JURNAL MANAJEMEN AKUNTANSI (JUMSI)
Vol. 1, No. 3 Juli 2021 Page 13-20
E-ISSN : 2774-4221

Lingkup Dan Jaringan Kerjasama Di Dunia Cyber

[1]Suci Arifah Lubis, [2]Adrie Fachrezi Harahap, [3]Nurbaiti

[1]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, suciarifah015@gmail.com
[2]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, adriefachreziharahap2001@gmail.com
[3]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, nurbaiti@uinsu.ac.id

ABSTRACT

Technology can be said to be a gift but if cn also be said to be a thret to its users. For ecample the virtul world and the internet, cyberspace or the internet can connect millions of peopple in variouse communications from various places. The internet is certainly very flower among people and the internet has also been recognized as very useful and supports almost every area of lifeIndonesia makes ASEAN countries to implement the proposals. Cybercrime is a matter of widespread concern in ASEAN. ASEAN is an association that works for the monetary progress of countries in Southeast Asia. These countries consist of Myanmar, Thailand, Laos, Cambodia, Vietnam, Malaysia, Singapore, Indonesia, Brunei, and the Philippines. In 2015, the ASEAN Community was established in three columns joining the ASEAN states. The main column is the ASEAN Political and Security Community, the next column is the ASEAN Economic Community, and the third column is the ASEAN Social and Cultural Community.

Keywords: *Technology Cyber, ASEAN*

PENDAHULUAN

Ancaman Cyber ini sangat terikat dengan teknologi dari komputer dan internet pastinya. Perkembangan teknologi komputer dan internet ini telah membuat dampak yang sangat besar. Maka dari itu setiap aktifitas yang ada slalu diawasi. Internetpun telah mempermudah kehidupan manusia karena segala informasi dapat diakses dengan sangat mudah. Karena dari internet mudah mengakses apa saja serangan cyber pun muncul. Terdapat banyak bahaya-bahaya yang ditimbulkan dari serangan cyber tersebut.

Ancaman dan kejahatan-kejahatan yang terdapat di dunia cyber ini membuat isu-isu yang sangat menyedihkan bagi setiap pengguna komputer. ASEAN adalah organisasi yang membangun kemajuan ekonomi negara-negara yang berada Di Asia Tenggara. Negara tersebut mencakup Myanmar, Thailand, Laos, Kamboha, Vietnam, Malaysia, Singapura, Indonesia, Brunei Dan Filiphina. ASEAN mempunyai komunitas yang didirikan untuk menyatukan negara-negara anggota ASEAN itu sendiri. Perkembangan dari cyber ASEAN sekarang hanya fokus pada sektor militer saja tidak terlalu memprihatinkan pada sektor publik. Ancaman dan kejahatan cyber ini merupakan kejahatan yang melibatkan langsung komputer dan jaringan (Network).

Penyelenggaraan keamanan dan kekuatan jaringan di Indonesia saat ini memiliki kerangka dan sistem yang dilengkapi oleh organisasi pemerintah dan otoritas daerah setempat. Strategi keamanan dan fleksibilitas digital telah disusun oleh Kementerian Komunikasi dan Informatika. Dalam kerangka dan prosedur perlindungan dan kekuatan digital, terdapat tiga asosiasi pemerintah yang bergerak di bidang keamanan dan fleksibilitas jaringan di Indonesia, khususnya Tim Koordinasi Keamanan Informasi, Direktorat Keamanan Informasi, dan Tim Tanggap Insiden Keamanan Indonesia pada Infrastruktur Internet.

Dengan demikian, selain pekerjaan publik, partisipasi global juga diharapkan dapat membantu terlaksananya keamanan dan fleksibilitas jaringan dengan baik. Partisipasi global adalah hubungan yang diselesaikan oleh suatu negara dengan negara yang berbeda yang berencana untuk mengatasi masalah individu dan untuk kepentingan negara-negara di planet ini. Partisipasi global, yang diarahkan oleh strategi internasional, mengingat kolaborasi untuk bidang masalah pemerintahan, sosial, perlindungan dan keamanan, budaya dan ekonomi.

Hingga saat ini, tugas kolaborasi dunia masih dilakukan oleh daerah, baik oleh organisasi, jaringan , dan zat sesuai dengan kapasitasnya. . Mereka membawa partisipasi ini melalui bergabung dengan afiliasi global. Salah satu sistem koalisi Indonesia dalam strategi perlindungan dan kekuatan jaringan adalah melalui pelaksanaan kerjasama dengan ASEAN untuk mengelola keamanan dan keserbagunaan jaringan.

Tujuan dari keamanan dan kekuatan jaringan adalah untuk mengamankan, mengatur, dan mengontrol informasi dan data. Perlindungan dan keserbagunaan jaringan publik terkait erat dengan tugas-tugas data termasuk berbagai kelompok, misalnya, militer, pemerintah, perusahaan yang diklaim negara, organisasi, dunia ilmiah, area pribadi, orang-orang, dan area lokal di seluruh dunia. Koherensi tugas data tidak hanya bergantung pada keamanan dunia digital itu sendiri. Ini juga bergantung pada keamanan aktual yang terkait dengan semua komponen aktual, seperti struktur Data Center, kerangka kerja pemulihan bencana, dan media transmisi.

Cyber crimes dapat dikatakan sebagai pelanggaran kejahatan yang dilakukan seorang atau sekelompok individu dengan motif kriminal dengan secara sengaja menyakiti korban yang menyebabkan kerugian fisik atau mentalnya dapat dikatakan juga sebagai kerugin yang baik secara langsung ataupun tidak langsung. Disebut dengan sektor jumlah komputer yang paling besar.

Bagaimana analisis kerjasama multilateral ASEAN mengatasi dalam mengatasi masalah ancaman yang terjadi di dunia cyber. Ancaman kejahatan dari cyber ini harus diantisipasi demgan menggunakan keamanan cyber disebut dengan cyber security, cyber security adalah aktifitas pengukuran maksudnya untuk melindungi serangan atau ancaman tersebut.Data-data dari penelitian ini didapatkan dengan membaca dan mempelajari referensi yang berkaitan dengan judul penelitian yang dilakukan .Alat yang digunakan dalam penelitian ini adalah: Seperangkat komputer dengan sistem operasi Microsoft Windows 7.

Objek penelitian ini bagaimana analisis kerjasama multilateral ASEAN mengatasi dalam mengatasi masalah ancaman yang terjadi di dunia cyber. Ancaman-ancaman dan kejahatan tersebut perlu diantisipasi, Salah satunya melalui Kemanan siber atau cyber security. Keamanan Siber atau cybersecurity dapat dikatakan sebagai sebuah rangkaian aktifitas ataupun pengukuran yang dimaksudkan untuk melindungi dari disrupsi, serangan, atau ancaman yang lainnya melalui elemen-elemen cyberspace baik software, hardware, computer network.

LANDASAN TEORI

Penanganan Insiden

Penanganan insiden merupakan seperangkat prosedur yang dilakukan untuk mengatasi berbagai jenis insiden serangan yang disebabkan oleh berbagai kerentanan. Banyaknya insiden serangan yang terjadi baik disengaja maupun tidak disengaja oleh orang yang tidak bertanggung jawab dalam memanfaatkan teknologi. Membuat instansi yang mengalami insiden serangan membentuk tim khusus yang bertujuan untuk menangani insiden serangan tersebut. Tim tersebut dibentuk untuk membantu menangani insiden seperti: mendeteksi, memantau, dan memberikan peringatan sebelum insiden serangan terjadi..

Pencegahan Insiden

Pencegahan Insiden adalah tindakan yang dilakukan secara sengaja untuk mencegah terjadinya kerusakan, dan gangguan kerusakan sebelum insiden serangan terjadi. Menurut Kamus Besar Bahasa Indonesia (2007), pencegahan adalah suatu proses, cara, tindakan mencegah atau tindakan menahan agar sesuatu tidak terjadi. Yunita (dalam L.Abate, 1990:10) definisi pencegahan (prevention) adalah pencegahan yang terdiri dari berbagai pendekatan, prosedur dan metode yang dibuat untuk meningkatkan kompetensi interpersonal seseorang dan fungsinya sebagai individu, pasangan, dan sebagai orang tua.

METODE PENELITIAN

Metode penelitian ini kami menggunakan metode kualitatif , metode kualitatif yang kami gunakan ini pengumpulan data dengan berbagai macam alat dan teknik-teknik untuk mencari informasi-informasi mengenai bagaimana mencegah agar tidak terjadinya ancaman-ancaman di dunia cyber. Kemudian dirangkum menjadi satu sehingga memudahkan bagi pembaca memahami fenomena tentang apa yang dialami oleh subjek penelitian. Penelitian kualitatif merupakan penelitian yang bersifat alamiah dan data yang dihasilkan berupa deskriptif. Pada penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian studi kasus. Penelitian ini memusatkan diri secara intensif pada satu obyek tertentu yang mempelajarinya sebagai suatu kasus. Data studi kasus dapat diperoleh dari semua pihak yang bersangkutan.ASEAN sendiri adalah salah satu negara berkembang tercepat di planet ini dengan populasi 634 juta orang (100 juta lebih banyak dari Uni Eropa). Hal ini menjadikan ASEAN pasar terpadat ketiga di planet ini dan dengan Produk Domestik Bruto (PDB) terkonsolidasi lebih dari $2,55 triliun, menjadikan ASEAN ekonomi terbesar ketujuh di planet ini. Sebuah konsentrat oleh ATKearney menunjukkan bahwa ekonomi maju dapat menambah 1 triliun USD.23 Namun, "Ekonomi Terkomputerisasi" yang sangat bergantung pada inovasi untuk kesepakatan membuka jalan baru untuk bahaya kejahatan dunia maya, seperti pemerasan berbasis internet, peretasan, dan penyebaran materi yang tidak pantas yang menjadikan keselamatan publik dan keamanan fondasi data diperlukan.

HASIL DAN PEMBAHASAN

Pembahasan

Bidang, aspek dari kehidupan negara ini mengalami berbagai perubahan dan pengembangan. Hal ini disama kan dengan semakin majunya perkembangan dunia yang ada maka semakin canggihan juga teknologi-teknologi. Tetapi, Dibelakang bersinarnya teknologi yang dapat memberikan kita akses ke seluruh penjuru dunia pasti ada sisi gelap nya, sisi gelap tersebut.

Sosial Media sekarang sangat banyak digemari kaum muda, karena mudah saling berinteraksi secara online, pendidikan, pembangunan ekonomi, Dan lain-lain dapat dikatakan bentuk yang nyata dari manfaat keberadaan dunia maya dan internet ini. Tetapi tidak dapat dibayangkan bahwa adanya teknologi inilah yang akan membawa dampak dari berbagai kejahatan-kejahatan yang ada didunia Cyber.Cyberspace ini adalah ruang yang dimana komunitas dapat saling menghubungkan melalui suatu jaringan contohnya seperti internet untuk mencari informasi. Cyberspace ini sebuah dunia komunikasi melalui komputer bisa dikatakan unik karna perkembangan pada setiap bidang akan membawa perubahan atau dampak yang sangat besar. Kemudahan dalam mengakses pada kecanggihan dari teknologi seperti internet ini mengajak pelaku yang tidak bertanggung jawab akan memanfaatkan pelaku cyber. Para pelaku cyber dapat melakukan tindakan yang dapat melanggar hukum. Hal ini pastinya akan berdampak pada kerugian yang ditanggung oleh orang lain. Tindakan itu memicu kejahatan yang berbeda-beda dari tindakan kejahatan yang ada. Kejahatan cyber ini yang di sebut cybercrime yaitu kejahatan dunia maya.

Semakin meningkatnya kegiatan dunia maya akan membuat kejahatan nasional yang berbasis cyber semakin merajalela. Data-data dan informasi yang menjadi sasaran karena, mengakibatkan serangan cyber : penyalahgunaan informasi, pengendalian sistem, kerusuhan, kekerasan, ketakutan, konflik sampai kekacauan dan masih banyak kerugian-kerugian yang daoat disebabkan agar berdampak pada kehancuran. Ancaman dunia Cuber ini sangat berbahaya karna mengintai seluruh dunia setiap celah akan dimanfaatkan untuk berbuat kejahatan. Kejahatan cyber meniliki bentuk dan jenis yang berbeda. Cybersecurity dapat dicirikan sebagai upaya yang dilakukan oleh orang-orang atau pertemuan, secara mandiri atau semua hal dipertimbangkan, untuk bergerak atau berusaha untuk memastikan, mengharapkan atau mempengaruhi terkait digital. Fungsi dari keamanan Siber sendiri dapat dijabarkan sebagai berikut :

1. Mewujudkan energi kooperatif dengan strategi pengamanan digital
2. Membangun asosiasi dan administrasi keamanan TI kerangka eksekutif
3. Membuat kerangka kerja yang menjamin aksesibilitas data di bidang pengamanan digital.
4. Membangun kerangka kerja untuk mencegah, mendakwa, dan memulihkan diri dariserangan digital.
5. Peningkatan kesadaran keamanan jaringan
6. Keamanan kerangka data dalam pengamanan
7. Menyelesaikan latihan kerja inovatif untuk membantu pergantian acara dan peningkatan kapasitas penjaga digital
8. Penataan partisipasi publik dan global untuk pergantian acara dan peningkatan kemampuangarda digital.

Proteksi jaringan atau proteksi digital sangat penting untuk diwaspadai dan mengantisipasi bahaya yang datang dari internet. Keamanan jaringan harus menjadi sistem biologis di mana hukum, asosiasi, kemampuan, kolaborasi, dan pelaksanaan khusus bekerja secara damai. menjadi produktif. Dilihat dari kekompakan anggota dan usaha bersama yang telah dicapai, cenderung ada 3 kemungkinan sebagai berikut:

1. Investment in the habit of dialog and cooperation. Bagi Indonesia, pertemuan ini merupakan diskusi untuk mendorong budaya wacana dan kolaborasi dalam mengelola kontras atau bentrokan di lokal. Indonesia juga menegaskan bahwa penggunaan kekuasaan atau bahaya penggunaan kekuasaan bukanlah pilihan untuk menentukan persoalan antar bangsa.
2. Early Warning System. Jadikan pertemuan ini sebagai kerangka peringatan awal untukmunculnya keamanan yang memerlukan pertimbangan tambahan dari pemerintah Indonesia.
3. Test The Water. Menjadikan Forum ini sebagai pintu terbuka terhadap data standarmengingat kepedulian yang sah bagi Negara Kesatuan Republik Indonesia yang belum berubah menjadi posisi khawatir untuk mendesak Peserta ARF lainnya untuk turut serta menjaga data tersebut.

Dengan pengembangan keamanan jaringan melalui upaya bersama di seluruh dunia atau pemanfaatan asosiasi global (ASEAN) sebagai pertemuan, Indonesia telah menunjukkan tanggung jawabnya dan menunjukkan kemampuan negara untuk menangani masalah. Partisipasi ini juga merupakan salah satu cara untuk berkontribusi atau menambah perhatian dan dukungan dunia. Oleh karena itu, upaya untuk membentengi proteksi digital tidak dapat dilawan oleh satu negara. Dukungan, partisipasi, dan keramahan yang berbeda dari pertemuan yang berbeda diperlukan untuk kemajuan perlindungan jaringan. Pemerintah Indonesia sangat menyadari kemungkinan bahwa perlindungan online ekologis tidak dapat dilakukan sendiri, tetapi sebaiknya dilakukan bersama-sama. Melihat gagasan ini, Indonesia

telah mengajukan upaya untuk membantu negara-negara dan asosiasi global. Sebuah model adalah kepentingan diskusi ASEAN Re di tingkat lokal atau provinsi. Dalam diskusi multilateral seperti ARF, Indonesia menggunakan diskresi sebagai aparatur untuk mencapai kepentingan publik dan sekaligus menjalin hubungan baik dengan berbagai negara. Indonesia tahu bahwa keadaan luar dan keamanan di dalam negeri dapat mempengaruhi keselamatan publiknya. Oleh karena itu, dengan kebijaksanaan ini, Indonesia dapat memastikan domainnya dan melakukan keamanan di distrik tersebut. Atas pertimbangannya sendiri, Indonesia memulai beberapa hal dalam diskusi ARF.

Hasil

Sebelum menguraikan manfaat yang dapat diperoleh ASEAN, perlu dicermati terlebih dahulu mengapa ASEAN adalah distrik yang tidak berdaya melawan bahaya digital. Ada beberapa penjelasan di balik kelemahan ini; pertama, sebagian besar klien Internet dunia adalah kelompok masyarakat ASEAN. Saat ini, dari 2,1 miliar klien web, 922 juta klien berasal dari kawasan ASEAN dan diperkirakan jumlah ini akan terus bertambah setiap tahunnya tahun. Kedua, ASEAN adalah asosiasi teritorial terbesar di Asia Pasifik, yang berarti Kolaborasi keuangan dan pasar juga besar di sini, sebagian besar komunikasi monetersaat ini terjadi di dunia digital yang juga signifikan untuk kawasan ASEAN, sampai batas tertentu Sebagian besar kerja sama moneter digital ada di ASEAN.

Selain itu, seperti yang ditunjukkan oleh Heinl ASEAN merupakan daerah berkreasi. Banyak kerangka kerja yang dibangun dengan kerangka kerja TIK, misalnya, organisasi transportasi, pertambangan, energi, perbankan dan meningkatkan inklusi dan ruang organisasi ponsel ke wilayahterpencil. terlepas. Sebagian dari kenyataan tersebut menunjukkan bahwa ASEAN merupakan kawasan dengan koneksi digital tinggi. Ketersediaan yang diperluas di internet dan ketergantungan pada digital juga berkembang peluang terjadinya kejahatan transnasional berbasis digital. Salah satu bahaya digital yang umumnya dialami oleh negara-negara di ASEAN mulai sekitar tahun 2012 – 2013 seperti yang ditunjukkan oleh Heinl adalah serangan terhadap situs web pemerintah. Menurut dia, meskipun beberapa Negara-negara ASEAN adalah negara-negara yang masih berkembang, namun tidak luput dari serangan dan bahaya digital yang telah ditunjukkan oleh semua negara di ASEAN telah rasakan serangan di situs web administrasi mereka.

Untuk mengelola bahaya digital di ASEAN, pada tingkat masing-masing dan teritorial, telah banyak Kegiatan yang dilakukan oleh ASEAN antara lain, ASEAN ICT Masterplan 2015, The ASEAN Program Kapasitas Digital, Deklarasi Mactan Cebu Menghubungkan ASEAN: EnableAspirations dan laporan yang berbeda. Meskipun demikian, sampai saat ini kegiatan yang dilakukan oleh ASEAN dalam menangani bahaya digital masih sebatas melegitimasi arsip dan perluasan partisipasi dalam implementasi hukum. ASEAN sebenarnya membutuhkan upaya yang lebih lengkap dan upaya yang lebih substansial dalam mengelola bahaya internet dikontraskan dengan hanya membuat dokumen. Sebagai wilayah yang sangat besar dengan kolaborasi digital yang tinggi, ada beberapaisu-isu digital yang penting untuk dipertimbangkan oleh ASEAN untuk mencapai inkorporasi keamanan jaringan yang lebih baik. Untuk memulainya, ASEAN belum memiliki peringkat dan kebutuhan kelemahan area kerangka kerja di setiap negara. Sampai saat ini, negara-negara ASEAN masih asyik dengan kekhasan digital yang merupakan kekhasan yang merepresentasikan bahaya sekaligus memiliki manfaat, namun ASEAN sebenarnya tidak memiliki kesadaran akan bahaya dan di daerah mana bahaya akan terjadi. Signifikan untuk masing-masing negara-negara di ASEAN untuk menentukan peringkat dan fokus pada kelemahan daerahkerangka kerja. Ini berguna untuk mengikuti pemeliharaan pergantian peristiwa yang ekonomis diselesaikan oleh ASEAN.

ASEAN mencatat tentang bahayadigital masih dipertanyakan dan sulit dijangkau. Catatan belum dibuat menggambarkan pengaturan pragmatis yang harus diambil ASEAN ketika bahaya muncul kerabat. Dengan cara ini, catatan yang disampaikan oleh ASEAN dalam hal digital masih terbatas penggambaran umum digital dan tayangan hanya sebagai jenis perhatian semu ASEAN tampaknya memiliki kesadaran yang sama dengan yayasan teritorial lainnya. Kekurangan kegiatan ASEAN sedemikian rupa membuat sistem yang seharusnya dilakukan oleh ASEAN saat menghadapi ancaman atau serangan digital karena tidak ada unit kerja yang jelas dan strategi yang harus diambil jika terjadi serangan juga sebagai metode untuk meningkatkan keamanan jaringan ASEAN. Isu selajutnya adalah bahwa ASEAN tidak berusaha membangun kesadaran akan bahaya masyarakat digital. Memang, siapa klien digital terbesar di ASEAN adalah masyarakat yang sopan, bukan militer atau pemerintah. Bagaimanapun, berusahalah untuk Penanggulangan digital yang dianut oleh ASEAN hingga saat ini telah memusatkan perhatian pada tambahan pemerintah dan militer. Ini harus terlihat dari laporan yang dibuat oleh ASEAN memiliki administrasi objektif dari negara-negara yang bergabung dengan ASEAN, Selain itu dengan penguatan digital yang lebih berpusat pada kekuatan militer, misalnya, kolaborasi antara India dan Vietnam dalam pengembangan pusat penelitian hukum yang maju di Vietnam, memperluas kemampuan pengamanan digital oleh Singapura dan Brunei Darussalam pada militer. Keempat, perluasan kapasitas penanggulangan digital ASEAN difokuskan pada militer. Memperluas kemampuan penjaga dan penyerangan digital militer adalah salah satunya salah satu upaya yang diperlukan dalam perlindungan jaringan. Meskipun demikian, serangan digital lebih berpusat di sekitar area publik, bukan sektor militer. dengan demikian, daerah publik lebih tidak berdaya dan membutuhkan kekuatan yang diperluas dalam kaitannya dengan peningkatan keamanan jaringan di militer. Pekerjaan ini belum dilakukan cukup besar oleh distrik ASEAN, sehingga cenderung terlihat bahwa sebagian besar serangan digital di ASEAN memusatkan perhatian pada area publik, misalnya, otoritas publik situs, penyebaran infeksi di ponsel dan computer. pengawasan dan perampokan cadangan perbankan mulai daridana investasi individu dan perkembangan berbagai jenis serangan publik. Selain itu, padaserangan digital tidak dapat ditegaskan apakah serangan itu dari militer atau masyarakat umum, tetapitujuan penyerangan benar-benar bisa lebih ke area publik. Masalah inimenyatakan bahwa militer tidak dapat dengan cepat melakukan serangan balikselanjutnya melakukan metodologi militer dalam kaitannya dengan serangan digital.Isu terakhir yang dialami ASEAN di bidang digital adalah ketimpangankapasitas negara-negara di ASEAN, beberapa negara di ASEAN adalahdengan inovasi trend setting dan telah tumbuh merata di seluruh wilayah tanah air,sementara beberapa kawasan ASEAN lainnya sebenarnya memiliki inovasi yang mendasar dan mendalamupaya kemajuan inovasi dan peningkatan area TIK untuk kerangka kerjasignifikan dan belum mengalami peredaran yang setara di seluruh tanah air. PerbedaanKondisi saat ini membuat tidak semua negara di ASEAN mewaspadai bahaya digitalsama, karena bahaya yang dirasakan oleh satu negara sebenarnya tidak berbahaya bagi lainnya karena bangsa tersebut belum memiliki inovasi komparatif atau masih dalam waktu yang lama kemajuan. Ini juga mempersulit ASEAN untuk membangun struktur pekerjaan yang jelas yang dapat diselesaikan oleh semua bangsa.

Hasilnya akan menunjukkan alasan di balik Indonesia Forum Regional ASEAN, karena keamanan siber Indonesia masih ada banyak celah, dan kepentingan nasional ada dalam bentuk kebutuhan keamanan Mutlak dan ancaman dari dunia maya. Saat melakukan kegiatan diplomatik Indonesia mengedepankan poin-poin khusus, yaitu : adanya kontak membentuk kelompok-kelompok untuk pengembangan kurikulum agar dapat meningkatkan kemampuan didirikan melihat penggunaan internet dan badan utamanya dibentuk atau lembaga khusus jaringan negaranya masing-masing. Indonesiapun mengusulkan agar negara ASEAN Mengirim proposal tersebut. Dua poin tersebut yang dikemukakan ASEAN Regional

Forum agar menjaga keamanan, keselamatan teknologi informasi dan komunikasi dari ancaman cyber.

KESIMPULAN

Mengingat internet juga bisa menjadi lubang untuk berbagai kesalahan yang bisamendapatkan keamanan dan keselamatan publik negara. Upaya keamanan diharapkan dapatmencegah dan mengantisipasi bahaya digital dengan menjaga keselamatan publik suatunegara. Keamanan publik suatu bangsa adalah kepentingan publik yang datar. Andabenar-benar ingin memiliki iklim yang mendukung persiapan keamanan jaringan. Menjadikesepakatan khusus antara undang-undang, konstruksi hierarkis yang jelas, memperluas batasdan partisipasi khusus dan prosedural. Indonesia memahami bahwa kemajuan keamananjaringan tidak mungkin dilakukan sendiri dan akan lebih layak jika diselesaikan denganIndonesia, yang secara efektif mengambil bagian dalam Forum Regional ASEAN. Padadiskusi yang diadakan pada tahun 2015, Indonesia mengusulkan empat hal. Pertama,Indonesia mendesak negara-negara ASEAN untuk membuat program limit building melaluikonsentrat pada sebuah pertemuan, karena tidak ada proyek atau konvensi khusus untukmengelola bahaya digital teritorial seperti Asia Tenggara. Kedua, meningkatkanpemanfaatan Internet Protocol Version 4 (IPv4) ke Internet Protocol Version 6 (IPv6) sebagaipengaturan yang pragmatis dan sukses dengan tujuan untuk lebih mengembangkan kerangkakeamanan. Ketiga, pemerintah Indonesia juga menyarankan agar setiap negara segeramendirikan kantor atau pendirian yang bertanggung jawab atas keamanan jaringan,mengingat masih banyak negara ASEAN yang belum memiliki kantor atau organisasi yangsecara tegas menangani masalah TI, fokus kontak bagi setiap negara untuk bekerja samadengan pemerintah Indonesia dalam menyelesaikan interaksi damai , baik delapan jeniskebijaksanaan dalam episode digital papan dan di bidang yang berbeda diidentifikasi denganmencapai tujuan bersama. Ada dua tanda yang didapat dalam Rencana Kerja Forum RegionalASEAN tentang Keamanan dan Penggunaan Teknologi Informasi dan Komunikasi Pertama,Indonesia mendesak negara-negara ASEAN untuk menyusun program pembangunan batasmelalui konsentrat pada pertemuan-pertemuan, mengingat adanya tidak ada proyek ataukonvensi khusus untuk mengelola bahaya digital provinsi seperti Asia Tenggara.meningkatkan penggunaan Internet Protocol Version 4 (IPv4) ke Internet Protocol Version 6(IPv6) sebagai pengaturan yang layak dan menarik dengan tujuan untuk lebihmengembangkan kerangka keamanan. Ketiga, pemerintah Indonesia juga menyarankan agarsetiap negara segera membangun kantor atau organisasi yang bertanggung jawab ataskeamanan jaringan, mengingat masih banyak negara ASEAN yang belum memiliki kantoratau lembaga yang secara tegas menangani masalah IT, fokus kontak bagi setiap negara untukbekerja sama dengan pemerintah Indonesia dalam menyelesaikan interaksi politik , baikdelapan jenis kebijaksanaan dalam kejadian digital eksekutif dan di bidang yang berbedadiidentifikasi dengan mencapai tujuan bersama. Ada dua tempat yang didapat di ASEANRegional Forum Work Plan on Security of and in The Use of Information andCommunications Technologies.

DAFTAR PUSTAKA

Fischer, E. A. 2009. Creating a National Framework for Cybersecurity: an Analysis of Issues and Options. New York: Nova Science Publishers, Inc.

Heywood, Andrew. 2011. Global Politics. New York: Palgrave Macmillan

Holsti, K. J. 1998. Politik Internasional: suatu kerangka Analisis Jilid I. Jakarta: ErlanggaID-SIRTII. 2017. Tren Serangan Siber Nasional 2016 dan Prediksi 2017.

ID-SIRTII. ITU. 2017. Global Cybersecurity Index 2017. International Telecommunication Unit.

Jackson, R., & Sorensen, G. 2013. Introduction to International Relations. United Kingdom:Oxford University Press.

KEMENHAN 2014. RI, Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun Tentang Pedoman Siber. Kementrian Pertahanan

Lewis, James Andrew. 2013. Hidden Arena: Cyber Competition and Conflct in Indo-Pacifi Asia. Lowy Institute MacArthur

Richardus Eko Indrajit. 2011. Pengantar konsep keamanan informasi di dunia siber. Aptikom

Samadikun, Samaun. 2000. Pengaruh Perpaduan Teknologi Komputer, Telekomunikasi dan Informasi. Jakarta: Kompas.