P-ISSN 1410-3648 E-ISSN 2406-7385
Kajian Masalah Hukum dan Pembangunan

PERSPEKTIF

DAFTAR ISI

VOLUME XXI NOMOR 3 TAHUN 2016 EDISI SEPTEMBER
Terbit 3 (Tiga) Kali: Januari, Mei, September

Penerbit:

Lembaga Penelitian dan Pengabdian Masyarakat (LPPM)
Universitas Wijaya Kusuma Surabaya

PUBLISH OR PERISH

Alamat Dewan Redaksi:

Jurnal ***PERSPEKTIF*** Fakultas Hukum Universitas Wijaya Kusuma Surabaya Gedung A Lantai 1
Jl. Dukuh Kupang XXV/54 Surabaya 60225 Telp. (031) 5677577 Pesawat 152 Fax: (031) 5679791
e-mail: perspektif_hukum@yahoo.com *Homepage*: http://jurnal-perspektif.org

REKONSTRUKSI PEMBENTUKAN *NATIONAL CYBER DEFENSE* SEBAGAI UPAYA MEMPERTAHANKAN KEDAULATAN NEGARA

Nur Khalimatus Sa'diyah
Fakultas Hukum Universitas Wijaya Kusuma Surabaya
e-mail: nurkhalimatus@yahoo.com

Ria Tri Vinata
Fakultas Hukum Universitas Wijaya Kusuma Surabaya
e-mail: riatrivinata@yahoo.com

ABSTRAK

Kecemasan terhadap *cyber crime* telah menjadi perhatian dunia, namun tidak semua negara di dunia ini memberikan perhatian yang lebih besar terhadap masalah *cyber crime* dan memiliki peraturannya kecuali negara-negara maju dan beberapa negara berkembang. Tujuan penelitian ini adalah dalam rangka menemukan, mengkaji dan menganalisa upaya pemerintah Indonesia dalam perlindungan terhadap data informasi rahasia negara dan meneliti tentang bentuk-bentuk perlawanan pemerintahan Indonesia terhadap *cyber war*. Menemukan rekonstruksi pembentukan *national cyber defense* atau *cyber army* dalam upaya mempertahankan kedaulatan negara. Dalam UU No. 3 Tahun 2002 tentang Pertahanan Negara, telah ditetapkan bahwa ancaman dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non militer, termasuk diantaranya ancaman siber. Salah satu efek samping negatif dari perkembangan dunia siber melalui internet antara lain adalah kejahatan dalam bentuk pelanggaran hukum atau *cyber crime*, di mana bila eskalasinya lebih meluas dapat mengancam kedaulatan negara, keutuhan wilayah maupun keselamatan bangsa. Sebagai upaya penanggulangan terhadap serangan-serangan di dunia maya ini, diperlukanlah sebuah lembaga yang bertugas menjadi benteng pertahanan dunia siber atau *cyber defense*.

Kata Kunci: pembentukan, *cyber defense*, kedaulatan negara.

ABSTRACT

Anxiety against cybercrime has become the world's attention, but not all countries in the world is giving greater attention to the problem of cybercrime by having the rule and unless the developed countries and some developing countries. The purpose of this research is in order to find, examine and analyze the efforts of the Indonesia Government in the protection of State secrets information and data, also to research the forms of Indonesia Government resistance against cyber war. Find a reconstruction of national cyber defense formation or cyber army in an attempt to defend the sovereignty of the country. In Act No. 3 of 2002 on State Defense, it has been established that the threat in the country's defense system consists of a military threat and non-military threat, which is including cyber threats. One of the negative effects of the cyber world development via the internet among other things is a crime in violation of the law cybercrime, where when the escalation widely spread, it could have threatened the country's sovereignty, territorial integrity or the safety of the nation. In an effort to combat against the attacks in this virtual world, will require an agency that is in charge of being the world's bulwark cyber or cyber defense.

Keywords: *formation, cyber defense, sovereignty.*

PENDAHULUAN

Negara Indonesia telah mengalami beberapa kejadian *cyber war* Serupa berikut ini beberapa contoh kasus yang penah terjadi di Indonesia, yaitu:[1] *Pertama*, Sejak 1998, Indonesia telah melakukan *cyber war* dengan negara lain, hal itu terkait masalah politik dan sosial yang terjadi, misalnya ketika terjadi kerusuhan rasial, Indonesia berperang di dunia maya dengan para *hacker* dari China dan Taiwan. *Kedua*, Sementara pada 1999 juga muncul kerusuhan di dunia maya antara Indonesia dan Portugal menyangkut kasus Timor Timur. Bahkan ketika terjadi *cyber war* dengan Portugal, saling serang terjadi hingga masuk sistem dan mampu menghapus semua data. *Ketiga*, Pada tanggal 6 Agustus 2010, Symantec sebagai produsen Antivirus Norton, mengumumkan bahwa Indonesia berada di urutan kedua setelah Iran di antara 10 negara yang mengalami serangan *worm* Stuxnet.[2] Peristiwa ini pun diduga dilakukan oleh Israel dan Amerika Serikat sebagai penentang utama Program Nuklir Iran. *Keempat*, Dalam beberapa tahun terakhir juga terjadi perang siber antara Indonesia dengan Malaysia. Saling susup antara hacker kedua negara mewarnai perseteruan ini. Aksi ini biasanya terjadi ketika muncul konflik politik ataupun persaingan kedua negara. Meskipun tidak melibatkan pemerintah kedua negara, namun aksi para *hacker* ini menyerang fasilitas siber milik pemerintah Malaysia maupun Indonesia. *Kelima*, Insiden penyalahgunaan gedung perwakilan diplomatik Australia terhadap penyadapan Kepala Negara Republik Indonesia yang menyebutkan Kedutaan Besar Australia di Jakarta menjadi lokasi penyadapan terhadap pemerintah Indonesia berdasarkan informasi dari Media Internasional *Sydney Morning Herald* 31 Oktober 2013.[3]

Pemerintah perlu bekerjasama dengan pihak-pihak maupun negara lain untuk membangun keamanan global. Satu negara tidak akan mungkin dapat membuat perlindungan terhadap dirinya sendiri dalam menghadapi ancaman global tersebut. Kerja sama antar negara diharapkan juga mampu mencetuskan sebuah regulasi di bidang siber atau *cyber law* yang lebih kuat dan memberi efek global. Dengan adanya *cyber law* yang tegas di dunia internasional tersebut kiranya mampu mengurangi maraknya kejahatan di dunia siber. Sebelum hal tersebut dilaksanakan akan lebih bijak apabila Indonesia melakukan tata ulang di dalam penguasaan teknologi serta pembuatan undang-undang spesifik mengenai ancaman siber.

Beberapa negara sudah memiliki unit khusus pasukan siber dalam pertahanan dan keamanan negaranya. Badan ataupun organisasi tersebut bertugas menghimpun segala usaha pertahanan dan serangan balik terhadap keamanan di dunia siber beserta sistem jaringannya. Melihat kekuatan dan ancaman yang dapat terjadi akibat kemajuan teknologi informasi, banyak negara mulai membangun kekuatan angkatan perang siber. Sebab perang ini bukan lagi sekadar *game virtual* dan cerita fiksi, tapi sudah menjadi bagian dari percaturan dunia. Dari uraian latar belakang, maka dapat dilakukan penelitian tentang Bagaimana upaya yang dilakukan pemerintahan Indonesia dalam perlindungan terhadap data informasi rahasia negara dan perlawanan terhadap *cyber war,* dan Upaya rekonstruksi pembentukan *national cyber defense* atau *cyber army* dalam upaya mempertahankan kedaulatan negara.

METODE PENELITIAN

Metode Penelitian yang digunakan dalam penelitian ini normatif-empiris yang bersifat diskriptif, penelitian normatif diartikan sebagai penelitian yang mencakup ilmu kaidah dan ilmu pengertian atau yang biasanya disebut ilmu dogmatik hukum atau *normwissenschacf*.[4] Penelitian hukum empiris adalah jenis penelitian yang dilakukan terutama dengan cara meneliti data primer. Penelitian ini mengkaji dan mengolah data penelitian dengan menelusuri upaya-upaya yang dilakukan oleh pemerintah Indonesia memberikan perlindungan terhadap data informasi rahasia negara dan faktor-faktor penghambatnya serta

[1] Reda Manthovani, *Problematika dan Solusi Penanganan Kejahatan CYBER di Indonesia,* Malibu, Jakarta, 2006, h. 67-68.

[2] Stuxnet adalah *worm* yang khusus menyerang komputer berbasis operasi Windows. Pada tanggal 20 dan 23 Nopember 2010 pihak militer Iran telah secara resmi menyatakan bahwa *worm* Stuxnet menyerang Natanz (fasilitas nuklir Iran). *Worm* ini bahkan berhasil me-*remote* ledakan berbahaya di pusat pengayaan uraninum negara pengembang nuklir tersebut.

[3] Penyadapan Australia terhadap Indonesia diinformasikan dan disebarluaskan di media internasional oleh mantan mata-mata Amerika Serikat Edward Snowden yang menyebutkan informasi dokumen rahasia tersebut ke *Australian Broadcasting Corporation* (ABC) dan surat kabar *The Guardian* Sandro Gatra, 2014, *"Code of Conduct" Ditandatangani, Indonesia-Australia Sepakat Tak Menyadap",* URL: http://nasional.kompas.com/read/2014/08/28/17412271 diunduh Sabtu 25 Oktober 2014.

[4] *Ibid*.

upaya pemerintahan Indonesia dalam melawan *cyber war*, sebagai upaya mempertahankan kedaulatan Negara Kesatuan Republik Indonesia. Pada penelitian hukum normatif ada kemungkinan kaedah hukum itu terhimpun dalam suatu kodifikasi atau bahan tertulis lainnya. Berbeda dengan penelitian normatif dalam penelitian empiris akan mengaitkan hukum pada usaha untuk mencapai tujuan-tujuan serta kebutuhan konkrit di dalam masyarakat. Penelitian ini bersifat diskriptif artinya melalui hasil penelitian yang diharapkan akan diperoleh gambaran yang menyeluruh dan sistematis mengenai upaya-upaya apa saja yang telah dilakukan pemerintah Indonesia memberikan perlindungan terhadap data informasi rahasia negara dan faktor-faktor penghambatnya serta upaya pemerintahan Indonesia dalam melawan *cyber war* dan Rekonstruksi pembentukan *National Cyber Defence* atau *Cyber Army* sebagai tanggung jawab Indonesia untuk mempertahankan kedaulatan negara.

PEMBAHASAN

Konsep Keamanan *Cyber*

Ancaman dan gangguan bagi kedaulatan negara, keselamatan bangsa, dan keutuhan wilayah sangat terkait dengan bentang dan posisi geografis yang sangat strategis, kekayaan alam yang melimpah, serta belum tuntasnya pembangunan karakter dan kebangsaan, terutama pemahaman mengenai masalah multikulturalisme, sementara itu kemampuan pertahanan dan keamanan saat ini dihadapkan pada situasi kekurangan jumlah dan ketidaksiapan alutsista dan alat utama lainnya yang jika tidak dilakukan upaya percepatan penggantian, peningkatan, dan penguatan akan menyulitkan penegakan kedaulatan negara, penyelamatan bangsa, dan penjagaan keutuhan wilayah di masa mendatang.[5] Keadaan tersebut diperburuk oleh terjadinya kelemahan sistemik komponen cadangan dan pendukung pertahanan yang merupakan prasyarat berfungsinya sistem pertahanan semesta.[6]

Arus globalisasi yang terjadi di seluruh dunia sekarang ini telah membawa dunia pada era perkembangan teknologi informasi dan komunikasi sehingga menciptakan era yang serba digital atau *digital world*. Dalam hal ini, perkembangan teknologi komputer dan internet menjadi sarana baru bagi negara-negara di dunia untuk dimanfaatkan sebagai alat untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai negara sehingga sangat mendorong dunia pada perkembangan yang kompleks, beragam dan majemuk.[7]

Melalui globalisasi, maka setiap negara dapat lalu lalang melintasi negara yang satu dengan negara yang lain tanpa ada kendali dan kontrol negara yang dominan.[8] Masing-masing negara melakukan ekspansi ekonomi, ekspansi sosial dan ekspansi budaya sehingga terjadilah perang ekonomi, perang sosial, dan perang budaya, perang ideologi dan perang pemikiran. Atas nama globalisasi, perdagangan bebas, dan pasar bebas, maka setiap negara berebut pengaruh untuk mencari sumber-sumber daya alam, pangan dan energi sehingga terjadilah konflik energi, konflik pangan dan konflik air di berbagai belahan dunia.[9]

Keamanan *cyber* mengacu pada keamanan informasi digital yang disimpan di jaringan elektronik, serta keamanan jaringan yang menyimpan dan mengirimkan informasi. Namun, ada sedikit pengertian tentang bagaimana sebenarnya itu didefinisikan. Keamanan cyber kadang-kadang digunakan bergantian dengan keamanan informasi.[10] Keamanan Informasi dan *cyber* pada umumnya merujuk untuk hal yang sama. Namun, keamanan informasi digunakan oleh organisasi dan TI profesional, sementara keamanan *cyber* lebih umum digunakan dalam kebijakan, dan ketika masalah keamanan informasi terbentuk sebagai masalah keamanan nasional.[11]

Definisi tersebut sedikit lebih luas dari keamanan informasi, bukan hanya melindungi sistem

---

[5] *Ancaman Cyber Insider,* M Akbar Marwan http://akbar.staff.gunadarma.ac.id

[6] Yoko Iwama, *International Donors and the Reform of Indonesian National Police*, Workshop 2010: Organizing Police Forces in Post-Conflict Peace-Support Operations, January 27-28th, 2010.

[7] Adi Joko Purwanto, "Peningkatan Anggaran Militer Cina dan Implikasinya terhadap Keamanan di Asia Timur", *SPEKTRUM Jurnal Ilmu Politik Hubungan Internasional*, Vol. 7, Juni 2010.

[8] *Ibid.*

[9] Noorhaidi Hasan dan Bertus Hendriks, *Counter-Terrorism Strategies in Indonesia, Algeria and Saudi Arabia,* Netherlands Institute of International Relations 'Clingendae.

[10] Perlindungan informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan dalam rangka memberikan kerahasiaan, integritas, dan ketersediaan.

[11] William S. Lind, "Understanding Fourth Generation War", *Military Review*, September-October 2004, http://www.au.af.mil/au/awc/awcgate/milreview/lind.pdf

informasi, tapi juga melindungi ruang *cyber* dan aset internet pengguna. Hal ini mengacu bukan hanya mengamankan sistem informasi, tetapi juga untuk penggunaan sistem informasi untuk mengamankan aset. Ketika keamanan *cyber* dibingkai sebagai masalah keamanan nasional, isu-isu mengenai teknologi dan internet akan diamankan dibawa ke dalam agenda keamanan negara. Keamanan *cyber* juga dapat digunakan untuk melindungi rahasia negara, dan mengkriminalisasi pelapor sebagai ancaman keamanan *cyber*. Masyarakat sipil dapat terpinggirkan sebagai akibat dari ini. Berfokus pada negara dan keamanan, mendesak pertimbangan untuk keamanan individu warga negara, dengan merugikan keamanan seluruh sistem.[12]

Konsep dari *Cybersecurity Mindset* atau pola pikir keamanan *cyber*, yang ditegaskan oleh William Dutton, menyatakan bahwa:[13] Sebagai pola pikir, kebutuhan akan keamanan akan tidak dipertanyakan atau tidak terus menerus ditinjau kembali. Ini akan dilihat bukan sebagai beban opsional, tetapi sebagai biaya melakukan bisnis. Untuk pengguna, itu tidak akan menjadi kriteria adhoc pilihan, tapi rutinitas dan dipelajari sebagai kumpulan respon yang hampir *instingtual*.[14]

Kode etik dalam penggunaan yang aman dari internet harus menjadi akrab dengan pengguna *web*. Tindakan yang mudah seperti otentikasi identitas dalam jaringan, *surfing* internet dengan aman, pemberitahuan tentang *spam*, atau melengkapi perangkat internet dengan program anti *malware* yang telah diperbarui mungkin bisa menjadi perlindungan yang efektif. Namun, banyak pengguna yang masih belum tahu tentang pentingnya mencegah dan mengurangi risiko *cyber* yang bahaya.[15]

Dalam *Cyber Warfare*, terdapat metode penyerangan yang tentunya berbeda dengan perang klasik, perang konvensional atau perang fisik lainnya. Domain dari *Cyber Warfare* berada dalam dunia maya, di mana yang menyerang adalah orang yang ahli teknologi informasi yang tidak harus datang langsung ke negara yang diserang. Wilayah yang diserang juga bukan wilayah fisik, wilayah teritorial, atau wilayah geografis, melainkan wilayah dunia maya.[16] Medan peperangan yang umum terjadi dalam perang fisik adalah perang di darat, perang di laut, perang di udara, dan perang di ruang angkasa. Namun, untuk perang *cyber* wilayahnya di dunia maya.

Berikut ini adalah metode penyerangan dalam *cyber warfare:*[17] *Pertama*, Pengumpulan Informasi. *Spionase cyber* merupakan bentuk aksi pengumpulan informasi bersifat rahasia dan sensitif dari individu, pesaing, rival, kelompok lain pemerintah dan musuh baik di bidang militer, politik, maupun ekonomi. Metode yang digunakan dengan cara eksploitasi secara ilegal melalui internet, jaringan, perangkat lunak dan atau komputer negara lain. Informasi rahasia yang tidak ditangani dengan keamanan menjadi sasaran untuk dicegat dan bahkan di ubah. *Kedua*, *Vandalism.* Serangan yang dilakukan sering dimaksudkan untuk merusak halaman *web* atau *Deface*, atau menggunakan serangan *denial of service* yaitu merusak sumber daya dari komputer lain. Dalam banyak kasus, hal ini dapat dengan mudah dikembalikan. *Deface* sering dalam bentuk propaganda. Selain penargetan situs dengan propaganda, pesan politik dapat didistribusikan melalui internet via *e-mail*, *instant mesages* atau pesan teks. *Ketiga*, *Sabotase* merupakan kegiatan militer yang menggunakan komputer dan satelit untuk mengetahui koordinat lokasi dari peralatan musuh yang memiliki resiko tinggi jika mengalami gangguan. Sabotase dapat berupa penyadapan Informasi dan gangguan peralatan komunikasi sehingga sumber energi, air, bahan bakar, komunikasi, dan infrastruktur transportasi semua menjadi rentan terhadap gangguan. Sabotase dapat berupa *software* berbahaya yang tersembunyi dalam *hardware* komputer. Keempat, Serangan pada jaringan listrik, bentuk serangan dapat berupa pemadaman jaringan listrik sehingga bisa

[12] J. Aioro, *Defense Lacks Doctrine to Guide it Through Cyberwarfare*, 13 September 2010, http://www.nextgov.com/defense/2010/09/defense-lacksdoctrine-to-guide-it-through-cyberwarfare/47575/

[13] Elizabeth Montabalno, *Auditor Find Dod Hasn't Defined Cyber Warfare*, September 2010, http://www.informationweek.com/government/security/auditorsfind-dod-hasnt-defined-cyber-wa/227400359.

[14] Ide ini merupakan peralihan penting untuk pendekatan yang lebih berorientasi pada pengguna untuk praktik keamanan *cyber*. Perspektif ini sesuai juga dengan adagium yang mengatakan bahwa cara terbaik untuk melindungi hak-hak rakyat adalah memungkinkan orang untuk melindungi hak-hak mereka sendiri.

[15] Frank G. Hoffman, *Conflict in the 21st Century, The Rise of Hybrid Wars*, Patomatic Institute, Virginia USA, Desember 2007, h. 35.

[16] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, 1999.

[17] Michael Evans, "From Kadesh to Kandahar: Military theory and the furute of war," *Naval War College Review*, Summer 2003, h. 136.

mengganggu perekonomian, mengalihkan perhatian terhadap serangan militer lawan yang berlangsung secara simultan, atau mengakibatkan trauma nasional. Serangan dilakukan menggunakan program sejenis *trojan horse* untuk mengendalikan infrastruktur kelistrikan.

Konsep Pertahanan Negara

Pertahanan negara meruapakan usaha untuk menegakkan kedaulatan, keutuhan dan keselamatan segenap bangsa dari ancaman dan gangguan. Usaha pertahanan negara dilakukan dengan mempertimbangkan adanya dinamika perkembangan lingkungan strategis yang dihadapi.[18] Perkembangan lingkungan strategis senantiasa membawa perubahan terhadap kompleksitas ancaman, baik ancaman militer maupun ancaman non militer. Pertahanan negara berfungsi untuk mewujudkan dan mempertahankan seluruh wilayah Negara Kesatuan Republik Indonesia (selanjutnya disingkat NKRI) sebagai satu kesatuan pertahanan. Pertahanan negara Indonesia diselenggarakan dalam suatu sistem pertahanan semesta yang melibatkan seluruh warga negara, wilayah, serta segenap sumber daya nasional yang dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut.[19] Dalam pengelolaan sistem pertahanan negara, Presiden menetapkan Kebijakan Umum Pertahanan Negara yang menjadi acuan bagi perencanaan penyelenggaraan dan pengawasan sistem pertahanan negara.

Kebijakan Umum Pertahanan Negara berlaku lima tahun dimulai dari awal Presiden menjabat. Kebijakan Umum Pertahanan Negara merupakan upaya membangun, memelihara, dan mengembangkan secara terpadu dan terarah segenap komponen pertahanan negara. Kebijakan Umum Pertahanan Negara dijadikan sebagai dasar oleh Kementerian Pertahanan dalam menetapkan Kebijakan Penyelenggaraan Pertahanan Negara. Kebijakan Umum Pertahanan Negara juga dijadikan dasar Kementerian/Lembaga Pemerintah non Kementerian dalam menetapkan kebijakan sesuai wewenang dan tanggung jawab serta fungsi masing-masing terkait bidang pertahanan. Kebijakan Penyelenggaran Pertahanan Negara dijabarkan menjadi kebijakan pertahanan negara untuk setiap tahun. Kebijakan Penyelenggaran Pertahanan Negara menjadi dasar dalam penyusunan Kebijakan Pertahanan Negara Tahun 2014. Kebijakan Pertahanan Negara Tahun 2014 menjadi pedoman bagi Kementerian Pertahanan dan Tentara Nasional Indonesia (yang selanjutnya disebut dengan TNI) dalam penyelenggaraan pertahanan sesuai dengan fungsinya masing masing.

Perubahan geopolitik internasional yang ditandai dengan memudarnya prinsip multilateralisme dan menguatnya pendekatan unilateralisme yang berdampak pada berkembangnya doktrin pertahanan *preemptive strike* akan mengubah sama sekali tataran politik internasional dan dapat menembus batas-batas yurisdiksi sebuah negara di luar kewajaran hukum internasional yang berlaku saat ini. Selain itu, menguatnya kemampuan militer negara tetangga yang secara signifikan melebihi kemampuan pertahanan Republik Indonesia telah melemahkan posisi tawar dalam ajang diplomasi internasional.[20]

Potensi dan ancaman konflik berintensitas rendah yang didukung dengan perkembangan metode dan alat teknologi tinggi diperkirakan akan makin meningkat pada masa mendatang. Potensi dan ancaman tersebut adalah terorisme, konflik komunal, kejahatan transnasional, kejahatan terhadap kekayaan negara terutama di wilayah yurisdiksi laut Indonesia dan wilayah perbatasan, serta berkembangnya variasi tindak kriminal konvensional. Tantangan lain dalam pembangunan pertahanan dan keamanan adalah meningkatkan profesionalisme Polri seiring dengan peningkatan kesejahteraan anggotanya agar mampu melindungi dan mengayomi masyarakat, mencegah tindak kejahatan, menuntaskan tindak kriminalitas, serta meningkatkan profesionalisme TNI seiring dengan peningkatan kesejahteraan prajurit serta penguatan kapasitas lembaga intelijen dan kontra intelijen dalam rangka menciptakan keamanan nasional.[21]

Pokok-Pokok Kebijakan Penyelenggaraan Pertahanan Negara disusun dalam rangka menjabarkan Kebijakan Umum Pertahanan Negara

[18] John Arquilla dan David Rondfelt, *Networks and Netwars*, *The Future of Terror, Crime, and Militancy*, Rand Corporation, 2001.

[19] Petri Huovinen, *Hybrid Warfare-Just a Twist of Compound Warfare*, views on Warfare from the United States Armed Forces Perspective, h. 8.

[20] Manuel W. Wik, *Revolution in Information Affairs Tactical and Strategic Implication of Information Warfare and Information Operation*, Defence Materiel Administration, hal. 27, diakses 12 Juni 2016, pada <mawik@fmv.se>

[21] *Ibid.*

yang meliputi: *Pertama,* Kebijakan Pertahanan Integratif Implementasi dari Kebijakan Pertahanan Integratif meliputi Percepatan Proses Legislasi Bidang Pertahanan, Pengintegrasian Komponen Pertahanan Negara, Perumusan Doktrin Pertahanan Nirmiliter dan Pembentukan Instansi Vertikal Kementerian Pertahanan di Daerah. *Kedua,* Kebijakan Pengelolaan dan Pendayagunaan Sumber Daya Nasional Pengelolaan sistem pertahanan negara disiapkan sejak dini melalui Pemberdayaan Wilayah Pertahanan diwujudkan dalam transformasi sumber daya nasional untuk menjadi kekuatan pertahanan negara, penyiapan komponen cadangan melalui pelatihan dasar kemiliteran secara wajib dan penyiapan komponen pendukung melalui kesadaran bela negara. *Ketiga,* Kebijakan Pembangunan Postur Pertahanan Militer Prioritas dan fokus pengembangan postur pertahanan militer diarahkan pada Kekuatan Pokok Minimum atau *Minimum Essential Force* (MEF) TNI melalui Rematerialisasi; Revitalisasi; Relokasi; dan Pengadaan dalam meningkatkan kemampuan mobilitas dan kemampuan satuan tempur TNI AD, TNI AL, dan TNI AU, khususnya Pasukan Pemukul Reaksi Cepat (PPRC), menyiapkan Pasukan Reaksi Cepat Penanggulangan Bencana (PRCPB), menyiapkan *Peace Keeping Operation* (PKO) dan menyiapkan Batalyon mekanis sebagai pasukan siaga (*standby force*). *Keempat,* Kebijakan Pemberdayaan Pertahanan Nirmiliter, Pertahanan Nirmiliter pada hakikatnya adalah bentuk peran serta rakyat dan segenap sumber daya nasional dalam pertahanan negara, baik sebagai unsur utama dan unsur lainnya untuk menghadapi ancaman nonmiliter yang dalam keadaan damai sebagai fungsi pertahanan sipil yang dilaksanakan melalui kebijakan strategis pertahanan nirmiliter, kebijakan pemberdayaan pertahanan nirmiliter, kebijakan penanganan ancaman nonmiliter dan melaksanakan koordinasi lintas sektoral. *Kelima,* Kebijakan Pengerahan Kekuatan Pertahanan Militer TNI sebagai komponen utama melaksanakan tugas operasi militer untuk perang dan operasi militer selain perang dan tidak hanya digunakan dalam menghadapi ancaman militer tetapi juga digunakan untuk membantu dalam menghadapi ancaman nonmiliter, maka kebijakan umum penggunaan kekuatan TNI meliputi penggunaan kekuatan TNI pada operasi militer untuk perang untuk menghadapi ancaman militer dan pada operasi militer selain perang sebagai unsur lainnya dalam menghadapi ancaman nonmiliter serta pengerahan kekuatan TNI diarahkan untuk merespon ancaman aktual. *Keenam,* Kebijakan Kerja Sama Internasional Bidang Pertahanan Semua bentuk kerjasama dilaksanakan dengan prinsip *one gate policy* dan menghindari pembentukan suatu pakta pertahanan. Kebijakan kerja sama diarahkan kepada negara-negara tetangga yang berbatasan langsung, dengan negara-negara sahabat pada pengembangan kemampuan atau *capacity building*. Mewujudkan ASEAN *Security Community* dan Peningkatan peran aktif dalam *Peacekeeping Operation* (PKO). *Ketujuh,* Kebijakan ilmu pengetahuan, teknologi dan Industri Pertahanan Pesatnya penggunaan Teknologi, Informasi dan Komunikasi (TIK) sebagai sarana dalam perang informasi, maka diperlukan *cyber defence* sebagai strategi pertahanan negara baik dalam mencegah, menangkal maupun mengatasi ancaman *cyber*. Percepatan penguasaan Ilmu Pengetahuan dan Teknologi (Iptek) juga akan memberikan kepastian terwujudnya kemandirian Industri Pertahanan (Indhan) melalui pemberdayaan Indhan dalam negeri yang dilakukan dengan program revitalisasi Indhan serta melibatkan perguruan tinggi, lembaga penelitian dan pengembangan, industri, dan TNI sebagai pengguna. *Kedelapan,* Kebijakan Pengamanan Wilayah Perbatasan dan Pulau-Pulau kecil terluar Pengamanan wilayah perbatasan merupakan satu kesatuan antara fungsi pemerintah (Kementerian/ Lembaga terkait) dan pelaksanaan tugas pokok TNI. Pemerintah menetapkan kebijakan pengamanan wilayah perbatasan dan TNI melaksanakan kebijakan yang diarahkan pada pembangunan wilayah perbatasan dilaksanakan oleh Pemda, TNI bekerjasama dengan Kementerian Pertahanan memperkuat fungsi dan kewenangan BNPP sebagai pemegang otoritas pengelolaan batas wilayah negara dan pembangunan kawasan perbatasan, serta pulau-pulau kecil terluar, mempercepat pembangunan kawasan perbatasan, mengintensifkan perundingan-perundingan perbatasan dan diplomasi internasional mengenai wilayah dan batas wilayah Indonesia.

Kebijakan Umum Pertahanan Negara disusun sebagai satu kesatuan arah kebijakan yang meliputi Kebijakan Pertahanan Integratif, Kebijakan Pengelolaan dan Pendayagunaan Sumber Daya Nasional, Kebijakan Pembangunan Postur Pertahanan Militer, Kebijakan Pemberdayaan Pertahanan Nirmiliter, Kebijakan Pengerahan Kekuatan Pertahanan Militer, Kebijakan Kerja Sama

Internasional Bidang Pertahanan, Kebijakan Ilmu Pengetahuan Teknologi dan Industri Pertahanan, Kebijakan Pengamanan Wilayah Perbatasan dan Pulau-Pulau Kecil Terluar, Kebijakan Penganggaran, dan Kebijakan Pengawasan.

Pertahanan dan keamanan negara merupakan salah satu objek yang mendapatkan pengaturan secara tegas dalam konstitusi Negara Kesatuan Republik Indonesia. Dalam Bab XII Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 terdapat pengaturan terkait dengan pertahanan negara yakni pada Pasal 30 ayat (2) yang berbunyi bahwa: Usaha pertahanan dan keamanan negara dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta oleh Tentara Nasional Indonesia dan Kepolisian Negara Republik Indonesia, sebagai kekuatan utama, dan rakyat sebagai kekuatan pendukungnya.

Artinya pertahanan negara ini merupakan sesuatu yang utama dalam proses menjaga integritas suatu bangsa dan negara terutama dari gangguan kedaulatan yang timbul baik dari dalam maupun dari luar wilayah negara kesatuan Republik Indonesia. Lebih lanjut dari Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara dapat diambil sebuah pernyataan bahwa pertahanan negara adalah upaya yang bertujuan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari segala bentuk ancaman.[22]

Konsep Kedaulatan Negara

Menurut Bodley, kedaulatan terdiri dari kedaulatan eksternal dan internal. Di mana kedaulatan eksternal adalah semua hal yang berkaitan dengan luar negeri serta kekuatan pertahanan untuk melindungi teritorial negara dari serangan negara lain.[23] Sedangkan kedaulatan yang internal adalah kewenangan yang dimiliki oleh suatu negara untuk menjalankan fungsinya dalam lingkup nasional. Dalam *Tallinn Manual The International Law Applicable to Cyber Warfare Rule Sovereignty* menyatakan bahwa *State may exercise control over cyber infrastructure and activities within its sovereign territory.*

Peraturan tersebut menjelaskan bahwa, suatu negara dapat menjalankan kontrol terhadap infrastruktur *cyber* dan aktivitas *cyber* di dalam wilayah kedaulatannya. Dari definisi yang diberikan oleh Bodley dan aturan yang tercantum dalam *Tallinn Manual* dapat disimpulkan bahwa, ketika suatu negara memiliki kapabilitas dalam hal infrastruktur *cyber* dan aktivitas *cyber*, negara tersebut dapat dikatakan telah memiliki kedaulatan di dalam *cyberspace*, dan syarat umum yang terdapat dalam hukum internasional mengenai *cyberspace* untuk dapat dikatakan sebagai *domain* terpenuhi.

Upaya Pemerintah Indonesia dalam Perlindungan Dokumen Negara

Hubungan internasional, regional, maupun bilateral merupakan faktor penting dalam menyikapi timbulnya berbagai ancaman. Kebijakan politik luar negeri yang diterapkan adalah politik luar negeri bebas aktif. Kebijakan ini sangat dipengaruhi oleh ideologi Bangsa Indonesia. Sebagai salah satu negara dalam kancah dunia, Bangsa Indonesia terkesan menganggap negara lain adalah sahabat sementara negara yang dianggap sahabat tersebut belum tentu konsisten dengan kesepakatan untuk bersahabat.

Dalam era globalisasi ini tiap negara berkompetisi untuk memajukan negaranya masing-masing. Dalam hal berkompetisi antar negara tersebut pemerintah Indonesia terkesan lebih mementingkan kemajuan bersama-sama dengan negara lain sementara negara tersebut belum tentu konsisten ingin juga bersama-sama memajukan Indonesia. Oleh karena itu diharapkan kebijakan politik luar negeri yang mengedepankan realisme merupakan upaya yang dapat ditempuh, sehingga Indonesia dapat memetakan negara-negara tersebut dalam kelompok negara *competitor*, *netral*, pendukung dengan Indonesia.[24]

Dengan demikian maka Indonesia dapat dengan mudah melakukan konsep hubungan diplomatis dengan negara-negara tersebut. Pemerintah perlu memiliki peraturan/perundang-undangan yang mengatur tentang kewenangan untuk menyatakan

[22] Kejahatan dengan menggunakan jaringan berdasarkan data yang telah dipaparkan sebelumnya sangat banyak terjadi di Indonesia. Kapabilitas Indonesia dalam mengatur tindakan yang menggunakan jaringan ini terdapat pada Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut menempatkan Bab VII dengan 11 Pasal yaitu Pasal 27 sampai dengan 37 yang khusus membahas tentang perbuatan yang dilarang dalam penggunaan jaringan di Indonesia. Akan tetapi, dalam bab perbuatan yang dilarang ini tidak secara jelas menyebutkan istilah *cybercrime* atau kejahatan siber.

[23] Devika Hovel, 2004, "Chinks in the Armour: International Law, Terrorism, and The Use of Force", *UNSW Journal*, h. 399.

[24] Alva A.G. Narande, "Perang Hibrida di Dunia", *Jurnal Yudhagama*, Volume 33 No. 2 Bulan Juni 2013, h. 20.

bahwa suatu pihak adalah lawan/musuh bangsa dan negara. Pada Pembukaan UUD 1945 sangat jelas dicantumkan bahwa pemerintah negara Indonesia harus dapat melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia.

Tragedi runtuhnya Twin Tower di New York pada 11 September 2001, merupakan tonggak pemicu meningkatnya angka jumlah negara yang melakukan antisipasi serangan kejahatan menggunakan cara-cara *Online Intrusion* seperti *internet filtering* dan *internet surveillence*. Tidak terbatas pada jaringan siber saja yang mengalami interupsi akan tetapi juga pada jalur komunikasi telepon (kabel dan nirkabel) juga tidak luput dari aktifitas pengawasan yang dilakukan oleh pemerintah. Beberapa contoh negara yang telah lama menerapkan kebijakan pengawasan terhadap jalur lalu lintas informasi dan telekomunikasi dalam kehidupan warga negaranya adalah Amerika Serikat, Australia, China dan India. Hal tersebut mereka lakukan dengan alasan bahwa mengawasi secara maksimal semua media dan data, teks, suara dan video yang disimpan dan dikirimkan melalui dunia siber adalah cara yang efektif untuk melindungi rakyatnya dari ancaman kejahatan dan ancaman keamanan negara.

Dalam hal ini, *internet surveillance* yang dilakukan oleh pemerintah tidak hanya menjanjikan *benefit* bagi keamanan dan pertahanan negara saja, akan tetapi secara langsung kebijakan ini juga akan menerobos hak-hak privasi warga negara yang hidup di dalam wilayah jurisdiksi negara tersebut.

Peran TI sebagai sarana pembinaan teritorial dalam perang hibrida. Seperti disampaikan di atas bahwa walaupun dengan pembinaan teritorial aspek sosial budaya dan aspek lain dalam masyarakat dapat dikuasai, namun kita juga tidak boleh melupakan faktor teknologi untuk dapat membantu memenangkan perang hibrida ini. Salah satu teknologi yang saat ini berperan penting adalah Teknologi Informasi khususnya untuk mendukung konsep perang informasi dan perang *cyber*. Oleh karenanya penguasaan dan kepemilikan teknologi ini secara aman dan secara mandiri merupakan satu hal yang penting untuk mendukung konsep perang hibrida ini. Pandangan umum menyatakan bahwa militer profesional adalah militer yang berperang secara konvensional, didukung oleh Alutsista yang modern dengan daya tempur yang tinggi, bertempur dalam jenis perang tertentu, dinilai sudah kurang relevan lagi.

Dalam perang hibrida, TI memainkan peran yang penting. Teknologi ini mampu memberikan informasi kepada prajurit secara *real time* tentang ancaman yang mereka hadapi dan memberi solusi bagi para prajurit tentang apa yang harus dilakukan. Bahkan saat ini mereka secara individual juga dapat langsung mengakses informasi itu melalui perangkat genggam atau *handheld* yang mereka bawa. Di samping keunggulannya, karena kemudahan pengoperasiannya dalam mendukung proses pengambilan keputusan, Teknologi informasi juga dapat digunakan dalam mendukung konsep penaklukan tanpa melaksanakan perang secara fisik yaitu menggunakan konsep perang informasi melalui sarana media massa, *mailing list*, dan bahkan sekarang ini menggunakan apa yang disebut sebagai media sosial atau *social media*. merupakan satu sarana yang cukup ampuh dalam rangka mendukung perang hibrida, bahkan dari pengalaman akhir-akhir ini di Timur Tengah dengan *Arab Spring*-nya yaitu media sosial mampu membuat revolusi di Tunisia, Mesir, Libya, dan sekitarnya.

Inilah pentingnya teknologi informasi dalam rangka mendukung konsep perang hibrida. Khusus untuk pemanfaatan teknologi informasi di bidang teritorial dalam meningkatkan ketahanan wilayah diperlukan satu langkah terobosan melalui pelaksanaan Pembinaan Ketahanan Wilayah.[25]

Ancaman yang dihadapi Indonesia akan semakin kompleks. Pada berbagai peristiwa perang yang terjadi di berbagai belahan dunia akhir-akhir ini, kita tidak bisa dengan mudah menilai siapa aktor/pelaku perang yang sebenarnya, apakah mereka itu mengatasnamakan suatu negara atau *state actor* atau bukan negara atau *nonstate actor*. Kita pun menemukan berbagai kesulitan tentang apa sebenarnya yang menjadi latar belakang terjadinya peperangan tersebut. Latar belakang terjadinya peperangan tersebut bercampur aduk antara kepentingan yang bersifat politik, ideologi, ekonomi, atau aspek sosial dan lain-lain. Sistem dan metode berperang juga bersifat kompleks karena perang dilakukan dengan menerapkan konsep perang konvensional dan perang modern.

Dimensi peperangan yang terjadi juga sudah merambah kepada dimensi dunia maya atau dunia *cyber* sebagai fasilitas/sarana/media peperangan

[25] Teguh Pudjo Rumekso, "Hybrid Warfare dan Implikasinya Bagi Indonesia", *Jurnal Yudhagama*, Volume 33 No. 2 Bulan Juni 2013, h. 45.

dunia maya atau *cyber warfare*. Peperangan yang bersifat kompleks, bercampur aduknya berbagai kepentingan yang menjadi latar belakang konflik, ketidakjelasan siapa pelaku perang yang sebenarnya, bercampuraduknya metode, cara, teknik dan taktik berperang itulah yang kemudian disebut sebut sebagai Perang Hibrida atau *Hybrid Warfare*.

Kekuatan *cyber defence* harus dipersiapkan secara maksimal. Kesungguhan pemerintah dalam menata pertahanan dan keamanan negara tersebut tidak hanya diproyeksikan untuk menghadapi musuh dari luar. Tetapi juga, menyiapkan kemungkinan berkembangnya perang hibrida dan masalah terorisme di dalam negeri. Pembelian perlengkapan senjata TNI dalam tiga tahun terakhir ini juga dipersiapkan untuk kemungkinan menghadapi perang tersebut. Kesiapan Indonesia dalam menghadapi *cyber war* dan strategi[26] yang akan dilaksanakan oleh Indonesia.

Adapun Strateginya adalah: *Pertama,* Strategi kesiapan. Untuk mempersiapkan menghadapi perang hibrida dibutuhkan adanya strategi untuk mengatasinya, terutama pengaturan tata ruang pertahanan wilayah Indonesia yang memiliki posisi strategis dengan membuat strategi baik strategi posisi garis luar maupun posisi garis dalam. Negara berada pada posisi garis luar apabila dapat mengepung lawan atau musuhnya. Posisi garis dalam adalah posisi satu negara yang menghadapi kemungkinan permusuhan dari negara di sekelilingnya. *Kedua,* Proses Strategi Militer. Proses strategi militer tersebut dipadukan dengan kondisi geopolitik wilayah Indonesia yaitu bagaimana memanfaatkan penataan ruang berdasarkan posisi strategis Indonesia baik secara geografis dan politik berdasarkan 4 unsur yang dapat mendukung pembangunan, yaitu keadaan geografis, politik dan strategi, hubungan timbal balik antara geografi dan politik, serta unsur kebijaksanaan. Proses strategi untuk menghadapi perang hibrida adalah menentukan tujuan keamanan nasional sebagai dasar proses strategi. Merumuskan strategi raya, lebih dikenal dengan istilah kebijakan mengembangkan strategi militer merancang strategi operasi serta merumuskan strategi medan tempur, lebih dikenal dengan istilah taktik.

Kesiapan TNI 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. Para pemikir baik dari militer, analis pertahanan maupun dari anggota perlemen Indonesia menjelaskan bahwa, Kementerian Pertahanan dan Tentara Nasional Indonesia (TNI) sudah mengantisipasi kemungkinan menguatnya apa yang diistilahkan dengan Perang Hibrida tersebut. Jajaran TNI tidak boleh berdiam diri dengan perkembangan terbaru dalam strategi perang tersebut. Sudah selayaknya TNI mewaspadai ancaman perang hibrida, selain ancaman perang konvensional. Dari segi darat, laut, dan udara, TNI harus mewaspadai segala bentuk ancaman, baik itu perang konvensional maupun perang non konvensional seperti perang hibrida.

Saat ini Kementerian Pertahanan tengah menetapkan kebijakan pembangunan kekuatan, dengan memfokuskan pengembangan dan pembangunan kekuatan pada TNI AL dan TNI AU serta melaksanakan pemantapan kemampuan TNI AD. Setidaknya arah pembangunan kekuatan militer nantinya akan sesuai dengan kebijakan pemerintah yang telah tertuang dalam undang-undang. TNI sebagai komponen utama pertahanan, memerlukan acuan yang dapat dijadikan sebagai pedoman dalam melaksanakan tugas pokoknya. Oleh karena itu, pemerintah perlu didorong untuk segera menyusun suatu strategi nasional yang menjadi kesepakatan semua komponen bangsa, yang oleh Kementerian Pertahanan bekerja sama dengan TNI akan diterjemahkan menjadi suatu kesiapan sistem pertahanan yang disesuaikan dengan kondisi geografis negara dengan melibatkan segenap instrumen kekuatan nasional.

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

[26] Pada level strategi, permasalahan dapat dilihat pada dokumen strategi yang disusun oleh masing-masing angkatan. Di lingkup TNI AL misalnya, telah disusun Strategi Pertahanan Laut Nusantara (SPLN) yang kemudian disempurnakan menjadi Strategi Pertahanan Maritim Indonesia (SPMI). Kedua strategi tersebut menyatakan bahwa operasi tempur yang dilaksanakan oleh TNI AL akan membutuhkan dukungan dari TNI AU dan TNI AD. Karenanya jajaran TNI yang terdiri dari tiga matra harus melakukan investasi besar-besaran di bidang pengadaan sumber daya, baik perangkat teknologi maupun dukungan personelnya

diamanatkan oleh Undang-Undang Nomor 34 Tahun 2004 tentang TNI.

Rekonstruksi Pembentukan *National Cyber Defense* (*Cyber Army*)

Politik hukum merupakan bagian dari ilmu hukum yang mengkaji perubahan *ius constitutum* menjadi *ius constituendum* untuk memenuhi perubahan kehidupan masyarakat. Untuk memahami perubahan kehidupan masyarakat itu perlu ditelaah mengenai pengertian perubahan,[27] pengertian kehidupan,[28] dan pengertian masyarakat.[29]

Hubungan yang ajeg antar manusia itu, Logemann bahkan merumuskan masyarakat sebagai lalu-lintas atau hubungan antar manusia. Dikatakannya bahwa masyarakat adalah suatu *verkeer tussen mensen*. Masyarakat adalah suatu skema koordinasi hubungan antar manusia yang ajeg. Hubungan ajeg antar manusia dalam masyarakat itu oleh Logemann disebut institusi atau lembaga. Lembaga-lembaga itu, sebagai hubungan ajeg antara manusia di dalam masyarakat, adalah sekumpulan perbuatan yang berkaitan dengan akibat tertentu yang diterima dan dipatuhi datan kehidupan masyarakat yang bersangkutan.[30]

Dari uraian tersebut dapat disimpulkan bahwa masyarakat itu adalah kumpulan lembaga-lembaga. Lembaga-lembaga itu ada yang merupakan lembaga hukum dan lembaga bukan lembaga hukum. Lembaga-lembaga itu adalah unsur-unsur kehidupan masyarakat. Perubahan kehidupan masyarakat dengan demikian adalah perubahan lembaga-lembaga tersebut. Perubahan itu dapat merupakan perubahan jumlah lembaga-lembaga itu, dapat pula merupakan perubahan susunan lembaga-lembaga tersebut tanpa perubahan jumlahnya, dan dapat juga merupakan perubahan unsur-unsur interen lembaga-lembaga itu.[31]

Lembaga-lembaga itu terbentuk dalam suatu masyarakat karena adanya persamaan penilaian anggota masyarakat yang bersangkutan bahwa untuk perbuatan-perbuatan tertentu diterima selayaknya mempunyai akibat-akibat demikian. Terdapat perubahan penilaian tentang perbuatan-perbuatan tertentu dengan dengan akibat-akibatnya yang demikian maka lembaga itu akan menjadi berubah. Dengan demikian perubahan lembaga dalam kehidupan masyarakat itu terutama disebabkan oleh karena adanya perubahan penilaian terhadap lembaga tersebut.

Perubahan dalam kehidupan masyarakat adalah sasuatu yang tak dapat dihindari. Adanya perubahan kehidupan masyarakat itu telah pula dipahami oleh masyarakat Yunani purba. Dalam masa itu orang-orang Yunani purba telah mengenal pepatah *panta rei*, yang berarti bahwa semua itu mengalir.[32]

Faktor-faktor yang mempengaruhi perubahan kehidupan suatu masyarakat dapat merupakan faktor-faktor yang terdapat di dalam masyarakat itu sendiri (faktor internal) dan dapat pula merupakan faktor-faktor yang datang dari luar (faktor eksternal). Faktor-faktor internal itu misalnya pemikiran manusia anggota masyarakat yang bersangkutan, kebutuhan hidup anggota masyarakat yang bersangkutan, dan cara hidup anggota masyarakat yang bersangkutan. Faktor-faktor eksternal yang dapat merubah

[27] Yang dimaksud dengan pengertian perubahan dalam penelitian ini adalah keadaan sesuatu yang berbeda dari keadaan semulanya. Segala sesuatu yang ada di dunia itu terdiri dari unsur-unsur atau bagian-bagian. Misalnya orang terdiri dari kepala, tubuh, tangan, dan kaki; pohon terdiri dari akar, batang, dahan, ranting, daun, bunga, dan buah. Masyarakat juga terdiri dari unsur-unsur. Perubahan sesuatu itu adalah perubahan unsur-unsur sesuatu tersebut. Perubahan unsur-unsur itu dapat merupakan perubahan jumlah dari unsur-unsur sesuatu tersebut, misalnya unsur-unsurnya bertambah atau berkurang. Di samping itu perubahan tersebut juga dapat merupakan perubahan susunan unsur-unsur dari sesuatu itu.

[28] Kehidupan dalam uraian ini diartikan sebagai keberadaan, namun keberadaan tidak selalu hidup. Dengan demikian dapat dirumuskan bahwa kehidupan itu adalah kehidupan yang dinamik. Hidup adalah keberadaan yang dinamik, yang berkembang yang berubah. Hidup adalah yang berubah. Kehidupan sesuatu merupakan perubahan yang positif yakni berkembang menjadi lebih baik, tetapi hidup, sampai taraf tertentu, juga merupakan perubahan yang negatif yakni surut menjadi lebih buruk. Sampai taraf tertentu perubahan negatif itu masih merupakan kehidupan dan berakhir pada kematian.

[29] Pada umumnya masyarakat diartikan sebagai sekumpulan orang yang terikat pada suatu Kebudayaan tertentu. Namun menurut Oppenheim merumuskan masyarakat adalah *a body of a number of individuals more or less bound together through common interests as create constant and manifold intercours between individuals*. Dari perumusan itu yang penting adalah pernyataan Oppenheim bahwa seperangkat individu itu menciptakan hubungan yang ajeg atau *constant* antar individu tersebut. Dengan lain kata dalam masyarakat itu terdapat hubungan ajeg antar manusia.

[30] Muntoha, "Demokrasi dan Negara Hukum", *Jurnal Hukum*, No. 3 Vol. 16 Juli 2009, h. 379.

[31] Sefriani, "Ketaatan Masyarakat Internasional terhadap Hukum Internasional dalam Perspektif Filsafat Hukum", *Jurnal Hukum*, No. 3 Vol. 18, Juli 2011, h. 407.

[32] Jumadi, "Negara Hukum Demokratis Konstitusi Baru Indonesia", *Al-Risalah,* Vol. 11 No. 1 Mei 2011.

kehidupan suatu masyarakat misalnya datangnya teknologi modern, masuknya alat-alat komunikasi dan transportasi modern dalam masyarakat tersebut.

Perubahan kehidupan masyarakat dapat semua bidang kehidupan dalam masyarakat yang bersangkutan. Perubahan suatu bidang kehidupan masyarakat dapat pula mempengaruhi perubahan bidang kehidupan yang lain. Sebut saja misalnya lima bidang kehidupan masyarakat, seperti bidang kehidupan hukum,[33] bidang kehidupan politik,[34] bidang kehidupan ekonomi,[35] bidang kehidupan sosial,[36] dan bidang kehidupan budaya.[37]

Perubahan bidang kehidupan yang satu dapat mempengaruni perubahan kehidupan yang lain. Bagi politik hukum yang perlu dicatat ialah bahwa perubahan bidang-bidang kehidupan selain perubahan hukum dapat mempengaruhi perubahan hukum dalam suatu masyarakat. Tetapi perubahan bidang kehidupan hukum juga dapat mempengaruhi perubahan bidang-bidang kehidupan yang lain.

Oleh karena itu dalam mengkaji hukum sebagai instrumen perubahan masyarakat harus juga memahami saling keterkaitan hukum itu dengan instrumen-instrumen lain tersebut. Namun demikian juga harus diingat bahwa sebagai instrumen perubahan masyarakat itu hukum merupakan instrumen yang mempunyai kelebihan bila dibanding dengan instrumen yang lain. Hukum merupakan-sarana yang kuat, karena hukum merupakan sarana yang dapat memaksakan keputusannya dengan *external power*. Oleh karena itu hukum sebagai instrumen perubahan kehidupan masyarakat bila digunakan dengan tepat akan merupakan instrumen yang berguna. Tetapi bila digunakan dengan salah hukum akan menjadi instrumen yang berbahaya bagi kehidupan masyarakat.

Kesenjangan yang terjadi karena kehidupan masyarakat lebih maju daripada ketentuan hukum yang berlaku. Dalam hal demikian terdapat kehidupan masyarakat yang tidak sesuai dengan keharusan yang dituntut oleh hukum. Dengan lain kata timbullah keharusan yang tidak sesuai dengan keharusan yang dituntut oleh hukum. Dalam hal demikian hukum tertinggal dari keharusan yang hidup dalam masyarakat.

Kesenjangan juga dapat terjadi bila ada ketentuan hukum baru yang ditetapkan yang tidak sesuai dengan tingkah laku manusia di dalam masyarakat. Daiam hal demikian tuntutan keharusan hukum yang beru ditetapkan tidak sesuai dengan tingkah laku yang hidup dalam masyarakat. Hal itu berarti kehidupan masyarakat tertinggal dari ketentuan hukum yang berlaku.[38]

Untuk mengatasi kesenjangan itu hukum dapat menetapkan tiga alternatif. *Pertama,* tetap berpegang pada hukum yang berlaku dan merubah tingkah laku kehidupan dalam masyarakat yang ada. *Kedua,* melegalisir perubahan kehidupan yang ada dan meniadakan ketentuan hukum yang berlaku. Dan yang *Ketiga,* sebagian ketentuan hukum yang berlaku dipertahankan dengan juga menerima sebagian perubahan kehidupan dalam masyarakat yang terjadi. Peran hukum dalam merubah kehidupan masyarakat dapat dilakukan secara langsung dan dapat juga dilakukan secara tidak langsung.[39]

Apakah hukum dapat merubah kehidupan masyarakat, menjawab pertanyaan ini teori Marx klasik dan teori hukum mashab sejarah menyatakan negatif. Teori Marx klasik membedakan kehidupan masyarakat dalam dua struktur, yakni struktur atas dan struktur bawah.[40]

Teori Von Savigny, dari mashab sejarah berpendapat bahwa hukum itu tidak dibuat tetapi hukum itu ada dan terbentuk bersama-sama dengan masyarakat atau *das Recht ist nicht gemacht, aber Es ist und wirdt mit dem Volke*. Bersarkan dalil itu von Savigny hukum, yang ditetapkan dalam perundang-undangan, tidak dapat merubah kehidupan

[33] Bidang kehidupan hukum adalah bidang kehidupan yang mengusahakan memenuhi kebutuhan hidup yang tertib dan adil.

[34] Bidang kehidupan politik adalah bidang kehidupan yang mengusahakan memenuhi kebutuhan hidup berkuasa dalam masyarakat.

[35] Bidang kehidupan ekonomi adalah bidang kehidupan yang mengusahakan memenuhi kebutuhan hidup jasmani.

[36] Bidang kehidupan sosial adalah bidang kehidupan yang mengusahakan memenuhi kebutuhan hidup dalam kebersamaan.

[37] Bidang kehidupan budaya adalah bidang kehidupan yang mengusahakan memenuhi kebutuhan hidup luhur.

[38] Hans Kelsen, 1971, *General Theory of Law and State*, New York: Russel and Russeu diterjemahkan oleh Raisul Muttaqien, *Teori Umum tentang Hukum dan Negara*, 2014, Nusa Media, Ujung Berung Bandung.

[39] Suhieno, 1986, *Ilmu Negara*, Liberty, Yogyakarta, h. 152-153.

[40] Yang dimaksud dengan struktur atas adalah alam pikiran. Adapun struktur bawah adalah kebutuhan jasmani. Menurut teori Marx struktur bawah menentukan struktur atas, dan tidak sebaliknya. Dengan demikian maka alam pikiran, termasuk hukum, tidak dapat mempengaruhi atau merubah struktur bawah, atau kehidupan masyarakat.

masyarakat. Hal itu disebabkan bahwa hukum itu tumbuh bersama kehidupan masyarakat yang bersangkutan.

Dror berpendapat bahwa pendapat dua teori itu tidak sesuai dengan kenyataan yang terjadi di dalam praktek. Kenyataan di dalam praktek menunjukkan bahwa hukum dapat merubah kehidupan masyarakat dan juga terdapat perundang-undangan yang menetapkan berlakunya hukum negara lain ke dalam hukum suatu negara dengan hasil yang baik.[41]

Berbicara tentang proses perubahan *ius constitutum* menjadi *ius constituendum* yang dikarenakan oleh adanya perubahan kehidupan masyarakat adalah berbicara tentang suatu rangkaian kegiatan yang merubah *ius constitutum* karena adanya kenyataan yang yang berbeda dengan unsur-unsur *ius constitutum* untuk kemudian menetapkan *ius constituendum* yang unsur-unsurnya memenuhi kenyataan kehidupan masyarakat yang berbeda tersebut. Berbicara tentang proses perubahan *ius constitutum* menjadi *ius constituendum* itu menyangkut dua hal, yang pertama mengenai prosesnya dan, yang kedua, mengenai pelakunya.

Proses dalam hal ini diartikan sebagai suatu rangkaian kegiatan yang membentuk suatu kejadian. Pengertian proses dengan demikian mencakup serangkaian kegiatan untuk mencapai suatu tujuan. Dalam uraian politik hukum ini proses itu adalah suatu rangkaian kegiatan untuk menetapkan *ius constituendum*.[42]

Rangkaian kegiatan untuk menetapkan *ius constituendum* terdiri dari beberapa kegiatan sebagai berikut; *Pertama,* Menguraikan unsur-unsur *constitutum*; *Kedua,* Menguraikan unsur-unsur perubahan kehidupan masyarakat; *Ketiga,* Membandingkan unsur-unsur *ius constitutum* dengan unsur-unsur perubahan kehidupan masyarakat hingga menemukan *trouble* dalam menerapkan *ius constitutum* pada kenyataan kehidupan masyarakat yang dihadapi; *Keempat,* Merumuskan permasalahan yang hendak diselesaikan; *Kelima,* Menentukan data yang diperlukan untuk menyelesaikan permasalahan; *Keenam,* Menganalisis data untuk menyelesaikan permasalahan hingga menemukan 3 (tiga) alternatif penyelesaian permasalahan: *Ketujuh,* Menetapkan filter untuk memilih salah satu alternatif yang telah ditemukan; *Kedelapan,* Menetapkan kesimpulan yang berupa *ius constituendnm*.

Pelaku proses politik hukum adalah alat pemerintahan dalam arti luas, yakni alat pemerintahan dalam bidang legislatif, alat pemerintahan dalam bidang pemerintahan dalam arti sempit, dan alat pemerintahan dalam bidang yudikatif. Yang dimaksud dengan alat pemerintahan dalam bidang legislatif adalah alat pemerintahan yang bertugas menetapkan ketentuan hukum yang berlaku umum.

Dewan Perwakilan Rakyat dengan persetujuan Presiden dalam menetapkan Undang-Undang. Presiden dalam menetapkan Peraturan Pemerintah dan Peraturan Pemerintah Pengganti Undang-undang. Adapun yang dimaksud dengan alat pemerintahan dalam bidang pemerintahan dalam arti sempit adalah alat pemerintahan yang bukan alat pemerintahan dalam bidang legislatif dan bukan alat pemerintahan dalam bidang yudikatif. Sedang yang dimaksud dengan alat pemerintahan dalam bidang yudikatif adalah alat pemerintahan yang bertugas menguji pelaksanaan hukum yang dilakukan oleh pihak lain. Dengan alat pemerintahan dalam bidang yudikatif menetapkan apakah suatu perbuatan yang dilakukan oleh suatu pihak atau peristiwa yang dialami oleh sesuatu pihak sesuai dengan hukum yang berdasarkan pengertian alat pemerintahan dalam bidang legislatif dan yudikatif maka alat pemerintahan dalam bidang pemerintahan dalam arti sempit itu adalah semua alat pemerintahan dalam bidang pemerintahan yang tidak termasuk dalam bidang legislatif atau pun bidang yudikatif.[43]

Alat pemerintahan dalam arti sempit, dalam melaksanakan tugasnya juga terikat pada ketentuan prosedur tertentu. Dengan kata lain proses politik hukum yang dilakukan oleh alat pemerintahan dalam arti luas itu dikemas sesuai dengan prosedur alat pemerintah yang melakukannya. Berdasarkan kemasan yang berbeda itu produk hasil proses politik hukum tersebut juga menyandang nama/sebutan yang berbeda pula. Hasil proses yang dilakukan oleh alat pemerintah di bidang legislatif adalah peraturan, yakni perbuatan bersegi satu, dilakukan di bidang legislatif (penetapan ketentuan hukum yang berlaku umum), oleh alat pemerintahan (dalam arti luas) berdasarkan wewenang istimewa. Peraturan itu berlaku umum, yang juga disebut undang-undang dalam arti material.

[41] Philip C. Jessup, *A Modern Law of Nation, Pengantar Hukum Antar Bangsa*, Nuansa, Bandung, 2012.

[42] Fred Iswara, *Pengantar Ilmu Politik*, Binacipta, Bandung, 1980, h. 108.

[43] *Ibid.*

Hasil proses yang dilakukan alat pemerintah di bidang pemerintahan dalam arti sempit adalah ketetapan yang menurut Prins, diartikan sebagai perbuatan bersegi satu, di bidang pemerintahan (dalam arti sempit) yang dilakukan oleh alat pemerintahan (dalam arti luas), berdasarkan wewenang istimewa. Adapun hasil proses yang dilakukan alat pemerintah di bidang yudikatif disebut vonis, yakni perbuatan bersegi satu, di bidang yudikatif (menguji pelaksanaan ketentuan hukum yang dilakukan pihak lain), yang dilakukan oleh alat pemerintahan (dalam arti luas) berdasarkan wewenang istimewa.[44]

Produk perubahan *ius consitutum* menjadi *ius constituendum* dalam memenuhi perubahan kehidupan masyarakat adalah ketentuan hukum, baik yang berupa satu ketentuan hukum atau pun yang berupa satu perangkat ketentuan hukum. Telah diutarakan bahwa ketentuan hukum yang merupakan hasil pemikiran potitik hukum itu dapat merupakan ketentuan hukum yang baru sesuai dengan tuntutan perubahan kehidupan masyarakat, dapat pula merupakan ketentuan kompromi yang sebagian memenuhi tuntutan perubahan kehidupan masyarakat dan sebagian tetap berpegang pada ketentuan yang lama (*ius constitutum*); dan bahkan dapat pula tetap merupakan ketentuan hukum yang lama (*ius constitutum*).

Dalam hal produk perubahan *ius constitutum* itu merupakan ketentuan hukum yang mengikuti seluruh perubahan kehidupan masyarakat, atau ketentuan hukum yang merupakan kompromi antara perubahan kehidupan masyarakat dan *ius constitutum*, produk perubahan *ius constitutum* menjadi *ius constituendum*, merupakan suatu pembaharuan hukum. Dalam hal demikian ketentuan hukum baru itu perlu dikaji arah dan kerangkanya agar tampak kedudukan ketentuan hukum yang baru itu dalam sistem hukum yang berlaku dan agar ketentuan hukum baru itu dapat terapkan sesuai dengan tujuan penetapannya. Pengkajian arah dan kerangka ketentuan hukum yang baru itu berlaku bagi produk pemikiran politik hukum yang berupa satu ketentuan hukum maupun bagi produk pemikiran politik hukum yang berupa seperangkat ketentuan hukum.

Pengkajian arah dan kerangka ketentuan hukum baru yang merupakan seperangkat ketentuan hukum, yang merupakan satu unit peraturan perundang-undangan, dapat dilakukan lebih rinci. Hal itu disebabkan oleh karena unit peraturan perundang-undangan itu telah tersusun dalam suatu sistem; Pada umumnya untuk peraturan perundang-undangan itu terdiri dari konsiderans dan batang tubuh peraturan perundang-undangan. Dalam konsiderans itu ditetapkan pertimbangan yang mendasari ditetapkannya ketentuan-ketentuan dalam batang tubuh peraturan perundang-undangan itu. Pertimbangan yang mendasari ketentuan-ketentuan batang tubuh itu pada umumnya dapat dibedakan menjadi dua bagian, yakni pertimbangan fakta dan pertimbangan hukum. Pertimbangan fakta dalam konsiderans itu pada umumnya mengutarakan fakta yang menjadi sebab ditetapkannya ketentuan hukum dalam batang tubuh peraturan perundang-undangan yang bersangkutan. Namun, di samping fakta yang merupakan penyebab ditetapkannya ketentuan hukum dalam batang tubuh itu, dalam konsiderans dapat juga diutarakan fakta atau kenyataan yang hendak diwujudkan dengan ditetapkannya ketentuan hukum dalam batang tubuh peraturan perundang-undangan yang bersangkutan.

Konsiderans itu dengan demikian menetapkan arah ketentuan hukum dalam peraturan perundang-undangan tersebut. Namun, di samping itu arah ketentuan hukum yang ditetapkan itu dapat juga ditetapkan dalam batang tubuh peraturan perundang-undangan. Adapun yang dimaksud dengan kerangka ketentuan hukum yang baru itu ialah rangkaian hubungan antara ketentuan hukum yang satu dengan yang lain yang mewujudkan sarana untuk mencapai tujuan yang telah ditetapkan. Bila arah ketentuan hukum dalam peraturan perundang-undangan kebanyakan ditetapkan dalam konsiderans peraturan perundang-undangan yang bersangkutan, kerangka ketentuan hukum peraturan perundang-undangan itu kebanyakan ditetapkan terutama dalam batang tubuh peraturan perundang-undangan yang bersangkutan. Namun, kerangka ketentuan hukum itu dapat juga telah ditetapkan dalam konsiderans.

Rekonstruksi Pembentukan *National Cyber Defence*

Pembangunan pada aspek regulasi perlu disusun sedemikian rupa, sehingga akses yang dilakukan oleh pihak lain bisa dikendalikan. Penguasaan dan keterampilan prajurit pada aspek teknologi informasi dan komunikasi perlu dikembangkan, sehingga memiliki kemampuan untuk melindungi infrastruktur

[44] *Ibid*.

milik sendiri, mampu melakukan pengintaian dan pengamatan terhadap data atau informasi pihak lawan sekaligus mampu melakukan manipulasi data atau informasi (kemampuan *cyber defense* dan *cyber attack*).[45]

Doktrin TNI khususnya tentang konsep menghadapi ancaman *hybrid warfare* yang dilakukan oleh *nonstate actor* perlu segera disusun untuk dapat dijadikan sebagai pedoman bagi seluruh kekuatan TNI dalam melakukan pembinaan maupun dalam penggunaan kekuatan dalam menghadapi ancaman *cyber warfare*. Pembentukan unit *cyber warfare* sangat diperlukan sebagai salah satu unsur yang memiliki kemampuan melaksanakan perang elektronika khususnya *cyber defense* dan *cyber attack*.

Konsep yang dapat Ditempuh Dalam Menghadapi Perang Hibrida:[46]

Pertama, penyempurnaan doktrin. Doktrin bukan merupakan sesuatu yang dogmatis dan tidak terbantahkan, justru sebaliknya, doktrin militer yang baik akan menyesuaikan dengan lingkungan operasi yang aktual, adaptif dengan segala bentuk situasi dan dapat dipahami serta dilaksanakan mulai dari pimpinan TNI sampai dengan prajurit pelaksana di lapangan dan doktrin harus aplikatif menyesuaikan dengan sifat peperangan. Sehingga untuk mendukung kesiapan TNI dalam menghadapi fenomena perang hibrida, doktrin TNI harus dapat menyesuaikan dengan perkembangan peperangan yang aplikatifnya pada taktik yang dioperasionalkan di lapangan. Taktik harus menyesuaikan dengan lingkungan operasi dan sifat dari musuh yang akan dihadapi, jangan sampai taktik peperangan yang digunakan oleh TNI tidak sinkron dengan pola peperangan hibrida yang cenderung menembus ruang dan waktu.

TNI AD sebagai tumpuan dalam pelaksanaan operasi TNI sudah seyogyanya menjadi *leading sector* perubahan doktrin perang yang mengarah kepada perang hibrida ke depan. Contoh keberhasilan dalam pembuatan doktrin seperti yang dilakukan oleh militer Amerika Serikat di mana perumusan doktrin diawali oleh angkatan darat, sedangkan angkatan lain akan menyesuaikan dalam bentuk *joint publication* yang berisi prinsip-prinsip dasar yang mengarahkan penggunaan militer dalam kegiatan yang terkoordinir untuk suatu sasaran yang sama.[47]

Kedua, Peningkatan SDM melalui pendidikan dan latihan di dalam dan luar negeri. Personel TNI mulai dari sekarang harus mulai memahami apa yang dimaksud dengan perang hibrida, bagaimana mengawaki Alusista untuk perang hibrida, bagaimana menghadapi *cyber warfare* dan perang informasi. Tuntutan kemajuan perang telah memaksa TNI untuk memiliki *nonwar skills*. Selain itu hubungan sipil dan militer perlu dilatihkan dalam wujud latihan yang terintegrasi, dimana dalam pola operasi yang dilakukan, instansi-instansi nonmiliter akan memberikan dukungan dalam bentuk personel, keahlian dan perlengkapan yang tidak dimiliki oleh TNI dalam menghadapi perang hibrida.[48]

Gejala perang hibrida tidak sama seperti perang konvensional di mana ancaman/musuh yang datang dapat benar-benar kelihatan nyata karena ancaman pada perang hibrida akan muncul dalam bentuk gejala atau sebaliknya dampak setelah terjadi. Guna menyikapi hal tersebut maka diperlukan suatu badan koordinasi di bawah kementerian pertahanan yang keanggotaannya berasal dari militer dan instansi-instansi nonmiliter. Baik anggota militer dan nonmiliter merupakan orang-orang yang memiliki kemampuan khusus dalam perang hibrida, seperti: ahli piranti lunak, anti *hacker*, pakar informasi, pakar telematika, ahli bahan peledak, ahli fisika atom, ahli biologi dan pakar taktik militer.[49]

Badan ini bertugas untuk mengkoordinasikan tindakan yang akan dilakukan terhadap segala bentuk potensi ancaman terhadap kedaulatan negara dihadapkan kepada perang hibrida. Kedua, satelit bersama. Sudah saatnya TNI memiliki satelit militer untuk mendukung kegiatan operasi, terlebih untuk mengantisipasi perang hibrida. Dengan memiliki satelit, TNI akan lebih terintegrasi dalam hal komando pengendalian, penyebaran informasi dan deteksi awal untuk mengetahui ancaman yang akan datang. Hal-hal yang diketahui sebagai ancaman akan lebih cepat terinformasi kepada seluruh matra, sehingga masing-masing matra akan menyiapkan satuan

[45] Devika Hovel, 2004, "Chinks in the Armour: International Law, Terrorism, and The Use of Force", *UNSW Journal*, h. 399.

[46] Supriyanto Aji, *Pengantar Teknologi Informasi*, Penerbit Salemba Infotek, Semarang, 2007.

[47] JS. Prabowo, 2009, h. 31.

[48] Barry Buzan, 1991, *People, State, and Fear: An Agenda for International Security Studies in the Post-Cold War Era,* Harvester Wheatsheaf, Hempstead.

[49] Dimitri Mahayana, 2000, *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*, Rosda, Bandung.

operasionalnya untuk melaksanakan penindakan secara terkoordinasi.

Analisa Pengembangan Teknologi Perang Hibrida dan Kesiapan Indonesia

Dalam perang *hibrida* aspek penguasaan atas kemajuan teknologi persenjataan memegang peranan yang sangat penting, terutama hal-hal yang terkait penggunaan ruang udara dan angkasa luar, perang informasi dan penggunaan *network centrik warfare* yang dapat dimanfaatkan di masa damai maupun ketika terjadi perang. Aspek penguasaan teknologi tersebut tidak akan banyak bermanfaat ketika jajaran TNI sebagai kekuatan utama sistem pertahanan belum mengembangkan strategi dan peningkatan kekuatan posturnya. Karena itu analisis kali ini akan berfokus pada pengembangan teknologi perang hibrida dan bagaimana kesiapan jajaran TNI menghadapinya.

Pengembangan teknologi *Network centric warfare*. *Cyber warfare* atau *cyberwar*, merupakan perang yang sudah menggunakan jaringan komputer dan Internet atau dunia maya atau *cyber space* dalam bentuk strategi pertahanan atau penyerangan sistem informasi lawan. *Cyber warfare* juga dikenal sebagai perang siber yang mengacu pada penggunaan fasilitas *world wide web* dan jaringan komputer untuk melakukan perang di dunia maya. Kegiatan *cyber warfare* dewasa ini sudah dapat dimasukkan dalam kategori perang informasi berskala rendah *low-level information warfare* yang dalam beberapa tahun mendatang mungkin sudah dianggap sebagai peperangan informasi yang sebenarnya atau *the real information warfare*.[50]

Di dalam konsep *cyber warfare*, penggunaan teknologi sistem informasi dimanfaatkan untuk mendukung kepentingan komunikasi antar prajurit atau jalur komando yang difasilitasi oleh satu sistem komando kendali militer modern, yaitu sistem NCW atau *Network Centric Warfare*.[51] Dengan adanya teknologi NCW yang didukung infrastruktur SIPRNet, berbagai komponen atau elemen militer di mandala operasi dapat saling terhubung atau *get connected* secara online system dan realtime, sehingga keberadaan lawan dan kawan dapat saling diketahui melalui visualisasi di layar komputer atau laptop. Dengan adanya teknologi Internet SIPRNet serta penggunaan satelit mata-mata dan satelit GPS, memungkinkan NCW memvisualisasikan seluruh kegiatan operasi militer gabungan yang sedang berlangsung di medan pertempuran atau *battle field* ke layar lebar ruang yudha atau *military operation room*, yang mungkin jaraknya terpisahkan ribuan kilometer jauhnya. Sehingga konsep NCW pada akhirnya akan merubah paradigma militer lama yang menyatakan bahwa suatu medan pertempuran dapat dimenangkan hanya oleh satu komponen militer saja.[52]

Penggunaan ruang cyber[53] atau *cyber space* dalam perang hibrida, penggunaan ruang udara dan angkasa luar. Penguasaan angkasa atau *space* dalam sistem pertahanan negara melalui perang hibrida merupakan bagian dari impian intelegensia manusia, dengan kemampuan sensornya yang mampu menjelajahi area melintasi batas negara dengan bebas, tanpa pagar dan batas. Tidak ada area terlarang untuk satelit.[54]

Pertempuran elektronik atau *electronic warfare* dengan memanfaatkan media ruang udara dan angkasa luar, pada saat ini adalah salah satu perangkat yang paling penting untuk mengumpulkan informasi dalam kondisi damai maupun perang. Radio mampu menyadap informasi mentah dari *link* radio yang *insecure*, bahkan bisa membuat gambaran dari suatu sebaran, pengaturan taktis, dan sebagainya. Aktivitas serapan/sadapan atau *intercept* informasi ini meliputi radio, radar, gelombang mikro, dan transmisi elektro magnetik lainnya.

---

[50] John Nana Naisbitt Nasibitt dan Douglas Philips, 2001, *High Tech, High Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi*, Mizan, Bandung.

[51] *Network Centric Warfare* (NCW) merupakan konsep Siskodal operasi militer modern yang mengintegrasikan seluruh komponen atau elemen militer ke dalam satu jaringan komputer militer NCW berbasis teknologi satelit dan jaringan Internet rahasia militer yang disebut SIPRNet (*Secret Internet Protocol Router Network*).

[52] Yono Reksoprodjo, "Kesiapan Nasional Bidang Pertahanan dalam Menghadapi Ancaman Siber", *Bahan Kuliah* dalam bentuk powerpoint, yang dipresentasikan di Sespim Polri, Lembang, 11 September 2014.

[53] Perpaduan antara teknologi telekomunikasi dan teknologi komputer akhirnya menciptakan dunia baru yang dinamakan *cyberspace*. Sebuah dunia komunikasi berbasis komputer atau *computer mediated communication* yang menawarkan realitas baru, yaitu realitas virtual atau *virtual reality*. *Cyberspace* (ruang *cyber*) menjelma menjadi sebuah ruang relasi sosial ketiga dalam kehidupan masyarakat, setelah ruang publik dan ruang privat. *Cyberspace* merupakan alat pemuas logika kecepatan atau *logic of speed*, di mana orang dapat saling berhubungan dalam ruang, tanpa harus mengurangi kecepatan dan tanpa harus meninggalkan tempatnya berada.

[54] Petrus Reinhart Gollese, "Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri", dalam *Buletin Hukum Perbankan*, Volume 4 Nomor 2, Agustus 2006.

Penggunaan ruang udara dan angkasa luar dalam pengembangan perang hibrida tidak lepas dari penggunaan teknologi satelit. Setidaknya terdapat empat jenis satelit yang dapat digunakan untuk kepentingan perang hibrida yaitu: *Pertama,* paling awal adalah satelit untuk tujuan mempelajari ruang angkasa.[55] *Kedua,* satelit telekomunikasi.[56] *Ketiga,* satelit militer yang dibekali dengan senjata laser.[57] *Keempat,* satelit pemantau langit atau satelit astronomi.[58]

Dengan satelit ini diharapkan pelanggaran wilayah laut oleh kapal-kapal asing, baik penyelundupan maupun penangkapan ikan secara liar atau *illegal fishing*, pembalakan hutan atau *illegal logging*, penambangan liar atau *illegal mining* hingga bencana alam, kecelakaan transportasi dan kerusuhan dapat di monitor secara terus menerus.

Pembangunan *cyber security* nasional ini dimaksudkan untuk menangkis serangan, khususnya dari luar yang bisa memperlemah bangsa. Sistem *cyber* yang akan dibentuk bukan malah untuk memata-matai warga negara sendiri. Dalam pembentukan badan *cyber*, pemerintah akan menggandeng berbagai kementerian dan lembaga.[59]

Badan Nasional dianggap super penting di Indonesia, dalam pembentukan badan *cyber*, lembaga atau badan *cyber* nasional itu tidak akan dijadikan alat pemerintah untuk memata-matai rakyat. Lembaga itu hanya untuk mengantisipasi serangan *cyber*, mencegah agar sistem informasi negara tidak *shut down*. Keberadaan lembaga yang khusus menangani masalah dunia maya penting karena setiap hari Indonesia menghadapi serangan dunia maya dengan frekuensi yang sering terjadi. Diungkapkan juga, ada kemungkinan dibentuk tentara *cyber* yang khusus menangani serangan dunia maya masuk dalam kajian tim pembentukan badan *cyber*.[60]

Tentara *cyber* sangat diperlukan mengingat hakekat ancaman sekarang ini yang tidak hanya ancaman yang bersifat militer semata melainkan ancaman yang bersifat nirmiliter, berupa salah satunya ancaman serangan *cyber*. Ancaman serangan *cyber* ini potensial terjadi karena era sekarang adalah era digital, era informasi, era komputer, era internet, dan era media sosial, di mana semua aktivitas manusia, semua transaksi ekonomi, semua data dilakukan dan disimpan dalam bentuk elektronik melalui *website, situs*, maupun berbagai data penyimpanan elektronik lainnya. Serangan *cyber* sangat mungkin terjadi mengingat sudah banyak berbagai kasus penyadapan, pencurian data, dan pengrusakan sistem informasi yang dilakukan oleh para *hacker* terhadap berbagai situs kementerian pertahanan di banyak negara.

Dalam negara, instansi yang berwenang membentuk tentara *cyber* adalah pemerintah yang didalamnya tentu ada Kementerian Pertahanan. Kementerian Pertahanan Indonesia harus segera merealisasikan terbentuknya tentara *cyber* sehingga bisa dipergunakan untuk melindungi dunia maya Indonesia dari berbagai serangan *cyber* yang setiap saat akan berpotensi terjadi. Kementerian Pertahanan harus melakukan kajian, riset, penelitian dan kelayakan pembentukan tentara *cyber*. Kementerian Pertahanan harus segera melakukan koordinasi dengan Mabes TNI untuk mengakselerasi pembentukan tentara *cyber* sehingga tidak hanya menjadi wacana semata, melainkan dapat direalisasikan secara kongkrit dan nyata.

Tentara *Cyber* harus memiliki kualifikasi yang kompeten dan mumpuni dalam mengoperasionalkan komputer, mengelola internet, menyelidiki media sosial, melakukan penyadapan, dan mengunakan berbagai perangkat lunak dan perangkat keras lainnya. Tentara *cyber* harus mampu membangun sistem, jaringan, dan melakukan operasi dunia maya, penyidikan dunia maya, dan menangkis berbagai virus dunia maya, serta melindungi berbagai data dan informasi dalam sistem elektronik di Indonesia. Bahkan, tentara *cyber* harus memiliki kualifikasi

[55] Inilah satelit pertama yaitu SPUTNIK yang diluncurkan Uni Soviet tahun 1959, juga satelit stasiun ruang angkasa internasional atau *International Space Station* atau ISS) yang sekarang menjadi tempat kerja sejumlah astronot Amerika, Eropa, Rusia dan Jepang

[56] Sebagai contoh adalah satelit Palapa yang dibeli Indonesia pada 1970-an dan sudah disusul berbagai generasi. Satelit jenis inilah yang faktanya paling populer.

[57] Inilah Proyek Star Wars Ronald Reagan, Presiden Amerika Tahun 1980-an di era Perang Dingin.

[58] Misalnya pembawa teleskop hubble, radio-astronomy *hyparchos* atau pemantau matahari *soho*. Kelima, satelit pemantau bumi atau *surveillance satellite*, sesuai misi NASA yang beralih dari misi ke planet lain ke *Mission to Planet Earth*. Fungsinya untuk memantau seluruh penjuru teritorial.

[59] Al Sentot Sudarwanto, "Cyber Bullying: Kejahatan Dunia Maya yang Terlupakan", *Jurnal Hukum Pro Justitia*, April 2009, Volume 27 No. 1.

[60] Deky Rosdiana, *Cyber Warfare menjadi Ancaman NKRI di Masa Kini dan Masa Depan*, dalam http://hankam.kompasiana.com/2013/09/23/cyber-warfaremenjadi-ancaman-nkri-dimasa-kini-dan-masa-depan-592343.html, diunduh pada 11 Maret 2015.

untuk melakukan serangan balik terhadap serangan *cyber* dari negara lain atau pihak lain untuk menjaga kedaulatan negara di domain dunia maya.

Tentara *cyber* harus direkrut oleh Kementerian Pertahanan melalui berbagai cara. Cara pertama adalah melalui tata cara pendaftaran sebagaimana yang umum dilakukan oleh TNI. Cara kedua adalah dengan cara menginventarisasi, mendata dan merekrut para anggota TNI aktif yang memang sudah memiliki keahlian dan kemampuan di bidang IT di berbagai kesatuan masing-masing sehingga dijadikan satu untuk dilakukan pelatihan khusus sehingga dapat mengisi unit khusus tentara *cyber* atau *cyber force*.

Pembentukan tentara *cyber* harus melalui berbagai kesiapan yang matang dan sistematis, khususnya dengan dukungan anggaran, sarana prasarana, dan piranti lunak atau regulasi yang lengkap dan terperinci. Anggaran yang besar sangat diperlukan untuk membentuk tentara *cyber* karena para tentara yang direkrut harus dididik, dilatih, dan dilakukan berbagai pendampingan, mentoring maupun pembinaan yang optimal sehingga akan terwujud tampilan dan sosok tentara *cyber* yang kompeten di bidangnya. Sarana prasarana berupa perangkat lunak dan perangkat keras komputer, jaringan dan berbagai perangkat pendukung lainnya perlu disiapkan sehingga akan mendukung tugas dan fungsi dari tentara *cyber*.[61]

Gelar kekuatan tentara *cyber* harus dilakukan di seluruh wilayah Indonesia. Artinya, tentara *cyber* berpusat di Kementerian Pertahanan sebagai komando pengendali utama, namun dalam gelar kekuatan harus dibentuk komando taktis di Mabes TNI dan Mabes Angkatan. Bahkan tentara *cyber* harus pula ditempatkan di setiap Kodam, Korem dan Kodim, sehingga akan mampu melindungi setiap data elektronik di setiap kesatuan, matra, maupun instansi teknis militer lainnya. Tentara *cyber* harus pula diberi tugas untuk melindungi berbagai situs, web maupun jaringan komunikasi yang dimiliki oleh pemerintah, lembaga negara, maupun berbagai instansi kementerian dari berbagai serangan *cyber* yang seringkali terjadi tanpa disadari oleh berbagai pihak.[62]

Badan Pertahanan *Cyber* Nasional sebenarnya sangat diperlukan oleh Indonesia. Badan Pertahanan *Cyber* Nasional atau apapun namanya harus segera dipikirkan untuk dibentuk agar terwujud mekanisme koordinasi, komunikasi, dan sinergi antar berbagai aktor keamanan dan pertahanan dalam melindungi kedaulatan dunia maya Indonesia dari berbagai ancaman serangan *cyber*. Kementerian Pertahanan, TNI, Polri, BIN, Kemenkominfo, Lembaga Sandi Negara, dan berbagai instansi terkait lainnya harus mampu bersinergi untuk menangkis, menangkal, dan mencegah serangan *cyber* dari pihak tertentu atau dari negara lain yang mencoba untuk menganggu kedaulatan dunia maya Indonesia saat ini dan di masa depan. Dalam kaitan ini, maka perlu sebuah analisis mendalam tentang penggunaan media sosial yang luar biasa pada masyarakat Indonesia dengan potensi perang siber.

Munculnya ancaman perang siber harus mendorong kesadaran semua pihak di Indonesia untuk memberikan perhatian lebih terhadap sistem pertahanan Indonesia. Seperti diketahui bahwa system pertahanan Indonesia adalah sistem pertahanan semesta (sishanta), di mana komponen utama adalah TNI, dan komponen pendukungnya adalah rakyat. Dalam konteks ini, system pertahanan semesta yang tertuang dalam UU No. 3 Tahun 2002 tentang Pertahanan Negara, harus mampu dimaknai sebagai semesta yang bersifat tidak hanya fisik semata, melainkan non fisik, khususnya digital dan dunia maya. Artinya, segala upaya dilakukan termasuk memberdayakan semua potensi dunia maya yang ada dalam menghadapi perang siber.

Kementerian Pertahanan bersama lembaga, pihak, dan instansi terkait lainnya harus saling bahu membahu memberdayakan potensi dunia maya dan potensi digital yang dimiliki, sebagai sumber daya buatan, untuk diberdayakan dalam membendung dan menghadapi perang siber. Pemerintah, kementerian pertahanan, TNI, Polri, BIN, Kemenkominfo, dan lain-lain harus melakukan berbagai inventarisasi, identifikasi, pembinaan, dan pengelolaan berbagai potensi kekuatan dunia maya yang dimiliki oleh Indonesia, khususnya masyarakat pengguna media sosial, netizen, dan berbagai komunitas informasi komunikasi dunia maya untuk saling bersinergi dalam menghadapi perang siber.

Dalam menghadapi ancaman *Cyber Warfare*, maka diperlukan sinergitas dari berbagai pihak

[61] Agus Subagyo, *"Sinergi dalam Menghadapi Ancaman Cyber Warfare Synergy on The Facing of Cyber Warfare Threat"*, diunduh https://agussubagyo1978.files.com/2015/08/sinergi-dalam-menghadapi-ancaman-cyber-warfare.pdf

[62] *Ibid*.

untuk bersatu padu, saling sinergi, saling komunikasi dan saling koordinasi. *Cyber Warfare* merupakan ancaman serius di era global sekarang ini sehingga diperlukan kesatuan pandangan dan satu persepsi untuk mensinergikan satu tindakan, satu kebijakan dan satu rencana aksi yang utuh. Ancaman *Cyber Warfare* harus memerlukan partisipasi dari berbagai pihak untuk menanganinya dan tidak mungkin hanya bisa dihadapi oleh satu instansi semata. Ancaman serangan *cyber* tidak bisa dilakukan secara parsial semata, melainkan memerlukan langkah penanganan yang dilakukan secara komprehensif, integral dan terpadu.

PENUTUP

Kesimpulan

Dalam menghadapi serangan *cyber*, diperlukan analisis terhadap eskalasi ancaman dan gradasi dalam menghadapi serangan *cyber*. Berikut ini diuraikan tentang eskalasi ancaman cyber dan lembaga terdepan sebagai ujung tombak yang menanganinya: Sinergitas antar *stakeholders* sangat penting dilakukan untuk menangani dan menghadapi ancaman *Cyber Warfare.* Kementerian Pertahanan dan TNI harus melakukan berbagai langkah dan tindakan sinergitas untuk menghadapi ancaman *Cyber Warfare.* Dalam kaitan untuk menciptakan sinergitas menghadapi *Cyber Warfare.*

Rekomendasi

Kementerian Pertahanan harus mampu melakukan koordinasi dan meningkatkan kerja sama dengan Kementerian Informasi dan Komunikasi (Kemenkominfo) dan membuat jalinan komunikasi, koordinasi dan kerja sama dengan komunitas pelaku informasi dan komunikasi, untuk mengantisipasi adanya serangan *cyber* berupa penyadapan telepon yang umum dilakukan oleh para penyerang dunia maya sehingga keamanan telepon dari masyarakat Indonesia, khususnya para pimpinan lembaga negara dapat terjamin dengan baik serta menjalin kerja sama dengan aktor-aktor keamanan, seperti Polri, BIN, Lembaga Sandi Negara, dan aktor keamanan lainnya untuk menyatukan pandangan tentang berbagai ancaman *cyber* beserta pembagian tugas dan langkah penanganan terpadu sehingga akan dapat menangkal berbagai serangan *cyber* ke dalam berbagai wilayah dunia maya Indonesia, termasuk penanganan *Cyber Crime* yang dapat meluas ke arah *Cyber Warfare*.

DAFTAR PUSTAKA

Peraturan Perundang-undangan:

Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang Republik Indonesia Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.

Undang-Undang Republik Indonesia Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJPN) Tahun 2005-2025.

Peraturan Presiden Republik Indonesia Nomor 5 Tahun 2010 tanggal 20 Januari 2010 tentang Rencana Pembangunan Jangka Menengah Nasional (RPJMN) Tahun 2010-2014.

Peraturan Presiden Republik Indonesia Nomor 41 Tahun 2010 tanggal 17 Juni 2010 tentang Kebijakan Umum Pertahanan Negara Tahun 2010-2014.

Peraturan Menteri Pertahanan Republik Indonesia Nomor 27 Tahun 2013 tanggal 12 September 2013 tentang Kebijakan Penyelenggaraan Pertahanan Negara tahun 2010-2014.

Peraturan Menteri Pertahanan Nomor 03 Tahun 2010 tanggal 29 Maret 2010 tentang Rencana Strategis Pertahanan Negara Tahun 2010-2014.

Peraturan Presiden Republik Indonesia Nomor 41 Tahun 2010 tanggal 17 Juni 2010 tentang Kebijakan Umum Pertahanan Negara Tahun 2010-2014

Peraturan Menteri Pertahanan Nomor 27 Tahun 2013 tentang Kebijakan Penyelenggaraan Pertahanan Negara Tahun 2010-2014

Buku:

Aji, Supriyanto, 2007, *Pengantar Tehnologi Informasi*, Semarang: Penerbit Salemba Infotek.

Arquilla, John dan David Rondfelt, 2001, *Networks and Netwars, The Future of Terror, Crime, and Militancy*, Rand Corporation.

Buzan, Barry, 1991, *People, State, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Hempstead: Harvester Wheatsheaf.

Frank G. Hoffman, *Conflict in the 21st Century, The Rise of Hybrid Wars*, Patomatic Institute, Virginia USA, Desember 2007.

Fred, Isjwara, 1980, *Pengantar Ilmu Politik*, Bandung: Binacipta.

Hadjon, Philipus M., 1987, *Perlindungan Hukum bagi Rakyat di Indonesia*, Jakarta: Bina Ilmu.

Iwama, Yoko, *International Donors and the Reform of Indonesian National Police*, Workshop 2010: Organizing Police Forces in Post-Conflict Peace-Support Operations, January 27-28th, 2010.

Jessup, Philip C., *A Modern Law of Nation, Pengantar Hukum Antar Bangsa*, Bandung: Nuansa.

Kelsen, Hans, 1971, *General Theory of Law and State*, New York: Russel and Russeu, diterjemahkan oleh Raisul Muttaqien, *Teori Umum Tentang Hukum dan Negara*, 2014, Bandung: Nusa Media Ujung Berung.

Liang, Qiao and Wang Xiangsui, 1999, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House.

Mahayana, Dimitri, 2000, *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*, Bandung: Rosda.

Manthovani, Reda, 2006, *Problematika dan Solusi Penanganan Kejahatan CYBER di Indonesia*, Jakarta: Malibu.

Nasibitt, John Nana Naisbitt dan Douglas Philips, 2001, *High Tech, High Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi*, Bandung: Mizan.

Noorhaidi, Hasan dan Bertus Hendriks, *Counter-Terrorism Strategies in Indonesia Algeria and Saudi Arabia*, Netherlands Institute of International Relations 'Clingendae".

Petri, Huovinen, *Hybrid warfare-Just a twist of compound warfare*, views on warfare from the United States Armed Forces perspective.

Reksoprodjo, Yono, 2014, *Kesiapan Nasional Bidang Pertahanan dalam Menghadapi Ancaman Siber*, Bahan Kuliah dalam bentuk power point, yang dipresentasikan di Sespim Polri, Lembang, 11 September.

Suhieno, 1986, *Ilmu Negara*, Yogyakarta: Liberty.

Jurnal:

Budiman, Ignatius, "Pesiapan Menghadapi Perang Hibrida", *Jurnal Yudhagama*, Volume 33 No. 2 Bulan Juni 2013.

Gollese, Petrus Reinhart, "Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri", *Buletin Hukum Perbankan*, Volume 4 Nomor 2, Agustus 2006.

Hovel, Devika, 2004, "Chinks in the Armour: International Law, Terrorism, and The Use of Force", *UNSW Journal*.

Jumadi, "Negara Hukum Demokratis Konstitusi Baru Indonesia", *Al-Risalah*, Vol. 11 No. 1 Mei 2011.

Muntoha, "Demokrasi dan Negara Hukum", *Jurnal Hukum*, No. 3 Vol. 16 Juli 2009.

Narande, Alva A.G., "Perang Hibrida di Dunia", *Jurnal Yudhagama*, Volume 33 No. 2 Bulan Juni 2013.

Purwanto, Adi Joko, "Peningkatan Anggaran Militer Cina dan Implikasinya terhadap Keamanan di Asia Timur", *SPEKTRUM Jurnal Ilmu Politik Hubungan Internasional*, Vol. 7, Juni 2010 .

Rumekso, Teguh Pudjo, "Hybrid Warfare dan Implikasinya Bagi Indonesia", *Jurnal Yudhagama*, Volume 33 No 2 Bulan Juni 2013.

Sefriani, "Ketaatan Masyarakat Internasional terhadap Hukum Internasional dalam Perspekti Filsafat Hukum", *Jurnal Hukum*, No. 3 Vol. 18, Juli 2011.

Sudarwanto, Al Sentot, "Cyber Bullying: Kejahatan Dunia Maya yang Terlupakan", *Jurnal Hukum Pro Justitia*, April 2009, Volume 27 No. 1.

Website:

Agus Subagyo, *"Sinergi dalam Menghadapi Ancaman Cyber Warfare Synergy on The Facing of Cyber Warfare Threat"*, diunduh https://agussubagyo1978.files.com/2015/08/sinergi-dalam-menghadapi-ancaman-cyber-warfare.pdf

Elizabeth Montabalno, *Auditor Find Dod Hasn't Defined Cyber Warfare*, September 2010, http://www. informationweek.com/government/security/auditorsfind-dod-hasnt-defined-cyber-wa/227400359

J. Aioro, *Defense Lacks Doctrine to guide it through Cyberwarfare*, 13 September 2010, http:// www.nextgov.com/defense/2010/09/defense-lacksdoctrine-to-guide-it-through-cyberwarfare/47575/

M. Akbar Marwan, *Ancaman Cyber Insider*, http://akbar.staff.gunadarma.ac.id

Manuel W. Wik, *Revolution in information affairs Tactical and strategic implication of information warfare and information operation*, Defence Materiel Administration, diakses 12 Juni 2016, pada < mawik@fmv.se>

Rosdiana, Deky, *"Cyber Warfare menjadi Ancaman NKRI di Masa Kini dan Masa Depan"*, dalam http://hankam.kompasiana.com/2013/09/23/cyber-warfaremenjadi-ancaman-nkri-dimasa-kini-dan-masa-depan-592343.html, diunduh pada 11 Maret 2015.

William S. Lind, *"Understanding Fourth Generation War"*, Military Review September-October 2004, http:// www.au.af.mil/au/awc/awcgate/milreview/lind.pdf