Perlunya Pembangunan Sistem Pertahanan Siber (*Cyber Defense*) yang tangguh bagi Indonesia

Oleh : Letkol Chb Ir. Bagus Artiadi Soewardi, M.Si.*)

Pendahuluan

Kemajuan ilmu pengetahuan dan teknologi membawa berbagai implikasi kompleks dalam kehidupan manusia dan hubungan antar negara. Semenjak dikenalnya pola komunikasi melalui dunia maya atau internet, batas-batas konvensional yang dahulu dianut dan dipatuhi oleh konsensus internasional menjadi semu. Dalam hampir satu dekade ini, isu tentang perang siber (*cyber war*) terus didengungkan, bahkan diramalkan bisa memicu ketegangan antar Negara yang berimbas pada terancamnya kedamaian dunia. Bahkan Kepala Badan Telekomunikasi PBB, Toure Hamadoun, pada Oktober 2009 telah memperingatkan bahwa perang dunia bisa terjadi di dunia maya.

Kenyataan bahwa perang siber telah menjadi mandala perang baru sudah di depan kita semua. Penyerangan secara terbatas telah terjadi berkali-kali oleh beberapa negara, dimana kondisi ini dapat juga diasumsikan sebagai uji coba, namun peperangan yang sesungguhnya dan jauh lebih besar telah dipersiapkan berdasarkan urutan kronologis kejadian pada jaringan komputer di dunia yang telah terjadi antara tahun 1990-an sampai 2012 yaitu : *Internet social engineering attacks, Network sniffers, Packet spoofing, Hijacking sessions, Automated probes and scans, GUI (Graphical User Interface) intruder tools, Automated widespread attacks, Widespread denial-of-service attacks, Executable code attacks (against browsers), Techniques to analyse code with Vulnerabilities without source, Widespread attacks on DNS*

infrastructure, Widespread attacks using NNTP to distribute attack, "Stealth" and other advanced scanning techniques, Windows-based remote controllable Trojans (Back Orifice), Email propagation of malicious code, Wide-scale Trojan distribution,Distributed attack tools, Distributed Denial of service (DDoS) attacks,Targeting of specific users, Anti-forensic techniques, Wide-scale use of worms, dan Sophisticated command and control attacks.

Trend ancaman serangan siber akan berkembang terus sesuai perkembangan teknologi informasi, oleh karenanya perlu dilakukan riset secara terus-menerus untuk mampu mengatasi berbagai teknik, taktik dan, strategi pertahanan siber yang akan terus berkembang ke depan. Bila kita berbicara pertahanan, maka terlebih dahulu harus ditetapkan ancaman. 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 (*cyber crime*), dimana 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 (*cyber defense*).

Sekilas Perang Siber (*Cyber Warfare*)

Perang di dunia siber merupakan perang yang sudah menggunakan jaringan komputer dan Internet atau ranah siber (*cyber space*) dalam bentuk strategi pertahanan atau penyerangan sistim informasi lawan. Perang siber mengacu pada penggunaan fasilitas www (*world wide web*) dan jaringan komputer untuk melakukan perang di dunia maya. Pelakunya memanfaatkan teknologi komputer dan internet untuk saling bersaing dan menguasai, mengganggu, menghentikan komunikasi dan bahkan merubah arus informasi dan isi serta berbagai tindakan lain yang dapat merugikan dan menghancurkan lawan. Pembentukan opini publik dan internasional terhadap suatu kepentingan baik berupa kampanye,

propaganda serta agitasi kini juga marak dilakukan melalui internet. Kelompok yang berkepentingan tersebut dapat dengan mudah melakukan hal tersebut tanpa perlu mengeluarkan banyak biaya dan sumber daya seperti halnya di masa lampau.

Cybercrime dan *cyberwar* tidak hanya membahayakan keamanan individu dengan terambilnya akses pada aset yang dimiliki. Kejadian yang menonjol antara lain: pencurian identitas dan data (sumber daya informasi) serta pembajakan akun, kasus penyebaran virus yang disisipkan di dalam file dan web site serta kode-kode penting, fitnah, penistaan maupun pencemaran nama baik. Demikian pula dengan spionase industri dan penyanderaan sumber daya informasi kritis yang marak terjadi saat ini. Kesemuanya telah menimbulkan keresahan di masyarakat karena telah hilangnya privasi dan ancaman kehilangan aset serta kekayaan yang dimiliki. Dunia siber juga dapat digunakan sebagai alat politik melalui penyebaran kabar bohong untuk tujuan provokasi politis maupun rekayasa ekonomi. Interkoneksi internet juga memungkinkan terjadinya serangan yang bertujuan melumpuhkan dan menghancurkan sumber daya negara lawan tanpa perlu mendekati objek tersebut. Hal tersebut perlu diwaspadai karena pelakunya bisa beraneka ragam dan saling bekerja sama walaupun memiliki kepentingan yang berbeda.

Paradigma keamanan nasional telah bergeser kepada aspek yang lebih luas yaitu termasuk jaminan keamanan pribadi warga negara. Kewajiban pokok dari suatu negara adalah memberikan keamanan terhadap warganyanya tersebut termasuk keamanan dari berbagai kejahatan siber. Data pada Kemkominfo mencatat bahwa rata-rata jumlah serangan dunia maya per hari pada tahun 2011 mencapai 1,25 juta insiden, dimana aktivitas ini cenderung semakin meningkat berbanding lurus dengan pengguna internet. Setiap saat warga negara dapat merasa terancam pada aset yang dimilikinya. Privasi dan berbagai informasi rahasia dapat dengan mudah dihancurkan oleh para pelaku kejahatan siber ini, dimana bila eskalasinya semakin meluas, dapat membuat keresahan yang meluas pada masyarakat. Dalam jangkauan yang lebih luas, keterbatasan penguasaan teknologi negara dan belum adanya regulasi yang lebih tegas mengenai pertahanan siber dapat membahayakan negara secara nyata. Negara lain ataupun kelompok dengan kepentingan tertentu dapat dengan mudah memasuki ranah infrastruktur vital yang dimiliki negara kita.

Semakin tinggi ketergantungan suatu masyarakat akan teknologi informasi, semakin tinggi pula resiko yang dihadapi. Saat ini semua aspek perekonomian, sosial dan pertahanan begitu tergantung kepada internet. Aktivitas perbankan, transaksi perekonomian, pemeliharaan dan penggunaan transportasi, pengendalian persenjataan hingga komunikasi sosial tidak bisa terlepas dari interkoneksi tersebut. Semua orang mendapatkan kesempatan dan kemungkinan yang sama di seluruh dunia untuk masuk di dalamnya, sehingga sangat dimungkinkan setiap individu mampu untuk mengobrak abrik sistem yang ada hingga mampu membobol dan menguasai aset serta pertahanan individu maupun negara lain dengan cara yang amat mudah. Pemerintah perlu bekerjasama dengan pihak-pihak maupun negara lain untuk

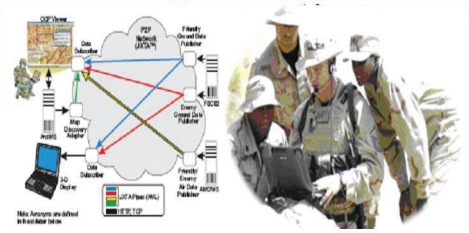
membangun keamanan global. Satu negara tidak akan mungkin dapat membuat perlindungan terhadap dirinya sendiri dalam menghadapi ancaman global tersebut.

Kerjasama antar negara diharapkan juga mampu mencetuskan sebuah regulasi dibidang siber (*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.

Organisasi Cyber Defense di dunia.

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. Al Jazeera (19/2/2012) menyebutnya sebagai *'fifth dimension of warfare'* selain darat, laut, udara, dan ruang angkasa. Alasannya, inovasi teknologi sedang mengubah taktik perang modern, mengubah dunia siber menjadi garis depan pertempuran.



Dijadikannya ranah siber sebagai matra perang kelima cukup beralasan, karena semua negara pasti ingin meningkatkan kemampuan untuk mengamankan diri dari serangan musuh. Kemajuan pesat teknologi informasi dan komunikasi dewasa ini akan menjadi landasan penting bagi pengembangan doktrin militer di masa mendatang. Dengan demikian teknologi informasi dan komunikasi akan sangat mempengaruhi perubahan strategi militer.

Amerika Serikat memiliki *United States Cyber Command* (US CYBERCOM) di bawah *United States Strategic Command* (US STRATCOM) yang mulai diaktifkan pada tahun 2009, sebagai antisipasi terhadap banyaknya serangan cyber terhadap jaringan komputer, internet, maupun infrastruktur di negara tersebut. Pada tahun 2011, Kementerian Pertahanan Amerika Serikat (US DoD) bahkan telah mendeklarasikan bahwa internet atau dunia maya sebagai matra tempur baru, seperti halnya darat, laut dan udara. Keputusan ini merupakan jawaban dari banyaknya insiden pencurian data dan teknologi militer Amerika Serikat.

NATO, NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) merupakan badan keamanan cyber pakta pertahanan atlantik utara (NATO) yang didirikan pada 14 Mei 2008 dalam rangka meningkatkan kemampuan pertahahanan cyber NATO. NATO CCD COE bermarkas di kota Tallinn, Estonia. Pusat keamanan cyber ini merupakan hasil kerjasama berbagai Negara anggota NATO untuk meningkatkan keamanan terhadap sistem jaringan komputer Negara-negara anggota NATO.

Israel, Israel diketahui mempunyai sebuah unit khusus bernama Unit 8200 yang mempunyai spesialisasi *cyber warfare* dibawah Israel *Defense Forces* (IDF). Salah satu catatan keberhasilan yang fenomenal dari unit ini adalah ketika Unit 8200 berhasil menghentikan operasi radar senjata anti pesawat udara Suriah. Bahkan serangan worm Stuxnet terhadap sistem komputer fasilitas nuklir Iran pada awal tahun 2011 ini disebut-sebut merupakan hasil kerja dari unit ini.

Australia, Australia melihat

tantangan kedepan potensi keamanan *cyber* yang menjadi sangat serius dan memungkinkan mempengaruhi pertahanan negara, sehingga Direktorat Pertahanan Sinyal Departemen Pertahanan Australia membuat sebuah badan bernama *Cyber Security Operations Centre* (CSOC) yang bertanggung jawab untuk mendeteksi dan menangkal ancaman kejahatan cyber terhadap kepentingan dan pemerintah Australia

Yang terbaru adalah Cina yang juga telah membentuk pasukan dunia maya. Pasukan tersebut diberi nama *"Blue Army"*, pasukan ini bertugas melindungi negara dari serangan cyber. Skuad digital ini akan berbasis di kawasan militer Guangzhou, sebelah selatan China.

Inggris juga membangun pertahanan cyber. Sistem yang disebut *Cyber Security Operations Centre* (CSOC) itu berada di *Government Communications Headquarters* (GCHQ) Inggris, di Cheltenham, sekitar 160 kilometer arah barat laut London.

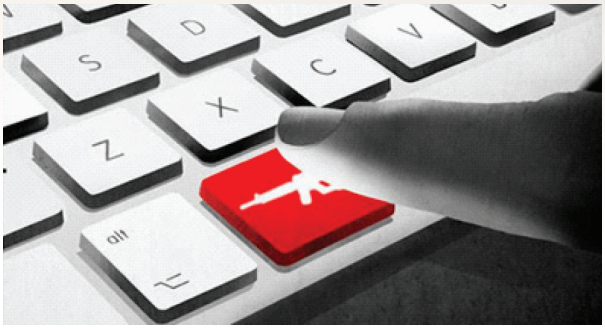
Bagaimana dengan Indonesia ?

Sejak 1998, Indonesia telah melakukan perang *cyber* 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. Sementara pada 1999 juga muncul kerusuhan di dunia maya antara Indonesia dan Portugal menyangkut kasus Timor-Timur. Bahkan ketika terjadi "perang" dengan Portugal, saling serang terjadi hingga masuk sistem dan mampu menghapus semua data.

Pada tanggal 6 Agustus 2010, Symantec (Produsen Antivirus Norton) mengumumkan bahwa Indonesia berada di urutan kedua setelah Iran diantara 10 negara yang mengalami serangan *worm Stuxnet*. *Stuxnet* adalah *worm* yang khusus menyerang komputer berbasis operasi Windows. Pada tanggal 20 dan 23 November 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. Peristiwa ini pun diduga dilakukan oleh Israel dan Amerika Serikat sebagai penentang utama Program Nuklir Iran.

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. Pertahanan militer berbasis siber penting bagi Indonesia. Karena di negara ini semakin banyak infrastruktur strategis dan layanan publik yang bergantung pada sistem informasi, teknologi dan jaringan internet. Sehingga rentan terhadap ancaman, gangguan dan serangan dari pihak lain, seperti sistem transmisi dan distribusi energi, sistem pertahanan udara, sistem transportasi, layanan publik, perbankan dan sebagainya.

Patut disyukuri, saat ini Indonesia pun mulai mengarahkan corong meriamnya ke arah pertempuran dunia maya. Kementerian Pertahanan menyikapi perang dunia maya ini dengan mulai aktif menggelar seminar maupun lokakarya yang melibatkan Kementerian/LPNK, Perguruan Tinggi, Pakar dan pihak lainnya untuk merumuskan sistem teknologi informasi terpadu dalam menghadapi perang teknologi informasi melalui dunia maya, yang dikemas dalam konsep Sistem Pertahanan Dunia Maya (*Cyber Defense*). Sehingga pada tanggal 23 Oktober 2012 Menteri Pertahanan telah membentuk Tim Kerja Pertahanan Dunia Maya, yang diketuai oleh Dirjen Pothan Kemhan dan beranggotakan unit terkait pada Satuan Kerja Kementerian Pertahanan serta Nara Sumber dari Kementerian/ LPNK, Perguruan Tinggi, Para Pakar maupun tokoh masyarakat dunia maya, dimana Tim Kerja ini secara garis besar bertugas merumuskan Roadmap Strategi Nasional pertahanan negara yang berkaitan dengan ancaman dunia maya serta menyiapkan pembentukan organisasi pertahanan dunia maya berskala nasional (*National Cyber Defense*). Demikian pula dengan TNI, sebagai kekuatan inti dalam pertahanan negara TNI juga menyadari semakin besarnya tantangan dalam



menjaga kedaulatan bangsa dan negara. Dalam konteks yang lebih luas dan modern, kedaulatan suatu bangsa pada saat ini tidak hanya dalam ruang lingkup tanah, air dan udara. Tapi juga memasuki kedaulatan di jagad maya (*cyberspace*).

Serangan melalui dunia maya tanpa harus menghadirkan kekuatan militer secara fisik di negara lawan, telah menjadi trend baru dalam perang modern di abad-21. Karenanya, Indonesia harus segera mempersiapkan kekuatan *cyber army* atau prajurit *cyber* yang terdiri dari individu-individu terampil serta ahli dalam *cyber warfare*, yang dituangkan dalam konsep Pembangunan National *Cyber Defense, sebagai garda terdepan dalam* menjawab tantangan perang informasi. Diharapkan Badan Pertahanan Dunia Maya tersebut dapat bertugas menyelamatkan database Indonesia, menyaring informasi, memberikan data informasi yang akurat bahkan melumpuhkan sistem pertahanan informasi dan komunikasi lawan sebelum menyerang Indonesia.

Cyber warrior

Dengan terbentuknya *National Cyber Defense,* diharapkan pembangunan kapasitas nasional dalam rangka meningkatkan ketahanan nasional terhadap berbagai ancaman dari dunia *cyber* akan dapat lebih ditingkatkan. Namun di sisi lain, pembangunan infrastruktur perlu juga segera direalisasikan secara terintegrasi, khususnya di lingkungan Kemhan/TNI maupun lembaga negara lainnya. Kemampuan yang telah ada saat ini, seperti APJII, ID SIRTI, ID CERT dan lainnya dapat dianggap sebagai modal dasar dalam rangka penyiapan konsep dan pembangunan awal atau *Backbone Cyber Defense* yang komprehensif, mengingat sejauh ini pembangunan konsep *Cyber Defense* masih bersifat sektoral atau belum menyeluruh sebagai satu kesatuan *National Cyber Defense*.

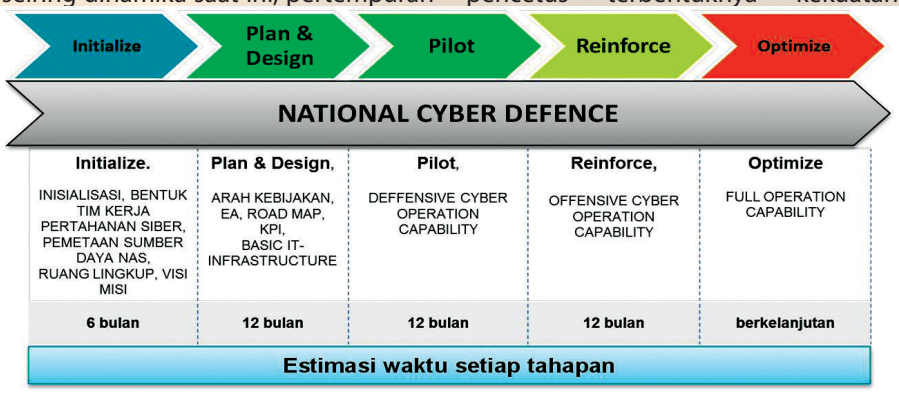
Penutup

Sebagai penutup, menarik untuk dicermati kenyataan bahwa setelah beberapa tahun pasca perang modern dewasa ini, seperti yang telah dilakukan oleh pasukan Amerika dan koalisinya (NATO) dipelbagai operasi militer di berbagai negara (Irak, Afganistan, Somalia, Serbia, Bosnia dan lainnya), ternyata belum menjamin keberhasilan menguasai keadaan atau kontrol situasi secara keseluruhan (absolut). Sehingga muncul satu pertanyaan, apakah hanya dengan teknologi militer modern yang diimplementasikan dalam konsep perang *cyber warfare* sudah dapat memenangkan suatu perang ?

Keberadaan pasukan elit atau khusus yang dimiliki Tentara Nasional Indonesia (TNI) diantaranya Kopassus (TNI AD), Denjaka (TNI AL) dan Korpaskhas (TNI AU), tidak diragukan lagi eksistensinya. Bahkan dunia internasional pun sudah mengakui kemampuan pasukan Garuda pada saat mengemban tugas negara, khususnya dalam operasi perdamaian dunia dibawah bendera PBB. Namun seiring dinamika saat ini, pertempuran tidak lagi hanya secara fisik, tetapi berkembang menjadi peperangan yang memanfaatkan jaringan komputer dan internet. Karenanya, orientasi pengembangan kekuatan pertahanan (TNI) dalam menjaga kedaulatan negara, perlu juga mengarah pada pembentukan pasukan khusus "tentara dunia maya" atau "*cyber army*".

Indonesia sebagai Negara berdaulat saat ini mempunya beberapa organisasi atau badan untuk keamanan jaringan. infrastruktur internet dan kejahatan siber, seperti keamanan siber internal di setiap organisasi maupun ID/SIRTII yang memonitor lalu lintas jaringan internet di Indonesia. Namun sampai dengan saat ini belum mempunyai sebuah badan atau organisasi yang bertanggungjawab terhadap pertahanan dan atau serangan balik jika terjadi perang *cyber* atau *cyber war.* Kondisi ini sangatlah menjadi kebutuhan mendesak bagi Kementerian Pertahanan/ TNI, mengingat ancaman terhadap keutuhan Negara Kesatuan Republik Indonesia saat ini bukan hanya berwujud pada serangan bersenjata namun lebih kepada perang pemikiran dan pembangunan opini yang banyak menggunakan media internet atau *cyber.* Sehingga sudah saatnyalah implementasi dari unit operasi pertahanan siber yang pentahapannya dapat dilaksanakan sebagai berikut :

Muaranya, tentu saja diharapkan konsep *National Cyber Defense* sebagai pencetus terbentuknya kekuatan pengganda dari kekuatan yang sudah ada, dapat segera terealisasi. Karena sudah waktunya Indonesia memlliki "tentara dunia siber" atau *cyber army* yang terampil dalam operasi militer *cyber warfare*.



Penulis adalah Analis Madya Nirmiliter Bididpol Ditkomduk Ditjen Pothan Kemhan.