ISSN 1829-8001
Terakreditasi No. 726/Akred/P2MI-LIPI/04/2016

LIPI

Jurnal Penelitian Politik

Vol.13, No.1, Juni 2016

KOMUNITAS ASEAN DAN TANTANGAN KE DEPAN

Jurnal Penelitian Politik	Vol. 13	No. 1	Hlm. 1-143	Jakarta, Juni 2016	ISSN 1829-8001

Jurnal Penelitian Politik

Jurnal Pusat Penelitian Politik-Lembaga Ilmu Pengetahuan Indonesia (P2P-LIPI), merupakan media pertukaran pemikiran mengenai masalah-masalah strategis yang terkait dengan bidang-bidang-bidang politik nasional, lokal, dan internasional; khususnya mencakup berbagai tema seperti demokratisasi, pemilihan umum, konflik, otonomi daerah, pertahanan dan keamanan, politik luar negeri dan diplomasi, dunia Islam, serta isu-isu lain yang memiliki arti strategis bagi bangsa dan negara Indonesia.

P2P-LIPI sebagai pusat penelitian milik pemerintah dewasa ini dihadapkan pada tuntutan dan tantangan baru, baik yang bersifat akademik maupun praktis kebijakan, khususnya yang berkaitan dengan persoalan dengan otonomi daerah, demokrasi, HAM dan posisi Indonesia dalam percaturan regional dan internasional. Secara akademik, P2P-LIPI dituntut menghasilkan kajian-kajian unggulan yang bisa bersaing dan menjadi rujukan ilmiah pada tingkat nasional maupun internasional. Sementara secara moral, P2P-LIPI dituntut untuk memberikan arah dan pencerahan bagi masyarakat dalam rangka membangun Indonesia baru yang rasional, adil dan demokratis. Karena itu, kajian-kajian yang dilakukan tidak semata-mata berorientasi praksis kebijakan, tetapi juga pengembangan ilmu-ilmu pengetahuan sosial, khususnya perambahan konsep dan teori-teori baru ilmu politik, perbandingan politik, studi kawasan dan ilmu hubungan internasional yang memiliki kemampuan menjelaskan berbagai fenomena sosial politik, baik lokal, nasional, regional, maupun internasional

Alamat Redaksi

Pusat Penelitian Politik-LIPI, Widya Graha LIPI, Lantai III & XI
Jl. Jend. Gatot Subroto No. 10 Jakarta Selatan 12710
Telp/Faks. (021) 520 7118, E-mail: penerbitan.p2p@gmail.com
Website: www.politik.lipi.go.id

ISSN

1829-8001

Jurnal Penelitian
Politik
Vol. 13, No. 1, Juni 2016

DAFTAR ISI

CATATAN REDAKSI

Tahun 2016 menjadi tahun yang sangat penting bagi Indonesia dan ASEAN, karenan di permulaan tahun ini Komunitas ASEAN resmi dijalankan. Pembentukan komunitas ini disepakati oleh sepuluh negara anggota ASEAN untuk mewujudkan cita-cita integrasi di antara mereka. Integrasi di kawasan ini juga diharapkan dapat membuka pintu yang lebih lebar bagi peluang kerja sama di tingkat ASEAN, sehingga dapat membawa peningkatan kesejahteraan bagi masyarakat di kawasan ini. Selain peningkatan kesejahteraan di kawasan, hal lain yang juga ingin dicapai oleh ASEAN adalah membangun komunitas yang menguatkan solidaritas di antara anggotanya dan lebih bersifat people-oriented. Di tengah dinamika politik dan ekonomi di tingkat internasional yang semakin kompleks, Komunitas ASEAN diharapkan mampu mendorong sepuluh anggotanya untuk meningkatkan daya saing mereka miliki, sehingga ASEAN siap menghadapi tantangan regional dan internasional yang ada. Dalam membangun komunitas yang dicita-citakan, dibentuklah tiga pilar utama, yaitu: Komunitas Politik dan Keamanan ASEAN, Komunitas Ekonomi ASEAN, dan Komunitas Sosial Budaya ASEAN.

Komunitas Politik dan Keamanan ASEAN diharapkan mampu menjaga ASEAN untuk tetap berkomitmen dalam memelihara stabilitas dan keamanan di kawasan. Hal ini diperlukan agar ASEAN dapat membangun lingkungan politik yang harmonis yang mampu menghadapi ancaman-ancaman dari luar ataupun potensi konflik di dalam tubuh ASEAN sendiri. Sementara untuk meningkatkan kesejahteraan masyarakatnya, ASEAN membangun Komunitas Ekonomi ASEAN dengan tujuan untuk mendorong pergerakan roda ekonomi dan perdagangan antarnegara anggota ASEAN yang mampu bersaing secara sehat. Peningkatan daya saing produk-produk dari masing-masing negara anggota ASEAN diperlukan agar ASEAN dapat mengambil peluang yang besar dari perdagangan bebas di dunia internasional. Komunitas Ekonomi ASEAN atau yang juga dikenal dengan Masyarakat Ekonomi ASEAN (MEA) diharapkan dapat memperkecil gap perkembangan ekonomi di antara negara anggota ASEAN dan mampu menciptakan kesejahteraan yang merata bagi seluruh anggota ASEAN. Selain peningkatan kesejahteraan ekonomi, ASEAN juga mengharapkan terbentuknya masyarakat yang memiliki solidaritas dan rasa kebersamaan yang kuat terhadap ASEAN. Untuk itulah dibentuk Komunitas Sosial Budaya ASEAN. Kedekatan geografis diharapkan tidak hanya mampu menjalin keterhubungan secara fisik di ASEAN, namun juga mampu menjalin keterhubungan di antara masyarakat di kawasan Asia Tenggara.

Implementasi tiga pilar Komunitas ASEAN pada dasarnya akan membawa peluang yang sangat besar bagi ASEAN. Akan tetapi, pemberlakuan Komunitas ASEAN juga harus menghadapi beberapa tantangan yang muncul baik dari dalam tubuh ASEAN ataupun dari luar. Perbedaan tingkat kemajuan di antara negara anggota merupakan tantangan internal yang harus dihadapi ASEAN. Perbedaan tingkat perkembangan ekonomi negara-negara anggota ASEAN dapat menjadi ganjalan intergrasi yang ingin dicapai oleh ASEAN, terutama dalam sektor ekonomi. Selain itu, perbedaan kesiapan masing-masing negara dalam menghadapi Komunitas ASEAN juga menjadi tantangan bagi ASEAN. Sementara tantangan dari luar misalnya adalah tantangan yang muncul dari konstelasi politik internasional yang masih didominasi oleh kekuatan-keuatan negara besar, seperti Amerika dan Tiongkok. Sengketa Laut Cina Selatan yang melibatkan empat negara anggota ASEAN (Brunei, Filipina, Malaysia, dan Vietnam) dan Tiongkok apabila tidak dapat dikelola dengan baik dapat menjadi ganjalan bagi kestabilan di kawasan ini.

Bagi Indonesia, Komunitas ASEAN juga membuka peluang yang besar, terutama dalam mendorong peningkatan daya saing yang dimiliki oleh Indonesia. Namun, dilihat dari kesiapannya, peluang yang ada tidak dapat diambil secara optimal oleh Indonesia apabila pembangunan sosial, ekonomi, dan politik di Indonesia masih belum memenuhi harapan. Kesiapan sumber daya manusia, tata kelola, pembangunan infrastruktur, kerangka hukum, serta kebijakan pemerintah yang mendorong partisipasi Indonesia dalam Komunitas ASEAN dirasa masih kurang. Dari segi sosial masyarakat, Indonesia masih harus menghadapi kenyataan bahwa kesadaran masyarakat akan Komunitas ASEAN masih rendah. Belum banyak masyarakat yang menyadari arti penting Komunitas ASEAN atau ASEAN sendiri bagi Indonesia. Melihat kenyataan ini, *Jurnal Penelitian Politik* kali ini mengangkat tema "Komunitas ASEAN dan Tantangan ke Depan" untuk melihat lebih lanjut sejauh mana implementasi Komunitas ASEAN akan membawa dampak bagi ASEAN ataupun Indonesia, dan tantangan apa saja yang akan dihadapi di masa mendatang. *Jurnal Penelitian Politik* edisi kali ini menyajikan lima artikel, dan tiga resume hasil penelitian yang telah dilakukan oleh tim-tim penelitian yang ada di Pusat Penelitian Politik LIPI.

Artikel pertama berjudul **"Diplomasi Pertahanan Indonesia dalam Pencapaian *Cyber Security* Melalui *ASEAN Regional Forum on Cyber Security Initiatives"*** yang ditulis oleh David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari mencoba membahas tentang upaya Indonesia dalam memanfaatkan ASEAN Regional Forum (ARF) on cyber security initiatives untuk memperjuangkan kepentingan nasionalnya dalam rangka mendukung keamanan nasional di bidang cyber. Kemajuan teknologi, terutama di bidang cyber telah membuat batas antarnegara menjadi semakin kabur. Hal ini memicu munculnya kejahatan dan ancaman nirmiliter di bidang teknologi bagi sebuah negara dalam bentuk ancaman cyber. Untuk menghadapi hal tersebut Indonesia memerlukan strategi untuk melindungi keamanannya. ARF menjadi salah satu forum yang dapat dimanfaatkan Indonesia untuk mengajak negara-negara ASEAN dan negara mitranya untuk bekerja sama dalam meningkatkan pertahanan dan menjaga stabilitas di kawasan.

Sumber daya manusia juga merupakan salah satu faktor yang perlu mendapatkan perhatian khusus ketika kita berbicara tentang kesiapan Indonesia dalam menghadapi Komunitas ASEAN. Artikel yang ditulis oleh Fathimah Fildzah Izzati yang berjudul **"Membaca 'PHK Massal': Rantai Nilai Industri Elektronik, MEA, dan Tantangan bagi Gerakan Buruh di Indonesia"** mencoba melihat dampak pemberlakuan MEA bagi buruh-buruh yang ada di Indonesia. Kebijakan ekonomi yang dikeluarkan oleh pemerintah dalam rangka menyongsong MEA sempat menimbulkan isu "PHK Massal". Tulisan ini bertujuan untuk menunjukkan peran gerakan buruh dalam menghadapi MEA, terutama dalam bidang industri elektronik.

Artikel berjudul **"Transformasi Ruang dan Partisipasi *Stakeholders:* Memahami Keterlibatan Masyarakat Sipil dan Usaha Kecil dan Menengah Indonesia dalam Proses Regionalisme ASEAN pasca-2003"** ditulis oleh Ahmad Rizky Mardhatillah Umar. Artikel ini menjelaskan keterlibatan para pemangku kepentingan dalam dua sektor regionalisasi ASEAN, yaitu Hak Asasi Manusia (HAM) dan Usaha Kecil dan Menengah (UKM). Sejak bertransformasi menjadi bentuk 'Masyarakat ASEAN' pada tahun 2003, mulai muncul interaksi yang lebih kompleks antara 'negara' dan aktor-aktor 'non-negara'. Artikel ini berargumen bahwa Masyarakat ASEAN telah membuka ruang yang lebih besar untuk mengakomodasi partisipasi 'pemangku kepentingan'/stakeholders yang ada di dalamnya.

Dengan adanya integrasi di kawasan ASEAN melalui implementasi Komunitas ASEAN, masyarakat yang paling merasakan dampak langsung keterhubungan dan menipisnya batas antarnegara melalui integrasi tersebut adalah masyarakat di perbatasan. Artikel berjudul **"Ketahanan Sosial Warga Perbatasan Indonesia menghadapi Masyarakat Ekonomi ASEAN: Studi di Kecamatan Entikong, Kalimantan Barat"** mencoba mengulas tentang sejauh mana kesiapan yang dimiliki oleh warga di wilayah perbatasan Indonesia dalam menyongsong

pemberlakuan Komunitas Ekonomi ASEAN. Artikel yang ditulis oleh Sandy Nur Ikfal Raharjo ini melihat ketahanan yang dimiliki masyarakat di Entikong melalui enam modal: modal alam, modal sosial, modal keuangan, modal politik/ pemerintahan, modal fisik, dan modal manusia. Dari hasil analisis ini direkomendasikan bahwa pemerintah perlu melakukan reoptimalisasi kerja sama lintas perbatasan dengan negara lain untuk meningkatkan ketahanan masyarakat di perbatasan, dan perlu membuat aturankhusus untuk perdagangan lintas batas di dalam MEA.

Selain lima artikel di atas, *Jurnal Penelitian Politik* edisi kali ini juga menampilkan tiga resume penelitian yang telah dilakukan oleh tim-tim penelitian di Pusat Penelitian Politik. Resume penelitian pertama adalah mengenai perkembangan intelejen di Indonesia. Dalam ringkasan penelitian yang berjudul **"Intelejen dalam Pusaran Demokrasi di Indonesia Pasca Orde Baru"** yang disusun oleh Ikrar Nusa Bhakti dan Diandra Mengko Megaputri dibahas mengenai perkembangan dinamika intelejen Indonesia terutama pada masa setelah orde baru. Hasil penelitian ini tidak hanya memberikan gambaran tentang teori intelejen, pergumulan intelijen dan demokrasi di beberapa negara yang mengalami perubahan politik dari sistem otoriter ke demokrasi dan sejarah singkat intelijen di Indonesia, melainkan juga memuat ulasan awal demokratisasi intelijen di Indonesia.

Tim Penelitian yang ada di Pusat Penelitian Politik LIPI pada tahun 2015 juga melakukan penelitian yang terkait dengan Komunitas ASEAN. Salah satunya adalah resume penelitian berjudul **"Problematika Kerja Sama Perbatasan Sepanjang Sungai Mekong antara Tiongkok dan ASEAN Bagian Utara"** yang disusun oleh Awani Irewati, dkk. Pada penelitian ini Tim Perbatasan Pusat Penelitian Politik LIPI melakukan penelitian tentang upaya pembangunan keterhubungan melalui kerja sama lintas perbatasan di sub-kawasan Sungai Mekong antara Tiongkok dengan lima negara ASEAN: Myanmar, Laos, Kamboja, dan Vietnam. Dalam kerja sama sub-kawasan ini, Tiongkok sebagai negara non-ASEAN menjadi salah satu penggerak aktif kerja sama *Greater Mekong Subregion.* Keterhubungan yang dilihat bukan hanya keterhubungan fisik saja, melainkan juga keterhubungan institusi dan keterhubungan masyarakat. Kerja sama sub-kawasan di ASEAN sangat penting, terutama untuk mempersempit adanya gap perkembangan antara ASEAN bagian utara dengan negara anggota ASEAN yang lainnya. Dalam artikel ini juga dibahas mengenai peran kerja sama sub-kawasan di ASEAN dalam membangun keterhubungan yang akan mendorong kesuksesan implementasi Komunitas ASEAN.

Sebagaimana yang telah dijelaskan di awal bahwa salah satu tantangan bagi Indonesia dalam melaksanakan Komunitas ASEAN adalah masih rendahnya tingkat kesadaran masyarakat di Indonesia terhadap Komunitas ASEAN. Hal ini sesuai dengan hasil survey yang dilaksanakan oleh Pusat Penelitian Politik pada tahun 2015. Dalam ringkasan penelitian terakhir berjudul **"Strategi Peningkatan Pemahaman Masyarakat tentang Masyarakat Ekonomi ASEAN"** yang disusun oleh Khanisa, dkk dijelaskan bahwa kesadaran dan pemahamann publik menjadi faktor kunci yang menentukan apakah pilar-pilar yang yang telah disusun untuk mewujudkan Komunitas ASEAN dapat direalisasikan dengan baik. Hasil penelitian ini menghasilkan beberapa rekomendasi yang ditujukkan untuk Kementerian terkait. Strategi yang disarankan salah satunya adalah menekankan sebuah upaya berkelanjutan dan memiliki sasaran yang lebih nyata dalam melaksanakan program-program sosialisasi mengenai ASEAN dan Komunitas ASEAN kepada masyarakat.

Catatan redaksi kali ini kami tutup dengan ucapan terima kasih kepada segenap pihak yang telah berkontribusi sehingga *Jurnal Penelitian Politik* edisi kali ini dapat terbit. Terima kasih kami ucapkan untuk penulis, mitra bestari, serta tim pengelola jurnal. Semoga *Jurnal Penelitian Politik* ini dapat bermanfaat dalam memperkaya khasanah keilmuan dan praktis terkait dengan kajian mengenai ASEAN dan Komunitas ASEAN, serta dampaknya bagi Indonesia. Selamat membaca.

Redaksi

Jurnal Penelitian Politik
Vol. 13, No. 1, Juni 2016

DDC: 324.2598

David Putra Setyawan, Arwin Datumaya Wahyudi Sumari

DIPLOMASI PERTAHANAN INDONESIA DALAM PENCAPAIAN CYBERSECURITY MELALUI ASEAN REGIONAL FORUM ON CYBERSECURITY INITIATIVES

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 1-20

Perkembangan teknologi informasi di dunia internasional berdampak pada penggunaan ruang cyber yang mencakup semua aspek kehidupan nasional. Dihadapkan pada kondisi ini, pemerintah harus memahami kondisi cybersecurity di Indonesia dan membangunnya agar mampu mengatasi berbagai ancaman yang datang melalui ruang cyber. Selain kondisi internal, ruang lingkup eksternal perlu diperhatikan mengingat ancaman cyber yang bersifat transnasional, melewati batas kedaulatan, dan telah dipandang sebagai ancaman bersama oleh negara-negara di dunia. ASEAN telah menjadi salah satu wadah bagi Indonesia untuk memperjuangkan kepentingan nasionalnya dalam rangka mendukung keamanan nasional di bidang cyber. Melalui ASEAN Regional Forum (ARF) on cybersecurity initiatives, strategi diplomasi pertahanan diarahkan untuk meningkatkan rasa saling percaya (confidence building measures) antar negara dan mengurangi potensi ancaman yang dapat ditimbulkan dari lingkup eksternal. Upaya tersebut, menghasilkan kesepakatan berupa point of contacts antar negara dan persamaan pandangan untuk terus mengadakan pelatihan cybersecurity dalam bentuk seminar maupun workshop untuk membangun kapasitas sumber daya manusia. Strategi dan upaya tersebut dianalisis melalui pendekatan kualitatif dan data-data primer dikumpulkan melalui wawancara dengan 15 informan dari berbagai instansi pemerintahan. Selain itu, literatur, jurnal, dan dokumen terkait juga digunakan sebagai data pendukung.

Kata Kunci: ARF, confidence building measures, cybersecurity, diplomasi pertahanan

DDC: 324.2598

Fathimah Fildzah Izzati

MEMBACA "PHK MASSAL": RANTAI NILAI INDUSTRI ELEKTRONIK, MEA, DAN TANTANGAN BAGI GERAKAN BURUH DI INDONESIA

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 21-32

"PHK Massal" sempat menjadi isu dalam politik perburuhan awal tahun 2016 setelah kemunculan paket kebijakan ekonomi yang dikeluarkan dalam rangka menyambut keterlibatan Indonesia dalam MEA. Adanya konstruksi kata "massal" dalam isu PHK ini tidak sejalan dengan data ketenagakerjaan, namun lebih terkait erat dengan politik produksi dalam industri elektronik. Pada sisi lain, kerentanan gerakan buruh di sektor elektronik pun kian meningkat seiring dengan meningkatnya fleksibilitas pasar tenaga kerja dalam rezim pasar bebas, termasuk dalam konteks MEA. Tulisan ini membahas hubungan antara isu PHK massal dengan rantai nilai industri elektronik di tingkat global, MEA, dan tantangan bagi gerakan buruh di Indonesia. Tujuannya untuk menunjukkan peran gerakan buruh dalam menghadapi skema ekonomi seperti MEA terutama di dalam industri elektronik melalui analisis teori rantai nilai. Dengan menggunakan metode kualitatif berupa studi literatur, tulisan ini menemukan bahwa gerakan buruh di Indonesia memiliki

peluang yang besar untuk membangun kekuatan di tingkat regional dengan memosisikan dirinya di dalam rantai nilai global dan rezim pasar tenaga kerja fleksibel.

Kata Kunci: PHK Massal, Rantai Nilai Industri Elektronik, Fleksibilitas Pasar Tenaga Kerja, MEA, Gerakan Buruh

---

DDC: 320.014

Ahmad Rizky Mardhatillah Umar

TRANSFORMASI RUANG DAN PARTISIPASI *STAKEHOLDERS*: MEMAHAMI KETERLIBATAN MASYARAKAT SIPIL DAN USAHA KECIL DAN MENENGAH INDONESIA DALAM PROSES REGIONALISME ASEAN PASCA-2003

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 33-52

Artikel ini mencoba untuk menjelaskan keterlibatan stakeholders tersebut dalam dua sektor regionalisasi ASEAN: Hak Asasi Manusia (HAM) dan Usaha Kecil & Menengah (UKM). Sejak bertransformasi menjadi bentuk 'Masyarakat ASEAN' pada tahun 2003, mulai muncul interaksi yang lebih kompleks antara 'negara' dan aktor-aktor 'non-negara'. Sebelum 2003, ASEAN hanya diposisikan sebagai 'organisasi internasional' yang berpusat pada negara anggota sebagai satu-satunya aktor di kawasan. Menyusul diberlakukannya Masyarakat ASEAN pada tahun 2003, artikel ini berargumen bahwa Masyarakat ASEAN telah membuka ruang yang lebih besar bagi kontestasi antara negara dan 'pemangku kepentingan'/ stakeholders yang ada di dalamnya, terutama kelompok bisnis (konglomerat dan UKM) serta organisasi masyarakat sipoil. Dengan menggunakan perspektif kritis, artikel ini mencoba untuk menunjukkan bahwa sebetulnya pola interaksi yang terbangun antara aktor-aktor 'non-negara' dan 'negara' dalam spektrum Masyarakat ASEAN dimungkinkan oleh interaksi yang kian besar antara aktor-aktor yang ada di dalamnya, sehingga membuka kontestasi antar-stakeholders dalam organisasi regional yang telah bertransformasi. Hal ini kemudian memberikan pemahaman yang lebih kompleks tentang regionalisme di Asia Tenggara. Argumen tersebut akan dijelaskan melalui dua studi kasus, yaitu aktivitas Organisasi Masyarakat Sipil HAM dan Usaha Kecil dan Menengah di Indonesia.

Kata Kunci: Regionalisme, Partisipasi, Pemangku Kepentinganj, Masyarakat ASEAN, Asia Tenggara, Organisasi Masyarakat Sipil, Usaha Kecil & Menengah

---

DDC: 320.014

Sandy Nur Ikfal Raharjo

KETAHANAN SOSIAL WARGA PERBATASAN INDONESIA MENGHADAPI MASYARAKAT EKONOMI ASEAN: STUDI DI KECAMATAN ENTIKONG, KALIMANTAN BARAT

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 53-68

Masyarakat Ekonomi ASEAN (MEA) sudah mulai diberlakukan pada akhir tahun 2015, dan akan ditarnsformasikan menjadi MEA yang inklusif pada tahun 2025. Sebagai penduduk kawasan perbatasan yang pintu gerbang lintas batas Indonesia-Malaysia, masyarakat Entikong harus memiliki ketahanan sosial yang kuat untuk menghadapi semakin bebasnya pergerakan orang dan barang di wilayah mereka. Tulisan ini mengkaji kondisi ketahanan sosial masyarakat Entikong dalam menghadapi MEA tersebut. Dengan menggunakan kerangka Sustainable Livelihood Approach yang dimodifikasi, tulisan ini mengidentifikasi bahwa masyarakat Entikong memiliki empat modal ketahanan sosial yang kuat, yaitu modal alam, modal sosial, modal keuangan, dan modal politik/pemerintahan, serta dua modal yang masih lemah, yaitu modal fisik dan modal manusia. Selain itu, ketahanan sosial masyarakat Entikong juga dibantu dengan pelaksanaan kerja sama lintas Indonesia-Malaysia.Tulisan ini menyarankan reoptimalisasi kerja sama lintas batas dan pengaturan khusus perdagangan lintas batas di dalam MEA.

Kata Kunci: Entikong, ketahanan sosial, kerja sama lintas batas, Masyarakat Ekonomi ASEAN

DDC: 320.014
Ikrar Nusa Bhakti, Diandra Mengko

INTELIJEN DALAM PUSARAN DEMOKRASI DI INDONESIA PASCA ORDE BARU

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 69-82

Intelijen merupakan topik kajian yang penting sekaligus rumit untuk dipahami karena sifat kerahasiaannya. Meski demikian, negara demokrasi selalu mendukung masyarakatnya untuk memiliki, setidaknya, pemahaman dasar terkait seluruh instansi pemerintah, termasuk intelijen. Pada tahun 2015, Pusat Penelitian Politik – Lembaga Ilmu Pengetahuan Indonesia (P2P-LIPI) telah melakukan penelitian yang berjudul "Intelijen dalam Pusaran Demokrasi di Indonesia Pasca Orde Baru". Penelitian ini bukan saja berisi mengenai teori intelijen, pergumulan intelijen dan demokrasi di beberapa negara yang mengalami perubahan politik dari sistem otoriter ke demokrasi dan sejarah singkat intelijen di Indonesia, melainkan juga memuat ulasan awal demokratisasi intelijen di Indonesia. Reformasi intelijen di Indonesia adalah suatu keniscayaan. Intelijen harus bekerja sesuai dengan sistem demokrasi yang kita anut. Paradigma lama intelijen Indonesia sudah pasti akan dan harus berubah, pengawasan terhadap intelijen pun suatu keniscayaan. Adalah suatu keniscayaan pula bahwa pengawasan terhadap intelijen bukan membuat kerja-kerja rahasia mereka menjadi terbatas atau terhambat, melainkan justru intelijen mendapatkan kepercayaan dan didukung oleh rakyat, sehingga meningkatkan legitimasi intelijen dan tentunya peningkatan anggaran intelijen.

Kata Kunci : Demokrasi, Intelijen, Indonesia, Politik, Pasca Orde-Baru

---

DDC: 352.14
Awani Irewati

PROBLEMATIKA KERJA SAMA PERBATASAN SEPANJANG SUNGAI MEKONG ANTARA TIONGKOK DAN ASEAN BAGIAN UTARA

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 83-104

Selama berabad-abad, sungai Mekong telah menjadi pusat kehidupan orang enam negara riparian ini. Secara geografis, mengalir melalui negara-negara tersebut untuk sekitar 4.900 km. Ini menciptakan sebuah DAS 795.000 km², didistribusikan antara Upper Mekong River Basin yang terbentuk oleh China (21 persen) dan Myanmar (3 persen), serta Lower Mekong River Basin, yang terdiri Laos (25 persen), Thailand (23 persen), Kamboja (20 persen), dan Viet Nam (8 persen) (FAO, 2011). Untuk memenuhi kebutuhan orang-orang mereka sendiri di atas Sungai Mekong dan sub regional yang, negara-negara riparian telah mengembangkan beberapa inisiatif kerjasama lintas batas di antara mereka. Greater Mekong Subregion (GMS), Mekong Ricer Komisi [MRC] dll adalah contoh dari kerjasama lintas batas. Selain itu, ada beberapa kerjasama lain yang mencakup seluruh atau sebagian dari sub regional Mekong tetapi tidak secara khusus fokus pada Mekong River, yaitu ASEAN-China Free Trade Area dan Komunitas ASEAN. Kondisi ini menciptakan kompleksitas hubungan antara kerjasama di sub regional Mekong. Analisis tulisan ini beberapa potensi/ masalah yang ada yaitu kemungkinan bahwa mereka kerjasama tumpang tindih; perbedaan profil negara-negara 'tampaknya membuat kepentingan yang berbeda di antara mereka dll Analisis tersebut didasarkan pada beberapa penelitian lapangan di beberapa tempat (Vietnam, Laos, Thailand) pada tahun 2015.

Kata kunci: kerjasama lintas batas, negara-negara ASEAN Utara, RUPS, MRC, Sungai Mekong, konektivitas.

DDC: 352.14
Khanisa

STRATEGI PENINGKATAN PEMAHAMAN MASYARAKAT TENTANG MASYARAKAT EKONOMI ASEAN

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 105-118

ASEAN tengah merubah pendekatan instutusinya dari top-to-bottom ke cara yang lebih memasyarakat. Penciptaan sebuah komunitas mendorong ASEAN untuk bersikap

lebih inklusif dalam implementasi program-programnya. Dalam mewujudkan Masyarakat Ekonomi ASEAN, kesadaran dan pemahaman publik adalah faktor kunci yang menentukan apakah pillar ini akan dapat direalisasikan dengan sukses. Mengingat popularitas dari ASEAN dan kerangka-kerangkanya tidak diketahui secara signifikan di Indonesia, survei dan policy paper yang kemudian diterbitkan bertujuan untuk mengetahui tingkat pemahaman mengenai Masyarakat Ekonomi ASEA yang mulai di terapkan tahun lalu.

Kata Kunci : ASEAN, Masyarakat Ekonomi ASEAN, Indonesia, Survei Publik.

DDC: 320.014

Nanto Sriyanto

NEOTRADISIONALISME DAN DISTOPIANISME: TINJAUAN ATAS TIGA BUKU ROBERT D. KAPLAN

Jurnal Penelitian Politik
Vol. 13 No. 1, Juni 2016, Hal. 119-136

Artikel ini bertujuan menganalisa tulisan Robert D. Kaplan terutama yang terungkap dalam tiga publikasinya yaitu *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Vintage Books. 2000), *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate* (New York: Random House Publishing. 2013), dan *Asia's Cauldron: the South China Sea and the End of A Stable Pacific* (New York: Random House. 2014). Robert D. Kaplan dengan pendekatan geopolitik dan berlatar belakang sebagai wartawan yang mengalami langsung sejumlah perubahan penting pasca-Perang Dingin membawa pesan tentang negaran gagal yang mengancam stabilitas global, utamanya negara-negara maju (2000), kebangkitan pemikiran klasik geopolitik dalam dunia yang semakin padat dengan kekuatan yang terpolarisasi (2013), dan implikasinya terhadap kawasan Asia Timur sebagai kawasan yang rawan konflik. Dari ketiga publikasi Kaplan tersebut, penulis melihat pesan senada yang berwujud dalam bentuk bangkitnya pemikiran neotradisionalisme realis dalam hubungan internasional dan distopianisme. Di lain pihak, penulis juga melihat kekurangan dalam uraiannya yang popular dan menarik minat banyak pembaca dari kalangan luas, baik akademisi, aktivis LSM, bahkan pengambil keputusan, Kaplan terbilang tidak cukup mengupas posisi teoritisnya dibandingkan teori yang ada yang menjadi diskursus akademik. Alih-alih memunculkan paparan yang holistik sebagaimana ia sebagai pengamat lapangan dan travel journalis menempatkan diri dalam setiap publikasinya, tulisan Kaplan harus dikritisi secara akademik karena tidak cukup utuh memberikan pandangan sebagaimana klaimnya yang banyak diungkap.

Kata Kunci: Robert D. Kaplan, geopolitik, realis neotradisonalisme, holistik, travel journalist

Jurnal Penelitian Politik
Vol. 13, No. 1, Juni 2016

DDC: 324.2598

David Putra Setyawan, Arwin Datumaya Wahyudi Sumari

INDONESIA DEFENSE DIPLOMACY IN ACHIEVING CYBERSECURITY THROUGH ASEAN REGIONAL FORUM ON CYBERSECURITY INITIATIVES

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 1-20

The development of information technology in the international world impacts to the use of cyberspace which covers all aspects of national life. Faced to this condition, Indonesian government needs to understand the state of cyber security and build it so that able to address any kind of threat which comes through cyberspace. In addition to internal conditions, the scope of the external noteworthy to be considered due the nature of cyber threats are transnational, cross the line of sovereignty, and has been seen as a common threat by the countries of the world. ASEAN has become a forum for Indonesia's to achieve national interests in order to support national security in the cyber field. Through the ASEAN Regional Forum (ARF) on cybersecurity initiatives, defense diplomacy strategy directed to increasing mutual trust (confidence building measures) between states and reduce any potential threats that may result from the external sphere. Those efforts, resulted in an agreement in the form of point of contacts between states and a shared vision for continuous training of cybersecurity in the form of seminars and workshops to build the capacity of human resources. Strategies and efforts are analyzed through a qualitative approach and primary data were collected through interviews with 15 informants from various government agencies. In addition, literature, journals, and related documents are also used as supporting data.

Key Words: *ARF, confidence building measures, cybersecurity, defense diplomacy*

DDC: 324.2598

Fathimah Fildzah Izzati

THE "MASS LAYOFFS": ELECTRONICS INDUSTRY VALUE CHAIN, AEC, AND CHALLENGES FOR LABOUR MOVEMENT IN INDONESIA

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 21-32

"Mass layoffs" issue has been rising in labour's political discourse in Indonesia since early 2016, following the announcement of economic policy package to face the Asean Economic Community (AEC). However, the word "mass" constructed in the issue goes against the employment data and is more closely related to political interests related to production in the electronics industry. On the other hand, labour movement issue in the electronics sector is also emerging along with the increase of labour market flexibility in this free market era, including the context of AEC. This study discusses the relationship between the mass layoffs issue, the implementation of AEC, and the labour movement in Indonesia, as well as the value chain of the electronics industry on the global level. It aims to show the role of labour movement in facing an economic scheme like AEC especially in electronics industry using value chain theory analysis. By using qualitative approach and literature review, the study found

that the labour movement in Indonesia has an excellent opportunity to build strength at the regional level by positioning themselves in the global value chain and flexible labour market regime.

Keywords: *Mass layoffs, Value Chain, Electronics Industry, Labor Market Flexibility, AEC, Labour Movement.*

DDC: 320.014

Ahmad Rizky Mardhatillah Umar

SPACE TRANSFORMATION AND STAKEHOLDERS PARTICIPATION: UNDERSTANDING INVOLVEMENTS OF INDONESIAN CIVIL SOCIETY ORGANISATIONS AND SMALL AND MEDIUM ENTERPRISES IN POST-2003 REGIONALISM IN ASEAN

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 33-52

This article aims to explain the participation of stakeholders in the making of ASEAN Community after the regional political-economic transformation in 2003. The establishment of ASEAN Community, which is based on three pillars (politics & security, economics, social and cultural) has led to a more complex interactions between actors in the region. Before 2003, ASEAN has been perceived only as an 'international organisation', which is centered around the 'member states' as the only influential actor in the region. Following the establishment of ASEAN Community as a new form of regionalism in 2003, this article argues that the newly-established regional community has opened up spaces for contestations between the state and other new actors in the region, most notably business actors (both big businesses and small-and-medium enterprises) and civil society organisations. Drawn upon the critical perspective, this article argues that emerging interactions between actors in the region has been enabled by the transformation of space structure in ASEAN, that opened up spaces for contestations between stakeholders in the newly-transformed regional organisation. It thus leads to the more complex understanding of regionalism in Southeast Asia. The arguments provided will also be assessed by two case studies on the regionalisation of Human Rights NGOs and Small-and-Medium Enterprises in Indonesia.

Keywords: regionalism, participation, stakeholders, ASEAN community, southeast asia, non-government organisations, small-and-medium enterprises.

DDC: 320.014

Sandy Nur Ikfal Raharjo

THE SOCIAL RESILIENCE OF INDONESIAN BORDER AREA RESIDENTS TOWARDS THE ASEAN ECONOMIC COMMUNITY: A STUDY IN ENTIKONG SUBDISTRICT, WEST KALIMANTAN

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 53-68

ASEAN Economic Community (AEC) was formally come into force at the end of 2015, and will be further transformed to be more inclusive by 2025. To deal with this issue, the residents of Entikong subdistrict at the Indonesia-Malaysia borderland should have a strong social resilience. This article explain the author's work on the social resilience assessment of the Entikong residents towards the AEC implementation. By using a modified Sustainable Livelihood Approach, the result shows that Entikong residents have four adequate social resilience assets, namely natural capital, social capital, financial capital, and political capital. Unfortunately, they are still weak on physical and human capitals. This work also shows that cross-border cooperation implementation gives positive effects to the residents. For recommendation, cross-border cooperation should be re-optimized and a special treatment of border trade in AEC should be arranged.

Keywords: *Entikong, Social Resilience, Cross-border Cooperation, ASEAN Economic Community.*

DDC: 320.014
Ikrar Nusa Bhakti, Diandra Mengko

INTELLIGENCE AND DEMOCRATIZATION IN INDONESIA POST NEW-ORDER

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 69-82

Intelligence is an important and also complicated topic to study and understand because of its nature of secrecy. However, democracy always pushes the people to have at least basic comprehension of all government agencies, including the world of intelligence. Along with that spirit, Center for Political Studies, Indonesian Institute of Sciences (P2P-LIPI) was conducting research entitled "Intelligence and Democratization in Indonesia Post New-Order" in 2015. This research not only discuss about intelligence theories, but also intelligence experience in transitional democracy states, brief history of Indonesian intelligence, and initial review on democratization of intelligence in Indonesia. We argue that intelligence reform in Indonesia is a requisite. Intelligence should operate under democratic system and principles. Oversight mechanism would not weaken intelligence role -in contrast, it would enhance intelligence professionalism by gaining public support, legitimacy, and adequate budget.

Keywords: *Democracy, Intelligence, Indonesia, Politics, Post New-Order*

DDC: 352.14
Awani Irewati

PROBLEMATIC BORDER COOPERATION ALONG THE MEKONG RIVER BETWEEN CHINA AND ASEAN NORTHERN

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 83-104

For centuries, the Mekong river has become the center of six riparian countries's people life. Geographically, it flows through these countries for about 4,900 km. It created a 795,000 km² river basin, distributed between the Upper Mekong River Basin that is formed by China (21 percent) and Myanmar (3 percent), as well as the Lower Mekong River Basin, which comprised Laos (25 percent), Thailand (23 percent), Cambodia (20 percent), and Viet Nam (8 percent) (FAO, 2011). To fullfill their own people's needs over the Mekong River and its subregion, those riparian states have been developing some transboundary cooperation initiatives among them. Greater Mekong Subregion (GMS), Mekong Ricer Commission [MRC] etc. are examples of the transboundary cooperation. Besides, there are some other cooperations that cover the whole or part of the Mekong subregion but do not specifically focus on Mekong River, i.e. ASEAN-China Free Trade Area and ASEAN Community. This condition creates a complexity of relationships among the cooperations in the Mekong subregion. This paper analysis some potential/existing problems i.e. a possibility that those cooperations overlap; the differences in the countries' profile seem to create different interests among them etc. The analysis is based on some field research in some places [Vietnam, Laos, Thailand] in 2015.

Keywords: transboundary cooperation, Northern ASEAN countries, GMS, MRC, Mekong River, connectivity.

DDC: 352.14
Khanisa

STRATEGY TO INCREASE PUBLIC UNDERSTANDINGS ABOUT ASEAN ECONOMIC COMMUNITY

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 105-118

ASEAN is gradually changing their approach from top-to-bottom to a more grassroot style institution. The idea of creating a community push ASEAN to be more inclusive in implementing its programes. In realizing ASEAN Economic Community, public awareness and undertsndings is the key factor in whether the implementation of this ASEAN's pillar will succeed. Recalling that the popularity of

ASEAN and its frameworks are not significantly known in Indonesia, the survey and the policy paper that followed aim to find out the level of public understandings about ASEAN Economic Community which started to be implemented last year.

Keywords: *ASEAN, ASEAN Economic Community, Indonesia, public survey.*

DDC: 320.014

Nanto Sriyanto

NEOTRADISIONALISME DAN DISTOPIANISME: REVIEW FOR THREE BOOKS OF ROBERT D. KAPLAN

Jurnal Penelitian Politik
Vol. 13 No. 1, June 2013, Page 119-136

This article is to analyze three publications of Robert D. Kaplan, which consist of The Coming Anarchy: Shattering the Dreams of the Post Cold War (New York: Vintage Books. 2000), The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate (New York: Random House Publishing. 2013), and Asia's Cauldron: the South China Sea and the End of A Stable Pacific (New York: Random House. 2014). In those three publications, Kaplan utilizes geopolitical approach and embedded journalism in examining turbulent world in post-Cold War era. His arguments contain in the three books could be summarized as follows: failed states has threatened the stability the world, especially the prosperous developed countries (2000), resurgent of classical geopolitical thinking on tackling shrinking space yet polarized world politics (2013), implication on East Asia region as the volatile zone prone to conflict in the future. Based on the three publications, it could be seen that Kaplan is a proponent of neotraditional realism in IR studies, and it brings about dystopian thesis in those publications. Nevertheless it is discernible to note that despite his prosaic nature in almost of his writings that has attracted wider readership spread from academics, NGO's activists, and decision maker, Kaplan has not given enough space to discuss his theoretical position before he comes up with single theoretical perspective. Therefore, instead of giving a holistic picture about his subject in those three publications, his arguments and thesis which he claims based on embedded journalism and field observation should be criticised due to imbalance description and short-sighted conclusion.

Key Words: Robert D. Kaplan, geopolitic, neotradisionalism realist, holistic, travel journalist

DIPLOMASI PERTAHANAN INDONESIA DALAM PENCAPAIAN *CYBERSECURITY* MELALUI ASEAN REGIONAL FORUM *ON CYBERSECURITY INITIATIVES*

INDONESIA DEFENSE DIPLOMACY IN ACHIEVING CYBERSECURITY THROUGH ASEAN REGIONAL FORUM ON CYBERSECURITY INITIATIVES

David Putra Setyawan dan Arwin Datumaya Wahyudi Sumari

Alumnus Program Pascasarjana Universitas Pertahanan Indonesia, Program Studi Diplomasi Pertahanan, Fakultas Strategi Pertahanan. Kawasan IPSC, Sentul, Bogor.
e-mail: fa.davidsetyawan@gmail.com

Diterima: 2 Mei 2016; direvisi: 21 Juni 2016; disetujui: 22 Juli 2016

Abstract

The development of information technology in the international world impacts to the use of cyberspace which covers all aspects of national life. Faced to this condition, Indonesian government needs to understand the state of cyber security and build it so that able to address any kind of threat which comes through cyberspace. In addition to internal conditions, the scope of the external noteworthy to be considered due the nature of cyber threats are transnational, cross the line of sovereignty, and has been seen as a common threat by the countries of the world. ASEAN has become a forum for Indonesia's to achieve national interests in order to support national security in the cyber field. Through the ASEAN Regional Forum (ARF) on cybersecurity initiatives, defense diplomacy strategy directed to increasing mutual trust (confidence building measures) between states and reduce any potential threats that may result from the external sphere. Those efforts, resulted in an agreement in the form of point of contacts between states and a shared vision for continuous training of cybersecurity in the form of seminars and workshops to build the capacity of human resources. Strategies and efforts are analyzed through a qualitative approach and primary data were collected through interviews with 15 informants from various government agencies. In addition, literature, journals, and related documents are also used as supporting data.

Keywords*: ARF, confidence building measures, cybersecurity, defense diplomacy*

Abstrak

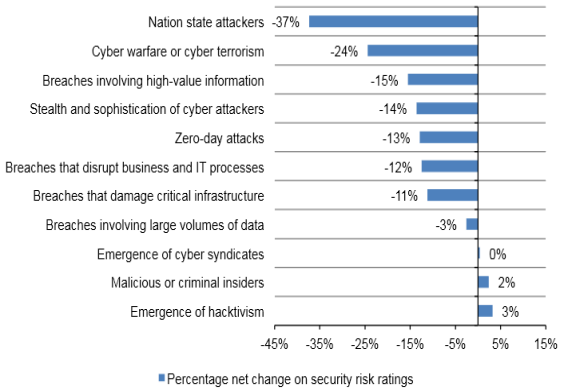
Perkembangan teknologi informasi di dunia internasional berdampak pada penggunaan ruang *cyber* yang mencakup semua aspek kehidupan nasional. Dihadapkan pada kondisi ini, pemerintah harus memahami kondisi *cybersecurity* di Indonesia dan membangunnya agar mampu mengatasi berbagai ancaman yang datang melalui ruang *cyber*. Selain kondisi internal, ruang lingkup eksternal perlu diperhatikan mengingat ancaman *cyber* yang bersifat transnasional, melewati batas kedaulatan, dan telah dipandang sebagai ancaman bersama oleh negara-negara di dunia. ASEAN telah menjadi salah satu wadah bagi Indonesia untuk memperjuangkan kepentingan nasionalnya dalam rangka mendukung keamanan nasional di bidang *cyber*. Melalui ASEAN Regional Forum (ARF) *on cybersecurity initiatives*, strategi diplomasi pertahanan diarahkan untuk meningkatkan rasa saling percaya (*confidence building measures*) antar negara dan mengurangi potensi ancaman yang dapat ditimbulkan dari lingkup eksternal. Upaya tersebut, menghasilkan kesepakatan berupa *point of contacts* antar negara dan persamaan pandangan untuk terus mengadakan pelatihan *cybersecurity* dalam bentuk seminar maupun *workshop* untuk membangun kapasitas sumber daya manusia. Strategi dan upaya tersebut dianalisis melalui pendekatan kualitatif dan data-data primer dikumpulkan melalui wawancara dengan 15 informan dari berbagai instansi pemerintahan. Selain itu, literatur, jurnal, dan dokumen terkait juga digunakan sebagai data pendukung.

Kata Kunci: ARF*, confidence building measures, cybersecurity,* diplomasi pertahanan

Pendahuluan

Perubahan yang terjadi dalam peradaban dunia, yang salah satunya ditandai dengan kemajuan teknologi, menyebabkan ancaman terhadap kedaulatan satu negara menjadi semakin kompleks. Dunia tidak lagi memandang militer sebagai satu-satunya potensi ancaman, melainkan mulai merespon terhadap ancaman nirmiliter. Salah satu ancaman nirmiliter di bidang teknologi, adalah ancaman *cyber*. Teknologi *cyber* yang terus berkembang dengan berbagai infrastrukturnya telah membuat batas antar negara menjadi semakin kabur. Konektifitas, kecepatan, dan kemudahan akses yang dimilikinya menjadi suatu hal positif yang dimanfaatkan oleh masyarakat di berbagai negara karena persebaran informasi yang semakin mudah. Sebagai gambaran, tercatat bahwa hingga kuartal ke-2 tahun 2015, pengguna internet di dunia telah mencapai 3.2 milliar[1]. Transaksi perbankan, analisis dan komputasi data di perusahaan maupun pemerintahan, teknologi militer, hingga masyarakat umum memanfaatkan *cyberspace* sebagai media komunikasi.

Meskipun menawarkan manfaat dan keuntungan yang begitu besar, *cyberspace* juga menjadi sumber dari berbagai ancaman, kerentanan, dan ketidakamanan. Menurut Smith ancaman tersebut dapat bersumber dari pemerintah, organisasi, individu, atau pengusaha, baik secara disengaja maupun tidak demi mendapatkan keuntungan secara finansial, militer, politik, maupun tujuan lainnya[2]. *Cyber* dapat menjadi ancaman bagi suatu negara karena ruang lingkupnya yang dapat digunakan untuk mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap sistem informasi di berbagai bidang, seperti data perbankan maupun jaringan militer dan sistem pertahanan negara. Survey yang dilakukan oleh Ponemon *Institute* pada tahun 2015 terhadap 1006 pemimpin senior *Information Technology* (IT) dan IT *Security* di berbagai perusahaan dan instansi pemerintah di Amerika, Eropa, Timur Tengah, dan Afrika menjelaskan tentang adanya peningkatan serangan terus menerus pada negara yang semakin canggih diikuti dengan *cyber warfare* atau terorisme *cyber* dan pembobolan data yang bernilai tinggi. Lebih lanjut, beberapa trend mengenai kejahatan *cyber* di dunia dapat dilihat pada Gambar 1 *Percentage net changes in cyber crime megatrends*.[3]



Sumber: Ponemon Institute, 2015

Gambar 1. *Percentage net changes in cyber crime megatrends*

Data yang ditampilkan menunjukkan bahwa keamanan *cyberspace* terhadap serangan yang mengarah kepada negara menurun sebesar -37%, yang diikuti dengan *cyber warfare* atau *cyber terrorism* sebesar 24%, pencurian data bernilai tinggi sebesar -15%, dan diikuti beberapa kategori ancaman lainnya. Kondisi dunia yang dihadapkan pada perang generasi keempat dan kelima juga membutuhkan strategi penangkalan yang berbeda. Jika, konsep perang generasi sebelumnya bersifat konvensional dan lebih banyak melibatkan kontak fisik, maka konsep perang generasi keempat berada pada masyarakat yang saling terhubungkan (*networked*), bersifat lintas negara, dan berbasis informasi.[4] Serangan yang dilakukan pun

[1] Miniwatts Marketing Group, "Internet Usage Statistics", 30 Juni 2015, http://www.internetworldstats.com/stats.htm, diakses pada tanggal 5 November 2015.

[2] Michael Smith, "Research Handbook on International Law and Cyberspace", (Massachusetts: Edwar Elgar Publishing Limited, 2015), hlm. 1.

[3] Ponemon Institute, "2015 Global Megatrends in Cybersecurity", Ponemon Institute LLC, 2015 http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf, diakses pada tanggal 19 November 2015.

[4] Alman Helvas Ali, "Angkatan Laut dan Peperangan Generasi Keempat", Forum Kajian Pertahanan dan Maritim, 30 Mei 2015, http://www.fkpmaritim.org/angkatan-laut-dan-peperangan-

bervariasi, baik itu berupa intervensi informasi melalui media maupun penggunaan virus komputer yang dapat menyebabkan kerusakan infrastruktur kritis negara. Selain itu, perang pemikiran/ide, pembangunan opini melalui media sosial pada akhirnya dapat mempengaruhi kondisi politik, sosial dan budaya suatu negara merupakan wujud nyata ancaman perang generasi ke-empat. Tanpa adanya penguasaan pada ruang *cyber*, sangat mungkin keamanan dan stabilitas politik suatu negara dapat terganggu. Oleh sebab itu, seorang pemimpin pada generasi ini dituntut bukan hanya untuk menguasai seni perang (tradisional) melainkan juga teknologi.[5]

Pada konteks legal, Indonesia sudah memiliki peraturan perundang-udangan yang menangani persoalan keamanan yang berkenaan dengan bidang *cyber*, yaitu Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun, UU tersebut lebih menekankan kepada perlindungan transaksi elektronik dan belum mampu mencakup aspek *cyberspace* yang begitu luas. Sebagai gambaran terhadap luasnya ancaman *cyber,* terdapat beberapa kasus yang pernah dialami Indonesia. Pada tahun 2013 menjadi korban penyadapan oleh badan intelijen Australia berdasarkan bocoran dokumen dari seorang mantan anggota National Security Agency (NSA) Amerika, Edward Snowden. Dokumen tersebut berisi daftar target penyadapan percakapan telepon yang menunjukkan nama Presiden Indonesia Susilo Bambang Yudhoyono dan sembilan orang terdekat di lingkaran presiden.[6] Kemudian, Lembaga Indonesia Security Incidents Response Team on Internet Infrastructure (ID-SIRTII) mencatat bahwa ada 48.4 juta serangan *cyber* yang dialami oleh Indonesia pada tahun 2014. Lebih lanjut, terdapat juga serangan yang ditujukan kepada situs-situs resmi pemerintah seperti kesad.mil.id, paspampres.mil.id, revolusi mental.go.id, dan Indonesia juga tercatat sebagai negara dengan jumlah komputer yang terjangkit peranti jahat atau *malware* terbesar di dunia pada awal tahun 2015.[7] Selain itu, penggunaan situs-situs lokal untuk propaganda, perekrutan anggota, maupun penyimpangan ideologi yang sering dilakukan oleh kelompok teroris dan gerakan radikal lainnya. Kondisi ini menunjukkan bahwa ancaman *cyber* sangat kompleks dan dapat melibatkan berbagai aspek kehidupan nasonial.

Pada tataran operasional, pemerintah sedang dalam upaya untuk mewujudkan sebuah Badan *Cyber* Nasional (BCN) seperti yang tertuang pada *Framework* dan *Roadmap* BCN 2015-2019.[8] Namun, sejauh ini pembentukan badan tersebut belum dapat terealisasi. Hal inilah yang menggambarkan bahwa kondisi internal Indonesia dianggap belum mampu menangani ancaman *cyber* yang sudah, sedang dan akan terjadi di masa mendatang secara terpadu. Memandang bahwa ancaman *cyber* yang bersifat lintas negara, maka bentuk-bentuk kerjasama internasional dapat menjadi salah satu solusi yang dapat dilakukan dalam mengatasi ancaman *cyber*. Pada lingkup regional, pengamanan *cyberspace* untuk menjadi sesuatu yang mendesak telah menjadi pembahasan dalam berbagai diskusi dalam salah satu forum kerjasama politik dan keamanan *Association of South East Asian Nations* (ASEAN), yaitu ASEAN Regional Forum (ARF). Melalui kerjasama internasional di ARF, kebijakan luar negeri pemerintah dapat dimaksimalkan untuk mencapai *cyber security* sebagai salah satu kepentingan nasional bangsa. Strategi diplomasi yang tepat perlu digunakan sebagai instrumen dalam pencapaian kepentingan nasional. Lebih lanjut, diplomasi pertahanan dapat digunakan sebagai salah sarana untuk mencapai kepentingan nasional di bidang pertahanan dan keamanan.

Diplomasi pertahanan memiliki peran untuk meningkatkan keamanan dan stabilitas

generasi-keempat/, diakses pada tanggal 24 November 2015.

[5] William S. Lind, et all., "The Changing Face of War: Into The Fourth Generation", (Marine Corps Gazette, 1989), hlm. 22.

[6] Ewen MacAskill dan Lenore Taylor, "Australia's spy agencies targeted Indonesian president's mobile phone", The Guardian, 28 November 2013, http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone, diakses pada tanggal 25 November 2015.

[7] Aditya Panji Rahmanto, "Indonesia Jadi Sarang Malware Dunia. CNN Indonesia", 30 April 2015, http://www.cnnindonesia.com/teknologi/20150430163413-185-50331/indonesia-jadi-sarang-malware-dunia, diakses pada tanggal 25 November 2015.

[8] Munawar Ahmad, "Visi & Misi Badan Cyber Nasional dan Diplomasi Cyber", 15 April 2015, disampaikan pada Seminar ITB-Deplu, http://www.slideshare.net/msyani/badan-cyber-nasional, diakses pada tanggal 7 November 2015.

kawasan dalam menghadapi permasalahan yang ada agar eskalasi tidak meningkat kearah konflik serta ditujukan untuk saling memperkuat *confidence building measures* (CBM) dan sekaligus memperkuat stabilitas kawasan.[9] Lebih lanjut, diplomasi pertahanan memiliki tiga varian utama dalam implementasinya, yaitu *defence dilplomacy for confidence building measures, defence diplomacy for defense capabilites,* dan *defence diplomacy for defence* industries. Hal ini pada dasarnya sejalan dengan konsep ARF yang menggunakan aspek CBM dan *preventive diplomacy* dalam hal pencegahan konflik serta memiliki perhatian terhadap kerjasama keamanan. Namun, implementasi diplomasi pertahanan di ARF-pun tidak terlepas dari tantangan yang perlu dipahami oleh pemeritah Indonesia. Dinamika situasi di ARF serta kondisi internal Indonesia dalam membawa kepentingan nasional, khusunya dalam bidang *cyber*, perlu dipahami secara lebih komprehensif.

Berdasarkan hal tersebut, terdapat dua aspek utama yang perlu dipahami dalam upaya pencapaian *cybersecurity* Indonesia di ARF. Pertama, mekanisme ARF, khususnya *ARF on cybersecuriy initiatives* dalam membahas berbagai permasalahan terkait *cybersecurity*. Hal ini diperlukan agar kondisi dimana proses pencapaian tujuan nasional dilakukan dapat dipahami, sehingga implementasi strategi diplomasi pertahanan dapat dilakukan dengan tepat. Kedua, diplomasi pertahanan merupakan salah satu sarana dalam proses pencapaian kepentingan nasional. Oleh sebab itu, telaah mengenai kepentingan nasional Indonesia dalam bidang *cybersecurity* diperlukan agar dapat dilihat adanya kesesuaian antara kepentingan nasional yang menjadi tujuan, proses yang meliputi kebijakan nasional dan kebijakan luar negeri, serta hasil yang dicapai dalam ARF *on cybersecurity initiatives.* Lebih lanjut, pemahaman akan kedua aspek tersebut akan memberikan pemahaman bagaimana implementasi serta kontribusi diplomasi pertahanan Indonesia di ARF *on cybersecurity initiatives*.

ARF on C*ybersecurity Initiatives*

ASEAN Regional Forum (ARF) yang dibentuk pada tahun 1994 merupakan suatu forum yang bertujuan untuk mengembangkan dialog dan konsultasi konstruktif mengenai isu-isu politik dan keamanan yang menjadi kepentingan dan perhatian bersama, dan memberikan kontribusi positif dalam berbagai upaya untuk mewujudkan *confidence building* dan *preventive diplomacy* di kawasan Asia Pasifik. Peran ARF dalam pembentukan keamanan di bidang *cyber* tidak terlepas dari tujuan dibentuknya ASEAN *Political-Security Community* (APSC) yang bertujuan untuk membentuk perdamaian bagi negara-negara di kawasan ASEAN dan dunia dalam lingkungan yang demorkatis dan harmonis. Landasan mengenai APSC tersebut dijelaskan dalam dokumen APSC *blueprint* yang pada Sub Bab B.4.1 menyepakati mengenai peningkatan kerjasama dalam hal ancaman non tradisional, secara khusus mengenai kejahatan transnasional dan lintas batas. Pasal xvii pada Bab tersebut menjelaskan mengenai pengembangan hukum bagi setiap negara untuk menangani kejahatan *cyber.*[10]

Konsep dari ARF adalah untuk memelihara stabilitas keamanan kawasan dan pencegahan konflik regional. Berdasarkan hal tersebut, ARF memperkenalkan norma baru dalam ASEAN mengenai proses *cooperative security* yang menekankan konsep keterbukaan melalui promosi dialog diantara negara-negara yang memiliki kesamaan maupun perbedaan pemahaman mengenai isu tertentu. Berbeda dengan konsep kerjasama keamanan oleh *North Atlantic Treaty Organization* (NATO) yang dibentuk berdasarkan traktat atau aliansi pertahanan pasca Perang Dunia II, ARF ditujukan untuk membangun rasa saling percaya yang mengadopsi pendekatan multilateral untuk mencegah konflik di kawasan. Pendekatan perjanjian keamanannya pun diimplementasikan dengan cara yang berbeda. Karakter ARF tidak seperti NATO yang identik dengan penggunaan kekuatan militer, melainkan lebih kepada dialog dan keterlibatan sebagai cara

[9] Salim, "Peningkatan Kerjasama Pertahanan Indonesia di Kawasan Asia Tenggara Guna Mendukung Diplomasi Pertahanan Dalam Rangka Mewujudkan Stabilitas Kawasan", (Jakarta: Pusat Pengkajian Maritim Seskoal, 2012).

[10] ASEAN Secretariat, "ASEAN Political-Security Community Blueprint", 2009, http://www.asean.org/archive/5187-18.pdf, diakses pada tanggal 2 Desember 2015

pencegahan konflik.[11] Dengan demikian, konsep ARF sejalan dengan pendekatan APSC sebagai dasar dari lahirnya ARF yang mempromosikan penolakan agresi terhadap ancaman melalui penggunaan kekuatan dan lebih mengedepankan penyelesaian damai.

Hal tersebut sesuai dengan pemahaman *cooperative security* yang ditegaskan oleh Moodie sebagai suatu proses kerjasama antar negara dengan kepentingan yang sama untuk meredakan ketegangan dan kecurigaan, menyelesaikan atau mengurangi sengketa, membangun rasa percaya diri, maupun memelihara stabilitas kawasan.[12] Hingga saat ini, ARF membentuk lingkungan keamanan pada kawasan dengan pendekatan *cooperative security* melalui kerjasama regional yang diciptakan bukan untuk mengatasi konflik, melainkan meminimalkan dampak perbedaan persepsi dan kepentingan. Kondisi tersebut memberi pemahaman bahwa konsep ARF lebih cenderung kepada pendekatan *soft institutionalism* yang menerima nilai-nlai bersama dibandingkan dengan *hard institusionalism* yang berdasarkan pada yuridiksi dan supremasi hukum.[13]

ARF *on cybersecurity initiatives* merupakan bagian dari mekanisme ASEAN dalam menangani kejahatan *cyber* yang tertuang dalam *ASEAN's Cooperation on Cybersecurity and against Cybercrime*. Kerjasama tersebut melibatkan berbagai pertemuan internasional selain ARF, seperti ASEAN *Ministerial Meeting on Transnational Crime* (AMMTC), ASEAN *Senior Officials Meeting on Transnational Crime* (SOMTC), ASEAN *Telecommunications Regulators Council* (ATRC), dan *Senior Officials Meeting on Social Welfare and Development* (SOMSWD). Berbagai pertemuan tersebut memiliki perannya masing-masing dalam mewujudkan keamanan *cyber* di kawasan. ARF *on cybersecurity initiatives* mulai dilaksanakan pada tahun 2006 melalui pernyataan bersama pada pertemuan di Malaysia dan ditegaskan kembali pada ARF *Statement on Cooperation in Ensuring Cyber Security*, di Phnom Penh, 12 July 2012, sebagai berikut.[14]

1. *Promote further consideration of strategies to address threats emerging in this field consistent with international law and its basic principles;*
2. *Promote dialogue on confidence-building, stability, and risk reduction measures to address the implications of ARF participants' use of ICTs, including exchange of views on the potential use of ICTs in conflict;*
3. *Encourage and enhance cooperation in bringing about culture of cyber security;*
4. *Develop an ARF work plan on security in the use of ICTs, focused on practical cooperation on confidence building measures, which could set out corresponding goals and a timeframe for their implementation;*
5. *Review a possibility to elaborate common terms and definitions relevant to the sphere of the use of ICTs.*

Hasil dari pernyataan tersebut kemudian diimplementasikan dalam bentuk *workshop*, seminar, dan berbagai pelatihan di tingkat regional.[15] Salah satu fokus dari *workshop* tersebut adalah bagaimana suatu negara dalam merespon dan berkoordinasi ketika ada suatu *cyber incidents*. Pembahasan tersebut meliputi koordinasi respon nasional, cara penanggulangan, cara penindakan pelaku kejahatan antar negara, dan cara pandang terhadap suatu insiden yang melibatkan pelaku dari negara lain serta sejauh mana suatu negara menanggapi suatu insiden yang muncul dari negaranya.[16]

[11] Sisouwath Dong Chanto, "The ASEAN Regional Forum – The Emergence of 'Soft Security': Improving the Functionality of the ASEAN Security Regime", Dialogue+cooperation, 2003, hlm. 41-47.

[12] Michael Moodie, "Cooperative Security: Implications for National Security and International Relations,", (Cooperative Monitoring Center Occasional Paper, 2000), hlm. 5.

[13] Sisouwath Dong Chanto, *Loc. Cit.*

[14] ASEAN Secretariat, "ASEAN's Cooperation on Cybersecurity and against Cybercrime", (Strasbourg: ASEAN Secretariat, 2013)

[15] Direktorat Politik dan Keamanan ASEAN Kementerian Luar Negeri, wawancara pribadi, 21 Januari 2016

[16] Direktorat Politik dan Keamanan Sekeretariat ASEAN, wawancara pribadi, 15 Januari 2016.

Kerangka kerja tersebut juga tertuang dalam dokumen ASEAN *Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies (Ict's)* pada tanggal 7 Mei 2015. Beberapa sasaran yang ingin dicapai dalam *workplan* ini adalah:[17]

1. *Promote transparency and develop confidence building measures to enhance the understanding of ARF Participating Countries in the ICT environment with a view to reducing the risk of misperception, miscalculation and escalation of tension leading to conflict;*
2. *Raise awareness on threats related to the security of and in the use of ICTs;*
3. *Enhance practical cooperation between ARF Participating Countries to protect ICT-enabled critical infrastructure with the view to also developing resilient government ICT environments; and*
4. *Improve cooperation including develop regional capacity to respond to criminal and terrorist use of ICTs through improved coordination and coordinated response*

Berdasarkan pada sasaran-sasaran tersebut, ditetapkan beberapa aktivitas yang diikuti oleh negara-negara ASEAN dan non ASEAN anggota ARF. Aktivitas tersebut dilaksanakan sesuai dengan panduan kebijakan dan prosedur dalam ARF yang telah disepakati bersama. Lebih lanjut, negara pemimpin (*Lead Countries*), *co-sponsors*, dan partisipan dapat mengajukan proposal berdasarkan rencana kegiatan yang telah ditetapkan, dan nantinya dapat ditetapkan dalam sebuah *workplan*. Beberapa kegiatan yang telah diimplementasikan dalam rencana kerja tersebut adalah:[18]

1. *"ARF Workshop on Cyber Confidence Building Measures" by Australia and Malaysia, 25-26 March 2014, Kuala Lumpur, Malaysia.*
2. *"ARF Workshop on Measures to Enhance Cyber Security-Legal and Cultural Aspects" by China and Malaysia, 11-12 September 2013, Beijing, China.*
3. *"ARF Seminar on Confidence Building Measures in Cyberspace" by Republic of Korea and Malaysia, 11-12 September 2012, Seoul, Republic of Korea.*
4. *"ARF Workshop on Cyber Security Incident Response" by Australia and Singapore, 6-7 September 2012, Singapore.*
5. *"ARF Workshop on Proxy Actors in Cyberspace" by the United States and Vietnam, 14-15 March 2012, Hoi An, Vietnam*

Tujuan dari diadakannya *workplan* ini adalah sebagai suatu sarana untuk mempromosikan lingkungan ICT yang damai, aman, terbuka, dan saling bekerjasama serta untuk mencegah konflik dan krisis dengan mengembangkan kepercayaan antar negara anggota ARF dan peningkatan kapasitas. Keterlibatan pemerintah Indonesia dalam berbagai *workshop* tersebut diwakili oleh berbagai instansi terkait seperti Kementerian Luar Negeri, Kementerian Pertahanan, Kementeriaan Koordinator Politik, Hukum, dan Keamanan, dan Desk Ketahanan Keamanan Informasi *Cyber* Nasional[19].

Kepentingan Nasional Indonesia dalam ARF on *Cybersecurity Initiatives*

Keikutsertaan Indonesia dalam ARF *on cybersecurity initiatives* menggambarkan keinginan Indonesia dalam pencapaian kepentingan nasionalnya melalui lingkup internasional. Tindakan ini juga merupakan salah satu pemahaman bahwa lingkungan eksternal memiliki pengaruh pada kondisi nasional Indonesia. Jika merujuk pada pemahaman Jackson&Sorensen yang menjelaskan bahwa kepentingan nasional terbentuk dari asumsi bersama suatu bangsa terhadap kondisi tertentu

[17] ASEAN Regional Forum, "ASEAN Regional Forum on Security of and in The Use of Information and Communications Technologies (ICT's)", Cooperation in Ensuring Cyber Security, ARF Library, Phnom Penh, 2015, hlm. 1.

[18] *Ibid*.

[19] Direktorat Politik dan Keamanan ASEAN Kementerian Luar Negeri, wawancara pribadi, 21 Januari 2016

yang mengharuskan suatu negara menjadikannya perhatian mendasar,[20] maka keikutsertaan Indonesia dalam ARF *on cybersecurity initiatives* menggambarkan bahwa bangsa Indonesia memandang ancaman *cyber* sebagai suatu situasi yang dapat mengancam kondisi keamanan nasional dan diperlukan suatu perhatian mendasar dalam mencegah ancaman tersebut.

Berdasarkan pandangan bahwa ancaman *cyber* merupakan ancaman yang dapat mengganggu pertahanan dan keamanan suatu negara serta dapat menimbulkan dampak ekonomi, politik, dan sosial, maka *cybersecurity* merupakan kepentingan nasional yang bersifat mutlak. Hal ini sesuai dengan pandangan kepentingan nasional berdasarkan Buku Putih Pertahanan Indonesia yang menyatakan bahwa kepentingan nasional yang bersifat mutlak adalah mengoptimalkan fungsi pertahanan negara untuk menjaga dan melindungi kedaulatan dan keutuhan Negara Kesatuan Republik Indonesia (NKRI) serta keselamatan bangsa dari segala ancaman. Di samping itu, perlu dipahami bersama bahwa *cyberspace* memiliki sifat yang sangat luas karena penggunaannya yang menyentuh berbagai aspek kehidupan bangsa seperti pendidikan, percepatan transaksi ekonomi, penyebaran informasi dan promosi, maupun teknologi militer. Oleh sebab itu, jika kepentingan nasional yang bersifat vital menyangkut keberlanjutan pembangunan nasional, dan kepentingan nasional yang bersifat penting atau utama adalah menyangkut perdamaian dunia dan stabilitas regional, maka peran *cyberspace* dapat menyentuh ke semua aspek kepentingan tersebut.

Cybersecurity akan selalu dihadapkan dengan ancaman yang bersifat lintas batas, tidak terduga, dan sulit dideteksi. Oleh sebab itu, perlindungan negara terhadap ancaman *cyber* tidak hanya dibangun dari dalam melainkan juga dari luar. Pada kondisi ini, pemerintah perlu membangun diplomasinya dalam mencari informasi dan membangun hubungan dengan negara lain sehingga mampu mencegah ancaman sebelum masuk ke Indonesia.[21] Pada lingkup regional, tindakan ini tercermin dalam peran Indonesia di ASEAN dan keikutsertaannya dalam ARF *on cybersecurity initiatives*. Melalui forum ini, pemerintah Indonesia mengupayakan adanya rasa saling percaya diantara negara-negara anggota ARF dengan menjaga wilayahnya masing-masing dari ancaman *cyber* dan mengajak agar antar negara tidak menyerang satu sama lain.[22] Forum ini juga digunakan oleh pemerintah Indonesia dalam menerapkan diplomasi internasionalnya untuk meng-*update* informasi mengenai ancaman-ancaman *cyber* yang baru akibat perkembangan teknologi informasi, seperti adanya virus atau *malware* baru.[23] Selain itu, pemerintah Indonesia juga mengupayakan kolaborasi antar negara dan *sharing informasi* mengenai pelaku kejahatan *cyber.*[24]

Upaya untuk membangun *cybersecurity* bukanlah sesuatu yang bisa diperjuangkan secara sendirian oleh suatu negara. Hal ini mengingat bahwa salah satu aspek yang paling menonjol dalam *cyber conflict* adalah ketidakpastian. Oleh sebab itu, pemerintah Indonesia melalui ARF mengusulkan adanya kontak poin masing-masing negara untuk memudahkan komunikasi ketika terjadi suatu serangan *cyber.* Ide ini disetujui dan dituangkan dalam dokumen ASEAN *Regional Forum Workplan on Security of and in The Use of Information and Communications Technologies* (ICT's). Kondisi tersebut menunjukkan bahwa peran dan kepemimpinan Indonesia melalui ARF diakui oleh negara partisipan dan menunjukkan keberhasilan diplomasi Indonesia. Hal ini berbanding lurus dengan kebijakan luar negeri pemerintah Indonesia yang menempatkan ASEAN sebagai pilar utama politik luar negeri Indonesia.

Usaha-usaha tersebut memberi gambaran bahwa kepentingan nasional Indonesia dalam ARF *on cybersecurity initiatives* adalah

[20] Robert Jackson dan Georg Sorensen, "Introduction to International Relations", (United Kingdom, Oxford University Press, 2013), hlm. 6.

[21] Munawar Ahmad (Ketua Staf Ahli DK2ICN), wawancara pribadi, 29 Februari 2016.

[22] Direktorat Politik dan Keamanan ASEAN Kementerian Luar Negeri, wawancara pribadi, 21 Januari 2016.

[23] Munawar Ahmad (Ketua Staf Ahli DK2ICN), wawancara pribadi, 29 Februari 2016.

[24] Prakoso (Asisten Deputi 2/VII Kedeputian Komunikasi, Informasi dan Aparatur, Kemenkopolhukam), wawancara pribadi, 7 Januari 2016.

membentuk dan meningkatkan rasa saling percaya diantara negara-negara ARF untuk melindungi keamanan nasionalnya dan membentuk stabilitas kawasan. Rasa saling percaya tersebut kemudian diimplementasikan dalam *study/working group* mengenai *cybersecurity*, *sharing* informasi mengenai ancaman *cyber*, diperolehnya kontak poin dalam penanganan insiden *cyber*, dan meningkatkan kapabilitas pertahanan dengan membentuk tata kelola pemerintahan yang baik dalam bidang *cybersecurity* pada lingkup ASEAN.

Politik Luar Negeri dan Kebijakan Pemerintah Indonesia dalam bidang *Cybersecurity*

Sesuai dengan amanat konstitusi, politik luar negeri dan diplomasi Indonesia diabdikan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan untuk ikut serta melaksanakan ketertiban dunia. Dalam melaksanakan amanat konstitusi tersebut, Indonesia menganut politik luar negeri yang bebas aktif. Pelaksanaan politik luar negeri RI memiliki dua aspek utama, yaitu untuk mendukung pencapaian kepentingan nasional dan sebagai upaya untuk ikut berkontribusi terhadap kemaslahatan dunia internasional.[25] Untuk mengimplementasikan hal tersebut, pemerintah perlu melihat kondisi dinamis di dalam dan di luar negeri.

Tidak dapat dipungkiri bahwa pada masa sekarang, isu-isu keamanan non-tradisional memiliki peran yang sama pentingnya dengan isu keamanan tradisional. Tantangan ini perlu dihadapi dan disikapi oleh Indonesia. Isu kejahatan seperti pencucian uang, kejahatan *cyber*, maupun penyelundupan narkoba merupakan salah satu persoalan yang dapat mengancam stabilitas kawasan, khususnya mengancam pembangunan nasional Indonesia.[26] Permasalahan ini akan mempengaruhi kondisi nasional bangsa secara dua arah, baik dari internal ke eksternal, maupun sebaliknya. Oleh sebab itu, perlu dibangun kerjasama global dan regional baik bilateral maupun multilateral untuk menangani ancaman tersebut demi tercapainya kerangka instrumen internasional yang komprehensif.

Kementerian Luar Negeri menempatkan ASEAN sebagai pilar utama politik luar negeri Indonesia dengan terus berpartisipasi aktif dalam kerjasama ASEAN di bidang politik-keamanan, ekonomi, sosial budaya, dan pembangunan. Peran Indonesia juga diarahkan untuk menjadi bagian dalam penyelesaian masalah global dan membangun hubungan baik dengan dunia internasional melalui berbagai organisasi regional dan internasional.[27] Pada lingkup *cybersecurity*, pemerintah Indonesia juga ikut terlibat dalam pertemuan ARF *on cybersecurity initiatives* untuk mebentuk rasa saling percaya antara negara-negara di kawasan dalam menjaga keamanan *cyber* yang dapat mengganggu kepentingan nasional.

Politik bebas aktif dalam pencapaian kepentingan nasional di bidang *cybersecurity* diterapkan pemerintah Indonesia dengan tidak berpatokan pada negara tertentu untuk membangun kebijakan atau sistem pertahanan *cyber*-nya. Hal ini karena ancaman yang ada di masing-masing negara belum tentu sama dengan ancaman yang dihadapi oleh kondisi yang ada di Indonesia.[28] Pemerintah memanfaatkan ARF *on cybersecurity initiatives* untuk saling berbagi informasi mengenai perkembangan yang ada di dunia *cyber* serta mempelajari sistem yang ada di negara lain sehingga dapat diserap hal-hal yang sesuai dengan kebutuhan negara.[29] Selain itu, pemerintah Indonesia juga mengupayakan agar forum tersebut tetap berdasar pada prinsip dasar ASEAN yaitu musyawarah mufakat. Hal ini dilakukan agar keputusan yang diambil berdasar pada tercapainya tujuan bersama dan tidak adanya kepentingan nasional negara tertentu yang memiliki pengaruh terlalu besar dalam keputusan yang diambil. Sebagai contoh, China sebagai salah satu anggota ARF begitu agresif untuk menawarkan sistem *cyber*-nya untuk diterapkan

[25] Kementerian Luar Negeri, "Rencana Strategis Kementerian Luar Negeri Tahun 2015-2019", (Jakarta: Kementerian Luar Negeri, 2015), hlm. 60.

[26] *Ibid*., hlm. 44.

[27] *Ibid*., hlm. 1.

[28] Yono Reksoprodjo (Staf ahli Panglima TNI bidang C4ISR), wawancara pribadi, 2 Februari 2016

[29] Arwin D.W. Sumari (Staf Ahli DK2ICN), wawancara pribadi, 12 Januari 2016.

di ASEAN dan bersikap menolak terhadap model yang ditawarkan Amerika. Pada kondisi ini, pemerintah Indonesia bersama dengan negara-negara ASEAN berusaha menghentikan atau memperlambat tindakan tersebut.[30]

Pada bidang pertahanan, pemerintah Indonesia melalui Kementerian Pertahanan juga memiliki beberapa pokok sikap yang menjadi landasan dalam membangun kerjasama internasionalnya, yang meliputi:[31] 1) Saling menghormati kedaulatan negara lain, 2) Tidak mencampuri urusan dalam negeri, 3) Saling menguntungkan, 4) Instrumen cegah konflik antar negara, 5) Membangun kapasitas pertahanan.

Lebih lanjut, Pada Tabel 1 dapat dilihat instrumen kebijakan *cyber* yang dimiliki berbagai instansi serta keterbatasan kewenangan yang ada sebagai berikut.

Pada tabel tersebut dapat dilihat beberapa kekurangan yang ada dalam kebijakan yang telah dimiliki pemerintah Indonesia. Sebagai contoh adalah terpisahnya fungsi keamanan yang dimiliki Polri (UU No.2 tahun 2002) dan fungsi pertahanan yang dimiliki TNI (UU No.3 tahun 2002). Hal inilah yang dapat menghambat tindakan pencegahan ancaman. Berdasarkan pengalaman, kondisi ini menjadikan bangsa Indonesia selalu terlambat bertindak dan cenderung baru bekerja ketika ada suatu kejadian yang telah menimbulkan korban, baik secara materi maupun non materi.[32] Tanpa adanya perbaikan dalam kebijakan tersebut, pemerintah Indonesia akan kesulitan dalam membentuk ketahanan *cyber*. Sebagaimana disampaikan oleh Edmond Makarim[33] yang menyatakan bahwa ketahanan bukan hanya kemampuan kita untuk

Tabel 1. Instrumen Kebijakan Pertahanan *Cyber*

Institusi	Dasar Hukum	Keterbatasan Kewenangan
Kemhan/TNI	-UU 3/2002 Pertahanan -UU 34/2004 TNI -UU 1999 Mobilisasi dan Demobilisasi -UU 43/2008 Wilayah Negara -PP 68/2014 Penataan Wilayah Negara	-Tugas pertahanan negara: tegaknya kedaulatan, keutuhan wilayah dan perlindungan bangsa. -*Cyberspace* belum menjadi wilayah pertahanan. -Dalam tugas nir militer TNI sebagai pendukung
Polisi	UU 2/2002 Kepolisian	Terbatas pada tugas Kamtibmas. *Attribution is not evidence but rather intelligence.* Utamakan asumsi
Intelijen	UU 17/2011 Intelijen	Kemampuan untuk melakukan *cyber espionage* maupun untuk merespon *cyber attack* terbatas.
Kominfo	-UU 36/199 Telekomunikasi -UU 32/2002 Penyiaran -UU 11/2008 ITE -UU 14/2008 KIP	Terbatas dalam konteks infrasruktur telekomunikasi, penyiaran dan informatika untuk pelayanan publik
Internasional	Talinn Manual	Draft NATO atas Konvensi Internasional untuk perang *Cyber*

Sumber: Materi Presentasi Direktorat Kebijakan Strategis Kementerian Pertahanan, 5 Februari 2015

[30] Direktorat Politik dan Keamanan ASEAN Kementerian Luar Negeri, wawancara pribadi, 21 Januari 2016.

[31] Direktorat Kebijakan Strategis Kementerian Pertahanan, materi presentasi, disampaikan dalam wawancara pribadi, 5 Februari 2016.

[32] Arwin D.W. Sumari (Staf Ahli DK2ICN), wawancara pribadi, 12 Januari 2016.

[33] Ketua Staf Ahli Bidang Hukum DK2ICN, wawancara pribadi, 29 Februari 2016.

bertahan dalam menghadapi serangan, melainkan juga seberapa cepat kita bangkit dari kondisi luluh lantah, dan melakukan serangan balasan/ tindakan represif yang masuk dalam tindakan *security.* Atas dasar hal tersebut maka pertahanan dan keamanan harus berada dalam satu bingkai utuh.

Kominfo dengan UU ITE tahun 2008 juga dianggap belum mampu mencakup seluruh aspek *cybersecurity* yang begitu luas. Jika ancaman *cyber* merupakan suatu ancaman yang dapat berdampak pada kondisi pertahanan dan keamanan negara, maka perlu pembahasan yang melingkupi keamanan nasional dan bukan hanya terbatas kepada penyelenggaraan informasi dan komunikasi tanpa adanya pertanggungjawaban untuk mengamankannya. Lebih lanjut, pada lingkup internasional, belum ada satu kebijakan yang mengikat mengenai *cybersecurity*. Menimbang bahwa ancaman *cyber* bersifat transnasional, maka tidak adanya kebijakan tersebut dapat dianggap sebagai suatu celah keamanan dalam bidang *cybersecurity*. Salah satu konvensi yang mengarah kesana adalah *Tallin Manual*. Namun, konvensi tersebut sejauh ini masih terbatas kepada negara NATO saja, walaupun terdapat kemungkinan diterapkan melalui PBB.

Selain ARF *on cybersecurity initiatives,* Indonesia pada dasarnya telah memiliki organisasi Indonesia *Computer Emergency Response Team* (ID-CERT) yang memiliki misi untuk melakukan koordinasi penanganan insiden cyber yang melibatkan pihak Indonesia dan luar negeri. ID-CERT juga secara aktif ikut serta dalam forum *Asia Pacific Computer Emergency Response Team* (APCERT). Namun, ID-CERT merupakan tim koordinasi teknis berbasis komunitas dan untuk komunitas yang bersifat independen. Sebagai organisasi non-pemerintah dan independen, ID-CERT tidak berada di bawah naungan insansi pemerintah dan tidak memiliki kewenangan untuk menentukan kebijakan yang mencakup kepentingan nasional suatu negara. Lebih lanjut, ID-CERT juga tidak memiliki kewenangan untuk menyelidiki kasus secara tuntas.[34] Hal inilah yang menyebabkan lemahnya legitimasi organisasi seperti ID-CERT atau APCERT dalam kewenangan kebijakan *cyber*.

Cyberspace merupakan aspek yang unik karena penggunaanya dapat menyentuh semua aspek kehidupan nasional, seperti pertahanan, keamanan, keuangan, dan kehidupan sosial. Namun, berdasarkan kondisi yang ada, Indonesia belum memiliki kebijakan yang secara komprehensif mengatur mengenai *cyberspace.* Lemahnya kewenangan pada internal pemerintahan dalam penanganan konflik *cyber* tentunya dapat menjadi ancaman bagi pertahanan dan keamanan negara. Pada kondisi inilah, aspek-aspek diplomasi pertahanan diperlukan sebagai salah satu instrumen pencegahan konflik yang dapat muncul dari lingkup eksternal.

Implementasi Diplomasi Pertahanan Indonesia dalam ARF on *Cybersecurity Initiatives*

Hubungan internasional mengenal istilah bawah salah satu penyebab terjadinya perang adalah karena kegagalan diplomasi. Oleh sebab itu, fungsi diplomasi maupun diplomasi pertahanan seringkali diarahakan sebagai instrumen pencegahan dan penyelesaian konflik, maupun pemeliharaan stabilitas kawasan. Jika melihat pada kondisi saat ini dimana lingkungan strategis semakin tidak pasti dan tidak dapat diprediksi, maka pemerintah Indonesia perlu menerapkan strategi yang mampu beradaptasi dan meningkatkan peran diplomasinya untuk mencegah konflik yang dapat mengganggu stabilitas kawasan dan kepentingan nasional.[35] Berdasarkan pada hal tersebut, Pemerintah Indonesia melalui Kementerian Luar Negeri telah menetapkan arah kebijakan luar negerinya untuk semakin meningkatkan perannya di ASEAN dengan salah satu strateginya, yaitu memperjuangkan prakarsa Indonesia di ASEAN dan forum terkait ASEAN dalam mewujudkan kawasan yang aman, stabil, dan sejahtera.[36] Pada salah satu forum, yaitu ARF, pemerintah

[34] Idcert, "Profil Indonesia Computer Emergency Response Team", http://www.cert.or.id/tentang-kami/id/, diakses pada tanggal 14 Agustus 2016.

[35] Direktorat Kerjasama Internasional Kementerian Pertahanan, dokumen wawancara, 12 Februari 2016.

[36] Direktorat Politik dan Keamanan ASEAN, Kementerian Luar Negeri, wawancara pribadi, 21 Januari 2016.

Indonesia terus berupaya meningkatkan peran diplomasinya dalam menghadapi ancaman *cyber* melalui ARF *on cybersecurity initiatives*.

Keanggotaan ARF terdiri dari 27 negara yang meliputi negara-negara ASEAN, dan negara maju lainnya seperti Rusia, Amerika Serikat, China, Jepang, maupun Korea Selatan. Berhadapan dengan negara-negara tersebut hingga terlibat konflik dalam bidang *cyber* tentu bukan pilihan yang tepat bagi Indonesia. Hal ini mengingat baik dari segi teknologi maupun sumber daya yang lain, penguasaan negara-negara tersebut mengenai *cybersecurity* jauh lebih baik dibandingkan dengan Indonesia. Oleh sebab itu, melalui ARF pemerintah perlu secara intens untuk terus meningkatkan hubungan baik dan rasa saling percaya dalam bidang *cyber*. Sebaliknya, dengan pengalaman dan pengetahuan yang dimiliki oleh negara-negara seperti Amerika, China, Korea Selatan yang sudah jauh lebih *settle* dalam *cybersecurity*-nya pemerintah perlu untuk terus secara aktif memanfaatkan kerjasamanya dalam hal pelatihan dan pembangunan infrastruktur *cyber*. Diplomasi pertahanan Indonesia perlu terus didorong untuk *capacity building* sehingga percepatan pembangunan kebijakan dan sistem keamanan *cyber* di Indonesia dapat berjalan secara maksimal.

Melalui mekanisme ARF yang memungkinkan terjadinya kerjasama dalam kerangka diplomasi *track* II, pengiriman delegasi baik pada level kementerian hingga akademisi dapat dimungkinkan dengan mengikuti berbagai pelatihan, seminar, maupun *workshop* yang diadakan. Dengan demikian, pembelajaran dan peningkatan SDM Indonesia akan pengetahuan *cybersecurity* yang komprehensif bisa diperoleh. Lebih lanjut, dengan rasa saling percaya yang didorong terus menerus melalui ARF diharapkan akan memberi pemahaman yang sama mengenai *cybersecurity*, sehingga kebijakan regional bisa segera dibentuk untuk menjaga kondisi dan stabilitas keamanan di kawasan. Satu hal yang perlu diperhatikan oleh pemerintah Indonesia, bahwa belum adanya kebijakan regional perlu dipandang sebagai suatu peluang. Kondisi tersebut memungkinkan pemerintah Indonesia untuk terus mempromosikan kepentingan nasionalnya akan kebutuhan keamanan *cyber* sesuai dengan keinginan pemerintah. Sehingga, ketika suatu kebijakan terbentuk, akan terdapat nilai-nilai kepentingan nasional Indonesia di dalamnya.

Salah satu pencapaian implementasi diplomasi pertahanan pemerintah Indonesia dalam ARF *on cybersecurity initiatives* adalah diperolehnya *point of contacts* (kontak poin) perwakilan negara-negara ASEAN dan beberapa negara di kawasan regional yang menangani masalah *cybersecurity.*[37] Beberapa negara tersebut diantaranya adalah semua negara ASEAN, China, Belanda, Rusia, AS, dan Australia.[38] Kontak poin ini merupakan ide murni dari pemerintah Indonesia yang diusulkan dalam ARF.[39] Ide tersebut kemudian dituangkan dalam dokumen ASEAN *Regional Forum Workplan on Security of and in the Use of Information and Communications Technologies* (ICT's). Hal tersebut tertuang dalam *proposed activitites* No.1, untuk membentuk sebuah *study gorup* yang menyatakan bahwa:[40]

> *"The Study Group should develop processes and procedures for sharing information between **ARF contact points** on preventing ICT crises, and criminal and terrorist use of ICTs; establishment of a contacts database (without duplicating existing CERT networks)."*

Melalui kontak poin yang didapatkan dari masing-masing negara, pemerintah Indonesia dapat lebih mudah melakukan proses diplomasinya dalam ranah *cyber*. Hal tersebut dapat berupa diplomasi dalam hal penanganan insiden *cyber,* maupun hal lain yang terkait pencapaian tujuan bersama. Lebih lanjut, kontak poin yang didapatkan bukan sebatas nama instansi atau nomor telpon instansi, namun juga nomor pribadi maupun email pribadi pejabat berwenang. Hal ini dapat dipandang sebagai pintu masuk bagi pemerintah Indonesia untuk

[37] Prakoso (Asisten Deputi 2/VII Kedeputian Komunikasi, Informasi dan Aparatur, Kemenkopolhukam), wawancara pribadi, 7 Januari 2016.

[38] Munawar Ahmad (Ketua Staf Ahli DK2ICN), wawancara pribadi, 29 Februari 2016.

[39] Direktorat Politik dan Keamanan ASEAN, Kementerian Luar Negeri, wawancara pribadi, 21 Januari 2016

[40] ASEAN Regional Forum, *Op. Cit,* hlm.3.

mendapatkan hasil yang lebih besar karena proses komunikasi dan diplomasi dapat berjalan lebih mudah.[41]

Kontak poin yang ada juga digunakan untuk melakukan identifikasi pelaku kejahatan *cyber*. Hal ini akan memberi masukan bagi pemerintah Indonesia untuk mengambil suatu tindakan. Sebagai contoh, jika ada serangan *cyber* yang teridentifikasi dari Malaysia, maka pemerintah harus tahu apakah itu serangan yang dilakukan oleh kelompok/organisasi tertentu atau *state actor*. Pemerintah bisa melakukan klarifikasi dengan kontak poin negara bersangkutan sehingga bisa memtusukan bagaimana melakukan tindakan atau serangan balasan. Jika serangan tersebut teridentifikasi dilakukan oleh negara, maka kita dapat membalasnya dengan kapasitas sebagai negara. Namun, jika serangan tersebut dilakukan oleh kelompok/organisasi maka akan sangat berlebihan dan terlalu membuang *resource* yang ada apabila kita meresponnya dengan kapasitas sebagai negara. Hal seperti ini pernah terjadi ketika pemerintah Indonesia akan mengeksekusi mati dua warga negara Australia. Pada saat itu, Indonesia hampir perang *cyber*, namun karena memiliki kontak poin dari Australia maka pemerintah berkoordinasi. Bagian dari koordinasi itu, masing-masing pihak saling menjaga sisi *cyber* di wilayahnya untuk menahan diri dan tidak saling menyerang.[42]

Selain itu, dengan diperolehnya kontak poin, pemerintah bisa jauh lebih mudah menangani insiden *cyber* yang terjadi. Hal tersebut karena negara tidak perlu bekerja secara sendirian, namun satu sama lain bisa bekerjasama dan berkoordinasi untuk menangani suatu kasus dan berbagi informasi mengenai ancaman *cyber* yang akan terjadi. Contoh kasus konflik Indonesia dengan Australia bisa dijadikan pelajaran bahwa dengan adanya koordinasi yang baik, setidaknya dalam dunia *cyber,* kedua negara masih memiliki rasa saling percaya satu sama lain dan bersama-sama menjaga wilayahnya untuk tidak melakukan serangan. Dengan demikian, sejauh kerjasama yang dilakukan tidak menganggu kepentingan nasional, diplomasi pertahanan yang dijalankan untuk membentuk rasa saling percaya akan selalu berkontribusi positif bagi kondisi keamanan Indonesia.

Implementasi diplomasi pertahanan Indonesia di ARF tidak terlepas dari kendala dan tantangan, baik yang bersumber dari lingkup internal maupun eksternal. Sebagai gambaran, pada salah satu *study group* di ARF Indonesia mengusahakan bagaimana menyikapi serangan *cyber* dan bagaimana mengatasinya melalui suatu simulasi kering. Salah satu tujuan diadakannya *study grup* ini adalah agar pemerintah Indonesia bersama dengan negara ASEAN dapat membentuk suatu kurikulum untuk meningkatkan *capacity building*. Selain itu, pemerintah juga mengusulkan perubahan penggunaan *Internet Protocol version 4* (IPv4) ke IPv6 untuk seluruh negara ASEAN sebagai salah satu solusi konkrit peningkatkan sistem keamanan internet. Namun dari dua usul tersebut respon yang diterima cukup kecil. Hal ini terjadi karena seringkali delegasi yang dikirim adalah seseorang yang tidak menguasi bidang *cyber.*[43]

ARF memang berada pada ranah Kementerian Luar Negeri karena menguasai *foreign policy*, namun idealnya pihak-pihak Kementerian Luar Negeri juga mampu mengedepankan orang-orang yang *expert* dalam bidang tertentu sesuai dengan topik yang dibahas. Selain itu, delegasi yang dikirim juga seringkali tidak mengetahui rekan mereka dari instansi lain karena undangan pertemuan tidak dikirim melalui satu pintu.[44] Kejadian tersebut memberikan gambaran mengenai lemahnya koordinasi nasional yang dapat berakibat pada terganggunya pencapaian kepentingan nasional di tingkat internasional karena masing-masing instansi merasa mewakili pemerintahan.[45] Selain itu, persyaratan keamanan yang belum dipenuhi oleh negara lain juga menjadi salah satu kendala yang harus dihadapi. Sebagai contoh, dalam hal *Domain Name Server* (DNS) *security*, Indonesia berada pada *grade* A di dunia. Selain itu, kemampuan Sumber Daya

[41] Arwin D.W. Sumari (Staf Ahli DK2ICN), wawancara pribadi, 12 Januari 2016.

[42] Kun Arief Cahyantoro (Kabid Ketahanan Informasi DK2ICN), wawancara pribadi, 7 Januari 2016.

[43] Direktorat Politik dan Keamanan Sekretariat ASEAN, wawancara pribadi, 15 Januari 2016.

[44] *Ibid,*.

[45] Arwin D.W. Sumari (Staf Ahli DK2ICN), wawancara pribadi, 12 Januari 2016.

Manusia (SDM) untuk membuat IPv6 *Map* yang sejauh ini belum semua negara ASEAN memiliki standar keamanan ini dan hanya Pemerintah Indonesia melalui Kemenkopolhukam dan Pemerintah Korea Selatan yang mampu memenuhi semua kriteria yang ada.[46] Kondisi seperti inilah yang menjadi salah satu kendala dalam proses diplomasi di ARF.

Kementerian Luar Negeri sebagai ujung tombak kebijakan luar negeri Indonesia telah memiliki dasar kebijakan untuk meningkatkan perannya di ASEAN dan ikut serta dalam proses pencapaian kepentingan nasional di berbagai forum regional, namun tanpa adanya dukungan dari kondisi kebijakan nasional yang mengatur *cyberspace* secara komprehensif, akan menyebabkan melemahnya usaha-usaha yang dilakukan. Oleh sebab itu, diperlukan adanya konsistensi dalam pemerintahan, satu interpretasi, dan satu pemahaman mengenai kebijakan, mulai dari struktur pemerintahan paling atas hingga paling bawah agar pemanfaatan forum yang ada dapat berjalan maksimal untuk mempercepat proses pencapaian kepentingan nasional. Berdasarkan pada kondisi tersebut, disamping Indonesia juga sedang dalam proses menyiapkan badan yang akan bertanggung jawab dalam keamanan *cyber*, pemerintah juga mengusulkan agar masing-masing negara segara membentuk badan atau lembaga yang bertanggung jawab mengenai *cybersecurity.*[47] Hal tersebut dilakukan karena masih terdapat beberapa negara yang belum memiliki badan khusus di bidang *cybersecurity*. Sehingga, terdapat beberapa kontak poin dari negara lain yang bersifat informal. Melalui badan resmi dan bersifat khusus, proses diplomasi akan jauh lebih mudah dalam pencapaian kepentingan nasional di bidang *cybersecurity*. Lebih lanjut, Pemerintah Indonesia dapat melakukan klarifikasi, memetakan jaringan serangan, dan mengambil tindakan yang efektif bersama negara-negara lain sehingga tidak ada *miss* dari sisi *cyber* diplomasi.

Pada lingkup eksternal, negara-negara di dunia internasional memiliki cara pandang yang berbeda-beda mengenai *cybersecurity*. Hal yang sama terjadi dengan ASEAN dan negara peserta ARF. Sebagai contoh, Malaysia dan Singapura adalah negara yang sangat berfokus mengenai pembatasan konten dalam ruang lingkup *cyber.* Jika Malaysia menerapkan sensor pada hal-hal yang berkaitan dengan penistaan agama, maka Singapura menerapkan sensor pada hal-hal yang menjurus ke makar dan bersuara jelek kepada pemerintah. Di sisi lain, negara-negara dengan sistem demokrasi yang menganut paham *free speech* seperti halnya Amerika Serikat, tentu tidak akan berfokus terhadap hal tersebut. Dalam lingkup *cyber*, Amerika dan Australia adalah contoh negara yang lebih berfokus pada pembangunan infrastruktur. China pun memiliki pandangan yang berbeda dan cenderung mengisolasi lingkungan *cyber*-nya dengan mendukung penggunaan situs dalam negeri. Disamping itu, terdapat beberapa negara yang belum menjadikan isu *cyber* sebagai perhatian utamanya. Seperti halnya Brunei, Myanmar, maupun Vietnam yang belum memprioritakan isu *cybersecurity*. Hal ini dipandang wajar karena berbagai alasan seperti kondisi dalam negeri yang tidak stabil, dan lebih memprioritaskan pembangunan ekonomi, serta berbagai hal lainnya.

Penggambaran pada kondisi eksternal tersebut menunjukkan bahwa Indonesia maupun negara ARF lainnya seringkali mengalami kendala dalam mencari persamaan nilai. Mekanisme pengambilan keputusan ARF berdasarkan pada ASEAN *Charter* adalah keputusan yang berdasarkan pada mufakat. Jika ada satu ketidaksetujuan dalam suatu perundingan, maka tidak akan ada kebijakan yang bisa tercapai. Oleh sebab itu, dengan perbedaan pandangan yang ada dan dihadapkan pada mekanisme yang diadopsi oleh ARF, pengambilan keputusan dalam ARF bukanlah suatu hal yang mudah. Hal inilah yang kemudian berdampak pada implementasi diplomasi pertahanan Indonesia di ARF *on cybersecurity initiatives*. Jika Indonesia menginginkan salah satu kepentingan nasionalnya tercapai melalui ARF, maka setidaknya Indonesia perlu meyakinkan negara-negara ASEAN

[46] Kun Arief Cahyantoro (Kabid Ketahanan Informasi DK2ICN), wawancara pribadi, 7 Januari 2016.

[47] Direktorat Politik dan Kemanan ASEAN, Kementerian Luar Negeri, wawancara, 21 Januari 2016

sebelum berdiplomasi dengan 17 negara anggota ARF lainnya.

Kontribusi Diplomasi Pertahanan Indonesia dalam ARF *on Cybersecurity Initatives*

Kontribusi diplomasi pertahanan Indonesia di ARF akan sangat dipengaruhi dengan lingkungan dan metode yang digunakan oleh ARF serta penyesuaian strategi diplomasi pertahanan Indonesia yang diterapkan dalam ARF. Diplomasi pertahanan Indonesia digunakan sebagai instrumen untuk pengejaran kepentingan nasional dalam hubungan diplomasi multilateral di ARF dan diplomasi pertahanan yang dikembangkan untuk membangun hubungan baik dengan negara lain untuk mengurangi ketidakpastian dalam kaitannya dengan *cybersecurity* di kawasan regional. Di sisi lain, dengan pemahaman jika kondisi keamanan suatu negara akan sangat dipengaruhi oleh kondisi keamanan eksternal dan stabilitas kawasan, maka diplomasi pertahanan Indonesia yang bertujuan untuk mengamankan wilayahnya juga akan berkontribusi kepada keamanan negara lain. Lebih lanjut, keberhasilan strategi diplomasi pertahanan suatu negara merupakan kolaborasi dari komponen diplomasi, pertahanan dan pembangunan yang memiliki tiga karakter utama, yaitu:[48]

1. *Defense Diplomacy for Confidence Building Measure*
2. *Defense Diplomacy for Defense Capabilities*
3. *Defense Diplomacy for Defense Industries*

Berdasarkan kondisi tersebut, bagaimana kontribusi diplomasi pertahanan Indonesia di ARF akan ditinjau melalui masing-masing karakter yang ada.

1. Defence Diplomacy for Confidence Building Measures (CBM)

Diplomasi pertahanan untuk CBM dilakukan untuk menurunkan ketegangan maupun menghilangkan perspektif negatif agar hubungan antar negara berjalan dengan baik. Selain itu, CBM diperlukan untuk menunjukkan transparansi kebijakan pertahanan agar satu negara tidak dianggap sebagai ancaman oleh negara lain.[49] Dalam hal ini, praktik diplomasi pertahanan untuk CBM dilakukan dalam bentuk kunjungan kenegaraan, pertukaran informasi, dialog dan konsultasi, deklarasi kerjasama strategis maupun kerjasama militer.[50] Pemerintah Indonesia menerapkan hal ini dengan mengajukan usulan mengenai *point of contacts* dalam bidang *cybersecurity*. *Sharing point of contacts* ini diharapkan akan mendukung CBM antar negara sehingga membentuk rasa aman dan saling percaya pada lingkup *cybersecurity*. Usulan ini diterima dan dituangkan dalam dokumen ASEAN *Regional Forum Workplan on Security of and in The Use of Information and Communications Technologies* (ICT's). Selain pada *proposed activities* No.1, ide mengenai diperlukannya kontak poin ini juga ditegaskan kembali pada *proposed* activities No.2, poin X mengenai pembentukan *workshops and seminars*, yang menyatakan bahwa: [51]

> *"consideration of establishment of senior policy* ***Point of Contacts*** *between ARF Participating Countries to facilitate real time communication about events and incidents in relation to security of and in the use of ICTs of potential regional security significance"*

Kontak Poin ini berguna bagi Indonesia dan negara-negara ARF lainnya dalam memetakan insiden *cyber*, mengetahui potensi ancaman, mengidentifikasi pelaku, dan memutuskan tindakan penanganan secara bersama-sama. Perlu dipahami bahwa tidak semua negara

[48] Idil Syawfi, "Aktifitas Diplomasi Pertahanan Indonesia dalam Pemenuhan Tujuan-Tujuan Pertahanan Indonesia (2003-2008)", Tesis Universitas Indonesia, 2009.

[49] Amitav Acharya, (2001), "Constructing a Security Community in South East Asia:ASEAN and the Problem of Regional Power", New York: Routledge, 2001, hal. 66

[50] Arifin Multazam, (2010), "Diplomasi Pertahanan Indonesia Terhadap KoreaSelatan Periode 2006-2009", Tesis Universitas Indonesia, hal. 19.

[51] ASEAN Regional Forum, *Loc. Cit.*

anggota ARF telah memiliki badan khusus yang menangani masalah *cyber* dan konsekuensi atas hal tersebut maka terdapat beberapa pejabat negara yang memberikan kontak poin pribadi kepada Indonesia. Hal ini menunjukkan bahwa Indonesia dipercaya oleh negara lain dalam berkerjasama jika ada suatu insiden *cyber* dan didukung dengan pemahaman bahwa ancaman *cyber* merupakan suatu ancaman yang tidak bisa ditangani oleh satu negara secara sendirian. Kombinasi kontak poin antara formal dan informal ini juga sejalan dengan metode ARF yang memungkinkan penggunan diplomasi *track* II didalamnya. Selain itu, tindakan memberi kontak poin menyiratkan pandangan bahwa negara-negara anggota ARF tidak ingin adanya konflik dalam ruang *cyber* dan oleh sebab itu maka kontak poin diperlukan sebagai sarana berkomunikasi dan berdiplomasi. Hal ini tentunya akan mendukung stabilitas keamanan kawasan dari ancaman *cyber*.

Sharing point of contacts antar negara ini menunjukkan bahwa kontribusi diplomasi pertahanan Indonesia ini sejalan dan berhasil memenuhi sasaran kerangka kerja ARF *Work Plan on Security of and in The Use of Information and Communications Technologies (Ict's)* pada poin pertama, yaitu "*a view to reducing the risk of misperception, miscalculation and escalation of tension leading to conflict"* atau bertujuan untuk mengurangi resiko kesalahpahaman dan eskalasi ketegangan yang mengarah kepada konflik. Lebih lanjut, pemerintah Indonesia dapat menggunakan media komunikasi tersebut untuk mengembangkan kerjasama yang lebih luas dalam membentuk *cybersecurity,* baik pada lingkup nasional maupun internasional.

Salah satu hal yang perlu dipahami bersama mengenai pentingnya kontak poin dalam *cybersecurity* adalah mengenai identifikasi pelaku. Hal ini menimbang bahwa, pertama *cyberspace* akan selalu melibatkan jaringan internasional, namun sejauh ini belum ada kebijakan khusus di dunia internasional mengenai *cybersecurity*. Kondisi tersebut juga terjadi di Indonesia dan negara ASEAN. Jika, pemerintah Indonesia tidak segera membentuk kebijakan *cyber* pada lingkup nasional dan lingkup regional, maka bukan tidak mungkin bahwa pemerintah Indonesia akan mengadopsi kebijakan internasional. Kedua, salah satu konvensi besar yang sedang berjalan saat ini mengenai masalah *cyber* adalah Tallin Manual yang sejauh ini dirumuskan oleh negara-negara NATO. Bukan tidak mungkin jika Tallin Manual sudah *final*, baik PBB maupun Indonesia akan mengadopsi peraturan dalam Tallin Manual, seluruhnya atau sebagian. Ketiga, dalam Tallin Manual terdapat penjelasan mengenai kategori "*the use of force*" dalam *cyber operations* yang salah satunya menyatakan bahwa: [52]

> "*...the more cosequences impinge on critical national interest, the more they will contribute to the depiction of a cyber operation as a use of force....*"
> *"...a cyber operation, like any operation, like any operation resulting in damage, destrucition, injury, or death is highly likely to be considered a use of force...*"

Hal ini menjelaskan bahwa *cyber operations* dapat dikategorikan sebagai *the use of force* jika berdampak kritis kepada kepentingan nasional yang mengakibatkan kerusakan, kehancuran, cidera, maupun kematian. Selain itu, jika *cyber operations* yang dikategorikan sebagai *the use of force* tersebut terbukti melibatkan negara atau dilakukan oleh kelompok atau individu yang disponsori oleh negara, seperti pada penjelasan *self defence* poin 15 Tallin manual sebagai berikut:[53]

> "*…if a group of private individuals under the direction of state A undertakes cyber operations directed against state B, and the consequences of those acitions reaches the requisite scale and effects, State A will have commited an armed attack...*"

maka suatu negara dapat melakukan serangan balasan termasuk menggunakan kekuatan militer berdasarkan artikel 51 PBB yang menyatakan bahwa negara berhak melakukan pembelaan diri baik secara individu maupun kolektif jika terjadi *armed attacks*.

[52] Michael N. Shmitt (*Ed.*), "Tallin Manual on The International Law Applicable to Cyber Warfare", Cambridge University Press, New York, 2013, hlm. 48.

[53] *Ibid.,* hlm. 58.

Walaupun peraturan tersebut masih dalam pembahasan oleh NATO, tapi pemerintah Indonesia dan negara-negara ASEAN perlu mempersiapkan diri sebaik mungkin. Berdasarkan kondisi tersebut, disinilah pentingnya kontak poin. Jika terjadi suatu serangan terhadap Indonesia, maka pemerintah bisa melakukan klarifikasi terhadap negara bersangkutan yang teridentifikasi lokasinya. Selain itu, jika lokasi Indonesia digunakan sebagai *proxy* oleh pelaku sebenarnya dalam serangan *cyber*, maka negara lain yang menjadi korban bisa melakukan klarifikasi ke Indonesia. Hal tersebut sangat penting agar Indonesia tidak dituduh sebagai pelaku dan menjadi salah sasaran dalam pembalasan serangan, mengingat bahwa, berdasarkan Tallin Manual, serangan balasan yang dilakukan bisa melibatkan penggunaan militer.

Berdasarkan kontribusi diplomasi pertahanan Indonesia dan mekanisme ARF yang memiliki tujuan untuk berkontribusi terhadap upaya-upaya *conficedence building* dan *preventive diplomacy* menunjukkan bahwa aspek diplomasi pertahanan untuk membentuk CBM dimungkinkan diterapkan di ARF. Di sisi lain, upaya yang dilakukan pemerintah Indonesa di ARF untuk membentuk jaringan kontak poin antar negara merupakan salah satu implementasi rasa saling percaya antara negara dan salah satu tindakan pencegahan peningkatan eskalasi konflik. Dengan demikian, kontribusi diplomasi pertahanan Indonesia sejalan dengan mekanisme ARF dan karakter *defense diplomacy for confidence building measures*. Lebih lanjut, tantangan yang harus dihadapai adalah bagaimana negara-negara dengan jejaring kontak poin tersebut, bekerjasama dan berkoordinasi dalam penanganan insiden *cyber*.

2. Defense Diplomacy for Defense Capabilities

Aspek kedua dalam diplomasi pertahanan adalah sebagai sarana untuk membangun kemampuan pertahanan. Berbeda dengan membangun kemampuan pertahanan secara umum, seperti halnya komponen militer dan jumlah alutsista serta aktor-aktor yang terlibat dalam perang konvensional, *cybersecurity* memiliki aspek yang begitu luas dengan melibatkan berbagai aktor di dalamnya. Sebagaimana yang didefiniskan oleh *international telecommunication union* bahwa *cybersecurity* merupakan kumpulan alat, kebijakan, konsep keamanan, pedoman, pendekatan, manajemen resiko, tindakan, latihan, *best practice,* jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber,* organisasi, aset, dan pengguna termasuk perangkat komputasi yang terkoneksi, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan segala sesuatu yang ditransmisikan dan/atau informasi yang tersimpan di lingkungan *cyber.*[54] Dalam membangun c*ybersecurity* atau keamanan *cyber* suatu negara, salah satu hal yang menjadi sangat sulit adalah memastikan darimana serangan tersebut berasal.

Berbeda dengan serangan konvesional seperti peluncuran misil yang meninggalkan jejak dan dapat dilacak lokasinya, pihak-pihak yang menggunakan taktik *cyber* dapat dengan mudah menyembunyikan keberadaannya. Hal ini karena ketidakpastian merupakan aspek yang menonjol dalam *cyber conflict* – dalam kaitannya dengan identitas penyerang, ruang lingkup dari *collateral damage*, dan efek yang potensial pada target tujuan dari serangan *cyber.*[55] Kondisi inilah yang dapat dijadikan suatu landasan bahwa pembangunan kapabilitas *cybersecurity* nasional tidak hanya dalam bentuk materi, melainkan juga pertukaran informasi dan pembangunan SDM yang berasal dari dalam (lingkup nasional) dan dari luar yang dapat melibatkan kerjasama internasional. Sebagai contoh, negara-negara yang lebih dulu memiliki pengetahuan mengenai keamanan *cyber* dapat membagi pengetahuannya dengan negara lain dalam kerangka kerjasama global.[56] Dalam hal ini, organisasi regional dapat memainkan perannya untuk mewujudkan

[54] International Telecommunication Union, "ITU News", https://www.itu.int/net/itunews/issues/2010/09/20.aspx, diakses pada tanggal 16 Agustus 2016.

[55] Derek S. Reverson, "Cyberspace and National Security: Threats, Opportunities, and Power in Virtual World*",* (Washington D.C: Georgetown University Press, 2012), hlm. 11.

[56] Zenonas Tziarras, "The Security Culture of a Global and a Multileveled Cybersecurity", In E. G. Carayannis, D. F. Campbell, & M. P. Efthymiopoulos (Eds.), Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice, (New York: Springer, 2014), hlm. 25.

hal tersebut. Hal ini diimplementasikan oleh Indonesia bersama dengan negara-negara ARF dengan melakukan berbagai seminar, pelatihan, maupun *workshop* yang bertujuan untuk berbagi pengetahuan mengenai *cybersecurity*. Dalam suatu *study group*, pemerintah Indonesia bersama dengan delegasi Rusia juga membentuk suatu simulasi mengenai penaganan insiden *cyber.*[57] Selain itu, dalam bentuk konkrit sebagai suatu solusi untuk meningkatkan kapabilitas pertahanan dan keamanan jaringan internet di ASEAN, pemerintah Indonesia juga mengusulkan perubahan penggunaan IPv4 ke IPv6, mengingat bahwa IPv6 memiliki sistem keamanan yang lebih baik dan bisa diubah sesuai kebutuhan.

Hal ini menunjukkan bahwa diplomasi pertahanan Indonesia juga berperan dalam memberikan kesadaran akan keamanan dalam penggunaan *cyberspace*. Dengan demikian, tindakan tersebut sejalan dengan kerangka kerja ARF *Work Plan on Security of and in The Use of Information and Communications Technologies (Ict's)* yang dinyatakan dalam poin nomor dua, yaitu "*Raise awareness on threats related to the security of and in the use of ICTs*". Sayangnya usulan tersebut tidak mendapat tanggapan yang diharapkan. Hal tersebut tidak sepenuhnya kesalahan dari pemerintah Indonesia mengingat bahwa kurangnya pemahaman teknis delegasi yang datang dan tidak semua negara-negara anggota ARF memenuhi kriteria sistem keamanan tersebut.

Pemerintah Indonesia juga menggunakan ARF sebagai sarana untuk meng-*update* dan berbagi informasi mengenai *cybersecurity*. Sebagai contoh, pengetahuan mengenai *malware botnet*. Program dari *malware* tersebut dianggap sangat berbahaya karena dapat menggunakan komputer dari pihak lain dalam jumlah banyak untuk melakukan serangan tanpa disadari oleh penggunanya. Melalui forum, *workshop*, maupun seminar yang ada pemerintah dapat cepat mendapat informasi dan cepat melakukan antisipasi.[58] Sebagaimana yang disampaikan oleh Yono Reksoprodjo bahwa dalam dunia *cyber,* politik yang dimainkan haruslah proaktif.[59] Jika pemerintah tidak proaktif, maka akan berdampak pada ketertinggalan informasi dan dapat menjadi sasaran. Sebagai contoh adalah perseteruan antara AS dan China. Walaupun kedua negara tersebut seringkali terlibat perbedaan pandangan dalam berbagai hal, namun dalam dunia *cyber*, kedua negara saling berkomunikasi dan terbuka. Hal inilah yang jarang diketahui masyarakat umum. Tanpa adanya komunikasi tersebut, bukan tidak mungkin akan terjadi peperangan *cyber* antara kedua negara.

Diplomasi pertahanan sebagai bagian dari kapabilitas pertahanan juga dilakukan dengan tujuan untuk memperkuat kapabilitas pertahanan negara secara material. Namun, mekanisme ARF yang cenderung kepada dialog dan konsultasi serta pertukaran informasi menyebabkan sulitnya terjalin bentuk kerjasama untuk membangun kapasitas pertahanan dalam bidang *cyber* yang bersifat material, seperti alutsista maupun komponen pertahanan lain. Oleh sebab itu, kontribusi yang dilakukan oleh Indonesia maupun oleh negara lain cenderung kepada pembangunan yang bersifat informasi, pengetahuan, dan pembangunan sumber daya manusia. Di sisi lain, hasil dari ARF dapat digunakan sebagai salah satu *input* untuk membuat kebijakan nasional dalam bidang *cybersecurity*. Dengan demikian, kerjasama yang terjalin dalam ARF *on cybersecurity initiatives*, dalam kaitanya dengan membangun kapabilitias pertahanan yang bersifat material, bukan bertujuan untuk membentuk suatu kesepakatan seperti pembelian alat pertahanan melainkan sebagai pintu masuk untuk mencari pandangan bersama dan membuka bentuk kerjasama yang lebih besar.

3. Defense Diplomacy for Defense Industries

Satu aspek yang belum mampu dipenuhi oleh diplomasi pertahanan Indonesia melalui ARF adalah diplomasi pertahanan untuk industri pertahanan. Beberapa hal yang menjadi hambatan adalah belum adanya badan resmi pemerintah

[57] Prakoso (Asisten Deputi 2/VII Kedeputian Komunikasi, Informasi dan Aparatur, Kemenkopolhukam), wawancara pribadi, 7 Januari 2016.

[58] Munawar Ahmad (Ketua Staf Ahli DK2ICN), wawancara pribadi, 29 Februari 2016.

[59] Yono Reksoprodjo (Staf ahli Panglima TNI bidang C4ISR), wawancara pribadi, 2 Februari 2016

yang menangani masalah *cyber*. Sehingga belum ada pemetaan yang jelas mengenai bagaimana *cyberspace* akan diterapkan dalam industri pertahanan. Selain itu, Indonesia tidak memiliki industri besar yang bergerak dalam bidang *cyber* dan berkontribusi kepada pertahanan. Oleh sebab itu, menjadi sulit bagi pemerintah Indonesia dalam memetakan kebutuhan *cybersecurity* pada lingkup industri. Implementasi diplomasi pertahanan Indonesia untuk membangun industri pertahanan juga sulit dilakukan dalam ARF mengingat masih banyak negara ASEAN yang mencari bentuk dalam membuat *cybersecurity*-nya. Seperti yang dijelaskan sebelumnya, bahwa beberapa negara ARF memiliki pandangan yang berbeda dalam memahami *cybersecurity*. Di sisi lain, isu *cybersecurity* belum menjadi *concern* utama bagi sebagian anggota ARF. Hal inilah yang kemudian menimbulkan kebutuan industri pertahanan masing-masing negara dalam aspek *cyber* berbeda.

Salah satu kerjasama yang perlu diupayakan oleh pemerintah Indonesia dalam hal ini adalah pembangunan *information infrastructure*, karena hal tersebut paling penting dalam mendukung adanya *cyber.*[60] Hal tersebut juga bertujuan agar diplomasi pertahanan Indonesia dapat berkontribusi lebih lanjut pada tujuan kerangka kerja ARF poin nomor tiga, yaitu, "*Enhance practical cooperation between ARF Participating Countries to protect ICT-enabled critical infrastructure with the view to also developing resilient government ICT environments"* dan peningkatan kerjasama dalam membangun kapasitas regional sebagaimana yang tertuang pada poin nomor empat. Dengan adanya kerjasama praktis dalam pembangunan infrastruktur, peran diplomasi pertahanan dalam *defense industries* dapat ditingkatkan dan berkontibusi bagi *cybersecurity* pada lingkup nasional dan regional.

Catatan-Catatan Penutup

Kondisi *cyber* di Indonesia dihadapkan pada situasi yang tidak seimbang. Penggunaan *cyberspace* telah menyentuh berbagai aspek kehidupan bangsa yang meliputi sosial, budaya, ekonomi, politik, dan keamanan. Penetrasi jaringan internet di Indonesia terus meluas, bahkan pengguna jejaring sosial merupakan salah satu yang terbesar di dunia. Di sisi lain, *trend* ancaman *cyber* yang semakin mengarah kepada kepentingan nasional suatu bangsa menjadi tantangan bagi pemerintah pada tingkat strategis maupun operasional yang belum sepenuhnya mampu untuk membentuk sistem *cybersecurity* yang komprehensif. Ketidaksiapan pemerintah pada lingkup nasional ini perlu ditanggapi dengan menerapkan upaya diplomasi demi meniadakan atau meminimalisir potensi ancaman yang ada.

Melalui ARF *on cybersecurity initiatives,* pemerintah Indonesia mengimplementasikan diplomasi pertahanannya dengan membentuk dan meningkatkan rasa saling percaya diantara negara-negara ARF untuk melindungi keamanan nasionalnya dengan mengurangi potensi ancaman dan membentuk stabilitas kawasan. Selain itu, Indonesia juga berupaya meningkatan kapasitas melalui berbagai pelatihan yang bertujuan untuk membangun pengetahuan dan informasi di bidang *cybersecurity*. Diplomasi Pertahanan Indonesia telah berkontribusi positif dengan membentuk jaringan informasi antar negara ASEAN, China, Belanda, Rusia, AS, dan Australia berupa *point of contacts*. Kontak poin berguna bagi negara-negara di ASEAN dan kawasan dalam berkoordinasi mengenai penanganan insiden *cyber* yang meliputi pemetaan serangan, identifikasi pelaku, dan respon yang harus diambil.

Beberapa hal yang menjadi kendala dalam implementasi diplomasi pertahanan Indonesia dalam ARF meliputi aspek internal dan eksternal. Pada aspek internal terdapat permasalahan seperti belum adanya kebijakan nasional *cybersecurity*, belum adanya badan khusus yang menangani permasalahan *cyber,* dan koordinasi yang buruk antar instansi. Sementara pada aspek eksternal adalah pemahaman dan *concern* yang berbeda-beda tiap negara mengenai *cybersecurity* yang dihadapkan pada mekanisme pengambilan keputusan berdasarkan mufakat di ARF. Tantangan kedepan yang harus dihadapi permerintah Indonesia adalah bagaimana implementasi dari sistem kerjasama tersebut. Bayang-bayang akan buruknya koordinasi tentu

[60] Arwin D.W. Sumari (Staf Ahli DK2ICN), wawancara pribadi, 12 Januari 2016.

menjadi salah satu hal yang perlu diwaspadai, mengingat negara-negara ASEAN seringkali terlibat konflik dan perbedaan kepentingan dalam berbagai hal. Di sisi lain, beberapa peluang yang bisa digunakan oleh Indonesia adalah pemanfaatan negara anggota ARF yang besar dan meliputi negara-negara maju, percepatan penyampaian informasi dan komunikasi melalui diplomasi *track* II, dan kemungkinan akan kerjasama dan koordinasi antar negara yang lebih baik dengan diperolehnya *point of contacts.*

Referensi

Buku

Acharya, Amitav. (2001). *Constructing a Security Community in South East Asia:ASEAN and the Problem of Regional Power*. New York: Routledge.

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

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilso, G. I. (1989). *The Changing Face of War: Into The Fourth Generation*. *Marine Corps Gazette*, 22.

Reverson, D. S. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in Virtual World*. (D. S. Reverson, Ed.) Washington D.C: Georgetown University Press.

Schmitt, M. N. (Ed.). (2013). *Tallin Manual on The International Law Applicable to Cyber Warfare.* New York: Cambridge University Press.

Smith, M. (2015). *Research Handbook on International Law and Cyberspace.* (N. Tsagourias, & R. Buchan, Eds.) Massachusetts: Edwar Elgar Publishing Limited.

Tziarras, Z. (2014). The Security Culture of a Global and a Multileveled Cybersecurity. In E. G. Carayannis, D. F. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice.* New York: Springer.

Jurnal

Chanto, S. D. (2003). The ASEAN Regional Forum – The Emergence of 'Soft Security': Improving the Functionality of the ASEAN Security Regime. *Dialogue+cooperation*, 41-47.

Moodie, M. (2000). Cooperative Security: Implications for National Security and International Relations. *Cooperative Monitoring Center Occasional Paper, 14*.

Laporan

ASEAN Secretariat. (2013). *ASEAN's Cooperation on Cybersecurity and against Cybercrime.* Strasbourg: ASEAN Secretariat.

ASEAN Regional Forum. (2015). ASEAN Regional Forum on Security of and in The Use of Information and Communications Technologies (ICT's). *Cooperation in Ensuring Cyber Security*. Phnom Penh: ARF Library.

Kementerian Luar Negeri. (2015). *Rencana Strategis Kementerian Luar Negeri Tahun 2015-2019.* Jakarta: Kementerian Luar Negeri.

Makalah

Arifin Multazam. (2010). *Diplomasi Pertahanan Indonesia Terhadap KoreaSelatan Periode 2006-2009*. Jakarta: Universitas Indonesia.

Salim. (2012). *Peningkatan Kerjasama Pertahanan Indonesia di Kawasan Asia Tenggara Guna Mendukung Diplomasi Pertahanan Dalam Rangka Mewujudkan Stabilitas Kawasan*. Jakarta: Pusat Pengkajian Maritim Seskoal.

Syawfi, I. (2009). *Aktifitas Diplomasi Pertahanan Indonesia dalam Pemenuhan Tujuan-Tujuan Pertahanan Indonesia (2003-2008)*. Jakarta: Universitas Indonesia.

Website

Ahmad, M. (2015, April 15). Visi & Misi Badan Cyber Nasional dan Diplomasi Cyber. *Badan Cyber Nasional*. Bandung: Materi Power Point Seminar ITB-Deplu. Diakses 7 November 2015, dari http://www.slideshare.net/msyani/badan-cyber-nasional

Ali, A. H. (2007, Agustus 27). *Angkatan Laut dan Peperangan Generasi Keempat*. Diakses 30 Mei 2015, dari Forum Kajian Pertahanan dan Maritim: http://www.fkpmaritim.org/angkatan-laut-dan-peperangan-generasi-keempat/

ASEAN Secretariat. (2009). *ASEAN Political-Security Community Blueprint.* Diakses 16 November 2015, dari Asean.org: http://www.asean.org/archive/5187-18.pdf

Idcert, *Profil Indonesia Computer Emergency Response Team*, http://www.cert.or.id/tentang-kami/id/, diakses pada tanggal 14 Agustus 2016.

International Telecommunication Union. (n.d.). *ITU News*. Diakses 16 Agustus 2016 dari

Cybersecurity: https://www.itu.int/net/itunews/issues/2010/09/20.aspx

MacAskill, E., & Taylor, L. (2013, November 28). *Australia's spy agencies targeted Indonesian president's mobile phone*. Diakses 28 Mei 2015, dari The Guardian: http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone

Rahmanto, A. P. (2015, 04 30). *Indonesia Jadi Sarang Malware Dunia*. Diakses 15 November 2015, dari CNN Indonesia: http://www.cnnindonesia.com/teknologi/20150430163413-185-50331/indonesia-jadi-sarang-malware-dunia/

TENTANG PENULIS

Ahmad Rizky Mardhatillah Umar

Penulis adalah Mahasiswa Pascasarjana di Department of Politics, University of Sheffield dengan Program Studi MSc in Politics with Research Method. Pernah bekerja di beberapa lembaga penelitian, serta melakukan beberapa aktivitas *freelance*. Selain menempuh studi pascasarjana, juga menulis kolom untuk beberapa media. Minat Kajiannya terletak pada keterkaitan antara Gerakan Sosial dan Politik Internasional, dengan isu spesifik pada Islam Politik, Masyarakat Sipil, Regionalisme, dan Politik Identitas. Aktif sebagai Ketua Divisi Kajian Lingkar Studi Cendekia dan Wakil Ketua PCI Muhammadiyah Inggris Raya 2015-2017. Penulis dapat dihubungi melalui *email:* armumar1@sheffield.ac.uk

Arwin Datumaya Wahyudi Sumari

Penulis saat ini aktif sebagai analis Kebijakan Rencana Kontijensi Ekonomi dalam Kedeputian Politik dan Strategi, Sekretariat Jenderal Dewan Ketahanan Nasional. Gelar Doktoral diperoleh dari Institute Teknologi Bandung, jurusan Teknik Elektro dan Informasi. Penulis juga pernah bergabung sebagai peneliti di Intelligent System Research Group (ISRG) dan Signal and System Laboratory (SSL) ITB. Penulis dapat dihubungi melalui *email:* arwin.sumari@dkn.go.id atau arwin.sumari@yahoo.com

Awani Irewati

Penulis adalah peneliti di bidang Perkembangan Politik Internasional, Pusat Penelitian Politik-LIPI. S1 ilmu Hubungan Internasional diselesaikan di FISIP Universitas Airlangga, Surabaya. Gelar S2 diperoleh dari Asia and International Studies di Griffith University, Brisbane, Australia. Ia menekuni kajian utama tentang perbatasan antarnegara, khususnya perbatasan laut Indonesia dengan negara tetangga seperti Malaysia dan Singapura. Selain itu juga melakukan kajian kajian perbatasan antara Thailand dengan negara-negara tetangganya, serta mengkaji pendekatan konsep *connectivity* maupun *interconnectivity* di wilayah ASEAN dan sekitarnya. Penulis dapat dihubungi melalui *email:* irewatiawani@yahoo.co.id.

David Putra Setyawan

Penulis adalah pemerhati masalah diplomasi pertahanan nasional dan aktif sebagai Deputi Informasi dan Komunikasi dalam Lingkar Studi Strategis. Gelar Magister diperoleh dari Universitas Pertahanan Indonesia, Program Studi Diplomasi Pertahanan. Penulis dapat dihubungi melalui *email:* fa.davidsetyawan @gmail.com

Diandra Mengko Megaputri

Penulis adalah peneliti pada Pusat Penelitian Politik LIPI. Pendidikan S1 Hubungan Internasional diselesaikan di Universitas Katolik Parahyangan, sementara pendidikan S2 pada bidang ilmu Manajemen Pertahanan diselesaikan di Universitas Pertahanan Indonesia. Pernah aktif sebagai peneliti pada Indonesia Center for Diplomacy, Democracy, and Defense pada tahun 2012-2013. Minat kajiannya adalah isu-isu yang berhubungan dengan pertahanan, keamanan, Security Sector Reform (SSR), dan Industri Pertahanan. Penulis dapat dihubungi melalui *email:* diandramengko@yahoo.com

Fathimah Fildzah Izzati

Penulis adalah peneliti di Pusat Penelitian Politik LIPI, anggota redaksi *Indoprogress*, dan penulis buku *Politik Serikat Buruh dan Kaum Precariat: Pengalaman Tangerang dan Karawang*. Pendidikan S1 di bidang Ilmu Politik di tempuh di Universitas Indonesia. Penulis menekuni studi-studi yang berkaitan dengan isu ekonomi politik, buruh, perempuan dan politik. Penulis dapat dihubungi melalui *email:* fildzah.izzati@gmail.com

Ikrar Nusa Bhakti

Penulis adalah peneliti senior di Pusat Penelitian Politik Lembaga Ilmu Pengetahuan Indonesia (P2P LIPI). Gelar sarjana ilmu politik diperolehnya dari FISIP-UI dan gelar Ph.D di bidang Sejarah dan Politik dari School of Modern Asian Studies, Griffith University Brisbane, Australia. Beberapa kontribusi tulisannya antara lain termuat dalam buku Tentara yang Gelisah, Tentara Mendamba Mitra, Bila ABRI Berbisnis, Militer dan Politik Kekerasan Orde Baru (Penerbit Mizan, Bandung), The Fall of Soeharto, Human Security in Asia, Beranda Perdamaian: Aceh Tiga Tahun Pasca MoU Helsinki (Pustaka Pelajar, Yogyakarta), serta di jurnal-jurnal ilmiah maupun surat kabar lainnya. Penulis dapat dihubungi melalui *email:* ikrar.lipi@gmail.com

Khanisa Krisman

Penulis adalah peneliti pada Pusat Penelitian Politik LIPI. Gelar S1 Hubungan Internasional diperoleh dari Universitas Gadjah Mada pada tahun 2010. Sementara pendidikan S2 jurusan Hubungan Internasional ditempuh di College of Asia and The Pacific, Australian National University. Ia menekuni studi-studi terkait perkembagan Information and Communications Technology (ICT), isu-isu cyber dan sosial media dalam Hubungan Internasional, serta isu-isu terkait regionalisme di Asia Tenggara dan ASEAN. Penulis dapat dihubungi melalui *email:* khanisa_krisman@yahoo.com.

Nanto Sriyanto

Penulis adalah peneliti pada Pusat Penelitian Politik LIPI. Gelar S1 Hubungan Internasional diperoleh dari Universitas Padjajaran. Sementara pendidikan S2 ditempuh di The University of Queensland, Australia, School of Political Science and International Studies. Ia menekuni studi-studi terkait perkembangan keamanan internasional dan kawasan, politik luar negeri Indonesia serta kajian teori hubungan internasional. Penulis dapat dihubungi melalui email: nantosriyanto@gmail.com

Sandy Nur Ikfal Raharjo

Penulis adalah peneliti pada Pusat Penelitian Politik LIPI. Latar belakang pendidikannya adalah Ilmu Hubungan Internasional untuk S1 dan Resolusi Konflik untuk S2. Ia menekuni studi-studi pembangunan wilayah perbatasan, sengketa dan konflik perbatasan, serta isu-isu stabilitas keamanan regional. Penulis dapat dihubungi melalui *email:* sandy.raharjo@gmail.com.

Informasi
Hasil Penelitian Terpilih