internasional Cyber Crime di Indonesia*, Makalah, IPB Bogor, 5 Desember 2010.

Wahid, Abdul, dan Mohammad Labib, 2005, *Kejahatan Mayaantara (Cyber Crime)*, Bandung: Refika Aditama.

Wiston, Kenny,2002, *The Internet: Issues of Jurisdiction and Controversies Surrounding Domain Names*, Bandung: Citra Aditya.

http://www.unodc.org/unodc/organized-crime/emerging-crimes.html, *Emerging* Crimes, diposting 25 Februari 2013 , diunduh 8 Nopember 2013.

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, diakses 05 Oktober 2012.

http://www.itu.int/osg/csd/cybersecurity/gca/pillar-goals/index.html, *Global Cybersecurity Agenda*, Diposting Januri 2007, diunduh 8 Nopember 2013.

http://www.unodc.org/unodc/en/organized-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html. Diposting 22 Februari 2013, diunduh 8 Nopember 2013.

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

Erdbrink, Thomas, *Iran Confirms Attack by Virus That Collects Information*, **N.Y. Times**, May 29, 2012.

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

Reuters, *2-Cyber Attack Appears to target Iran-tech Firms,* **http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE68N1OI20100924.**

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

Zeiter, Kim, *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.