Perlu Waspada Terhadap Serangan Cyber

Nurcahaya Tandang

Berbagai upaya yang dilakukan untuk melawan *cyber crime*. Namun *cyber crime* tetap melaju memasukkan dunia internasional dalam perang *cyber*. Bahkan cyber kini dimasukkan dalam alutsista (alat utama sistem persenjataan) dan masuk matra perang kelima setelah Angkatan Darat, Laut, Udara Dan Angkasa Luar. *Cyber* dimasukkan pula sebagai pertahanan militer dan nir-militer tergantung tujuan kejahatannya terkait dengan instalasi militer atau tidak, sasarannya mengganggu stabilitas nasional, keamanan negara dan kedaulatan negara atau tidak? Sebelum kita mengulas apa dan mengapa terjadi perang *cyber* terlebih dahulu kita perlu memahami beberapa hal berikut:

Apakah *Cyber Crime* itu?

Dalam beberapa literatur, *cyber crime* sering diidentikkan dengan *computer crime*. The U.S. Department of Justice memberikan pengertian *computer crime* sebagai:"*...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution*". Pengertian lainnya diberikan oleh *Organization of European Community Development*, yaitu:"*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Andi Hamzah dalam bukunya Aspek-aspek Pidana di Bidang Komputer (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari pengertian di atas, *computer crime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memper-

oleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih (Wisnubroto, 1999).

Internet sebagai hasil rekayasa teknologi bukan hanya menggunakan kecanggihan teknologi komputer tapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya. Apalagi pada saat internet sudah memasuki generasi kedua, perangkat komputer konvensional akan tergantikan oleh peralatan lain yang juga memiliki kemampuan mengakses internet. Untuk itu, ada upaya untuk memperluas pengertian computer agar dapat melingkupi segala kejahatan di internet dengan peralatan apapun, seperti pengertian computer dalam *The Proposed West Virginia Computer Crimes Act*, yaitu: "*an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or type-setter, a portable hand-held calculator, or other similar device*" (http://www.cybercrimes.net/). Namun begitu, tetap saja pada prakteknya pemahaman publik akan pengertian computer adalah perangkat komputer konvensional (PC, Notebook, Laptop) yang biasa terlihat.

Berdasarkan beberapa literatur serta prakteknya, *cyber crime* memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (*cyber space*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya;
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan jaringan telekomunikasi dan/atau internet;
3. Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional;
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya; dan
5. Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

Beberapa Bentuk *Cyber Crime*

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi

ini dalam beberapa literatur dan praktek-nya dikelompokkan dalam beberapa bentuk, antara lain:

1. ***Unauthorized Access to Computer System and Service***

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

   Kita tentu tidak lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, hacker juga telah berhasil menembus masuk ke dalam database berisi data para pengguna jasa *America Online* (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang *e-commerce*, yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal *Bureau of Investigation (FBI)* juga tidak luput dari serangan para hacker, yang mengakibatkan tidak berfungsinya situs ini dalam beberapa waktu lamanya (http://www.fbi.org).

2. ***Illegal Contents***

   Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.

3. ***Data Forgery***

   Merupakan 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.

4. *Cyber Espionage*

Merupakan 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 yang *computerized*.

5. *Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, 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 tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

6. *Offense Against Intellectual Property*

Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. *Infringements of Privacy*

Kejahatan ini 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 computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya. (http://www.cybercrimes.net/)

Cyber Matra Perang Kelima

Jagat *cyber* kini bahkan telah didudukkan pula sebagai matra perang kelima--setelah Darat, Laut, Udara, Dan Angkasa Luar. Inovasi di bidang teknologi telah mengubah taktik dalam konflik di zaman modern dan membuat dunia

maya menjadi medan perang terbaru.

Banyak perangkat mutakhir telah dibuat untuk keperluan ini. Dibantu oleh kemajuan teknologi elektromagnetik serta teknologi komunikasi dan informasi, sebuah bentuk pertempuran elektronik telah tercipta dan membuat pemerintahan berbagai negara melihat perang dunia maya sebagai ancaman terbesar di masa depan.

Alon Ben David, analis militer dari Channel 10 Israel menyebutkan: "Jika Anda punya beberapa orang pintar dan sebuah komputer yang bagus, Anda bisa melakukan banyak hal. Anda tidak perlu pesawat udara, tank, pasukan tentara. Anda bisa memasuki negara lain, menciptakan kerusakan besar tanpa perlu meninggalkan kursi empuk Anda,"ucapnya.

Dalam sebuah laporan eksklusif di harian Le Monde Perancis, jurnalis Nicky Hager berhasil menguak keberadaan instalasi Urim milik Unit 8200, yang merupakan salah satu instalasi pengintaian terbesar di dunia, setara dengan instalasi milik Amerika Serikat di Menwith Hill, Yorkshire, Inggris.

Instalasi yang dibangun sejak satu dekade yang lalu itu awalnya hanya bertugas memonitor percakapan internasional di jaringan satelit Intelsat dan stasiun relay telepon antar negara besar. Tapi kini ia juga bertugas mengawasi percakapan via satelit Inmarsat, juga menyadap kabel-kabel bawah laut. Menurut sumber orang dalam, komputer-komputer di instalasi Negev diprogram untuk dapat memilah-milah kata serta berbagai pesan di percakapan telepon, email, dan data yang diintersepnya. Pesan-pesan yang berhasil disadap itu langsung dikirim ke markas besar Unit 8200 di Camp Glilot di kota Herzliya, sebelah utara Tel Aviv.

Di tempat itulah pesan-pesan dari berbagai bahasa itu diterjemahkan dan diteruskan ke agen-agen Mossad di negara lain maupun berbagai badan lain yang berkepentingan. Yang harus dicatat dari Unit 8200 adalah kekuatan pasukan elite *cyber*nya. Upaya dan obsesi Israel untuk memiliki kekuatan *cyber* yang handal, telah dimulai sejak 1990-an. Saat itu para peretas (*hacker*) Israel cuma disodori dua pilihan: masuk bui atau bergabung dengan *The Unit*.

Kini, hasilnya tak main-main. Sebuah konsultan di AS memperhitungkan The Unit sebagai salah satu ancaman *cyber* terbesar dunia, di samping China, Rusia, Iran, dan Perancis. Stuxnet adalah salah satu bukti konkritnya.

Angkatan Perang *Cyber*

Kekuatan sebuah angkatan perang *cyber* ditentukan oleh kemampuan serangan, pertahanan, serta ketergantungan suatu negara terhadap Internet. Dalam buku

"Cyber War", pakar keamanan komputer asal AS dan profesor di Universitas Harvard Richard A. Clarke dan Robert A. Knake memetakan kekuatan negara-negara dalam menghadapi perang *cyber*.

Amerika Serikat, meski punya kemampuan serangan yang baik, tidak punya kemampuan untuk memutuskan jaringan Internet saat diserang, mengingat sebagian terbesar jaringan Internet di negara ini dimiliki dan dioperasikan oleh swasta. Sebaliknya, China memiliki kemampuan memutus seluruh jaringan Internet di negaranya bila suatu saat diserang. China juga mampu membatasi utilisasi trafik, dengan memutus koneksi dari para pengguna yang tak terlalu berkepentingan.

Namun negara yang dinilai paling mampu bertahan jika terjadi perang dunia maya, menurut Clarke, adalah Korea Utara. Negara ini mampu memutus koneksi internetnya dengan lebih mudah ketimbang China. Bisa dibilang Korea Utara tak akan mengalami kerugian akibat serangan *cyber* musuh, karena tak ada infrastruktur kritikal seperti pembangkit listrik, jalur kereta, atau jalur pipa yang tersambung ke Internet.

Perang Melawan *Cyber Crime*

Saat ini berbagai upaya telah dipersiapkan untuk memerangi *cyber crime*. *The Organization for Economic Co-operation and Development (OECD)* telah membuat *guidelines* bagi para pembuat kebijakan yang berhubungan dengan *computer-related crime*, di mana pada tahun 1986 OECD telah mempublikasikan laporannya yang berjudul *Computer-Related Crime: Analysis of Legal Policy*. Laporan ini berisi hasil survey terhadap peraturan perundang-undangan negara-negara Anggota beserta rekomendasi perubahannya dalam menanggulangi *computer-related crime* tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting dalam kejahatan tersebut.

Melengkapi laporan OECD, *The Council of Europe (CE)* berinisiatif melakukan studi mengenai kejahatan tersebut. Studi ini memberikan *guidelines* lanjutan bagi para pengambil kebijakan untuk menentukan tindakan-tindakan apa yang seharusnya dilarang berdasarkan hukum pidana negara-negara anggota, dengan tetap memperhatikan keseimbangan antara hak-hak sipil warga negara dan kebutuhan untuk melakukan proteksi terhadap *computer-related crime* tersebut. Pada perkembangannya, CE membentuk *Committee of Experts on Crime in Cyberspace of the Committee on Crime Problems*, yang pada tanggal 25 April 2000 telah mempublikasikan *Draft Convention on Cyber-Crime* sebagai hasil kerjanya (http://www.cybercrimes.net), yang menurut Prof. Susan Brenner (brenner@cybercrimes.net) dari *University of Daytona School of Law*, merupakan perjanjian internasional per-

tama yang mengatur hukum pidana dan aspek proseduralnya untuk berbagai tipe tindak pidana yang berkaitan erat dengan penggunaan komputer, jaringan atau data, serta berbagai penyalahgunaan sejenis.

Sebuah survei dari McAfee mengungkapkan, serangan berbasis internet pada sistem-sistem penting seperti gas, energi, dan air meningkat di seluruh dunia. Survei itu dilakukan atas 200 petinggi IT yang bekerja di berbagai perusahaan di 14 negara.

Delapan dari sepuluh eksekutif itu menyatakan, jaringan mereka pernah menjadi sasaran *hackers* tahun lalu. Mereka juga melihat China sebagai sumber serangan utama, diikuti Rusia dan Amerika Serikat.

Dunia maya atau dunia *cyber* bukanlah tempat yang sepenuhnya aman. Kita mengenal berbagai gangguan yang mengancam aktivitas dunia maya, mulai dari *virus*, *malware*, *worm*, hingga trojan.

Beberapa dari gangguan itu hanya berskala kecil dan menyasar pengguna personal. Tapi, ada pula yang menyasar perusahaan, mencuri data besar-besaran, bahkan menjurus ke tindak kriminal. Lebih canggih lagi, serangan *cyber* itu bermotif politis.

Lebih seram lagi apa yang dikatakan Richard Clarke, mantan penasihat pertahanan Presiden Amerika Serikat. Ia bilang, serangan *cyber* dapat mengakibatkan bencana kolapsnya infrastruktur pokok suatu negara alias *critical national infrastructure* (CNI). Ia mengisahkan skenario ketika AS lumpuh saat virus dan senjata *cyber* bisa menyebabkan pesawat terbang jatuh dan meledakkan bom nuklir.

Skenario kiamat akibat aksi di dunia maya (*cybergeddon*) saat ini bak cerita di film-film *science fiction*. Tapi sebenarnya tak mustahil jika melihat begitu bergantungnya sistem perbankan, listrik, dan air pada jaringan komputer.*Cyber crime* dapat menyebabkan lumpuhnya semua kehidupan yang berhubungan dengan digital.Orang yang sedang melahirkan, orang yang sedang dioperasi, data-data yang belum terinput, system persenjataan nuklir, meledaknya berbagai jaringan, lift, pemanas, pendingin tiba-tiba stop, kereta bawah tanah tiba-tiba berhenti dll peristiwa yang mengerikan dapat terjadi hanya karena *cyber attack (*serangan *cyber)*.

Kini setidaknya ada tiga macam serangan *cyber* di dunia maya yaitu kejahatan *cyber* (*cyber crime*), spionase *cyber* (*cyber espionage*), dan perang *cyber* (*cyber warfare*). Para ahli *internet security* menggolongkan *cyber crime* sebagai kejahatan yang banyak terjadi, namun efeknya kecil. Mereka menyarankan cara mengatasinya adalah dengan penegakan hukum di dunia maya.

Sementara itu, dua kategori yang lain merupakan area sensitif dan masih sangat abu-

abu. Sampai sekarang belum kesepakatan soal aturan bahkan definisi umum terkait spionase dan perang di dunia *cyber*.

Ditambah lagi, sulit untuk melacak dari mana serangan itu berasal? Jaringan internet yang saling berhubungan memunculkan celah bagi para *hacker* untuk memalsukan lokasi mereka. Dengan teknik menyembunyikan nama, mereka bisa menjadi siapa saja dan di mana saja.

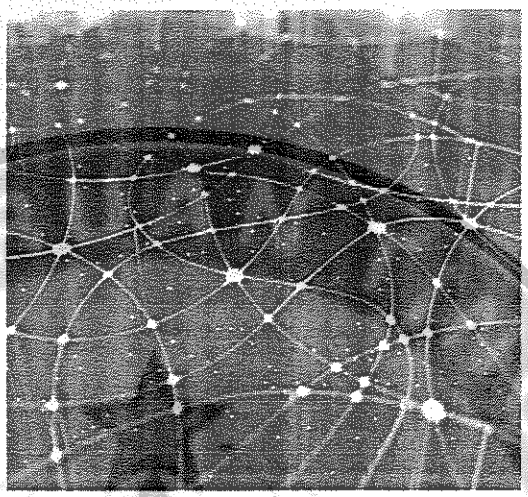
Kerentanan di dunia maya ini membuat banyak negara, khususnya negara maju, berlomba-lomba menguatkan pertahanan di dunia maya. Tak hanya itu, negara-negara kini mengembangkan juga senjata *cyber* rahasia. AS merupakan salah satu pemimpin dalam produksi senjata *cyber* ini.

Namun, negara-negara lainnya pun tak ketinggalan, misalnya Rusia, China, Israel, Prancis, dan Inggris. Sekarang pertanyaannya, akankah perang *cyber* menjadi perang di abad ke-21?

Beberapa contoh Perang ***Cyber (Cyber War)*** atau serangan *Cyber (Cyber Attack)* dapat diikuti di bawah ini:

1. ***Worm Stuxnet*** (2010)

Serangan *worm Stuxnet* banyak dipandang oleh para pakar sebagai salah satu serangan terbesar yang melibatkan kode program yang sangat kompleks.



Serangan worm ini memanfaatkan berbagai macam celah yang ada di sistem operasi Windows yang belum banyak diketahui, dan mengincar sistem industri yang mengendalikan berbagai perangkat mesin di instalasi pembangkit listrik maupun di pabrik-pabrik.

Tak salah bila banyak yang curiga bahwa worm ini didalangi oleh pihak yang besar, bahkan disponsori oleh negara besar, dalam hal ini adalah negara Barat. Iran menjadi negara yang paling banyak tertular oleh worm ini, dan banyak yang curiga, pihak Barat sengaja ingin melumpuhkan pembangkit nuklir Bushehr dengan worm ini.

2. Operasi Aurora (2009)

Pada 2009, sekitar 30 perusahaan besar termasuk Google dan Adobe Systems, dikabarkan menjadi korban serangan *cyber* yang sangat rumit. Para *hacker* berhasil

mencuri properti intelektual dari perusahaan-perusahaan tadi dengan memanfaatkan celah keamanan pada *browser Internet Explorer.*

Vice President of Threat Research McAfee, Dmitri Alperovitch mengatakan bahwa ia menemukan kata 'Aurora' pada direktori file di komputer penyerang, saat melakukan pelacakan dari komputer yang telah terinfeksi. Dipercaya, *hacker* menamakan Aurora sebagai nama operasi ini.

Tak cuma orang-orang yang bekerja pada perusahaan multinasional yang harus berhati-hati dengan upaya intrusi ini, namun beberapa tokoh oposisi China juga diincar. Dari dokumen yang dibocorkan oleh Wikileaks, serangan ini diinstruksikan oleh seorang petinggi di pemerintahan China.

3. Sentral Komando Amerika Serikat (2008)

Pencurian data informasi pribadi di komputer/notebook pada 2008 Departemen Pertahanan Amerika, mendapat serangan. Sumbernya: sebuah USB flash drive yang tidak berwenang yang diselipkan ke salah satu laptop di sebuah markas militer Amerika Serikat di Timur Tengah.

Flash disk tersebut mengandung kode berbahaya yang dikembangkan oleh intelijen asing dan menyebar melalui sistem komputer Departemen Pertahanan AS dan menyebabkan data dikirim ke server asing.

Serangan militer lainnya yang dilakukan melalui media portabel adalah peristiwa penyalinan 250 ribu data memo diplomatik AS dan video serangan heli Apache pasukan AS terhadap sekelompok sipil oleh Prajurit Satu Bradley Manning ke dalam CD Lady Gaga dari salah satu markas militer AS di Irak.

4. Rusia vs Georgia (2008)

Pada 2008 Rusia dan Georgia terlibat konflik di Ossetia Selatan. Serangan *cyber* melumpuhkan beberapa situs pemerintah Georgia dan situs-situs media lokal, setelah Georgia menyerang Ossetia Selatan. Ini merupakan serangan yang mirip dengan serangan ke Estonia pada 2007.

Serangan terhadap Georgia juga dilakukan menggunakan metoda *Distributed Denial of Service*. Siapapun dalang serangan ini sepertinya telah mengembangkan botnet, di mana masyarakat bisa mengunduhnya untuk membantu serangan terhadap situs-situs Georgia.

5. Estonia (2007)

Estonia menghadapi gelombang serang-

an *cyber* yang melanda segenap infrastruktur internet negara itu, mulai dari situs-situs pemerintahan, perbankan, hingga situs-situs surat kabar lokalnya.

Serangan ini terjadi bersamaan dengan perseteruan antara Estonia dan Rusia terkait dengan rencana pemindahan makam Tallinn oleh pemerintahan Estonia. Para analis media menyebut konflik ini sebagai perang *cyber* pertama. Namun, pihak Rusia sendiri membantah bahwa serangan-serangan terhadap Estonia dilancarkan oleh pemerintah Rusia.

Kelima perang *cyber* di atas merupakan perang *cyber* terbesar dalam sejarah.

Ancaman Militer dan Nir-Militer

Apakah ancaman *cyber* masuk dalam kelompok ancaman Militer atau Nir Militer? dan Kapan *Cyber Security* masuk dalam ranah Pertahanan Negara?

Cyber Security menjadi aktivitas Pertahanan Negara, apabila eskalasi Ancaman *Cyber* telah beresiko/berdampak pada : Kedaulatan Negara, Keutuhan Wilayah NKRI dan Keselamatan bangsa. (Keamanan *Cyber* dalam Pertahanan Negara Laksma (Pur) Iwan Kustiyawan Universitas Pertahanan Indonesia)

Kesimpulan

Dari berbagai upaya yang dilakukan tersebut, telah jelas bahwa *cyber crime* membutuhkan *global action* dalam penanggulangannya mengingat kejahatan tersebut seringkali bersifat transnasional. Beberapa langkah penting yang harus dilakukan setiap negara dalam rangka kewaspadaan penanggulangan *cyber crime* adalah:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut;

2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional

3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber crime*;

4. Meningkatkan kesadaran warga negara mengenai masalah *cyber crime* serta pentingnya mencegah kejahatan tersebut terjadi;

5. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber crime*, antara lain melalui perjanjian

ekstradisi dan *mutual assistance treaties* (*Cyber Crime* Sebuah Fenomena di Dunia Maya,Internet,26 September 2000); dan

6. Strategi Pertahanan Negara :
   a. Menghadapi Ancaman Nir Militer, identik dengan strategi hadapi ancaman militer, yaitu dengan aktivitas: Penangkalan, Penindakan atau Penanggulangan dan Pemulihan, namun kekuatan militer tidak digunakan sebagai Kekuatan Utama.

   b. Khusus dlm hadapi Ancaman Cyber, perlu penyesuaian dan penjabaran terhadap UU, Aturan & Ketentuan Pertahanan Negara yang tersedia secara baik dan proporsional, dalam membina kekuatan dan kemampuan *cyber* serta pengoperasian dan kerjasama Nasional. ❑

Daftar Pustaka

Clough Jonathan , 2010, *Principles of Cybercrime,* UK: Cambridge University Press.

Baylis John & Smith Steve, 2001, *The Globalization of World Politics, An Introduction to International Relations,* New York, Oxford University Press.

Goesniadhie Kusnu, 2006, *Harmonisasi Hukum dalam Perspektif Perundang-Undangan,* Surabaya : PT. Temprina Media Grafika.

Sanusi M. Arsyad, 2004, *Teknologi Informasi & Hukum E-commerce,* Jakarta : PT Dian Ariesta , Jakarta.

Kusumaatmadja Mochtar, Etty R. Agoes, 2003, *Pengantar Hukum Internasional,* Bandung: PT. Alumni.

Mugasejati Nanang Pamuji dan Ucu Martanto (ed), 2006, *Kritik Globalisasi & Neoliberalisme,* Yogjakarta: Fakultas Ilmu Sosial dan Ilmu Politik UGM.

Nir Kshetri, 2010, *The Global Cybercrime Industry,* New York : Springer Heidelberg Dordrech.

Roger LeRoy Miller and Gaylord A. Jentz, 2001, *Law for E-Commerce,* USA : West Thomas Learning.

Roni Hanitijo Soemitro, 2001, *Metodologi Penelitian Hukum dan Jurimentri,* Jakarta, Ghalia Indonesia.

Steven Furnel, 2002, *Cybercrime Vandalizing the Information Society,* Great Britain: Pearson Education Limited.

Soeyono Soekanto, 1982, *Pengantar Penelitian Hukum Edisi Kedua,* Jakarta : UI Press, Jakarta.

Soeryono Soekanto, 1998, *Penelitian Hukum Normatif Suatu Tinjauan Singkat,* Jakarta: CV Rajawali.

Sunaryati Hartono, 2006, *Bhineka Tunggal Ika Sebagai Asas Hukum bagi Pembangunan Hukum Nasional,* Jakarta: Penerbit PT Citra Aditya Bakti.

Thomas L. Friedman, 2006, *The World is Flat,* London: Penguin Books.

Branscomb, 1983 , *Information is the Lifeblood that sustain political, social and business decision,* dalam Anne W. Branscomb, Global Governance of Global Networks: "A survey of

Transborder Data Flows in Transition", *Vanderbilt Law Review*, Vol. 36.

Ian J , 2000, *Information Technology Law*, Maureen S. Dorney, 1998, "Privacy and the Internet", *Hasting Communications and Entertainment Law Journal*, Vol 19.

Kofi A. Anan , 2004, dalam *UNCTAD E-commerce and Development Report.*

Stein Schjolberg, 2010, *A Cyberspace Treaty-A United Nations Convention or Protocol on Cybersecurity and Cybercrime,* Background Paper dalam dalamThe Twelfth United Nations Conggress on Crime Prevention and Criminal Justice.

Stein Schjolberg & Amanda M. Hubbard, 2005, Jenewa, *Harmonizing National legal Approaches on Cybercrimw,* Paper dalam WSIS Thematic Meeting on Cybersecurity, ITU, 2005.

Stein Schjolberg, 2010, Paper dalam Twelfh United Nations Conggres on Crime Prevention and CriminalJustice, Brazil.

Susan W.Brenner and Marc D. Goodman, 2002, *Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice,* Paper.

Izwan Ismail, 2008, Understanding Cyber Criminal, New Straits Times, 18 Februari.

Petrus Reinhard Golose, 2006, Perkembangan Cybercrime dan Usaha Penangannya di Indonesia oleh Polri, Buletin Hukum dan Kebanksentralan, Volume 4 Nomor 2, Agustus.

Stein Schjolberg, 2010, Paper dalam Twelfh United Nations Conggres on Crime Prevention and CriminalJustice, Brazil.

MohamadSalahuddiendalam http://www.idsirtii.or.id/index.php/news/2010/01/21/81/mewaspadai-kejahatan-layananperbankan-elektronik-himbauan-kepadamasyarakat-dan-keterangan-pers.html, diakses tanggal 10 September, 2010.

HamadounToure, http://www.pwc.com/gx/en/communications/review/perspective/hamadoun-toure.jhtml, diaksea tanggal 31 Oktober, 2010.

http://www.internetworldstats.com/stats.htm, diakses tanggal 26 oktober, 2010.

http://www.oecd.org/dataoecd/53/60/37019786.pdf, diakses tanggl 10 Desember, 2010.

http://www.itu.int/ITU-*Sinta Dewi, Cybercrime Dalam Abad 21 : Suatu Perspektif Menurut Hukum Internasional*D/cyb/cybersecurity/legislation.html, diakses tanggal 10 desember, 2010

http://www.conventions.coe.int/treaty/commun/cherchesig.html, diakses tanggal 25 Oktober, 2010.

http://www.conventions.coe.int/treaty/EN/treaties/185.html, diakses tanggal 25 Oktober, 2010.

http://www.justice.gov/ Diakses tanggal 27 Oktober, 2010.

http://www.smh.com.au/news/technology/nabcloses-eight-bogus-websites-overseas/2005/12/29/1135732681755.html, diakses tanggal 28 Oktober,

2010.

ITU Toolkit, dalam http://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf, halaman diakses tanggal 25 Oktober, 2010.

Laporan ITU, Understanding Cybecrime for Developing Countries, 2009,dalam http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understandingcybercrime-guide.pdf, diakses tanggal 24 Oktober, 2010.

http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ituunderstanding-cybercrime-guide.pdf, diakses tanggal 24 oktober, 2010.

http:// *www.jim.geovedi.com*
http://www.id.wikipedia.org
http://www.infokomputer.com
http://www.konche.org

Browser China 'Tembak' Perusahaan Amerika, http://www.namadomain.com/, Feb 2010.

Cyber Warfare: Strategy & Tactics, Kenneth Geers, http://www.internetevolution.com/, Feb 2010.

Cyberwarfare, http://en.wikipedia.org/, Feb 2010.

Hacker Menyerang Situs Pemerintahan Georgia, http://www.erakomputer.com/, Feb 2010.

List of cyber attack threat trends, http://en.wikipedia.org/wiki/, Feb 2010.

Network-2, http://expertvoices.nsdl.org/cornell-info204/files/2008/02/network2.jpg, Feb 2010.

Sejarah internet dunia, http://www.kuliah-informatika.com/, Feb 2010.

TOP-500 List - November 2009, http://www.top500.org/, Feb 2010.

Twitter dan Facebook Lumpuh Diserang Zombie, http://tekno.kompas.com/, Feb 2010.

Waspada terhadap Serangan Cyber, http://www.sda-indo.com/, Feb 2010.