Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional

Dr. Darmawan Napitupulu, ST, M. Kom
Dosen Pengajar TIK Universitas Budi Luhur
darwan.na70@gmail.com

Abstract

Increasingly increasing the Information Technology also positive and negative impact. The positive aspect of this virtual world of course adds to the trend of world technological development with all forms of human creativity. In addition, the negative impact can lead to the emergence of crime called cyber crime or crime through the Internet network. The increasingly widespread crime that is closely related to the use of computer-based technology and telecommunication networks is increasingly making the Internet network users become uneasy. The most important information system security policy is in the national legal order in the form of Cyber Law in this case the related ITE and Criminal Law regulating cyberspace activities including sanctions on adverse activity. The research method used is the study of the library (desk research) related to the role of cyber law and its application approach in Indonesia. The results show that the role of cyber law in strengthening the security of national information systems is very strategic. With the existence of cyber caw in addition to protecting the public or the public nationally from the threat of cyber crime, cyber law is a tool to convince the international community that there is already a firm regulation on cyber defense in the country so that inter-state cooperation can be established in building global security. Cooperation between countries is expected also able to trigger a stronger regulation and give global effect.

Keywords*: Cyber Law, Cyber Crime, Security, Information System*

Pendahuluan

Kemajuan ilmu pengetahuan dan teknologi membawa berbagai implikasi kompleks dalam kehidupan manusia dan hubungan antar negara. Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan yang disebut dengan *cyber crime* atau

kejahatan melalui jaringan Internet. Munculnya beberapa kasus *cyber crime* di Indonesia, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Adanya *cyber crime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Beberapa pendapat mengindentikkan *cyber crime* 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 tersebut identik dengan yang diberikan Organization of European Community Development, yang mendefinisikan *computer crime* sebagai: "*any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Adapun Andi Hamzah (1989) dalam tulisannya "Aspek-aspek Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai: "Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dalam dua dokumen Kongres PBB mengenai *The Prevention of Crime* and the *Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal:

1. *Cyber crime* dalam arti sempit disebut *computer crime*, yaitu prilaku ilegal atau melanggar secara langsung menyerang sistem keamanan suatu komputer atau data yang diproses oleh komputer
2. *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu perilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pengertian diatas, secara ringkas dapat dikatakan bahwa *cyber crime* dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. *Cyber crime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet. Maraknya tindak kriminal di dunia maya tergantung dari sejauh mana sumber daya baik berupa *hardware/software* maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya.

Semenjak dikenalnya pola komunikasi melalui dunia maya atau internet, batas-batas konvensional yang dahulu dianut dan dipatuhi oleh konsensus internasional menjadi semu. Dalam hampir satu dekade ini, isu tentang *cyber war* terus didengungkan, bahkan diramalkan bisa memicu ketegangan antar negara yang berimbas pada terancamnya kedamaian dunia. Penyerangan secara terbatas telah terjadi berkali- kali oleh beberapa negara, dimana kondisi ini dapat juga diasumsikan sebagai uji coba, namun peperangan yang sesungguhnya dan jauh lebih besar telah dipersiapkan berdasarkan urutan kronologis kejadian pada jaringan komputer di dunia yang telah terjadi antara tahun 1990-an sampai saat ini yaitu mulai dari Sniffers, DNS (Denial of Service), Trojan, DDoS hingga yang terakhir virus Ramsonware.

Trend ancaman serangan *cyber* akan berkembang terus sesuai perkembangan teknologi informasi serta berbagai bentuk kejahatan *cyber crime*, oleh karenanya perlu dilakukan riset secara terus-menerus untuk mampu mengatasi berbagai teknik, taktik dan, strategi pertahanan *cyber* yang akan terus berkembang ke depan. Bila kita berbicara pertahanan, maka terlebih dahulu harus ditetapkan ancaman. Dalam UU No 3 Tahun 2002 tentang Pertahanan Negara, telah ditetapkan bahwa ancaman dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non militer, termasuk diantaranya ancaman *cyber*. Dengan kata lain, perlu adanya upaya penanggulangan terhadap *cyber crime*, yakni salah satunya berupa penegakan hukum *cyber* (*cyber law*) sebagai benteng pertahanan melawan *cyber crime*.

Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi. Saat ini semua aspek perekonomian, sosial dan pertahanan begitu tergantung kepada internet. Aktivitas perbankan, perekonomian, pemeliharaan dan penggunaan transportasi, pengendalian persenjataan hingga komunikasi sosial tidak bisa terlepas dari interkoneksi tersebut. Data pada Kemkominfo mencatat bahwa rata-rata jumlah serangan dunia maya per hari pada tahun 2011 mencapai 1,25 juta insiden, dimana aktivitas ini cenderung semakin meningkat berbanding lurus dengan pengguna internet. Privasi dan berbagai informasi rahasia dapat dengan mudah dihancurkan oleh para pelaku kejahatan *cyber* ini, dimana bila eskalasinya semakin meluas dapat membuat keresahan yang meluas pada masyarakat. Oleh karena itu *cyber law* sangat mutlak dibutuhkan serta bersifat strategis khususnya untuk melindungi

masyarakat (*community*) yang merupakan perangkat intelektual (*brainware*), baik dalam kedudukannya sebagai pelaku usaha, profesional penunjang maupun pengguna. Penelitian ini bertujuan mengkaji peranan *cyber law* dalam memperkuat keamanan sistem informasi nasional sehingga pada gilirannya dapat mendukung kedaulatan bangsa di kancah global.

Tinjauan Pustaka

1. Potensi Kejahatan Dunia Maya

Kejahatan dalam bidang teknologi informasi dengan melakukan serangan elektronik berpotensi menimbulkan kerugian pada bidang politik, ekonomi, sosial budaya, yang lebih besar dampaknya dibandingkan dengan kejahatan yang berintensitas tinggi lainnya. Di masa datang, serangan elektronik dapat mengganggu perekonomian nasional melalui jaringan yang berbasis teknologi informasi seperti perbankan, telekomunikasi satelit, listrik dan lalu lintas penerbangan. Hal ini dipicu oleh beberapa permasalahan yang ada dalam konvergensi teknologi, misalnya internet membawa dampak negatif dalam bentuk munculnya jenis kejahatan baru, seperti *hacker* yang membobol komputer milik bank dan memindahkan dana serta merubah data secara melawan hukum. Teroris menggunakan internet untuk merancang dan melaksanakan serangan, penipu menggunakan kartu kredit milik orang lain untuk berbelanja melalui internet. Perkembangan TI di era globalisasi akan diwarnai oleh manfaat dari adanya *e-commerence, e-government, foreign direct investment*, industri penyedia informasi dan pengembangan UKM.

Dapat dibayangkan, bagaimana jika sebuah infrastuktur teknologi informasi yang bersentuhan dengan hajat hidup orang banyak tidak dilindungi dengan sistem keamanan. Misalnya jaringan perbankan, dikacau balaukan atau dirusak data-datanya oleh pihak yang tidak bertanggung jawab, sehingga informasi yang ada di dalamnya juga kacau dan rusak. Dengan demikian masyarakat yang bersentuhan hanyalah sederetan tulisan, akan tetapi angka-angka dalam sebuah data dan informasi perbankan merupakan hal yang sensitif. Kacaunya atau rusaknya angka-angka tersebut dapat merugikan masyarakat dan bahkan dapat merusak lalu lintas perekonomian dan keuangan serta dapat berdampak pada keamanan, ketentraman dan ketertiban dalam masyarakat. Demikian pula, infrastuktur TI lainnya seperti Penerbangan, Pertahanan, Migas, PLN dan lain-lainnya, dapat dijadikan sebagai sarana teror bagi teroris. Di masa depan, bukan tidak mungkin

teroris akan menjadikan jaringan teknologi informasi sebagai sarana untuk membuat kacau dan teror dalam masyarakat.

Motivasi untuk melakukan kejahatan dunia maya meningkat secara eksponensial. Ditambah lagi dengan potensi yang dihasilkan dari kejahatan dunia maya. Pada kejahatan perampokan bank, rata-rata dihasilkan US$ 14,000 sedangkan dalam kejahatan berbasis teknologi informasi (*cyber crime*) kerugian yang dihasilkan rata-rata bisa mencapai US$ 2 juta. Berapa besar kerugian yang sebenarnya terjadi akibat *cyber crime* tidak dapat dinilai secara pasti, karena sangat sedikit perusahaan atau organisasi yang melaporkannya. Hal ini terjadi karena mereka takut akan adanya kepanikan yang dapat mengakibatkan kerugian yang lebih besar lagi.

Pemerintah juga memberikan perhatian serius pula terhadap masalah keamanan informasi. Kementerian Kominfo telah membentuk ID- SIRTI (Indonesian Security Incident Response Team on Information Infrastructure), POLRI juga membentuk Cyber Task Force Center, disamping itu juga ada ID-CERT sebagai institusi independen yang bertujuan melakukan sistem keamanan teknologi informasi. Pada era global sekarang ini, keamanan sistem informasi berbasis internet menjadi suatu ”keharusan” untuk diperhatikan, karena jaringan komputer internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer yang lain dalam internet, data itu akan melewati sejumlah komputer yang lain yang berarti akan memberi kesempatan pada *user* internet lainnya untuk menyadap atau mengubah data tersebut. Dalam perjalanan data tersebut, memungkinkan orang lain untuk ikut serta ”mendengarkan” melalui alat bantu yang lazim disebut dengan ”*sniffer*”. Oleh karena itu, keamanan sistem informasi nasional menjadi penting untuk senantiasa ditingkatkan secara komprehensif.

2. Keamanan Sistem Informasi

Teori informasi menekankan bahwa agar benar-benar mampu memberikan dukungannya kepada proses pengambilan keputusan manajerial dan agar aplikasinya tepat dan akurat, informasi yang dibutuhkan oleh suatu organisasi harus memenuhi persyaratan kelengkapan, kemutakhiran, kehandalan, terolah dengan baik, tersimpan dengan rapi dan mudah ditelusuri pada tempat penyimpanannya. Persyaratan-persyaratan tersebut hanya mungkin

terpenuhi apabila data yang merupakan bahan baku untuk informasi, digali dari sumber-sumber yang tepat dan benar, dan dengan mutu yang tinggi. Teori ini perlu mendapat penekanan karena, seperti dimaklumi, data tidak mempunyai nilai intrinsik dalam proses pengambilan keputusan. Oleh karena itu, data yang dikumpulkan dari berbagai sumber, memerlukan pengolahan lebih lanjut agar sifatnya berubah menjadi informasi yang memiliki nilai sebagai alat pendukung proses pengambilan keputusan.

Menciptakan informasi tidak terlepas dari identifikasi dan penggalian sumber-sumber yang tepat dan benar. Sumber-sumber informasi yang dapat dan layak digali sangat bervariasi dari satu organisasi ke organisasi lain karena sangat tergantung pada proses pengambilan keputusan apa yang akan didukungnya dan untuk kepentingan apa infomasi tersebut akan dipergunakan. Setiap orang yang pernah berkecimpung dalam kegiatan pengolahan informasi pasti mengetahui bahwa sumber-sumber tersebut dapat berada di dalam suatu organisasi seperti berbagai satuan kerja yang terdapat di dalamnya akan tetapi dapat pula berada di luar organisasi yang bersangkutan. Instrumen untuk memperolehnya pun dapat beraneka ragam.

Masalah keamanan sistem informasi menempati kedudukan yang sangat penting, akan tetapi perhatian para pemilik dan pengelola sistem informasi relatif masih kurang, bahkan menempati kedudukan kedua atau berikutnya dalam daftar-daftar berbagai hal yang dianggap penting dalam pengelolaan sistem informasi berbasis internet. Ada beberapa hal yang harus dilindungi dalam sebuah sistem jaringan informasi global berbasis internet (*cyberspace*), yaitu :

1. Isi/substansi data dan/atau informasi yang merupakan input dan output dari penyelenggara sistem informasi dan disampaikan kepada publik atau disebut juga dengan *content*. Dalam hal penyimpanan data dan /atau informasi tersebut akan disimpan dalam bentuk *data base* dan dikomunikasikan dalam bentuk data messages;
2. Sistem pengolahan informasi (*computing and/or information system*) merupakan jaringan sistem informasi organisasional yang efisien, efektif dan legal. Dalam hal suatu sistem informasi merupakan perwujudan penerapan perkembangan teknologi informasi ke dalam suatu bentuk organisasional /organisasi perusahaan (bisnis);

3. Sistem komunikasi (c*ommunication*) merupakan perwujudan dari sistem keterhubungan (*interconnection*) dan sistem pengoperasian global (*inter operational*) antar sistem informasi /jaringan komputer (*computer network*) maupun penyelenggaraan jasa dan/atau jaringan telekomunikasi; dan
4. Masyarakat (*community*) sebagai subyek atau pengguna Internet

Menjaga keempat aspek tersebut merupakan bagian dari *policy* keamanan sistem informasi. Keamanan sistem informasi berbasis internet merupakan suatu keharusan yang harus diperhatikan karena jaringan komputer internet sifatnya publik dan global pada dasarnya tidak aman. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar informasi yang berharga itu dapat terlindungi secara efektif. Untuk mencapai semua itu, jaringan komputer harus dianalisis sehingga diketahui apa yang harus dan untuk apa diamankan, serta seberapa besar nilainya.

Keamanan komputer (*computer security*) melingkupi 4 (empat) aspek, yaitu *privacy, integrity, authentication* dan *availability*. Selain keempat aspek itu masih ada 2 (dua) aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non- repudiation*. Aspek utama dari *privacy* atau *confidentially* adalah usaha untuk menghindarkan penggunaan informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data yang sifatnya *private*, sedangkan c*onfidentially* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Aspek *integrity* menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi tersebut. Aspek *authentication* berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi tersebut adalah betul-betul orang yang dimaksud. Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. *Access control* berhubungan dengan cara pengaturan akses pada informasi. Hal ini biasanya berhubungan dengan masalah *authentication* dan juga *privacy*. Aspek *non-repudiation* ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Hasil dan Pembahasan

1. Ruang Lingkup Cyber Law

Aspek hukum yang istilahnya berasal

dari *cyberspace law*, yang ruang lingkupnya meliputi, setiap aspek yang berhubungan dengan orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai *online* dan memasuki *cyber space* atau dunia maya.

Menurut Jonathan Rosenoer dalam *Cyber Law – The Law of Internet* menyebutkan ruang lingkup *cyber law*:

1. Copy Right
2. Trademark
3. Defamation
4. Hate Speech
5. Hacking, Viruses, Illegal Access
6. Regulation Internet Resource
7. Privacy
8. Duty Care
9. Criminal Liability
10. Procedural Issuses (Jurisdiction, Investigation,
Evidence, etc)
11. Electronic Contract
12. Pornography
13. Robbery
14. Consumer Protection
15. E-Commerce, E-Government
16. Urgensi pengaturan *cyber law* di Indonesia adalah:
17. Kepastian hukum
18. Untuk mengantisipasi implikasi – implikasi yang timbul akibat pemanfaatan teknologi informasi
19. Adanya variabel global, yaitu persaingan bebas dan pasar terbuka

Ruang lingkup *Cyber Law* di Indonesia adalah :

- Hukum Publik : Juridiksi, Etika Kegiatan *Online*, Perlindungan Konsumen, Anti Monopoli, Persaingan Sehat, Perpajakan, *Regulatory Body*, *Data Protection* dan *Cyber Crimes*.
- Hukum Privat : HAKI, *E-Commerce*, *Cyber Contract*, *Domain Name*, *Insurance*.

Penegakan hukum tentang *cyber crime* terutama di Indonesia sangatlah dipengaruhi oleh lima faktor yaitu undang-undang, mentalitas aparat penegak hukum, perilaku masyarakat, sarana dan kultur. Hukum tidak bisa tegak dengan sendirinya selalu melibatkan manusia didalamnya dan juga melibatkan tingkah laku manusia didalamnya. Hukum juga tidak bisa tegak dengan sendirinya tanpa adanya penegak hukum. Penegak hukum tidak hanya dituntut untuk profesional dan pintar dalam menerapkan norma hukum tapi juga berhadapan dengan seseorang bahkan kelompok masyarakat yang diduga melakukan kejahatan.

Dengan seiringnya perkembangan jaman dan perkembangan dunia kejahatan, khususnya perkembangan *cyber crime* yang semakin mengkhawatirkan, penegak hukum dituntut untuk bekerja

keras karena penegak hukum menjadi subjek utama yang berperang melawan *cyber crime*. Misalnya Resolusi PBB No.5 tahun1963 tentang upaya untuk memerangi kejahatan penyalahgunaan Teknologi Informasi pada tanggal 4 Desember 2001, memberikan indikasi bahwasanya ada masalah internasional yang sangat serius, gawat dan harus segera ditangani. Kitab Undang-undang Hukum Pidana (KUHP) masih dijadikan sebagai dasar hukum untuk menjaring *cyber crime*, khususnya jenis *cyber crime* yang memenuhi unsur-unsur dalam pasal- pasal KUHP.

Beberapa dasar hukum dalam KUHP yang digunakan oleh aparat penegak hukum antara lain: pasal 167 KUHP; pasal 406 ayat (1) KUHP; pasal 282 KUHP; pasal 378 KUHP; pasal 112 KUHP; oasal 362 KUHP dan pasal 372 KUHP. Selain KUHP, tentunya UU yang berkaitan dengan hal ini, yaitu UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dimana aturan tindak pidana yang terjadi didalamnya terbukti mengancam para pengguna internet. Sejak ditetapkannya UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada 21 April 2008, telah menimbulkan banyak korban. Berdasarkan pemantauan yang telah aliansi lakukan paling tidak telah ada 4 orang yang dipanggil polisi dan menjadi tersangka karena diduga melakukan tindak pidana yang diatur dalam UU ITE. Para tersangka atau korban UU ITE tersebut merupakan pengguna internet aktif yang dituduh telah melakukan penghinaan atau terkait dengan muatan penghinaan di internet.

Orang-orang yang dituduh berdasarkan UU ITE tersebut kemungkinan seluruhnya akan terkena pasal 27 ayat (3) dan Pasal 45 ayat (1) UU ITE yakni dengan ancaman 6 tahun penjara dan denda 1 miliar rupiah. UU ITE dapat digunakan untuk melindungi dan menindak seluruh pengguna dan aktivitasnya di internet tanpa terkecuali jurnalis atau bukan.

Tindak pidana yang menjadi perhatian serius dalam UU ITE selama ini :

1. Pasal 27 (1) : Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2. Pasal 27 (3) : Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan / atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki

muatan penghinaan dan/atau pencemaran nama baik.

3. Pasal 28 (2) : Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

2. Pendekatan Penerapan Cyber Law

Seperti disebutkan sebelumnya bahwa di Indonesia semakin banyak infrastruktur strategis dan layanan publik yang bergantung pada sistem informasi, teknologi dan jaringan. Paradigma keamanan nasional telah bergeser kepada aspek yang lebih luas yaitu termasuk jaminan keamanan pribadi warga negara. Kewajiban pokok dari suatu negara adalah memberikan keamanan terhadap warganyanya tersebut termasuk keamanan dari berbagai kejahatan *cyber*. Setiap saat warga negara dapat merasa terancam pada aset yang dimilikinya.

Dalam jangkauan yang lebih luas, keterbatasan penguasaan teknologi negara dan belum adanya regulasi yang lebih tegas mengenai pertahanan *cyber* dapat membahayakan negara secara nyata. Negara lain ataupun kelompok dengan kepentingan tertentu dapat dengan mudah memasuki ranah infrastruktur vital yang dimiliki negara kita. Oleh karena itu diperlukan kebijakan keamanan sistem informasi yang menyediakan kerangka- kerangka untuk membuat keputusan yang spesifik, misalnya mekanisme apa yang akan digunakan untuk melindungi jaringan dan bagaimana mengkonfigurasi servis-servis. Kebijakan keamanan juga merupakan dasar untuk mengembangkan petunjuk pemrograman yang aman untuk diikuti user maupun bagi administrator sistem.

Kebijakan keamanan sistem informasi yang paling penting ada pada tatanan hukum nasional dalam bentuk Undang-undang Dunia Maya (*cyber law*) yang mengatur aktivitas dunia maya termasuk pemberian sanksi pada aktivitas jahat dan merugikan. Pengaturan hukum dalam internet masih relatif baru dan terus berkembang, ada dorongan pengaturan yang bersifat global, namun kedaulatan hukum menjadikannya tidak mudah terlaksana. Hal ini menjadi salah satu kelemahan dari penegakan *cyber law*, terutama jika menyangkut perkara kejahatan yang dilakukan oleh individu atau teroris dan entitas bisnis yang berada di negara lain. Konstitusi suatu negara tidak dapat dipaksakan kepada Negara lain, karena dapat bertentangan dengan kedaulatan dan konstitusi negara

lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja. Masyarakat peduli keamanan teknologi informasi sangat menaruh perhatian dan kerjasama global dalam menyikapi kejahatan-kejahatan TI yang sudah terjadi, sedang terjadi dan akan terjadi, seperti misalnya *Convention on Cyber Crime* 2001 yang digagas oleh Uni Eropa pada tanggal 23 November 2001 di Budapest, Hongaria. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari *cyber crime* baik melalui undang- undang maupun kerjasama international. Dalam konvensi ini telah dicakup adanya ”ekstradisi otomatis”, artinya, walau tidak ada perjanjian ektradisi dengan negara tertentu, cukup dengan meratifikasi konvensi ini atau ikut dalam konvensi ini, maka telah dianggap adanya perjanjian ekstradisi dengan negara-negara peserta konvensi, guna mempersempit ruang yurisdiksi suatu negara terhadap negara lainnya khususnya dalam menegakkan hukum *cyber* secara global. Dengan kata lain, pemerintah perlu bekerjasama dengan pihak-pihak maupun negara lain untuk membangun keamanan global. Satu negara tidak akan mungkin dapat membuat perlindungan terhadap dirinya sendiri dalam menghadapi ancaman global tersebut. Kerjasama antar negara diharapkan juga mampu mencetuskan sebuah regulasi dibidang siber (*cyber law*) yang lebih kuat dan memberi efek global. Dengan adanya *cyber law* yang tegas di dunia internasional tersebut kiranya mampu mengurangi maraknya kejahatan di dunia *cyber*.

Kejahatan maya (*cyber*) dapat dipicu oleh adanya transisi dari *single* vendor ke multi vendor. Banyak jenis perangkat dari berbagai vendor yang harus dipelajari, misalnya untuk router Cisco, Bay Networks, Nortel, 3Com, Juiper, Linux-Based router dan sebagainya. Dan untuk server seperti Solaris, Windowa NT/2000/XP, SCO Unix, Linux, BSD, AIX, HP-UX dan sebagainya. Untuk mencari satu orang yang menguasai semuanya sangatlah sulit. Apalagi jika dibutuhkan sumber daya manusia (SDM) yang lebih banyak. Disamping itu, kesulitan penegak hukum untuk mengejar kemajuan dunia telekomunikasi dan komputer, *cyber law* masih dalam proses pembuatan, tingkat awareness masih rendah, technical capability juga masih rendah, dan potensi lubang-lubang keamanan semakin besar, karena meningkatnya kompleksitas sistem, program menjadi semakin besar, dari *megabytes* menjadi *gigabytes*, ketergantungan komputer dan jumlah komputer yang digunakan semakin bertambah, nilai informasi

semakin berharga/tinggi, jumlah operator komputer semakin bertambah, jaringan sistem semakin luas, hukum kurang menjangkau kejahatan teknologi informasi, belum ada manajemen yang melakukan aksi *preventive* yang pro-aktif, pola bisnis berubah, *partners, alliance*, *inhouse development*, *outsource* dan sebagainya. Untuk itu, tanggung jawab keamanan sistem informasi nasional merupakan tanggung jawab kita bersama.

Sebagai tanggung jawab kita bersama, maka kita perlu untuk melakukan pencegahan dan penanggulangan, khususnya dalam jajaran pemerintah dengan instansinya yang terkait dan bersinergi dengan pihak non pemerintah. Hal ini perlu dilakukan, mengingat adanya ”*Lack of Law*”, dimana KUHP tidak mengatur secara khusus kejahatan berbasis TI, walaupun beberapa kasus dapat dipakai pasal-pasal tertentu. UU No: 36 Tahun 1999 tentang Telekomunikasi lebih fokus pada *pipeline issues* sehingga kurang memadai untuk menganggulangi masalah- masalah yang terkait dengan ICT, dan di lain sisi adanya *procedure* versus *protecting privacy*, *Lack of Cybercrime Expertise, Jurisdiction versus Internet is borderless World*, dan kurangnya kerjasama antara pihak-pihak terkait.

Pendekatan lainnya dalam menerapkan *cyber law* di Indoneia atau memitigasi meningkatnya jumlah kejadian kejahatan (*cyber crime*) di dunia maya, perlu diperhatikan akar penyebabnya terlebih dahulu. Dari berbagai pendapat dan pendekatan yang ada, terlihat adanya tiga jenis aspek usaha mengatasinya, yaitu masing-masing dipandang dari sisi teknis, bisnis, dan sosial. Berdasarkan konteks ini Aspek teknis digunakan sebagai pendekatan karena menimbang bahwa pada tataran infrastruktur, internet tidak lain terbentuk dari gabungan sejumlah komponen teknis - seperti komputer, *router, hub, modem, database*, aplikasi, printer, website, *firewalls*, dan lain-lain yang membentuk sebuah jejaring raksasa, dimana secara bebas data dan informasi dapat dipertukarkan untuk beragam keputusan. Berdasarkan konteks ini maka terlihat jelas adanya langkah-langkah secara teknis yang harus dilakukan untuk dapat mengawasi keberlangsungan operasional infrastruktur jejaring internet. Sementara itu dipandang dari perspektif bisnis, internet dianggap sebagai suatu medium atau alat atau sarana berbagai pemangku kepentingan dalam usahanya untuk melakukan kegiatan pertukaran barang dan/atau jasa. Tanpa adanya konteks kebutuhan, maka tidak terjadi peristiwa bisnis. maka terlihat jelas adanya

langkah-langkah secara teknis yang harus dilakukan untuk dapat mengawasi keberlangsungan operasional infrastruktur jejaring internet. Sementara itu dipandang dari perspektif bisnis, internet dianggap sebagai suatu medium atau alat atau sarana berbagai pemangku kepentingan dalam usahanya untuk melakukan kegiatan pertukaran barang dan/atau jasa. Tanpa adanya konteks kebutuhan, maka tidak terjadi peristiwa bisnis. Di satu sisi ada perusahaan yang jika internetnya tidak jalan akan menimbulkan kerugian yang luar biasa, sementara di pihak lain ada organisasi yang tanpa internet masih dapat berjalan dengan baik. Sehingga kebutuhan untuk mengamankan sistem informasi harus dipandang dari sisi ini. Sementara itu aspek sosial menekankan bahwa walau bagaimanapun juga, yang berinteraksi dalam internet adalah manusia - bukan robot atau mesin, sehingga harus diperhatikan pula aspek psikologis dan perilaku mereka sebagai individu yang berakal budi. Perlu diingat bahwa dalam implementasinya, ketiga aspek ini biasanya dilihat sebagai sebuah kesatuan holistik - dalam arti kata bahwa untuk meningkatkan keamanan sistem informasi nasional secara optimal, maka ketiga aspek tersebut harus dapat diakomodasi baik oleh lembaga pemerintah maupun swasta.

Kesimpulan

Semakin meningkatnya Teknologi Informasi semakin banyak juga dampak positif dan negatifnya. Segi positif dari dunia maya ini tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Selain itu dampak negatifnya dapat menyebabkan munculnya kejahatan yang disebut dengan *cyber crime* atau kejahatan melalui jaringan Internet. Semakin maraknya tindakan kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini semakin membuat para kalangan pengguna jaringan Internet menjadi resah.

Kebijakan keamanan sistem informasi yang paling penting adalah pada tatanan hukum nasional dalam bentuk Undang-undang Dunia Maya (*Cyber Law*) dalam hal ini UU ITE dan KUHP terkait yang mengatur aktivitas dunia maya termasuk pemberian sanksi pada aktivitas yang merugikan. Peran *cyber law* dalam memperkuat keamanan sistem informasi nasional sangat lah strategis. Dengan adanya *cyber law* selain untuk melindungi masyarakat atau publik

secara nasional dari ancaman kejahatan *cyber crime*, *cyber law* menjadi alat untuk meyakinkan dunia internasional bahwa sudah ada regulasi yang tegas mengenai pertahanan *cyber* di dalam negeri sehingga dapat terjalin kerjasama antar negara dalam membangun keamanan global. Kerjasama antar negara tersebut diharapkan juga mampu mencetuskan sebuah regulasi yang lebih kuat dan memberi efek global. Dengan adanya *cyber law* yang tegas di dunia internasional tersebut kiranya mampu mengurangi maraknya kejahatan di dunia maya.

Daftar Pustaka

Abidin, D. 2015. Kejahatan dalam Teknologi Informasi dan Komunikasi. Jurnal Ilmiah Media Processor, Vol. 10, No.2, pp: 1-8.

Ahmadjayadi, C. 2008. Perlunya Cyber Law dalam Rangka Menghadapi dan Menanggulangi Kejahatan Dunia Maya. Buletin Hukum Perbankan dan Kebanksentralan, Vol. 6, No. 1, pp: 1-6.

As-Saber, S., Srivastava, A., & Hossain, K. 2006. Information Technology Law and E-Government : A Developing Country Perspective. JOAAG, Vol. 1, No. 1, pp: 84-101.

Ketaren, E. 2016. Cyber Crime, Cyber Space dan Cyber Law. Jurnal Times, Vol. 5, No. 2, pp: 35-42.

Marita, L. 2015. Penerapan Cyber Law dalam Pemberantasan Cyber Crime di Indonesia. Jurnal Cakrawal, Vol. 15, No. 2, pp: 44-52.

Nasution, M. 2008. Urgensi Keamanan pada Sistem Informasi. Jurnal Iqra, Vol. 2, No. 2, pp:41-54

Soewardi, B. 2013. Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh bagi Indonesia. Potensi Pertahanan, Media Informasi Ditjen Pothan Kemhan.