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 3 | Number 2 | July - December 2019

Jurnal Asia Pacific Studies
http://dx.doi.org/10.33541/japs.v3i1.1081
Volume 3 Number 2 / July – December 2019
pp. 181-192

STRATEGI KEAMANAN *CYBER SECURITY* DI KAWASAN ASIA TENGGARA: *SELF-HELP* ATAU *MULTILATERALISM?*

Iqbal Ramadhan

Program Studi Hubungan Internasional, Universitas Pertamina

iqbal.ramadhan@universitaspertamina.ac.id

Abstract

Cyber security is a new kind of topic in security studies. This issue came as prominent discourse when all the human aspect range from politics, military, economics and societal are connected to the cyber space. Cyber terrorism, cyber crime and cyber war are the most potential threat who come from the cyber world. As the strategic region in the world, South East Asia who has promising economic growth cannot escape from those threats. The aim of this research is to explain what kind of strategy that can be implemented in protecting the cyber security of South East Asia. To answer the research question, the author used mainstream approach such neorealism and neoliberalism. From the author's perspective, ASEAN countries need to develop their technological power without ignoring the weightiness of interstate cooperation.

Keywords: *cyber security, neorealism, neoliberalism, security studies, South East Asia*

Abstrak

Keamanan *cyber* pada hakikatnya merupakan isu dalam studi keamanan yang terbilang masih sangat baru. Isu ini muncul ketika semua aspek kehidupan politik, militer, ekonomi, sosial dan budaya terhubung ke dunia maya. Ancaman *cyber* yang berpotensi sebagai ancaman adalah *cyber terrorism, cyber crime* dan *cyber war*. Asia Tenggara sebagai salah satu kawasan penting di dunia dengan tingkat pertumbuhan ekonomi yang cukup tinggi tidak terlepas dari ancaman tersebut. Penelitian ini bertujuan untuk membahas strategi seperti apakah yang paling tepat dalam menjaga keamanan *cyber* di kawasan Asia Tenggara. Dalam menjawab *research question*, peneliti menggunakan pendekatan *mainstream* seperti neorealism dan neoliberal. Pada intinya, negara yang tergabung sebagai anggota ASEAN perlu mengembangkan kemampuan *power* teknologinya tanpa mengesampingkan pentingnya kerja sama antar negara.

Kata Kunci: keamanan *cyber*, neorealis, neoliberalis, studi keamanan, Asia Tenggara

1. Latar Belakang

Berbicara tentang studi keamanan, kajian dalam ilmu Hubungan Internasional ini sangatlah menarik. Barry Buzan dalam bukunya yang berjudul *Security: A New Framework of Analysis* menjelaskan bahwa pada masa Perang Dingin, studi keamanan hanya memfokuskan diri pada sektor keamanan bidang politik dan militer. Akan tetapi pada perkembangannya, sektor keamanan semakin meluas dengan masuknya isu lingkungan, ekonomi dan sosial (Buzan, 1998). Di era yang semakin terdigitalisasi seperti saat ini, sektor dalam studi keamanan pun ikut terpengaruh. Joseph S. Nye (2011) menjelaskan bahwa sektor keamanan tidak hanya lima, melainkan enam sektor. Nye menambahkan dalam bukunya yang berjudul *The Future of Power,* siber (*cyber*) perlu mendapatkan prioritas dalam studi keamanan. Ia menjelaskan bahwa dimensi kehidupan negara-bangsa termasuk tatanan sosial yang diatur di dalamnya tidak akan terlepas dari peranan dunia maya. Sehingga mau tidak mau, negara-bangsa perlu memasukkannya sebagai prioritas strategis negara.

Definisi keamanan *cyber* tidak memiliki definisi yang ajeg. Sama seperti definisi keamanan yang dipaparkan oleh Buzan bahwa tidak ada penjelasan yang pasti terkait apa itu "keamanan" (Buzan, 1998). Terlepas dari semua itu, beberapa literatur berupaya menjelaskan apa itu *cyber security*. Roxana Radu memaparkan bahwa *cyber security* merupakan seperangkat kebijakan, alat, instrumen, manajemen risiko dalam mencegah ancaman yang datang dari dunia maya (Radu dalam Kremer & Muller, 2014). Adapun Madeline Carr menjelaskan dalam jurnalnya yang berjudul *Crossed Wires: International Cooperation on Cyber Security* bahwa keamanan *cyber* merupakan permasalahan *post-state*. Artinya adalah keamanan *cyber* merupakan bentuk ancaman yang tidak bisa ditangani menggunakan paradigma *Westphalia* yaitu mengatasi ancaman melalui instrumen negara seperti militer. Carr menegaskan bahwa ancaman yang datang dari dunia maya bersifat *borderless* dan tidak terlihat namun dampaknya sangat terasa (Carr, 2015).

Bagaimana kedudukan keamanan *cyber* dalam konteks relasi antar negara? Nir Kshetri dalam tulisannya yang berjudul *Cyber Security and International Relations: The US Engagement with China and Russia* mengatakan bahwa keamanan negara tidak hanya di darat, laut, udara dan militer, tetapi juga di dunia maya (Kshetri, 2011). Lebih lanjut Kshetri mengatakan bahwa hubungan bilateral antar negara saat ini sangat terpengaruh oleh aktifitas yang dilakukan aktor-aktor tersebut di ranah maya. Salah satu contohnya adalah bentuk *cyber espionage* ataupun pencurian data serta upaya melumpuhkan sistem informasi negara oleh negara lain untuk mendapatkan keuntungan politik atau ekonomi (Kshetri, 2011). Seperti yang telah dijelaskan sebelumnya oleh Nye, setiap dimensi kehidupan yang diatur dan dikelola oleh negara telah terdigitalisasi. Dengan demikian, tidak tertutup kemungkinan bentuk ancaman yang datang dari aktor negara di dunia maya adalah sesuatu yang mudah terjadi.

Tipologi ancaman terhadap keamanan *cyber* dapat bermacam-macam. Myriam Dunn Cavelty menjelaskan ancaman tersebut ke dalam tiga tipologi. Contoh tipologi tersebut adalah *cyber crime, cyber war* dan *cyber terrorism* (Cavelty dalam Mauer dan Cavelty, 2010). Kejahatan *cyber* adalah aktifitas kejahatan yang menggunakan teknologi informasi untuk mencapai kepentingan ekonomi yang dilakukan oleh organisasi kriminal. Sedangkan *cyber war* adalah bentuk perang Von Clausewitz versi digital. Adapun *cyber terrorism* adalah kegiatan peretasan ataupun pelumpuhan sistem informasi negara-bangsa yang dilakukan oleh kelompok terorism (Cavelty dalam Mauer dan Cavelty, 2010). Di satu sisi, Jonathan D. Aronson memberikan tiga tipologi berbeda yaitu *intelligence gathering, hacking* dan *cyber war* (Aronson dalam Bayliss, 2005). Aronson memaparkan tipologi tersebut sebagai ancaman yang melibatkan aksi spionase digital, peretasan sistem informasi dan kemampuan negara-

bangsa untuk melumpuhkan sistem pertahanan negara oleh aktor negara lainnya (Aronson dalam Bayliss, 2005).

Bentuk ancaman yang dipaparkan di atas dapat mengancam siapapun tanpa terkecuali, termasuk negara-negara yang berada di kawasan Asia Tenggara. Pada dasarnya, ASEAN telah memiliki ASEAN ICT Masterplan 2012 yang bertujuan untuk mengamankan sistem informasi dalam menyambut Masyarakat Ekonomi ASEAN 2015 (Ramadhan, 2017). Pengamanan sistem informasi tersebut dilakukan menggunakan format *sharing knowledge* antar negara ASEAN untuk saling membantu dalam mengamankan jaringan sistem informasi negara anggota. Pada akhirnya, ASEAN ICT Masterplan 2012 memiliki *output* untuk dapat menghasilkan *guideline* yang dapat diimplementasikan pada *level* negara anggota karena ASEAN pada dasarnya menganut prinsip non-intervensi (Ramadhan, 2017).

Namun demikian, persoalan keamanan *cyber* di Asia Tenggara masih sangat jauh dari kata sempurna. Perlu ditekankan bahwa keamanan *cyber* ini pada hakikatnya berdampak signifikan terhadap perkembangan ekonomi digital yang ada di ASEAN. Pada tahun 2025, perkembangan ekonomi digital di ASEAN akan mencapai 102 miliar dolar AS (E-Trade for All, 2018). Hal ini relevan dengan yang dipaparkan oleh para ahli ekonomi bahwa pangsa pasar ekonomi digital pada tahun 2018 saja meraup keuntungan hingga 20 miliar dolar AS (ASEAN-UP, 2019). Serangan *cyber* terhadap sistem informasi yang ada di Asia Tenggara setidaknya dapat menimbulkan disrupsi dan gangguan terhadap perekonomian digital di wilayah tersebut. Oleh karenanya, negara-negara anggota ASEAN tidak bisa abai dari adanya ancaman *cyber* tersebut.

Saat ini penguasaan teknologi informasi yang ada di Asia Tenggara dikuasai oleh Singapura. Walaupun Singapura menjadi pusat TI di seluruh Asia Tenggara, pada kenyataannya negara itu adalah salah satu target dari serangan *cyber*. Berdasarkan data yang dikumpulkan oleh Tech Collective, Singapura pada tahun 2018 menderita kerugian ketika 19.000 data kartu kredit nasabah mereka bocor dan diperjualbelikan di Internet (Kr-Asia, 2018). Tidak hanya di Singapura, Vietnam pun harus mengalami kebocoran data ketika 410.000 data pengguna Vietnam Airlines diretas oleh *hacker*. Berdasarkan hasil investigasi, Malaysia pun mengalami kebocoran data di mana ribuan pengguna Jobstreet.com dicuri oleh peretas (Lago, 2018). Mengacu pada laporan Asia Pacific Risk Centre, kerugian akibat ancaman *cyber* ini berpotensi menimbulkan kerugian sebesar 2.1 triliun dolar AS di tahun 2019 (Ariffin, 2018).

Permasalahan yang dihadapi di Asia Tenggara adalah masih belum meratanya kemampuan teknologi informasi dari masing-masing negara anggotanya. Melihat fenomena tersebut, Asia Tenggara memiliki kerentanan keamanan *cyber* yang harus dibenahi. Seperti yang telah dipaparkan sebelumnya, penguasaan teknologi kini masih berfokus pada Singapura. Ketimpangan teknologi tersebut menjadi beban ketika yang terancam bukan negara tersebut. Bagaimana jika serangan *cyber* justru menyerang negara seperti Laos atau Myanmar? Setiap ancaman *cyber* yang muncul bersifat holistik. Artinya ancaman itu berdampak pada setiap negara yang berada di Asia Tenggara. Negara di Asia Tenggara tentunya perlu mengembangkan kemampuan teknologinya selain membangun kerja sama antar negara. Kondisi negara di ASEAN dihadapkan pada dua pilihan. Secara mahzab neo-realisme khususnya konsep *defensive realism*, semua negara memiliki kepentingan untuk *survive* dalam tatanan politik global. Mengacu pada asumsi dasar konsep tersebut, setiap negara memiliki hak untuk mengembangkan kemampuan militer, ekonomi dan teknologi tidak untuk menjadi *revisionist state*, melainkan mempertahankan kelangsungan hidup mereka (Elman & Jensen dalam Williams, 2013). Berbanding terbalik dengan *defensive realism*, neo-liberal institusionalisme justru memandang ancaman harus ditangkal dengan kerja sama antar negara yang terejawantahkan dalam bentuk institusi/organisasi internasional. Robert Keohane secara gamblang menjelaskan bahwa memitigasi risiko ancaman tidak hanya

mengandalkan *self-help* negara, tetapi juga membutuhkan koordinasi dan kerja sama antar negara (Navari dalam Williams, 2013). Namun demikian, manakah strategi yang paling baik? Inilah yang menjadi *research question* dalam jurnal ini. Rumusan masalah yang dipaparkan di dalam jurnal ini adalah: **strategi apa yang dapat digunakan oleh negara untuk menjaga keamanan *cyber* di Asia Tenggara? Apakah model *defensive-realism* versi neo-realisme atau kerja sama multilateral versi liberal institusionalisme?**

2. Tinjauan Pustaka

Pada hakikatnya, penelitian dalam tulisan ini memfokuskan pada area kajian keamanan. Konsep dan *point of view* kajian keamanan yang digunakan oleh penulis menggunakan pendekatan *Copenhagen School*. Kajian keamanan ini dicetuskan oleh Barry Buzan dan Ole Weaver. Mereka berdua mengembangkan studi yang sangat komprehensif dan detail terkait keamanan tradisional maupun non-tradisional. Konsep-konsep keamanan yang digunakan dalam penelitian ini antara lain *threat*, *referent object*, *security sector*, dan *vulnerability* (Buzan dkk, 1998). Secara definisi *threat* (ancaman) adalah segala sesuatu yang menghalangi negara atau individu mencapai tujuan atau kepentingannya. Sedangkan *referent object* adalah aktor yang sering menjadi target ancaman. *Referent object* dapat berwujud dalam bentuk individu, aktor non-negara maupun negara itu sendiri (Buzan dkk, 1998). Terkait dengan *security sector*, Buzan membaginya menjadi lima sektor yaitu militer, politik, ekonomi, sosial dan lingkungan. Adapun *vulnerability* merupakan ketidakmampuan *referent object* dalam mengatasi ancaman yang dapat menganggu kepentingan nasionalnya (Buzan dkk, 1998). Pendekatan *Copenhagen School* tersebut menjadi acuan dalam menjawab *research question* yang ada dalam penelitian ini.

Teori yang digunakan dalam penelitian ini adalah neo-realisme dan neo-liberal. Dari kedua teori besar tersebut, peneliti menggunakan konsep *defensive realism* dan *multilateralism*. Untuk menjawab *research question* yang diajukan, kedua teori di atas memiliki asumsi dasar yang berbeda dalam memandang ancaman dalam kajian keamanan. Secara teoritis, neo-realisme merupakan turunan dari realisme yang mana teori tersebut berkembang pada dekade 1970-an (Viotti & Kauppi, 2014). Neo-realisme muncul melalui tokoh utamanya, Kenneth Waltz, yang menolak asumsi realisme versi Morgenthau yang menyatakan bahwa tujuan utama negara dalam tataran politik global adalah mencapai *power*. Waltz menjelaskan bahwa *power* hanya sekadar alat untuk mencapai tujuan utama negara yaitu *survive* (Viotti & Kauppi, 2014). Waltz sendiri merupakan "pencetus" munculnya *defensive realism*. Ada tiga asumsi dasar *defensive realism* yang akan digunakan dalam penelitian ini yaitu, negara dapat memanfaatkan kemampuan teknologi maupun aspek geografis untuk membantu pertahanan mereka. Poin ketiga adalah peningkatan kekuatan untuk mendukung *status quo* bukan menjadi negara revisionis karena tujuan utama negara adalah *survive* (Elman & Jensen dalam Williams, 2013). Tiga asumsi dasar tersebut akan dijadikan rujukan dalam menganalisis *research question* terkait bagaimana negara melihat ancaman dan cara memitigasinya.

Selain penggunaan *defensive realism*, penulis menggunakan pula konsep multilateralisme yang sering digunakan oleh mahzab neo-liberal khususnya institusionalisme. Ada beberapa asumsi dasar yang tentunya dijadikan rujukan bagi peneliti untuk menjawab *research question* melalui sudut pandang neo-liberal institusionalisme. Robert Axelrod menjelaskan bahwa multilateralisme mendorong terjadinya kerja sama strategi antar negara khususnya dalam menyelesaikan isu yang bersifat strategis. Poin lainnya yang dipaparkan oleh Axelrod adalah kondisi dunia bersifat anarki yang mengakibatkan negara berada dalam posisi *prisoner dilemma* (Navari dalam Williams, 2013). Menurut Axelrod, posisi tersebut

memaksa negara untuk bekerja sama satu sama lain karena isu dan permasalahan yang dihadapi oleh mereka semakin kompleks sehingga mau tidak mau negara akan membentuk organisasi internasional. (Navari dalam Williams, 2013). Di satu sisi, Robert Keohane menambahkan bahwa kerja sama multilateral perlu dibentuk dalam bentuk institusi internasional. Pembentukan institusi tidak terlepas dari kemudahan dalam bertukar informasi dan resolusi konflik. Keohane menekankan bahwa institusi internasional dapat berjalan sebagaimana mestinya dengan implementasi negosiasi diplomasi, penguatan perjanjian antar negara dan pembentukan norma internasional. Lebih lanjut, neo-liberal institusionalisme ini melihat bahwa persoalan keamanan tidak bisa diatasi oleh negara secara *self-help*, melainkan perlu koordinasi dan kerja sama di antara negara yang ada di dunia (Navari dalam Williams, 2013).

3. Metodologi Penelitian

Paradigma dalam penelitian ini menggunakan paradigma *pragmatism*. Apa itu paradigma *pragmatism*? Menurut John W. Creswell, *pragmatism* merupakan paradigma penelitian yang menitikberatkan pada *research question* bukan pada aspek metodologi seperti yang difokuskan oleh paradigma positivisme (Creswell, 2007). Paradigma pragmatisme pada hakikatnya akan menjawab *research question* dalam tataran praktis yang dapat dijadikan sebuah solusi (Creswell, 2007). Kelebihan dalam paradigma adalah peneliti bebas untuk memilih metodologi, cara pengambilan data ataupun teknik analisis yang tentunya sesuai dengan kebutuhan mereka (Creswell, 2007). Hal lainnya yang menjadi fokus dalam paradigma ini adalah rumusan masalah dalam penelitian berbasis paradigma menitikberatkan pada "apa" dan "bagaimana" serta apa yang akan dilakukan dari hasil penelitian tersebut (Creswell, 2007). Penelitian ini pada dasarnya membahas tentang bagaimana strategi negara-bangsa di ASEAN mengantisipasi ancaman yang dapat menganggu stabilitas keamanan *cyber* di Asia Tenggara. Melalui paradigma pragmatisme, simpulan dari rumusan masalah tersebut dapat menjadi salah satu acuan dalam membangun strategi keamanan *cyber* di antara anggota negara ASEAN.

Dalam menganalisis permasalahan yang ada di dalam penelitian ini, peneliti menggunakan metodologi kualitatif. Creswell mengatakan bahwa metodologi kualitatif digunakan untuk menganalisis sebuah fenomena sosial menggunakan berbagai macam teori ataupun penelitian terdahulu serta memandang penting *point of view* dalam melihat permasalahan yang sedang dianalisis (Creswell & Creswell, 2015). Penggunaan metodologi kualitatif tidak bisa menafikkan aspek *reflexivity*. Sebuah konsep yang menegaskan bagaimana sudut pandang peneliti memandang fenomena sosial yang beranjak dari pendekatan teori, data hasil observasi ataupun penelitian terdahulu (Creswell & Creswell, 2015). Melalui metodologi tersebut, peneliti dapat mengelaborasi berbagai macam data yang dapat memperkuat argumen peneliti dalam menjawab *research questions* terkait strategi keamanan *cyber* di Asia Tenggara. Adapun pendekatan penelitian menggunakan *case study* dengan *embedded analysis* sebagai teknik analisis penelitian. *Case study* digunakan untuk menganalisis, menjelaskan dan mendeskripsikan fenomena sosial yang terjadi di masyarakat serta bertujuan untuk mencari solusi atau makna dari fenomena tersebut (Creswell, 2007). Sedangkan *embedded analysis* adalah bagian teknik analisis dari *case study* yang bertujuan untuk menganalisis suatu kasus secara lebih mendalam tidak bersifat holistik atau meluas (Creswell, 2007). Pada penelitian ini, peneliti menggunakan pendekatan studi kasus di tingkat regional ASEAN dengan cara menganalisis *level of analysis* yaitu *nation-state* secara satu kesatuan sebagai anggota organisasi ASEAN.

4. Ancaman Keamanan *Cyber*

Bentuk ancaman *cyber* yang dapat mendisrupsi stabilitas politik dan ekonomi ASEAN dapat muncul dalam beragam bentuk. Salah satu bentuk ancaman yang dapat mengganggu stabilitas tersebut adalah *cyber terrorism*. Pada jurnal yang ditulis oleh Kobuye Oluwafemi Samuel dan Wan Rozaini Sheik Osman dalam jurnalnya yang berjudul *Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consquences and Panacea* mengatakan bahwa *cyber terrorism* adalah sebuah aktifitas kelompok teroris yang mendisrupsi keamanan teknologi informasi sebuah negara dengan cara menyebarkan rasa takut untuk memperoleh keuntungan politik (Samuel & Osman, 2010). Menurut mereka, kelompok teroris di era digital saat ini dapat melumpuhkan sistem informasi setiap negara ataupun mencuri data tanpa harus memiliki peralatan teknologi yang canggih. Penelitian tersebut mengatakan bahwa saat ini banyak diperjualbelikan *malware* yang dapat digunakan untuk melumpuhkan sistem teknologi informasi negara (Sameul & Osman, 2010). Namun demikian, Joseph S. Nye menyangsikan bahwa *cyber terrorism* dapat melumpuhkan sistem informasi, ekonomi dan pertahanan sebuah negara karena keterbatasan sumber daya. Walaupun begitu, Nye tetap memberikan penekanan pada negara untuk tidak menutup mata terhadap ancaman *cyber terrorism* tersebut (Nye, 2011).

Ancaman lainnya yang perlu diwaspadai oleh negara-negara di kawasan Asia Tenggara adalah *cyber war* dan *cyber crime*. Perang siber atau *cyber war* merupakan bentuk digitalisasi perang antar negara versi Von Clausewitz. *Cyber war* dapat menjadi ancaman karena pada dasarnya di era digital saat ini alat-alat tempur telah terhubung ke dunia maya (Albert & Papp, 2001). Daniel S. Papp dan David Albert secara tegas menjelaskan bahwa aspek digital telah mengubah strategi perang antar negara. Apabila sebuah negara tidak mampu mengamankan aspek digital dalam bidang pertahanan, maka hal itu tidak menutup kemungkinan negara lain dapat memanfaatkan kerentanan yang ada (Albert & Papp, 2001). Ketika *cyber war* terjadi dan negara tidak memiliki kemampuan untuk melakukan serangan balik atau mempertahankan diri, maka keamanan militer mereka pasti terancam. Negara yang tidak dapat mempertahankan dirinya dari serangan musuh pada saat perang berlangsung sudah dipastikan bahwa mereka akan mudah dikuasai oleh negara lain. Oleh karenanya, negara perlu mempersiapkan diri dari ancaman *cyber war* karena di era digital perang kini lebih bersifat *proxy war*. Kemampuan untuk melumpuhkan negara lain tidak perlu dilakukan secara langsung, melainkan dengan cara menggunakan negara satelit baik secara sadar ataupun tidak (Albert & Papp, 2001). Terlebih lagi, dunia maya memiliki kemampuan anonim yang dapat menyamarkan jejak pengguna Internet.

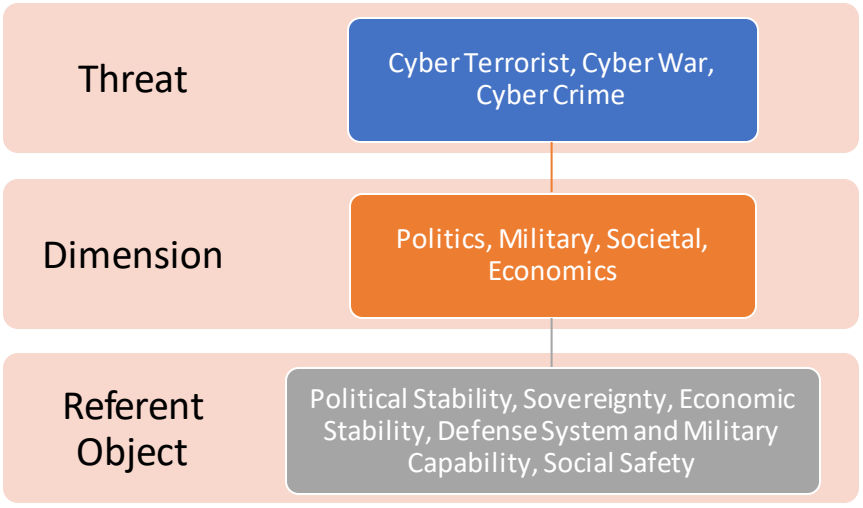
Negara tidak hanya perlu mewaspadai, ancaman *cyber terrorism* dan *cyber war*. Dimensi sosial pun terancam dengan semakin maraknya *cyber crime* yang menjadi ancaman utama di dunia maya. Melihat kondisi ASEAN yang kini menjadi pusat dari pasar *e-commerce*, potensi tersebut dapat dimanfaatkan oleh organisasi kriminal untuk mengeruk keuntungan dengan cara-cara ilegal. Penelitian yang dilakukan oleh Lennon Chang dengan judul *Cyber Crime and Cyber Security in ASEAN* menjelaskan bahwa wilayah Asia Tenggara terdeteksi memiliki tingkat populasi *cyber crime* sebanyak 10 persen di seluruh regional Asia-Pasifik (Chang, 2017). Lebih lanjut, Chang memaparkan bahwa Thailand dan Malaysia terindikasi memiliki komputer yang disusupi *malware* dengan total populasi sebanyak 35 persen. Sedangkan Filipina memiliki total populasi *malware* sebanyak 47,7 persen. Adapun Vietnam dan Indonesia memiliki populasi *malware* sebanyak 50,7 dan 60 persen (Chang, 2017). *Malware* sendiri adalah program komputer yang diciptakan untuk menyusup dan mencuri data ataupun informasi keuangan. Peter Hough mengemukakan bahwa organisasi

kriminal memanfaatkan fleksibilitas dan anonimitas Internet untuk menyembunyikan aksi kejahatan yang mereka lakukan. Mereka tidak hanya mencuri uang menggunakan komunikasi enkripsi, tetapi juga menutupi transaksi ilegal seperti penjualan narkoba, perdagangan manusia dan jual beli senjata ilegal (Hough, 2008).

Melihat dari tiga ancaman besar di atas, peneliti melihat bahwa *cyber threat* yang dapat mengancam stabilitas kawasan Asia Tenggara memiliki dimensi keamanan yang berbeda. Namun demikian, semua dimensi keamanan tersebut bertautan satu sama lain. *Cyber terrorism* pada dasarnya tidak bermotif ekonomi melainkan politik. Kelompok teroris pada dasarnya menyebarkan rasa takut untuk mengganggu stabilitas politik yang kemudian akan mereka ganti sesuai dengan ideologi politik mereka. Pada aspek *cyber war*, negara tetap menjadi *referent object* ketika kedaulatan mereka terancam oleh negara lain. Perang siber mengancam tidak hanya kedaulatan negara secara politik, melainkan juga kemampuan tempur negara. Ketika semua sistem pertahanan telah terintegrasi ke dalam sistem informasi, maka akan muncul kerentanan yang dapat dieksploitasi lawan mereka apabila sistem mereka tidak ter-*update*. Di sisi lain, perekonomian negara dan keselamatan warga negara menjadi *referent object* tatkala organisasi kriminal memanfaatkan teknologi untuk melaksanakan aksi kejahatan mereka. Dengan demikian, *cyber threat* bukan lagi sebuah *perceive threat* melainkan telah menjadi *real threat* yang harus mendapatkan perhatian dari setiap negara anggota ASEAN.

Secara sistematis, ancaman *cyber* yang berpotensi menjadi ancaman negara-negara ASEAN dapat digambarkan dalam alur di bawah ini:

Tabel 1. Potensi Ancaman Cyber di Asia Tenggara



Pada dasawarsa 1990-an Kenneth Waltz mengatakan bahwa Perang Dingin yang telah berlangsung lebih dari 30 tahun telah berakhir. Ia menjelaskan bahwa persaingan antar negara akan semakin kompleks. Poin penting yang ditekankan oleh Waltz adalah negara-bangsa tidak lagi terpaku pada persaingan senjata, melainkan juga ekonomi dan teknologi. Dalam tulisannya yang diterbitkan dalam *International Security*, Waltz menyimpulkan bahwa negara yang dapat menguasai aspek politik, militer, ekonomi dan teknologi akan menjadi salah satu *the next superpower* (Waltz, 1993). Melihat dari aspek kekinian, pendapat Waltz tersebut tidaklah salah. Saat ini negara-bangsa berlomba-lomba untuk menjadi penguasa terdepan dalam penguasaan teknologi. Saat ini penguasaan teknologi dikuasai oleh Amerika Serikat, Jepang dan India (Tiwari, 2017).

Penguasaan teknologi tentunya berkorelasi pula dengan keamanan *cyber* yang menjadi pokok pembahasan dalam tulisan ini. Asumsi dasar pertama yang dijadikan rujukan dalam

penelitian ini adalah, "negara dapat memanfaatkan kemampuan teknologi maupun aspek geografis untuk membantu pertahanan mereka." Kemampuan teknologi dalam memitigasi ancaman *cyber* yang datang silih berganti dapat dikembangkan melalui pengembangan sumber daya manusia. Tidak bisa dimungkiri bahwa manusia merupakan sumber daya yang paling terpenting dalam memajukan teknologi di setiap negara yang ada di Asia Tenggara. Inovasi yang muncul setiap saat merupakan bukti bahwa negara maju merupakan negara yang peduli terhadap perkembangan sumber daya manusianya. Negara di Asia Tenggara setidaknya patut mencontoh program India dalam memajukan aspek teknologi informasi di negaranya dengan memberikan banyak pelatihan dan beasiswa (Europe, 2018). Hal ini berimbas pada banyaknya diaspora India yang menjadi CEO di beberapa perusahaan teknologi seperti Sunai Pichai di Google ataupun Satya Nadella di Microsoft (Koran Sindo, 2019).

Tujuan pengembangan manusia dalam konsep *defensive realism* tidak terlepas kepentingan negara untuk memajukan teknologi dalam mengantisipasi ancaman *cyber*. Ketika negara dapat memajukan kemampuan teknologinya, setidaknya negara tersebut dapat menciptakan inovasi yang dapat diimplementasikan di industri pertahanan. Industri strategis seperti pertahanan membutuhkan teknologi sebagai salah satu *support* untuk menjaga kedaulatannya. Selain itu, inovasi yang dilakukan dapat menciptakan pula teknologi yang dapat mengantisipasi serangan *cyber* seperti *malware* ataupun *cyber espiionage*. Pada saat negara dapat mengembangkan kemampuan sumber daya manusia dalam bidang teknologi, setidaknya negara dapat berdikari secara *self-help* untuk menjaga kepentingan nasionalnya. Apabila negara terlalu bergantung sepenuhnya pada bantuan teknologi luar negeri, kepentingan nasional negara tersebut dapat dengan mudah diintervensi. Setidaknya dalam pengembangan teknologi, negara-bangsa dapat memulainya dengan membangung manusianya terlebih dahulu.

Negara yang secara teknologi sangat maju, setidaknya kekuatan mereka pun mulai diperhitungkan. Seperti yang telah dipaparkan oleh Kenneth Waltz sebelumnya bahwa kekuatan negara tidak lagi diukur dari aspek militernya saja, tetapi juga kemampuan teknologinya. Sesuai dengan asumsi *defensive realism*, peningkatan kekuatan teknologi tidak diperuntukkan menjadi *revisionist state*. Peningkatan teknologi yang perlu dikembangkan oleh negara di Asia Tenggara tidak terlepas dari kepentingan mereka untuk *survive* dari ancaman *cyber terrorism*, *cyber crime* ataupun *cyber war*. Secara kultur, negara di Asia Tenggara bukanlah negara ekspansionis yang sangat bercorak kolonialistik. Mereka perlu mengembangkan kemampuan teknologi tidak terlepas dari kenyataan yang ada bahwa ancaman *cyber* suatu saat dapat melumpuhkan kestabilan keamanan politik, negara, maupun ekonomi yang ada di Asia Tenggara. Pada saat pengembangan teknologi untuk memitigasi ancaman *cyber*, negara-negara di Asia Tenggara pun perlu menakar kemampuan mereka untuk tidak dianggap sebagai *revisionist state*. Bagaimanapun juga, pada tataran politik global saat ini negara *status quo* tidak ingin kehilangan pengaruhnya. Negara yang dianggap sebagai *revisionist state* pada hakikatnya akan dianggap sebagai ancaman yang dapat mengganggu eksistensi mereka. Kekuatan teknologi yang dikembangkan diperuntukkan sebagai acuan bagi negara di Asia Tenggara dalam menjaga keamanan *cyber* mereka. Tujuan utamanya adalah *survive* dan bukan untuk menjadi *revisionist state*.

5. Kerja sama Multilateral dalam Penanganan Ancaman *Cyber*

Robert Axelrod pada penjelasan sebelumnya mengatakan bahwa negara-bangsa pada saat ini mengalami sebuah posisi *prisoner dilemma*. Ancaman yang datang kini semakin kompleks dan pelik. Hal ini ditambahkan pula oleh Robert Keohane bahwa negara-bangsa tidak bisa lagi bersifat *self-help* dan perlu memperhatikan kerja sama antar bangsa untuk

mengatasi setiap permasalahan yang ada. Di kawasan Asia Tenggara sendiri, ASEAN menjadi salah satu soko guru utama dalam mengembangkan kerja sama yang bersifat strategis. Organisasi regional tersebut dapat menjadi wadah utama dalam memfasilitasi kerja sama multilateral yang terintegrasi dalam institusi internasional. Melalui kerja sama multilateral di tingkat ASEAN, negara anggota yang di dalamnya dapat mengkonsepkan rencana strategis untuk menjaga keamanan *cyber* di Asia Tenggara sekaligus mendorong terciptanya Masyarakat Ekonomi ASEAN yang kondusif.

Kerja sama multilateral ini tidak dapat dihapuskan begitu saja dalam membangun strategi keamanan *cyber* di Asia Tenggara. Ada tiga *point of view* yang dapat dicapai dari sudut pandang peneliti dalam mencapai keamanan *cyber* yang kondusif. Pandangan pertama mengutip asumsi dasar neoliberal institusionalisme itu sendiri bahwa institusi internasional berfungsi untuk mewadahi kerja sama multilateral dalam mencapai *common interest*. Pada konteks keamanan *cyber*, negara dapat menjadikan ASEAN sebagai tempat untuk memetakan ancaman yang berasal dari dunia maya. Melalui pola kerja sama seperti ini, negara anggota dapat menyamakan persepsi terkait ancaman *cyber* seperti apa yang berpotensi menganggu kestabilan politik dan perekonomian di Asia Tenggara. Tidak hanya memetakan ancaman, ASEAN dapat menjadi media pula dalam mencari solusi yang tepat mengatasi ancaman *cyber* tersebut yang sesuai dengan kepentingan nasional masing-masing negara.

Aspek pengembangan kerja sama tidak hanya bertujuan untuk melakukan pemetaan terkait ancaman *cyber*. Organisasi ASEAN dapat mewadahi kerja sama multilateral untuk menjembatani kesenjangan teknologi yang ada di antara negara anggotanya. Seperti yang telah dipaparkan dalam penjelasan sebelumnya, teknologi yang dimiliki oleh negara anggota ASEAN sangatlah timpang. Penguasaan teknologi saat ini masih dikuasai oleh Singapura. Namun demikian, ASEAN dapat menjembatani kesenjangan tersebut dengan mengoptimalkan kerja sama strategis dalam hal *sharing technology*. Singapura sebagai negara yang memiliki teknologi canggih dapat menjadi pemimpin dalam kerja sama tersebut. Organisasi ASEAN pada dasarnya tidak menerapkan asas intervensi. Setidaknya Singapura dapat menjadi mentor dan pemandu dalam mengembangkan teknologi informasi di antara sesama negara anggota. Metode yang digunakan dapat berupa *technical assistance* dalam membuat panduan keamanan *cyber* yang dapat disesuaikan dengan kebutuhan masing-masing negara. Selain itu, Singapura perlu menjadikan negaranya untuk menjadi salah satu *hub* pengembangan sumber daya manusia dalam bidang teknologi informasi.

Aspek yang tak kalah pentingnya dalam pengembangan kerja sama multilateral dalam bidang kerja sama *cyber* adalah *sharing information*. Mengacu pada asumsi dasar neoliberal institusionalis bahwa organisasi internasional perlu dibangun untuk mengejar kepentingan bersama, ASEAN harus menjadi pelindung keamanan *cyber* negara anggotanya. Patut ditekankan dalam penanggulangan ancaman *cyber* tersebut adalah bentuk ancaman di dunia maya bersifat asimetris dan *proxy*. Secara harafiah, ancaman itu sangat sulit untuk dikenali karena bersifat anonim. Sebagai satu-satunya organisasi regional di Asia Tenggara, ASEAN perlu membuat panduan dalam *sharing information* untuk menangkal segala bentuk ancaman *cyber*. Pada hakikatnya, ancaman *cyber* bukanlah tipologi ancaman yang bisa ditangkal secara individual negara. Ancaman tersebut perlu ditangkal melalui peran aktif kerja sama negara anggota ASEAN. Ketika muncul sebuah serangan yang melumpuhkan satu negara anggota, maka dampaknya akan berimbas pada negara anggota lainnya. Hal ini mendorong pentingnya *sharing information* di antara negara anggota ASEAN untuk saling bekerja sama secara multilateral dalam rangka menangkal ancaman *cyber*.

6. Sinergi Strategi Kebijakan

Berbicara tentang strategi kebijakan negara anggota ASEAN dalam menangkal ancaman *cyber* tentunya tidak dapat dimungkiri bahwa sektor-sektor dalam studi keamanan perlu dipertimbangkan. Secara pendekatan *Copenhagen School*, ancaman *cyber* berpotensi mengancam *referent object* dalam aspek politik, militer, sosial, dan ekonomi. Setiap sektor memiliki *referent object* yang berbeda satu sama lain. Namun begitu, semua sektor tersebut terhubung satu sama lain dan perlu dijaga secara holistik. Satu serangan *cyber* yang destruktif dapat melumpuhkan koordinasi di antara negara-negara Asia Tenggara. Sebagai aktor HI yang sangat "sakral", negara dihadapkan pada banyak pilihan. Negara dapat berdiri sendiri untuk menjaga keamanan negara di dunia maya atau memanfaatkan kerja sama multilateral yang terwadahi di bawah lembaga ASEAN.

Dikaji secara teori neorealis, negara berhak mengembangkan kepabilitas militer, politik, ekonomi dan sosial budayanya untuk *survive* di tengah kancah politik global yang anarki. Pengembangan kapabilitas teknologi informasi negara dipandang sebagai langkah untuk menjaga eksistensinya dan bukan untuk menjadi negara *revisionist*. Sejatinya negara anggota ASEAN tidaklah memiliki pengaruh dan kekuatan politik seperti layaknya Amerika Serikat atau Rusia. Walaupun demikian, negara berhak untuk mengembangkan kemampuan teknologi informasinya. Dengan mengembangkan kapabilitas tersebut, setidaknya negara dapat berdikari secara *power* dan tidak terlalu mengandalkan peran negara lain. Sayangnya, ancaman *cyber* tidak dapat diatasi sendiri. Pola *self-help* seperti itu tidak terlalu relavan dalam mengatasi ancaman *cyber* yang sangat dinamis dan anonim. Kemandirian negara dalam pengembangan *power* secara teknologi dapat diperkuat melalui kerja sama multilateral.

Ancaman *cyber* seperti *cyber crime*, *cyber terrorism* ataupun *cyber war* perlu diatasi menggunakan pola kerja sama multilateral. Sudut pandang peneliti tidak terlepas dari bentuk ancaman yang pada dasarnya adalah *real threat* yang harus dihadapi oleh semua aktor negara. Artinya adalah negara manapun memiliki ancaman yang sama terkait serangan *cyber*. Sudut pandang kedua adalah ancaman *cyber* tidak dapat dihadapi sendiri karena negara anggota ASEAN saling ketergantungan. Satu serangan *cyber* pada negara anggota yang lemah secara teknologi tentunya akan berdampak langsung pada negara anggota yang jauh lebih kuat. Poin ketiga yang patut dikaji sebagai langkah strategis negara adalah sifat ancaman *cyber* yang bersifat asimetris dan *proxy*. Ancaman secara asimetris di era digital berarti sangat sulit untuk mendeteksi siapa menyerang siapa. Ketimpangan ini pada dasarnya dapat diatasi melalui *sharing information* di antara negara anggota ASEAN. *Sharing information* tersebut akan memudahkan negara anggota ASEAN untuk saling berkoordinasi satu sama lain. Oleh karenanya, penggabungan strategi pengembangan keamanan *cyber* di Asia Tenggara tidak hanya dilihat dari aspek neorealis, tetapi juga memperhatikan kerja sama multilateral yang diwadahi oleh ASEAN.

7. Kesimpulan

Tidak bisa dimungkiri bahwa strategi yang dapat dikembangkan oleh negara-negara di Asia Tenggara dalam mengantisipasi ancaman *cyber* adalah penggabungan strategi *self-help* versi neorealis dan kerja sama multilateral yang digaungkan oleh neoliberal institusionalis. Secara kemandirian, negara perlu mengembangkan kekuatannya secara teknologi. Hal ini tidak terlepas dari kepentingan nasional setiap negara yang memiliki preferensi tersendiri dalam pengembangan teknologinya. Namun demikian, mengantisipasi ancaman *cyber* yang bersifat dinamis tidak dapat diatasi secara mandiri. Sifat interdependensi yang menaungi negara di kawasan Asia Tenggara mengharuskan adanya pola kerja sama multilateral yang terkoordinasi satu sama lain. Melalui pola kerja sama multilateral tersebut, setidaknya di antara negara anggota ASEAN dapat mencapai *common interest* yang sama dalam

menghadapi ancaman *cyber* yang berpotensi memberikan disrupsi pada kestabilan politik, militer, ekonomi dan sosial di awasan Asia Tenggara.

DAFTAR PUSTAKA

Buku

Albert, David & Papp, Daniel S. (2001). *Information Age Anthology: The Information Age Military*. USA: CCRP Publishing.

Aronso, D. Jonathan. (2005). Causes and consequences of the communication and Internet Revolution dalam John Baylis & Steve Smith (ed), *The Globalization of World Politics: An Introduction to International Relations*. London: Oxford University Press

Buzan, Barry dkk. (1998). *Security: A New Framework of Analysis*. Colorado: Lynne Rienner

Cavelty, Myriam Dunn. (2014). Cyber Threats dalam Victor Mauer & Myriam Dunn Cavelty (ed), *The Routledge Handbook of Security Studies*. New York: Routledge

Creswell, John W. (2007). *Qualitative Studies and Inquiry Method*. California: Sage Publishing

Creswell, John W. & Creswell, J. David. (2015). *Reserach Design: Qualitative, Quantitatve and Mix Methods Design 5th Edition*. London: Sage Publishing

Elman, Colin & Jensen, Michael A. (2013). Realism dalam Paul Williams (ed), *Security Studies: An Introduction (2nd Edition)*. New York: Routledge.

Hough, Peter. (2008). Understanding Global Security, 2nd Edition. London: Routledge Taylor and Francis Group.

Navari, Cornelia. (2013). Liberalism dalam Paul Williams (ed), *Security Studies: An Introduction (2nd Edition)*. New York: Routledge

Nye, Joseph S. (2011). *The Future of Power*. USA: Perseus Book Group

Radu, Roxana. (2014). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace dalam Jan Frederik Kremer & Benedikt Muller (ed), *Cyberspace and International Relations: Theory, Prospect and Challenges*. Bonn: Springer

Viotti, Paul R. & Kauppi, Mark V. (2014). *International Relations Theory (5th Edition)*. England: Pearson

Jurnal

Carr, Madeline. (2015). Crossed Wires: International Cooperation on Cyber Security dalam *Interstate Journal of International Affairs, 2015/2016, Issue II*

Chang, Lennon. (2017). *Cyber Crime and Cyber Security in ASEAN*. Available at https://www.researchgate.net/publication/318474107_Cybercrime_and_Cyber_Security_in_ASEAN/download. DOI: [10.1007/978-3-319-54942-2_10]

Kshetri, Nir. (2014). *Cybersecurity and International Relations: The U.S. Engagement with China and Russia*. Diambil dari Prosiding FLACSO-ISA 2014, University of Buenos Aires, School of Economics, Buenos Aires, Argentina, July 23-25 2014

Ramadhan, Iqbal. (2017). Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber dalam *Jurnal Populis Vol 2 (4) 2017*. ISSN: 2640-4208

Samuel, Kuboye Oluwafemi & Osman, Wan Rozaini Sheik. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consquences and Panacea dalam JCSMC, Vol. 3, Issue. 5.

Website

Ariffin, Eijas. (2018). *Strengthening ASEAN's cybersecurity*. Available at https://theaseanpost.com/article/strengthening-aseans-cybersecurity. [Diakses, 19 Juni 2019]

ASEAN-UP. (2019). *Overview of e-commerce in Southeast Asia [market analysis]*. Available at https://aseanup.com/overview-of-e-commerce-in-southeast-asia/. [Diakses, 19 Juni 2019]

E-Trade for All. (2018). *ASEAN: E-commerce set to dominate the region in 2019*. Available at https://etradeforall.org/asean-e-commerce-set-to-dominate-the-region-in-2019/. [Diakses, 19 Juni 2019]

Kr-Asia. (2018). *Singapore is the most vulnerable to cyber attacks in Southeast Asia: Report* https://kr-asia.com/singapore-is-the-most-vulnerable-to-cyber-attacks-in-southeast-asiareport. [Diakses, 19 Juni 2019].

Lago, Cristina. (2018). *The biggest data breaches in the ASEAN region*. Available at https://www.cio.com/article/3293060/the-biggest-data-breaches-in-the-asean-region.html. [Diakses, 19 Juni 2019]