LITERATUS
Jurnal Ilmiah Internasional Bidang Sosial dan Budaya
e-ISSN: 2686-5009

Diplomasi Pertahanan Indonesia dalam Pencapaian Keamanan Siber Melalui ADMM-Plus Tahun 2014-2019

Samuel Mangara Sianturi
Departemen Hubungan Internasional, Universitas Indonesia
Depok, Jawa Barat

Abstrak

Isu keamanan siber mulai muncul seiring terjadinya kemajuan dalam bidang teknologi informasi dan peningkatan penggunaan internet secara pesat. Namun, semakin besarnya kebutuhan internet dalam aktivitas sehari-hari masyarakat dunia maka semakin banyak pula potensi munculnya ancaman keamanan internasional dari aktivitas di dalam ruang lingkup siber. Mengingat sifat kejahatan siber yang "borderless", maka perlu penanganan yang melibatkan negara lain. Keikutsertaan Indonesia dalam ADMM-Plus menggambarkan upaya Indonesia dalam mencapai kepentingan nasional yaitu keamanan siber melalui lingkungan eksternal. Penelitian ini bertujuan untuk membahas diplomasi pertahanan Indonesia dalam pencapaian keamanan siber melalui ADMM-Plus Tahun 2014-2019. Dengan menggunakan teori diplomasi pertahanan dan metode kualitatif, penelitian ini memberikan gambaran bahwa diplomasi yang dilakukan Indonesia dalam ADMM-Plus masih berada pada tahap awal sehingga sulit jika dikatakan diplomasi yang dilakukan belum maksimal. Walaupun demikian, kehadiran ADMM -Plus memberikan dampak positif bagi Indonesia, khususnya dalam hal keamanan siber.

Kata kunci: *ADMM, ADMM-plus, diplomasi pertahanan, keamanan siber*

PENDAHULUAN

Isu keamanan internasional yang dihadapi oleh negara-negara di dunia senantiasa mengalami perubahan maupun perluasan. Kini isu keamanan internasional mulai menuju kepada masalah keamanan non-tradisional yang memiliki beragam bentuk ancaman keamanan baru. Salah satunya adalah isu *cybersecurity* atau keamanan siber. Isu keamanan siber mulai muncul seiring terjadinya kemajuan dalam bidang teknologi informasi dan peningkatan penggunaan internet secara pesat. Namun, semakin besarnya kebutuhan internet dalam aktivitas sehari-hari masyarakat dunia maka semakin banyak pula potensi munculnya ancaman keamanan internasional dari aktivitas di dalam ruang lingkup siber atau *cyberspace*.

Kittichaisaree (2017) dalam karyanya yang berjudul *Public International Law of Cyberspace* melihat beberapa bentuk permasalahan dalam dunia *cyberspace* yang bisa menjadi ancaman bagi negara. Pertama adalah *Cyber Espionage*. *Cyber espionage* adalah kegiatan mengintai atau memata-matai untuk mengumpulkan informasi tanpa mendapatkan izin dari pemilik yang sah dari informasi tersebut. Kedua adalah *cybercrime.* Kejahatan siber sendiri memiliki beragam bentuk seperti; *malicious* domain, *ransomware, malware, botnets, cryptojacking*, dan kejahatan-kejahatan siber lainnya yang terus bertambah seiring dengan kemajuan teknologi. Ketiga adalah *cyber terrorism.* Terorisme siber sendiri berarti tindakan terorisme yang berada pada dunia maya atau perangkat jaringan komputer, seperti pembajakan navigasi pesawat, pembajakan transportasi umum dengan menggunakan perangkat komputer dan lain-lain (Kittichaisaree, 2017: 297).

Permasalahan keamanan siber yang dipaparkan Kittichaisaree (2017) ini ternyata juga pernah terjadi di Indonesia. Permasalahan pertama adalah *cyber espionage*. Dilansir dari Tempo.com, terdapat empat penyadapan besar yang pernah terjadi di Indonesia dan dua di antaranya dilakukan oleh Australia. Pertama adalah penyadapan rumah dinas Gubernur DKI Jakarta saat itu, Joko Widodo pada tahun 2014. Kedua adalah penyadapan KPK terhadap Kabareskrim Susno Duadji. Ketiga adalah Penyadapan oleh Operator Telepon. New York Times dan Canberra Times melaporkan adanya dugaan penyadapan 1,8 juta pelanggan Telkomsel dan Indosat oleh NSA dan badan intelijen Australia. Keempat adalah Penyadapan Pemerintah Indonesia oleh Australia. Penyadapan yang dilakukan pada tahun 2009 ini berfokus pada lingkar

https://doi.org/10.37010/lit.v3i2.300

Vol. 3, No. 2, Oktober 2021, hal. 152-158

e-ISSN: 2686-5009

Istana Kepresidenan Indonesia, yaitu Susilo Bambang Yudhoyono, termasuk keluarga presiden. (Istman, 2014)

Permasalahan kedua adalah *cybercrime* atau kejahatan siber. Berdasarkan data dari jaringan keamanan Kaspersky (KSN) bahwa bank dan UKM (Usaha Kecil dan Menengah) di Indonesia menjadi sasaran *hacker* pada kuartal I tahun 2020. UKM di Indonesia mengalami serangan *cyber* kedua terbanyak di Asia Tenggara (CNN Indonesia, 2020). Tidak hanya itu saja, pada tahun 2010, menurut data perusahaan antivirus Sophos dan Symantec, Indonesia berada di posisi tiga besar dalam daftar negara yang terinfeksi *Stuxnet* (Detik.com, 2010). *Website* resmi pemerintah Indonesia pun tak luput dari serangan *cyber*. Menurut Lembaga Indonesia Security Incidents Response Team on Internet Infrastructure (ID-SIRTII) situs web milik pemerintah Indonesia dengan nama domain Internet .go.id menjadi target yang paling banyak diserang oleh peretas di dunia maya, dibandingkan dengan domain-domain lain. Tercatat, pada tahun 2014 lalu ada 3.288 insiden serangan terhadap situs pemerintah dengan domain .go.id. (Rahmanto, 2015).

Permasalahan ketiga adalah *cyber terrorism.* Pada tahun 2016, menurut Kapolri Jenderal Tito Karnavian bahwa saat ini pelaku terorisme melakukan rekrutmen anggota dan pelatihan merakit bom melalui media sosial. Selain itu, pelaku teroris juga mencari dana melalui Bitcoin. Salah satu kasusnya, terduga teroris Nur Solihin yang kerap kali melakukan aksi terorisme melalui media sosial (Hidayat, 2016).

Berdasarkan permasalahan-permasalahan tersebut, ancaman yang berasal dari ruang siber dapat mengakibatkan gangguan pada sektor ekonomi, politik, dan sosial bahkan mengganggu keamanan dan pertahanan negara. (Primawati & Pangestu, 2020: 8) Mengingat sifat kejahatan siber yang *"borderless"*, maka perlu penanganan yang melibatkan negara lain. Keikutsertaan Indonesia dalam ADMM-Plus menggambarkan upaya Indonesia dalam mencapai kepentingan nasional melalui lingkungan eksternal.

ADMM adalah forum pertemuan Menteri Pertahanan dari negara-negara anggota ASEAN. Forum ini menjadi ajang diplomasi pertahanan yang mengangkat tema-tema kerja sama keamanan seperti kerja sama penanggulangan bencana alam, pembangunan kepercayaan dan keterbukaan, serta pertukaran informasi. ADMM juga mengalami perkembangan signifikan dengan mengikutsertakan negara-negara mitra yang berada di luar ASEAN. Perluasan tersebut berujung pada bertambahnya nama ADMM menjadi ADMM-Plus. Bidang-bidang keamanan yang menjadi fokus dalam ADMM-Plus juga memasukkan kerja sama keamanan yang praktis, yaitu mengenai kerja sama dalam bidang keamanan non-tradisional.

Salah satu fokus utama ADMM-Plus adalah permasalahan siber dan penguatan keamanan siber. Sampai pada tahun 2019, sudah ada lima pertemuan ADMM-Plus terkait dengan keamanan siber. Dalam kurun waktu tersebut, terdapat beberapa capaian di antaranya adalah terbentuknya *cyber security portal*, *glossary of cyber terminologies* serta *points of contact and technical personnel directory* di mana ketiganya telah diujicobakan dalam latihan *Table Top Exercise* di Filipina (Kemenhan, 2019). Hal ini menunjukkan bahwa permasalahan siber menjadi salah satu isu penting yang dibahas di dalam ADMM-Plus.

Menurut Fitri (2018) dalam karyanya yang berjudul *Kebijakan Siber Nasional di Era Globalisasi*, kerja sama dalam ruang lingkup internasional dapat menjadi solusi untuk meningkatkan keamanan siber Indonesia saat ini. Oleh karena itu, tulisan ini akan melihat diplomasi pertahanan Indonesia dalam ADMM-Plus dengan menggunakan teori diplomasi pertahanan.

METODE

Penelitian ini merupakan penelitian kualitatif. Menurut Bryman (2004), penelitian kualitatif cenderung lebih berfokus pada kata-kata dibanding kuantifikasi angka dalam pengumpulan dan analisis data. Metode penelitian kualitatif menekankan pada deskripsi konteks karena bahasan detail sangat penting menunjukkan signifikansi subjek penelitian dan menyediakan penjelasan tentang konteks di mana suatu kejadian yang menjadi fokus penelitian terjadi (Bryman, 2004: 366–367). Selain itu, menurut Neumann (2014) metode kualitatif merupakan penelitian yang menginterpretasikan data-data dengan cara memberi arti terhadap data yang diperoleh. Dalam penelitian kualitatif ada yang disebut dengan teori dan data. Data dan teori

LITERATUS adalah jurnal yang diterbitkan oleh Neolectura, diterbitkan dua kali dalam satu tahun. LITERATUS adalah media publikasi ilmiah dalam bentuk makalah konseptual dan penelitian lapangan yang terkait dengan bidang kajian sosial dan budaya. Diharapkan LITERATUS dapat menjadi media bagi akademisi dan peneliti untuk menerbitkan karya ilmiah mereka dan menjadi sumber referensi untuk pengembangan ilmu pengetahuan.

Fokus:
Sosial dan Budaya

Ruang lingkup:
Humaniora, Pendidikan, Manajemen, Sejarah, Ekonomi, Linguistik, Sastra, Agama, Politik, Sosiologi, Antropologi, dan lainnya.

merupakan sebuah kesatuan di mana data yang diperoleh diliteraturkan, diinventarisasi, dikualifikasikan, kemudian permasalahan digambarkan dengan fakta-fakta yang ada dan disusun dalam sebuah tulisan (Neumann, 2014:13).

Penelitian ini menggunakan dua teknik dalam mengumpulkan data, pertama adalah studi kepustakaan. Penulis mempelajari berbagai literatur yang berkaitan dengan fenomena penelitian, khususnya mengenai konsep dan teori-teori yang digunakan dalam penelitian. Kedua adalah wawancara. Wawancara dilakukan dengan pedoman yang telah disusun, Hal ini dilakukan untuk memperoleh data-data penting yang berkaitan dengan fenomena penelitian. (Creswell, 2010: 266–270).

HASIL DAN PEMBAHASAN

Penelitian ini menggunakan diplomasi pertahanan sebagai kerangka analisis utama. Diplomasi pertahanan merupakan konsep yang ditujukan untuk mengintegrasikan instrumen militer dan diplomatik terkait pencegahan konflik dan mengelola krisis. Secara umum terdapat beberapa definisi dari diplomasi pertahanan. Yasuhiro (2006) dalam tulisannya yang berjudul *An Essay on China's Military Diplomatic: Examination of Intentions in Foreign Strategy* memberikan pengertian diplomasi pertahanan sebagai semua kegiatan diplomatik yang berkaitan dengan keamanan nasional dan kegiatan diplomatik militer. Menurut Cheyre (2013), aktivitas diplomasi pertahanan di era modern merupakan satu komponen dari diplomasi publik yang memiliki tujuan untuk menjaga perdamaian, melindungi integritas wilayah negara, dan menghindari kemunculan konflik melalui kerja sama yang dilakukan secara internasional.

Dalam perkembangannya, terdapat tiga bentuk atau varian dari diplomasi pertahanan, yaitu *Defense diplomacy for confidence building measures*, *Defense diplomacy for defense capabilities*, dan *Defense diplomacy for defense industry* (Multazam, 2010: 14). Dengan menggunakan tiga varian diplomasi pertahanan tersebut, penulis akan melihat sejauh mana diplomasi pertahanan Indonesia terkait keamanan siber dalam ADMM-Plus.

Bentuk diplomasi pertahanan pertama adalah *Defense diplomacy for confidence building measures* (CBM). Diplomasi pertahanan ini dilakukan untuk membangun hubungan baik dengan negara lain dan bertujuan untuk menurunkan ketegangan atau menghilangkan persepsi negatif antar negara (Cottey & Foster, 2004: 15-16). Keberhasilan hubungan diplomasi pertahanan yang baik dalam hal CBM akan membentuk kondisi lingkungan yang saling mempercayai antar pihak.

Berdasarkan penjelasan terkait capaian ADMM-Plus yang telah dijelaskan sebelumnya terlihat bahwa kerja sama yang dilakukan oleh Indonesia dengan negara-negara yang tergabung dalam ADMM-Plus terkait keamanan siber masih tahap penjajakan awal. Pada lima pertemuan sejak tahun 2017 hingga 2019, pembahasan terkait keamanan siber masih seputar definisi dari keamanan siber dan kerangka hukum. Walaupun masih tahap awal, namun hal ini merupakan satu langkah penting karena perlu adanya pemahaman terkait keamanan siber.

> *"Pada intinya pemahaman dikembalikan kepada masing-masing negara di dalam negeri atau pemahaman nasional karena jika kita berbicara mengenai cybersecurity, itu pun cybersecurity yang dipahami oleh satu negara dengan negara lain juga belum tentu sama. Misalnya, jika kita Indonesia memahami itu sebagai cybersecurity, Rusia memahami itu sebagai information security" (Wawancara dengan Wely, ASN BSSN pada tanggal 7 Mei 2021).*

Bentuk diplomasi pertahanan kedua adalah *Defense diplomacy for defense capabilities.* Diplomasi pertahanan untuk kapabilitas pertahanan dilakukan dalam rangka memperkuat kapabilitas pertahanan secara material seperti alutsista dan komponen pertahanan lain (Matthews, 2001: 1-9). Seperti yang dijelaskan sebelumnya bahwa belum ada hal yang signifikan dari diplomasi pertahanan yang dilakukan Indonesia dalam ADMM-Plus, khususnya terkait keamanan siber. Namun, dengan berubahnya ADMM menjadi ADMM-Plus di mana melibatkan negara-negara di luar ASEAN diharapkan ke depannya dapat meningkatkan kapabilitas pertahanan anggota ADMM, khususnya terkait keamanan siber. Hal ini seperti yang dijelaskan oleh Chalermpalanupap (2011) dalam tulisannya yang berjudul *Potential, Prospects and Direction of Practical Cooperation within the Framework of ADMM-Plus* bahwa salah satu alasan berubahnya ADMM menjadi ADMM – Plus adalah tidak hanya sebagai wadah dialog dan diskusi, ADMM-Plus juga dapat menjadi wadah untuk meningkatkan kerja sama praktikal bagi angkatan bersenjata

https://doi.org/10.37010/lit.v3i2.300

dari negara-negara ASEAN beserta mitra-mitranya. Hal ini akan semakin menguatkan kapabilitas kawasan untuk menghadapi berbagai tantangan keamanan bersama.

Menurut penelitian dari Trisni, Isnarti & Halim (2017) dengan judul *Peningkatan Keamanan Siber Asean Melalui Kerja Sama Keamanan Siber Dengan Australia* bahwa Australia yang merupakan mitra wicara ASEAN sekaligus bagian dari ADMM-Plus mampu membantu negara-negara ASEAN untuk meningkatkan kapabilitas keamanan siber. Oleh karena itu, pada tahun 2018 Pemerintah Republik Indonesia dan Pemerintah Australia sepakat menjalin kerja sama di bidang siber melalui penandatanganan *Memorandum of Understanding* (MoU). Melalui MoU ini, Indonesia dan Australia dapat mewujudkan kepentingan bersama sehingga saling menguatkan hubungan persahabatan antar kedua negara yang didasarkan pada prinsip-prinsip persamaan dan resiprositas. Indonesia dan Australia akan melakukan kerja sama dalam berbagai bidang, antara lain: berbagi informasi dan *best practices*, peningkatan kapasitas dan penguatan koneksi, serta kerja sama dalam bidang ekonomi digital; dan dalam bidang penanganan kejahatan siber. (Biro Hukum dan Humas BSSN, 2018) Salah satu realisasi dari MoU antara Indonesia dan Australia terkait keamanan siber adalah diadakannya *Cyber Bootcamp* yang bekerja sama dengan Australia National University (ANU). Tujuan adanya program Cyber Bootcamp adalah memberikan pelatihan kepada peserta dari Indonesia terkait keamanan siber.

Selain Australia, China dan Amerika Serikat juga menjadi negara mitra dalam pengembangan kapabilitas keamanan siber. Namun, menurut Fery bahwa dua negara yang juga merupakan bagian dari ADMM-Plus ini lebih kepada hubungan antara negara dengan Swasta, yaitu perusahaan Huawei dan Cisco. Pemerintah Indonesia dengan perusahaan swasta bekerja sama dalam bentuk penelitian dan pengembangan.

> *"Ada juga kegiatan yang diadakan bukan oleh pemerintah, tetapi justru B to G (Bussiness to Government). Contohnya, perusahaan telekomunikasi Huawei dan Cisco. Itu mereka sudah melakukan kegiatan kerja sama dengan pemerintah, termasuk dengan BSSN. Mereka membuat MOU dan tindak lanjut kerja sama. Dan rata-rata kita bergerak pada bidang peningkatan kapasitas atau kompetensi. Namun, pada tempat-tempat tersebut kami juga sekaligus melakukan tawar-menawar untuk melakukan joint research. Jadi, yang menarik adalah adanya kegiatan B to G tersebut dan bahkan kadang kegiatan G to G ditindak lanjuti menjadi kegiatan B to G. Bahkan ada juga kegiatan B to B dengan mendasarkan pada kegiatan yang sudah ada" (Wawancara dengan Fery, ASN BSSN pada tanggal 7 Mei 2021)*

Bentuk diplomasi yang ketiga adalah *Defense diplomacy for defense industry*. Diplomasi pertahanan untuk industri pertahanan merupakan diplomasi yang bertujuan untuk pembangunan dan penguatan industri pertahanan suatu negara. *Outcome* yang ditimbulkan dalam diplomasi ini adalah independensi politik dan ekonomi sehingga menurunkan tingkat interdependensi atau ketergantungan suatu negara dalam pengadaan alutsista (Multazam, 2010: 20).

Negara anggota ASEAN merupakan *net-purchaser* atas peralatan militer dari negara-negara yang memiliki industri pertahanan yang maju. Hal ini juga kemudian didukung oleh semakin meningkatnya anggaran pertahanan negara ASEAN. Agar anggaran persenjataan yang meningkat tersebut tidak mengalir ke negara selain negara ASEAN lain yang memiliki kemampuan memproduksi alutsista, maka diperlukan suatu mekanisme agar negara ASEAN dapat saling membantu dalam mengembangkan industri pertahanannya. Mekanisme ini juga akan dibutuhkan untuk membantu negara ASEAN mengurangi dependensi persenjataan yang memiliki risiko embargo. Berangkat dari hal ini, ASEAN Defense Industrial Collaboration (ADIC) dibentuk. (Tomotoka, 2013, dalam Dilahwangsa, Bhakti & Pedrason, 2019: 7)

Gagasan tentang kolaborasi industri pertahanan pertama kali didiskusikan pada ASEAN Defense Ministrial Meeting (ADMM) yang ke empat di Hanoi. ADIC dibentuk untuk mengurangi belanja senjata ASEAN ke luar, sehingga anggaran belanja ASEAN dapat dihemat. Dengan semua lingkup kegiatan yang dimiliki oleh ADIC, diekspektasikan bahwa kolaborasi industri pertahanan ini akan mereduksi impor pertahanan di negara anggota ASEAN dari 25 miliar dolar AS menjadi 12.5 miliar dolar AS secara akumulatif. (CSIS, 2011: 1)

Namun melihat data yang dikeluarkan oleh Stockholm International Peace Research Institute antara tahun 2011 hingga tahun 2016, kerja sama antar anggota ASEAN kurang signifikan. Dalam kolaborasi industri pertahanan, setiap negara memiliki tendensi untuk membatasi informasi atau data dalam pengembangan suatu persenjataan. Hal ini dikarenakan industri pertahanan menyangkut kepentingan nasional dan berhubungan erat dengan kapasitas militer suatu negara. Terlebih lagi, sebagian besar negara anggota ASEAN masih belum yakin sepenuhnya dalam hal berbagi teknologi atau dalam hal melonggarkan sikap proteksionis atas

Vol. 3, No. 2, Oktober 2021, hal. 152-158

e-ISSN: 2686-5009

LITERATUS adalah jurnal yang diterbitkan oleh Neolectura, diterbitkan dua kali dalam satu tahun. LITERATUS adalah media publikasi ilmiah dalam bentuk makalah konseptual dan penelitian lapangan yang terkait dengan bidang kajian sosial dan budaya. Diharapkan LITERATUS dapat menjadi media bagi akademisi dan peneliti untuk menerbitkan karya ilmiah mereka dan menjadi sumber referensi untuk pengembangan ilmu pengetahuan.

Fokus:
Sosial dan Budaya

Ruang lingkup:
Humaniora, Pendidikan, Manajemen, Sejarah, Ekonomi, Linguistik, Sastra, Agama, Politik, Sosiologi, Antropologi, dan lainnya.

industri pertahanan mereka masing-masing. Oleh karena itu, hal ini masih menjadi tantangan dalam kerja sama industri pertahanan. (Dilahwangsa, Bhakti & Pedrason, 2019: 19-21)

Perbedaan perkembangan industri pertahanan antar negara ASEAN juga menjadi penghambat. Tercatat bahwa dari sepuluh negara ASEAN, hanya empat yang memiliki fondasi industri pertahanan yang memadai. Disparitas perkembangan industri pertahanan ini mengakibatkan negara ASEAN sulit untuk menentukan titik awal mulai dalam kolaborasi pertahanan, di mana setiap negara mampu untuk berkontribusi. Disparitas ini muncul karena beberapa negara memiliki pertumbuhan ekonomi yang berbeda. Umumnya, semakin baik ekonomi suatu negara tersebut, maka anggaran untuk pertahanan akan semakin besar. Kemudian, perspektif kebutuhan pengembangan industri pertahanan setiap pemerintah berbeda. Singapura, misalnya, mengembangkan industri pertahanan dalam negeri dilihat sangat diperlukan. Hal ini dikarenakan perspektif *midget psychosis* mereka yang selalu merasa rentan sebagai negara kecil namun dikelilingi negara-negara besar seperti Malaysia dan Indonesia (Bitzinger, 2013 dalam Dilahwangsa, Bhakti & Pedrason, 2019:21),

Dalam ruang lingkup ADMM-Plus, Seperti yang dijelaskan sebelumnya bahwa pembahasan terkait keamanan siber dalam ADMM-Plus masih pada tahap awal. Belum mencapai pada kerja sama ataupun pembahasan terkait industri pertahanan. Namun, Menteri Pertahanan RI Ryamizard Ryacudu dan Menteri Pertahanan Australia Marise Payne melakukan pertemuan dalam forum *Defence Ministers' Meeting* di Fleet Base East Garden Island, Sidney, Australia pada bulan Maret tahun 2017. Pada pertemuan ini, kedua Menteri Pertahanan telah membahas kerja sama bilateral pertahanan di bidang keamanan maritim, industri pertahanan, serta ilmu pengetahuan dan teknologi terkait keamanan siber. Dibicarakan pula mengenai kerja sama di bidang industri pertahanan untuk memperkuat kerja sama bilateral sekaligus meningkatkan industri pertahanan kedua negara. Menteri Pertahanan Australia juga membahas mengenai kerja sama bidang ilmu pengetahuan dan teknologi pertahanan yang telah terjalin lama antara kedua negara. (Kemhan, 2017)

Berdasarkan pemaparan di atas, dapat dikatakan bahwa walaupun masih berada pada tahap awal, kehadiran ADMM-Plus memberikan dampak positif bagi Indonesia, khususnya dalam hal keamanan siber. Melalui ADMM-Plus, maka terciptanya hubungan yang baik dan saling percaya antar negara yang tergabung dalam ADMM-Plus. Selain itu, ADMM-Plus juga dapat menjadi gerbang awal untuk Indonesia melakukan hubungan bilateral kepada negara yang juga tergabung dalam ADMM-Plus untuk meningkatkan kapabilitas serta industri keamanan siber.

PENUTUP

Setelah melakukan analisis terhadap fakta empirik dalam literatur maupun hasil penelitian mengenai diplomasi Indonesia terkait keamanan siber dalam forum ADMM-Plus, diplomasi yang dilakukan Indonesia dalam ADMM-Plus masih berada pada tahap awal sehingga sulit jika dikatakan diplomasi yang dilakukan belum maksimal. Walaupun demikian, kehadiran ADMM-Plus memberikan dampak positif bagi Indonesia, khususnya dalam hal keamanan siber. Melalui ADMM-Plus, maka terciptanya hubungan yang baik dan saling percaya antar negara yang terabung dalam ADMM-Plus. Oleh karena itu, penulis memberikan beberapa rekomendasi kebijakan berkaitan dengan keamanan siber di Indonesia

Rekomendasi pertama adalah perlu menjadikan isu keamanan siber sebagai isu prioritas, maka dapat tergambar dengan baik kepentingan Indonesia yang akan dibawa dalam proses diplomasi pertahanan baik bilateral maupun multilateral. Rekomendasi kedua adalah perbaikan tata kelola keamanan siber baik ditingkat nasional maupun regional. Rekomendasi ketiga adalah membuka hubungan baik serta kerja sama dengan negara lain.

DAFTAR PUSTAKA

ASEAN Defence Minister's Meeting. 2017. *About the ASEAN Defence Ministers' Meeting (ADMM)*. Diakses dari https://admm.asean.org/index.php/about-admm/about-admm.html

Biro Hukum dan Hubungan Masyarakat BSSN. 2018. *Press Release Indonesia Dan Australia*

https://doi.org/10.37010/lit.v3i2.300

Sepakat Jalin Kerjasama Di Bidang Siber. Diakses dari https://bssn.go.id/press-release-indonesia-dan-australia-sepakat-jalin-kerjasama-di-bidang-siber/

Bryman, A. (2004). *Social Research Methods.* New York: Oxford University Press.

Center for Strategic & International Studies. (2011). *ASEAN Defense Industry Collaboration.* Washington: CSIS diunduh dari https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/110907_DIIG_Current_Issues_25_ASEAN.pdf

Chalermpalanupap, T. (2011). *Carving Out a Crucial Role for ASEAN Defence Establishments in the Evolving Regional Architecture* dalam Singh, Bhubhindar and Tan. *From 'Boots' to 'Brogues': The Rise of Defence Diplomacy in Southeast Asia.* Singapore: RSIS

Cheyre, J. E. (2013). *Defence Diplomacy*. dalam A. F. Cooper, J. Heine, & R. Thakur, *The Oxford Handbook of Modern Diplomacy*. Oxford: Oxford University Press.

CNN Indonesia. (2020). *Bank dan UKM Indonesia Jadi Sasaran Hacker Kala Pandemi.* Diakses dari https://www.cnnindonesia.com/teknologi/20200723104339-185-528047/bank-dan-ukm-indonesia-jadi-sasaran-hacker-kala-pandemi

Cottey, A. & Anthony, F. (2004). *Strategic Engagement: Defence Diplomacy as a Means of Conflict Prevention.* New York: Routledge.

Creswell, J. W. (2010). *Research Design; Pendekatan Kuantitatif, Kualitatif dan Mixed.* Yogyakarta: Pustaka Pelajar

Dilahwangsa, Z., Ikrar N. B., Rodon P. (n.y). *Asean Defense Industrial Collaboration (ADIC. Sebagai Media Diplomasi Pertahanan Negara Anggota Asean.* Dalam jurnal Diplomasi Pertahanan. Jakarta: Universitas Pertahanan

Fitri, A. (2018). *Kebijakan Siber Nasional di Era Globalisasi Informasi*. Dalam buku *Keamanan Siber dan Pembangunan Demokrasi di Indonesia.* Jakarta: Pusat Badan Keahlian DPR RI

Hidayat, F. (2016). *Kapolri: Ada terorisme siber, rekrutmen & pelatihan bom lewat online.* Diakses dari https://www.merdeka.com/peristiwa/kapolri-ada-terorisme-siber-rekrutmen-pelatihan-bom-lewat-online.html

Itsman, M.P. (2014). *4 Kasus Penyadapan Besar di Indonesia.* Diakses dari https://nasional.tempo.co/read/556304/4-kasus-penyadapan-besar-di-indonesia?page_num=2

Kementerian Pertahanan Republik Indonesia. 2017. *Indonesia – Australia Sepakat Tingkatkan Kerjasama Bilateral Pertahanan Kedua Negara.* Diakses dari https://www.kemhan.go.id/2017/03/16/pertemuan-menteri-pertahanan-ri-dengan-menhan-australia-pada-defence-ministers-meeting.html

Kementerian Pertahanan Republik Indonesia. 2019. *Kapushansiber Menghadiri Pertemuan Admm Ke 5 Di Selandia Baru.* Diakses dari https://www.kemhan.go.id/bainstrahan/2019/10/27/kapushansiber-menghadiri-pertemuan-admm-ke-5-di-selandia-baru.html

Kittichaisaree, K. (2017). *Public International Law of Cyberspace.* Switzerland: Springer International Publishing.

Matthews, R. & John, T. (2001). *Managing the Revolution in Military Affairs.* New York: Palgrave MacMilan.

Multazam, A. (2010). *Diplomasi Pertahanan Indonesia Terhadap Korea Selatan Periode 2006-2009.* Tesis. Depok: Universitas Indonesia.

Neumann, W. L. (2014). *Social Research Method : Qualitative and Quantitative Approach.* Edinburgh: Pearson Education Limited

Rahmanto, A. P. (2015). *Situs Web Pemerintah Paling Sering Diserang Hacker.*

Sekretariat Nasional ASEAN – Indonesia. (2020). *ASEAN Defence Ministers Meeting (ADMM).* Diakses dari http://setnas-asean.id/asean-defence-ministers-meeting-admm

Tomotaka, Shoji. 2013. *ASEAN Defense Ministers' Meeting (ADMM) and ADMM Plus: A Japanese Perspective.* Diunduh dari http://www.nids.mod.go.jp/english/publication/kiyo/pdf/2013/bulletin_e2013_2.pdf

Trisni, S., Rika, I. & Abdulhalim. (n.y). *Peningkatan Keamanan Siberasean Melalui Kerja Sama Keamanan Siber Dengan Australia.* Dalam Jurnal ASEAN Studies Center. Padang: Universitas Andalas.

Vol. 3, No. 2, Oktober 2021, hal. 152-158

e-ISSN: **2686-5009**

Yasuhiro, M. (2006). *An Essay on China's Military Diplomatic: Examination of Intentions in Foreign Strategy*. Tokyo: National Institute for Defense Studies.

LITERATUS adalah jurnal yang diterbitkan oleh Neolectura, diterbitkan dua kali dalam satu tahun.
LITERATUS adalah media publikasi ilmiah dalam bentuk makalah konseptual dan penelitian lapangan yang terkait dengan bidang kajian sosial dan budaya.
Diharapkan LITERATUS dapat menjadi media bagi akademisi dan peneliti untuk menerbitkan karya ilmiah mereka dan menjadi sumber referensi untuk pengembangan ilmu pengetahuan.

Fokus:
Sosial dan Budaya

Ruang lingkup:
Humaniora, Pendidikan, Manajemen, Sejarah, Ekonomi, Linguistik, Sastra, Agama, Politik, Sosiologi, Antropologi, dan lainnya.