ANALISIS WACANA CYBERWAR PADA ARTIKEL DI SITUS KOMPASIANA

Oleh: Bima Oktoriawan (070915053) - D
serulingkayu3@gmail.com

ABSTRAK

Penelitian ini berfokus pada analisis wacana *cyberwar* pada artikel di situs Kompasiana. Peneliti menggunakan analisis wacana Norman Fairclough untuk menganalisis isi artikel. *Cyberwar* merupakan sebuah aksi menghancurkan, memanipulasi, dan mencuri informasi-informasi penting menggunakan medium *cyberspace* yang berkaitan dengan kepentingan negara. Kegiatan-kegiatan *cyberwar* berkaitan dengan aksi penyerangan terhadap ekonomi, militer, informasi, dan fasilitas fisik melalui medium *cyberspace.* Peneliti akan menganalisis tiga artikel yang mengandung wacana *cyberwar* pada tulisannya. Artikel yang diposting di situs *macroblogging* ini berusaha mewacanakan *cyberwar* dan kaitannya dengan konsep-konsep kekuasaan. Artikel-artikel ini menuliskan wacana *cyberwar* dalam kondisi geopolitik dunia. Berdasarkan hasil analisis, peneliti menemukan bahwa wacana *cyberwar* merupakan suatu bentuk perang modern. Internet sebagai barang yang telah kita terima sebagai bagian dari kehidupan masyarakat modern memiliki aspek-aspek yang sulit untuk diprediksi potensi penggunaannya. Salah satunya, Internet dipandang sebagai medan perang baru. Informasi, asset, dan keterkaitan erat antara internet dan fasilitas fisik menyebabkan internet menjadi ranah konflik baru. Sifat internet yang *borderless*, anonym, dan bebas mengakibatkan serangan-serangan terhadap fasilitas fisik, ekonomi negara, dan informasi-informasi penting menjadi amat berbahaya bagi masyarakat dan keamanan negara. Wacana *cyberwar* terkait erat dengan konsep-konsep kekuasaan negara, keamanan negara, dan kepentingan-kepentingan militer dan sipil.

Kata kunci : Wacana, *Cyberwar,* Kekuasaan, Negara, *Cyberspace, Internet,* Norman Fairclough

PENDAHULUAN

Penelitian ini berfokus pada interpretasi *netizen* pengguna Kompasiana sebagai situs macroblogging terbesar di Indonesia mengenai konsep cyberwar. Peneliti ingin mengeksplorasi bagaimana interpretasi konsep cyberwar yang dituliskan oleh *netizen* pengguna Kompasiana pada artikel yang diposting di situs Kompasiana. Penelitian ini penting untuk diteliti karena konsep cyberwar masih menjadi perdebatan di berbagai *public sphere* yang ada di dunia maya, dan juga diperdebatkan oleh para akademisi. Ini bisa dibuktikan melalui sanggahan oleh beberapa artikel yang ditulis peneliti dunia cyber seperti Ryan Singel (Singel,

2010), Ian Wallace (Wallace, 2013) terhadap buku *Cyberwar: The Next Threat to National Security and What to Do About It* (Clarke, 2010).

Pada buku ini, Richard Clarke mengemukakan kekhawatirannya mengenai *nature* dari internet itu yang merupakan:

> *"Open, highly interconnected, decentralized, and largely unsecured / unencrypted — makes cyberspace more vulnerable to various forms of attacks."*

Internet muncul sebagai media yang memiliki karakteristik yang berbeda dengan media biasa. Internet memiliki karakteristik kebaruan, kebebasan berekspresi, *borderless, anonymity,* dan merupakan sebuah domain yang baru dijelajah sehingga internet menjadi sebuah domain yang memerlukan penelitian lebih lanjut untuk menjelaskan berbagai fenomena yang timbul sebagai akibat lahirnya internet.

Clarke dalam bukunya melihat bahwa *cyberwar* amat terkait dengan kepentingan-kepentingan pertahanan negara, dan bahkan menyarankan agar pemerintahan mengambil tindakan-tindakan militer untuk melindungi aset-aset sipil. Wallace, sebaliknya, dalam artikel sanggahannya justru menentang pendapat Clarke yang dianggap berpotensi mengancam kebebasan berinternet karena seakan-seakan dibutuhkan intervensi militer untuk melindungi serangan-serangan *cyber* yang sebagian besar ditujukan kepada instansi atau individu-individu sipil. Problem-problem dilematis yang berkaitan dengan kepentingan pertahanan negara, kebebasan berinternet, aset-aset bisnis yang terkoneksi online, dan hubungan diplomatik dengan negara-negara lain inilah yang membuat perdebatan mengenai definisi dan aplikasi *cyberwar* selalu ramai dibicarakan di media-media sosial,

blog, hingga jaringan media massa. Sejauh ini, konsep-konsep *cyberwar* yang dikemukan di media massa maupun di internet berkaitan erat dengan kekuasaan informasi. Kasus-kasus serangan *cyberwar* dengan skala besar hampir seluruhnya merupakan serangan peretasan data-data dan informasi-informasi rahasia seperti *database* bank dan kartu kredit, informasi rahasia negara, dan data-data rahasia individu mulai dari password email sampai dengan PIN ATM. Tak pelak, ketika media massa menggemakan eksistensi *cyberwar, netizen* berbondong-bondong untuk mengupas, menelaah, dan menyumbangkan pendapat mengenai *cyberwar.*

Histeria *netizen* kepada *cyberwar* terutama *netizen* di Indonesia memuncak ketika peristiwa penyadapan telepon genggam Presiden RI Susilo Bambang Yudhoyono oleh pihak intelijen Australia. Penyadapan ini, dianggap oleh *netizen* di Indonesia sebagai bentuk *cyberwar* terang-terangan pihak Australia terhadap Indonesia. Dialektika yang muncul antara *netizen* Indonesia pun bermacam-macam. Contohnya pada situs macroblogging terbesar di Indonesia yaitu Kompasiana. Apabila kita melakukan *search* pada situs Kompasiana menggunakan *keyword* "Penyadapan SBY" maka akan didapati ratusan artikel yang dikhususkan membahas isu ini. Salah satu *netizen* Kompasiana dengan akun "Buletin Dakwah Al-Islam" menyebutkan bahwa penyadapan terhadap SBY merupakan suatu bentuk cyberwar karena posisi SBY sebagai kepala negara (Kompasiana,2013). Peneliti memutuskan untuk menggunakan situs Kompasiana karena situs ini merupakan situs dimana *netizen* mempunyai kebebasan untuk menuliskan berbagai macam topik tulisan. Kompasiana juga mengizinkan *netizen* bebas untuk menuliskan opini, unek-unek, kritik, maupun saran dan mempostingnya untuk dibaca oleh sesama *netizen.* Meskipun *netizen* bebas untuk menulis apa saja, pertanggungjawaban yang

berkaitan dengan tulisan mereka merupakan tanggung jawab si penulis itu sendiri, sehingga administrator Kompasiana tidak ikut bertanggungjawab apabila terjadi sesuatu pada si penulis berkaitan dengan tulisannya di Kompasiana. Kompasiana, apabila dibandingkan dengan *blog* atau media sosial yang lain, menawarkan gabungan konsep unik antara *citizen journalism* dan *blogging.* Media massa, umumnya memiliki wartawan, redaktur, dan profesi-profesi lainnya yang terikat pada perusahaan media massa tersebut bernaung untuk menghasilkan sebuah karya jurnalistik. Tulisan-tulisan di Kompasiana, sebaliknya, belum tentu dikategorikan menjadi sebuah karya jurnalistik (dimana sebagian besar merupakan opini penulis), serta artikel-artikel di Kompasiana ditulis oleh warga "Kompasianer" (istilah *netizen* "penghuni" website Kompasiana) tanpa ada ikatan kontrak kerja dengan website Kompasiana. Dengan kata lain, Kompasiana dapat diistilahkan sebagai salah satu website dengan aktivitas *macroblogging* terbesar di Indonesia. *Traffic* Kompasiana sebagai web *macroblogging* sendiri per Juli 2011 adalah 75.000 anggota terdaftar, 600-800 tulisan perhari, dan 6-8 juta *view* perbulannya (Kompasiana, 2011). Sebagai perbandingan, situs *macroblogging* besar di Indonesia adalah Tempo Interaktif. Portal *macroblogging* milik Grup Tempo ini mencatatkan jumlah pengunjung yang besar tiap bulannya. Catatan Google Analytics menyebutkan bahwa sepanjang 2010 terjadi peningkatan jumlah pengunjung Tempo Interaktif sebesar 190 persen, yaitu dari rata-rata 1 juta pengunjung naik menjadi 3,5 juta pengunjung per bulan. Sementara itu, jumlah halaman yang dibuka oleh satu pengunjung juga mengalami peningkatan menjadi 11 juta halaman per bulan.

Dalam menganalisis wacana *cyberwar,* peneliti ingin menggunakan metode *critical discourse analysis* yang dikemukakan oleh Norman Fairclough. Dalam teorinya, Fairclough menyatakan bahwa wacana teks tidak hanya dipahami sebagai bahasa tradisional saja. Menurut Fairclough, teks dibangun dalam tiga aspek analisis; tekstual, kultural, dan praktik diskursif. (Jorgensen&Philips, 2007: 124). Melalui tiga aspek ini, bahasa dapat dilihat bukan lagi hanya menjadi sepotong teks namun juga sebagai alat untuk melanggengkan praktek penerapan ideologi. Ketiga aspek ini dapat digunakan oleh peneliti teks untuk membongkar bagaimana relasi kekuasaan berkembang dalam konstruksi realitas sosial dalam masyarakat. Fairclough mengemukakan bahwa ada tiga dimensi analisis yang dapat dilakukan untuk melakukan analisis wacana, yaitu teks, praktik diskursif, dan praktik sosio-kultural. (Ibnu Hamad, 20004:47).

Dalam penelitian ini, metode analisis wacana Fairclough akan melihat secara komprehensif bagaimana teks dikonstruksikan oleh penulis artikel di situs Kompasiana. Teori analisis wacana milik Fairclough dalam penelitian ini berfungsi untuk melihat hubungan kekuasaan serta motif-motif ideologis didalam teks serta praktik sosial yang menjadi basis lahirnya teks. Selain menjadi sandaran teoritis, analisis wacana kritis dari Fairclough ini juga akan dipakai sebagai metode analisis.

PEMBAHASAN

Peneliti telah melakukan pengamatan pada situs Kompasiana untuk mendapatkan data-data yang berkaitan dengan penelitian ini. Peneliti telah melakukan pengamatan pada situs Kompasiana selama tanggal 10 Oktober – 10 November 2014. Peneliti telah memilih dan menganalisis tiga artikel yang memuat wacana mengenai *cyberwar*. Peneliti

menggunakan metode Critical Discourse Analysis dengan level analisis teks, praktik wacana, dan praktik social budaya dari artikel di Kompasiana.

Alasan peneliti memilih tiga artikel pada situs Kompasiana karena ketiga artikel tersebut dianggap peneliti mengandung wacana-wacana *cyberwar* yang sesuai dengan konsep *cyberwar* yang dipahami peneliti. Konsep-konsep yang diwacanakan tersebut antara lain tentang serangan-serangan yang terhadap suatu negara menggunakan medium *cyberspace*, dan langkah-langkah pertahanan suatu negara dalam menghadang serangan *cyber*. Penelitian ini melihat bagaimana ketiga artikel ini memunculkan wacana mengenai *cyberwar* dengan objek tulisan yang berbeda-beda. Penelitian ini juga melihat bagaimana konsep-konsep *cyberwar* dan kaitannya dengan kekuasaan dimunculkan dalam wacana-wacana tersebut.

Pada judul artikel 1, penulis artikel yaitu kodenama "Ragile" memilih judul "Tumben, Hacker Saudi Menewaskan Israel (Cyberwar: 0xOmar vs Hannibal). Penggunaan judul ini menyiratkan bahwa hacker Israel yang dikenal memiliki kemampuan tinggi di dunia peretasan mampu dikalahkan secara telak oleh hacker Saudi. Pada paragraf awal, penulis menjabarkan kronologi pertempuran antara 0xOmar dengan Hannibal. Penulis mengkaitkan awal mula pertempuran dunia maya ini dipicu oleh serangan Israel ke Jalur Gaza, serta dibahasnya rancangan undang-undang SOPA PIPA di Washington sehingga memicu hacker Saudi untuk menjebol jutaan akun kartu kredit yang terafiliasi dengan Israel. Pada bahasan selanjutnya, penulis menjelaskan sikap pemerintah Saudi terhadap aksi yang diklaim dilakukan oleh warganya. Namun, Ragile berpendapat bahwa dalam konflik global, tidak menutup kemungkinan bahwa kejadian serangan-serangan ini merupakan permainan politik antara Saudi dengan Israel untuk mencapai tujuan-tujuan politik di negara tetangganya seperti Iran.

Ada beberapa fenomena yang dianggap oleh Ragile merupakan indikasi permainan politik antara Saudi dengan Israel, seperti kecaman yang diterima oleh Raja Saudi atas sikap agresifnya yang mendukung NATO dalam menghancurkan Libya dan Syiria. Kemudian Emir Qatar yang sedang berusaha untuk menggantikan posisi Raja Saudi sebagai pemimpin dunia Islam. Faktor-faktor ini dapat dianggap sebagai tekanan bagi Saudi untuk mengubah stigma Saudi sebagai negara yang dekat dengan Israel. Pasukan khusus Saudi yang dilatih oleh Israel, pendudukan Jalur Gaza, dan posisi Irana sebagai kekuatan militer ketiga di semenanjung Teluk menyebabkan tegangnya hubungan Israel dan Saudi dengan negara-negara Islam lainnya. Hubungan Israel dengan negara-negara Teluk lain yang tidak seharmonis dengan Saudi menyebabkan Saudi mengevaluasi posisi diplomatisnya dengan Israel menyusul situasi perang di Libya dan Syiria. Namun, penulis artikel juga menuliskan poin asumsinya yang mengambil sudut pandang dari pihak ketiga. Bahwa ada negara tetangga yaitu Iran yang juga memiliki kepentingan di Teluk sedang berusaha memecah hubungan harmonis antara Saudi dengan Israel. Ragile juga berpendapat bahwa pada kondisi peperangan modern yang beralih pada perang dunia maya akan menjadi trend baru. Hal ini sejalan dengan berkembang pesatnya teknologi-teknologi informasi dan mahalnya biaya berperang menggunakan metode konvensional yaitu mengirim pasukan ke medan perang. Pada penutup, Ragile menyampaikan sebuah kutipan

> *new definition about terror: terrorism is what THEY do, counterterrorism is what WE do. Definisi baru tentang teror: terorisme adalah apa yang MEREKA lakukan, kontraterorisme adalah apa yang KITA lakukan.*

Kutipan ini dapat disimpulkan sebagai pendapat Ragile yang menyatakan bahwa perbedaan tindakan-tindakan yang mengatasnamakan terror atau kontraterorisme hanyalah pada siapa yang melakukan tindakan tersebut. Dengan tidak langsung, Ragile menyindir negara-negara seperti Amerika Serikat, Inggris, dan negara-negara lain yang tergabung dalam

Blok NATO sebagai pihak yang menggunakan cara yang dianggap sebagai terror, namun dialihbahasakan dan dicari pembenarannya sehingga dapat disebut sebagai kontra terorisme. Selanjutnya adalah artikel 2 yang ditulis oleh Ahmad Sofyan dengan judul "Mengapa Kita "Mesra" dengan China?". Kedekatan pemerintah China dengan Indonesia sudah menjadi pengetahuan umum, terkait dengan kerjasama kedua belah negara di bidang ekonomi dan pertahanan. Kedekatan kedua negara ini mempengaruhi gejolak politik di wilayah Asia Pasifik, mengingat posisi laut Indonesia sebagai gerbang lalu lintas perdagangan dunia dan China. Sebuah laporan yang dilansir oleh badan intelijen Amerika menyebutkan bahwa geopolitik di Asia akan didominasi oleh China dan India. Ahmad menuliskan berbagai factor yang mendukung pesatnya pertumbuhan ekonomi China, mulai dari sektor ekonomi, migas, perdagangan, dan politik.

Kemajuan dan pertumbuhan China ini diwaspadai oleh Amerika yang melakukan militerisasi kawasan. Kettegangan China dengan Amerika yang menggunakan negara-negara ASEAN sebagai proxy untuk mengganjal pertumbuhan China di wilayah Asia Pasifik pun terus bertambah. Salah satu kebijakan Amerika untuk mengganjal China adalah melakukan *cyberwarfare* yang diprediksi akan menjadi ujung tombak Amerika untuk meruntuhkan hegemoni China. Peperangan siber antara kedua negara ini mencapai eskalasi yang cukup tinggi dengan dirilisnya laporan-laporan rahasia negara China oleh WikiLeaks. China yang kecolongan menuduh Amerika berada di balik bocornya laporan-laporan rahasia China dan menjalankan kampanye disinformasi untuk mengaburkan aktivitas-aktivitas siber Amerika yang mengancam kerahasiaan negara lain. China juga menuduh terlibatnya Israel dalam proses perang siber dan disinformasi yang dilakukan oleh Amerika. Salah satu kasus disinformasi yang dilakukan oleh Amerika menurut China adalah percobaan peretasan perusahaan *search engine* terbesar di dunia yaitu Google. Amerika menuduh *hacker* yang

diduga bekerja untuk pemerintah China meretas perusahaan bendera Amerika dengan tujuan mendukung pembajakan dan memiliki motif tersembunyi.

Indonesia pun memilih untuk mengembangkan pertahanan sibernya dengan bekerjasama dengan pemerintah China. Hal ini tidak lepas dari strategi jangka panjang China untuk menguasai 80% dari system komunikasi dunia melalui perusahaan-perusahaan telekomunikasi terkemukanya seperti Huawei. Pilihan pemerintah untuk bekerja sama dengan China tidak lepas dari murahnya harga perangkat system informasi yang ditawarkan serta kemudahan akses backdoor untuk negara-negara sekutu China. Meskipun Indonesia masih bergantung pada negara lain untuk menyediakan system pertahanan informasinya, namun dengan kerjasama dengan pemerintah China, Indonesia berharap dapat membangun system pertahanan elektronik untuk mengatasi terjadinya serangan-serangan elektronik dari negara lain.

Penulis Mohamad memilih menggunakan judul yang terkesan provokatif, yaitu "Sedap Menyadap Australia-Indonesia". Mohamad melihat bahwa kasus penyadapan presiden oleh pihak intelijen Australia merupakan hal yang lumrah terjadi di dunia intelijen. Terbongkarnya fakta bahwa telah terjadi penyadapan ini berkat Edward Snowden yang membocorkan data-data rahasia CIA yang menunjukkan bahwa pemerintahan Australia dibawah komando Perdana Menteri Australia pada saat itu Kevin Rudd melakukan penyadapan terhadap Presiden Indonesia Susilo Bambang Yudhoyono dan sembilan orang lain yang berada pada ring satu presiden. Hubungan Australia dan Indonesia pun merenggang yang berimbasnya pada dibatalkannya beberapa kerjasama di bidang militer. Mohamad menyayangkan lemahnya tingkat keamanan informasi negara sehingga Indonesia kecolongan. Meskipun aktivitas sadap menyadap menurut beberapa pejabat intelijen adalah hal yang biasa, namun Indonesia harus melakukan revitalisasi dan pembaharuan berbagai teknologi pertahanan

terutama di bidang informasi. Mantan Danjen Kopasus Prabowo Subianto menegaskan bahwa kegiatan sadap menyadap adalah hal yang lumrah, namun tetap harus diwaspadai terutama apabila menyangkut rahasia kenegaraan. Prabowo juga mengingatkan untuk tidak membahasa rahasia negara melalui medium yang mudah untuk dicegat arus informasinya seperti internet dan telepon.

Analisis Sosio Kultural

Kepentingan Nasional Negara Indonesia untuk dapat menjaga kedaulatan dan melindungi keutuhan wilayah serta keselamatan segenap bangsa dari ancaman baik dari dalam maupun luar negeri merupakan salah satu elemen pokok suatu negara. Kehandalan sistem pertahanan/ militer sampai saat ini diyakini sebagai kekuatan paling ampuh untuk melindungi seluruh kepentingan strategis tersebut. Indonesia dengan segala potensi yang dimiliki dari aspek kondisi geografi, demografi dan kekayaan resources menjadikannya sangat kuat sekaligus lemah (vulnerable) terhadap kemungkinan ancaman yang ada.

Anggapan bahwa spektrum ancaman yang paling memberi pengaruh terhadap pembentukan sistem pertahanan Negara selama ini adalah adanya ancaman nyata berupa kemungkinan kekuatan militer asing yang akan menyerang atau merebut kedaulatan wilayah Negara (Threat Based). Dengan semakin meningkatnya hubungan politik dan kerjasama antar Negara serta munculnya kestabilan karena perimbangan kekuatan (balance of power) dunia telah menghasilkan suatu analisa bahwa tidak akan ada ancaman nyata berupa agresi militer asing terhadap Indonesia dalam 10 hingga 15 tahun ke depan. Hasil analisa tersebut selanjutnya menimbulkan asumsi bahwa menambah kekuatan/ modernisasi bidang militer bukanlah hal yang penting.

Perkembangan ilmu pengetahuan dan teknologi militer dalam persenjataan dan mobilitas serta kebutuhan militer dalam melaksanakan peperangan, telah merubah spektrum ancaman, dari yang semula bersifat konvensional berupa ancaman kekuatan bersenjata militer asing dari luar negeri berubah menjadi multidimensional. Hal tersebut terjadi sebagai akibat pengaruh perkembangan penerapan teknologi informasi dan Alutsista dan sama sekali berbeda dengan ancaman peperangan pada generasi sebelumnya. Spektrum ancaman berkembang tidak hanya yang bersifat kasat mata berupa teknologi Alutsista tanpa awak dan teknologi Nano, tetapi juga yang tidak kasat mata berupa ancaman dunia maya (Cyber Threat), aksi kriminal lintas Negara (Transnational Crime) dan perang Hibrida (Hybrid Warfare).

Perkembangan lingkungan strategis dan kemajuan teknologi senjata di dunia membentuk suatu strategi perang, doktrin operasional dan taktik bertempur baru sesuai dengan konsep Revoluton in Military Affairs, dimana kecanggihan teknologi informasi/ komunikasi menggunakan satelit dan peningkatan kemampuan daya jangkau serta akurasi tembakan senjata yang semakin tinggi menjadikan pengendalian pasukan di lapangan dapat mencakup wilayah operasi yang lebih luas dengan pengerahan jumlah kekuatan pasukan lebih besar.

Penggunaan teknologi informasi saat ini sudah merambah setiap aspek kehidupan manusia. Teknologi tersebut tidak hanya digunakan dalam menunjang kebutuhan sederhana dalam kehidupan sehari-hari, namun juga diterapkan secara massive dalam bidang ekonomi, industri bahkan kemiliteran dengan implementasi yang sangat luas dan beragam. Dalam bidang militer kemajuan pesat teknologi informasi diaplikasikan dalam konsep Perang Informasi

(Information Warfare), yang selanjutnya menjadi landasan utama dan penting bagi pengembangan doktrin pertempuran masa depan. Dengan kata lain bahwa teknologi informasi telah memberi pengaruh signifikan terhadap terjadinya perubahan dalam strategi militer.

Sementara itu Davids Dickend, Direktur pusat kajian strategis Universitas Victoria di Wellington memiliki pandangan bahwa ada 4 faktor utama yang menjadi indikator yang mendukung terjadinya proses revolusi peperangan masa depan yaitu : 1) C4ISR (Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance). 2) Kerjasama antar matra, 3) Teknologi militer modern dan 4) Doktrin pertempuran modern. Kemampuan suatu Negara untuk mengoptimalkan aspek-aspek tersebut akan memberikan keunggulan dalam pembentukan Doktrin Militer/ pertempuran yang memadai dihadapkan dengan tantangan perang masa depan.

Kebutuhan Komando dan pengendalian. Dengan perkembangan tehnologi digital dan teknologi komunikasi yang sangat pesat, maka pengendalian pasukan dapat dilakukan secara langsung oleh pimpinan militer tertinggi dengan memanfaatkan sistem komunikasi digital, yang dapat ditanam pada peralatan militer, perlengkapan perorangan prajurit yang memungkinkan para jenderal dapat langsung melihat gerakan pasukan dilapangan. Para pimpinan tertinggi pasukan di Markas Besar dapat melakukan intervensi langsung terhadap pelaksanaan peperangan, melalui tele conference dan dapat memutuskan apa yang harus dilakukan oleh sebuah unit tempur, bahkan memutuskan untuk memberi perintah kepada perorangan prajurit. (Lemjiantek, Perang Masa Depan, 2011;)

Ancaman terbesar pada abad modern ini adalah Information Warfare. Ini

berkaitan dengan sistem informasi dan kemampuan yang berkaitan dengan diseminasi dan monopoli informasi. Di masa lalu militer memandang informasi hanya merupakan pendukung pertempuran. Di masa yang akan datang informasi tidak lagi merupakan fungsi pendukung tetapi sudah memegang peranan yang utama di dalam pertempuran. Teknologi informasi ini membantu unsur pimpinan/ komandan untuk melakukan pengintaian, pengamanan, pengolahan data dan komunikasi data, munisi, dan peralatan penentu posisi. (GPS-Global Positioning System).serta penentuan sasaran dengan akurat.

Space Warfare. Konsep ini lebih populer dikenal dengan nama Star Wars yang merupakan matra perang keempat yang memanfaatkan lingkungan angkasa luar. Jangan bayangkan peperangan dengan menggunakan kapal induk yang menggunakan laser yang mampu menghancurkan bintang, yang dimaksud dengan Star Wars disini mengacu pada kemajuan teknologi komunikasi terutama satelit memungkinkan space warfare terjadi. Dengan menggunakan satelit, dari ketinggian tertentu dapat memperbaiki dan memperluas pengintaian. Satelit juga dapat menyajikan data rinci sasaran dan menyediakan sistem navigasi, terutama kepada pasukan tempur, dan memberikan informasi tentang permukaan bumi.

Berbagai rekayasa model dan karakter perang masa depan mulai bermunculan sebagai akibat kemajuan teknologi yang turut didorong oleh munculnya globalisasi. Cyber Warfare (dunia maya) kini bahkan telah didudukkan sebagai matra perang kelima setelah darat, laut, udara, dan angkasa luar. Inovasi di bidang teknologi telah mengubah taktik dalam konflik di zaman modern dan membuat dunia maya menjadi medan perang terbaru. Banyak perangkat mutakhir telah dibuat untuk keperluan ini. Dibantu oleh kemajuan teknologi elektromagnetik

serta teknologi komunikasi dan informasi, sebuah bentuk pertempuran elektronik telah tercipta dan membuat pemerintahan berbagai negara melihat perang dunia maya sebagai ancaman terbesar di masa depan.

Kekuatan sebuah angkatan perang siber ditentukan oleh kemampuan serangan, pertahanan, serta ketergantungan suatu negara terhadap Internet. Dalam buku "Cyber War", pakar keamanan komputer asal AS dan profesor di Universitas Harvard Richard A. Clarke dan Robert A. Knake memetakan kekuatan negara-negara dalam menghadapi perang siber.

Amerika Serikat, meski punya kemampuan serangan yang baik, tidak punya kemampuan untuk memutuskan jaringan Internet saat diserang, mengingat sebagian terbesar jaringan Internet di negara ini dimiliki dan dioperasikan oleh swasta. Sebaliknya, China memiliki kemampuan memutus seluruh jaringan Internet di negaranya bila suatu saat diserang. Namun negara yang dinilai paling mampu bertahan jika terjadi perang dunia maya, menurut Clarke, adalah Korea Utara. Negara ini mampu memutus koneksi Internetnya dengan lebih mudah ketimbang China. Bisa dibilang Korea Utara tak akan mengalami kerugian akibat serangan siber musuh, karena tak ada infrastruktur kritikal seperti pembangkit listrik, jalur kereta, atau jalur pipa yang tersambung ke Internet.

Muhammad Salahuddien, Wakil Ketua Indonesia Security Incident Response Team on Internet Infrastructure known (Id-SIRTII) menyebutkan, perang siber di negeri ini juga bukanlah hal baru. Sebagaimana perang-perang siber lain yang mewarnai tensi politik dan hubungan antara Indonesia dengan negara-negara lainnya, Indonesia sudah mulai terlibat perang siber sejak satu dekade yang lalu--mulai dari perang siber dengan Portugal pada 1999, dengan

Australia, hingga cyberwar dengan Malaysia beberapa tahun terakhir.

Seiring dengan pertumbuhan Internet di Indonesia yang begitu cepat, dia percaya akan lebih banyak lagi infrastruktur strategis dan layanan publik yang akan semakin bergantung pada sistem informasi, teknologi, dan jaringan Internet, sehingga rentan terhadap serangan siber. Jika sudah begitu, dia mengingatkan, "Ancaman perang informasi dan serangan cyber akan semakin meningkat dan menjadi medan pertempuran utama di masa mendatang, termasuk di Indonesia.

Beberapa negara maju telah mengarahkan perhatian secara khusus kepada tren baru ancaman, yaitu Perang Hibrida (hybrid war). Perang Hibrida merupakan sebuah strategi militer yang memadukan antara perang konvensional, perang yang tidak teratur dan ancaman cyber warfare, baik berupa serangan nuklir, senjata biologi dan kimia, alat peledak improvisasi dan perang informasi. Demikian sepenggal amanat Panglima TNI Laksamana TNI Agus Suhartono, S.E., yang dibacakan oleh Kapuskes TNI Mayjen TNI dr. Dedy Achdiat Dasuki, S.p.M pada upacara 17 Februari 2013, bertempat di Mabes TNI Cilangkap Jakarta, Senin (18/2/2013).

Berbagai dinamika dan keriuhan dalam pengadaan alat utama sistim pertahanan selama tiga tahun belakangan ini, semakin memberikan kedewasaan peran bagi Militer. Kesungguhan pemerintah dalam menata pertahanan dan keamanan negara, tidak hanya diproyeksikan untuk menghadapi musuh dari luar, tetapi juga menyiapkan kemungkinan berkembangnya Perang Hibrida dan masalah terorisme di dalam negeri.

Lebih lanjut dikatakan bahwa, dalam menghadapi ancaman Perang

Hibrida, Militer harus mampu merespon dan segera beradaptasi dengan situasi yang berkembang agar dapat mengantisipasi serta mengatasinya secara lebih cepat dan tepat. sebagai contohnya, pengadaan pesawat tempur sergap yang sejalan dengan pengadaan pesawat Counter Insurgency (COIN) , guna mengantisipasi kemungkinan berkembangnya aksi terorisme.

Berkaitan dengan perkembangan tersebut, keterpaduan, koordinasi dan komunikasi antar matra dan dengan segenap institusi terkait, merupakan kata kunci yang paling penting. Semakin kuat keterpaduan dan koordinasi yang dilakukan, maka upaya yang ditempuh dalam mengatasi segala permasalahan di daerah akan semakin efektif, sebagaimana yang diamanatkan oleh Undang-Undang nomor 34 tahun 2004, dan dioperasionalkan sesuai instruksi Presiden nomor 2 tahun 2013, dalam penanganan gangguan keamanan secara terpadu, termasuk konflik sosial dan terorisme. (http://www.tandef.net/tni-harus-siap-hadapi-perang-hibrida)

Perkembangan ilmu pengetahuan dan teknologi saat ini tidaklah berhenti begitu saja. Masih banyak perang dalam artian denotatif dan konotatif yang menjadi motivasi para peneliti untuk terus mengembangkan ilmu pengetahuan dan teknologi (dan memang nature peneliti itu harus terus berkreatifitas membuat inovasi-inovasi baru di bidang teknologi). Satu inovasi yang relatif baru adalah penggunaan mahluk hidup sebagai media pembawa peralatan canggih.

Sebuah artikel tahun 2007 yang dimuat di Washington Post mengindikasikan bahwa teknologi mata-mata kecil ini sudah digarap para ilmuwan di Amerika Serikat sejak beberapa tahun terakhir ini. Ternyata, DARPA (Defense

Advanced Research Projects Agency) sendiri membuat satu inovasi yang berbeda melalui proyek The Hybrid Insect Micro-Electro-Mechanical Systems, atau gabungan sistem elektrik dan mekanik berukuran sangat kecil (mikro), yang tujuannya saya terjemahkan dari teks aslinya: "Membuat serangga pengangkut (kamera) yang memiliki saraf-saraf yang tumbuh dalam chip silikon internal, sehingga pengendali (manusia) dapat mengendalikan aktivitas mereka".

Jelas bahwa inovasi ini mengusung teknologi neurocybernetics, yaitu teknologi komunikasi yang biasanya diaplikasikan ke dalam sistem mekanik dan elektrik, dengan menggunakan saraf mahluk hidup sungguhan. Bidang ilmu cybernetics sendiri biasanya hanya melakukan peniruan terhadap cara berkomunikasi pada saraf-saraf mahluk hidup, jadi tidak melakukan komunikasi menggunakan saraf mahluk hidup.

Sedangkan neurocybernetics melakukan hal yang lebih "gila", yaitu dengan menggunakan saraf mahluk hidup sebagai jalur komunikasi.

KESIMPULAN

Berdasarkan analisis diatas dan hasil penelitian didapatkan bahwa isu cyberwar yang ditampilkan pada artikel di Kompasiana merupakan isu yang cukup baru sehingga muncul macam-macam pandangan *netizen* terhadap isu *cyberwar* ini. Konsep-konsep yang diartikulasikan pada artikel-artikel tersebut bertujuan untuk membuat *summary* kondisi geopolitik antar negara. Konsep *cyberwar* dipandang sebagai salah satu instrumen perang zaman modern, dimana pemerintahan suatu negara dan agresi. Dengan semakin terkoneksinya manusia dengan internet, maka semakin rentan pula masyarakat, korporasi, dan negara

untuk terkena serangan-serangan cyber. Berbeda dengan serangan militer konvensional, serangan-serangan cyber yang terjadi tidak bisa dideteksi secara *preemptive,* sehingga yang bisa dilakukan adalah *cyber deterrence*. Tindakan mempersuasi atau mengancam musuh potensial yang dicurigai akan melancarkan *cyberwar* ini dapat dapat menyerang negara lainnya tanpa harus mengerahkan kekuatan militer konvensional. Konsep *cyberwar* merupakan produk dari teknologi yang merevolusi definisi perang dikategorikan sebagai salah satu bentuk hegemoni dan *coercion.*

DAFTAR PUSTAKA
Buku :

Arquilla, J. (1993). *Cyberwar is Coming!* New York: National Security Research Division.

Clarke, R. A. (2010). *Cyberwar: The Next Threat to National Security and What to Do About It* . New York: Harper-Collins.

Collin, F. (1997). *Social Construction.* New York: Routledge.

Gordon, C. (1980). *Power/Knowledge: Selected Interviews and Other Writings 1972-1977.* New York: Pantheon Books.

Ida, R. (2011). *Metode Penelitan Kajian Media dan Budaya.* Surabaya: LP3 UNAIR.

Lister, M., Dovey, J., Giddings, S., Grant, I., & Kelly, K. (2003). *New Media: A Critical Introduction.* London: Routledge.

Jurnal :

Beidleman, S. W. (2009). Defining and Deterring Cyberwar. *USAWC Strategy Research Project* .

Billo, C., & Chang, W. (2004). *Cyber Warfare : An Analysis of the Means and Motivations of Selected Nation States.* Hanover: Institute for Security Technology Studies at Dartmouth College.

Conway, M. (2008). Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures. *Working Papers in International Studies Centre for International Studies Dublin City University* .

Dunlap, C. J. (2012). *The Intersection of Law and Ethics in Cyberwar.*

Sharma, A. *Cyber Wars : A Paradigm Shift from Means to Ends.* Institute for System Studies and Analysis, Defence Research and Development Organization.

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy* .

Stevens, T. (2012). *On Information Warfare: A Response to Taddeo.* London: King's College.

Tabansky, L. (2011). Basic Concepts in Cyber Warfare. *Military and Strategic Affairs , 3* (1), 1-18

Website / Blog :

Ronfeldt, D. (2012). *http://twotheories.blogspot.com/2012/03/miscellany-cyber-war-isnt-same-as.html*. Retrieved April 21, 2013

Singel, R. (2010). *http://www.wired.com/threatlevel/2010/04/cyberwar-richard-clarke/*. Retrieved 2013

Wallace, I. (2013). *http://www.thedailybeast.com/articles/2013/03/10/why-the-u-s-is-not-in-a-cyber-war.html?utm_medium=referral&utm_source=pulsenews*. Retrieved 2013

http://politik.kompasiana.com/2013/11/25/tak-sepantasnya-lembek-di-depan-australia-614015.html

http://www.infoplease.com/world/events/cyberwar-timeline.html#ixzz3JyISvZcP