ANALISIS *MINIMUM ESSENTIAL FORCE* (MEF) DALAM RANGKA PEMBANGUNAN *CYBER-DEFENSE*[1]

ANALYSIS OF MINIMUM ESSENTIAL FORCE (MEF) IN BUILDING CYBER-DEFENSE

Alex Firmansyah Rahman[2], Syaiful Anwar[3], dan Arwin DatumayaWahyudi Sumari[4]

Universitas Pertahanan Indonesia
(alexfirmansyahrahman@gmail.com, moroloawe7760@yahoo.com.au, arwin.sumari@yahoo.com)

Abstrak – Tujuan penelitian ini adalah untuk menganalisis pengakomodasian postur *Minimum Essential Forces* (MEF) terhadap pembangunan *cyber defense* di Indonesia. Permasalahan yang dihadapi adalah postur MEF yang dirumuskan oleh Kementerian Pertahanan (Kemhan) RI selama ini masih difokuskan pada upaya pemenuhan kebutuhan dan modernisasi alat utama sistem senjata (alutsista) pada konteks *Revolution in Military Affairs* (RMA) dalam organisasi Tentara Nasional Indonesia (TNI), dalam upaya pembangunan kekuatan pertahanan militer. Sementara itu, realita ancaman nir militer berupa *cyber attack* sudah sangat nyata. Penelitian ini menggunakan metode kualitatif dengan pendekatan analisis deskriptif. Hasil akhir dari studi ini menunjukkan bahwa hingga saat ini Kemhan dan Markas Besar TNI telah memberikan perhatian terhadap ancaman *cyber* berikut upaya-upaya penanggulangannya, namun masih dalam skala yang terbatas. Di sisi lain, pada postur MEF belum secara konkrit menyebutkan kandungan pembangunan kekuatan *cyber-defense,*sehingga diajukan solusi perlu adanya revisi postur MEF agar secara eksplisit mengakomodasi pembangunan *cyber defense* di Indonesia. Untuk mencapai tujuan tersebut, terdapat tiga komponen inti untuk mewujudkannya melalui RMA yaitu dengan melakukan perubahan doktrin; perubahan organisasi yang berbasis *cyber-defense;* dan pembangunan teknologi untuk mengakomodasi *cyber-defense.*

Kata kunci: *cyber attack, cyber-defense, minimum essential force, revolution in military affairs*

Abstract *-- The aim of this research is to analyse how to accomodate posture of minimum essential force into the development of cyber defence in Indonesia. The problem that this research raised is the posture of the MEF formulated by the Indonesian Ministry of Defense (MoD) has been focused to the efforts to fulfill the need and to modernize primary weaponry system in the context of*

[1] Artikel ini merupakan rangkuman dari hasil penelitian tesis, disusun oleh Alex Firmansyah Rahman, di Program Studi Strategi Perang Semesta, Fakultas Strategi Pertahanan, Universitas Pertahanan Indonesia.

[2] Alumnus Program Studi Strategi Perang Semesta *Cohort* 6 Fakultas Strategi Pertahanan Universitas Pertahanan Indonesia, Sentul, Bogor.

[3] Dosen tetap Fakultas Strategi Pertahanan, Universitas Pertahanan Indonesia, Sentul, Bogor.

[4] Analis Kebijakan Rencana Kontinjensi Ekonomi, Kedeputian Politik dan Strategi, Dewan Ketahanan Nasional Republik Indonesia, dan Dosen Tetap Program Studi Ekonomi Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan Indonesia, Sentul, Bogor.

Revolution in Military Affairs (RMA) within the Indonesian National Armed Forces, in the effort in developing military defense forces. Meanwhile, the reality of non-military threat in form of cyber attack is truly real. This reseach was done by using qualitative method with descriptive analysis approach. The final result of this study shows that up to now the MoD dan headquarters of the Indonesian National Armed Forces have given attention to cyber attack along with the efforts of its handling but it is still in limited scale. On the other side, the posture of the MEF has not concretely defined the load of cyber-defense forces development. Therefore a solution is proposed to revise the MEF posture so as to accommodate the cyber-defense development in Indonesia explicitly. In order to reach that aim, there are three core components to realize it through RMA namely, perform doctrine changing, organization changing, and technology development to accommodate cyber-defense.

Keywords: *cyber attack, cyber-defense, Minimum Essential Force, Revolution in Military Affairs*

Pendahuluan

Sebagai negara yang memiliki kondisi geografi yang luas (peringkat ke-15 dunia)[5] dan terdiri atas ribuan pulau dengan wilayah perairan yang luas dan terbuka, Indonesia sangat rawan terhadap beragam bentuk ancaman baik militer maupun nir-militer. Kondisi ini membuat Indonesia membutuhkan postur pertahanan yang kuat, sehingga membutuhkan pembangunan kekuatan pertahanan berdasarkan pada kapabilitas (*capability-based defense*).[6]

Dalam pembangunan postur pertahanan yang kuat, pemerintah Indonesia menggunakan konsep *capability-based planning*, yang dituangkan dalam program Kekuatan Pokok Minimum (*Minimum Essential Force*/MEF). Dalam Kebijakan Umum Pertahanan Negara (Jakum Hanneg) tahun 2010-2014, MEF adalah standar kekuatan pokok dan minimum TNI, yang mutlak disiapkan sebagai prasyarat utama dan mendasar bagi terlaksananya secara efektif tugas pokok dan fungsi TNI untuk menghadapi ancaman aktual.[7] Dengan demikian, MEF merupakan sebuah kebijakan yang berfokus pada pembangunan kekuatan militer.

MEF dibentuk sebagai jawaban akan kebutuhan mandala pertahanan Negara Kesatuan Republik Indonesia (NKRI) yang dihadapkan kepada anggaran pertahanan yang

[5] Lihat, "Indonesia: The World Fact Book", dalam https://www.cia.gov/library/publications/the-world-factbook/geos/id.html, diunduh pada 22 Maret 2015.

[6] Buku Putih Pertahanan Indonesia, (Jakarta: Kementerian Pertahanan, 2008), hlm. 119.

[7] Kebijakan Umum Pertahanan Negara, Peraturan Presiden Nomor 41 Tahun 2010, hlm. 8. Pengertian MEF, penerapannya, dan acuan kebijakan pertahanan secara umum masih mengacu pada Perpresini, belum ada pemutakhiran dari presiden selanjutnya hingga tesis ini disusun.

terbatas. MEF merupakan komponen utama yang mendesak untuk pembangunan sistem (*system building*) dan pembangunan kekuatan (*force building*), yang dilakukan untuk membangun kekuatan pertahanan Indonesia secara bertahap dari tahun 2010 sampai dengan 2024.[8] MEF berfokus pada terpenuhinya kekuatan pada ketiga matra dalam melakukan operasi gabungan dan mampu meningkatkan efek penggetar dengan 100 persen kesiapan alat utama sistem senjata (alutsista) pada skala minimum. Dengan kata lain, MEF diarahkan kepada pemenuhan alat-alat berat yakni peralatan perang konvensional.

Perkembangan Teknologi Informasi dan Komunikasi (TIK) di era globalisasi telah mengubah perang tradisional dengan cara-cara konvensional tidak lagi digunakan oleh sebagian besar negara di dunia. Kondisi ini melahirkan konsekuensi adanya percepatan global yang mendorong setiap negara meningkatkan perekonomiannya. Untuk menjamin keberlangsungan aktivitas ekonomi negara, persenjataan dan pertahanan juga ditingkatkan kemampuannya.[9] Hal ini membuat persaingan dan peperangan menjadi semakin kabur batas-batasnya. Persaingan ekonomi dilengkapi dengan kekuatan-kekuatan fisik yang digunakan untuk meningkatkan seluruh kapabilitas dalam menghadapi persaingan tersebut. Dengan demikian, episentrum gravitasi peperangan berada pada irisan ruang kerjasama ekonomi dan perang, yakni TIK yang menjadi pondasi dibentuknya ruang *cyber*.

Selain berubahnya paradigma dalam pertempuran yang semakin nir manusia, revolusi persenjataan juga semakin berkembang lagi ke arah pemanfaatan ruang bersama yang tidak bisa dimiliki kedaulatan negara manapun (*the global commons*), yakni ruang *cyber* sebagai medan pertempuran (*battlefield*) baru. Ruang *cyber* sebagai ruang bagi pertukaran informasi di dunia, menempatkan peperangan modern ke level yang lebih

[8] Lihat Pengantar Menteri Pertahanan dalam Penyelarasan *Minimum Essential Forces (MEF)* sebagai Komponen Utama, (Jakarta: Kementerian Pertahanan RI, 2011).

[9] Seperti yang diungkapkanoleh Adam M. Segal,"*Chinesecyber attacks are driven by the desire to collect political and military intelligence, as well as to bolster economic competitiveness*" dalam Adam M. Segal, "Cyberspace: The New Strategic Realm in US–China Relations", *Strategic Analysis Journal*, Vol.38, No.4, 2014, hlm. 577.

tinggi dan lebih elegan serta tersistematisasi dengan sangat canggih, dan yang pasti semakin tidak menimbulkan korban jiwa (*bodyless*).[10]

Penanganan ancaman serangan *cyber* di Indonesia yang masih belum optimal dalam pengembangan kapabilitas melakukan perang di ranah *cyber* (*cyberspace*), membuat *Revolution in Military Affairs* (RMA) Indonesia masih harus dipertanyakan kembali.[11] Indonesia masih melihat ancaman *cyber* (*cyberthreat*) sebagai masalah hukum dan kejahatan transnasional. Hal ini dapat dilihat dari sistem yang masih menganut ancaman *cyber* sebagai praktek kriminal semata, bukan sebagai praktik realisme-politik yang harusnya dihadapi dengan paradigma strategis yang memperhatikan aspek *means, ways,* dan *ends*. Hal ini ditegaskan Kementerian Pertahanan (Kemhan) Republik Indonesia melalui Peta Jalan Strategi Nasional Pertahanan Siber :[12]

> "b. Institusi yang secara legal formal bertindak selaku *leading sector* dalam menangani masalah keamanan *cyber* atau *cyber security* secara nasional adalah Kementerian Komunikasi dan Informatika. Namun saat ini yang ditangani adalah dalam penataan dan standarisasi kebijakan tentang keamanan informasi nasional".
>
> "e. Indonesia sudah memiliki *cyberlaw* yaitu Undang Undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun regulasi yang khusus untuk mengatur pertahanan *cyber* yang lebih spesifik dari regulasi keamanan informasi yang sudah ada, belum ada. Sebagai perbandingan di negara lain ada undang undang khusus pertahanan *cyber*."

Tindakan saling menyadap antarnegara, seperti yang dibongkar oleh Julian Assange dengan Wikileaks-nya, serta terbongkarnya aksi sadap oleh pemerintah Australia terhadap Indonesia oleh Edward Snowden (mantan staf *National Security Agency* (NSA) Amerika Serikat), menambah daftar semakin maraknya ancaman peperangan *cyber* sebagai bentuk ancaman non-konvensional. Bahkan *World Economic Forum* (WEF) menggolongkan ancaman yang berkaitan dengan *cyber-defense* sebagai tantangan global

[10] Michael Hardt dan Antonio Negri, *Multitude: War and Democracy in the Age of Empire*, (USA: The Penguin Press, 2004), hlm. 44.

[11] Kementerian Pertahanan, *Peta Jalan Strategi Nasional Pertahanan Seber*, (Jakarta: KementerianPertahanan RI, 2014), hlm. 1-2.

[12] *Ibid,* hlm. 1-10.

nomor empat terbesar setelah perubahan iklim, pengangguran, ketidakadilan, dan kemiskinan.[13]

Menurut *Akamai Technologies*, salah satu perusahaan produk TIK di Amerika Serikat, Indonesia digolongkan sebagai negara terbesar ketiga yang rawan terhadap ancaman *cyber*. Hal ini menjadi peringatan bahwa serangan *cyber* dapat terjadi sewaktu-waktu karena keberadaannya di area yang virtual dan sulit dideteksi.[14] Menteri Pertahanan Republik Indonesia Ryamizard Ryacudu menegaskan bahwa Indonesia sedang menghadapi ancaman *cyber* yang jelas dan nyata. Muhammad Salahudin, ketua *Indonesian-Security Incident Response Team on Internet Infrastructure* (ID-SIRTII), menjelaskan bahwa serangan telah berlipat ganda.[15] Sikap Indonesia terkait hal ini menjadi krusial karena serangan yang tidak dapat diprediksi dan dideteksi.

Dari kondisi tersebut, peperangan *cyber* (*cyberwarfare*) menjadi kondisi yang tidak dapat dielakkan. Sebagai contoh, serangan virus *stuxnet* ke infrastruktur nuklir Iran menandai semakin besarnya pengaruh kekuatan TIK terhadap keamanan global. Menurut Symantec (Produsen Antivirus Norton), pada 6 Agustus 2010, Indonesia menempati urutan kedua setelah Iran dari 10 negara yang terkena virus *stuxnet* tersebut.[16] Begitu pula penggunaan teknologi militer Amerika Serikat di Afghanistan dengan tujuan meminimalisir jumlah korban tentara (*casualties*) juga menandai nilai penting, efektivitas dan efisiensi dari pemanfaatan teknologi dalam peperangan.[17] Maka dengan demikian, Indonesia dapat dinyatakan masih belum siap menghadapi ancaman *cyber* yang dapat terjadi sewaktu-waktu. Perspektif pertahanan memandang persoalan *cyber* sebagai hal yang harus dikelola oleh lembaga non-pertahanan karena bersifat nir-militer. Oleh karena itu, tampak bahwa aspek pertahanan cenderung tidak digunakan untuk meghadapi ancaman *cyber* secara strategis.

---

[13] World Economic Forum, *Insight Report: Risk and Responsibility in a Hyperconnected World*, Januari 2014, hlm. 2.

[14] Lihat dalam Prashanth Prameswaran, "Indonesia's Cyber Challenge Under Jokowi", dalam http://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/, 21 Januari 2015, diunduh pada 9 Februari 2015.

[15] *Ibid.*

[16] Bagus Artiadi Soewardi, "Perlunya Membangun Sistem *Cyber-defense* yang tangguh bagi Indonesia", *Majalah Potensi Pertahanan*, Maret 2013, hlm. 34.

[17] Jeffrey Carr, *Inside Cyber Warfare, Second Edition, (*Sebastopol: O'Relly Media, 2012), hlm. 36-37.

Indonesia dituntut untuk melangkah ke ranah pengembangan kekuatan untuk menghadapi perang di mandala *cyber*. Hal ini dibutuhkan anggaran yang memadai dan kebijakan yang mendukung. Anggaran dan kebijakan pengembangan kekuatan menghadapi perang jenis ini dilakukan dengan memasukkan dimensi pertahanan *cyber* sebagai salah satu urgensi dalam MEF. Ancaman baik eksternal maupun internal, baik tradisional maupun non-tradisional, konvensional maupun non-konvensional, dan militer maupun nir-militer; dapat ditangani jika sistem komando dan kendali (siskodal) militer semakin mengandalkan aspek TIK. Meskipun alat berat masih menjadi fokus utama dalam membangun postur pertahanan yang dirumuskan dalam MEF, lingkungan strategis yang semakin gencar terhadap pemanfaatan TIK menjadi pertimbangan yang kuat bagi adanya revolusi ke arah tersebut. Oleh karenanya, memfokuskan anggaran dan pertumbuhan ekonomi kepada investasi modernisasi persenjataan merupakan hal yang sangat penting untuk Indonesia.

Rumusan Masalah

Serangan *Cyber* muncul sebagai ancaman baru terhadap pertahanan Indonesia dari aspek militer dan nir-militer. Sebagai negara yang menggunakan Sishanta untuk menghadapi pelbagai ancaman yang masuk ke dalam negeri, Indonesia menganggap serangan *cyber* bukan merupakan hal yang krusial. Hal ini ditunjukkan dengan belum adanya pembangunan *cyber-defense* yang dituangkan dalam MEF. Indonesia masih memandang serangan *cyber* sebagai permasalahan transnasional yang tidak memerlukan penyelesaian dengan paradigma strategis, padahal sudah banyak serangan *cyber* yang terjadi. Perspektif ini yang menyebabkan pembangunan *cyber-defense* masih belum diakomodasi. Berdasarkan hal tersebut, penelitian ini mengangkat permasalahan tentang MEF dalam rangka pembangunan *cyber-defense*. Permasalahan tersebut dirumuskan ke dalam 2 (dua) pertanyaan penelitian berikut:

a. Bagaimana MEF dalam pembangunan *cyber-defense*?
b. Bagaimana MEF seharusnya mengakomodasi pembangunan *cyber-defense* untuk mewujudkan *cyberwarfare-making capabilities*?

Kerangka Konseptual

Tulisan ini menggunakan kerangka konseptual untuk menjelaskan perspektif peneliti dalam melihat permasalahan. Kerangka konseptual menurut Mas'oed adalah proposisi yang diambil dari suatu konsep yang tingkatannya lebih tinggi dari sistem klasifikasi topologis,[18] yang berarti kerangka konseptual telah memberikan penjelasan keterkaitan antara variabel-variabel ataupun indikator-indikator dalam topologi.

Untuk melihat konteks penelitian ini, dengan MEF sebagai objeknya maka yang ingin dilihat adalah bagaimana posisi MEF terhadap situasi keamanan dan pertahanan yang sedang gencar oleh ancaman *cyber.* Kerangka konseptual yang dibangun adalah mengenai kemampuan suatu negara dalam membangun *smart power* dan *soft power*. Adapun menurut Joseph Nye, *smart power* adalah gabungan dari *soft power* dan *hard power* dari suatu negara, dimana *soft power* dapat dikatakan kekuatan diplomasi dan ekonomi sedangkan *hard power* adalah kekuatan militer.

Melihat *cyber-defense* sebagai salah satu bentuk *smart power* tentu bukan menyederhanakan bahwa Indonesia harus menunjukkan gelar kekuatan yang ofensif dan ekspansif baik dari sisi kekuatan diplomatik maupun koersif. Hal ini tentu harus dikembalikan pada prinsip pertahanan Indonesia yang berdasarkan politik luar negeri bebas aktif dan berdasarkan kemampuan anggaran. Namun, dengan melihat dari perspektif *smart power*, kekuatan *cyber-defense* dapat menjadi kunci dalam melihat efektivitas dan efisiensi anggaran dengan mengurangi *exposure* berlebihan pada alutsista berat. Dengan demikian dapat dipahami bahwa pendekatan *soft power* sedikit lebih dikedepankan ketimbang *hardpower*. Prinsip peperangan memenangkan hati dan pikiran (*winning the heart and mind*) terbukti efektif dan efisien di berbagai negara seperti Amerika Serikat, Eropa, dan Tiongkok, tanpa harus menurunkan pasukan massal dan persenjataan berat. Merujuk pada konsep *smart power*, MEF dapat mengusung *cyber-defense* sebagai bentuk upaya *winning the heart and mind* negara-negara (maupun non-negara) yang mengancam. Terlebih Indonesia telah mengadopsi kebijakan Poros Maritim Dunia yang mengedepankan aspek ekonomi ketimbang politik-militer.

[18] Mohtar Mas'oed, *Ilmu Hubungan Internasional: Disiplin dan Metodologi,* (Yogyakarta: LP3ES, 1990), hlm. 190-191.

Konsep *Cyber-Defense*

Cyber dalam konteks pertahanan mempunyai beberapa istilah yang saling berkaitan seperti, *cyberwarfare, cybersecurity, cyberspace, cyberpower*, dan *cyberstrategy*. Sebagaimana domainnya, istilah-istilah tersebut mengacu pada penggunaan TIK dalam fungsi pertahanan. Berikut pengertian domain *cyber* menurut Franklin D. Kramer, Stuart H. Starr, dan Larry K. Wentz : [19]

Cyberspace adalah domain global, dengan lingkungan informasi yang berbeda dan unik, dikerangkakan oleh penggunaan spektrum elektronik dan elektromagnetik untuk membuat, menjual, memodifikasi, menukar, mengeksploitasi informasi melalui jaringan interdependen dan interkoneksi menggunakan TIK. Sementara itu, *cyberpower* adalah kemampuan menggunakan *cyberspace* untuk membuat keuntungan dan pengaruh dalam segala lingkungan operasional dan melintasi segala instrumen kekuasaan. *Cyberstrategy* adalah pengembangan dan pendayagunaan dari kapabilitas strategis untuk bekerja dalam *cyberspace*, terintegrasi dan terkoordinasi dengan domain operasional yang lain, untuk mencapai atau mendukung pencapaian kekuatan nasional dalam rangka mendukung strategi keamanan nasional.[20]

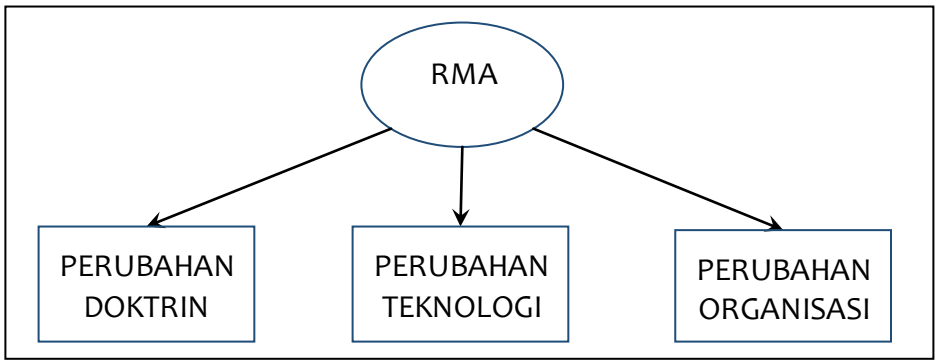
Konsep *Revolution in Military Affairs (RMA)*

RMA merupakan istilah yang pertama kali dikembangkan oleh Amerika Serikat untuk menjelaskan upaya negara tersebut untuk memodernisasi persenjataannya pasca-perang dingin. RMA secara filosofis merupakan upaya revolusionis mengubah paradigma berperang, tidak hanya dari sisi persenjataan dan teknologi pertahanan, melainkan manajerial organisasi militer berkaitan dengan pemerintah dan doktrin-doktrin atau cara-cara berperang.

[19] Franklin D. Kramer, et al., *Cyberpower and National Security*, (Washington DC: National Defense University, 2009), hlm. xvi.

[20] Scott Jasper, "Deterrence of Cyber Agression", dalam*A Comprehensive Approach to Operations in Complex Environments*, (Monterey: Naval Postgradute School, 2014), hlm. 27-29.

Gambar 1. Implementasi RMA



Sumber: diolah oleh penulis

Menurut William S. Cohen, RMA terjadi ketika militer suatu negara mendapatkan peluang untuk mentransformasikan strategi, doktrin militer, pelatihan, pendidikan, organisasi, peralatan, operasi, dan taktik untuk mencapai tujuan militer yang maksimal dalam cara-cara baru yang fundamental.[21] Untuk memungkinkan terwujudnya RMA, inovasi harus diupayakan dalam tubuh militer. Menurut Emily Goldman, inovasi terjadi dalam tiga tahap: spekulasi, eksperimentasi, dan implementasi.[22] Spekulasi adalah makalah-makalah konsep, buku-buku, jurnal, artikel, pidato, dan kajian mengenai metode berperang; membentuk kelompok belajar untuk mempelajari perang; dan melahirkan koleksi intelijen berfokus pada aktivitas inovasi asing. Indikator dari eksperimen adalah eksistensi dari organisasi; adanya organisasi eksperimental dan tempat uji coba; latihan untuk mengeksplorasi konsep peperangan; *war gaming by war colleges*, industri pertahanan, dan *think tank* mengenai area peperangan baru; dan eksperimentasi dengan metode kombat baru dalam masa peperangan. Implementasi membutuhkan strategi transformasi formal; unit baru untuk eksploitasi, merevisi doktrin dalam misi-misi baru; membuat cabang baru dan jalur karir bagi militer; mengubah kurikulum dari institusi pendidikan militer profesional; dan pelatihan untuk menyaring konsep-konsep.

[21] Peter Dombrowski dan Eugene Gohlz, *Buying Military Transformation: Technological Innovation and Defense Industry*,(New York: Columbia University Press, 2006), hlm. xi.

[22] Emily Goldman dan Thomas Mahnken,*Information Revolution in Military Affairs in Asia*, (New York: Palgrave McMillan, 2004), hlm. 17.

Konsep *Smart Power*

Joseph Nye mengajukan konsep *smart power* sebagai bentuk perilaku baru yang paling relevan dalam menghadapi sistem internasional pasca-Perang Dingin, yang didominasi oleh kerjasama ekonomi dan diplomasi.[23] Landasan liberalisme yang digunakan Nye sebagai perspektifnya dalam memandang hubungan internasional, melihat dengan perspektif perdamaian demokratik (*democratic peace*), yakni bahwa negara demokrasi tidak mungkin melawan negara demokrasi lain. Dalam hal ini, *soft power* hanya dapat dimungkinkan oleh sistem yang demokratik.[24]

Penelitian ini melanjutkan pemikiran Chong mengenai *smart power* dan menggabungkannya dengan prinsip-prinsip RMA. Menurut Chong, *smart power* dapat dibangun di negara manapun dalam konteks hubungan sipil-militer (*Civil-Military Relations*).[25] Perubahan revolusionis organisasi, teknologi, dan doktrin militer; dapat diselaraskan dengan menggunakan kerjasama antara sipil dan militer. Hal ini tidak sekedar mengaplikasikan adagium *King* Frederick *The Great*, bahwa diplomasi tanpa persenjataan sama halnya seperti musik tanpa instrumen (*diplomacy without arms is like music without instrument*),[26] melainkan menerapkannya pada doktrin dalam organisasi militer, dimana organisasi dan teknologi melibatkan baik sipil dan militer.

Metodologi

Penelitian ini menggunakan pendekatan kualitatif. Pengumpulan datanya dilakukan menggunakan data primer dan didukung dengan data kuantitatif berupa tabel dan angka sebagai data sekunder. Sifat penelitian kualitatif seperti dijelaskan oleh Bogdan, adalah seperti orang yang sedang melakukan piknik, yakni ia baru tahu seluk beluk permasalahan setelah melakukan penelitian di lapangan dan setelah melakukan perjalanan yang panjang.[27] Penelitian kualitatif, oleh karenanya, selalu berjalan dengan sangat dinamis dan

[23] *Ibid,* hlm. 237.

[24] *Ibid.*

[25] *Ibid.*

[26] Henry R. Nau, "The Best Diplomacy is Armed Diplomacy",18 September 2013 dalam www.wsj.com/articles/SB10001424127887324665604579079430154269384, diunduh pada 20 Juli 2015.

[27] Sugiyono, *Metode Penelitian Kombinasi (Mixed Methods*), (Bandung: Alfabeta, 2011), hlm. 32-33.

penuh perubahan. Bahkan permasalahan yang diambil dapat berubah seiring dengan berjalannya penelitian.

Untuk mencapai dependabilitas (validitas) dan konfirmabilitas (reliabilitas) dalam penelitian ini, digunakan prinsip triangulasi. Triangulasi yang dilakukan dalam pengumpulan data, di antaranya menggunakan data hasil wawancara mendalam (pakar dan praktisi di lingkungan Kementerian Pertahanan dan Universitas Pertahanan); data dari dokumen resmi negara; dan data berdasarkan tinjauan literatur ilmiah.

MEF dalam Pembangunan Cyber-Defense: Sebuah Tinjauan RMA

Untuk masuk lebih dalam mengenai peran MEF dalam pembangunan *cyber-defense* bukan suatu perwujudan yang mudah untuk diimplementasikan, untuk itu para *stake-holder* yang terlibat dalam rangka pembangunan *cyber-defense* harus berangkat dari pelaksanaan RMA terlebih dahulu. Ada banyak tahapan dan proses yang harus dilaksanakan secara berkesinambungan, terutama dalam hal perwujudan teori RMA. Secara sederhana, RMA adalah upaya-upaya mengubah paradigma berperang. Inti dari RMA adalah perubahan cepat yang disebut revolusi.

Pentingnya RMA sebagai salah satu isu strategis pernah disampaikan Presiden ke-5 Susilo Bambang Yudhoyono. Dijelaskan bahwa di tengah perkembangan dunia dan implikasinya bagi Indonesia terutama berkaitan dengan strategi pertahanan dan doktrin perang. Sistem persenjataan dan teknologi militer telah berkembang pesat dalam kurun waktu 30 tahun terakhir yang kesemuanya tentu mengubah taktik dan teknik bertempur serta doktrin pertempuran yang ada. Peperangan konvensional saat ini telah memiliki corak perang modern, sebagai hasil dari revolusi yang terjadi di dunia militer yaitu RMA. Strategi, taktik dan doktrin pertempuran yang dijalankan harus benar-benar tepat dan mutakhir. Semuanya harus menggambarkan kemampuan untuk melaksanakan perang modern di banyak front termasuk pelibatan berbagai matra dalam operasi gabungan efektif.[28]

[28] Bagus Artiadi Soewardi, "Perlunya Membangun Sistem Cyber-defense yang tangguh bagi Indonesia", *Majalah Potensi Pertahanan,* Maret 2013.

Dalam konteks hubungan MEF dan pembangunan *cyber-defense* dengan RMA, MEF merupakan suatu kebijakan, bukan sekedar *output* alutsista dan infrastruktur saja. Maka penekanan peran MEF dalam pembangunan *cyber-defense* berupa revolusi teknologi, organisasi dan doktrin, termasuk produk turunannya berupa Peraturan Pemerintah, Peraturan Menteri Pertahanan, atau Buku Putih Pertahanan. Dalam hal ini akan dikelompokkan implementasi perwujudan pembangunan *cyber-defense* melalui pelaksanaan teori RMA yang terdiri dari tiga komponen yaitu melakukan perubahan doktrin; melakukan perubahan teknologi; dan melakukan perubahan organisasi, ketiga langkah tersebut akan dijabarkan dalambagian-bagianselanjutnyadalamnaskahini.

Perwujudan *Revolution in Military Affairs (RMA):* Melalui Perubahan Doktrin *Cyberwarfare*

Dalam mengimplementasikan *cyberwarfare* pada doktrin militer, berbagai angkatan bersenjata atau militer di berbagai negara melakukan penyesuaian. Angkatan bersenjata Amerika Serikat membuat doktrin tersendiri untuk menghadapi *cyberwarfare*. Doktrin itu disebut dengan doktrin transformasi militer yang dicetuskan oleh Donald Rumsfeld selaku *UnitedStatesSecretary of Defense*. Doktrin ini bertujuan membangun postur angkatan bersenjata yang lebih efektif, efisien, dan modern. Dalam doktrin tersebut terdapat tiga kemampuan kunci sebagai tulang punggung, yaitu: *knowledge*, *speed,* dan *precision*. Ketiga kemampuan ini ditujukan juga agar mempelajari sistem informasi seperti sistem satelit, sistem *Global Positioning System* (GPS), sistem komunikasi sistem komando dan kendali terintegrasi medan tempur (*integrated battle field command and control system*).

Pandangan yang lebih spesifik adalah adanya pertanyaan tentang perlunya merevolusi doktrin pertahanan Indonesia, khusus dalam sektor *cyber* saja. Selama ini Indonesia mengadopsi doktrin pertahanan yang defensif aktif, maksudnya tidak akan menyerang lebih dulu sebelum diserang pihak lain. Tentunya dengan harapan muncul suatu daya tangkal dari upaya bertahan tersebut. Hal ini seperti tidak berlaku dalam konteks perang *cyber* yang bersifat kebalikan dari doktrin pertahanan Indonesia.

Keberhasilan untuk implementasi suatu doktrin *cyberwarfare* sangatlah dipengaruhi oleh kualitas Sumber Daya Manusia (SDM) sendiri, yakni kemampuan untuk

memahami, menerima, dan menerapkan suatu konsep yang ditanamkan. Hal terpenting dalam rencana pembangunan pertahanan *cyber* adalah penyediaan dan kesiapan SDM yang berkualitas dan memadai jumlahnya karena *cyber defense* sangat sarat dengan TIK yang modern dan canggih. Hal yang harus dipertimbangkan lagi adalah spesifikasi doktrin dalam hal *cyber*, merupakan salah satu bidang yang memiliki sifat massif dan berkembang dengan pesat. Oleh karena itu faktor SDM adalah fokus pertama yang harus diperhatikan terlebih dahulu dalam implementasi doktrin *cyberwarfare* di Indonesia.

Perwujudan *Revolution in Military Affairs (RMA)*: Melalui Perubahan Organisasi Berbasis *Cyber-defense*

Langkah konkrit untuk merumuskan RMA *of cyber-defense* yang memuat peta jalan strategi nasional yaitu melalui pembentukan organisasi yang berbasis *cyber-defense.* Berdasarkan informasi langsung yang diperoleh dari para narasumber, beberapa di antaranya menyatakan bahwa RMA sangat berperan dan berkontribusi dalam upaya-upaya mengatasi *cyber-attack/cyber-threat*. Dalam tahap awal, kekuatan *cyber* yang hendak dibangun lebih berorientasi pada kemampuan bertahan (pasif), selanjutnya meningkat kemampuanya dalam kapasitas menyerang (aktif). Sementara itu, perlu dibentuknya organisasi khusus (semacam *cyber command*) lengkap dengan perangkatnya yang bertugas menangani permasalahan *cyber*. Organisasi tersebut mencakup sistem informasi, sistem jaringan, infrastruktur dan SDM.

Apa yang sudah dikerjakan oleh Mabes TNI dalam hal ini melalui Disinfohlahta sebenarnya merupakan bentuk representasi dari upaya antisipatif terhadap *cyber attack*. Namun demikian, kemampuan yang dimiliki tersebut masih terbatas, sehingga pendidikan dan pelatihan SDM di bidang *cyber* (pasukan *cyber*) perlu terus ditingkatkan agar personil TNI memiliki pengetahuan, keterampilan dan kemampuan (*capability*) yang lebih besar dalam menghadapi *cyber attack.* Tuntutan ini tidak lepas dari dinamika perkembangan TIK yang sangat cepat dan masif, disamping juga perkembangan dinamika lingkungan strategis yang berubah sangat cepat.

Dinamika perubahan lingkungan strategis telah mengakibatkan pergeseran konsep peperangan masa kini yang tidak sama dengan konsep peperangan konvensional

di masa sebelumnya. Sementara pada sisi lain, menurut narasumber lainnya, postur MEF yang ada saat ini belum secara optimal mengakomodasi upaya-upaya pembangunan kekuatan pertahanan *cyber* walaupun beberapa tindakan, inisiatif dan *concern* telah diarahkan untuk memenuhi kebutuhan tersebut. Artinya, bahwa pemerintah, dalam hal ini Kementerian Pertahanan, sudah menunjukkan upaya akomodatif untuk pembangunan kekuatan pertahanan *cyber* melalui postur MEF, namun alokasi sumber daya masih dalam skala kecil.

Hal ini disebabkan permasalahan yang dihadapi dalam postur MEF, diantaranyapostur MEF belum mampu mengakomodasi pembangunan kekuatan pertahanan *cyber* secara besar-besaran karena anggaran khusus pertahanan *cyber* belum memadai. Namun, anggaran dalam jumlah terbatas (relatif kecil) sebenarnya sudah tersedia melalui anggaran informatika yang pengggunaannya untuk kepentingan *cyber defense,* tetapi masih dalam skala yang terbatas. Postur MEF selama ini masih menitikberatkan pada kebutuhan TNI akan alat persenjataan yakni berupa *shopping list* alat utama sistem persenjataan (alutsista) yang hendak diakuisisi sehingga MEF masih terfokus pada prioritas pembangunan kekuatan alutsista. Perlunya Kemhan merevisi kembali postur MEF untuk tahun-tahun yang akan datang dengan memasukkan muatan pembangunan kekuatan pertahanan *cyber* dalam postur MEF. Hal ini diperkuat melihat bahwa pembangunan kekuatan *cyber* sangat penting bagi setiap negara. Hal tersebut tidak dapat ditunda lagi dan pembangunan kekuatan *cyber* dapat dilakukan beriringan dengan pembangunan kekuatan alutsista.

Dari uraian di atas, pada hakikatnya, MEF menjadi modal utama keberlangsungan proses RMA dalam institusi TNI dan totalitas proses RMA tersebut, secara ideal, sejatinya dituntut pula mampu mengakomodasi upaya-upaya pembangunan kekuatan pertahanan *cyber*. Hal ini dibutuhkan karena perubahan dinamis dari lingkungan strategis yang dihadapi Indonesia telah mengakibatkan perubahan paradigma ancaman yang memunculkan ancaman-ancaman nyata dalam bentuk yang berbeda. Selama ini, orientasi tujuan RMA lebih ditekankan untuk memperkuat dan memodernisasi peralatan dan sistem persenjataan karena pembangunan kekuatan secara militer tersebut masih diyakini mampu memberikan *detterent effect* yang ampuh kepada negara lain. Konsekuensi logis dari proses RMA yang masih diarahkan pada tujuan tersebut

mengakibatkan MEF juga masih berfokus pada upaya pemenuhan kebutuhan pengadaan (akuisisi) alutsista modern, belum mampu secara optimal mengakomodasi kebutuhan pembangunan kekuatan pertahanan *cyber.*

Menilik pada hasil temuan, sebagian besar narasumber yang telah diwawancara menerangkan bahwa MEF belum memasukkan unsur *cyber* dalam perencanaannya. Hal ini diterangkan dengan alasan karena MEF merupakan perencanaan berbasis kapabilitas yang prioritasnya difokuskan pada pengadaan alat-alat berat. Namun Purnomo Yusgiantoro selaku Menteri Pertahanan berpandangan justru MEF telah mengakomodir *cyber-defense* melalui undang-undang penyelarasan MEF pada tahun 2011. Namun hal ini merupakan kontradiksi antara teori dan praktik, karena kebijakan penyelarasan tidak dimaksudkan untuk me-*review* MEF, melainkan hanya menambahkan penyesuaian. Oleh karenanya perlu peninjauan secara empirik posisi *cyber-defense* pada MEF.

Perwujudan Revolution in Military Affairs (RMA): Melalui Perubahan Teknologi Cyber-defense

Dalam pemahaman konsep RMA yang lebih luas, seharusnya konsep RMA tidak sebatas diartikan sebagai proses pembaharuan/revolusi berbasis teknologi tinggi, modern dan canggih yang hanya diimplementasikan pada peralatan dan sistem persenjataan semata dalam organisasi TNI. Selama ini revolusi tersebut lebih didorong dalam konteks membangun kekuatan pertahanan militer dan menciptakan *detterent effect* terhadap negara lain. Namun, dalam kenyataannya, ancaman non militer, khususnya yang berkaitan dengan ancaman *cyber* semakin nyata dan aktual terjadi di Indonesia, sehingga dalam konteks RMA, seharusnya RMA juga dapat memenuhi kebutuhan pertahanan *cyber*. Konsekuensi logis dari hal ini, maka pembangunan kekuatan militer juga harus mencakup pembaharuan sistem pertahanan yang berkaitan dengan sistem TIK.

TIK yang canggih dan handal adalah basis infrastruktur utama dari kekuatan pertahanan *cyber*, sehingga apabila *cyber defense* hendak dibangun maka Kemhan dan TNI tidak dapat mengabaikan proses RMA yang seharusnya juga mencakup pembangunan sistem jaringan informasi dan komunikasi. Lebih lanjut, aspek SDM juga harus disiapkan dan ditingkatkan terus kualitasnya. Dengan demikian, urgensi

pembangunan kekuatan *cyberdefense* sudah seharusnya diimplementasikan dalam skema RMA dan terakomodasi dalam postur MEF.

Cyber Defense yang Ideal dalam Rangka Mewujudkan Cyberwar-Making Capabilities

Indonesia menganut *capability-based defense* dalam perencanaan pembangunan pertahanan, dan hal ini tertuang dalam Kebijakan Umum Pertahanan Negara (Jakumhaneg) tahun 2010-2014. Dalam hal ini, memajukan industri pertahanan menjadi sangat penting, dengan karakteristik oligopoli-monopsoni (beberapa penjual dengan satu pembeli), yang tidak lagi mengandalkan sepenuhnya kepada pemerintah dalam hal permodalan serta proses bisnis melainkan juga menjalankan usaha bisnis sendiri guna menopang produksi. Oleh karenanya, industri pertahanan dengan pola oligopoli-monopsoni merupakan kondisi yang dimungkinkan sekaligus memungkinkan adanya perencanaan berbasis kapabilitas yang menjadi karakter dari MEF.

Dari relasi ini, yakni antara industri pertahanan dan perencanaan anggaran pertahanan oleh pemerintah, dapat disimpulkan bahwa, industri pertahanan tidak dapat terus menerus berada di bawah kendali dan bantuan dari pemerintah selaku pemangku kepentingan maupun satu-satunya pembeli dalam pasar industri pertahanan. Industri pertahanan harus menjalankan bisnisnya juga secara mandiri di sisi yang lain. Oleh karenanya muncul konsep *dual-use*, yakni strategi industrial dengan memproduksi barang yang juga dapat dikonsumsi oleh publik sipil.

Berdasarkan problematika di atas, maka peningkatan kualitas produk yang diinginkan oleh *User*, dalamhaliniTNI dapat dicapai dengan beberapa kebijakan yang sudah dilakukan seperti pembentukan KomiteKebijakanIndustriPertahanan (KKIP), keharusan menggunakan produk alutsista lokal dalam negeri, meningkatkan Tingkat Komponen Dalam Negeri (TKDN) sampai dengan 35%, adanya program alih teknologi, offset, dan produksi bersama ketika ada pembelian alutsista dari luar negeri. Namun, ada beberapa tambahan gagasan yang kami anggap diperlukan agar terjadi sinkronisasi antara produsen (industri pertahanan) dengan konsumen (TNI/Polri) dapat diciptakanagar produk yang dihasilkan oleh industri pertahanan dalam negeri semakin meningkat kualitasnya.

Pembentukan pusat riset/badan penelitian dan pengembangan industri pertahanan merupakan hal yang dibutuhkan untuk mengatas hal ini. Penelitian yang dilakukan oleh industri pertahanan dan institusi-institusi terkait masih sporadisatauterpisah-pisah. Akibatnyaadalahterjadipenelitian dengan objek yang sama, namun tidak terdapat perbedaan yang signifikan, atau masing-masing mengembangkan produk yang sama, namun tidak terintegrasi dengan produk lainnya. Impikasinyaadalahdana riset yang dikeluarkan cukup banyak, namun belum mampumencapai kualitas yang canggih dan unggul.

Pembangunan Cyber-Defense Berdasarkan Konsep Smart Power

Pentingnya *smart power* dapat dilihat dari pernyataan Kaisar Prusia, Frederick *The Great* bahwa diplomasi tanpa senjata seperti musik tanpa instrumen. Pembangunan *cyber-defense* memiliki analogi yang sama dan masuk dalam konsep *smart power*. Ada sinergi antara komponen-komponen yang selama ini dianggap terpisah, padahal sama-sama berperan penting. Misalnya, *cyber-defense* berbasis koordinasi sipil-militer atau *cyber-defense* dengan diplomasi dan senjata (infrastruktur).

Wacana koordinasi sipil-militer dalam *cyber-defense* menarik untuk dibahas lebih mendalam. Pasalnya, kedua komponen yang sering didikotomikan tersebut memiliki masing-masing karakteristik terkait *cyber-defense*. Komponen sipil lebih peka terhadap ancaman *cyber* yang berada dalam kehidupan sehari-hari, namun memiliki kesadaran bela negara yang rendah. Namun, komponen militer sebaliknya, cenderung kurang peka terhadap ancaman *cyber* yang termasuk ancaman nir-militer. Hal ini bisa dipahami mengingat organisasi militer lebih ditujukan menghadapi ancaman-ancaman militer. Namun komponen militer memiliki kesadaran bela negara yang tinggi.

Melihat kelemahan dan kekuatan kedua komponen, disinilah pentingnya suatu hubungan yang sinergis dan koordinatif. Bentuk hubungan semacam ini pun telah diakui beberapa narasumber penelitian. Seperti contoh koordinasi antara Kementerian Pertahanan dengan MarkasBesar (Mabes) TNI yang membentuk *Cyber Operation Command* (COC), atau TNI AngkatanLaut (AL) dengan InstitutTeknologi Bandung (ITB) yang bekerjasama membangun sistem data.

Konsep *smart power* menarik secara teori, namun pada praktiknya tidak. Hal ini terjadi dalam kasus pembentukan armada keempat yang diinisiasi Kemhan dan TNI, wacananya lebih banyak masyarakat sipil yang masuk didalamnya disamping personil militer. Diharapkan bahwa sipil dapat berkontribusi lebih dalam pertahanan nir-militer ini. Akan tetapi wacana ini justru lebih mengandung muatan ancaman daripada peluang oleh karena kesadaran bela negara yang masih rendah.

Penerapan *smart power* pun terganjal oleh salah satu permasalahan yang telah dikemukakan di awal, yakni SDM. Idealnya, baik masyarakat sipil dan personil militer sama-sama memiliki kesadaran bela negara yang tinggi dan *skill* pertahanan yang mumpuni. Jika kedua hal tersebut dipenuhi, barulah dibicarakan soal kerjasama sipil-militer untuk menghadapi ancaman *cyber*. Untuk meningkatkan kesadaran masyarakat sipil, pemerintah dapat melakukan sosialisasi peningkatan kesadaran bela negara dengan gencar. Hal ini pun diakui oleh narasumber yang berasal dari TNI AL, sebelum masuk ke tingkatan kerjasama. Masyarakat sipil yang diajak terlibat dalam Pusat *Cyber* kedepannya harus dibina dan dilatih terlebih dahulu.

Selain kerjasama sipil-militer, konsep *smart power* juga dapat direalisasikan melalui peningkatan teknologi dan infrastruktur *cyber* skala nasional dan upaya-upaya diplomasi *cyber-defense*. Sudah menjadi hukum alam di sistem internasional bahwa suatu negara melakukan diplomasi untuk mencapai kepentingan nasionalnya. Ketika kita sepakat bahwa *cyber-defense* merupakan salah satu kepentingan nasional di masa depan dan saat ini pemerintah Indonesia belum mampu merealisasikannya sendiri, maka diplomasi *cyber-defense* mutlak dilakukan. Hal tersebut, salah satunya adalah dengan mengirimkan 104 personil dari instansi pemerintah dan perguruan tinggi untuk belajar ke *Naval Postgraduate School* (NPS) di Monterey, California, Amerika Serikat. Langkah ini patut diapresiasi mengingat Amerika Serikat sedang berfokus dalam pengembangan *cyber-defense*-nya.

Selain itu, hubungan sipil dan militer di Amerika Serikat juga dapat diposisikan sebagai pendukung untuk terwujudnya *cyber-defence.* Hal ini terlihat beberapa institusi sipil dan militer seperti *Center of Civil-Military Relation* (CCMR) yang berada di NPS membahas program mengenai ancaman nir-militer terutama dalam hal *cyberwarfare*. Dalam menangani ancaman tersebut tidaklah cukup ditangani dari segi militer saja,

melainkan dari komponen sipil dituntut untuk berperan aktif dalam mengahadapi ancaman *cyber*. Dari institusi tersebut, Amerika Serikat banyak mengundang para ilmuwan dari berbagai negara untuk mewujudkan suatu konsep *smart-power* dengan melakukan diplomasi, tukar informasi melalui diskusi, sehingga mendapatkan banyak perspektif dalam menanggulangi suatu ancaman. Namun, diplomasi ke Amerika Serikat tidaklah cukup. Studi perbandingan dapat dilakukan ke Rusia dan Tiongkok yang dalam statistik merupakan dua negara tempat asal serangan *cyber* terbanyak ke seluruh dunia.

Pada bagian ini perlu digarisbawahi bahwa dalam berbicara *cyber-defense* konteks strategis, Indonesia tidak bisa hanya belajar atau bekerjasama dengan satu negara dengan satu referensi saja. Indonesia harus belajar bertahan dari Amerika Serikat yang menerima serangan *cyber* paling banyak dan belajar menyerang dari Tiongkok serta Rusia yang mengirim serangan *cyber* paling banyak, disamping memperlihatkan bahwa perilaku menyerang (*offensive*) dalam ruang lingkup *cyber* jauh lebih murah biayanya daripada perilaku bertahan (*defensive*). Setiap orang dapat melakukan serangan *cyber* hanya dengan bermodalkan *gadget* atau laptop. Tidak sekompleks dan serumit upaya bertahan.

Hal ini pernah terjadi ketika perang *cyber* antara peretas Indonesia dan peretas Australia berlangsung saat dipicu skandal penyadapan yang dilakukan Australia terhadap telepon genggam Presiden ke-5 Susilo Bambang Yudhoyono. Saat itu, para peretas Indonesia mengambil inisiatif untuk menyerang beberapa situs milik Australia.[29] Contoh lainnya adalah perilaku menyerang Rusia yang selalu menggunakan serangan *cyber* terhadap negara-negara tetangganya seperti Estonia pada 2007, Georgia pada 2008 dan Ukraina pada 2014. Hasilnya adalah efek getar terhadap *North Atlantic Treaty Organization* (NATO) yang lebih menyiapkan pasukan khusus untuk menghadapi serangan *cyber* Rusia kedepannya. Pilihan ofensif atau defensif ini sangat tergantung dari doktrin pertahanan Indonesia kedepan. Apakah dengan adanya fenomena RMA di seluruh dunia, maka doktrin pertahanan Indonesia akan berubah? Setidaknya dalam ranah *cyber* saja. Akan tetapi, dengan pertimbangan biaya saja, perubahan tersebut sangat mungkin terjadi.

Berbicara *cyber-defense* dalam konteks RMA maka komponen *hard power* paling utama adalah pengadaan satelit. Wacana pengadaan satelit *cyber-defense* pernah

[29]"BIN: Perang Siber, Hacker Indonesia Jago-jago", dalam http://us.m.news.viva.co.id/news/read/460064-bin–perang-*cyber*–hacker-indonesia-jago-jago, 20 November 2013, diunduh pada 1 Agustus 2015.

mengemuka sekitar 2013 ketika Menteri Pertahanan saat itu, Purnomo Yusgiantoro menyebutkan bahwa pengadaan satelit *cyber-defense* masuk rencana anggaran 2014. Urgensi pengadaan satelit tergolong penting dalam *cyber-defense*. Disebutkan bahwa TNI sebenarnya mempunyai jaringan komunikasi satelit yang dioperasikan oleh Mabes TNI. Akan tetapi satelit yang dimaksud masih menyewa milik PT. Telkom dan tidak mendukung optimal latihan operasi militer yang membutuhkan komunikasi di segala kondisi.[30]

Ditambah lagi kondisi bahwa sebagian teknologi komunikasi TNI masih menggunakan teknologi radio dan belum terintegrasi. Banyak contoh di TNI AL dan TNI AngkatanUdara (AU) yang menggambarkan kesulitan-kesulitan di lapangan dikarenakan faktor teknologi komunikasi yang rendah. Kondisi di TNI AL misalnya, Pos Komando dan Pengendalian belum dapat terhubung ke kapal. Jika saja ada kapal perang asing melanggar kedaulatan negara, maka keputusan menembak atau tidak, bakal sulit diperoleh dengan cepat karena kapal tidak memiliki komunikasi langsung ke Pos Kendali Pusat di Jakarta.Lain halnya jika melihat sistem *cyber-defense* yang sudah berjalan dengan baik di negara Inggris.Penerapan sistem *cyber-defense* di Inggris sudah meliputi penggunaan *spacecraft,* proteksi penggunaan laser, dan pertahanan informasi melalui *Unmanned Aerial Vehicles* (UAVs).[31]

Beberapa hal menarik dari wacana pengadaan satelit *cyber-defense* adalah penggunaan industri pertahanan dan SDM dalam negeri untuk membangun satu unit. Seperti diutarakan oleh Wakil Ketua Komisi I DewanPerwakilan Rakyat (DPR) RI dari Fraksi Partai Golkar, Agus Gumiwang Kartasasmita, yang mendukung rencana pengadaan satelit keperluan militer dengan menggunakan buatan dalam negeri. Pertimbangannya, berbicara *cyber* jauh lebih aman menggunakan produk sendiri daripada membeli satelit dari negara lain. Jika hal tersebut benar, maka inilah bentuk lain dari *smart power* yaitu menggunakan kemampuan sendiri *(soft)* untuk menciptakan daya tangkal *(hard)* terhadap negara-negara lain. Penguasaan teknologi pertahanan yang mumpuni oleh Indonesia bisa memunculkan kekhawatiran oleh negara-negara di sub-kawasan.

[30] "Pengadaan Satelit Militer Indonesia", dalam http://jakartagreater.com/pengadaan-satelit-militer-indonesia/, 23 Agustus 2013, diunduhpada 1 Agustus 2015.

[31] "UK Set for Military Space Launch", dalam http://news.bbc.co.uk/2/hi/science/nature/7079876.stm, 9 November 2007, diunduhpada 1 Agustus 2015.

Kesimpulan

Dari hasil penelitian, dapat ditarik beberapa kesimpulan, bahwaperanan MEF di Indonesia sejauh ini masih belum dapat dilihat terutama dalam hal pembangunan *cyber-defense*. Belum adanya kebijakan yang dituangkan dalam MEF terkait *cyber-defense* sebagai postur kekuatan pertahanan yang dimiliki Kemhan dan Mabes TNI. Saat ini penanganan serangan *cyber* belum dilaksanakan secara integratif antara komponen pertahanan militer dan nir-militer. Hal tersebut terjadi karena belum adanya keselarasan pandangan antara para pengambil kebijakan dan para pelaksana pembangunan *cyber-defense.* Dari permasalahan tersebut digunakan pendekatan RMA terlebih dahulu untuk mewujudkan pembangunan *cyber-defense,* setelah *cyber-defense* diwujudkan baru dapat dilihat peran sebenarnya dari MEF. MEF yang ada ternyata belum ideal karena belum memasukkan secara eksplisit dan tegas (dinyatakan secara jelas) komponen *cyber-defense* dengan konsep RMA dan *smart power,* yaitu penggabungan antara *hard power* dan *soft power*.

Saran

Dari hasil-hasil penelitian ini, disampaikan beberapa saran dan rekomendasi kritissebagaiberikut:

a. untuk mewujudkan RMA yang berkaitan dengan *cyber-defense* di Indonesia, diperlukan 3 (tiga) komponen perubahan yaitu melalui perubahan doktrin, perubahan organisasi yang berbasis *cyber-defense,* dan pembangunan teknologi;
b. bahwapemahaman RMA tidak hanya sebatas pada pemahaman revolusi berbasis teknologi yang hanya diimplementasikan dalam peralatan alutsista saja namun juga harus diimplementasikan dalam Undang-Undang dan Peraturan yang mengubah cara pandang terhadap perlunya revolusi pada Teknologi, Organisasi, dan Doktrin Pertahanan yang diimplementasikan dalam peralatan non-alutsista atau peralatan TIK yang berhubungan dengan ranah *cyber*;
c. diperlukan upaya merevisi isidari MEF pada RencanaStrategi (Renstra)-2 yang sedang berjalansaatini serta merencanakan ulang MEF Renstra-3 dengan skala prioritas memasukkan komponen *cyber-defense* dalamrangka menghadapi ancaman *cyber*;

d. dibutuhkan kesesuaian pandangan RMA antara para pengambil kebijakan dan para pelaksana pembangunan *cyber-defense* (Kemhan RI dan Mabes TNI). Hal tersebut sangat terkait dengan masalah penganggaran dalam pembangunannya;

e. penelitian analisis MEF ini dapat dilanjutkan dengan lebih mendalam pada aspek *Civil-Millitary Relations* (CMR);

f. mengusulkan pengembangan konsep dan program pertahanan *cyber* Indonesia yang memiliki karakter Indonesia dengan menekankan pada aspek defensif daripada ofensif;

g. mengusulkan pengembangan pertahanan *cyber* Indonesia yang konkrit, pengembangan kerjasama dengan lembaga-lembaga lain seperti perguruan-perguruan tinggi untuk bersama-sama mengembangkan sistem pertahanan *cyber* sendiri, dan mengirim ahli-ahli Indonesia untuk belajar mengenai *cyber-defense* keluar negeri.

Daftar Pustaka

Buku

Buku Putih Pertahanan Indonesia. 2008. Jakarta: Kementerian Pertahanan.

Carr, Jeffrey. 2012. *Inside Cyber Warfare, Second Edition.* Sebastopol: O'Relly Media.

Dombrowski Peter, dan Eugene Gohlz. 2006. *Buying Military Transformation: Technological Innovation and Defense Industry*. New York: Columbia University Press.

Goldman, Emily dan Thomas Mahnken. 2004. *Information Revolution in Military Affairs in Asia*. New York: Palgrave McMillan.

Hardt, Michael dan Antonio Negri. 2004. *Multitude: War and Democracy in the Age of Empire*. USA: The Penguin Press.

Jasper, Scott. 2014. "Deterrence of Cyber Agression", dalam *A Comprehensive Approach to Operations in Complex Environments*. Monterey: Naval Postgradute School.

Kementerian Pertahanan RI. 2011. *Penyelarasan Minimum Essential Force (MEF) sebagai Komponen Utama*. Jakarta: Kementerian Pertahanan RI.

Kramer, Franklin D. et al. 2009. *Cyberpower and National Security*. Washington DC: National Defense University.

Mas'oed, Mohtar. 1990. *Ilmu Hubungan Internasional: Disiplin dan Metodologi.* Yogyakarta: LP3ES.

Sugiyono. 2011. *Metode Penelitian Kombinasi (Mixed Methods*). Bandung: Alfabeta.

Jurnal

Chong, Alan. 2015. "Smart Power and Military Force: An Introduction",*Journal of Strategic Studies*, Vol.38.No.3.

Segal, Adam M. 2014."Cyberspace: The New Strategic Realm in US–China Relations." *Strategic Analysis Journal*, Vol.38. No.4.

Majalah

Soewardi, Bagus Artiadi. 2013."Perlunya Membangun Sistem *Cyber-defense*yang tangguh bagi Indonesia". *Majalah Potensi Pertahanan*. Maret.

World Economic Forum. 2014. *Insight Report: Risk and Responsibility in a Hyperconnected World*. Januari.

Website

"BIN: Perang Cyber, Hacker Indonesia Jago-jago" dalam http://us.m.news.viva.co.id/news/read/460064-bin--perang-*cyber*--hacker-indonesia-jago-jago, 20 November 2013, diunduh pada 1 Agustus 2015.

"Indonesia: The World Fact Book",https://www.cia.gov/library/publications/the-world-factbook/geos/id.html, diunduh pada 22 Maret 2015.

Nau, Henry R, "The Best Diplomacy is Armed Diplomacy",18 September 2013,dalamwww.wsj.com/articles/SB10001424127887324665604579079430154269384, diunduh pada 20 Juli 2015.

Prameswaran, Prashanth, "Indonesia's Cyber Challenge Under Jokowi", dalamhttp://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/, 21 Januari 2015, diunduh pada 9 Februari 2015.

"Pengadaan Satelit Militer Indonesia", dalam http://jakartagreater.com/pengadaan-satelit-militer-indonesia/, 23 Agustus 2013, diunduh pada 1 Agustus 2015.

"UK Set for Military Space Launch "http://news.bbc.co.uk/2/hi/science/nature/7079876.stm, 9 November 2007, diunduh pada 1 Agustus 2015.

Perundang-undangan

Kebijakan Umum Pertahanan Negara. 2010. Peraturan Presiden No. 41 Tahun 2010.

Peta Jalan Strategi Nasional Pertahanan Seber. 2014. Kementerian Pertahanan RI.