JURNAL KETAHANAN NASIONAL
Vol. 25, No. 3, Desember 2019, Hal 331-347
DOI:http://dx.doi.org/ 10.22146/jkn.50344
ISSN:0853-9340(Print), ISSN:2527-9688(Online)
Online sejak 28 Desember 2015 di :http://jurnal.ugm.ac.id/JKN

VOLUME 25 No. 3, Desember 2019 Halaman 331-347

Penerapan *Military Confidence Building Measures* dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber

Hidayat Chusnul Chotimah
Program Studi Ilmu Hubungan Internasional Universitas Teknologi Yogyakarta
email: hidayat.chotimah@staff.uty.ac.id

Muhammad Ridha Iswardhana
Program Studi Ilmu Hubungan Internasional Universitas Teknologi Yogyakarta
email: muhammad.ridha@staff.uty.ac.id

Tiffany Setyo Pratiwi
Program Studi Ilmu Hubungan Internasional Universitas Teknologi Yogyakarta
email: tiffany.subarman@gmail.com

ABSTRACT

This research discussed implementation of military confidence building in responding various threats that may arised in Indonesian cyber sovereignty.

This study used qualitative approach with data collection through literature study and in-depth interviews namely Director for International Security and Disarmament Ministry of Foreign Affairs of The Republic of Indonesia, Deputy of Protection National Cyber and Crypto Agency of the Republic of Indonesia (BSSN), and Ministry of Communications and Informatics of the Republic of Indonesia.

The results showed that implementation of military confidence building to upheld national resilence in cyberspace consisted of three aspects, namely the exchange of information and communication, transparency and verification, and military restraint in the field of cyber.

Keywords: Military CBM, National Resilience, Cyberspace, Indonesia.

ABSTRAK

Penelitian ini membahas penerapan *military confidence building* dalam merespon berbagai ancaman yang mungkin timbul di ranah kedaulatan siber Indonesia.

Pendekatan yang digunakan dalam penelitian ini yaitu melalui pendekatan kualitatif dengan teknik pengumpulan data melalui studi pustaka dan wawancara mendalam dengan Direktorat Jenderal Kerja Sama Multilateral Kementerian Luar Negeri Republik Indonesia sub bagian Direktorat Keamanan Internasional dan Perlucutan Senjata Kementerian Luar Negeri, Badan Siber dan Sandi Negara (BSSN) Deputi Bidang Proteksi dan Kementerian Komunikasi dan Informatika Republik Indonesia.

Hasil penelitian menunjukkan bahwa penerapan *military confidence building* untuk menegakkan ketahanan nasional di ruang siber dilakukan melalui tiga aspek yaitu pertukaran informasi dan komunikasi, transparansi dan verifikasi, dan pembatasan militer (*military restraint*) di bidang siber.

Keywords: Military CBM, Ketahanan Nasional, Ruang Siber, Indonesia.

PENGANTAR

Perkembangan teknologi informasi dan komunikasi (TIK) telah meningkatkan jumlah pengguna internet dari hanya 3 juta pada tahun 1990 menjadi lebih dari 3,2 miliar pada tahun 2015 dan diperkirakan akan mencapai 4,7 miliar pada 2025 (Pawlak, 2016:129). Dalam hal ini, internet membawa dimensi baru pada keamanan informasi dan siber, yang pada akhirnya memberikan implikasi terhadap hubungan internasional, dimana, apa pun yang dikirim melalui internet, berpotensi untuk dapat disebarluaskan dengan bebas (Westcott, 2008:14).

Dengan adanya perkembangan TIK tersebut mendorong negara-negara untuk menyusun strategi pertahanan salah satunya di domain atau ruang siber. Aktor di dalam domain siber sendiri melibatkan tidak hanya aktor negara tetapi juga melibatkan aktor lain seperti perusahaan, organisasi non-pemerintah maupun masyarakat. Ikut diperhitungkannya domain siber di samping domain darat, laut dan udara dalam hubungan internasional pada dasarnya masih menimbulkan perdebatan seperti sejauh mana perlombaan senjata (*arm race*) di ruang siber dapat dibatasi dan sejauh mana efek destruktif dari serangan siber terhadap infrastruktur kritis sebuah negara dapat diberikan sanksi (Borghard dan Lonergan, 2018:10-11).

Sementara itu, baik kapabilitas militer di ruang siber dari sebuah negara maupun kemampuan musuh di ruang siber tidak mudah dilihat ataupun diprediksi. Kondisi ini tentu mengantarkan pada perlombaan senjata di ruang siber apabila terus dibiarkan. Hal ini kemudian mendorong negara-negara di dunia untuk membangun kepercayaan dan menciptakan rezim yang mampu membatasi kompetisi di ruang siber salah satunya melalui *confidence building measures* (CBM). CBM dalam persenjataan konvensional dibangun berdasarkan mekanisme pemantauan (*monitoring*) dan verifikasi. Hal ini konstras sekali dengan mekanisme pemantauan dan verifikasi di domain siber karena kedua mekanisme ini sulit diterapkan. Domain siber yang bersifat anonimitas dan kompleks seringkali menghalangi adanya perjanjian internasional untuk membatasi perilaku aktor khususnya negara di domain ini. Melalui CBM inilah langkah-langkah dalam membangun kepercayaan melalui peningkatan transparansi, kerja sama, dan stabilitas.

CBM sendiri terbagi menjadi *military CBM dan Non-military CBM*. Penelitian ini akan melihat bagaimana penerapan *military Confidence Building Measures* (CBM) dalam menjaga ketahanan nasional Indonesia di ruang siber. Pendekatan CBM di sini merupakan upaya pencegahan konflik secara berkelanjutan maupun mispersepsi yang dimungkinkan timbul di kancah internasional. Dalam konteks ini, peneliti akan menganalis penerapan *military CBM* dalam konteks ketahanan nasional Indonesia di ruang siber.

Ketahanan nasional sebagai sebuah konsep yang berkembang di Indonesia lahir pada masa perjuangan Perang Kemerdekaan Indonesia melalui Tentara Nasional Indonesia (TNI), dimana pada awalnya masih digunakan istilah Belanda yaitu *nationale weerbaarheid.* Makna dari istilah tersebut yaitu ketahanan bangsa Indonesia terhadap berbagai goncangan dan ancaman. Istilah *weerbaarheid* kemudian disinonimkan dengan istilah ketahanan, sehingga *nationale weerbaarheid* berarti ketahanan nasional (Suryohadiprojo, 1997:13). Dengan demikian, definisi ketahanan nasional sebagaimana disebutkan dalam Penelitian Suryohadiprojo (1997) merupakan sebuah

kondisi dinamis suatu bangsa, berisikan keuletan dan ketangguhan, yang membentuk kekuatan nasional yang mampu menghadapi dan mengatasi setiap macam ancaman, tantangan, hambatan dan gangguan, baik yang datang dari luar maupun dari dalam negeri, secara langsung atau tidak langsung membahayakan kelangsungan hidup bangsa serta pencapaian tujuan nasionalnya.

Suryohadiprojo (1997) menyebutkan bahwa aspek-aspek yang diperhitungkan dalam ketahanan nasional terdiri dari aspek yang bersifat alamiah seperti geografi, penduduk dan kekayaan alam maupun yang bersifat sosial yang terdiri atas ideologi, politik, ekonomi, sosial budaya dan pertahanan keamanan. Sementara Jafar, Sudirman dan Rifawan (2019) menyebutkan bahwa ketahanan nasional terdiri dari beberapa aspek yang saling berintegrasi untuk memperkuat komponen nasional dalam menghadapi segala ancaman yang ada.

Peneliti lain yang juga mengkaji tentang ketahanan nasional adalah Prasanti dan Fitriani (2017) dimana salah satu cakupan ketahanan nasional adalah ketahanan informasi nasional. Prasanti dan Fitriani (2017) menganggap pentingnya keterlibatan dan kerjasama antara masyarakat, pemerintah, dan media dalam menjaga ketahanan informasi nasional.

Melihat konsep dan definisi yang telah ada di penelitian-penelitian sebelumnya di bidang ketahanan nasional, memberikan khasanah pengetahuan bagi peneliti untuk mengkaji lebih jauh mengenai aspek ketahanan nasional di ruang siber melalui penerapan *military Confidence Building Measures* (CBM). Untuk menggali lebih jauh terkait dengan penelitian tersebut, peneliti menggunakan pendekatan penelitian kualitatif yang dilakukan melalui pencarian sebuah jawaban dengan memeriksa berbagai pengaturan sosial dan kelompok atau individu di suatu *setting* sosial (Berg dan Lune, 2017:15). Pengaturan sosial di sini terkait dengan ketahanan nasional di ruang siber yang dilakukan oleh pemerintah Indonesia. Sementara itu, penelitian ini beranjak dari pengamatan terhadap ancaman terhadap kedaulatan siber di Indonesia sebagai titik awal dalam pengamatan. Kemudian konsep CBM digunakan sebagai strategi dalam membangun ketahanan nasional Indonesia di ruang siber.

Penelitian ini akan melihat pola hubungan antar variabel yaitu variabel dependen dan independen. Konsep CBM akan menjadi variabel independen dan ketahanan nasional Indonesia di ruang siber akan menjadi variabel dependen. Kedua variabel tersebut akan dianalisis dan digunakan untuk menjawab rumusan masalah dalam bentuk eksplanatif.

Penelitian ini menggunakan jenis data yang terdiri dari data primer yang didapatkan dari wawancara mendalam, dan data sekunder yang berasal dari studi pustaka. Wawancara mendalam dilakukan dengan sejumlah narasumber yang berasal dari Direktorat Jenderal Kerja Sama Multilateral Kementerian Luar Negeri Republik Indonesia sub bagian Direktorat Keamanan Internasional dan Perlucutan Senjata, Badan Siber dan Sandi Negara (BSSN) Deputi Bidang Proteksi dan Kementerian Komunikasi dan Informatika Republik Indonesia.

PEMBAHASAN

Tren Pengguna Internet Di Indonesia: Sebuah Peluang dan Tantangan

Sebagai salah satu negara dengan jumlah pengguna internet terbesar ke-lima di dunia (apjii.or.id), telah menempatkan Indonesia menjadi negara dengan serangan siber terbesar

ke-dua di dunia (www.cnnindonesia.com). Menurut Asosiasi Penyelenggara Jaringan Internet Indonesia (APJII) sebanyak 171,2 juta penduduk Indonesia telah mengakses internet pada 2019. Jumlah ini meningkat hampir 30 juta dibandingkan tahun sebelumnya (tekno.kompas.com). Di samping sebagai salah satu negara pengguna internet yang terus meningkat, menurut laporan dari OECD pada tahun 2019, Indonesia merupakan salah satu negara dengan tingkat pertumbuhan PDB tercepat di Asia, yaitu sebesar 5,1% per tahun. Lintasan pertumbuhan tersebut dapat disimpulkan bahwa pada tahun 2050 Indonesia akan menjadi ekonomi terbesar keempat di dunia dalam hal paritas daya beli (Paterson, 2019:217).

Realitas-realitas yang ada tersebut menunjukkan bahwa penggunaan siber di Indonesia memiliki peluang sekaligus ancaman yang besar. Meskipun memberikan berbagai kemudahan pada satu sisi, akan tetapi dapat menyebabkan ancaman siber pada sisi lainnya (Danuri dan Suharnawi, 2017). Hal ini dibuktikan bahwa negara ini merupakan negara kelima tujuan serangan siber terbanyak di kawasan Asia Pasifik pada 2018. Bahkan, ketika sedang marak invasi *virus ransomware* dan *wannacry*, Indonesia menjadi negara terbanyak kedua di dunia yang mendapatkan serangan setelah Tiongkok. Australia, Hongkong, dan Singapura sebagai salah satu negara maupun wilayah maju pun bertengger jauh di bawah Indonesia dalam hal serangan siber (teknologi.bisnis.com).

Tren lain dalam dunia siber (*cyber world*) adalah meningkatnya penggunaan data di dunia siber sebagai alat dalam kegiatan politik, baik dalam lingkup nasional maupun hubungan internasional. Di masa lalu, data yang diperoleh melalui spionase dunia maya/ siber dikumpulkan secara diam-diam, diklasifikasikan dan disimpan untuk analisis intelijen atau untuk keuntungan finansial. Sekarang, data yang dikumpulkan, digunakan sebagai modal politik untuk mempermalukan target dan menyebabkan reputasi aktor tersebut rusak maupun mengalami kerugian secara finansial akibat tindakan tersebut. Sebagai contohnya adalah pencurian profil Komite Nasional Demokrat AS (*US Democratic National Committee*) pada Juli 2016 yang dirilis melalui WikiLeaks, sehingga telah mempermalukan Demokrat selama masa sensitif kampanye pemilu di sana. Tindakan tersebut tentu memiliki efek destabilisasi politik dan juga dianggap bahwa penggunaan ruang maya/ siber (*cyberspace*) telah mengganggu proses demokrasi (ASPI, 2016:4-5).

Contoh lain diungkapkan dari hasil wawancara pada 24 Juni 2019 dengan narasumber Kementerian Komunikasi dan Informatika yang sekaligus juga merupakan Akademisi dari CfDS UGM yang menyebutkan bahwa di Brasil ada operasi informasi dimana cara berfikir dan persepsi masyarakat terhadap satu kandidat tertentu diputar balikan dengan *hoax*, dengan *hate speech*, dengan *cyber bullying*, dan sebagainya. Hal ini kemudian mengakibatkan pada pembalikkan suara di mana yang tadinya menang menjadi kalah, dan yang semula kalah menjadi menang.

Di Indonesia sendiri pelaksanaan pemilihan umum baik menyangkut isu pemilihan kepala daerah maupun pemilihan presiden diwarnai pula dengan pemanfaatan big data dan media sosial untuk mempengaruhi opini publik. Hal ini bisa dilihat misalnya pada Pilpres 2014, Pilkada 2017 maupun Pilpres 2019 (Indrawan, 2019:2). Pada tahun 2014, salah satu kampanye pilpres di Indonesia

memanfaatkan cluster *cybertroop* untuk mendukung maupun menyerang tokoh tertentu. Yang tidak kalah penting dalam isu kajian politik di Indonesia adalah adanya cluster *cybertroop* yang kontra terhadap pemerintah misalnya *Muslim Cyber Army* (MCA) yang dianggap sebagai agen *proxy war* dari luar negeri dan seringkali dianggap menyebarkan *hate speech* maupun *hoax* di Indonesia (Fahmi, 2018). Hal ini diperkuat dengan hasil wawancara pada 24 Juni 2019 dengan narasumber dari Kementerian Komunikasi dan Informatika yang menyebutkan bahwa:

> *"Dalam konteks Indonesia, kalau saya ditanya ada operasi informasi mas di Indonesia? Ada. Efeknya seberapa besar? Tidak sebesar di Brazil. Di Brazil membalikkan hasil, di Indonesia hanya mendistorsi prosentase kemenangan. Belum banyak orang tau konteks besar itu, dan orang begitu yakin terhadap posisi politiknya karena di alam bawah sadar mereka, mereka sudah dipengaruhi. Itu namanya micro targetting. Micro targetting itu bagaimana informasi disebarluaskan kemudian mempengaruhi psikologis setiap orang yang menerima." (Wawancara dengan Dedy Permadi, Kemenkominfo, 2019).*

Di samping aspek ekonomi dan politik, ancaman terhadap keamanan siber juga menyangkut pelumpuhan terhadap *Critical National Infrastructure* (CNI), seperti energi, air dan komunikasi, sehingga melumpuhkan aktivitas di kota-kota besar dan pusat ekonomi. Seperti Peristiwa yang terjadi di *western* Ukraina pada bulan Desember 2015. Peristiwa tersebut menggambarkan apa yang mungkin terjadi ketika suatu bangsa dihadapkan dengan agresor siber yang tangguh dan canggih dimana insiden di dunia maya/ siber mampu menargetkan jaringan listrik sehingga menyebabkan lebih dari 230.000 penduduk tanpa listrik. Peristiwa serupa yang mengancam CNI juga terjadi di Asia-Pasifik. Pada bulan Juli 2016, sehubungan dengan adanya konflik atau sengketa di Laut Cina Selatan, sistem audio dan video di dua bandara internasional Vietnam terganggu dimana terdapat pesan yang ofensif dan mengancam. Selain itu, situs *web* Vietnam Airlines juga telah diambil alih oleh pihak yang tidak dikenal sehingga berdampak pada lebih dari 400.000 data penumpang terganggu dan *dumped*' secara *online*. Insiden di Vietnam tersebut merupakan kelanjutan insiden siber akibat dari putusan *Permanent Court of Arbitration*, yang berpihak pada Filipina yang bersengketa dengan Cina atas klaimnya di Laut Cina Selatan, dimana situs web *Permanent Court of Arbitration* di Den Haag dibajak pada tahun 2015, dan diikuti dengan pembajakan terhadap situs web pemerintah Filipina sehingga menjadi *offline* (ASPI, 2016:4-5).

Melihat tren insiden siber yang terjadi di beberapa negara menandakan bahwa ada hubungan antara peristiwa di dunia maya/ siber dengan dunia fisik dimana insiden siber yang terjadi tersebut mengancam infrastruktur kritis akibat adanya gesekan geopolitik dengan negara lain. Dengan demikian, tingginya tingkat konektivitas lintas batas di dunia siber, memerlukan adanya pendekatan baru untuk keamanan dunia maya/ siber sehingga menjadi salah satu faktor penting dalam dimensi internasional (Gady dan Austin, 2010:1). Oleh sebab itu, selain berfokus pada pertahanan siber atau perang siber, juga penting untuk mengembangkan diplomasi siber mengingat bahwa beberapa pemerintah bahkan telah memikirkan dimensi diplomatik keamanan siber, namun belum mengembangkan strategi diplomatik yang sepadan dengan ancaman yang ditimbulkan.

Di Indonesia sendiri, diplomasi siber memang sudah dirancang namun masyarakat luas masih belum banyak yang mengetahuinya dan masih berrsifat terbatas. Fungsi diplomasi siber sendiri melibatkan beberapa kementerian seperti Kementerian Luar Negeri sebagai ujung tombaknya, kemudian melibatkan BSSN, Kemenkominfo, Kementerian Pertahanan, Kemnko Polhukam, maupun TNI. Seperti yang disebutkan oleh narasumber dari Kementerian Komunikasi dan Informatika dan Kementerian Luar Negeri.

> *"Kalau ditanya bagaimana perkembangan Indonesia sekarang? Indonesia baru sampai ke taraf digital diplomacy. Cyber diplomacy digarap tetapi belum serius. Pernah gak denger diplomat kita negosiasi tentang ee cyber war misalnya? Dibahas, tetapi levelnya masih level terbatas, misalnya free flow of data. Data ini harus kita kelola kemudian kalau data ini apakah bisa berseliweran, bertukar antar negara itu yang kita diskusikan. Di forum G20 kemarin ada digital ministerial meeting. Pak menteri juga hadir. Disitu dibicarakan free flow of data. Bagaimana di satu sisi itu ada dua pertentangan itu. Satu sisi kita punya kepentingan yang sangat besar untuk ada free flow of data. Data is the new oil. Data sekarang menjadi aset yang luar biasa bagi negara manapun. Dengan data you bisa kuasai dunia." (Wawancara dengan Dedy Permadi, Kemenkominfo, 2019).*

> *"Ee sebentar Kemlu dalam hal ini sesuai dengan Undang-Undang hubungan luar negeri kita menjadi ujung tombak pelaksanaan diplomasi siber terkait dengan peran Kementerian Luar Negeri. Tentunya kita juga akan menyertakan beberapa Kementerian dan lembaga terkait seperti tentunya BSSN, juga ada Kementerian terkait seperti Kemenko Polhukam, Kominfo juga kita libatkan, terus Kemhan dan TNI juga kita libatkan. Jadi peran Kemlu disini lebih ke koodinir diplomasi siber kedepan. Memang BSSN sifatnya lebih keamanan kedalam aja.... dalam koordinasi Kementerian kita sepakati bahwa BSSN ini khusus penangan siber di dalam negeri, di domestik, termasuk juga kerjasama peningkatan kapasitas dengan negara lain,. Tapi untuk diplomasi siber memang Kemlu masih menjadi ujung tombak. Kenapa? Karna kebetulan dalam forum-forum internasional itu tidak dibahas mengenai teknis, tapi dibahasnya adalah politis. Misalkan hukum internasional berlaku di bidang siber, bagaimana state behaviour di ruang siber. Artinya apakah pertanyaan itu bisa dijawab oleh BSSN? Kan tidak. Itu kan karna sifatnya politis bukan teknis." (Wawancara dengan Harditya Suryawanto, Kemenlu, 2019).*

Konsep *Confidence Building Measures*

Pawlak (2016) menyebutkan bahwa *Confidence-Building Measures* (CBM) merupakan salah satu strategi dalam diplomasi yang bertujuan untuk mencegah atau mengurangi risiko konflik dengan mengurangi atau menghilangkan penyebab ketidakpercayaan (*mistrust*), kesalahpahaman (*misunderstanding*) dan salah perhitungan (*miscalculation*) di antara negara-negara yang berkonflik. Dasar-dasar pengembangan konsep CBM ini dapat ditelusuri pada *The 1975 Helsinki Final Act*, *The 1986 Stockholm Document on Confidence- and Security-Building Measures and Disarmament in Europe*, dan *The 1990 Vienna Document* (Pawlak, 2016:3).

CBM di sini dapat digunakan dalam diplomasi siber untuk menghindari potensi kesalahpahaman dan eskalasi konflik ketika hubungan antara negara-negara yang berkaitan dengan keamanan siber/ ICT memburuk (Stauffacher dan Kavanagh, 2013:3). Dalam kasus agresi siber, CBM dapat berfungsi sebagai katup tekanan yang memungkinkan

pelepasan ketegangan yang aman sebelum konflik meningkat baik yang dilakukan secara bilateral maupun multilateral (Meer, 2015:202). Stauffacher dan Kavanagh (2013) menyebutkan ada dua model CBM yaitu *military* CBM dan *non-military* CBM. Tulisan ini lebih menitikberatkan pada penerapan model CBM di bidang militer. Dalam hal ini, merujuk pada konsep dari Stauffacher dan Kavanagh (2013), *Military* CBM terdiri dari tiga kategori, yaitu (1). Pertukaran informasi dan komunikasi yang bertujuan untuk meningkatkan saling pengertian (*mutual understanding*) tentang kapabilitas militer nasional; (2). Transparansi dan verifikasi yang memungkinkan negara-negara memonitor fasilitas dan kegiatan militer masing-masing negara untuk memastikan tindakan militer yang tidak agresif sesuai dengan piagam PBB; (3). Pembatasan militer (*military restraint*) untuk membatasi kemampuan daya kejut militer (*offensive military attacks*).

Berdasarkan konsep yang telah dipaparkan di atas, maka dapat dilihat operasionalisasi konsep dalam CBM sebagai berikut (tabel 1).

Penerapan *Military* CBM Dalam Menjaga Ketahanan Nasional Di Ruang Siber

Penerapan strategi dalam menghadapi polarisasi siber global sangat penting dilakukan dimana kesatuan pemahaman dengan pihak lain, perlu dijalin sebagai amunisi dalam menghadapi pengaruh dari para pemain-pemain besar dunia di dalam konsteks siber global. Isu internasional mengenai *norms and behavior on cyberspace*, *confidence building measure*, *ICT posture, cyber-related issue* dan *cyber capacity building* merupakan isu-isu penting yang sering menjadi kajian baik dalam format kerjasama bilateral, regional maupun multilateral (bssn.go.id).

Dalam rangka membangun ketahanan nasional, pemerintah Indonesia perlu melakukan berbagai upaya dengan tidak hanya terbatas pada penggunaan media sosial, tetapi bagaimana berbagai kebijakan dapat diambil terkait dengan seluruh aktivitas

Tabel 1
Operasionalisasi Konsep

Konsep CBM	Dimensi	Indikator Pengukuran
Bidang Militer	Pertukaran Informasi dan komunikasi	- Pertukaran informasi secara bilateral, plurilateral dan multilateral mengenai strategi, doktrin militer, budaya organisasi CERT maupun tentang *Intelligence malware.*
		- Saluran komunikasi melalui *hotline*.
		- *Global public consultations*
	Transparansi dan Verifikasi	- Laporan tingkat *compliance* dari satu perjanjian di bidang teknologi siber
		- *Joint exercise and joint investigative* di bidang siber
		- monitoring dari pihak ketiga apabila terjadi konflik
		- *Joint working groups* tentang doktrin maupun perkembangan teknologi siber
	Pembatasan Militer	- *International treaties and norms* tentang keamanan siber
		- Pembatasan terhadap penggunaan sistem tertentu yang dapat menjadi target seperti instalasi internet untuk kepentingan sipil maupun infrastruktur penting lainnya.

Sumber: Diolah dari Stauffacher dan Kavanagh (2013).

yang dilakukan pada dunia maya demi kemaslahatan rakyat Indonesia. Dalam penyusunan sebuah strategi, termasuk untuk menjaga ketahanan nasional, ada tiga unsur pokok yang perlu diperhatikan yaitu *means, ways*, dan *ends* (Lykke, 1998). *Mean,* adalah segala sumber daya dan upaya yang dilakukan oleh seluruh elemen nasional. *Means* dalam aspek ketahanan nasional meliputi aspek militer maupun non militer seperti politik, ekonomi, sosial dan budaya. *Ways*, artinya cara yang dilakukan untuk mencapai suatu tujuan. Dalam konteks ketahanan nasional di sini *ways* yang digunakan yaitu melalui penerapan konsep CBM. Sedangkan *Ends* berisi tentang tujuan, dalam hal ini adalah menjaga kedaulatan siber Indonesia.

Penerapan konsep CBM dalam upaya membangun ketahanan nasional Indonesia di ruang siber khususnya di bidang militer dapat dilakukan melalui pertukaran informasi dan komunikasi, transparansi dan verifikasi, serta pembatasan militer.

Pertama, pertukaran informasi dan komunikasi. Penerapan *military CBM* dalam aspek pertukaran informasi dan komunikasi di bidang siber dibagi ke dalam tiga kategori yaitu pertukaran informasi dalam ukuran bilateral, plurilateral dan multilateral; saluran komunikasi di bidang siber; dan *global public consultation* di bidang siber.

(1). Pertukaran informasi. Dalam aspek pertukaran informasi, Indonesia telah menandatangani MoU dengan Australia pada 31 Agustus 2018. Dalam MoU tersebut, telah diatur dalam Paragraf 2 Bidang Kerjasama di mana kedua belah pihak akan berbagi informasi mengenai hukum, peraturan perundang-undangan, strategi siber nasional dan kebijakan, serta prosedur manajemen penanganan insiden siber. Hal ini dipertegas dalam wawancara dengan narasumber Kementerian Luar Negeri yaitu:

> *"Kalau pertukaran informasi kita sudah ada. Jadi.. ee.. saya jujur lupa jumlahnya, tapi kita sudah ada forum konsultasi billateral terkait isu siber. Kalau tidak salah itu dengan Australia, dengan Inggris, terus yang lainnya saya lupa. Tapi sepanjang yang saya tau sudah ada beberapa". (Wawancara dengan Harditya Suryawanto, Kemenlu, 2019).*

Pertukaran informasi di bidang siber mengenai strategi, doktrin militer, budaya organisasi CERT maupun tentang *Intelligence malware* masih bersifat sangat terbatas dikarenakan bahwa setiap negara tidak mungkin mengungkapkan sejauh mana kapabilitas militer di dunia siber dalam menghadapi berbagai ancaman maupun serangan siber. Hal ini ditujukan untuk menjaga kedaulatan siber dari negara yang bersangkutan. Demikian juga dengan Indonesia bahwa Indonesia tidak bisa serta merta mengungkapkan kapabilitas militer di bidang siber ke negara lain. Hal ini dipertegas dalam wawancara dengan BSSN yang menyebutkan bahwa:

> *"Jadi ketika serangan terjadi bisa dideteksi nih oh serangan tipe C, berarti negara mana yang mampu. Nah, kita bisa tau serangan-seranagn siber seperti itu. Tetapi, setiap negara kan ada melakukan tindak sesuatu hal yang tidak, hal yang disebut sebagai kedaulatan. Nah, tidak serta merta kita mengungkapkan seluruh kemampuan kita kan. Masih ada batas-batas rahasia, oh ini rahasia negara, tidak boleh sama sekali dibaca oleh negara lain. Nah, posisi Indonesia sekarang masih di situ. Belum mengungkapkan kemampuan siber yang dimiliki Indonesia. Artinya Indonesia pun tergolong ke dalam negara swing state bersama India dan Brazil." (Wawancara dengan Willy Ginanjar, BSSN, 2019).*

Oleh sebab itu, di lingkup nasional, Pemerintah Indonesia bekerja sama dengan sektor privat membuat forum yaitu Indonesia (*Information Sharing and Analysis Center*) sebagai forum berbagi informasi tentang isu, ancaman, kerawanan, risiko, *counter measure cybersecurity* di sektor TIK, yang berbasis *voluntary* dan beranggotakan sektor publik dan privat. Forum ini beranggotakan PT Telkom, PT Telekomunikasi Seluler, PT Indosat, PT XL Axiata, PT Smart Telecom, PT Xynexis International, APJII, PwC, KPMG, PT Aplikanusa Lintasarta, PANDI, PT Data Sinergitama Jaya (Elitery), dan PT Sampoerna Telematika (https://kominfo.go.id).

(2). Saluran komunikasi. Salah satu saranan pertukaran informasi dan komunikasi yang dilakukan oleh Pemerintah Indonesia dengan negara lain adalah melalui *hub* atau forum pertemuan rutin. Hal ini dapat dilihat dari hasil wawancara pada 24 Juni 2019 dengan narasumber Kementerian Komunikasi dan Informatika yang sekaligus juga merupakan Akademisi dari CfDS UGM yang menyebutkan bahwa di level internasional ITU merupakan *hub* dalam membahas isu mengenai siber. Sementara di level regional, Indonesia telah melakukan upaya-upaya negosiasi di kawasan melalui ASEAN dalam forum TELMIN (*Telecomunication Ministrial Meeting*). Forum tersebut sebelumnya hanya membahas mengenai isu-isu di bidang telekomunikasi. Oleh sebab itu, Indonesia kemudian menginisiasikan untuk mengubah forum ini menjadi ADMIN (*ASEAN Digital Ministerial Meeting*) yang dikhususkan membahas mengenai isu digital dan isu siber. Perubahan forum ini direncanakan akan diumumkan secara resmi pada bulan Oktober 2019.

"Kalau hub ya forum aja, pertemuan gitu ya secara rutin. Kalau di level internasional itu ITU itu hub-nya untuk ngomongin siber. Kalau di level regional nah ini Indonesia i think we have done a quite big movement in term of the negosiation di kawasan. Sekitar dua bulan yang lalu.. ee ada, jadi Menteri-menteri telekomunikasi di ASEAN itu punya forum. Nah forum itu namanya TELMIN, TELMIN itu (Telecomunication Ministrial Meeting). Dibawahnya ada TELSOM (Telecomunication Senior Official Meeting) jadi level Menteri, level senior official itu kayak level direktur, level eselon 3, eselon 2. Ada TELMIN, ada TELSOM. Kemudian turunannya ada apa namanya POKJA (Kelompok Kerja). Nah kalau di level ASEAN itu pembicaranya begitu, TELMIN. Nah kemarin yang terakhir ada minestrial retreat di Phuket. Kebetulan pak Menteri gak bisa datang, kemudian saya sama pak Samy mewakili beliau di Phuket. Di Phuket kita bicarakan dengan menteri-menteri lain di ASEAN. Kita sepakat untuk menggeser isu telekomunikasi menjadi isu digital, isu telekomunikasi itu sudah terlalu jadul. Tidak bisa meng-address isu-isu digital. Maka kalau dari sisi Kominfo kita sangat mendorong ayolah pertemuan antar menteri. Tadi yang kalau Bu Retno mungkin istilahnya hotline atau apa. Mungkin Pak Menteri juga punya group sih, saya gak tahu, group WA atau apa. Tetapi pertemuan itu ayo mulai kita transformasikan supaya lebih menjawab kebutuhan zaman. Nah transformasi itu diawali dengan sesuatu yang sangat sederhana. Nama pertemuannya. Jadi di Phuket kemarin kamu sepakati nama pertemuannya setelah puluhan tahun menggunakan istilah TELMIN, kita ganti walaupun officialy baru akan di-announce bulan Oktober besok. Kita ganti menjadi ADMIN. ADMIN apa? Dari telecommunication diubah menjadi ADMIN (ASEAN Digital Ministerial Meeting). Jadi kita sudah sedikit. Bukan sedikit ya, itu menurut saya satu lompatan yang luar biasa setelah sekian puluh tahun kita hidup dalam negosiasi yang namanya TELMIN sekarang kita punya ADMIN. Jadi

isunya semua digeser ke isu digital dan isu siber." (Wawancara dengan Dedy Permadi, Kemenkominfo, 2019).

Pada dasarnya pertukaran informasi dan komunikasi dalam format kerjasama bilateral yang telah dilakukan pemerintah Indonesia dengan sejumlah negara misalnya dilakukan dengan Amerika Serikat melalui penandatanganan Pernyataan Kehendak oleh kedua belah pihak pada 28 September 2018. Sementara kerangka kerjasama dalam bentuk Memorandum Saling Pengertian dilakukan dengan Australia dan Kerajaan Inggris Raya.

Komunikasi yang dilakukan oleh Indonesia dengan Kerajaan Inggris Raya sesuai dengan MoU yang telah ditandatangani pada 14 Agustus 2018, yaitu melalui dialog keamanan siber di mana perwakilan dari Indonesia didelegasikan kepada Badan Siber dan Sandi Negara (BSSN). Sementara penandatangan MoU antara Indonesia dengan Australia merupakan tindak lanjut dari komitmen dalam Pernyataan Bersama pada *Cyber Policy Dialogue* 2018. Kerjasama ini dibentuk untuk mencegah adanya kesalah pahaman yang sebelumnya pernah terjadi terkait isu penyadapan yang dilakukan oleh Australia melalui Gedung Perwakilan Diplomatiknya di Jakarta pada 31 Oktober 2013. MoU yang ditandatangani oleh Indonesia dan Australia pada 31 Agustus 2018 salah satunya juga membahas dialog kebijakan siber, sehingga menjadi forum pertukaran pandangan dan peninjauan terhadap isu-isu keamanan siber maupun terkait kerjasama antara dua belah pihak.

(3). *Global public consultation.* Di samping pertukaran informasi secara bilateral, Indonesia juga telah melaksanakan *global public consultation* di mana Indonesia telah mengadakan kegiatan *Policy Planning Consultation* (PPC) ke Jenewa, pada 26 Februari - 2 Maret 2017. Dalam hal ini, Institusi-institusi yang menjadi mitra PPC adalah (1). ITU, (2). ICT4D-UNCTAD, (3). UNIDIR, serta *think-tank* lainnya yang memiliki rekam jejak dalam memberikan edukasi dan mendukung perundingan-perundingan norma-norma siber internasional, yaitu *Diplo Foundation, Geneva Center of Security Policy* dan *Graduate Institute of Geneva*. Kegiatan lain yang diikuti oleh Indonesia adalah Partisipasi pada *5th Annual Cyber Intelligence Asia*, Kuala Lumpur, 14 - 17 Maret 2017. Konferensi tersebut bertujuan untuk membahas mengenai tantangan dan ancaman yang dihadapi dalam hal keamanan sistem komputer, utamanya dalam sektor pemerintahan. Konferensi ini juga mendiskusikan mengenai kebijakan dan strategi nasional beberapa negara di Asia-Pasifik mengenai keamanan siber (*cybersecurity*). Beberapa hal yang mengemuka pada pembahasan adalah mengenai kondisi keamanan siber di Malaysia, kerja sama keamanan siber Malaysia di kawasan, strategi dan kebijakan keamanan siber di Filipina, kondisi keamanan siber di Thailand, kondisi kemanan siber di Taiwan, serta kondisi keamana siber di Indonesia (Kemenlu, 2018).

Sementara untuk forum konsultasi global dalam ukuran plurilateral dan multilateral, Indonesia mengikuti *Open-Ended Working Group (OEWG) on International Information Security,* yang keanggotaannya terdiri dari seluruh anggota PBB dan *Group of Govermental Expert* (GGE)/ (UN GGE) *of International Information Security* yang anggotanya hanya 25 negara saja (Wawancara dengan Kemenlu, 2019).

Kedua, transparansi dan verifikasi. Dalam rangka membangun pertahanan siber melalui penerapan *Military CBM* dapat dilihat

dari tingkat *compliance* sebuah negara dalam perjanjian di bidang siber maupun melalui *joint excercise* yang dilakukan dengan negara lain.

(1). Laporan tingkat *compliance* dalam perjanjian di bidang siber. Tingkat *compliance* yang dilakukan oleh Indonesia dalam berbagai forum regional maupun global masih bersifat terbatas. Misalnya di tingkat ASEAN, akan memiliki tingkat *compliance* yang berbeda dengan tingkat global. Di ASEAN bahkan belum memiliki *guide line* yang jelas dalam menyikapi adanya agresi di bidang siber. Hal ini dapat dilihat dari pernyataan yang disampaikan dari narasumber BSSN, yaitu:

> *"Untuk sementara di ASEAN sendiri kesepakatan adopsi UN GGE 2015 dalam 11 norma ini masih dalam level 'oke kita sepakat', tapi belum ada sanksi yang secara nyata disepakati juga. Karena dari 2015 itu hanya menyatakan oke kita sepakat adopsi 2015 UN GGE tetapi secara praktis belum ada istilahnya kayak guidelin- nya, belum ada do and don't-nya kan itu masih belum ada. Dan sanksi-sanksi pun dulu sudah pernah dibahas tuh masalah istilahnya suatu negara enggan memberikan atau pun melangggar salah satu artikel sanksinya akan seperti apa belum ada kesepakatan karena istilahnya ASEAN sendiri kan sifatnya asosiasi yang tidak seperti Uni Eropa yang istilahnya bisa menjadi institusional. Karena ASEAN non-interfensi, sehingga tidak semerta-merta mislanya contoh Singapura memberikan sanksi kepada Indonesia, kira-kira seperti itu. Tapi kalau Uni Eropa ada keterikatan oh Uni Eropa bisa memberikan sanksi kepada let's say Italia karena tidak patuh terhadap satu peraturan itu bisa. Kalau kita kan nggak bisa." (Wawancara dengan Willy Ginanajar, BSSN, 2019).*

Di level internasional, meskipun Indonesia mengikuti forum *UN GGE* karena sifatnya hanya sebatas forum dan bukan perjanjian internasional, maka tidak bersifat mengikat. Hal ini disebutkan oleh narasumber dari Kementerian Luar Negeri, yaitu:

> *"**UN GGE** itu kan bukan perjanjian, masih forum saja. Jadi tidak ada perjanjian yang mengikat" (Wawancara dengan Harditya Suryawanto, Kemenlu, 2019).*

(2). *Joint Exercise* di bidang siber. Indonesia telah melaksanakan proses transparansi dan verifikasi dalam bidang siber di antaranya melalui pelaksanaan *joint exercise* yang diselenggarakan oleh BSSN dengan 10 negara ASEAN dan Jepang yaitu dalam kegiatan *Cyber Exercise* yang dilaksanakan secara online secara serentak (bssn.go.id). Pada tahun 2013, Indonesia mendirikan Pusat Operasi Pertahanan Siber (*Cyber Defence Operations Centre*), dan *NEC Corporation* Jepang baru-baru ini sepakat untuk mendirikan Pusat Operasi Keamanan (*Security Operations Centre*) untuk melatih para pejabat Indonesia dan memerangi ancaman siber nasional. Sementara dengan China, Indonesia juga merencanakan akan melakukan latihan simulasi perang siber bersama dengan negara tersebut (ASPI, 2016:41).

Hal ini dipertegas pula dalam hasil wawancara pada 25 Juni 2019 yang telah dilakukan dengan narasumber dari BSSN yang menyebutkan:

> *"BSSN tegakkan juga sudah kita lakukan joint-exercise sama Jepang, sama China untuk menanggulangi simulasi mengenai serangan-serangan siber seperti itu kemudian forensik yang sedang kita galakkan, tapi masih dalam pembangunan-pembanguann apa sih namanya, membuat building concept-nya dulu, konsepnya seperti apa sih di BSSN ini. Bekerja sama dengan Polri kemudian cyberterrorism dan BNPT ini area cooperation kita lakukan ketika kerja sama dengan negara-negara mitra dalam bentuk MOU dan LOA"(Wawancara dengan Willy Ginanjar, BSSN, 2019).*

Sementara di forum multilateral sendiri Indonesia juga telah ikut terlibat dalam kerjasama misalnya di Asia-Pasifik melalui APCERT, ITU-IMPACT, FIRST, OIC-CERT dan ASEAN, dan memprakarsai serta menjadi tuan rumah dalam Kompetisi Keamanan Siber ASEAN (*ASEAN Cyber Security Competition*) pertama pada November 2015 (ASPI, 2016:40).

(3). Monitoring dari pihak ketiga. Pelaksanaan monitoring di ruang siber sangat sulit dilakukan mengingat bahwa instrumen yang digunakan dalam dunia maya tidak berwujud, seperti perangkat lunak yang mudah disembunyikan karena adanya komponen alogaritma matematika yang sulit dikenali. Meskipun monitoring ini bisa diterapkan dengan menggunakan perangkat lunak pun, negara-negara di dunia internasional tidak akan mau perangkat komputernya dipindai karena beragamnya dan banyaknya data yang disimpan oleh negara baik yang bersifat rahasia maupun tidak (Ziolkowski, 2013:8-9). Oleh sebab itu, di Indonesia sendiri juga belum diterapkan kegiatan monitoring di ruang siber untuk menjaga kedaulatan siber Indonesia.

(4). *Joint working groups*. Indonesia ikut dalam kegiatan *joint working group* pada KTT ASEAN ke-32 dalam rangka membina kerja sama keamanan siber yang lebih besar di kawasan dan pembangunan kapasitas, termasuk penegakan hukum, pelatihan tentang keamanan siber dan kejahatan dunia maya melalui Pertemuan Tingkat Menteri ASEAN tentang Kejahatan Transnasional (AMMTC - *ASEAN Ministerial Meeting on Transnational Crime*), TELMIN, AMCC, *ASEAN Cyber Capacity Progr*amme, *ASEAN Regional Forum* (ARF) maupun ADMM-Plus Experts' *Working Group Meeting on Cyber Security* (http://setnas-asean.id).

Ketiga, pembatasan militer. Pembatasan militer dalam penerapan *military CBM* dapat dikaji dari keberadaan norma internasional tentang ruang siber maupun pembatasan terhadap sistem tertentu yang dapat menjadi target serangan siber dari pihak lain.

(1). Norma internasional tentang ruang siber. Salah satu norma internasional yang membahas mengenai permasalahan-permasalahan di ruang siber terdapat dalam forum PBB yaitu *United Nations UN Group of Governmental Experts* (UN GGE). Pembentukan UN GGE pada akhir tahun 1990-an ini ditujukan untuk mengkaji tentang *Developments in the Field of Information and Telecommunications in the Context of International Security*. Pada tahun 2009 atas inisiatif dari *NATO Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE) di Talinn, Estonia dibentuk sebuah norma yang mengatur tentang perang siber yaitu Tallinn Manual. Di dalam Talinn Manual ini diatur mengenai pembatasan dalam operasi siber yang memberlakukan prinsip-prinsip hukum internasional seperti *jus ad bellum* dan *jus in bello* (Henriksen, 2019:3).

Hal ini sesuai dengan hasil wawancara dengan narasumber dari Kementerian Luar Negeri yang menyebutkan bahwa:

> *"...Kalau tidak salah sejak tahun.. sejak di.. di.. apa.. sejak PBB membentuk ee UN GGE (United Nation Group of Governmental Experts on International Information Security (IIS)) nah makanya isu siber makin terus menjadi perhatian masyarakat internasional. Fokus utama dari diplomasi siber yang ada di dunia internasional memang saat ini lebih mengarah, mengatur tanggung jawab negara dan perilaku negara dalam ruang siber. Termasuk salah satunya isu yang menonjol adalah.. ee bagaimana hukum internasional dapat diberlakukan di ruang siber." (Wawancara dengan Harditya Suryawanto, Kemenlu, 2019).*

Norma internasional sebagai salah satu cara dalam membatasi aktivitas dunia maya/ siber diperlukan untuk menghindari berbagai ancaman serangan siber yang ditujukan pada suatu negara. Dunia siber sendiri merupakan salah satu komponen kebijakan luar negeri sebuah negara yang sekarang ikut diperhitungkan selain ranah darat, laut maupun udara. Namun demikian, forum-forum internasional seperti UN GGE hingga saat ini masih memperdebatkan hukum internasional terhadap pelaku serangan *cyber*, aturan perilaku yang dapat diterima di dunia virtual atau penghormatan hak asasi manusia di dunia maya (Chotimah, 2015:118).

Pada dasarnya perjanjian internasional pertama yang menangani permasalahan kejahatan siber adalah Dewan Konvensi Eropa tentang Kejahatan Dunia Maya (*Council of Europe's Convention on Cybercrime*), yang ditandatangani pada 23 November 2001. Perjanjian ini dirancang untuk menangani beberapa kategori kejahatan yang dilakukan melalui internet dan jaringan komputer. Sudah ada 29 negara yang telah meratifikasi perjanjian tersebut, meskipun Rusia dan Inggris belum meratifikasinya. Meskipun telah ada perjanjian internasional dalam menangani kejahatan siber namaun sistem internasional tetap perlu mengembangkan konsep tentang apa yang dimaksud dengan perdamaian dunia maya dan kode perilaku di dunia maya. Dalam ranah militer, para diplomat perlu membingkai ide-ide tentang pencegahan, kontrol senjata, dan bagaimana membangunan kepercayaan di dunia maya. Dengan demikian perlu semacam *hotline cyber* untuk memungkinkan komunikasi cepat antara spesialis teknologi informasi dan komunikasi (TIK) dalam kasus-kasus yang diduga serangan siber oleh satu negara di negara lain (Gady dan Austin, 2010:2).

Sejak tahun 2011 terbentuk norma internasional yaitu *International Multilateral Partnership Againts Cyber Threats* (IMPACT), pertama kalinya sebuah kerjasama multilateral yang terbentuk antara swasta dan publik untuk menghadapi ancaman siber. Wadah Internasional tersebut bermarkas di Cyberjaya, Malaysia yang mana IMPACT ini menjalin kerjasama pula dengan ITU (Kittichaisaree, 2017:4). Di Asia Tenggara juga telah terbentuk norma yang sama, ASEAN sebagai wadah organisasi regional telah menjadi wadah dalam masalah-masalah keamanan siber di kawasan. Negara-negara anggota ASEAN sudah memiliki *Computer Emergency Response Teams* (CERTs) untuk menghadapi ancaman siber (Kittichaisaree, 2017:7).

Dalam konteks kedaulatan siber di Indonesia, Indonesia belum menandatangani hukum internasional yang membatasi tindakan negara di ruang siber. Hal ini sesuai dengan hasil wawancara dengan narasumber dari narasumber dari Kementerian Luar Negeri yang menyebutkan:

> *"Sebenarnya, apakah sudah ada perjanjian siber? Selama ini cuma ada satu di Budapest Convention yang perjanjian mengenai siber. Walaupun memang anggotanya masih terbatas, sebatas negara-negara Eropa dan juga Amerika kalau tidak salah, Jepang, Korea, dan Australia, di luar Eropa ya. Sementara kita, Indonesia belum menjadi pihak atau anggota di Konvensi Budapest.....Jadi termasuk juga dalam pembahasan keamanan siber, karna kita tidak mau norma keamanan siber di dunia internasional itu dilakukan hanya demi kepentingan negara-negara maju tapi juga harus mencerminkan kepentingan negara berkembang. Makanya salah satunya Budapest Convention banyak negara berkembang tidak ikut karna penyusunannya diinisiasi negara maju. Makanya kita mau pendekatannya lain kita*

> *ingin agar konvensi internasionl, norma internastional terkait keamanan siber ini juga harus mencerminkan kepentingan negara berkembang." (Wawancara dengan Harditya Suryawanto, Kemenlu, 2019).*

Indonesia hanya berupaya melindungi seluruh rakyat dalam setiap kegiatan yang berhubungan dengan internet melalui Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) menjelaskan apabila telah berkembang rezim hukum baru dengan nama hukum siber terkait pemanfaatan teknologi informasi dan komunikasi. Dalam UU ITE ini, mengatur berbagai macam aktivitas yang menggunakan media internet / siber baik dalam arti positif maupun pelanggaran. Selain UU ITE, terdapat pula ketentuan KUH Pidana dan KUH Perdata yang dapat memberikan hukuman kepada setiap orang maupun institusi yang merugikan pihak lain, meskipun tidak dalam kehidupan nyata melainkan menggunakan media internet (Ersya, 2017).

> *"Sebenarnya ini koordinasi kita dengan pihak terkait dari sisi Kominfo dan juga BSSN sudah berupaya untuk menangkal adanya hoax atau proganda, atau negatif campaign yang dilakukan. Kominfo sendiri sudah mempunyai aturannya, aturan nasionalnya. Sementara kita secara koordinasi berusaha untuk juga melakukan deteksi dini, lalu juga konter narasi juga kalau ada propaganda atau hoax ya." (Wawancara dengan Harditya Suryawanto, Kemenlu, 2019).*

(2). Pembatasan terhadap sistem yang menjadi target serangan siber. Pembatasan militer dalam bidang siber dapat ditemukan di sejumlah negara. Misalnya di Amerika Serikat, yaitu melarang prajurit menggunakan *Black Berry Messanger*. Sementara di Israel ada pelarangan penggunaan media sosial terhadap prajurit. Untuk Indonesia sendiri, pembatasan militer di bidang siber salah satunya dilakukan dalam penggunaan media sosial oleh TNI/ TNI AU yaitu prajurit dilarang memberikan komentar dalam media sosial terhadap situasi dan kondisi ideologi, politik, ekonomi, sosial dan budaya (ipoleksosbud) serta militer dan pertahanan (milhan) yang justru dapat membawa kerugian dan merusak citra institusi TNI/TNI AU (bbc.com).

Dalam Talinn Manual Chapter V disebutkan bahwa ketika terjadi konflik bersenjata, selain perlindungan umum terhadap warga sipil, ketentuan khusus juga mengatur tentang perlindungan terhadap kelas, objek, dan aktivitas tertentu. Sebagai contohnya, misalnya, pihak-pihak yang berkonflik dapat membuat perjanjian khusus yang memberikan perlindungan lebih besar untuk komputer dan jaringan komputer yang mendukung operasi pekerjaan dan instalasi yang mengandung kekuatan berbahaya yang diatur dalam *Rule 80* dengan menyetujui larangan mutlak serangan terhadap obyek tersebut, baik dengan cara siber maupun kinetik. Demikian pula, persetujuan khusus dapat disimpulkan untuk melindungi komputer dan jaringan komputer yang mendukung fasilitas sensitif yang tidak dibahas oleh Peraturan Perang, seperti instalasi produksi minyak, platform pengeboran minyak, fasilitas penyimpanan minyak bumi, kilang minyak, atau fasilitas produksi bahan kimia (Schmitt, 2013:166).

SIMPULAN

Berdasarkan analisis yang telah dilakukan maka dapat ditarik kesimpulan, sebagai berikut.

Pertama, terdapat tiga jenis upaya dalam penerapan *military confidence building measures* Indonesia di ruang siber yaitu

pertukaran informasi dan komunikasi, transparansi dan verifikasi, serta pembatasan militer di ruang siber.

Kedua, pertukaran informasi dan komunikasi di bidang siber dilakukan melalui *hub* atau forum pertemuan rutin baik yang bersifat regional ASEAN yaitu melalui TELMIN dan ADMIN maupun secara internasional melalui ITU. Di samping itu, Indonesia juga melakukan *global public consultation* dalam rangka membahas tantangan, ancaman dan strategi kebijakan di bidang keamanan siber.

Ketiga, dari aspek transparansi dan verifikasi di ruang siber, Indonesia telah melakukan *cyber exercise* bersama dengan negara ASEAN dan menjalin kerjasama di bidang siber di forum-forum multilateral. Indonesia juga bekerja sama dengan Jepang untuk mendirikan Pusat Operasi Keamanan sebagai pusat pelatihan dalam menghadapi ancaman siber. Selain itu, bersama dengan China, Indonesia juga merencanakan adanya simulasi perang siber.

Keempat, dari aspek pembatasan militer di ruang siber, Indonesia ikut serta dalam UN GGE yang merupakan salah satu forum internasional dalam kerangka siber yang kemudian menghasilkan salah satu norma internasional yaitu Talinn Manual. Pemerintah Indonesia sendiri telah mengeluarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE) untuk mengatur berbagai tindakan dan perilaku di ruang siber. Indonesia juga membatasi penggunaan media sosial khususnya oleh TNI/TNI AU yaitu tentang pelarangan memberikan komentar dalam media sosial terhadap situasi dan kondisi ideologi, politik, ekonomi, sosial dan budaya (ipoleksosbud) serta militer dan pertahanan (milhan) yang justru dapat membawa kerugian dan merusak citra institusi TNI/TNI AU.

Kelima, penerapan *military CBM* di ranah siber di Indonesia masih terbatas mengingat bahwa tidak semua informasi bisa di-*share* dengan negara lain. Adanya arus *big data* yang sangat cepat menjadi salah satu ancaman bagi kedaulatan siber di Indonesia. Dari tiga aspek penerapan *military CBM* di Indonesia masih belum mengaplikasikan transparansi dan veriifikasi pada tingkat *compliance* terhadap pemberlakuan norma internasional di bidang siber. Hal ini dikarenakan satu-satunya perjanjian internasional di bidang siber yaitu Konvensi Budapes bukan merupakan forum yang dapat diikuti oleh Indonesia mengingat Konvensi tersebut dibuat oleh negara-negara maju dan merepresentasikan kepentingan negara maju. Di tingkat regional ASEAN, tingkat *compliance* masih berada pada menyepakati terhadap 11 norma dalam UN GGE saja dan Indonesia juga belum menandatangani ataupun meratifikasinya.

DAFTAR PUSTAKA

ASPI. (2016). *Cyber Maturity in the Asia-Pasific Region 2016.* Australia: Australian Strategic Policy Institute (ASPI).

Berg, B.L. dan Lune, H. (2017). *Qualitative Research methods for The Social Sciences,ninth edition.* England, Essex: Pearson Education Limited.

Borghard, E. D. Dan Lonergan, S. W. (2018). Confidence Building Measures for the Cyber Domain. *Strategic Studies Quarterly,* Fall, 10-49.

Chotimah, Hidayat Chusnul. (2015). Membangun Pertahanan dan Keamanan Nasional dari Ancaman *Cyber* di Indonesia. *Jurnal Diplomasi*, 7 (4), 103-123.

Danuri, Muhamad dan Suharnawi. (2017). Tren Cyber Crime dan Teknologi Informasi di Indonesia. *Infokam*, No.2.

Ersya, Muhammad Prima. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education* Edisi 2017.

Fahmi, Ismail. (2018). *Analisis Jaringan Pasukan Siber di Indonesia (Kolam Hoax dan Hate Speech)*. Jakarta: ISPI (Ikatan Sarjana dan Profesi Perpolisian Indonesia).

Gady, Franz-Stefan dan Austin, Greg. (2010). *Russia, The United States, And Cyber Diplomacy Opening the Doors*. New York: EastWest Institute.

Henriksen, Anders. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, 2019, 1–9.

Indrawan, Jerry. (2019). Cyberpolitics sebagai Perspektif Baru Memahami Politik di Era Siber. *Politica***,** 10 (1), 1-15.

Jafar, TF, Sudirman, A dan Rifawan, A. (2019). Ketahanan Nasional Menghadapi Ancaman *Lone Wolf Terrorism* Di Jawa Barat. *Jurnal Ketahanan Nasional*, 25 (1), 73-91.

Kementerian Luar Negeri Republik Indonesia. (2018). LAKIP Kemenlu.

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

Lykke Jr., Arthur F. (1998). *Military Strategy: Theory and Application*. Carlisle, PA: U.S. Army War College.

Meer, Sico van der. (2015). Enhancing International Cyber Security: A Key Role for Diplomacy. *Security and Human Rights*, 26, 193-205.

Paterson, Thomas. (2019). Indonesian cyberspace expansion: a double-edged sword. *Journal of Cyber Policy*, 4(2), 216-234, DOI: 10.1080/23738871.2019.1627476.

Pawlak, Patryk. (2016). Chapter 7 Confidence-Building Measures in Cyberspace: Current Debates and Trends. Dalam Anna-Maria Osula and Henry Rõigas (Eds). *International Cyber Norms: Legal, Policy & Industry Perspectives.* NATO CCD COE Publications, Tallinn.

Prasanti, D dan Fitriani, DR. (2017). Membangun Ketahanan Informasi Nasional Dalam Komunikasi Kesehatan Bagi Kalangan Perempuan Urban Di Jakarta. *Jurnal Ketahanan Nasional*, 23 (3), 338-358.

Schmitt, Michael N. (2013). *Talinn Manual on The International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Stauffacher, Daniel dan Kavanagh, Camino. (2013). Confidence Building Measures and International Cybersecurity. *Cyber Policy Process Brief,* ICT4Peace Publishing, Geneva,*http://ict4peace.org/wpcontent/uploads/2015/04/processbrief_2013_cbm_wt-71.pdf.*

Suryohadiprojo, S. (1997). Ketahanan Nasional Indonesia. *Jurnal Ketahanan Nasional*, II(1), 13-31.

Westcott, Nicholas. (2008). Digital Diplomacy: The Impact of the Internet on International Relations. *Research Report 16*, July, Oxford Internet Institute, *https://www.oii.ox.ac.uk/archive/downloads/publications/RR16.pdf.*

Data Internet:

https://bssn.go.id/asean-japan-online-cyber-exercise/, *diakses pada 26 Juni 2019.*

https://bssn.go.id/building-a-national-soft-power-on-cyber-space-through-cyber-diplomacy/, diakses pada 29 Agustus 2019.

https://teknologi.bisnis.com/read/20190306/84/896967/ancaman-siber-di-indonesia-terbanyak-kelima-se-asia-pasifik, diakses pada 28 Agustus 2019.

https://apjii.or.id/content/read/104/348/BULETIN-APJII-EDISI-22---Maret-2018, diakses pada 10 Agustus 2019.

https://www.bbc.com/indonesia/berita_indonesia/2016/03/160327_indonesia_medsos_tni, diakses pada 19 September 2019.

https://tekno.kompas.com/read/2019/05/16/03260037/apjii-jumlah-pengguna-internet-di-indonesia-tembus-171-juta-jiwa, diakses pada 28 Agustus 2019.

https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesiatertinggi-kedua-kejahatan-siber-di-dunia, diakses pada 13 Agustus 2019.

https://kominfo.go.id/content/detail/14605/ciip-id-summit-2018-tingkatkan-koordinasi-proteksi-keamanan-siber-indonesia/0/sorotan_media, diakses pada 25 Oktober 2019.

http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-coorporation.pdf. diakses pada 25 Oktober 2019.

Wawancara:

1. Willy Ginanjar, Direktorat Bidang Proteksi, BSSN.
2. Harditya Suryawanto, Direktorat Keamanan Internasional dan Perlucutan Senjata, Kemenlu.
3. Dedy Permadi, Tenaga Ahli Bidang Kebijakan Digital, Kementerian Komunikasi dan Informatika dan Direktur CfDS Universitas Gadjah Mada