ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 9548-9556
Volume 7 Nomor 2 Tahun 2023

Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara

Muhammad Hafid[1], Favian Zhuhri Firjatullah[2], Billyco Windy Pamungkaz[3]

[1,2,3]Progam Studi Magister Ilmu Hukum, Universitas Wijaya Kusuma Surabaya

e-mail: mhafid74@gmail.com[1], fzhuhri@gmail.com[2], billycowpamungkaz81@gmail.com[3]

Abstrak

Perkembangan teknologi khususnya dibidang telekomunikasi dan transportasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasi di pelbagai aspek kehidupan. Setiap negara harus menghadapi kenyataan bahwa informasi dunia saat ini dibangun berdasarkan suatu jaringan yang ditawarkan oleh kemajuan bidang teknologi. Sebagai media penyedia informasi internet juga merupakan sarana kegiatan komunitas komersial terbesar dan terpesat pertumbuhannya. Arus globalisasi yang terjadi di seluruh dunia sekarang ini telah membawa dunia pada era perkembangan teknologi informasi dan komunikasi sehingga menciptakan era yang serba digital (digital world).Dalam hal ini, perkembangan teknologi komputer dan internet menjadi sarana baru bagi negara-negara di dunia untuk dimanfaatkan sebagai alat untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai negara sehingga sangat mendorong dunia pada perkembangan yang kompleks, beragam dan majemukBerbagai kasus pelanggaran hukum melalui media internet kini kerap terjadi di Indonesia, kondisi Indonesia secara global dalam persoalan *ciber crime* sudah sangat memprihatinkan. tantangan yang di hadapi oleh masyarakat terkait adanya cyber crime berupa hilangnya data pribadi bisa juga hilangnya uang, ada juga penyelwengan informasi dan masih banyak lagi jenis dan macam dari kejahatan cyber ini, maka dari itu untuk menjawab tantangan bagi masyarakat menghadapi perubahan-perubahan dari zaman multimedia ini dituntut untuk faham akan bahaya menggunakan teknologi sehingga masyarakat harus meningkatkan kewaspadaan akan arus gobalisasi dizaman teknologi ini

Kata Kunci : Kejahatan Cyber, Teknologi Informasi, Kejahatan Dunia Maya

Abstract

Technological developments, especially in the field of telecommunications and transportation, are regarded as a locomotive and have contributed to accelerating the process of globalization in various aspects of life. Every country must face the fact that the world's information is currently built based on a network offered by advances in technology. As a media provider of information, the internet is also the largest and fastest growing means of commercial community activity. The flow of globalization that is happening all over the world today has brought the world into the era of development of information and communication technology so as to create an all-digital era (digital world). as a tool for penetrating, influencing and infiltrating various countries so that it greatly encourages the world to develop complex, diverse and pluralistic forms. Various cases of violations of law via the internet are now common in Indonesia, Indonesia's global condition in terms of cybercrime is very concerning. the challenges faced by the community are related to cyber crime in the form of loss of personal data as well as loss of money, there is also misappropriation of information and many other types and types of cyber crime, therefore to answer the challenge for society to face changes from the multimedia era It is required to understand the dangers of using technology so that people must increase their awareness of globalization in this technological era.

Keywords : Cybercrime, Information Technology, Criminal Policy

PENDAHULUAN

Saat ini dunia tengah berada dalam era informasi yang merupakan tahapan lanjutan dari era prasejarah, era agraris, dan era industri. Pada era informasi, keberadaan suatu informasi mempunyai arti dan peranan yang sangat penting bagi semua aspek kehidupan, serta merupakan salah satu kebutuhan hidup bagi semua orang baik individual maupun organisasi, sehingga dapat dikatakan bahwa dalam masyarakat informasi, informasi telah berfungsi sebagaimana layaknya aliran darah sumber kehidupan bagi tubuh manusia.

Perkembangan politik dunia yang selalu mengalami perubahan dari waktu ke waktu sehingga mempengaruhi seluruh tatanan kehidupan dunia. Dunia yang dinamis terus mengalami perubahan yang kadangkala diwarnai turbulensi yang mempengaruhi relasi antar negara dan konstelasi isu global sehingga mempengaruhi sendi-sendi kehidupan berbangsa dan bernegaraa tak lupa pula kehidupan sosial masyarakat. Setiap perkembangan global di dunia selalu akan mempengaruhi seluruh kehidupan nasional di masing-masing negara sehingga memaksa setiap negara untuk selalu mencermati dan menelaah setiap perkembangan lingkungan strategis baik di tingkat global, regional, nasional, maupun lokal.

Arus globalisasi yang terjadi di seluruh dunia sekarang ini telah membawa dunia pada era perkembangan teknologi informasi dan komunikasi sehingga menciptakan era yang serba digital (digital world).Dalam hal ini, perkembangan teknologi komputer dan internet menjadi sarana baru bagi negara-negara di dunia untuk dimanfaatkan sebagai alat untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai negara sehingga sangat mendorong dunia pada perkembangan yang kompleks, beragam dan majemuk.

Salah satu temuan yang memberikan pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi. Internet telah menyebabkan terjadinya satu lompatan besar dalam kehidupan. Sama halnya dengan teknologi lainnya, internet tidak bebas nilai. Teknologi akan menjadi efektif jika kita memberi perhatian pada kegunaan dari teknologi yang disesuaikan dengan nilai-nilai sosial maupun pribadi serta adanya peraturan pemerintah yang melindungi masyarakat dari dampak negatif yang ditimbulkannya.

Terkait dengan internet terdapat sejumlah konsep yang berhubungan yaitu telematika, multimedia dan cyber space. Istilah telematika dikenal sebagai the new hybrid of technology yang muncul karena perkembangan teknologi digital yang membuat perkembangan teknologi telekomunikasi dan informatika semakin terpadu atau yang biasa disebut dengan konvergensi. Konvergensi antara teknologi telekomunikasi, media dan informatika tersebut akhirnya mendorong penyelenggaraan sistem elektronik berbasis teknologi digital yang kemudian di kenal dengan istilah the net. Konvergensi itu sendiri adalah merupakan gejala yang mengemuka dalam industri jasa Teknologi Informasi Komunikasi (TIK) yang muncul sejalan dengan pesatnya kemajuan teknologi elektronika pada akhir abad 20. Dampak konvergensi secara sosial telah dirasakan masyarakat baik itu positif maupun negatif. Salah satu dampak negatif yang muncul dalam cyber-space adalah terjadinya cyber crime. Maraknya cyber crime memerlukan perhatian dan keseriusan dalam mengembangkan cyber security bagi sebuah negara termasuk Indonesia.

Di masa sekarang ini dalam perkembangan zaman masyarakat Indonesia banyak menggunakan teknologi informasi pada taraf teknologi sebagai alat komunikasi yaitu biasa disebut media sosial yang berfungsi untuk berkomunikasi satu sama lain. Tidak menutup kemungkinan adanya pengaruh negatif dari perkembangan teknologi tersebut untuk masyarakat, maka dari itu perlu upaya-upaya untuk meningkatkan kewaspadaan untuk masyarakat supaya terhindar dari kejahatan cyber crime di era digital ini.

Banyaknya pengaruh yang ada dalam teknologi multimedia berperan penting dalam pergeseran budaya, maksudnya ketika belum mengenal teknologi masyarakat mengandakan bertemu untuk berkomunikasi kemudian untuk mengumpulkan banyak orang pada zaman itu menggunakan alat seperti halnya kentongan/toa speaker, dan masih banyak hal. Setelah

adanya internet atau multimedia seseorang tanpa bertemu pun dapat berkomunikasi sehingga lama-kelamaan orang akan kehilanggan kebiasaan untuk bersosial dalam hal ini untuk bertemu langsung. Belum lagi tantangan yang di hadapi oleh masyarakat terkait adanya cyber crime berupa hilangnya data pribadi bisa juga hilangnya uang, ada juga penyelwengan informasi dan masih banyak lagi jenis dan macam dari kejahatan cyber ini, maka dari itu untuk menjawab tantangan bagi masyarakat menghadapi perubahan-perubahan dari zaman multimedia ini dituntut untuk faham akan bahaya menggunakan teknologi sehingga masyarakat harus meningkatkan kewaspadaan akan arus gobalisasi dizaman teknologi ini.

Indonesia sebenarnya saat ini tengah dalam keadaan mendesak cyber-security atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau cyber crime di Indonesia sudah mencapai tahap memprihatinkan. Namun berbeda dengan penangganan kejahatan lainnya. Berdasarkan hal tersebut maka permasalahan yang akan dibahas dalam kajian ini adalah analisa kebijakan cybersecurity yang telah dijalankan di Indonesia dan dampak yang terjadi dalam masyarakat.

Menajemen teknologi informasi

Ada 4 (empat) pondasi utama yang mendukung perkembangan teknologi informasi yaitu: perkembangan perangkat lunak (software) seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (content management), telecommunication and networking, perkembangan internet serta perdagangan online atau melalui internet.

Sementara untuk pengorganisasian terkait dengan pengunaan sistem teknologi informasi setidaknya ada empat hal utama yang harus diperhatikan yaitu: pertama, sistem informasi (information systems) dan kedua, kompetisi organisasi (organizational competition); ketiga, information systems (sistem informasi) dan organizational decision making (sistem informasi dan pengambilan keputusan dalam organisasi); keempat, pengorganisasian penggunaan sistem informasi (organizational use of information systems).

Pada dasarnya sistem informasi itu terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dan pengambilan keputusan dalam organisasi. Teknologi Informasi Komunikasi (TIK) adalah salah satu komponen paling penting dalam pengembangan sistem informasi.

Pengelolaan sumber daya sistem informasi adalah permasalahan selanjutnya terkait dengan tantangan pengembangan TIK. Ada empat kunci utama yang harus diperhatikan agar pengelolaan sumber daya sistem informasi berhasil yaitu: pertama, bahwa pengelolaan sumber daya sistem informasi haruslah ditempatkan sebagai proses manajemen bisnis. Kedua, Pembangunan sistem informasi. Ketiga, sumber daya external sistem informasi. Keempat, manajemen sumber daya informasi.

Cyber-security dan Pertahanan Negara

Cyber-security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.

Cyber-security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap *Global cyber-security* dibangun di atas lima bidang kerja: *Global cyber-security* dibangun di atas lima bidang kerja: Kepastian Hukum (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) (undang-undang *cyber crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan

perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman cyber crime risiko keamanan yang relevan dalam lingkungan cyber. Tujuan keamanan umum terdiri dari: ketersediaan; Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan.

Cyber-security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun cyber attack. Cyber-security merupakan upaya untuk melindungi informasi dari adanya cyber attack, adapun elemen pokok cyber-security adalah:

1. Dokumen security policy merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. Information infrastructure merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah router, switch, server, sistem operasi, database, dan website.
3. Perimeter Defense merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan firewall.
4. Network Monitoring System merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan performance infrastruktur informasi.
5. System Information and Event Management merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. Network Security Assessment merupakan elemen cyber-security yang berperan sebagai mekanisme kontrol dan memberikan measurement level keamanan informasi.
7. Human resource dan security awareness berkaitan dengan sumber daya manusia dan awareness- nya pada keamanan informasi.

Selain cyber-security kelangsungan operasi informasi juga bergantung pada physical security yang tentunya berkaitan dengan semua elemen fisikal misalnya bangunan data center, disaster recovery system, dan media transmisi.

METODE

Jenis penelitian yang penulis pergunakan dalam penyusunan penulisan hukum ini adalah penelitian hukum yuridis normatif atau kepustakaan, yaitu penelitian hukum yang dilakukan dengan cara meneliti bahan pustakaatau data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan- bahan tersebut disusun secara sistematis, dikaji, kemudian ditarik suatu kesimpulan dalam hubungannya dengan masalah yang diteliti. Penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka, dapat dinamakan penelitian hukum normatif atau penelitian hukum kepustakaan.

Dengan menggunakan jenis penelitian yuridis normatif, pendekatan penelitian yang digunakan adalah Pendekatan perundang-undangan (statute approach) yaitu pendekatan penelitian yang dilakukan dengan cara menelaah undang-undang dan regulasi yang berkaitan dengan isu hukum yang diteliti. Dan Pendekatan Kaus (Case Approach)yaitu pendekatan penelitian yang dilakukan dengan cara menelaah kasus- kasus yang terkait dengan isu hukum yang dihadapi dan telah memperoleh putusan yang mempunyai kekuatan hukum tetap (incracht).

Bahan hukum diperoleh dalam penelitian ini dengan cara studi kepustakaan, Teknik penelusuran bahan hukum berupa literatur atau buku diperoleh dengan cara membuat daftar buku yang akan dicari, kemudian penulis menelusuri buku di Perpustakaan Universitas Wijaya Kusuma dan Perpustakaan Kota Mojokerto. Bahan hukum berupa Undang-Undang, Putusan, artikel ilmiah diperoleh dari website yang terkait dengan Pembaharuan Hukum Pidana Positif.

PEMBAHASAN

Penegrtian Cyber Crime

Dalam beberapa literatur, cybercrime sering diidentikkan sebagai computer crime. The U.S. Department of Justice memberikan pengertian com- puter crime sebagai:"…any illegal act requiring knowledge of computer technology for its perpe- tration, investigation, or prosecution". Pengertian lainnya diberikan oleh Organization of European Community Development, yaitu: "any illegal, un- ethical or unauthorized behavior relating to the automatic processing and/or the transmission of data". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan computer crime sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, computer crime didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang cyber melalui internet, muncul istilah cybercrime.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (virtual) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau cybercrime membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (victim) dan kerugian moril dan materil akibat cybercrime. Korbannya dapat berupa netizen (penduduk dunia virtual/penghuni cyberspace) dan masyarakat luas yang awam.

Karakertsitik dan Jenis Cyber Crime

Cybercrime 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 (cyberspace), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan 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
5. Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

Beberpa kejahatan dalam cybercrime

1. *Illegal acces/unauthorized access to computer system and service*

   Ini adalah bentuk kejahatan yang dilakukan dengan cara meretas/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, atau tanpa izin dari pemilik sistem jaringan komputer yang dimasukinya.
2. *Illegal contents*

   Memasukkan data atau informasi tentang hal yang tidak benar, tidak etis, serta dapat dianggap melanggar hukum atau mengganggu ketertiban umum kedalam internet, itu adalah suatu modus kejahatan *cybercrime* ini.
3. *Data forgery*

   Ini merupakan modus kriminal di dunia maya yang dilakukan dengan memalsukan data dokumen penting yang disimpan sebagai dokumen tanpa kertas melalui internet. Kejahatan sejenis ini biasanya menargetkan dokumen *e-commerce*, seolah-olah ada

"*typo*" yang pada akhirnya akan menguntungkan pelaku, karena korban akan memasukkan data pribadi dan nomor kartu kredit kepada pelaku.

4. *Cyber espionage*
   Ini ialah bentuk kejahatan yang memakai jaringan internet dengan cara memasuki sistem jaringan komputer pihak yang akan ditargetkan menjadi sasaran untuk dimata-matai.
5. *Cyber sabotage and extortion* (sabotase dan pemerasan dunia maya)
   Dalam jenis kejahatan ini, modus biasanya dijalankan dengan mengganggu, merusak, atau menghancurkan data yang terhubung ke internet, program komputer, atau sistem jaringan komputer. Biasanya kejahatan semacam ini dilakukan dengan cara memasukkan *logic bomb*, virus komputer atau program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan dan tidak dapat beroperasi secara normal atau tidak dapat berjalan, tetapi telah dikendalikan oleh penjahat sesuai kebutuhan.
6. *Offense against intellectual property* (pelanggaran terhadap Hak atas Kekayaan Intelektual)
   Modus operandi kejahatan ini adalah menyasar hak kekayaan intelektual yang dimiliki pihak lain di Internet. Misalnya, meniru tampilan website orang lain secara ilegal.
7. *Infringements of privacy*
   Jenis kejahatan ini rata-rata menargetkan informasi pribadi yang disimpan dalam formulir data pribadi yang tersimpan secara computerized, apabila orang lain mengetahuinya, hal itu dapat menyebabkan kerugian terhadap korban secara *materiil* maupun *immaterial*, seperti bocornya nomor PIN ATM, dan lainnya.

Kepastian Hukum dalam Kajian Cyber Crime

Kerangka hukum *cyber-security* di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar UU Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta surat edaran menteri dan peraturan menteri. Secara nasional, terdapat sejumlah permasalah terkait dengan pembangunan *cyber-security* yang tangguh di antaranya lemahnya pemahaman penyelenggara negara atan *security* terkait dengan dunia *cyber* yang memerlukan pembatasan pengunaan layanan yang *server*nya berada di luar negeri dan diperlukan adanya pengunaan *secured system*; belum adanya legalitas yang memadai terhadap penanganan penyerangan di dunia *cyber;* tata kelola kelembagaan *cyber-security* secara nasional yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber-security;* masih lemahnya industri kita dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi.

Pengaturan dan penataan kelembagan *cyber-security* nasional yang kuat merupakan salah satu prasyarat terwujudnya *cyber-security* yang handal. penangganan *cyber-security* harus terintegrasi secara kuat dan melibatkan berbagai lembaga terkait yaitu intelejen, penegak hukum, pertahanan dan keamanan baik itu kementerian pertahanan maupun TNI serta pemerintah sebagai regulator yang dalam hal ini diwakili oleh Kominfo dan ISSIRTI serta Lembaga Sandi Negara.

Tantangan dalam Kehidupan Bermasyarakat dalam Bernegara

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaanteknologi oleh negara berkembang seperti Indo- nesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per- *sonal Computer* (PC), dan ponsel. Sungguh ironismemang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malay sia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasisteknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan untuk menggunakan teknologi komunikasi di In- donesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di In donesia marak sekali kejahatan cyber. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para hacker hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, corporate software, com- puter server, Harley Davidson, hingga senjata M- 16 (Warta Ekonomi.com, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah carding. Para carder (hacker hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, Notebook bermerk Sony seharga 20 Juta yang dipesan melalui carding, dijual seharga 4 Juta ru- piah. Untuk yang satu ini, ClearCommerce, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (Koran Tempo, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam cybercrime jenis carding di Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel Nokia Communicator yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Agar tidak diketahui identitasnya, ia melakukan carding di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk cybercrimejenis carding.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar di sekeliling kita terdapat kejahatan yang “inno- cent”, seolah tanpa dosa dan begitu halus.

Karenanya, pengembangan strategi nasional dalam membangun cyber-security di Indonesia ke depan dilakukan dengan memenuhi empat pondasi yang mendukung perkembangan teknologi pengembangan perangkat lunak (software) seperti sistem dan aplikasi dan perkembangan alat keras (hardware) perkembangan sarana dan prasarana teknologi informasi, manajemen isi (content management), telecommunication and networking, perkembangan internet serta perdagangan online atau melalui internet.

Mengingat pesatnya perkembangan teknologi maka pengelolaan sumber daya cyber security haruslah ditempatkan sebagai proses manajemen bisnis. Hal ini diperlukan karena penangganan cyber-security bukanlah sesuatu yang murah dan mengalami perkembangan yang sangat pesat. Pengembangan kapasitas infrastruktur dengan ditempatkan sebagai proses manajemen bisnis maka potensi kerugian atau biaya yang harus dikeluarkan karena perkembangan teknologi dapat dikurangi.

Demikian pula dengan pengembangan kapasitas SDM yang bergerak di bidang

cybersecurity. Dengan dikelolanya SDM cyber-security dengan manajemen bisnis maka diharapkan akan mampu mempercepat terpenuhinya kebutuhan SDM yang menguasai bidang cybersecurity.

Indonesia saat ini tengah dalam keadaan mendesak cyber-security atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau cyber crime di Indonesia sudah mencapai tahap memprihatinkan. Salah satu fakta yang menunjukkan cyber crime di Indonesia sudah mengkhawatirkan adalah data CIA yang menyebutkan kerugian yang disebabkan karena tindak kejahatan dengan memanfaatkan maupun di dunia cyber di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat cyber crime yang terjadi di dunia.

Pencegahan dan Penanggulangan Cyber Crime

Tindak pidana cybercrime memakan korban dengan jumlah sangat besar, terutama dari segi finansial. Kebanyakan dari korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman mereka saat ini, dan yang perlu dilakukan sekarang adalah mencegah kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan tersebut dapat berupa:

1. *Educate user* (memberikan pengetahuan baru tentang *Cyber Crime* dan dunia internet)
2. *Use hacker's perspective* (menggunakan pemikiran hacker untuk melindungi sistem anda)
3. *Patch system* (menutup lubang-lubang kelemahan pada sistem)
4. *Policy* (menetapkan kebijakan dan aturan untuk melindungi sistem Anda dari orang-orang yang tidak berwenang)
5. *IDS* (Intrusion Detection System) *bundled with IPS* (Intrusion Prevention System)
6. *Firewall*.
7. *AntiVirus*.

Beberapa langkah penting yang harus diambil dalam menanggapi Cybercrime adalah :

1. Melakukan pembaruan hukum pidana nasional dan hukum acara, sesuai dengan kesepakatan internasional yang terkait dengan kejahatan tersebut.
2. Meningkatkan sistem keamanan jaringan komputer nasional sesuai dengan standar internasional.
3. Meningkatkan pengetahuan dan keahlian aparat penegak hukum dalam upaya pencegahan, investigasi, dan penuntutan kasus-kasus yang berkaitan dengan cybercrime.
4. Meningkatkan kesadaran warga negara tentang masalah cybercrime dan pentingnya mencegah kejahatan itu terjadi.
5. Meningkatkan kerjasama dari berbagai negara, baik kerja sama bilateral, regional maupun multilateral dalam upaya mengatasi cybercrime, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan timbal balik (mutual assistance treaties).

SIMPULAN

Demi mewujudkan kondisi kedamaian serta keamanan dalam aktifitas bermasyarakat dan bernegara, negara harus hadir dalam segala bentuk tindakannya. Dengan hal demikian maka negara menjadi pertahanan utama dan pertama untuk mengendalikan kegiatan atau aktifitas dalam kehidupan masyarakat dan bernegara.

Perlunya langkah taktis yang di ambil oleh segala elemen yang ada dalam masyarakat guna meningkatkan kualitas sumber daya manusia yang lebih baik, sehingga akan menjadi nilai yang akan trerus di pakai, maksudnya nilai yang akan menjadikan kebudayaan dalam era teknologi informasi yang akan berkembang sampai waktu yang tidak bisa ditentukan.

DAFTAR PUSTAKA

Anne W. Brascomb (ed), *Toward A Law of Global Communication Network*, New York: Lognman, 1986.

Agung Banyu Perwita & Yanyan Moch Yani, *Pengantar Ilmu Hubungan Internasional*, (Bandung: Rosda, 2005).

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), *Kajian Konvergensi Teknologi Informasi dan Komunikasi*, Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007.

Ronald Thompson & William Cats Barril, *Information Technology and Management,* New York: Mc Graw Hill, 2003.

Indonesian Defense University, *Technology Perscpetive: National Cyber Security*, http://binkorpspelaut.tnial.mil.id/index.php?option=com_docman&task=doc_download&gid=6&Itemid=22. diakses 14 April 2023.

Yuni Fitriani dan Roida Pakpahan, "*Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace*," Cakrawala: Jurnal Humaniora 20, no. 1 (Maret 2020).

Ade Arie Sam Indradi, *Carding: Modus Operandi, Penyidikan dan Penindakan* (Jakarta: Grafika Indah, 2006).

Dista Amalia Arifah, "*Kasus Cybercrime di Indonesia*," *Jurnal Bisnis dan Ekonomi (JBE)* 18, no. 2 (September 2011).

.