ISSN 2580 6378
E-ISSN 2580 7048

JURNAL ASIA PACIFIC STUDIES

Journal of International Relations Study Program
Faculty of Social and Political Sciences
Universitas Kristen Indonesia

Volume I | Number 2 | July - December 2017

Jurnal Asia Pacific Studies
ejournal.uki.ac.id/index.php/japs/article/view/624
Volume 1 Number 2/ July - December 2017
pp. 220-233

BABAK BARU REJIM KEAMANAN SIBER DI ASIA TENGGARA MENYOSONG ASEAN CONNECTIVITY 2025

Indah Novitasari

Ilmu Politik, Fakultas Ilmu Sosial dan Ilmu Politik, Univesitas Kristen Indonesia
Jl. Mayjen Sutoyo No. 2 Cawang, Jakarta

indah.novitasari@uki.ac.id

Abstract

This article discusses the relevance phenomenon of the world community's dependence on the use of cyber space, and the form of cyber security cooperation in Southeast Asia after ASEAN Community 2015. The use of cyber as an implication of information and communication technology progresses not only gives positive impact by shortening the distance, space and time, but in fact negatively impacted by the emergence a new generation of non-traditional threats which called cybercrime. This non-traditional threat appears latent, but has a massive impact on countries in Southeast Asia that have relatively high cyber consumptive levels with low cyber security. This spectrum of non-traditional threats needs to be addressed by efforts to implement a regional cooperation in order to strengthen the civic resilience actively within the global and regional framework. After ASEAN Community 2015, the integration of the region in various fields has also opened the vulnerability of various countries in the region against cybercrime. In facing this threat, ASEAN needs to create a more comprehensive cyber security cooperation framework through cyber security regime in Southeast Asia as an implementation of ASEAN values and norms in realizing the stability of the region. The cyber security regime in Southeast Asia is considered to be a rational choice especially in achieving ASEAN Connectivity in 2025 as an agenda in realizing integration in Southeast Asia

Keywords: Cyber, Cyber Security Cooperation in South East Asia, Cyber Security Regime in South East Asia, ASEAN Connectivity 2025.

Abstrak

Artikel ini merupakan kajian yang membahas keterkaitan fenomena ketergantungan masyarakat dunia terhadap penggunaan ruang Siber, dan bentuk kerjasama Keamanan Siber di kawasan Asia Tenggara pasca berjalannya ASEAN Community tahun 2015. Penggunaan siber sebagai implikasi kemajuan teknologi informasi dan komunikasi, tidak hanya memberikan dampak positif dengan mempersingkat jarak, ruang dan waktu, namun nyatanya memberikan dampak negative dengan munculnya ancaman non-tradisional generasi baru yaitu kejahatan siber. Ancaman non-tradisional ini muncul secara laten, namun berdampak massif bagi negara-negara di Kawasan Asia Tenggara yang memiliki tingkat konsumtif siber relatif tinggi dengan keamanan siber yang rendah. Spektrum ancaman non-tradisional ini kemudian perlu disikapi dengan upaya melaksanakan sebuah kerjasama regional guna memperkuat ketahanan siber yang dilakukan secara aktif dalam kerangka global dan regional. Pasca Komunitas ASEAN 2015, integrasi kawasan dalam berbagai bidang nyatanya juga telah membuka kerentanan berbagai Negara di kawasan terhadap serangan kejahatan siber. Dalam menghadapi ancaman ini, maka ASEAN perlu membuat sebuah kerangka kerjasama keamanan siber yang lebih komprehensif melalui rejim keamanan siber di Asia Tenggara sebagai sebuah implementasi nilai dan norma ASEAN dalam mewujudkan stabilitas kawasan. Rejim Keamanan Siber di Asia Tenggara dinilai menjadi sebuah pilihan rasional terlebih dalam mencapai konektivitas ASEAN tahun 2025 sebagai sebuah agenda dalam mewujudkan integrasi di kawasan Asia Tenggara.

Kata Kunci**:** Siber, Kerjasama Keamanan Siber di Asia Tenggara, Rejim Keamanan Siber di Asia Tenggara, ASEAN Connectivity 2025

1. PENDAHULUAN

Dunia *Siber* atau Siber dinyatakan sebagai dimensi kelima dari kehidupan manusia setelah dimensi darat, air, udara, dan luar angkasa. Dunia ini digambarkan sebagai suatu ruang dimensi yang dibentuk dari dan berkaitan dengan perangkat lunak dan perangkat keras komputer, serta jaringan komunikasi informasi yang bersifat paralel, virtual, dan tidak berdiferensiasi, dimana setiap data yang ada didalamnya bergerak secara dinamis, dan berkelanjutan dari suatu simpul ke simpul lainnya secara *rapid* dan tidak terdeteksi. Saat ini dunia siber kemudian lebih dikenal luas dengan jaringan komunikasi informasi yang menghubungkan miliaran komputer di seluruh dunia atau yang lebih dikenal dengan internet.

Pada tingkat strategis, dunia atau ruang siber muncul sebagai domain militer yang signifikan disamping domain udara, darat, laut sebagaimana dinyatakan diatas. Dengan potensi serangan yang dapat mengganggu maupun merusak aktivitas individu maupun negara, ruang siber disebut-sebut sebagai bentuk baru peperangan yang tidak dapat dihindari karena ketergantungan pemerintah maupun masyarakat pada siber ruang siber untuk kegiatan sehari-hari. Keterhubungan yang ditawarkan oleh siber memberikan dampak positif, yaitu keleluasaan hubungan komunikasi yang tidak mengenal batas ruang dan waktu. Namun demikian, bagaikan dua sisi mata uang, keleluasaan yang diberikan oleh dunia siber juga membawa ancaman tersendiri. Salah satunya adalah serangan siber menjadi salah satu dari isu-isu keamanan non-tradisional yang dapat mengancam kedaulatan Negara yang terjadi dalam berbagai bentuk semisal, sabotase, penyadapan, spionase maupun kejahatan yang sulit untuk terdeteksi namun menyebabkan kerugian besar pada masyarakat maupun Negara pada sector perekonomian nasional dan keamanan internasional.

Bagi Uni Eropa ancaman siber merupakan salah satu ancaman non tradisional, yang menjadi risiko utama terhadap keamanan, stabilitas dan daya saing bagi negara-negara Anggota dan sektor swasta (Parlemen Uni Eropa 2012, 4). James R. Clapper Junior yang mewakili Komunitas Intelijen Amerika Serikat dalam *Worldwide Threat Assessment* tahun 2013 menyatakan, ancaman siber telah menjadi peringkat pertama ancaman non tradisional di atas terorisme, kejahatan transnasional terorganisir, senjata proliferasi pemusnah massal, kontra-intelijen, kompetisi dan ketidakamanan sumber daya alam, kesehatan dan ancaman pandemi serta konflik kekerasan (Mazzeti dan Sanger, 2013). Hal ini menjadi catatan penting, karena untuk pertama kalinya sejak serangan 11 September 2001, terorisme internasional tidak lagi menjadi peringkat pertama dalam penilaian Komunitas Intelijen AS sebagai ancaman global terhadap keamanan nasional.

Dengan tingginya serangan siber yang terjadi saat ini, ancaman siber kini ditetapkan oleh masyarakat internasional sebagai ancaman utama yang paling relevan terhadap keamanan nasional dan internasional. Untuk menyikapinya sejumlah organisasi internasional dan regional, badan dan forum seperti halnya OEC, OSCE (*Organization For Security and Co-operation in Europe), European Union, European Council*, BRICS , OAS (*Organization of American States),* AU *(African Union),* APEC *(Asia-Pacific Economic Cooperation)* , G8/G20 , UN (*United Nations), Internet Governance Forum*, ICANN, NATO (*North Atlantic Treaty Organization),* dan *World Economic Forum* telah menjadikan siber sebagai salah satu isu utama perlu yang perlu mendapatkan perhatian dan respon cepat dari berbagai Negara terlebih dengan bentuk ancaman yang tidak mengenal batas ruang dan waktu.

Hingga saat ini, upaya-upaya regional dan global guna menciptakan keamanan siber yang komprehensif telah dilakukan, namun sayangnya terkesan lambat dan terfragmentasi. Demikian pula, upaya negara-negara anggota ASEAN untuk mengadopsi kerangka kerjasama yang komprehensif guna mencapai kerjasama keamanan siber. Hingga kini kerangka keamanan siber ASEAN - yang komprehensif belum dapat dikembangkan meskipun telah dilaksanakan berbagai pertemuan resmi yang dilaksanakan ASEAN. Misalnya dalam *ASEAN*

Ministerial Meeting on Transnational Crime/AMMTC pada tahun 2003 yang sepakat memasukkan kejahatan siber sebagai salah satu isu keamanan kejahatan transnasional, akan tetapi tindak lanjut yang komprehensif semisal regulasi bersama untuk menyikapi atau menindak kejahatan siber belum terwujud. Selain itu, pembahasan mengenai siber nyatanya lebih banyak dilakukan dalam bentuk workshop maupun diskusi antar pemangku kepentingan sekaligus melibatkan para pakar dan akademisi dalam rangka membangun kepercayaan, akan tetapi belum mampu memberikan dampak signifikan terhadap pembentukan kebijakan yang tepat sasaran mengenai siber (Isu siber belum tersekuritisasi diantara seluruh negara-negara ASEAN, hal ini terkait dengan adanya *ASEAN way* dalam poin non-intervensi yang umumya menghindari masalah politisasi) (Heinl 2013, 2).

ASEAN juga harus menghadapi permasalahan yaitu proses perkembangan beberapa Negara anggota ASEAN yang rawan dengan berbagai ancaman. Terlebih dengan kebutuhan masyarakat terhadap teknologi informasi dan komunikasi (ICT) sebagai unsur pendukung kegiatan sehari-hari. Hampir sebanyak 78% masyarakat ASEAN menggunakan ICT sebagai unsur pendukung kegiatan sehari-hari (*ASEAN Secretariat*, 2011*)*. Kompleksitas ancaman dan permasalahan siber di wilayah Asia Tenggara menjadi sebuah permasalahan yang harus dihadapi oleh ASEAN sebagai sebuah Organisasi yang bertujuan menciptakan stabilitas di wilayah Asia Tenggara. ASEAN perlu mengembangkan pendekatan yang komprehensif namun juga dinamis dalam menangani masalah keamanan siber yang bersifat lintas batas negara. Negara-negara anggota ASEAN dan warganya harus siap untuk bisa beradaptasi dan membuat kemajuan dalam bidang siber sehingga tidak mengalami ketertinggalan dan dapat dengan mudahnya dijadikan sebagai sasaran serangan siber oleh Negara atau pihak lain. Tulisan ini secara khusus akan membahas mengenai upaya Asosiasi Bangsa-Bangsa di Asia Tenggara (ASEAN) dalam menghadapi ancaman siber di Asia Tenggara. Terkhusus setelah disepakati integrasi kawasan ASEAN melalui ASEAN Community 2015 yang sesungguhnya telah membuka peluang kerjasama keamanan siber di kawasan Asia Tenggara sekaligus menjadi jembatan dalam mewujudkan kerangka kerjasama siber yang lebih solid guna mencapai *ASEAN Connectivity* (Konektivitas ASEAN) 2025.

2. Kajian Pustaka

2.1 Rejim Keamanan Internasional

Menurut Krasner, rezim internasional adalah suatu tatanan yang berisi kumpulan prinsip, norma, aturan, proses pembuatan keputusan, baik bersifat eksplisit maupun implisit, yang berkaitan dengan ekspektasi atau pengharapan aktor-aktor, dan memuat kepentingan aktor tersebut dalam Hubungan Internasional (Krasner 1983, 186). Prinsip yang dimaksud adalah berkaitan dengan kepercayaan akan fakta, sebab-akibat, dan kejujuran; norma adalah standar perilaku yang dimanifestasikan sebagai hak dan kewajiban; peraturan adalah larangan yang jelas dan spesifik tentang tindakan yang dilakukan; sedangkan prosedur pembuatan keputusan adalah sebagai tata cara yang harus ditempuh dalam mengimplementasikan pilihan bersama (Krasner 1983, 186). Dengan adanya prinsip, norma, aturan dan prosedur pengambilan ini, maka rezim menjadi sebuah institusi internasional yang membatasi pengambilan keputusan suatu Negara secara mandiri dan mengandalkan pembuatan keputusan secara kolektif (*joint decision)*.

Pembuatan keputusan secara kolektif Rezim harus dipahami sebagai sebuah entitas yang lebih dari sekedar susunan temporer yang dapat berubah sesuai dengan perubahan kekuatan (*power)* dan kepentingan (*interest)* seperti halnya kerjasama sebagaimana disebutkan diatas. Di dalamnya terdapat interaksi dan dialektika antara kekuatan dan kepentingan yang dilaksanakan berdasarkan berbagai aturan prosedur yang inheren sehingga dapat merubah

tatanan yang ada. Aturan, procedure dan norma yang ada di dalam rejim mengatur dan menjadi kontrol perilaku dari anggota rezim.

Rezim merupakan sebuah bentuk yang berbeda dari kerjasama diantara negara-negara. Hal ini didefinisikan oleh Krasner sebelumnya yang melihat bahwa rejim harus dipisahkan dari sebuah kesepakatan atau perjanjian sementara, yang mana perjanjian tersebut dapat begitu saja berubah karena adanya perubahan distribusi kekuatan atau kepentingan. Secara lebih jauh, Krasner menyebutkan bahwa tindakan rejim tidak bisa dilakukan berdasarkan kepentingan, namun berdasarkan sebuah norma atau aturan umum dengan mengedepankan prinsip timbal balik sebagai sebuah bentuk dinamika rezim.Dalam rezim dalam memberikan sebuah aturan dan paksaan guna mengatur interaksi antara pihak yang satu dengan yang lain.

Rezim menjadi contoh dari perilaku kerjasama sebagai upaya untuk memfasilitasi kerjasama, namun kerjasama dapat terjadi terlebih dahulu tanpa adanya rezim (Haggard & Simmons, 1987:495). Sehingga dapat dikatakan rezim merupakan sebuah kelanjutan bentuk kerjasama, dan mendorong terjalinnya kerjasama dengan lebih baik. Perbedaan mendasar antara rezim dengan institusi adalah bagaimana memandang aktor-aktor dalam hubungan internasional. Rezim mengacu pada pengaruh perilaku yang ditimbulkan dari organisasi internasional pada aktor-aktor yang lainnya, terutama aktor negara dengan berfokus pada ekspektasi aktor. Berbeda dengan institusi yang lebih melihat kepada apa yang terjadi dalam organisasi daripada melihat pengaruh yang ditimbulkan organisasi internasional terhadap aktor-aktor lainnya (Barkin, 2006:27).

Dalam konteks keamanan, rezim dibentuk dengan asumsi dasar bahwa sifat Negara pada dasarnya hidup dalam prinsip "timbal balik". Prinsip timbal balik membuat Negara-negara yang berdaulat mengorbankan kepentingan jangka pendek guna mendapatkan keuntungan yang lebih besar di masa depan, yang berasal dari sikap timbal balik yang dilakukan oleh actor atau Negara lain. Arthur Stein, menyatakan bahwa akar dari terbentuknya rejim adalah relasi diantara Negara yang berdaulat yang terjadi karena masing-masing Negara berupaya memenuhi kebutuhannya, hingga akhirnya Negara tersebut dapat bergantung pada diri sendiri dan mampu mengembangkan kemampuannya (Stein 1993, 17). Sekalipun dalam hal keamanan rejim sangat sulit untuk dicapai, namun kebutuhan Negara untuk bertahan hidup memberikan celah terbentuknya sebuah relasi yang didesain untuk mengelola kompleksitas, melalui relasi yang ada pada rejim.

Rejim keamanan siber ASEAN merupakan sebuah kondisi yang "lazim" terbentuk di Asia Tenggara dalam menghadapi bentuk ancaman non-tradisional yang muncul dalam kondisi yang "tidak pasti". *Regime* mengkalkulasikan hasil yang bisa didapatkan suatu actor atau Negara dalam sebuah kondisi ketidakpastian atau ketika tidak adanya kalkulasi yang spesifik.

2.2 Kejahatan dan Keamanan Siber (*Cyber Security)*

Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, dijelaskan adanya dua istilah yang terkait dengan pengertian *Cybercrime*, yaitu *cybercrime dan computer related crime*. (Barda Nawawi Arief, 2007: 24). Istilah *cybercrime* dibagi dalam dua kategori yaitu pertama, *cybercrime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*, serta *cybercrime* dalam arti luas (in a broader sense) yang disebut sebagai *computer related crime*.

Kejahatan siber (*Cybercrime*) dalam arti sempit diartikan sebagai berbagai bentuk tindakan illegal yang diarahkan oleh berbagai bentuk operasi elektronik yang menargetkan sistem keamanan computer dan data-data yang diproses oleh system tersebut. Sedangkan, kejahatan siber dalam arti luas didefinisikan sebagai berbagai kegiatan illegal yang dilakukan terkait dengan system atau jaringan computer, yang termasuk didalamnya adalah sejumlah

kejahatan criminal seperti kepemilikan illegal, menawarkan atau menyebarluaskan informasi dengan menggunakan system atau jaringan computer. Sehingga dengan kata lain kejahatan siber, adalah kejahatan yang dilakukan dengan *menargetkan* computer atau jejaring computer, atau kejahatan yang digunakan dengan perangkat atau jaringan computer.

Indra Safitri mengemukakan bahwa kejahatan siber atau kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet. Kejahatan siber dapat meliputi hal-hal berupa penyusupan pada computer (*hacking)* guna melakukan penyerangan terhadap property, spionase ekonomi (pencurian data atau melakukan transaksi rahasia, pemerasan secara online, pencucian uang, pencurian identitas, dan sejumlah serangan-serangan yang difasilitasi melalui jaringan internet yang nyatanya jenisnya terus bertambah setiap hari (Govil 2007, 610-615). Secara lebih lanjut, kejahatan siber sebagaimana disebutkan diatas tidak mudah untuk diidentifikasi, khususnya terkait dengan metode yang digunakan, lokasi hingga waktu terjadinya tindakan kejahatan siber. Anonimitas internet, membuat kejahatan siber semakin merajalela dengan berbagai instrument dan bentuk kejahatan.

Dalam beberapa kasus besar, serangan siber yang terjadi tidak hanya berasal dari satu Negara atau satu sumber. Bahkan serangan siber, lebih sering dilakukan oleh actor non Negara dengan sasaran yang beragam. *Cyberspace* atau ruang siber yang tidak terbatas dan *lawless* memberikan berbagai kemungkinan bagaimana dan darimana serangan berasal, sehingga kejahatan siber seringkali tidak dapat ditangani dengan cara yang mudah dan singkat, ataupun hanya mengandalkan kinerja dari satu actor.

Kejahatan siber dilakukan dengan berbagai latar belakang, seperti halnya kebutuhan akan pengakuan, uang, kelemahan dalam bidang hokum dan penegak hokum dalam menindak kejahatan siber, minimnya tingkat pelaporan (terutama di Negara berkembang) hingga kesulitan untuk mengindikasikan kejahatan, hingga pada pemberitaan media yang minim terkait kejahatan siber (kejahatan siber "kurang popular" dibandingkan dengan tindakan criminal yang nyata (kejahatan konvensional). (Jones, 305-309).

Tabel 2.1 Perbedaan kejahatan siber dengan kejahatan konvensional (Mercubuana 2010)

Kejahatan siber	Kejahatan konvensional
Terdapat penggunaan teknologi informasi	Tidak ada penggunaan Teknologi Informasi secara langsung
Alat bukti digital (non fisik) dalam bentuk *log files*.	Alat bukti fisik (sebagaimana pasal 184 KUHAP)
Kejahatan dilakukan dalam ruang siber sehingga serangan sebagian besar merupakan serangan non-fisik. Meskipun dalam sejumlah kasus, dapat berdampak pada fisik.	Pelaku dan korban berada pada tempat yang sama. Sehingga penyidikan dilakukan pada dunia nyata
Merupakan bentuk kejahatan yang *borderless* (tanpa batas) sehingga terlihat transnasional	Lokasi kejahatan ada dalam wilayah tertentu.

Sementara itu, dalam arti yang sederhana, keamanan siber diartikan sebagai usaha-usaha yang dilakukan dalam melindungi teknologi informasi dan jaringan informasi. Dengan

keterkaitannya yang luas, konsep keamanan siber seringkali bersifat kabur, namun demikian terdapat tiga definisi penting yang dapat mendefinisikan keamanan siber:
A. Serangkaian kegiatan dan tindakan lain yang dimaksudkan untuk melindungi-dari serangan, gangguan, atau ancaman lainnya, terhadap komputer, jaringan komputer, perangkat keras terkait dan perangkat lunak dan informasi yang dikandungnya dan termasuk perangkat lunak dan data, serta elemen lain dari dunia maya
B. Perlindungan yang diberikan kepada suatu negara dalam menghadapi ancaman diatas
C. Sebuah kegiatan yang bertujuan untuk menerapkan dan memperbaiki aktivitas dan kualitas dalam memberikan perlindungan sebagaimana disebutkan diatas.

Istilah keamanan siber (*cyber security)* pertama kali digunakan oleh ilmuwan computer pada awal tahun 1990 untuk menjelaskan serangkaian celah ketidakamanan pada computer yang disambungkan pada jejaring. Kerentanan ini menjadi ancaman dari teknologi digital yang dapat berdampak social kepada penggunanya (Nissembaum, 2005). Keamanan siber menjadi sebuah konsep sekuritisasi dalam laporan *Computer Science and Telecommunications Board's* (CSTB) pada tahun 1991, yang mendefinisikan "keamanan" sebagai sebuah upaya perlindungan dari upaya modifikasi, penyingkapan, atau penghancuran data pada sebuah system, sekaligus sebagai upaya pengamanan dalam system tersebut (CSTB 1991, 2).

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

3. Hasil dan Pembahasan

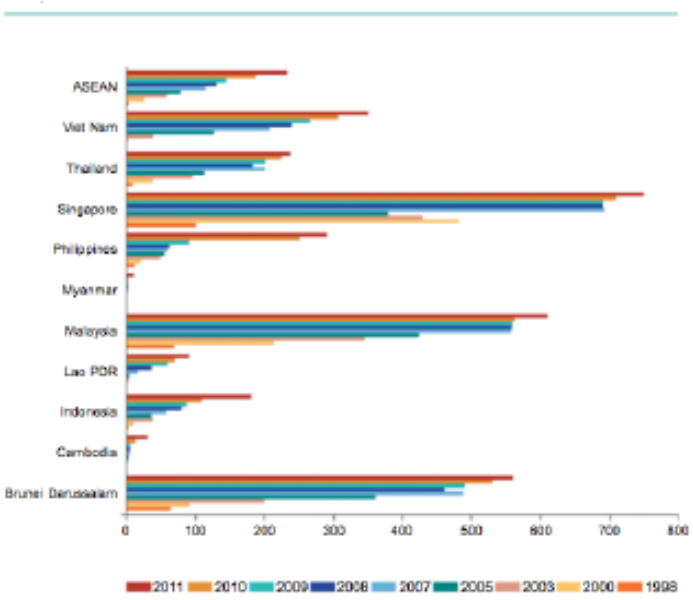
3.1 Kompleksitas Ancaman Siber di Asia Tenggara

ASEAN adalah kawasan yang sangat signifikan dalam hal isu-isu keamanan siber internasional. Hal ini disebabkan karena,

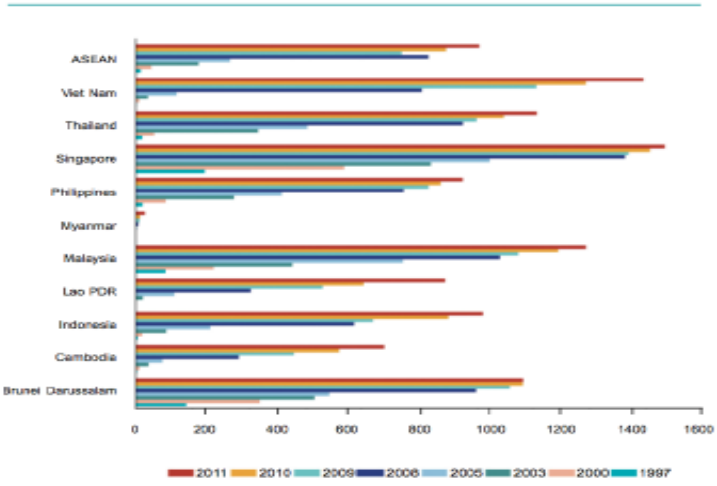
a. Pertama, sentralitas ASEAN dalam arsitektur kawasan yang lebih luas di kawasan Asia Pasifik dan peran potensialnya sebagai "daerah netral" yang signifikan dalam hal kerjasama keamanan siber internasional. Sebagai "daerah netral" ASEAN telah menjadi wilayah tengah dalam upaya persaingan antara AS-China. Meskipun sering diperhadapkan dalam kondisi dilematis dalam hubungannya dengan kedua Negara tersebut, ASEAN dapat memetik poin positif dengan menikmati berbagai bantuan yang diberikan oleh kedua Negara tersebut, dalam rangka memperluas pengaruhnya di kawasan Asia Tenggara.
b. Kedua, meskipun warga di banyak tersebut itu masih kesulitan dalam memiliki akses Teknologi Informasi dan Komunikasi (TIK), namun diperkirakan jumlah penggunaan internet dan alat komunikasi terus meningkat. Menurut *World Threat Assessment* 2013 report dalam proposal Komisi Eropa dari 2,1 miliar pengguna internet di seluruh dunia, sebagian besar pengguna berada di Asia (922.200.000). Sementara itu, Daerah berikutnya yang paling signifikan dalam hal jumlah pengguna internet adalah Eropa dengan 476.200.000 pengguna. China sendiri memiliki 485 juta pengguna internet - lebih dari negara atau wilayah (termasuk Eropa dan sisanya dari Asia) lain - dan memiliki serangan internet hanya 36,3 persen.

Pertumbuhan ICT di Asia Tenggara sebenarnya tidak terlalu jauh tertinggal dari AS, Eropa dan negara-negara di Asia Timur Laut seperti Jepang dan Republik Korea. Menurut Proyek Database *E Commerce ASEAN* yang dirilis pada tahun 2010, ASEAN mewakili 6 persen pengguna Internet dan jumlah tingkat penetrasi global ASEAN negara anggota 20 persen, dengan Brunei Darussalam, Singapura dan Malaysia memiliki pangsa penetrasi internet terbesar, dan Indonesia, Filipina, dan Vietnam memiliki pengguna internet terbesar.

Di Asia Tenggara (Lihat Gambar 1) jumlah pengguna internet telah hampir mencapai dua kali lipat selama periode 2008-2011 dengan penggunaan telepon genggam sebagai alat komunikasi (Lihat gambar 2) mencapai 967,5 unit per 1.000 orang pengguna, dan diperkirakan mendekati 70 persen dari total penduduk dunia pada tahun 2017. Secara global, ada dua kali lebih banyak langganan mobile broadband dan selanjutnya, teknologi mobile GSM / EDGE akan mencakup lebih dari 90 persen dari populasi dunia, dengan 85 persen mengakses WCDMA / HSPA teknologi mobile di kecepatan hingga 2MB per detik pada 2017.



Gambar 1. Pengguna Internet di ASEAN per 1000 orang



Gambar 2. Pengguna Telepon Genggam di ASEAN per 1000 orang

Dengan meningkatnya penggunaan Internet dan telepon genggam di wilayah Asia Tenggara per-tahunnya, maka dapat dipastikan bahwa tingkat ketergantungan terhadap teknologi

informasi dan komunikasi semakin meningkat. Ketergantungan tersebut nyatanya juga menimbulkan berbagai implikasi negative dengan munculnya berbagai insiden serangan siber pada sejumlah Negara ASAN yang meliputi serangan terhadap website milik pemerintah maupun milik swasta dan individu. Tabel berikut merupakan data yang berisi Insiden ancaman Siber di Wilayah ASEAN Untuk Periode Januari 2012- 2013

Tabel 1.1 Data Serangan Siber di Asia Tenggara pada tahun 2012-2013

Negara	Insiden Siber	Bulan / Tahun
Brunei Darussalam	IT Perlindungan Keamanan (ITPSS) mencatat lebih dari 2.000 serangan siber untuk periode 2010-2012 (62% serangan virus, 26% spam, 7% perusakan dan 4% penipuan	November 2012
Kamboja	a. Sekelompok hacker yang disebut Nullcrew menyerang website Kamboja untuk memprotes sensor internet dan penangkapan Gottfrid Svartholm Warg (co-pendiri The Pirate Bay). Nullcrew mengumumkan bahwa akan menargetkan bisnis Kamboja dan pemerintah termasuk angkatan bersenjata sebagai target serangan berikutnya b. Terjadi serangan pada Website Polisi Militer Nasional Kamboja dan Mahkamah Agung. Seorang hacker Indonesia yang disebut "Hmei7" mengaku bertanggung jawab atas serangan tersebut, tetapi tidak ada atribusi yang bisa dibuat untuk menyerang situs Mahkamah Agung. c. Pemerintah Kamboja telah menjadi sasaran beberapa serangan siber di masa lalu, salah satunya di mana Anonymous mencuri dan membocorkan lebih dari 5.000 dokumen dari Departemen Luar Negeri.	September 2012
Indonesia	a. Sebuah kelompok yang disebut Anonymous Indonesia merusak lebih dari dua belas situs web pemerintah, menyusul penangkapan Wildan Yani Ashair yang dituduh meretas situs Presiden. b. Dalam tiga tahun, website Pemerintah telah diserang lebih dari 36,6 juta kali c. Skema penipuan online serius yang melibatkan kerugian lebih dari USD500, 000 menyumbang 40% dari 176 kasus kejahatan siber yang dilaporkan selama empat bulan pertama pada tahun 2013.	Januari 2013
Malaysia	a. Polisi mencatat 24 kasus peretasan antara Januari dan September 2012 dengan estimasi kerugian dari USD 1,1 million b. Kelompok Hacker memposting pernyataan di website Departemen Penerangan yang menyatakan Perdana Menteri Datuk Seri Najib Tun Razak telah mengundurkan diri. c. Stasiun radio alternatif untuk oposisi dan portal berita Sarawak Report mengaku menjadi sasaran serangan DDoS.	November 2012 Februari 2013 Maret 2013

	Contoh FinSpy - bagian dari intrusi terpencil dan software surveilans FinFisher yang didistribusikan oleh Gamma International - tampaknya khusus ditujukan untuk siaran dalam bahasa Melayu	
Myanmar	a. Website Kementerian Informasi dirusak untuk memberikan peringatan agar menghentikan pembunuhan terhadap kaum Muslim. b. Anonymous mengumumkan kampanye baru untuk mendukung kaum Muslim. c. Komunitas Rohingya berfokus pada situs pemerintah, menyuarakan agar PBB (untuk tidak melibatkan diri dengan operasi penjaga perdamaian), dan Aung San Suu Kyi atas kurangnya tindakan nya tentang kekerasan anti-Rohingya. Eleven Media dirusak oleh grup Hacker Blink (http://www.blinkhackergroup.org/) dalam menanggapi sebuah editorial yang mengutuk kebencian pidato. Kelompok ini juga telah menyerang situs pro-Rohingya dalam kaitannya dengan kekerasan antara orang-orang Muslim Rohingya dan Buddha di negara bagian Rakhine Myanmar.	Agustus 2012 Mei 2013
Filipina	1. Dugaan defacements dari beberapa situs pemerintah oleh hacker China terkait dengan sengketa Laut China Selatan. Hacker Filipina membalas dengan meluncurkan serangan serupa terhadap situs China. 2. *Anonymous* Filipina meretas website Presiden untuk menyuarakan protes terkait "kesalahan penanganan" konflik Sabah dan menuduh Pemerintah mengizinkan pasukan Malaysia untuk membunuh penduduk. 3. Anonymous Filipina menyerang entitas komersial terkemuka, organisasi masyarakat sipil, dan pemerintah sebagai protes atas perdebatan Kejahatan Siber 4. Setelah Penjaga Pantai Filipina menembak sebuah kapal nelayan Taiwan, hacker Taiwan dan Filipina melakukan " pertempuran maya dengan menggunakan situs web pemerintah Taiwan dan Filipina Kelompok asal Taiwan, Anon TAIWAN, mengaku bertanggung jawab atas informasi DNS dan merilis situs pemerintah Filipina .	Juni 2012 Maret 2013 September 2012 Mei 2013
Singapura	Sebuah laporan oleh Trend Micro Pintar Jaringan Perlindungan menunjukkan bahwa lebih dari 900 warga Singapura adalah korban penipuan perbankan online pada kuartal pertama tahun 2013	Mei 2013
Thailand	1. Grup Hacker dari Turki merilis informasi 2.000 kontak pengguna McDonald Thailand Kelompok yang sama mengklaim bertanggung jawab atas serangan terhadap situs Palang Merah Thailand guna memprotes lambing bendera Turki yang dinilai tidak menghormati Nabi Muhammad. Kelompok itu sebelumnya merusak situs Pepsi Hongaria dengan pesan yang sama. 2. Dari Januari sampai Mei 2013, ada 1.475 intrusi ke dalam situs pemerintah, dan ratusan serangan malware dan *phishing* .	Oktober 2012 Juni 2013

Vietnam	Versi Vietnam dari Baidu, sebuah perusahaan mesin pencari China, ternyata telah terinfeksi dengan spyware dan adware sehingga setelah melakukan proses pengunduhan, computer yang mengunduh tersebut dapat dikendalikan dari jarak jauh (remote), dan data yang diambil digunakan sebagai "zombie" untuk serangan DDoS	Juli 2012

Data insiden siber yang tertera diatas menunjukkan bahwa ancaman siber yang menyerang berbagai Negara sangat kompleks. Serangan siber dapat dilakukan tidak hanya oleh Negara, namun demikian dilakukan oleh actor non-negara dengan bentuk serangan yang sulit terdeteksi dan sulit diprediksi.

Sekalipun belum menyebabkan kelumpuhan seperti yang dialami Estonia pada tahun 2007 ataupun Georgia pada tahun 2008, ancaman siber ini perlu disikapi secara cepat dan tepat. Negara-negara di kawasan Asia Tenggara sangat mudah terpapar serangan siber, terlebih dengan tingkat kerentanan yang tinggi namun juga memiliki ketergantungan yang signifikan terhadap teknologi. Sehingga Negara ASEAN perlu bersinergi dalam menghadapi ancaman ini melalui kebijakan, regulasi hingga penindakan serta respon cepat.

3.2 Babak Baru Rejim Keamanan Siber di Asia Tenggara dalam Menyongsong *ASEAN Connectivity 2020*

Dalam Piagam ASEAN, Negara-negara Anggota ASEAN sepakat untuk membangun Komunitas ASEAN yang terdiri dari Komunitas Politik - Keamanan, Komunitas Ekonomi ASEAN, dan Komunitas Sosial-Budaya ASEAN pada tahun 2015. Dalam rangka membangun komunitas tersebut, Negara-negara ASEAN mendukung terwujudnya kohesif (kesatuan) politik", mampu terintegrasi secara ekonomi dan dapat bertanggung jawab sosial dalam rangka memanfaatkan peluang saat ini dan masa depan, dan secara efektif merespon tantangan-tantangan regional dan internasional.

Kini, tantangan siber menjadi salah satu tantangan regional yang paling signifikan bagi kepentingan bersama untuk Negara-negara Anggota ASEAN. Kejahatan siber menjadi tantangan baru disebabkan karena a) meningkatnya volume dan kompleksitas ancaman; b) dilema atribusi yang akurat; c) Peningkatan jumlah aktor negara dan non-negara; d) Kurangnya definisi harmonis dan pemahaman tentang terminology "dunia maya"; e) belum tercapainya kerjasama sektor publik-swasta yang efektif khususnya dalam menciptakan keamanan siber; f) Keterbatasan tingkat R & D khususnya bagi sejumlah negara ASEAN; g) ketidakcukupan dan tersedianya keahlian dalam bidang siber; h) Kurangnya kesadaran masyarakat, dan i) Regulasi yang mengatur kebebasan sipil khususnya dalam bidang siber masih terbatas.

Dalam merespon tantangan tersebut, sejak tahun 2001 pada AMMTC (ASEAN Ministerial Meeting on Transnational Crime), isu keamanan siber telah menjadi salah satu agenda pertemuan yang menghasilkan kesepakatan para Menteri ASEAN yang bertanggung jawab untuk kejahatan transnasional. Negara-negara di ASEAN sepakat untuk memasukkan kejahatan siber (*cybercrime)* dalam program kerja untuk melaksanakan Rencana Aksi ASEAN (ASEAN *Plan of Action)* dalam melawan kejahatan transnasional (*ASEAN Secretariat, 2011)*. Selanjutnya pada tahun 2003 dalam pertemuan ke-9 AMMTC yang diselenggarakan di Vientiane, Lao PDR, para Menteri ASEAN menyambut terciptanya Kelompok Kerja SOMTC baru mengenai Kejahatan siber yang merupakan bagian dari kejahatan transnasional (*ASEAN Senior Officials Meeting on Transnational Crime*)

Respon dari ASEAN ini semakin disempurnakan dengan *ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space*, di Kuala Lumpur pada tanggal 28 Juli 2006, yang secara garis besar menekankan terciptanya kerangka hukum

(regulasi) dalam melawan kejahatan siber, mendorong kerjasama dan kolaborasi dalam dan kolaborasi dalam menangani kejahatan, termasuk *cyber terrorism (*terorisme siber), penyalahgunaan ruang siber dan mendorong peningkatan kesadaran masyarakat dalam menggunakan siber. (*ASEAN Secretariat, 2011).*

Sejak tahun 2003, Singapore *ASEAN Telecommunications and IT Ministers Meeting* (TELMIN), dan *Telecommunications Senior Officials Meeting* (TELSOM) menekankan upaya pembentukan Infrastruktur informasi ASEAN dengan maksud untuk mempromosikan inter-operabilitas, inter-konektivitas, dan integritas keamanan. Para Menteri dari Telekomunikasi dan TI memutuskan bahwa semua Negara Anggota ASEAN perlu mengembangkan dan mengoperasionalkan nasional Tim Tanggap Darurat Komputer Nasional(CERT) pada tahun 2005 sesuai dengan kriteria kinerja minimum yang disepakati bersama. Seiring dengan terbentuknya kesepakatan tersebut, forum virtual untuk keamanan siber ASEAN sedang dibentuk untuk mengembangkan kerangka kerja umum untuk mengkoordinasikan pertukaran informasi, pembentukan standar dan kerjasama antar lembaga penegak hukum. Upaya ini disempurnakan dengan dibentuknya ASEAN ICT Masterplan 2015 (AIM 2015) yang disetujui pada pertemuan TELMIN ke-10 Tanggal 13-14 Januari 2011 di Kuala Lumpur, Malaysia. AIM 2015 menekankan pada pembangunan kepercayaan terkait dengan keamanan siber melalui pemberdayaan dan keterikatan masyarakat serta upaya pembangunan infrastruktur dengan inisiatif untuk mempromosikan integritas jaringan dan keamanan informasi, perlindungan data dan kerjasama CERT.

Dengan berjalannya komunitas ASEAN 2015, integrasi ICT dan konektivitas ASEAN menjadi isu penting dan factor pendorong serta syarat dalam mewujudkan komunitas ASEAN. ASEAN kemudian menyepakati Master Plan ASEAN Connectivity 2020, yang menekankan pada konektivitas Fisik dimana didalamnya terdapat factor ICT, konektivitas psikologi dan konektivitas di antara manusia. Secara terkhusus dalam hal ICT, ASEAN mendorong terciptanya kemampuan dalam melaksanakan konektivitas digital dan mendorong tersedianya infrastruktur teknologi informasi dan komunikasi yang memadai, agar tercipta komunitas ASEAN yang terintegrasi, satu visi dan satu identitas. Mengingat ICT merupakan sebuah mesin perdagangan, pertumbuhan ekonomi, inovasi dan pemerintahan yang lebih baik di wilayah ASEAN.

Pasca terbentuknya komunitas ASEAN, sebagian besar fokus ASEAN pada keamanan siber telah diarahkan untuk memerangi kejahatan transnasional dan, yang semakin, mengamankan integrasi ekonomi regional. Kejahatan siber dan terorisme siber, secara eksplisit dicantumkan pada berbagai deklarasi dan komunike ASEAN mengenai kejahatan transnasional pasca serangan teroris 2001 di Amerika Serikat. Sejak saat itu, dorongan untuk mengintegrasikan masyarakat ASEAN pada tahun 2015 telah mengubah fokus ASEAN khususnya dalam menciptakan keamanan siber.

Sesungguhnya pencapaian kemakmuran ekonomi sebagai basis stabilitas politik telah menjadi prioritas ASEAN sejak awal, sehingga mewujudkan ASEAN sebagai wilayah pertama di negara berkembang yang mengadopsi kerangka hukum harmonis *untuk e-commerce*. Hal ini didorong oleh rencana percepatan untuk integrasi regional melalui, antara lain, ASEAN ICT Masterplan dan ASEAN connectivity 2020. Dalam visi konektivitas ASEAN, Negara-negara di Asia Tenggara tetap berupaya menjadi kawasan berkembang yang paling maju dan harmonis guna mencapai kemajuan secara menyeluruh, khususnya kemajuan dalam teknologi Teknologi informasi dan komunikasi merupakan sebuah mesin perdagangan, pertumbuhan ekonomi dan wujud inovasi wilayah ASEAN. Sehingga ASEAN menyepakati untuk mempercepat pembangunan Infrastruktur dan layanan ICT di masing-masing Negara anggota ASEAN sembari berupaya mengantisipasi hadirnya berbagai kejahatan siber sebagai implikasi pembangunan ICT dan konektivitas diantara berbagai Negara, dengan meningkatkan keamanan integritas jaringan dan informasi perlindungan data dan kerjasama *Computer Emergency*

Response Team (CERT) melalui pengembangan kerangka kerja umum dan membangun standar minimum yang tepat, untuk memastikan tingkat kesiapan dan integritas jaringan di seluruh ASEAN 2020.

Sebagaimana disebutkan diatas, pasca komunitas ASEAN 2015, Negara-negara di Asia Tenggara dinilai telah berevolusi dalam mengembangkan strategi kerjasama keamanan siber yang didasarkan pada sentralitas teknologi informasi dan keamanan komunikasi terhadap pertumbuhan ASEAN dan kemakmuran masa depan. ASEAN, dengan bentuk kerjasama yang khas berdasarkan nilai-nilai ASEAN (*ASEAN WAY)* nyatanya berhasil membangun sebuah rejim keamanan baru yang membuka kesempatan bagi Negara-negara Asia Tenggara untuk mengembangkan kapasitas, pembangunan infrastruktur ruang siber, membangun kepercayaan diri dan promosi tindakan untuk merangsang transparansi, kepercayaan, dan dialog. Rejim keamanan siber di Asia Tenggara memfasilitasi negara-negara di Asia Tenggara yang terdiri dari beragam latar belakang, potensi serta ancaman, agar dapat terhubung satu dengan lainnya, dan mampu memberikan keuntungan secara "timbal balik". Dengan adanya rejim keamanan siber, Negara-negara Asia Tenggara dapat meningkatkan kewaspadaan dan kemampuan dalam menghadapi ancaman siber, sekaligus membangun koordinasi dalam mengantisipasi ancaman siber.

Di tahun 2017, dalam menyongsong konektivitas ASEAN, ASEAN telah membentuk strategi *cyber proactive* yang dibangun berdasarkan kesadaran bahwa dunia maya adalah sarana yang menciptakan kemajuan ekonomi dan peningkatan standar hidup. Contoh real, AMCC pada bulan Oktober 2016 telah membangun sebuah platform diskusi mengenai isu-isu cyber di tingkat menteri hingga pembahasan keamanan siber menggunakan perspektif harmonisasi diantara para pemangku kebijakan. Di tahun ini, perwakilan ASEAN menyetujui Strategi Kerjasama *Cybersecurity* yang menetapkan peta jalan yang berfokus pada pentingnya kerjasama yang kuat dan berkoordinasi di berbagai bidang seperti kebijakan keamanan dunia maya, pengembangan strategi, legislasi, norma dan pengembangan kapasitas. Dalam hal ini, pada TELMIN ke-16 pada bulan November 2016 dan pada Retreat Pemimpin TELSOM-ATRC pada bulan Maret 2017, Strategi Kerjasama Cybersecurity ASEAN disahkan dan disetujui, peta jalan yang berfokus pada tiga bidang: respon insiden; pembuatan kebijakan dan koordinasi antara Tim Kesiapan Darurat Komputer (CERT); dan peningkatan kapasitas cybersecurity.

4. Kesimpulan dan Rekomendasi

Dunia siber digambarkan sebagai suatu ruang dimensi yang dibentuk dari dan berkaitan dengan perangkat lunak dan perangkat keras komputer, serta jaringan komunikasi informasi. Salah satu bentuk paling populer adalah yang saat ini dikenal luas dengan sebutan Internet, yaitu jaringan komunikasi informasi yang menghubungkan miliaran komputer di seluruh dunia. Keterhubungan yang ditawarkan oleh siber memberikan dampak positif, yaitu memberikan keleluasaan hubungan komunikasi yang tidak mengenal batas ruang dan waktu, Hingga mampu meminimalisasi biaya. Akan tetapi bagaikan dua sisi mata uang, keleluasaan yang diberikan oleh dunia siber juga membawa ancaman tersendiri, salah satunya munculnya isu-isu keamanan non-tradisional yang dapat mengancam kedaulatan Negara.

Untuk merespon serangan siber yang muncul, ASEAN berupaya untuk menerapkan kerangka kerja yang komprehensif terkait dengan keamanan siber. Upaya mewujudkan keamanan siber yang komprehensif diwujudkan dengan menciptakan kerangka regulasi yang mendorong terciptanya kerjasama internasional antara Negara-negara di kawasan Asia Tenggara. ASEAN akan berupaya untuk mendorong *win-win solution* untuk mencerminkan kepentingan semua Negara Anggota ASEAN.

Munculnya visi Komunitas ASEAN 2015, telah memberikan implikasi positif terhadap terciptanya kerjasama keamanan siber bagi Negara-negara ASEAN. Dengan adanya visi

Komunitas ASEAN 2015, Negara-negara ASEAN akan terdorong untuk menciptakan konektivitas secara fisik melalui konektivitas teknologi informasi dan Komunikasi. Konektivitas ini tentunya harus diimbangi dengan jaringan siber yang aman dan menunjang aktivitas di dalamnya. Meskipun terkesan lambat, akan tetapi secara perlahan namun pasti ASEAN tengah mewujudkan kerjasama keamanan siber tersebut secara komprehensif. Komunitas ASEAN 2015 akan memberikan babak baru peluang dan inisiatif Negara-negara untuk mendorong konektivitas ICT dan kerjasama keamanan siber Internasional untuk mengamankan konektivitas (integrasi) di kawasan Asia Tenggara.

DAFTAR PUSTAKA

Buku

ASEAN Secretariat. 2011. *ASEAN ICT Masterplan 2015 (AIM)*

ASEAN. 2013. *Chairman's Statement of the 22nd ASEAN Summit - "Our People, Our Future Together"*

Jervis R. 1983. *International Regimes.* Ithaca: Cornell University Press

Komisi Uni Eropa. 2013. *Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union SWD(2013) 32 final*

Parlemen Uni Eropa. 2012. Komite Luar Negeri: *Draft Report on Siber Security and Siber Defence (2012/2096(INI).*

Stein A. 1993. *Neo-realism and Neo Liberalism: The Contemporary Debate*. New York : Columbia University Press.

S. Rajaratnam School of International Studies Singapore, *Regional Siber Security: Moving*

UNODC (United Nations Office on Drugs and Crime), *Comprehensive Study on Cybercrime*, Draft – February 2013.

Jurnal

Hasenclever, Andreas, Peter Mayer, and Volker Rittberger. 2000. "Integrating Theories of International Regimes." *Review of International Studies* 26, no. 1 (2000): 3-3

Heinl, CH. 2013. "Regional Cyber Security: Moving Towards a Resilient ASEAN Cyber Security Regime". *S Rajaratnam School of International Studies*. 263 : 31-35.

Internet

ASEAN Secretariat, *ASEAN's Cooperation On Siber Security and against Siber Crime.* France, 4 December 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Sibercrime/Octopus2013/Presentations/Workshop1/ASEAN's_Cooperation_on_Sibercrime_and_Sibersecurity.pdf, diakses pada tanggal 5 April Pk. 09.54 WIB.

Mark Mazzetti and David E. Sanger. 2013. The New York Times, *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-siberattacks-pose-threat-to-us.html?pagewanted=all, diakses pada 05 April 2014 Pk 05.45 WIB.