PERAN INSTITUSI INTERNASIONAL DALAM PENANGGULANGAN ANCAMAN *CYBER*

Iqbal Ramadhan
Dosen Program Studi Hubungan Internasional Universitas Pertamina
Email: iqbal.ramadhan@universitaspertamina.ac.id

ABSTRAK

Artikel ini menjelaskan tentang pengelolaan ancaman cyber dengan menggunakan peran institusi internasional. Ancaman cyber tidak berbatas dan negara sulit mempertahankan keamanannya di era digital. Mengelola ancaman cyber tidak seperti kontrol senjata. Ini juga tidak bisa mengandalkan konsep self-help realis karena ancaman tersebut berasal dari aktor negara dan non-negara. Untuk mengantisipasi ancaman tersebut, kerja sama melalui lembaga internasional sangat penting. Aktor negara dapat saling berbagi informasi dan bekerja sama dalam mengelola ancaman dengan menggunakan lembaga internasional. Di Asia Tenggara, Komunitas Ekonomi ASEAN harus didukung oleh lingkungan cyber yang stabil. Indonesia dan anggota lainnya harus bekerja sama untuk mencegah ancaman cyber yang dapat membahayakan Komunitas Ekonomi ASEAN.

Kata kunci: Ancaman *cyber*, institusi internasional, aktor negara dan non-negara, Indonesia, ASEAN.

ABSTRACT

This article describes about managing cyber threat by using the role of international institution. Cyber threat is borderless and state is hard to maintain its security in digital age. Managing cyber threat is not like arms control. It also cannot rely on realist's self-help concept because the threat comes from state and non-state actor. In order to anticipate the threat, cooperation through international institution is very important. The state actor can share information and cooperate in managing the threat by using international institution. In South East Asia, ASEAN Economic Community must be supported by stable cyber environment. Indonesia and other members should work together to prevent any cyber threat that can jeopardize ASEAN Economic Community.

***Keywords**: Cyber threats, international institutions, state and non-state actors, Indonesia, ASEAN.*

Latar Belakang

Di dunia yang saling terkoneksi saat ini, *cyber* atau dunia maya adalah dunia yang tanpa batas dan diibaratkan seperti *wild west*. Keberadaan *cyber* sendiri tidak bisa dilepaskan dari kehidupan manusia dan kini telah menjadi bagian dari tulang punggung peradaban dunia. Salah satu kantor konsultan ternama dunia, Pricewaterhouse Cooper (PwC) Global pada tahun 2014 yang lalu pernah merilis

tentang keamanan *cyber* di dunia saat ini. Setidaknya ada peningkatan serangan *cyber* pada tahun 2013 dan angka tersebut meningkat pada sebanyak 23 persen pada tahun 2014. Mereka pun memprediksi bahwa jumlah serangan tersebut dapat saja meningkat pada tahun-tahun yang akan datang (Pwc Global, 2014). Persoalan *cyber* bukan lagi permasalahan teknis TI semata, melainkan telah melibatkan aktor-aktor negara.

Walaupun *cyber* adalah dunia yang tanpa batas, kini hampir semua negara telah menggantungkan kehidupannya baik secara politik ataupun ekonomi pada aspek tersebut. Di aspek militer contohnya, kini telah dikenal istilah *cyber defense*. Pakta Pertahanan Atlantik Utara (NATO) telah memasukkan *cyber defense* sebagai bagian dari *collective defense*. Alasan NATO cukup logis. Mereka menjelaskan bahwa ancaman tidak hanya datang secara fisik, tetapi juga dunia maya. *Rogue actor* dalam pandangan NATO dapat memanfaatkan *sophisticated technology* untuk melumpuhkan sektor-sektor kritis suatu negara seperti energi, listrik, air dan perbankan (NATO, 2014). NATO pertama kali memprioritaskan aspek tersebut ke dalam kebijakannya pasca lumpuhnya Estonia pada tahun 2008 akibat serangan *cyber*.

Banyak sekali contoh nyata tentang serangan *cyber* yang berpengaruh pada hubungan bilateral sebuah negara. Salah satu contohnya adalah serangan *hacker* yang disinyalir berasal dari Tiongkok. *Hacker* tersebut berhasil meretas sistem informasi milik Office of Personal Management (OPM), sebuah institusi di AS yang khusus menangani informasi dan data para pegawai pemerintahnya termasuk data staf intelijen. Serangan tersebut berhasil membocorkan 21,6 juta data pegawai AS sehingga membuat berang Presiden Barack Obama (CISO, 2015). Permasalahan itu sempat memaksa Presiden Obama untuk menjatuhkan sanksi ekonomi pada Tiongkok. Walaupun rencana tersebut ditunda karena sejumlah pakar di Gedung Putih mengkhawatirkan sanksi tersebut akan berdampak pada perekonomian AS yang masih bergantung penuh pada pertumbuhan ekonomi Tiongkok.

Penggunaan teknologi informasi tidak hanya digunakan untuk meretas sistem keamanan sebuah negara. Jauh dari itu, dunia *cyber* adalah wadah yang tepat untuk menyimpan *spyware*. Sebuah program yang khusus dibuat untuk memata-matai komunikasi menggunakan media seperti komputer, PC, laptop, tablet ataupun *smartphone*. Hal ini pernah terjadi pada tahun 2015 yang lalu ketika sebuah firma keamanan menemukan adanya *spyware* yang terpasang di sistem informasi sebuah hotel yang dijadikan tempat negosiasi nuklir Iran dengan anggota delegasi lima negara anggota tetap Dewan Keamanan PBB (CISO, 2015). *Spyware* dapat dianalogikan sebagai alat untuk menghimpun informasi secara ilegal dan diam-diam seperti yang lazim digunakan pada masa Perang Dingin. Walaupun secara teknologi, *spyware* jauh lebih canggih dibandingkan teknologi pada zaman itu.

Meningkatnya serangan *cyber* seperti yang dipaparkan oleh laporan PwC menjadi sebuah tanda bahwa isu itu tak lagi sekadar isapan jempol belaka. Di masa globalisasi sekarang ini, keamanan *cyber* layak mendapatkan prioritas utama di samping isu lainnya yang telah lebih dulu hadir seperti politik, militer ataupun ekonomi. Terlepas dari semua itu, keamanan *cyber* memiliki keterkaitan yang sangat erat dengan semua dimensi kehidupan sebuah negara.

Setidaknya ada dua pertanyaan mendasar yang muncul mengapa perlu melakukan penelitian keamanan *cyber* yang melibatkan hubungan interaksi antar negara. Pertanyan pertama adalah mengapa kerja sama antar negara dalam hal keamanan *cyber* perlu dilakukan? Kalaupun harus ada bentuk kerja sama, mengapa peran institusi internasional sangat penting? Di sisi lain, peneliti pun ingin memaparkan seperti apa kerja sama yang bisa dilakukan oleh Indonesia sebagai negara untuk melindungi keamanan *cyber* mereka? Bagaimanapun juga pemerintah Indonesia memiliki peranan yang sangat penting baik di kawasan Asia Tenggara dan juga dunia.

_Cyber S_ebagai Sebuah Ancaman

Kenneth Waltz, salah seorang pemikir HI bermahzab neo-realis pernah mengatakan bahwa pasca Perang Dingin, negara-negara tidak akan lagi berkompetisi dalam perlombaan senjata baik dari kapasitas dan kapabilitas secara militer. Waltz justru menjabarkan bahwa negara akan meningkatkan *power* mereka dalam bidang ekonomi dan teknologi (Waltz, 1993). Dalam tulisannya tersebut, Waltz memaparkan beberapa penjelasan menarik tentang teknologi. Ketika Perang Dingin berlangsung, dunia terbelah menjadi dua kekuatan antara Barat dan Timur. Dua kekuatan terbesar yang dikendalikan oleh AS dan Uni Soviet menjadi poros utama kekuatan dunia saat itu. Kedua negara tersebut berusaha untuk meluaskan pengaruhnya baik secara politik, militer dan ekonomi di negara-negara Dunia Ketiga. Pasca runtuhnya Tembok Berlin dan lunturnya kekuasaan Uni Soviet menjadi "gong" dimulainya peradaban dunia baru.

Beberapa orang percaya bahwa kekuatan liberal akan menjadi penguasa tunggal di dunia. Hal ini tercermin dari para penstudi seperti Francis Fukuyama dalam bukunya *End of History* yang mengatakan bahwa runtuhnya komunisme merupakan embrio dari kemenangan paham liberalisme. Sebaliknya, ada pula yang menyangsikan bahwa liberalisme akan menjadi kekuatan tunggal dunia karena di masa depan mulai bermunculan kekuatan yang dapat menandingi negara Barat. Tesis Samuel Huntington yang berjudul *Clash of Civilization* adalah salah satu kontribusi terbesar dalam studi HI yang menjelaskan bahwa liberalisme akan mendapatkan "lawan sepadan" dari dua kekuatan dunia yaitu Tiongkok dan Islam. Melihat alur politik dunia saat ini, jelas sudah bahwa tesis Huntington terbukti nyata dibandingkan pemikiran Fukuyama.

Adapun Waltz sendiri sudah memprediksikan bahwa beberapa negara akan muncul sebagai kompetitor AS baik secara ekonomi ataupun teknologi. Waltz menjelaskan bahwa bipolar adalah kondisi di mana dunia dalam keadaan "damai". Ketika komunisme runtuh, Waltz mengatakan bahwa sistem internasional menjadi lebih anarki. Alasannya adalah paham liberal sebagai kekuatan utama tidak memiliki lawan politik. Justru menurutnya, negara-negara yang dulu berada di bawah bayang-bayang bipolar akan bermunculan. Secara teknologi, Waltz melihat bahwa Jepang dan Jerman akan menjadi kekuatan utama dalam bidang teknologi. Di sisi lain, ia sendiri tidak menampik bahwa Tiongkok akan menjadi kekuatan yang mampu menandingi negara Barat di bidang ekonomi. Pada akhirnya Waltz menyimpulkan bahwa di era digital negara harus dapat bertahan di tengah sistem internasional yang

anarki dengan terus meningkatkan kapabilitasnya di bidang politik/militer, ekonomi dan teknologi.

Kekuatan sebuah negara tidak lagi diukur dari seberapa besar kekuatan militernya. Ekonomi dan teknologi menjadi salah satu indikator dari kekuatan sebuah negara. Berbicara tentang teknologi, hampir semua dimensi kehidupan manusia telah tersambung ke Internet. Infrastruktur kritis seperti energi, air, listrik, perbankan dan bahkan pertahanan sangat bergantung pada dunia *cyber*. Untuk memenuhi kebutuhan dasarnya itu, negara perlu meningkatkan kapabilitasnya di bidang teknologi. Peningkatan kapabilitas tersebut tentu saja akan membuat rasa tidak aman aktor-aktor HI seperti negara, organisasi transnasional ataupun individu. Akibat rasa tidak aman itu, perang di dunia *cyber* menjadi tidak terelakkan. Motif politik, ekonomi ataupun kuriositas yang tidak pada tempatnya dapat memicu *cyber war*. Seperti yang pernah dilakukan Rusia pada Estonia tahun 2008 yang mengirimkan *malware* untuk melumpuhkan infrastruktur kritis ke bekas negara bagian Uni Soviet tersebut.

Konflik di dunia *cyber* tidak hanya dilakukan oleh aktor negara karena teknologi dapat dikendalikan oleh siapa saja, termasuk aktor transnasional seperti kelompok terorisme. Beberapa kelompok seperti ISIS memiliki divisi *cyber* untuk meretas sistem informasi lawan-lawan politiknya. Bahkan beberapa penelitian menyatakan bahwa di tahun 2016 sekarang ini, ISIS akan lebih gencar untuk melakukan serangan di dunia maya (CISO, 2015). Potensi konflik tidak lagi muncul secara fisik lagi. Sehingga mau tidak mau, negara sebagai entitas yang menaungi jutaan manusia perlu meningkatkat *awareness* dan keamanan *cyber* mereka. Konflik di dunia *cyber* disebut dengan *emergent modes of conflict (*Arquilla dan Rondfelt, 1993). Arquilla dan Ronfeldt menjelaskan bahwa peningkatan teknologi sebuah negara ikut memicu munculnya potensi konflik baru yang mana salah satunya adalah *cyber war*.

Kedua peneliti itu menjelaskan beberapa poin penting tentang potensi konflik ataupun perang yang dapat terjadi akibat meningkatnya kapabilitas negara dalam bidang teknologi. Poin pertama adalah efektifitas yang dapat mengurangi jatuhnya korban jiwa ketika konflik berlangsung. Arquilla dan Rondfelt mengatakan bahwa kemenangan sebuah negara ketika berperang tidak ditentukan dari seberapa banyak mereka menempatkan jumlah pasukan ataupun angkatan perang di medan perang. Kemenangan justru diraih oleh negara yang menguasai informasi. Sedangkan informasi diperoleh dengan memanfaatkan teknologi. Mereka memaparkan pula bahwa teknologi mendorong negara untuk meningkatkan kekuatan militernya seperti *laser guided system, aircraft control* dan bahkan *intelligence gathering*. Pengumpulan data intelijen tidak hanya menggunakan agen mata-mata, tetapi memanfaatkan kecanggihan komputer dengan mengembangkan teknologi *spyware*. Menurut pandangan mereka, *cyber war* adalah bagian dari *future war* (Aronson dalam Bayliss, 2005).

Pendapat yang senada dipaparkan pula oleh Jonathan D. Aronson bahwa perkembangan teknologi memicu arus globalisasi menjadi semakin dekat. Teknologi informasi yang dimaksud adalah penggunaan Internet yang semakin masif, meluasnya peredaran telepon seluler dan hilangnya batas-batas negara secara fisik di dunia maya (Aronson dalam Bayliss, 2005). Masifnya penggunaan teknologi dalam

analisis Aronson memberikan banyak konsekuensi yang harus dibenahi oleh negara. Tiga poin konsekuensi yang menjadi tantangan negara di masa depan adalah permasalahan keamanan, transformasi praktik pemerintahan menjadi lebih terdigitalisasi (*e-government*) dan pertumbuhan ekonomi yang bergantung pada pertumbuhan digital. Apabila dilihat dari sisi keamanan, Aronson menjelaskan bahwa negara dihadapkan pada persoalan serius untuk menjaga keamanannya. Ancaman terhadap keamanan negara di dunia *cyber* tidak lagi datang dari aktor sesama negara, tetapi juga dari aktor transnasional ataupun individu.

Ada tiga persoalan keamanan *cyber* yang menjadi penekanan. Pertama adalah *intelligence gathering, activism* dan *cyberwar* (Aronson dalam Bayliss, 2005). Seperti yang telah disebutkan pada contoh di atas, dunia *cyber* merupakan *hub* yang sangat tepat untuk mengumpulkan informasi penting. *Intelligence gathering* sangat berdampak pada perumusan kebijakan luar negeri. Melalui pemanfaatan teknologi, sebuah negara tidak perlu lagi menempatkan agen intelijen. Mereka hanya membutuhkan peretas (*hacker*) pintar dan teknologi *spyware* untuk menyusup pada jaringan Internet atau Intranet pemerintah tertentu untuk mengumpulkan data. Pada beberapa kasus, *cyber espionage* (mata-mata siber) melibatkan aktor negara yang kerap kali disebut dengan *state-sponsored hacker* (NBC, 2015). Motif peretasan sistem informasi sebuah negara tidak hanya dilandasi faktor politik, tetapi juga ekonomi. Mereka tidak hanya meretas insititusi negara tetapi juga perusahaan multinasional dan lembaga perbankan. Rahasia dagang dan informasi finansial adalah target utamanya. Contohnya adalah Tiongkok yang seringkali dituduh oleh pemerintahan Obama karena mereka mencari informasi keuangan dan perdagangan untuk kepentingan perekonomiannya (Reuters, 2015). Pada intinya, *intelligence gathering* memberikan informasi penting bagi sebuah negara dan menjadikannya sebagai *bargaining power*.

Permasalahan kedua dalam keamanan *cyber* adalah *activism*. Di dunia *cyber*, aktivitas peretasan sebagai bentuk protes terhadap kebijakan sebuah negara atau organisasi tertentu dikenal dengan istilah *hacktivism*. Peretasan semacam ini umumnya tidak untuk mencuri data tetapi menggunakan media *cyber* untuk melakukan *defacement* (perubahan tampilan laman situs Internet) sebagai bentuk protes. Aktor yang melakukan hal semacam ini lazim dilakukan oleh kelompok Anonymous. Secara geografi, anggota Anonymous tersebar di seluruh dunia dan tidak dibatasi oleh batas-batas wilayah. Mereka seringkali menjadi ancaman bagi negara karena sering melumpuhkan sistem informasi dan melakukan *defacement* pada situs Internet milik pemerintah. Secara umum, Anonymous tidak memiliki musuh yang tetap. Mereka akan menyasar pada negara atau organisasi tertentu yang dipandang telah menginjak-injak hak asasi manusia. Anonymous pernah melakukan operasi *cyber* yang bernama *operation holocaust* untuk melumpuhkan sistem informasi negara Israel (Jewish Exponent, 2015). Tindakan tersebut mereka lakukan karena menentang penjajahan Israel terhadap Palestina yang masih ada hingga saat ini. Bukan hanya aktor negara yang menjadi target utama Anonymous, pasca serangan teroris di Paris, mereka pun melakukan operasi serupa dengan nama *#OpParis* sebagai bentuk protes mereka pada kelompok teroris ISIS.

Permasalahan ketiga yang dijelaskan oleh Aronson adalah pergeseran perang fisik menjadi perang *cyber*. Menurutnya, informasi adalah aset potensial

untuk memenangkan sebuah peperangan. Sebagai cintoh, sistem informasi, komputer dan Internet kini menjadi alat untuk menerbangkan pesawat *drone*. Fungsi utamanya adalah pengintaian, walaupun *drone* memiliki fungsi untuk melakukan penyerangan. Lebih luas, *cyber war* kini menjadi salah satu perhatian khusus Pentagon. Berdasarkan pandangan Aronson, Pentagon telah mengembangkan suatu teknologi untuk melumpuhkan sistem informasi dan komputer milik negara lain. Di masa depan, *cyber war* tidak lagi berlangsung antar negara tetapi juga dengan kelompok teroris. Perkembangan teknologi dimanfaatkan pula oleh teroris untuk memuluskan kepentingannya.

Terlepas dari tiga isu keamanan di atas, Aronson pun memprediksi bahwa ancaman *cyber* dapat berasal dari kelompok kriminal internasional. Berbeda dengan *hacktivism* atau teroris yang memiliki motif politik, organisasi kriminal memanfaatkan teknologi untuk memperoleh keuntungan ekonomi dengan cara yang ilegal. Teknologi informasi kini memudahkan mereka untuk berkomunikasi dengan cepat dan rahasia. Organisasi kriminal dimudahkan pula dengan teknologi sehingga mereka dapat membuat strategi untuk menghindari penegak hukum ketika akan menyelundupkan barang-barang ilegal yang melewati batas negara tertentu. Menurut United Nations Conference on Transnational Crime, organisasi kriminal internasional kini semakin lihai dan aktif untuk menyelundupkan uang, organ tubuh manusia, perdagangan manusia, narkoba dan senjata. Masih menurut analisis Aronson, keuntungan yang diperoleh dari penyelundupan itu mencapai triliunan dolar. Permasalahan keamanan *cyber* ini bukan lagi sekadar menjaga kedaulatan dan ketahanan negara di dunia maya, tetapi bagaimana menjaga lingkungannya dari ancaman tersebut. Mengingat dunia maya yang tanpa batas, negara tidak lagi harus bersikap *self-help* seperti pandangan realis, tetapi harus bisa membangun kerja sama mengatasi ancaman serupa yang dihadapi oleh negara lainnya.

Pentingnya Kerja Sama Internasional

Mahzab realis tidak begitu optimis memandang kerja sama internasional. Mereka menganggap bahwa negara pada intinya harus bertahan sendiri (*self-help*) di tengah sistem internasional yang anarki. Secara garis besar, realis lebih melihat organisasi ataupun kerja sama internasional sebagai alat untuk mencapai kepentingan nasionalnya. Pada akhirnya, kerja sama adalah sebuah alat untuk mencapai kepentingan nasionalnya ketimbang konsensus bersama. Sedikit berbeda dengan realis, liberal institusionalisme justru memandang bahwa kerja sama adalah media yang tepat untuk mengatasi berbagai problematika keamanan. Hal yang paling ditekankan dalam pandangan liberal institusionalisme adalah negara perlu membentuk organisasi internasional untuk mengatasi permasalahan bersama daripada mengandalkan kekuatan sendiri yang sangat terbatas geraknya. Walaupun pada intinya, liberal institusionalisme memiliki koridor yang sama dalam memandang isu keamanan. Berikut adalah tabel empat pendekatan dalam mengatasi keamanan internasional:

Tabel 1
Tabel Pendekatan Keamanan Internasional

Security Approach	Sources of Insecurity	World Political System	Armaments Strategy	Primary Peacekeeping Mechanism	Strategy
Unlimited self-defense	Many, probably inherent in humans	State-based; national interest and rivalries;fear	Have many and all types to guard against threat	Armed states, deterence, alliances, balance of power	Peace through strength
Limited self-defense	Many, perhaps, but weapons intesify them	State based; limited cooperation based on mutual interest	Limit amount and types to reduce capabilities, damage, tension	Armed states: defensive capabilities, lack of offensive capabilities	Peace through limited offensive ability
International Security	Anarchical world system; lack of law or common security mechanism	International political integration; regional or world government	Transfer weapons and authority to international force	International peacekeeping/peace enforcement	Peace through law and universal collective defense
Abolition of warr	Weapons; personal and national greed and insecurity	Various options from pacifistic states to libertarian global village model	Eliminate weapons	Lack of ability; lack of fear; individual and collective pacifism	Peace through being peaceful

Sumber: T. Rourke, John. 2005. *International Politics on the World Stage 10th ed.* Boston: McGraw-Hill, hal 341

Berdasarkan tabel di atas, poin pertama dan kedua berfokus pada negara sebagai *level of analysis* dan cara-cara menjaga keamanan internasional adalah menggunakan kekuatan politik dan militer. Hal tersebut terlihat dari pentingnya *balance of power* sebagai sumber utama untuk menjaga keamanan internasional. *Limited self-defense* memiliki kesamaan dengan *unlimited self-defense* walaupun pendekatan keamanannya mulai memperhatikan aspek kerja sama internasional secara terbatas. Adapun pendekatan *international security* mulai memfokuskan pada kerja sama internasional. Pendekatan ketiga tersebut sangat cocok dengan situasi politik global saat ini dimana integrasi politik menjadi demikian penting. Contohnya

adalah berkembangnya organisasi regional seperti Uni Eropa dan ASEAN serta semakin pentingnya peran PBB. Untuk menjaga keamanan internasional, pendekatan ketiga menggunakan mekanisme hukum internasional dan *collective defense* seperti apa yang lazim digunakan oleh NATO.

Pendekatan keempat yaitu *abolition of war* digunakan apabila negara yang ada di dunia saat ini menganut sistem demokrasi. *Abolition of war* erat kaitannya dengan konsep kosmopolitanisme yang diusung oleh Immanuel Kant. Konsep *global village* pada pendekatan keempat tersebut dalam pandangan mahzab Kantian akan tercipta ketika semua negara telah memiliki sistem demokrasi. Pada penelitian ini, peneliti akan menggunakan pendekatan ketiga mengingat ancaman *cyber* bukanlah persoalan pengendalian senjata seperti masa Perang Dingin. Dunia saat ini sudah terkoneksi satu sama lain sehingga negara ataupun individu memiliki ancaman yang sama. Untuk mengatasi persoalan keamanan *cyber*, kerja sama internasional adalah mekanisme yang paling baik.

Joseph S. Nye menjelaskan bahwa ada empat ancaman *cyber* yang harus diatasi di era global saat ini yaitu *cyber war* dan *economic espionage* yang identik dengan aktor negara; *cyber crime* dan *cyber terorrism* yang erat kaitannya dengan aktor non-negara. Nye pun memaparkan bahwa mengatasi ancaman *cyber* tidak bisa menggunakan paradigma ataupun konsep seperti era Perang Dingin. Dalam pandangannya, teknologi mendorong pertumbuhan ekonomi dan mempercepat globalisasi. Sehingga ancaman *cyber* tidak bisa diatasi dengan cara mengendalikan teknologi yang dimiliki oleh aktor HI. Ia menyimpulkan bahwa dibutuhkan sebuah kesepakatan atau hukum yang jelas dan dapat mengatur tentang ancaman *cyber* serta tata cara bagaimana menjaga keamanan di dunia maya (Nye, n.d).

Setiap negara membutuhkan kerja sama dengan negara lainnya karena keamanan *cyber* adalah masalah yang dihadapi bersama. Adapun bentuk kerja sama yang dapat dilakukan bisa berupa hubungan bilateral ataupun multilateral dengan memanfaatkan keberadaan organisasi regional ataupun internasional. Di tengah situasi internasional yang semakin dinamis, pendekatan liberal institusional lebih tepat untuk menghadapi ancaman *cyber* melalui kerja sama dibandingkan pendekatan realis yang memandang pesimis aktor-aktor negara. Liberal institusional setidaknya sepakat dengan realis bahwa untuk meningkatkan *power* sebuah negara, kekuatan militer tidak dapat disampingkan. Namun, kerja sama internasional setidaknya dapat membuat sebuah *framework* yang dapat membantu untuk menghadapi ancaman yang sama (Bayliss dan Smith, 2005). Keamanan *cyber* adalah permasalahan yang harus dihadapi bersama sehingga melalui entitas organisasi internasional, negara dapat mengatasi ancaman tersebut.

Liberal institusionalis menempatkan organisasi internasional sebagai lembaga supranasional. Artinya adalah lembaga tersebut mengatur kebijakan dan tindakan negara dalam bidang-bidang tertentu. Institusi atau organisasi internasional memiliki peran yang sangat penting untuk mengatasi ancaman *cyber*. Kebijakan yang dihasilkan oleh organisasi internasional dapat berupa ataturan yang disebut dengan "rezim". Bentuk rezim tersebut ada pula yang tanpa organisasi seperti Protokol Kyoto ataupun Konferensi Hukum Laut yang diselenggarakan di bawah pengawasan PBB. Mengacu pada pendekatan keamanan internasional di atas, peneliti menganalisis bahwa keberadaan organisasi/institusi internasional sangatlah

dibutuhkan. Menggunakan pendekatan liberal institusional, institusi internasional merupakan wadah yang tepat untuk mengatasi permasalahan keamanan dunia.

Peneliti merujuk pada pernyataan Robert Keohane, seorang pakar liberal institusional bahwa institusi dapat menyediakan informasi, mengurangi biaya transaksi dan menjadi titik penting koordinasi. Menurut pandangan mereka, organisasi internasional menjadi pemain penting untuk menciptakan stabilitas dan keamanan dunia pasca Perang Dingin (Bayliss dan Smith, 2005). Adapun kebijakan atau aktivitas untuk mengatasi ancaman *cyber* tergantung pada mekanisme insititusi tersebut. Pakta pertahanan seperti NATO akan mengedepankan aspek *collective defense* untuk mengatasi ancaman *cyber*. Mekanisme NATO dalam mengatasi ancaman *cyber* masih tetap berkorelasi dengan militer karena fokus utama organisasi tersebut adalah menjaga pertahanan negara-negara anggotanya baik secara fisik ataupun maya. Kebijakan yang dimiliki NATO tentu akan berbeda dengan Interpol ataupun Uni Eropa. Untuk mengatasi ancaman *cyber*, Uni Eropa memberlakukan kebijakan *data hub* yang mana semua data warganya yang tergabung dalam keanggotaannya hanya boleh dikelola di dalam wilayahnya. Begitu pula dengan Interpol yang fokus menangani ancaman *cyber* dari sisi penegakan hukum.

Situasi konstelasi politik global saat ini tidak lagi berada di era Perang Dingin. Teknologi telah mendorong globalisasi dan hal tersebut erat kaitannya dengan masa keterbukaan di mana pada masa Perang Dingin transparansi adalah sesuatu yang sangat unik. Negara tetap perlu meningkatkan kapabilitasnya baik dari sisi politik, militer, ekonomi, sosial budaya ataupun teknologi. Namun, mereka tidak bisa melakukan isolasi ataupun menutup diri. Pada intinya negara tetap membutuhkan kerja sama dan peran penting institusi internasional. Dalam permasalahan *cyber* ini seperti yang dikatakan oleh Nye bahwa ancaman *cyber* tidak bisa dilakukan dengan cara *arms control* seperti di era Perang Dingin. Hal pertama yang bisa dilakukan oleh negara adalah saling bekerja sama dan menghilangkan rasa tidak percaya di antara satu sama lain. Bentuk ancaman yang dihadapi oleh negara di era sekarang ini tidak lagi bersifat *high politics* tetapi juga *soft politics*. Oleh karena itu, ancaman yang dihadapi oleh negara saat ini tidak lagi harus dipecahkan sendiri tetapi juga memanfaatkan organisasi internasional untuk memperjuangkan kepentingan nasionalnya.

Poin penting mengapa institusi internasional sangat penting dalam mengatasi ancaman *cyber* adalah kestabilan dan keamanan dunia saat ini dapat dicapai melalui kerja sama dan kooperasi ketimbang menggunakan ketakutan dan kekuatan yang menjadi corak khas realis. Melalui institusi internasional, negara tidak hanya berusaha untuk mencapai *international interest* tetapi juga *common interest* yang menjadi tujuan institusi internasional tersebut. Mengatasi ancaman *cyber* melalui pendekatan liberal institusional dapat menggunakan tiga langkah khusus, yaitu kebersamaan, kekhususan dan otonom (Jackson dan Sorensen, 2005). Dilihat dari aspek kebersamaan, tujuan dari institusional dapat diintepretasikan dalam bentuk partisipasi negara pada institusi tersebut. Permasalahan ancaman *cyber* dalam pandangan liberal institusional dapat diatasi melalui pembentukan lembaga supranasional yang dapat mengakomodir kepentingan setiap negaranya. *Outcome* yang dihasilkan pada akhirnya adalah setiap negara akan melihat bahwa ancaman

cyber adalah masalah bersama dan salah satu cara untuk mengatasinya adalah saling berkooperasi serta menghilangkan sikap chauvinisme antar negara.

Secara aspek kekhususan, liberal institusional memandang bahwa institusi internasional merupakan derajat harapan negara yang tertuang dalam bentuk aturan-aturan. Pembentukan institusi internasional tidak terlepas dari kepentingan negara untuk berkolaborasi dengan negara atau aktor HI lainnya karena memiliki ancaman yang serupa. Institusi internasional dapat mengeluarkan kebijakan atau aturan yang mengatur negara-negara anggotanya dalam mengatasi ancaman *cyber*. Walaupun belum semua organisasi regional ataupun internasional memiliki aturan khusus tentang keamanan *cyber*, beberapa lembaga supranasional seperti Uni Eropa ataupun NATO telah memiliki aturan tersebut. Uni Eropa memiliki aturan yang disebut dengan *EU International Cyberspace Policy* yang mana aturan tersebut mengatur kebijakan luar negeri anggotanya dari sisi dunia maya (*cyberspace*).

Kebijakan tersebut setidaknya memuat empat aturan utama yaitu *freedom and openness, EU's laws, norms and core values, developing cyber security building* dan *international cooperation* (EU, 2014). Aturan pertama membahas tentang nilai-nilai dan hak dasar Uni Eropa di dunia maya. Sedangkan aturan kedua dan ketiga menjelaskan tentang penegakkan norma, hukum dan aturan yang berlaku serta pembangunan kapabilitas tiap-tiap negara anggota Uni Eropa untuk menjaga keamanan *cyber*-nya. Poin terakhir membahas tentang pentingnya kerja sama internasional antara Uni Eropa dengan negara Dunia Ketiga, masyarakat dan sektor swasta untuk memperkuat ketahanan *cyber*. Uni Eropa sebagai organisasi penting di kawasan Eropa melihat ancaman *cyber* sebagai permasalahan bersama. Untuk mengatasinya, Uni Eropa membangun konsensus bersama dalam menghadapi ancaman *cyber* dengan cara membuat aturan bagi negara anggotanya. Hal tersebut dapat diadopsi pada institusi regional ataupun internasional lainnya.

Pada aspek ketiga yaitu otonom, institusi dapat mengubah aturannya sesuai dengan kepentingan perluasannya. Institusi internasional memiliki wewenang untuk menempatkan aturan atau kebijakan mereka tergantung pada isu atau kepentingan yang akan mereka capai. Pada permasalahan ini, institusi internasional berwenang mengubah aturannya apabila isu keamanan *cyber* ini semakin dinamis. Contoh nyatanya adalah Uni Eropa telah memberlakukan aturan *Privacy Shield* untuk melawan balik inisiasi *Safe Harbour* yang diprakarsai oleh pemerintah AS. Aturan *Privacy Shield* dikeluarkan karena negara anggota Uni Eropa khawatir data warga mereka yang keluar dari wilayah otoritasnya dan disimpan di AS akan menyalahi hak-hak privasi mereka (CISO, 2016).

Sebelumnya, Uni Eropa telah lebih dulu memiliki aturan tertentu tentang keamanan *cyber* yang menyangkut hak privasi warga negaranya. Namun, pemerintah AS menginginkan adanya kolaborasi dengan Uni Eropa untuk mengelola data warga mereka sebagai langkah *deterence* terkait adanya kelompok terorisme yang menggunakan teknologi seperti media sosial untuk menyebarkan pengaruhnya. Tetapi, Uni Eropa memutuskan bahwa mengakomodasi kebijakan AS dapat membahayakan privasi warganya dan mayoritas negara anggota menolak inisiasi *Safe Harbour*. Isu dan permasalahan keamanan *cyber* yang berkembang dengan cepat pada akhirnya memaksa institusi internasional mengubah kebijakannya agar kepentingan bersama yang ingin dicapai negara anggotanya dapat tercapai.

Kontribusi Indonesia di ASEAN

Uni Eropa atau NATO sudah lebih dewasa dalam menyusun dan mengaplikasikan kebijakan organisasi mereka dalam hal keamanan *cyber*. Bagaimana dengan Indonesia? Sebagai negara yang cukup terpandang di kawasan Asia Tenggara, Indonesia dan negara anggota ASEAN lainnya dapat mengadopsi langkah-langkah Uni Eropa dan menyesuaikannya sesuai kebutuhan. International Telecommunication Union (ITU) pada tahun 2014 pernah merilis sebuah survei yang berjudul *Global Cyber Security Index 2014*. Tujuan dari pembentukan survei tersebut adalah memetakan tingkat kedewasaan sebuah negara dalam mengimplementasikan *cyber security awareness*. *Global Cyber Security Index* ini tidak berusaha untuk mengukur tingkat kesuksesan sebuah negara dalam menghadapi keamanan *cyber*. Aspek yang mereka ukur adalah sejauh mana negara membangun *national structure* untuk mempromosikan dan mengimplementasikan *security awareness building* di masyarakatnya.

Lima aspek mendasar yang menjadi penilaian adalah *legal measures, technical measures, organizational measures, capacity building, and cooperation*. Pada tatanan Asia-Pasifik Australia, Malaysia dan Selandia Baru adalah negara yang memperoleh *Global Cyber Security Index* terbaik. Australia dan Malaysia sama-sama memperoleh indeks sebesar 0,7647. Namun, Australia mengungguli Malaysia karena dalam aspek penilaian *capacity building*, negara Kangguru itu unggul lebih baik. Di posisi ketiga adalah Selandia Baru dengan perolehan indeks sebanyak 0,7353. Bagaimana dengan Indonesia? Negara kita boleh berbangga hati karena berhak menempati urutan ke-5 dengan perolehan indeks sebesar 0,4706. Negara kita tertinggal dari India, Jepang, Republik Korea Selatan dan Singapura. Namun, Indonesia mengungguli China, Thailand, Sri Lanka dan Brunei Darussalam. Indonesia di tingkat Asia Tenggara berada di urutan ketiga.

Lembaga ASEAN adalah sarana yang tepat bagi Indonesia untuk mengembangkan kerja sama dalam mengatasi ancaman *cyber*. Melalui visi misi yang sama yaitu *one vision, one mission* dan *one identity*, Masyarakat Ekonomi ASEAN (MEA) dapat terbentuk. Di tahun 2016 ini, Indonesia sedang berjalan menuju sebuah komunitas dimana halangan (*barrier*) yang menghalangi bersatunya sebuah kawasan perlahan mulai hilang. Terbentuknya MEA semakin menegaskan bahwa perekonomian dunia yang dahulu masih berada di sektor Trans-Atlantik kini telah bergeser ke kawasan Asia-Pasifik. Ketika pusat perekonomian sudah mulai bergeser ke kawasan tersebut khususnya Asia Tenggara, maka tantangan pun semakin beragam. Salah satu tantangan tersebut adalah ancaman *cyber* yang mana hampir semua perekonomian di kawasan Asia Tenggara telah bergantung sepenuhnya pada teknologi.

Berdasarkan ASEAN ICT Masterplan 2012, salah satu tugas pokok negara anggota ASEAN dalam menyambut MEA adalah memperkuat keamanan *cyber* untuk memperkuat perekonomian kawasan melalui kerja sama. Negara anggota dapat memanfaatkan kelembagaan ASEAN untuk mempererat kerja sama keamanan *cyber* dengan cara *information sharing* serta saling membangun *trust* di antara sesama anggota. Menurut Deputi Bidang Kerja Sama ID-SIRTII/CC, Muhammad Salman bahwa ancaman *cyber* sangat dinamis. Hal tersebut menurutnya hanya dapat diatasi ketika negara-negara anggota ASEAN mampu menghilangkan ego

nasionalistiknya serta berkontribusi dalam menjaga keamanan *cyber* di wilayah Asia Tenggara (Salman, 2015). Mengacu pada konsep liberal institusional, ASEAN bisa mengembangkan ICT Masterplan-nya menjadi sebuah rezim ataupun *guideline* yang dapat dijadikan panduan. Tentunya, *guideline* yang disusun tidak boleh menyalahi kesepakatan non-intervensi yang sudah menjadi *trademark* ASEAN.

Kerja sama antar negara di lembaga ASEAN sangat tepat bagi Indonesia. Selain sebagai *founding father* ASEAN, Indonesia adalah pengguna Internet terbesar di wilayah Asia Tenggara. Untuk memitigasi ancaman *cyber*, wilayah Asia Tenggara sudah memiliki *hub* atau wadah yang tepat untuk mengatasinya. Menggunakan tiga pendekatan liberal institusional yaitu kebersamaan, kekhususan dan otonom, Indonesia bisa menjadi pendorong untuk merumuskan kebijakan atau aturan keamanan *cyber* yang dapat diterapkan oleh negara anggota ASEAN lainnya. Strategi pertama adalah Indonesia perlu memetakan ancaman *cyber* sebagai ancaman bersama sehingga tercapai konsensus bersama bahwa kawasan Asia Tenggara memiliki permasalahan serupa.

Dintinjau dari aspek kekhususan, Indonesia dapat mendorong usulan di lembaga ASEAN untuk segera membentuk aturan, rezim ataupun *guideline* tentang keamanan *cyber* yang dapat diterapkan secara umum oleh negara anggotanya. Aturan tersebut setidaknya harus memiliki beberapa kriteria. Pembentukan aturan didasari pada kepentingan bersama (*common interest*), tidak bersinggungan dengan visi misi ASEAN dan berorientasi pada terciptanya suasana kondusif MEA 2016. Sedangkan bila ditinjau dari aspek otonom, aturan yang disusun dapat disesuaikan dengan dinamika keamanan *cyber* itu sendiri. Hal terpenting adalah negara anggota ASEAN dapat mengadopsi aturan yang disusun serta disesuaikan dengan kebutuhan dan kepentingan nasional masing-masing. Kontribusi Indonesia di ASEAN dalam mengatasi ancaman *cyber* merupakan tindakan nyata perwujudan negara untuk mencapai kepentingan nasional dan masyarakat dunia yang tercantum di UUD 1945.

Kerja sama internasional itu sendiri dapat diperluas tidak hanya di antara negara-negara anggota ASEAN, tetapi juga dengan aktor HI lainnya. ASEAN dapat memanfaatkan kerja sama dengan negara lain seperti ASEAN Plus Three (Korea, Jepang dan RRT) untuk saling berkolaborasi dalam mengatasi permasalahan keamanan *cyber*. Selain itu, ASEAN sendiri perlu menjalin kerja sama strategis dengan Uni Eropa, Interpol ataupun NATO yang telah lebih dahulu memiliki konsep dan kebijakan keamanan *cyber*. Melalui kerja sama tersebut, ASEAN akan memperoleh informasi dan rujukan untuk memperkuat kolaborasi antar organisasi dalam bidang keamanan *cyber* sekaligus mempererat kerja sama strategis. Hal ini memiliki korelasi langsung dengan pendekatan otonom liberal institusional. ASEAN setidaknya dapat memperluas atau menyesuaikan aturan dan kebijakan keamanan *cyber* sesuai dengan situasi politik global yang berkembang sesuai dengan zamannya.

Kerja sama internasional antar institusi sendiri memiliki efek positif bagi Indonesia. Efek pertama adalah negara ini memiliki *benchmarking* terkait pengembangan keamanan *cyber* sesuai dengan konsep NKRI. Poin kedua yang dapat diimplementasikan adalah Indonesia perlu terus berupaya mengembangkan teknologi informasi untuk meningkatkan kapabilitas *power* negara sekaligus alat untuk menjaga keamanan di dunia maya. Langkah terakhir yang diperoleh Indonesia

dari kerja sama tersebut adalah negara ini perlu melibatkan semua *stakeholder* seperti pemerintah, swasta, profesional dan komunitas TI untuk saling bersinergi mencipatakan keamanan di lingkungan *cyber* baik di tataran domestik, regional dan global.

Simpulan

Ancaman *cyber* merupakan ancaman yang nyata dan perlu untuk diatasi. Persoalan tersebut bukanlah mitos, melainkan ada dan nyata. Tidak seperti Perang Dingin dimana *balance of power* menjadikan interaksi antar negara sangat mudah diprediksi. Di era teknologi saat ini, ancaman bukan hanya politik atau militer. Sumber ancaman justru muncul dari aspek *soft power*. Mengantisipasi ancaman *cyber* tidak bisa dilakukan dengan cara *arms control* seperti era Perang Dingin. Ancaman pun tidak bisa diatasi dengan mengandalkan konsep *self-help*. Justru keamanan internasional dapat diatas melalui wadah lembaga supranasional seperti Uni Eropa dan ASEAN. Mengingat ancaman *cyber* yang tidak mengenal batas negara dapat dicegah ketika negara bekerja sama dalam institusi internasional karena memiliki permasalahan yang sama. Bagi Indonesia sendiri, kerja sama melalui wadah institusi internasional mengatasi permasalahan keamanan *cyber* adalah perwujudan dari politik bebas aktif dan menjaga perdamaian dunia.

Daftar Pustaka

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

Bayliss, John dan Smith, Steve. (2005). *The Globalization of World Politics*. London: Oxford University Press.

Rourke, T. John. (2004). *International Politics on the World Stage 10th ed*. Boston: McGraw-Hill.

Jackson, Robert dan Sorensen, George.(2005). *Pengantar Studi Hubungan Internasional*. Yogyakarta: Pustaka Pelajar

Jurnal

Arquilla, John dan David Rondfelt. (1993). Cyberwar is Coming. *Comparative* Strategy 12(2)

Waltz, Kenneth. (1993). The Emerging Structure of International Politics. *International Security* 18 (2)

Riset

PwC Global, *Managing Risk Cyber With Insurance*, 2014.
Global Security Index 2014, International Telecommunication Union, 2015.

Majalah

ASEAN Cyber Security di MEA 2015 di CISO Magazine Edisi April 2015.

Situs Internet

http://www.nato.int/cps/en/natohq/topics_78170.htm, diakses 4 April 2016.

"Ada Spyware di Negosiasi Nuklir Iran", http://www.ciso.co.id/2015/06/ada-spyware-di- negosiasi-nuklir-iran/, diakses 4 April 2016.

"Cyberattack Pentagons Joint Staff Email Take System Offline", http://www.nbcnews.com/tech/security/cyberattack-pentagons-joint-staff-emails-take- system-offline-n405321, diakses, 7 April 2016.

"Cyberattack Pentagons Joint Staff Email Take System Offline",http://www.nbcnews.com/tech/security/cyberattack-pentagons-joint-staff- emails-take-system-offline-n405321, diakses, 7 April 2016.

"International Hackers Threaten Repeat Cyber Attack Against Israel", http://www.jewishexponent.com/headlines/2015/04/international-hackers-threaten- repeat-cyber-attack-against-israel, diakses 7 April 2016.

"Is Cybersecurity like arm control?", http://www.huffingtonpost.com/joseph-nye/is-cybersecurity-like-arm-control_b_7302200.html, diakses 8 April 2016.

"Presiden Obama Pertimbangkan Sanksi Peretasan OPM", http://www.ciso.co.id/2015/06/presiden-obama-pertimbangkan-sanksi-peretasan-opm/, diakses 4 April 2016.

"Safe Harbour Ditolak di Menit Terakhir", www.ciso.co.id/2016/safe-harbour-ditolak-di-menit- terakhir/, diakses 14 April 2016.

"Statistik Pengguna Internet dan Media Sosial Terbaru 2015", https://id.techinasia.com/talk/statistik-pengguna-internet-dan-media-sosial-terbaru-2015, diakses 19 April 2016.