PERANG DUNIA MAYA: CYBERWAR

Budi Rahardjo

rahard@gmail.com
http://rahard.wordpress.com
budi@indocisc.com

PT INDOCISC
Indonesia Computer Emergency Response Team (ID-CERT)

DAFTAR ISI

1. Pengantar

Belakangan ini kata "*cyberwar*" banyak disebut-sebut. Perang di dunia maya. Entah hal ini disebabkan oleh banyaknya kasus yang terkait dengan dunia maya, atau hanya sekedar *issues* yang dilemparkan banyak orang untuk menakut-nakuti. *Fear, Uncertainty, Doubt*. *FUD*.

Jika memang *cyberwar* merupakan masalah serius, maka muncul pertanyaan-pertanyaan berikutnya. Apakah Indonesia siap dalam menghadapi cyberwar ini? Apa saja yang harus dipersiapkan untuk mengantisipasi hal tersebut dilihat dari kacamata pemerintah, penegak hukum, tentara, dan masyarakat? Langkah-langkah apa yang harus dilakukan?

Akhirnya saya putuskan untuk mengumpulkan informasi yang terkait dengan topik ini dan membuat tulisan (buku) mengenai topik ini. Saat ini tulisan ini masih belum lengkap. Masih ada banyak istilah, konsep, dan isu yang harus saya jelaskan dengan lebih rinci akan tetapi belum mendapatkan *treatment* yang lengkap. Sementara ini saya catatkan di tulisan ini dulu dan Anda terpaksa harus mencari informasinya dari sumber lain.

Ini semua menyebabkan buku ini masih dalam status draft, akan tetapi saya tetap mendistribusikan tulisan ini agar dapat langsung bermanfaat. Jika saya tunda-tunda sampai sempurna, mungkin akan dibutuhkan waktu yang cukup lama. Sementara itu kebutuhan akan referensi dan bahan bacaan terkait dengan topik cyberwar ini sudah sangat mendesak. Itulah sebabnya dokumen ini sampai ke tangan Anda dalam format yang belum sempurna seperti ini.

Semoga tulisan ini bermanfaat bagi kita semua.

Bandung, Oktober 2012

Budi Rahardjo

2. Pendahuluan

Benarkah kita akan menghadapi perang di dunia maya, *cyberwar*? Jika ya, perangnya seperti apa? Lawannya siapa? Tentara kita itu siapa saja? Apakah tentara yang ada sekarang ini dipersenjatai dengan senjata teknologi informasi? Atau kita membuat tentara baru saja? Senjatanya apa? Kalau kita "tertembak" di dalam perang cyber ini apa efeknya kepada kita, sebagai rakyat biasa? Dan masih banyak pertanyaan lain. Intinya adalah apakah memang kita sudah atau akan mengalami perang dunia maya?

Penggunaan teknologi informasi dan jaringan komputer memang sudah menjadi bagian dari kehidupan kita sehari-hari. Berbagai aplikasi berbasis teknologi informasi sudah kita gunakan. Kita lebih sering mengambil uang melalui mesin ATM dibandingkan hadir secara langsung berhadapan dengan *teller* di bank. Menelepon dan mengirim pesan (SMS) melalui telepon genggam sudah menjadi kebiasaan dan bahkan menjadi kebutuhan.

Untuk membuktikan ketergantungan ini, coba Anda tidak menggunakan ATM dan tidak menggunakan telepon genggam selama sebulan. Sanggupkah? Rasanya berat. Bagi banyak orang, lebih baik ketinggalan dompet daripada ketinggalan telepon genggam.

Bagaimana bila kegagalan tersebut disebabkan oleh pihak ketiga. Ada pihak yang melakukan penyerangan terhadap layanan berbasis teknologi informasi tersebut. Misalnya ada upaya dengan sengaja untuk mematikan layanan ATM (atau internet banking) dari sebuah bank. Akibatnya nasabah tidak dapat melakukan transaksi secara online dan harus secara fisik hadir di kantor cabang. Dapat dipastikan banyak nasabah yang akan marah (dan bahkan dapat pindah ke bank lain).

Serangan untuk meniadakan layanan tersebut sering disebut *Denial of Service (DoS) attack*. DoS attack ini dapat ditujukan kepada jaringan dan aplikasi.

Contoh kegagalan layanan di atas hanya terkait dengan aplikasi komersial. Meskipun ada efek ekonomisnya, tetapi masih dapat dihitung. Bagaimana jika kegagalan tersebut terkait dengan eksistensi negara kita? Mungkinkah eksistensi sebuah negara terganggu oleh serangan yang dilakukan di dunia maya? Misalnya situs web perkantoran dilumpuhkan, seberapa besar impaknya? (Kalau dalam kondisi sekarang, mungkin impaknya masih minimal karena belum banyak layanan publik yang diberikan melalui internet.)

Dahulu untuk melakukan propaganda ideologi dari sebuah bangsa (negara) ke bangsa lain agak sulit dilakukan. Orang harus dikirim secara fisik ke negara target yang bersangkutan. Atau, setidaknya, bahan bacaan propaganda harus dapat sampai ke negara yang dituju. Infiltrasi seperti ini dapat terdeteksi oleh penjaga kedaulatan negara dan dapat dilakukan filter seperlunya.

Propaganda melalui cara non-fisik mulai muncul dengan adanya siaran televisi. Pemerintah di jaman dahulu melakukan sensor terhadap paham-paham asing yang masuk melalui acara di televisi. Bahkan lagu-lagu asingpun disensor.

Teknologi informasi mendobrak batas ruang. Saat ini lebih mudah menyusupkan ideologi ke masyarakat tujuan dengan menggunakan berbagai aplikasi di internet. Bolehkan sebuah negara menghasut warga negara lain, untuk melakukan makar misalnya, melalui sebuah situs web? Atau mungkin serangan yang tidak terlalu kasar dapat berupa propaganda anti negara atau pola hidup tertentu. Sebagai contoh, penyisipan ideologi Komunisme akan dapat dilakukan dengan menggunakan jaringan internet. Apakah perlu negara kita membatasi akses warganya dengan menerapkan *filtering* terhadap *content* yang bertentangan dengan ideologi bangsa?

Hal di atas dapat dikategorikan serangan secara pasif. Bagaimana jika terjadi serangan yang lebih akif? Bolehkah tentara sebuah negara menyerang situs dari pemerintahan negara lain? Jika situs web dianggap tidak terlalu penting, bagaimana jika yang diserang adalah infratruktur yang terkait dengan teknologi informasi? Misalnya yang diserang adalah jaringan telekomunikasi sehingga negara yang diserang tidak dapat melakukan kordinasi untuk mengantisipasi serangan perang fisik.

Apakah pelanggaran terhadap hal-hal di atas dapat memicu terjadinya "perang dunia maya?" Tentara dari kedua negara yang bersiteru saling serang menyerang di dunia internet. Serang menyerang dapat dilakukan untuk menjatuhkan server lawan atau sampai menyusup ke server.

Meskipun internet sudah banyak digunakan oleh masyarakat Indonesia, efeknya terhadap masyarakat belum terukur. Misalnya, jika jaringan internet putus untuk waktu yang cukup lama – katakanlah satu bulan – apakah ada efek yang terasa secara langsung? Jika tidak terjadi "perang" dan tidak terasa efeknya, apakah kita perlu peduli?

Dengan latar belakang di atas maka perlu sebuah kajian tentang perang dunia maya ini bagi Indonesia. Mari kita bahas.

2.1 Kejadian, Statistik, dan Fakta

Ada beberapa berita yang terkait dengan keberadaan perang di dunia maya. Berita ini terkadang sulit dikonfirmasi kebenarannya, namun setidaknya dapat menjadi gambaran tentang hal-hal yang melatarbelakangi.

2.1.1 Kejadian Yang Terkait Dengan Indonesia

Dalam bukunya tentang *Cyber Warfare*, Jeffrey Carr (Carr, 2012) memberikan beberapa contoh kejadian terkait dengan perang dunia maya. Untuk kasus yang terkait dengan Indonesia diberikan contoh tentang kejadian kerusuhan anti-Cina yang terjadi di bulan Mei 1998. Pada saat itu berbagai hackers dari berbagai organisasi – seperti misalnya China Hacker Emergency Center – menyerang berbagai situs yang terkait dengan pemerintah Indonesia sebagai protes.

Serangan yang dilakukan pada saat itu tidak hanya ditujukan kepada situs pemerintahan Indonesia saja tetapi terhadap situs-situs lain yang dimiliki oleh

pelaku bisnis Indonesia. Perlu diingat bahwa pada tahun 1998 itu wawasan pemerintah Indonesia terhadap internet belum besar. Belum banyak instansi pemerintah yang memiliki situs web. Akhirnya serangan di arahkan ke mana saja selama terkait dengan Indonesia.

Pada saat itu saya sempat membantu sebuah perusahaan penyedia jasa internet yang salah satu servernya dirusak situs webnya. Situs web ini terkait dengan layanan pelanggannya untuk mengakses email dari tempat yang berbeda, mobile, sehingga tidak dapat dilakukan pembatasan terhadap nomor IP, misalnya. Perlu diingat juga pada waktu itu penggunaan Virtual Private Network (VPN) belum lazim sehingga sangat sukar membatasi akses dari server tersebut. Sayangnya aplikasi yang digunakan memiliki lubang keamanan sehingga dapat dieksploitasi oleh penyerang dari jarang jauh. Penyerang ini kemudian dapat mengubah berkas halama depan situs webnya.

Yang menarik dari serangan ini adalah penyerang tidak berusaha untuk merusak atau melumpuhkan server. Sang penyerang ingin server tetap menyala sehingga dapat menampilkan halaman web dengan tampilan yang sudah diubah (*deface*). Pengetahuan tentang karakteristik dan itikad penyerang ini sangat bermanfaat dalam memilih pengamanan yang digunakan. Dalam kasus yang saya alami, solusi yang kami pilih adalah dengan mengupdate halaman web secara berkala secara otomatis (dalam sistem UNIX ini dilakukan dengan fasilitas cron). Berkas di halaman web di-copy dari sebuah direktori secara periodik sehingga biarpun halaman diubah, maka dalam waktu tertentu halaman akan kembali menjadi benar.

Pada kasus yang lain, yaitu kasus Timor Timur, sempat terjadi serang menyerang antara hackers Indonesia dan Portugal. Untuk kasus yang ini, serangan dilakukan untuk melumpuhkan komputer yang ditargetkan. Jika penyerang dapat masuk, maka dia akan berusaha menghapus semua berkas atau memformat disk. Perhatikan bahwa itikad dari penyerang berbeda dari contoh sebelumnya.

Bagaimana dengan kondisi Indonesia saat ini? Dilihat dari sudut instansi pemerintahaan, sekarang semakin banyak yang menggunakan sistem komputer dan terhubung ke internet. Hal ini semakin meningkatkan risiko keamanan.

Semakin banyak aplikasi penting yang menggunakan teknologi informasi. Sistem informasi satu atap, *egovernment*, sampai eKTP mulai mengumpulkan data pribadi warga negara Indonesia. Pengamanan data yang terkait dengan aplikasi-aplikasi ini harus dilakukan secara serius.

Sayangnya banyak pengembang dan pihak penyelenggara layanan ini yang belum menerapkan keamanan secara optimal. Sebagai contoh ada banyak aplikasi yang menggunakan data pribadi – seperti tanggal lahir – sebagai bagian dari nomor identitas. Ini merupakan kesalahan fatal jika ditinjau dari kacamata keamanan karena seringkali pengguna menggunakan angkat tersebut sebagai bagian dari password. Demikian pula banyak situs-situs pemerintahan yang sangat lemah keamanannya sehingga mudah dirusak (deface). “Untungnya” data yang ada di sana masih berupa data yang publik (berita-berita). Jika sistem sudah digunakan untuk mengambil keputusan, maka kondisi keamanan seperti ini tidak dapat dibiarkan. Ini dapat menjadi target dalam perang dunia maya.

2.1.2 Kejadian Terkait Dengan Negara Lain

Kejadian yang dianggap sebagai bukti telah terjadinya perang teknologi informasi – meskipun tidak terang-terangan – adalah ditemukannya virus *Stuxnet* di sekitar bulan Juni 2012[1]. Virus yang menyerang sistem operasi Microsoft Windows ini dipercaya dibuat untuk menyerang infrastruktur dari negara Iran dengan menyerang perangkat (hardware dan software) yang dibuat oleh Siemens. Perangkat Siemens tersebut banyak digunakan sebagai basis dari SCADA (*supervisory control and data acquisition*) yang digunakan di berbagai tempat industri dan pertahanan Iran. Sampai saat ini masih diduga siapa pembuat virus Stuxnet tersebut.

Setelah *Stuxnet*, kemudian muncul malware baru yang bernama *Flame* yang memiliki karakteristik serupa dan bahkan dianggap memiliki fitur yang lebih baik.

Serangan yang dianggap pertama kali terhadap infrastruktur utama (*critical infrastructure*), yaitu listrik, terjadi di tahun 2015. Serangan dilakukan terhadap penyedia jasa listrik di Ukraina. Penyerangan dilakukan secara bertahap dan terstruktur[2]:

- Sebelum Juni 2015: penyerang mencari informasi mengenai jaringan distribusi, mengirimkan email ke pimpinan perusahaan yang mengandung *malware Black Energy*, mencuri *credential* untuk mengakses sistem SCADA;
- Juni – Desember 2015: melakukan eksplorasi terhadap sistem SCADA dan merencanakan penyerangan, mengembangkan firmware gadungan untuk menyerang perangkat di *substation*;
- 23 Desember 2015: melakukan serangan terkordinasi (*synchronized*) dari jarak jauh terhadap (*circuit*) *breakers* di *substation* sehingga terjadi pemadaman listrik, listrik cadangan di ruang pengendali juga dimatikan dari jarang jauh, telepon di-jam sehingga operator tidak sadar bahwa telah terjadi serangan, malware merusak data unuk menjalankan perangkat.

Akibat dari serangan di atas sekitar 225 ribu orang (pengguna jasa listrik) kehilangan layanan. Hari-hari berikutnya setelah serangan diketahui, sistem juga belum dapat beroperasi sepenuhnya. Diduga sistem SCADA yang digunakan oleh penyedia jasa listrik di Amerika (dan seluruh) dunia juga dapat diserang dengan cara yang sama. Menurut *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) dari *Departement of Homeland Security* Amerika Serikat, penyerangan ini tidak dilakukan secara sembrono melainkan sudah sistematik.

2.1.3 Spy vs. Spy

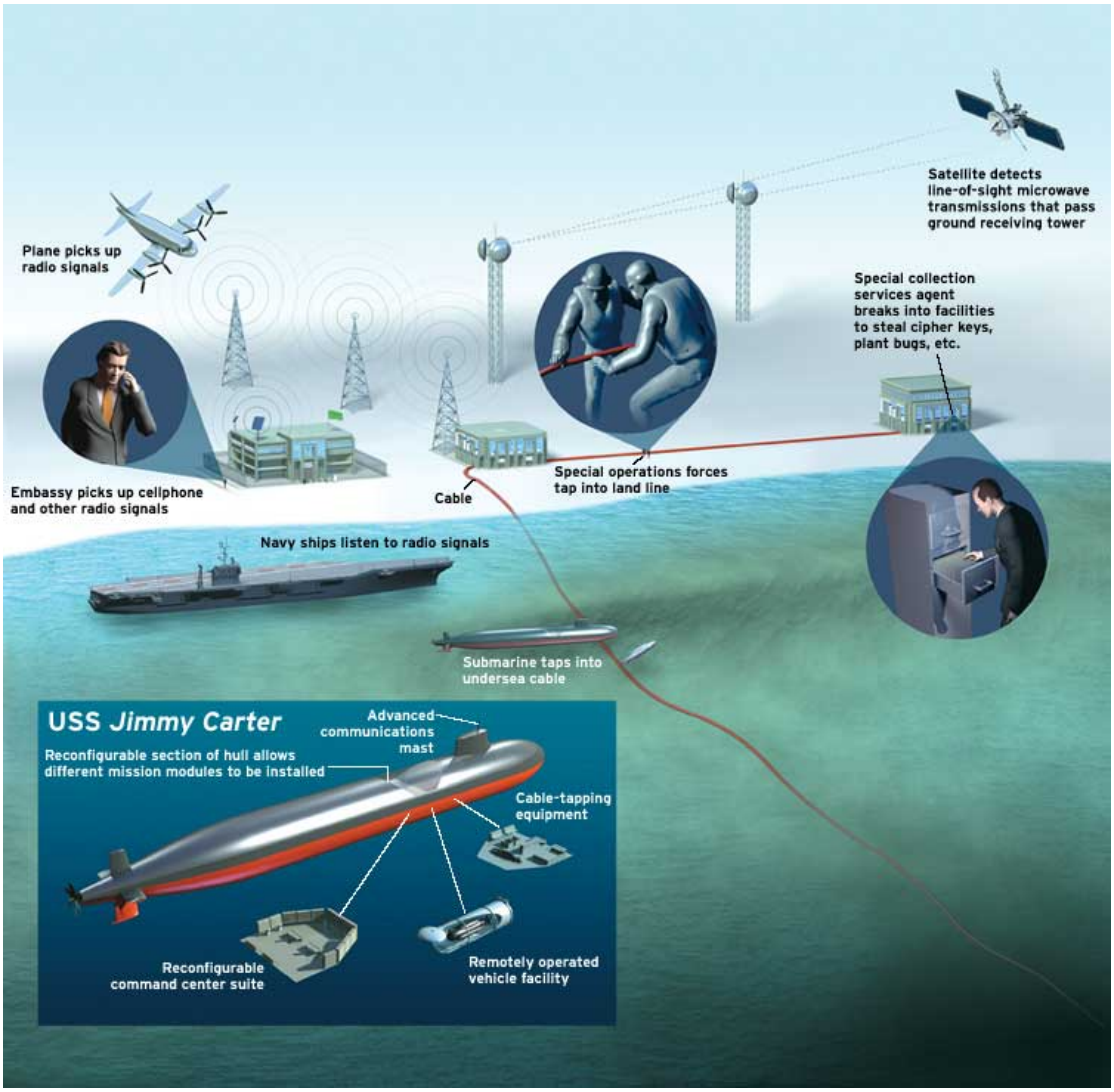
Sebetulnya kasus yang sering digunakan untuk menjadi contoh upaya negara lain untuk mendapatkan data dari negara lain adalah Echelon. Ini adalah proyek penyadapan yang dilakukan oleh Amerika Serikat beserta partnernya. Pada

---

[1] Informasi mengenai Stuxnet dari Wikipedia dapat diperoleh dari halaman http://en.wikipedia.org/wiki/Stuxnet

[2] _____, "Cybersecurity at U.S. Utilities Due For an Upgrade: Tech to detect intrusions into industrial control systems will be mandatory", *IEEE Spectrum*, May 2016, hal. 7-9.

mulanya proyek ini dianggap tidak pernah ada, namun fakta-fakta mulai muncul sehingga mulai didokumentasikan. Salah satu pembahasannya dilakukan oleh majalah IEEE Spectrum, April 2003.



Sumber: IEEE Spectrum, April 2003

Gambar 1. Penyadapan Echelon

Proyek Echelon melakukan penyadapan secara fisik di seluruh lini; darat, laut, dan udara. (Lihat Gambar 1.) Pada intinya data harus dilewatkan ke titik penyadapan tersebut. Di kemudian hari, penyadapan dapat dilakukan pada jaringan yang dilalui oleh data. Data harus dirutingkan ke sistem yang memiliki fitur penyadapan.

Penyadapan ini dilakukan di beberapa lokasi di dunia. (Lihat Gambar 2.) Bagian yang terdekat dengan Indonesia kemungkinan di Australia atau Guam. Ini adalah yang kita ketahui. Kemungkinan masih banyak hal lain yang belum kita ketahui dari proyek Echelon ini.

Gambar 2. Titik Penyadapan Echelon

Kasus penyadapan lain juga terjadi di Yunani, dikenal dengan nama "the Athens Affair"[3]. Kasus ini bermula dengan kejadian bunuh diri dari seorang teknisi Vodafon-Panafon (salah satu operator seluler Yunani) pada tanggal 9 Maret 2005. Keesokan harinya diberitakan bahwa telepon dari perdana menteri Yunani beserta lebih dari seratus orang pejabat lainnya telah disadap. Bagaimana ini dapat terjadi? Apakah ini hanya kasus di dalam negeri saja? Ataukah ini kasus penyadapan yang dilakukan oleh negara lain?

Baru-baru ini (tahun 2012) pemerintah Amerika Serikat melakukan evaluasi terhadap perusahaan Huawei, sebuah perusahaan dari Cina yang memproduksi perangkat jaringan dengan harga yang relatif lebih murah dari siangannya. Ditakutkan pemerintah Cina menyusupkan kode-kode penyadap pada perangkat yang dibuat oleh Huawei[4]. Sebelumnya, secara informal, ada larangan untuk menggunakan produk Huawei untuk sistem yang terkait dengan pemerintahan. Apakah kita dapat mengetahui bahwa produk yang kita gunakan bebas dari "fitur" penyadapan oleh pihak asing?

3. Perlindungan

Bagaimana kita dapat melindungi dunia maya kita dari serangan pihak lain, khususnya yang terkait dengan perang dunia maya? Bagian ini akan membahas aspek-aspek yang perlu dilindungi dan strategi untuk mencapai perlindungan.

[3] "The Athens Affair", http://www.spectrum.ieee.org/print/5280/
[4] http://www.reuters.com/article/2012/10/17/us-huawei-spying-idUSBRE89G1Q920121017

3.1 Perlindungan Infrastruktur Utama

Untuk melakukan perlindungan perlu diketahui dahulu aset apa yang ingin dilindungi. Setelah itu baru dapat kita buatkan rencana dan strategi perlindungannya.

Bagi perusahaan, sebelum melakukan perlindungan dilakukan pendataan aset. Hal yang sama juga dapat dilakukan pada level negara. Untuk ini biasanya perlindungan pada level negara dikenal istilah "*national critical infrastructure protection*". Langkah awal adalah dilakukan pemetaan apa yang masuk ke dalam kategori "*critical infrastructure*". Beberapa negara telah melakukan proses ini. Nampaknya perlu dilakukan sebuah pemetaan untuk skala Indonesia.

Secara umum yang dapat dikategorikan sebagai infrastruktur dari sistem berbasis teknologi informasi adalah:

- sumber daya energi / listrik;
- infrastruktur telekomunikasi (telepon);
- dan infrastruktur internet.

Selain infrastruktur fisik, ada juga kecukupan sumber daya manusia beserta senjata & teknologi terkait. Bayangkan sebuah perang fisik konvensional. Dalam perang itu tentu ada manusia (tentara) yang berperang, persenjataan (dan teknologi), serta infrastruktur (dan logistik). Hal yang serupa juga terdapat dalam perang dunia maya.

3.2 Kesiapan Sumber Daya Manusia

Salah satu aspek utama dalam perang dunia maya adalah aspek manusia. Ada beberapa isu terkait dengan aspek manusia ini. Apakah pelaku dalam perang dunia maya hanya terbatas kepada tentara saja? Pada kenyataannya, rakyat ikut berperang. Tentu saja rakyat ini harus dilatih dulu agar dapat ikut berperang dan bertahan.

Hal yang sudah pasti harus dilakukan adalah menyiapkan dan melatih tentara yang secara resmi memahami berbagai aspek perang dunia maya. Mereka harus memiliki kemampuan (skill) teknis.

Bidang ini merupakan bidang yang baru, untuk itu biasanya dikembangkan sumber daya dari usia muda. Hal ini bukan berarti bahwa tentara yang sudah berusia lanjut tidak perlu dilatih. Justru penguasaan teknologi informasi tidak dibatasi dengan kemampuan fisik yang biasanya terkendala dengan usia. Artinya siapapun dengan usia berapapun dapat dilatih. Hanya kemauan yang membatasi.

Salah satu tantangan yang harus dihadapi adalah kecepatan perkembangan teknologi di bidang ini. Untuk itu penguasaan kemampuan harus terus dilatih dengan teknologi terbaru. *Training* dan *re-training* merupakan salah satu kunci yang penting.

Secara keilmuan, *information and communication technology security* dapat dianggap masih baru meskipun pemanfaatannya sudah dilakukan sejak dari jaman dahulu. Pendidikan secara formal di bidang ini juga masih terbatas. Belum banyak perguruan tinggi yang menyediakan kuliah security. Saya sendiri

memulai memberikan kuliah security di kampus ITB baru sejak awal tahun 2000. Pendidikan *security* untuk tingkat pasca sarjana secara resmi baru akan dibuka di ITB pada tahun depan (2013). Sementara itu melalui perusahaan, kami juga melakukan training kepada profesional di dunia IT. Ini semua bertujuan untuk meningkatkan jumlah SDM yang memahami security.

Khususnya untuk keperluan militer, perlu ada semacam tempat untuk melakukan pendidikan dan pelatihan *security*. Sama halnya dengan pelatihan fisik yang membutuhkan fasilitas, pelatihan teknologipun membutuhkan fasilitas. Tentara dilatih dan disiapkan di sini. Salah satu tempat yang pernah kami usulkan adalah Cimahi. Cimahi sudah menjadi tempat untuk pelatihan (secara fisik). Sementara itu dekat tempat pelatihan ini (bersebelahan) sudah ada tempat IT yang cukup memadai, Baros IT Center. Sinergi dapat dilakukan untuk memberdayakan IT center ini dengan pelatihan yang sudah ada.

Untuk yang terkait dengan komunitas dan penegak hukum, ID-CERT telah terlibat dalam berbagai kegiatan pencerahan (*awareness*), training untuk peningkatan skill, dan kordinasi. Upaya-upaya ini masih harus terus ditingkatkan mengingat jumlah dan kualitas SDM yang dibutuhkan masih sangat banyak.

3.3 Penguasaan Teknologi

Teknologi selalu memiliki peran dalam perang. Kemampuan pihak Sekutu dalam memecahkan sistem sandi (kriptografi) dari Jerman (yang menggunakan *Enigma*) dianggap sebagai sebuah hal yang membantu mempercepat selesainya perang dunia kedua. Bahkan teknologi-teknologi banyak yang berkembang dari dunia pertahanan (*defense*). Terlebih lagi dengan perang di dunia maya, peran teknologi adalah mutlak. Penguasaan teknologi adalah mutlak.

Beberapa bidang yang harus dikuasai terkait dengan perang dunia maya antara lain: jaringan, sistem operasi, pemrograman, kriptografi, protokol, malware, security tools, dan security secara umum. Ini sebuah bidang yang sangat luas.

Jaringan (*Network*)

Masalah *security* pada awalnya identik dengan *network security* (keamanan jaringan). Berbagai aspek penyerangan (*attack*) dan perlindungan dilakukan terhadap jaringan. Penyerangan dapat dilakukan dengan melihat kelemahan dari protokol yang digunakan. Secara berkala ditemukan kelemahan terhadap protokol (atau implementasinya).

Perlindungan di jaringan menghasilkan berbagai perangkat pemantauan dan perlindungan jaringan (*network security devices*), seperti *firewall* dan *intrusion detection system* (IDS). Perangkat ini tentu saja belum dapat 100% melindungi jaringan. Kadang perangkat ini juga masih memiliki celah keamanan.

Malware

Salah satu cara untuk melakukan serangan yang sudah dilakukan adalah dengan membuat *malicious software* (*malware*) dalam bentuk *computer virus* atau *trojan horse*. Malware ini dapat kita program sesuai dengan tujuannya. Sebagai contoh, malware dapat kita program agar mengirimkan berkas-berkas yang berada di komputer yang tersusupi ke sebuah server. Malware ini kemudian kita sebarkan

dengan berbagai cara, seperti misalnya melalui email. Bayangkan apabila komputer yang berhasil disusupi malware ini berisi data tentang peta kekuatan militer Indonesia atau data rahasia lainnya.

Berbagai serangan lain dapat dilakukan oleh malware. Malware dapat diminta untuk mematikan komputer pada waktu tertentu atau pada kondisi tertentu. Bayangkan apabila komputer yang terkena serangan ini adalah komputer yang mengendalikan reaktor nuklir atau pengatur listrik di seluruh Indonesia.

Komputer-komputer yang sudah disusupi oleh malware ini dapat dikendalikan dari jarak jauh. Mereka disebut *zombie* atau (ro)*bot*. Kelompok komputer-komputer yang tersebar dan sudah diambil alih ini dapat disebut sebagai *botnet*.

Kemampuan mendeteksi dan mengatasi *malware* ini sangat penting. Terkait dengan bidang ini ada penelitian *Intrusion Detection System* (IDS), dan *honeypot* (*honeynet*).

Penyusupan di dalam software

Kita harus berhati-hati dengan sumbangan perangkat (hardware dan software) dari negara lain jika akan digunakan untuk keperluan militer. Seharusnya hardware dan software tersebut dibuat terbuka sehingga dapat dievaluasi oleh pakar keamanan kita. Itulah sebabnya penggunaan *open source* sangat penting. Di beberapa tempat bahkan penggunakan *closed source* tidak diperkenankan. Jika memang software yang digunakan memiliki intellectual property yang rahasia, bisa saja software tersebut tidak di-open-source-kan tetapi kita sebagai pembeli harus memiliki hak untuk mengevaluasi (mengaudit) *source code*-nya.

Tentu saja ini mengambil asumsi kita memiliki SDM yang mampu menguasai teknologi ini, bukan hanya sekedar pandai memasang saja. Itulah sebabnya – seperti telah diuraikan pada bagian sebelumnya – kemampuan SDM sangat penting.

Penguasaan Security Tools

Saat ini telah tersedia banyak *security tools* yang dapat digunakan untuk memantau, menangkal, dan melakukan serangan (*attack*). Penguasaan akan tools ini sama seperti penguasaan senjata pada perang konvensional. Esensial ketika terjadi perang.

Permasalahan yang dihadapi dalam penguasaan tools adalah adanya tools yang baru setiap harinya. Untuk menguasai satu tools saja sudah sulit, apalagi adanya banyak tools. Untuk itu perlu dilakukan pendidikan (formal, training) terus menerus dengan melibatkan banyak pihak (perguruan tinggi, training center, pakar, pelaku) baik di dalam maupun di luar negeri.

Kriptografi

Salah satu cara untuk menghindari penyadapan adalah dengan menggunakan kriptografi. Data disandikan menjadi pesan yang tidak dapat dimengerti oleh pihak penyadap. Ilmu kriptografi ini merupakan gabungan dari Matematika,

Elektro, dan Ilmu Komputer. Kriptografi ini kemudian diimplementasikan dalam produk tertentu.

Sejak dari jaman dahulu, perang dilengkapi dengan kemampuan merahasiakan pesan. Kriptografi merupakan salah satu kunci kemenangan dalam perang. Lihatlah bagaiman keberhasilan Sekutu untuk memecahkan Enigma (sistem kriptografi yang digunakan oleh Jerman) pada perang dunia kedua dianggap sebagai kunci untuk mempercepat mencapai kemenangan. Berbagai cerita sejarah mengenai hal ini dapat dibaca pada buku David Kahn (Kahn, 1996). Demikian pula dalam perang dunia maya, kriptografi akan (semakin) memiliki peran penting.

Salah satu kelemahan yang sering kami temui di lapangan adalah komunikasi dan penyimpanan data tanpa menggunakan kriptografi. Ini adalah faktor manusia. Meskipun kita memiliki teknologi kriptografi yang canggih, selama dia tidak digunakan maka akan percuma saja. Salah satu cara untuk memastikan bahwa pengamanan dilakukan adalah dengan menggunakan aturan dan standar.

Di Indonesia, Lembaga Sandi Negara merupakan sebuah institusi yang berkepentingan dengan bidang ini. Mereka harus diberdayakan dan dilibatkan dalam hal perlindungan data yang melibatkan kriptografi di Indonesia. Riset di bidang kriptografi perlu dilakukan di perguruan tinggi.

4. Penutup

Semoga tulisan ini dapat membuka wawasan dan menjadi awal untuk melakukan diskusi tentang pentingnya Indonesia untuk menyiapkan diri terhadap kemungkinan terjadinya perang dunia maya. Kita, dan semua orang, tentunya tidak menyukai adanya perang. Siapa yang suka dengan kehadiran perang? Namun, suka atau tidak suka, kita perlu menyiapkan diri untuk menghadapi perang.

Masih ada banyak hal yang perlu kita kerjakan. "*The devils are in details*", demikian yang sering disebutkan oleh orang. Masih banyak pekerjaan rumah kita. Beberapa hal yang perlu kita perhatikan.

- Perlu ada inisiatif untuk memetakan infrastruktur yang penting dan bagaimana cara melindunginya (*national critical infrastructure protection*).
- Perlu meningkatkan jumlah dan kemampuan sumber daya manusia yang menguasai bidang ilmu *security*. Untuk tingkat pimpinan, harus diberikan wawasan mengenai pentingnya security.
- Perlu ada tempat pelatihan tentara security di Indonesia.
- Perlu ada sebuah organisasi yang melakukan koordinasi hal-hal yang terkait dengan perang cyber.
- Mengembangkan kerangka hukum (bersama dengan negara-negara lain) terkait dengan perang cyber.

5. Bahan Bacaan

1. Jeffrey Carr, "*Inside Cyber Warfare: Mapping the Cyber Underworld*," O'Reilly, 2012.
2. Stephen Cass, "Are the glory days of electronic spying over – or just beginning?", *IEEE Spectrum*, April, 2003.
3. David Kahn, "*The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*," Scribner; Rev Sub edition, 1996.
4. Budi Rahardjo, "Perang Siber: Cyberwar," online, http://rahard.wordpress.com/2012/06/19/perang-siber-cyberwar/, diakses 13 Oktober 2012.
5. Budi Rahardjo, "Memetakan Komunitas Security di Indonesia," online, http://rahard.wordpress.com/2012/10/17/memetakan-komunitas-security-di-indonesia/, diakses 18 Oktober 2012.

Mengenai Penulis

Budi Rahardjo saat ini merupakan staf pengajar di Sekolah Teknik Elektro dan Informatika (STEI), Institut Teknologi Bandung. Dia juga merupakan pendiri dari PT INDOCISC, sebuah perusahaan yang bergerak di bidang jasa IT security. Sebelumnya dia ikut mengamankan sistem IT pemilu di tahun 1999. Budi Rahardjo juga menjadi pimpinan pengelola nama domain Indonesia (.ID) dari tahun 1997 sampai dengan 2012 dan pendiri dari ID-CERT (Indonesia Computer Emergency Response Team – www.cert.or.id) yang dibentuk tahun 1998. Budi Rahardjo mendapatkan gelar S1 dari Teknik Elektro ITB, Master's dan PhD. dari Electrical Engineering, University of Manitoba, Canada.