URGENSI KOMANDO PERTAHANAN SIBER *(CYBER DEFENSE COMMAND)* DALAM MENGHADAPI PEPERANGAN ASIMETRIS

B.T. Sutrisno SP [1]

Abstrak: Kemajuan teknologi jaringan internet membawa dampak positif dan negatif. Dampak positifnya adalah semakin mudahnya manusia untuk saling berkomunikasi dan mengembangkan jaringan sosial dan ekonomi, sedangkan dampak negatifnya adalah dunia maya (siber) telah menjadi sarana dan medan perang baru dalam peperangan asimetris. Sampai saat ini Indonesia belum mempunyai badan pertahanan siber nasional, sehingga sudah menjadi kebutuhan mendesak bagi Tentara Nasional Indonesia (TNI) untuk membentuk komando pertahanan siber *(cyber defense command)* dalam menghadapi peperangan asimetris di dunia maya sebelum perang tersebut terjadi di dunia nyata dan membahayakan kedaulatan dan keutuhan wilayah negara serta keselamatan segenap bangsa dan tumpah darah Indonesia.

Kata Kunci: *Perang Asimetris, Perang Informasi, Cyber Attack, Cyber Defense Command*

1. PENDAHULUAN

Perkembangan teknologi informasi yang didalamnya mencakup teknologi komunikasi dengan menggunakan jaringan internet menjadikan interaksi antar manusia di muka bumi semakin bebas tanpa dibatasi ruang dan waktu. Batas-batas Negara yang selama ini menjadi sekat pemisah komunikasi antar penduduk bumi saat ini semakin samar dan bukan lagi menjadi penghalang mengalirnya arus informasi dimana ketika terjadi sebuah peristiwa di bagian bumi belahan lain maka hampir pada waktu bersamaan informasi tentang peristiwa tersebut dapat diketahui di belahan bumi bagian lainnya, walaupun keduanya dipisahkan oleh jarak yang jauh dan zona waktu yang berbeda. Perkembangan tersebut di satu sisi merupakan sebuah keniscayaan yang sangat menguntungkan karena dapat mendukung perkembangan ekonomi dan hubungan sosial antar manusia, namun disisi lain juga merupakan ancaman jika dikaitkan dengan kedaulatan sebuah negara karena dengan semakin samarnya batas-batas Negara serta semakin terbatasnya kontrol Negara atas informasi yang mengalir tersebut. Kementrian Pertahanan Republik Indonesia dalam Buku Putih Pertahanan Indonesia tahun 2008 mendefinisikan ancaman sebagai berikut:

> *"Ancaman adalah setiap usaha dan kegiatan, baik dari luar maupun dari dalam negeri, yang dinilai mengancam atau membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan bangsa"*[2]

Dari definisi ancaman tersebut, kemudian berdasarkan sifatnya digolongkan dalam 2 bentuk yaitu ancaman militer dan ancaman nirmiliter. Ancaman militer adalah ancaman yang menggunakan kekuatan bersenjata dan terorganisasi yang dinilai mempunyai kemampuan membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa. Ancaman militer dapat berupa agresi, pelanggaran wilayah, pemberontakan bersenjata, sabotase, spionase, aksi teror bersenjata, ancaman keamanan laut dan udara, serta konflik komunal. Sedangkan Ancaman nir militer atau dikenal juga sebagai ancaman asimetris *(Asymmetric Threats)* adalah ancaman yang menggunakan faktor-faktor nir militer yang dinilai mempunyai kemampuan yang membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa yang dapat berdimensi ideologi, politik, ekonomi, sosial budaya, teknologi dan informasi.

Perkembangan jaringan internet merupakan bagian dari budaya manusia yang terus berevolusi mencari

[1] Bambang Trisutrisno, Pemerhati pertahanan dan mantan ketua Lembaga Kajian Pertahanan untuk Kedaulatan NKRI "KERIS" dapat dihubungi melalui email denbambang@gmail.com

[2] Departemen Pertahanan Republik Indonesia,2008.*Buku Putih Pertahanan Indonesia Tahun 2008*. Jakarta: Dephan RI.

kesempurnaan tanpa batas dalam mencari kemudahan berkomunikasi. Internet (kependekan dari *interconnection-networking*) mulai dikembangkan pada 1969 oleh Departemen Pertahanan Amerika Serikat *(US Department of Defense)* melalui proyek bernama ARPANET *(Advanced Research Project Agency Network)* dengan tujuan merancang dan membuat jaringan komputer yang tersebar namun saling terkoneksi satu dengan yang lain dan terpusatnya sebuah informasi hanya dalam satu station, sehingga apabila terjadi perang maka data dan informasi dapat cepat dipindahkan dari satu station ke station lain dan tidak mudah dihancurkan. Dalam pengembangannya, jaringan internet dibagi menjadi empat tahap jika didasarkan pada pemanfaatannya[3]. **Tahap pertama** disebut *Connectivity* yaitu dimana internet difokuskan untuk mendukung konektivitas dan pertukaran data antar komputer dalam jaringan. Dalam tahap ini, internet lebih banyak digunakan untuk pencarian *online, file sharing, browsing*, dan mengakses email. **Tahap kedua** dinamakan *Networked Economy* dengan fokus utama menjadikan internet untuk mendukung perdagangan dan bisnis sehingga pada tahap ini perdagangan via *online* dan *online shop* begitu populer. **Tahap ketiga** dinamakan *Immersive Experiences* dengan fokus menjadikan internet sebagai media dan memungkjnkan manusia dapat membangun relasi yang spesifik berdasarkan visi, misi, ide, gagasan, pertemanan, asal daerah, profesi dan lain-lain secara global tanpa memandang ruang dan waktu. **Tahap keempat** dari siklus pengembangan internet dinamakan *Internet of Everything* dimana pada tahap ini internet memungkinkan dan menjadi sebuah kewajaran jika manusia, data dan benda-benda saling berkomunikasi satu sama lain melalui internet. Jika melihat tahapan-tahapan tersebut, maka saat ini kita berada di tahap ketiga dan bersiap memasuki tahap keempat dalam pengembangan internet. Saat ini pengguna internet mulai akrab memanfaatkan situs jejaring media sosial, *Cloud Storage, Video Sharing*, Blog dan forum-forum diskusi di dunia maya. Kemunculan berbagai aplikasi situs jejaring sosial seperti *Myspace, Linkedin, Faceebok, Twitter* dan lain-lain menjadi suatu fenomena luar biasa dan dalam perkembangan di tahap ketiga ini, dimana jejaring sosial tersebut sudah menjadi bagian dari gaya hidup bahkan menjadi sebuah kebutuhan di masyarakat yang mempunyai dampak positif dan negatif. Dampak positifnya adalah masyarakat secara luas dapar dengan mudahnya mengakses informasi, berkomunikasi, dan mendapatkan wawasan lebih tentang perkembangan terbaru di dunia. Sedangkan dampak negatifnya adalah meningkatnya ancaman asimetris terhadap pertahanan dan kedaulatan Negara dengan menggunakan dunia maya seperti penyebaran informasi yang tidak benar, penggalangan opini, penghasutan dan kebocoran informasi rahasia.

2. PERANG ASIMETRIS DI DUNIA MAYA

Perang asimetris *(asymmetric warfare)* merupakan salah satu komponen utama dari perang generasi keempat *(fourth generation warfare)* dengan ciri semakin kaburnya batas antara perang dan politik atau antara tentara dan sipil, melibatkan dua aktor atau lebih, yang dilakukan oleh negara atau organisasi selain Negara *(non state actor),* kekuatan yang tidak seimbang dan mencakup spektum peperangan yang sangat luas. Banyak definisi tentang perang asimetris. Rod Thorton, dalam buku yang berjudul *"Asymmetric Warfare: Threat and Response in the 21st Century"*, mendefinisikan perang asimetris, sebagai berikut:

> *"Asymmetric Warfare is violent action undertaken by the "have-nots" against the "have" whereby the have-nots, be that state or sub-state actor, seek to generate profound effects-at all levels or warfare (however defined), from the tactical to the strategic-by employing their own specific relative advantages against*

[3] Detikinet,2013.*Ini Empat Tahapan Perkembangan Internet Dunia*. [online] terdapat di:<http://inet.detik.com/read/2013/06/27/083125/2285450/398/ini-empat-tahapan-perkembangan-internet-dunia> [diakses 20 Desember 2014].

the vulnerabilities of much stronger opponents"[4]

Sedangkan Dewan Riset Nasional (DRN) Komisi Teknis Pertahanan dan Keamanan dalam loka karya berjudul, *Suatu Pemikiran tentang Perang Asimetris* (*Asymetric Warfare*) pada 10 juli 2010 mendefinisikan perang asimetris sebagai berikut:

> *"Perang asimetris adalah suatu model peperangan yang dikembangkan dari cara berpikir yang tidak lazim, dan di luar aturan peperangan yang berlaku, dengan spektrum perang yang sangat luas dan mencakup aspek-aspek astagatra (perpaduan antara trigatra (geografi, demografi, dan sumber daya alam) dan pancagatra (ideologi, politik, ekonomi, sosial, dan budaya). Perang asimetris selalu melibatkan peperangan antara dua aktor atau lebih, dengan ciri menonjol dari kekuatan yang tidak seimbang".*[5]

Dari dua definisi diatas, menjadi salah satu ciri yang menonjol dalam perang asimetris adalah semakin kaburnya batasan akan perang dan semakin bervariasinya palagan yang digunakan, selain itu hadirnya *Non State Actor* yang mempu menimbulkan berbagai ancaman baik secara langsung atau tidak langsung terhadap pertahanan dan kedaulatan sebuah Negara seperti terrorisme, perdagangan manusia, kejahatan lintas Negara, pembajakan kapal di laut, pemberontakan, Narkotika dan *Cyber Crime* menjadikan perang asimetris lebih menakutkan dan lebih merusak daripada perang simetris. Hampir semua bentuk perang asimetris diatas dapat dilakukan di dunia maya (siber), namun yang saat ini paling menonjol adalah serangan siber *(Cyber Attack)* dan perang informasi *(Information Warfare)*:

2.1 Serangan Siber *(Cyber Attack)*

Kita dapat membayangkan ketika terdapat satu divisi pasukan yang ahli komputer da jaringan kemudian menggunakan keahliannya untuk mengoperasikan dan membajak jaringan komputer fasilitas-fasilitas publik seperti situs-situs pemerintah, pangkalan militer, perbankan, jaringan telekomunikasi, infrastruktur dan layanan transportasi. Apa yang akan terjadi?, apa yang akan masyarakat lakukan?. Gambaran singkat diatas merupakan contoh dampak yang bisa diakibatkan serangan siber yang bisa lebih menghancurkan dan mengacaukan daripada serangan bom. Banyak definisi tentang serangan siber, namun secara umum didefinisikan sebagai serangan yang dilakukan oleh sebuah Negara atau kelompok *(Non State Actor)* yang menggunakan jaringan komputer, internet dan dunia maya *(Cyber Space)* dengan tujuan melakukan gangguan, pencurian data atau membuat kerusakan sistem komputer dan jaringan sebuah Negara atau kelompok lain. Beberapa serangan siber terkenal diantaranya adalah: **Pertama**, serangan Titan Rain pada tahun 2003 yang kemudian diketahui berasal dari beberapa lokasi di Tiongkok, walau belum dapat dipastikan apakah pelakunya individu atau memang sengaja disponsori oleh negara tirai bambu tersebut dengan tujuan untuk memata-matai negara lain terutama Amerika Serikat dan sekutunya. Serangan ini berlangsung secara terus menerus selama tiga tahun dan menyasar institusi penting di Amerika Serikat seperti NASA dan Lockheed Martin. **Kedua**, serangan siber besar-besaran melanda Estonia pada 27 April 2007, yang melumpuhkan berbagai institusi penting negeri tersebut seperti parlemen, situs-situs pemerintahan, perbankan dan situs-situs surat kabar lokal. Akibat serangan ini, sistem pemerintahan Estonia hampir lumpuh selama 2 (dua) minggu. Beberapa pengamat meyakini serangan ini merupakan salah satu yang tercanggih dan sistematis dengan menggunakan *Distributed Denial of Service* (DDOS) dengan berbagai macam metode, dan menduga pelakunya didukung Rusia sebagai protes kebijakan Perdana Menteri Estonia saat itu Andrus Ansip yang membongkar sebuah monumen tentara

[4] Thornton, Rod, 2006. *Asymmetric Warfare: Threat and Response in the 21st Century*. Cambridge: Polity Press.
[5] Kompas Tekno,2008. *Perang Asimetris, Bentuk Perang Baru*. [online] terdapat di: <http://tekno.kompas.com/read/2008/07/10/21091857/perang.asimetris.bentuk.perang.baru> [diakses 20 Desember 2014].

Rusia dari ibu kota Estonia, Stallin. **Ketiga**, serangan Aurora pada tahun 2009 dimana para hacker yang diyakini berasal dari tiongkok menyerang dan berhasil mencuri properti intelektual dari perusahaan-perusahaan besar seperti Google dan Adobe Systems. **Keempat**, serangan Stuxnet dengan menggunakan cacing komputer *(Worm)* yang berhasil melumpuhkan pembangkit nuklir Bushehr atau Natanz di Iran pada tahun 2010 yang sempat menjadi isu hangat karena menyangkut fasilitas nuklir yang cukup berbahaya. Awalnya Stuxnet dikira hanya worm biasa yang cukup canggih, namun para peneliti kemudian menemukan worm itu menargetkan sistem khusus bernama *Supervisory Control and Data Acquisition* (SCADA) yang digunakan untuk mengendalikan sistem pipa, pembangkit listrik tenaga nuklir dan perangkat manufaktur lainnya. Serangan Stuxnet merupakan 'worm' pertama yang secara khusus dibuat untuk menyerang infrastruktur dunia nyata seperti pembangkit listrik dan pembangkit tenaga air. Seorang peneliti keamanan siber asal Jerman, bernama Ralph Langner yang telah berhasil memecahkan kode Stuxnet mengatakan Stuxnet adalah 100 persen diarahkan untuk serangan siber yang bertujuan menghancurkan proses industri di dunia fisik, dan bukan tentang spionase. Pemerintah Iran saat itu meyakini dalang serangan ini adalah Amerika Serikat atau Israel, dan seiring waktu diketahui bahwa memang Amerika Serikat dan Israel berada dibalik program virus Stuxnet berdasarkan laporan wartawan New York Times, David Sanger pada Juni 2012[6]. **Kelima,** serangan Flame pada tahun 2012 yang juga menyerang jaringan komputer yang menangani sektor minyak Iran. Virus flame diduga merupakan turunan dari Stuxnet dan disebut sebagai salah satu virus komputer paling perkasa karena mempunyai kemampuan "menyambar" setiap data yang ada dan "menguping" di komputer si pengguna. Pemerintah Iran lagi-lagi meyakini dalang serangan ini adalah Amerika Serikat atau Israel. **Keenam,** serangan siber yang terakhir dan masih hangat adalah yang diduga dilakukan oleh hacker Korea Utara terhadap perusahaan film Sony Pictures karena pembuatan film komedi berjudul "The Interview" yang isinya mengolok-olok rezim ditaktor Kim Jong-un.

Gambar 1.1 *Cyber Attack by Country* (http://www.intellectualtakeout.org/library/chart-graph/cyber-attack-country)

Dari rangkaian beberapa contoh diatas terlihat bahwa serangan siber merupakan bentuk perang asimetris yang sangat efisien, sistematis, terstuktur dan mempunyai resiko yang kecil namun dapat mengakibatkan kerusakan yang bisa jadi lebih besar daripada perang secara konvensional.

2.2 Perang Informasi Menggunakan Siber

Banyak definisi tentang perang informasi. Departemen Pertahanan Amerika Serikat (US DOD) dalam *DOD Dictionary of Military and Associated Terms* mendefinisikan perang informasi sebagai berikut:

> *"Information Operations (IO) The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. See also electronic warfare; military deception; operations security; military information support operations".*[7]

[6] Tempo,2013. *Stuxnet, Senjata Cyber AS-Israel Melawan Iran*. [online] terdapat di: <http://www.tempo.co/read/news/2013/08/21/116506224/Stuxnet-Senjata-Cyber-AS-Israel-Melawan-Iran> [diakses 20 Desember 2014].

[7] DOD Dictionary of Military and Associated Terms, 2010. *DOD Dictionary of Military and Associated Terms 08 November 2010, as amended through 15 November 2014.* [pdf] DOD Dictionary of Military and Associated Terms. terdapat di

Dalam perang informasi, data atau informasi merupakan target utama yang diserang dengan beberapa strategi sebagai berikut: **Pertama**, membuat penolakan akses terhadap data *(Deny)* dengan tujuan untuk penghapusan data atau menghambat pihak lawan mengakses datanya sendiri, **Kedua**, mengacaukan atau menghancurkan data *(Disrupt)*. **Ketiga**, melakukan pencurian data *(Steal)*. **Keempat**, melakukan manipulasi data *(Manipulation)* dengan cara melakukan penambahan, pengurangan, maupun perubahan data sehingga lawan memiliki persepsi yang berbeda terhadap maksud dan tujuan sebenarnya dari data atau informasi yang mereka miliki.[8] Seiring kemajuan teknologi informasi khususnya jaringan internet, perang informasi saat ini tidak lagi dilakukan saat krisis atau konflik sedang berlangsung, namun cenderung dibangun jauh-jauh hari melalui media dan dunia maya (siber). Jumlah pengguna internet saat ini yang hampir menembus angka 3 miliar pengguna menjadikan jaringan internet merupakan sarana yang sangat efektif untuk melakukan perang informasi, sehingga sekarang banyak kita jumpai berbagai situs-situs "mainstream" yang berisi propaganda untuk membentuk opini para pengguna internet sehingga mendukung tujuan tertentu.

Gambar 1.2 Tampilan situs propaganda Orgnisasi Papua Merdeka (OPM)
http://www.komnas-tpnpb.net

Selain menggunakan situs, tren penggunaan aplikasi media sosial seperti facebook, twitter, youtube, skype untuk mengorganisir, mengumpulkan informasi, berkomunikasi, propaganda dalam perang informasi sudah terbukti mampu mendorong sebuah perlawanan, pemberontakan bahkan revolusi sebuah negara. Gelombang kebangkitan dunia arab atau yang lebih dikenal dengan *The Arab Spring* merupakan contoh nyata dimana perang informasi dan perang asimetris saat ini semakin mudah hadir seiring perkembangan jaringan internet, sehingga sudah menjadi keharusan Negara untuk dapat menjaga informasi yang dimilikinya serta mempunyai kemampuan untuk melakukan perang informasi tandingan terhadap data dan informasi yang tidak benar dengan ikut terjun secara aktif di media sosial sehingga dapat dengan segera membuat data dan informasi tandingan sebelum data dan informasi yang tidak benar tersebut sampai kepada masyarakat secara luas.

3. URGENSI KOMANDO PERTAHANAN SIBER

Semakin tinggi tingkat ketergantungan pemerintah dan masyarakat sebuah Negara terhadap suatu teknologi maka pada waktu yang bersamaan maka semakin besar pula ancaman dengan menggunakan teknologi tersebut terhadap masyarakat dan kedaulatan Negara. Begitu juga dengan kemajuan teknologi jaringan internet yang saat ini hampir mampu menghubungkan seluruh dimensi kehidupan manusia kedalam dunia maya (siber), membuat Negara-negara barat maupun negara "kekuatan baru" seperti China, Rusia dan Iran menjadikan dunia siber sebagai matra atau dimensi baru yang harus dijelajahi, dikuasai dan dipertahankan setelah darat, laut, udara dan angkasa luar. Selain menetapkan dunia siber sebagai matra baru, Negara-negara tersebut juga berlomba-lomba membangun infrastruktur keamanan dan pertahanan siber *(Cyber Defense)* serta merekrut para ahli melalui kompetisi di universitas-universitas ternama dan menjadikan mereka sebagai tentara siber *(cyber soldier)* yang tidak lagi dibekali dengan senapan serbu namun seperangkat komputer yang terhubung dengan jaringan internet. Angkatan Darat Amerika Serikat (US Army) dalam *Cyberspace Operations Concept Capability*

<http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf> [diakses 20 Desember 2014].

[8] Hutchinson, Bill, & Warren, Matt,2001. *Information Warfare: Corporate attack and defence in a digital world*. Massachusetts: Butterworth-Heinemann, pp.03-04.

Plan 2016-2028 mendefiniskan pertahanan siber atau *cyber defense* sebagai berikut:

> *"Cyber Defense (CyD) is actions combine information assurance, computer network defense (to include response actions), and critical infrastructure protection with enabling capabilities (such as EP, critical infrastructure support, and others) to prevent, detect, and ultimately respond to an adversaries ability to deny or manipulate information and/or infrastructure. CyD is integrated with the dynamic defensive aspects of CyberWar to provide defense in depth"*[9]

Sampai saat ini Indonesia belum mempunyai badan yang secara khusus menangani keamanan dan pertahanan siber secara nasional, dan hanya memiliki beberapa badan dibawah kementrian, kepolisian dan komunitas independen yang fokus melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet, antara lain: *Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center* (Id-SIRTII/CC) dibawah Kementrian Komunikasi dan Informatika (KOMINFO), Sub dit IT/Cyber Crime Mabes POLRI dan komunitas *Indonesia Computer Emergency Response Team* (ID-CERT). Padahal, menurut lembaga riset pasar e-Marketer Indonesia menempati urutan ke enam sebagai Negara dengan pengguna internet terbanyak setelah Tiongkok, Amerika Serikat, India, Brasil, dan Jepang dimana jumlah pengguna internet di Indonesia pada tahun 2014 ini mencapai 83,7 juta orang.[10] Hal tersebut membuktikan bahwa dunia maya telah menjadi bagian dari kehidupan masyarakat Indonesia dan bukan tidak mungkin telah dijadikan "medan perang baru" para musuh Indonesia untuk melancarkan serangan asimetris yang dapat mengganggu, merugikan bahkan membahayakan kedaulatan dan keselamatan negara. Dengan potensi ancaman tersebut, maka sudah menjadi kebutuhan yang mendesak bagi Kementrian Pertahanan dan Tentara Nasional Indonesia untuk membentuk komando pertahanan siber *(Cyber Defense Command)* agar mampu sejak dini mengantisipasi segala ancaman dan sebelum ancaman itu benar terjadi di dunia nyata. Untuk mengembangkan komando pertahanan siber tersebut, setidaknya diperlukan tiga hal penting yang harus dipersiapkan dan disepakati para *stakeholder* yaitu landasan hukum, infrakstuktur dan bentuk dan kendali organisasi.

3.1 Landasan hukum

Indonesia telah mempunyai berbagai piranti undang-undang yang dapat digunakan sebagai landasan hukum pembentukan komando pertahanan siber TNI. Undang-undang tersebut antara lain adalah:

a. Undang-undang RI nomor 36 Tahun 1999 tentang Telekomunikasi;
b. Undang-undang RI nomor 3 Tahun 2002 tentang Pertahanan Negara;
c. Undang-undang RI nomor Tahun 2003 tentang Penerapan Peraturan Pemerintah Pengganti Undang-undang RI No 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme;
d. Undang-undang RI nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia;
e. Undang-undang RI nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
f. Undang-undang RI nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
g. Peraturan Presiden Republik Indonesia Nomor 10 Tahun 2010 tentang Susunan Organisasi Tentara Nasional Indonesia.

3.2 Infrastuktur

Infrastuktur jaringan internet merupakan salah satu bagian terpenting

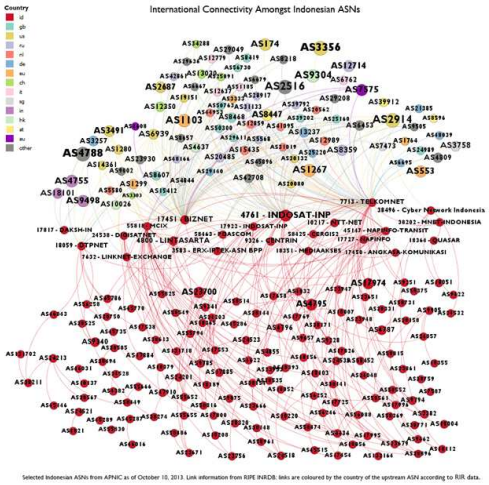
[9] The U.S. Army, 2010. *The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028*. [pdf] The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028. terdapat di < https://www.fas.org/irp/doddir/army/pam525-7-8.pdf> [diakses 20 Desember 2014].

[10] Kompas Tekno,2014. *Pengguna Internet Indonesia Nomor Enam Dunia*. [online] terdapat di:<http://tekno.kompas.com/read/2014/11/24/07430087/Pengguna.Internet.Indonesia.Nomor.Enam.Dunia> [diakses pada 20 Desember 2014].

dari pertahanan siber. Saat ini Indonesia tidak memiliki sistem infrastruktur Internet yang tersentralisasi dan memiliki banyak sambungan ke jaringan internasional yang dikenal dengan sebutan *Autonomous System Numbers* (ASN). Banyaknya jumlah ASN tersebut mengakibarkan sambungan Internet Indonesia rawan putus dan rawan potensi penyadapan, penyusupan dan penyerangan karena ibarat rumah, terdapat banyak pintu yang dapat digunakan untuk keluar masuk.

Gambar 1.4 Konektivitas internasional diantara ASN di Indonesia (Sumber APNIC)

Untuk mendukung pembentukan komando pertahanan siber, perlu dilakukan pembenahan secara terus menerus terhadap infrastruktur jaringan domestik maupun sambungan ke jaringan internasional khususnya penataan tentang sentralisasi sambungan internasional sehingga akan menunjang konektivitas dan sinergi pengamanan data dan informasi dari potensi penyusupan dan serangan dapat dicegah sejak dini. Selain masalah ASN, Kecepatan akses Internet Indonesia saat ini masih sangat lambat bahkan mas kategori paling lambat di kawasan. Data yang dirilis perusahaan penyedia jasa *cloud* dan *Internet Monitoring*, Akamai Technologies dalam laporan *State of the Internet* untuk kuartal kedua tahun 2014 menempatkan Indonesia di urutan ke-101 dengan kecepatan rata-rata dengan rata-rata 2,5 Mbps, kalah jauh dibandingkan dengan Singapura dengan kecepatan 10,4 Mbps dan Malaysia dengan kecepatan 4,3 Mbps[11]. Sebenarnya Kementrian Komunikasi dan Informatika (Kominfo) telah berusaha untuk meningkatkan konektivitas tersebut dengan meluncurkan program *"Indonesia Connected"* melalui jaringan kabel fiber-optic "Palapa Ring" di seluruh Indonesia. Proyek Palapa Ring memiliki 35.280 kilometer kabel bawah laut dan banyak dari kabel-kabel tersebut dihubungkan ke Singapura yang berada di persimpangan jalan antara Asia Pasifik dan Eropa dan merupakan pusat untuk banyak kabel bawah laut yang digunakan untuk infrastruktur Internet dan telekomunikasi [12].



Gambar 1.4 Infrastuktur jaringan kabel bawah laut yang aktif dan melalui Indonesia (http://submarinecablemap.com/#/country/indonesia)

3.3 Bentuk dan Kendali Organisasi

Banyak definisi dari bentuk komando pertahanan siber *(cyber defense command)*, namun umumnya didefinisikan sebagai badan atau satuan militer yang bertugas memonitor dan mengelola operasi pertahanan dunia maya dan keamanan siber militer serta mampu melaksanakan serangan terhadap menggunakan jaringan internet terhadap target tertentu. Melihat urgensinya, maka bentuk dan kendali organisasi komando pertahanan siber TNI setara dengan komando utama operasi (Kotama Ops) yang berkedudukan di bawah dan bertanggung jawab langsung kepada panglima TNI, dan personelnya merupakan gabungan prajurit dari TNI Angkatan Darat, TNI Angkatan Laut dan TNI Angkatan Udara yang memiliki kemampuan lebih dalam teknologi jaringan

[11] Liputan6,2014. *Kecepatan Internet Indonesia Masuk Kategori Paling Lambat*.[online] terdapat di < http://tekno.liputan6.com/read/2113835/kecepatan-internet-indonesia-masuk-kategori-paling-lambat > [diakses 22 desember 2014]

[12]Citizenlab,2013. *Pemaparan Infrastruktur dan Tata Kelola Internet di Indonesia*.[online] terdapat di < https://citizenlab.org /2013/10/igf2013-pemaparan-infrastruktur-dan-tata-kelola-internet-di-indonesia> [diakses 21 Desember 2014]

internet, teknologi informasi komunikasi dan komunikasi media sosial.

4. PENUTUP

Dunia maya (siber) merupakan sebuah keniscayaan bagi kehidupan umat manusia di era globalisasi yang mampu menjadi alat penghubung interaksi antar manusia dimuka bumi tanpa dibatasai jauhnya jarak dan perbedaan zona waktu. Kondisi ini bukannya tanpa resiko, karena semakin tinggi tingkat ketergantungan masyarakat sebuah Negara terhadap suatu teknologi maka pada waktu yang bersamaan maka semakin besar pula ancaman yang dapat ditimbulkan akibat penyalahgunaan teknologi tersebut yang merusak atau mengacaukan kehidupan masyarakat bahkan Negara. Serangan worm stuxnet terhadap sistem komputer fasilitas nuklir iran, gelombang *arab spring* yang berujung pada tergulingnya presiden mesir dan perang saudara di suriah adalah salah satu contoh nyata dimana internet dan dunia siber sangat ampuh digunakan untuk perang asimetris dimasa kini dan akan datang. Indonesia sebagai Negara berdaulat sampai saat ini belum mempunyai lembaga keamanan dan pertahanan siber nasional untuk menghadapi perang siber *(Cyber Warfare)*, sehingga sudah menjadi kebutuhan mendesak pembentukan komando pertahana siber *(Cyber Defense Command)* untuk mendukung tugas pokok TNI dalam menghadapi perang generasi keempat yang tidak lagi hanya berwujud serangan bersenjata namun lebih kepada serangan asimetris dengan menggunakan jaringan internet dan dunia siber.

DAFTAR PUSTAKA

Departemen Pertahanan Republik Indonesia,2008.Buku Putih Pertahanan Indonesia Tahun 2008. Jakarta: Dephan RI.

Detikinet,2013.Ini Empat Tahapan Perkembangan Internet Dunia. [online] terdapat di:<http://inet.detik.com/read/2013/06/27/083125/2285450/398/ini-empat-tahapan-perkembangan-internet-dunia> [diakses 20 Desember 2014].

Thornton, Rod, 2006. Asymmetric Warfare: Threat and Response in the 21st Century. Cambridge: Polity Press.

Kompas Tekno,2008. Perang Asimetris, Bentuk Perang Baru. [online] terdapat di: <http://tekno.kompas.com/read /2008/07/10/21091857/perang.asimetris. bentuk.perang.baru> [diakses 20 Desember 2014].

Tempo,2013. Stuxnet, Senjata Cyber AS-Israel Melawan Iran. [online] terdapat di: <http://www.tempo.co/read/news /2013/08/21/116506224/Stuxnet-Senjata-Cyber-AS-Israel-Melawan-Iran> [diakses 20 Desember 2014].

DOD Dictionary of Military and Associated Terms, 2010. DOD Dictionary of Military and Associated Terms 08 November 2010, as amended through 15 November 2014. [pdf] DOD Dictionary of Military and Associated Terms. terdapat di <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf> [diakses 20 Desember 2014].

Hutchinson, Bill, & Warren, Matt,2001. Information Warfare: Corporate attack and defence in a digital world. Massachusetts: Butterworth-Heinemann, pp.03-04.

The U.S. Army, 2010. The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028. [pdf] The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028. terdapat di < https://www.fas.org/irp/doddir/army/pam525-7-8.pdf> [diakses 20 Desember 2014].

Kompas Tekno,2014. Pengguna Internet Indonesia Nomor Enam Dunia. [online] terdapat di:<http://tekno.kompas.com/read/2014/11/24/07430087/Pengguna.Internet.Indonesia.Nomor.Enam.Dunia> [diakses pada 20 Desember 2014].

Liputan6,2014. Kecepatan Internet Indonesia Masuk Kategori Paling Lambat.[online] terdapat di < http://tekno.liputan6.com/read/2113835/kecepatan-internet-indonesia-masuk-kategori-paling-lambat > [diakses 22 desember 2014]

Citizenlab,2013. Pemaparan Infrastruktur dan Tata Kelola Internet di Indonesia.[online] terdapat di < https://citizenlab.org /2013/10/igf2013-pemaparan-infrastruktur-dan-tata-kelola-internet-di-indonesia> [diakses 21 Desember 2014]