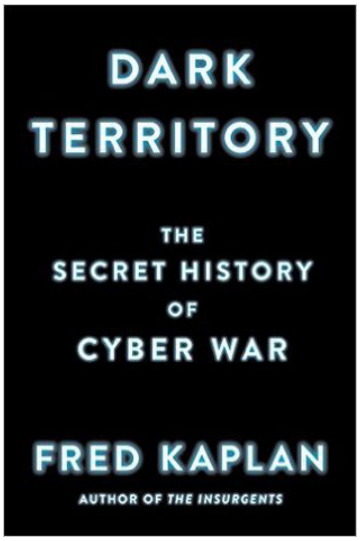
Book Review

Lembaran Sejarah | Volume 14 Number 2 October 2018 | ISSN 2314-1234 (Print) ISSN 2620-5882 (Online) | Page 216—222

Dark Territory: The Secret History of Cyber War

SATRIO DWICAHYO
Alumni Rajaratnam School of International Studies, Singapura
Email: ody.dwicahyo@yahoo.com



Title:
Dark Territory: The Secret History of Cyber War
Author:
Fred Kaplan
Publisher:
Simon & Schuster Paperbacks (2016)
Pages:
338
ISBN:
978-1-5011-4083-9

Ilmu sejarah mendapat banyak tuntutan dan tantangan dewasa ini. Sebagai disiplin yang fokus mempelajari masa lalu, satu tuntutan yang dialamatkan kepada ilmu sejarah (dan sejarawan sebagai aktor intelektual di balik disiplin ini) adalah menanggapi perkembangan zaman yang terjadi secepat kilat. Satu dari sekian tuntutan itu adalah tanggapan ilmu sejarah terhadap kemunculan domain baru bernama dunia siber. Tantangan inilah yang berusaha dijawab oleh Fred Kaplan dalam *Dark Territory: The Secret History of Cyber War*.

Sebelum menjadi wilayah yang lebih ramah sebagai sarana perdagangan elektronik atau media sosial, internet pertama kali dibangun untuk kepentingan militer. Jejaring yang dirancang sebagai sarana komunikasi rahasia antara Pentagon, Militer AS, dan peneliti-peneliti universitas yang tergabung dalam ARPA (*Advanced Research Projects Agency*) sehingga dinamai ARPA-Net. Tak lama setelah perkembangan pertamanya, ARPA-Net (dan internet) telah menunjukkan karakter yang ironis. Meski bertujuan untuk membangun sarana pertukaran informasi tertutup, ARPA-Net sebagai cikal bakal internet dapat diakses oleh lebih dari satu komputer. Hal ini yang membuatnya rentan terhadap intrusi, sesuatu yang kelak dikenal sebagai peretasan (*hacking*).

Lebih dari sekadar sejarah perkembangan internet sebagai platform komunikasi, Kaplan mengungkap perkembangan siber sebagai sebuah domain kelima dari perang modern. Mayantara dianggap setara dengan empat matra pertahanan yang telah mapan sebelumnya; darat, laut, udara, dan luar angkasa. Kehadiran domain kelima ini telah mengubah pola pikir penyelenggaraan perang di empat domain pertama. Dengan begitu, penyelenggaraan kekuatan pada empat matra pertama pada perang generasi 4.0 wajib terkoneksi dengan dunia siber yang membuat pembagian data mengenai hampir semua persoalan dapat berjalan dengan baik.

Selayaknya karya sejarah, Kaplan mengungkapkan bahwa prinsip-prinsip dasar perang siber telah diaplikasikan sejak periode Romawi ketika pihak-pihak yang terlibat dalam perang berusaha menyadap informasi dengan cara yang paling sederhana. Merebut informasi lawan memang sebuah bentuk upaya pemenangan perang yang amat klasik sebagaimana telah ditulis oleh Sun Tzu dalam karya agung yang dalam bahasa Inggris dikenal dengan *The Art of War*. Satu perbedaan yang mencolok dari upaya penyadapan sebelum era siber dengan periode internet adalah ruang tempat pesan rahasia tersebut berada.

Istilah *dark territory* bahkan tidak diciptakan dalam konteks peperangan siber, Fred Kaplan meminjam istilah yang digunakan oleh jawatan perkeretapian AS untuk menyebut rel-rel kereta api yang tidak dioperasikan oleh sinyal perkeretapian. Kaplan berpikir bahwa dunia siber yang begitu luas dan liar sangat cocok dengan metafor tersebut.

Teknik penyadapan informasi yang ditransmisikan dengan hewan, kurir manusia, maupun telepon sebagaimana yang berkembang pada era perang dingin dapat terjadi karena proses komunikasi rahasia terjadi pada semata-mata satu saluran saja. Sementara internet merupakan ruang tidak terbatas yang amat sulit mewujudkan satu saluran sebagaimana metode-metode sebelumnya. Pada aspek inilah diskontinuitas dari prinsip perang siber diungkap. Dengan kata lain, meskipun prinsip merebut informasi lawan telah dilakukan sejak perang di periode klasik; perang siber tetap memiiliki sebuah karakteristik yang belum ada sebelumnya.

Sebagaimana karya Fred Kaplan lainnya, buku ini lebih nampak sebagai novel sejarah dibandingkan dengan tulisan sejarah pada umumnya. Hal ini disebabkan oleh format penulisan yang tidak menunjukkan pengutipan di tengah-tengah tulisan baik dalam bentuk catatan kaki maupun catatan tubuh (*bodynote*). Kaplan tetap mencantumkan referensi yang ia gunakan di akhir bagian buku tanpa secara spesifik menjelaskan di mana pengutipan tersebut dilakukan.

Ulasan atas buku ini akan dilakukan dengan secara kronologis perkembangan perang siber dan persinggungannya dengan aspek-aspek lain. Dalam hal ini, aspek-aspek tersebut disusun mengikuti kerangka penyusunan

bab-bab di dalam buku ini yang dibagi berdasarkan tema keterkaitan perang siber dengan perang di level strategis-operasional, kebijakan pertahanan, kebijakan keamanan dalam negeri, dan kebijakan politik luar negeri Amerika Serikat.

Sebagai contoh; bab pertama mengupas latar belakang pemikiran konsep keamanan siber oleh Amerika Serikat yang pada awalnya terasa sebagai fenomena yang hanya ada pada film sains-fiksi. Dengan judul "Could Something Like This Really Happen?", bab pertama menghadirkan cerita Presiden Ronald Reagan yang membawa cerita sains-fiksi ke meja rapat kementerian pertahanan. Presiden Reagan dengan serius menanyakan kepada para petinggi kementerian pertahanan dan pejabat lain di bidang keamanan apakah kasus-kasus pada karya sains-fiksi dapat terjadi pada dunia nyata. Kasus yang kala itu ia tanyakan adalah kasus peretasan sistem komputer pemerintah oleh seorang remaja ahli komputer yang dinukil dari film *WarGames.*

Dunia Maya dan Senjakala Perang Konvensional

Serupa dengan kajian-kajian sejarah teknologi peperangan pada umumnya; Amerika-sentris dalam karya ini sangat menonjol dan memang secara terbatas membahas perkembangan perang siber yang dilakukan atau dihadapi oleh Amerika Serikat. Meski pada bagian awal buku ini menarik linimasa sejarah siber sejauh perang informasi yang terjadi sejak perang sipil di Amerika Serikat, penjelasan elaboratif pada bab-bab berikutnya hanya dimulai dari Operasi Badai Gurun (*Operation Desert Storm*) yang dilancarkan AS terhadap Irak di bawah Saddam Husein.

Bukan hanya invasi militer murni terbesar setelah Perang Dunia II, Operasi Badai Gurun merupakan operasi pertama yang berkarakter C-C2 (*Counter Command and Control*). C-C2 adalah bentuk perang yang menjadikan sistem komunikasi antara pasukan lawan sebagai target utama yang harus dilumpukan. Keputusan untuk menarget sesuatu yang tidak terlihat (dalam hal ini adalah jaringan komunikasi antara tentara Irak) dianggap sebagai suatu bentuk embrio dari peperangan siber yang jauh lebih kompleks. Sebagai debut dari perang yang menempatkan jaringan sebagai target utama; tak semua pemimpin militer AS berpendapat bahwa perang dapat dimenangkan dengan cara tersebut. Jenderal Norman "Stormin" Schwarzkopf sebagai komandan tertinggi tentara AS pada operasi tersebut bahkan masih berpikir sangat konvensional. Menghancurkan pasukan lawan secara fisik adalah target yang lebih realistis dibanding bersabar menunggu dan mengumpulkan data-data intelijen berbasis sinyal (sigint-*signal intelligence*) untuk dieksploitasi untuk kepentingan yang lebih luas.

Contoh dari strategi C-C2 yang diterapkan terhadap Irak adalam infiltrasi AS kepada jaringan kabel fiber yang digunakan oleh Saddam Hussein dalam berkomunikasi dan memberikan komando. Kesuksesan AS dalam

meretas jaringan komunikasi ini berbuah pengetahuan AS mengenai segala percakapan Saddam dengan para jenderalnya dan memberikan suatu bahan penyusun laporan intelijen yang mendekati akurat. Menurut Kaplan bahkan Saddam merespon ini dengan mengganti piranti transmisi komunikasinya dari telepon terproteksi menjadi kurir bermotor. Namun, salah satu invasi militer terbesar di penghujung abad ke-20 tersebut berjalan dengan sangat cepat. Kurir bermotor memang cenderung aman namun sebelum semua pesan tersebut sampai kepada pihak yang dituju, banyak target strategis AS telah porak poranda oleh jet tempur dan pembom strategis AS.

Efek tangkal dan gertak (*deterrence*) yang ditimbulkan dari penguasaan AS terhadap domain siber sebagai domain perang baru serupa dengan periode ketika AS memulai perang bintang dengan Soviet di era Perang Dingin. Penggunaan kekuatan siber pada masa-masa awal ini tidak hanya ditujukan kepada musuh AS yang tidak berimbang secara kekuatan seperti Irak pada Perang Teluk. Pembangunan ARPANet telah membuat negara-negara adidaya lainnya seperti Soviet dan Tiongkok berusaha keras untuk menandinginya. Kemutakhiran teknologi AS hari itu hanya baru ditanding kurang lebih satu dekade kemudian oleh kedua negara pesaing AS tersebut.

Perlindungan Tak Terlihat dan Paradigma Baru Keamanan Nasional

Upaya membuka rahasia lawan melalui dunia mayantara tidak hanya dilakukan AS pada perang-perang terbuka seperti di Irak dan Afghanistan. Pada bab ke-3 berjudul "A Cyber Pearl Harbor", Kaplan menghadirkan cerita yang berkaitan dengan sikap pemerintah AS pasca serangan terorisme oleh Timothy McVeigh pada kompleks perkantoran federal Alfred P. Murrah di Oklahoma atau dikenal dengan *Oklahoma City Bombing*. Serangan teroris terdahsyat sebelum peristiwa 9/11 tersebut mendorong pemerintahan AS di bawah Bill Clinton untuk memikirkan ulang skema perlindungan terhadap fasilitas federal. Salah satu buah pikiran dari pertemuan itu adalah pembangunan "pagar siber" bagi fasilitas federal AS dan objek vital nasional lainnya.

Perencanaan tersebut menandai sebuah kesadaran bahwa perang siber tidak hanya akan terjadi pada perang berkarakter konflik antar negara melainkan pula proteksi keamanan dalam negeri. Masih berkaitan dengan kasus *Oklahoma City Bombing*, komisi yang dibentuk oleh Bill Clinton memikirkan suatu prinsip yang mengubah manajemen keamanan selama-lamanya. Salah satu anggota dari komisi tersebut adalah Rich Wilhelm, Direktur Peperangan Informasi pada unit intelijen sinyal terkemuka di Amerika Serikat, NSA (*National Security Agency* yang karena kerahasiaannya sering diplesetkan sebagai *No Such Agency*).

Salah satu sumbangsih pemikiran Wilhelm dalam program ini adalah

pertanyaan kritis dan dekonstruktif tentang definisi keamanan. Wilhelm menganggap bahwa secara fisik, aset-aset federal bisa saja dijaga oleh pasukan bersenjata lengkap sehingga hampir tidak mungkin ditembus oleh siapapun secara konvensional. Namun, pada era informasi seperti abad 21, ancaman terhadap aset federal mampu melewati dan memecundangi penjagaan bersenjata tersebut. Hal ini disebabkan oleh karakteristik serangan yang langsung menarget jaringan komputer yang mengendalikan hampir seluruh aspek; kelistrikan, keuangan, dan bahkan dalam beberapa tempat adalah sirkulasi udara dan air.

Pemahaman tersebut memaksa banyak pihak untuk memikirkan ulang definisi keamanan. Penjagaan konvensional oleh tenaga manusia maupun hewan, sesuatu yang telah dilakukan sejak zaman praaksara, harus dilengkapi dengan perlindungan pada dunia yang tak nampak. Meskipun tak dipungkiri ada kompleksitas yang lebih, peran piranti perlindungan di mayantara memiliki prinsip yang sama dengan penjagaan keamanan di dunia nyata. Antara lain dengan membangun *digital fortress* atau *wall* dalam menjaga informasi tertentu.

Melalui episode sejarah ini pula, AS menyadari bahwa perang siber bukanlah sekadar tindakan meretas komputer atau membunuh kemampuan teknologi lawan. Ketika semua hal terkoneksi satu sama lain melalui jaringan internet, maka semua hal tersebut amat rentan terhadap serangan dunia maya. Pada prinsip yang paling dasar, perang adalah penggunaan kekerasan dan secara biologis kekerasan hanya dapat dirasakan jika tubuh manusia merasakannya. Setidaknya, ketika proyeksi kekuatan siber dapat membuat manusia merasa terancam maka tujuan perang siber dapat tercapai.

Peperangan Siber dan Ambisi Politik Luar Negeri AS

Amerika Serikat sebagai negara adidaya dikenal dengan ambisinya untuk "mengupayakan demokratisasi" bagi negara-negara lain yang dianggap bertentangan dengan ideologinya. Ambisi ini setidaknya begitu gamblang terlihat pasca "kemenangan bersama" AS dan Soviet pada Perang Dunia II. Setelah kemenangan tersebut, AS menaruh perhatian pada negara-negara yang bangkit pasca perang terutama berkenaan dengan kecenderungan ideologis mereka.

Negara-negara di benua Amerika sebagai halaman depan AS jelas tak luput dari perhatian politik Amerika Serikat. Di bawah kepemimpinan Presiden Clinton, AS berambisi untuk menyerang Haiti secara terbuka untuk menggulingkan pemimpin diktator, Jean Bertrand Aristide, di negara tersebut. Berbeda dengan invasi ke Irak, invasi ke Haiti tidak disebabkan oleh tindakan militer Haiti terhadap wilayah lainnya tetapi merupakan kejahatan pemimpin terhadap rakyatnya.

Sebagaimana operasi militer lainnya pada era tersebut, invasi akan

diproyeksikan melalui udara. Clinton meminta Direktur NSA, Kenneth Minihan, seorang perwira tinggi angkatan udara Amerika Serikat berbintang tiga untuk melumpuhkan sistem pertahanan udara Haiti untuk memberi jalan kepada armada pesawat pengangkut milik AS. Meskipun secara motif berbeda dengan Irak, terdapat kesamaan dalam objek komunikasi yang ditarget oleh AS yaitu saluran telepon. Tidak hanya berkenaan dengan *command and control* oleh pemimpin negara terhadap militernya; pertahanan udara Haiti ternyata bergantung banyak kepada saluran telepon.

Tidak hanya berniat untuk menyadap, AS melalui Kenneth Minihan dan stafnya pada direktorat peperangan siber NSA berencana untuk membuat saluran telepon Haiti menjadi super sibuk. Rencana ini diajukan oleh seorang teknisi NSA yang sejak kecil sering menjahili saluran telepon di sekitarnya. Dengan begitu, upaya melumpuhkan pertahanan udara Haiti tidak perlu dilakukan dengan menyerang langsung satuan-satuan pertahanan udaranya atau melumpuhkan meriam-meriamnya dari jarak dekat.

Rencana penyerangan Haiti dibatalkan oleh Presiden Bill Clinton. Sebagai gantinya, Clinton mengirim utusan ke Haiti untuk menyampaikan ultimatum Amerika Serikat jika Haiti melanjutkan segala bentuk kediktatorannya. Namun, ide untuk meretas saluran telepon Haiti memberi warna baru dalam metode perang elektronik bagi Amerika Serikat. Di kemudian hari, ketika saluran telepon tidak lagi menjadi piranti utama komunikasi, saluran internet menjadi sasaran strategis untuk "dibanjiri".

Sejarah Perang Siber: Topik Baru dengan Masalah Klasik?

Pilihan untuk membahas sejarah perang siber adalah sebuah terobosan dalam penulisan sejarah militer. Sebab teknologi perang siber terhitung mutakhir, maka belum banyak kajian sejarah yang membahas tema ini. Bagaimanapun, perlu dijadikan catatan bahwa karya Kaplan masih terjebak dengan masalah klasik sejarah militer yaitu kerangkeng institusi. Militer sebagai objek kajian sejarah memang memiliki karakteristik institusional yang kuat. Di negara manapun, militer selalu lekat dengan institusi ketentaraan. Secara tradisional, urusan peperangan pula didominasi oleh institusi ketentaraan milik negara. Penggunaan kata tradisional mengacu kepada perkembangan terkini tentang kehadiran kontraktor militer swasta atau awam disebut tentara bayaran.

Pembahasan Kaplan seringkali terbatas kepada sejarah atau bahkan sekadar profil dari unit intelijen sinyal terkemuka di AS: NSA. Perluasan pembahasan kepada institusi lain pula hanya sekadar menjelaskan bagaimana institusi tersebut berhubungan dengan NSA atau memainkan peran intelijen sinyal sebelum NSA didirikan. Sebagai contoh bagaiman peran intelijen angkatan laut dan angkatan udara AS yang memang turut berperan dalam formasi kekuatan perang elektronika yang kelak menjadi perang siber.

Masalah klasik lain yang terdapat pada karya Kaplan adalah narasi

elitis yang mendominasi. Sejarah militer sejak awal penulisannya pada masa Herodotus dan Thucydides memang merupakan sejarah para jenderal. Pada perkembangannya, kritik terhadap pendekatan ini dilontarkan dengan maksud "mengadvokasi" para prajurit untuk mendapat tempat di dalam sejarah. Karya Kaplan ini masih terjebak dalam narasi elitis tersebut; cerita yang dominan dihadirkan oleh Kaplan adalah dialog antara pemimpin di level strategis dan jarang menyentuh perihal yang terjadi pada lapisan bawah.

Nilai lebih dari karya ini adalah gaya penceritaannya yang khas Fred Kaplan; sang penulis menarasikan sejarah perang siber di AS layaknya novel fiksi-sains. Hal ini menarik karena ide mengenai perang siber, perang luar angkasa, dan revolusi sistem persenjataan 4.0 seringkali diawali dari narasi fiksi-sains yang dipikirkan kemungkinannya dalam dunia nyata. Dibandingkan dengan literatur sejenis seperti *Inside Cyber Warfare: Mapping the Cyber Underworld* karya Jeffrey Carr, karya Fred Kaplan lebih nampak mengalir meskipun kurang terstruktur.

Berbeda dengan Jeffrey Carr, Fred Kaplan memposisikan Amerika Serikat sebagai patron dan inti dari perkembangan peperangan siber di dunia sejak abad ke-20. Sebagaimana telah diungkapkan sebelumnya, karya Kaplan memang sangat amerika-sentris dan menganggap bahwa tren peperangan siber diawali di negeri paman sam tersebut. Sementara Carr, lebih "adil" dalam mengungkap perkembangan siber di dunia. Sebelum berbicara tentang lawan Amerika Serikat dalam konteks dunia yang bipolar, Israel adalah contoh kekuatan siber yang diungkap oleh Kaplan. Sebagai salah satu kekuatan siber di abad ke-21, Israel tentu tak bisa diekslusi dari sejarah perang siber. Terutama dengan pertanyaan utama bagaimana negara tersebut memperoleh dan terus membangun kekuatan sibernya.

Sebab narasi yang digunakan cenderung populer, Kaplan menarget pembaca yang lebih luas daripada kalangan akademisi semata. Karya ini juga seharusnya dibaca oleh pengambil kebijakan yang kerap menganggap bahwa fiksi memiliki kontribusi yang minim terhadap proses pembentukan kebijakan. Karya Kaplan ini pula dapat dijadikan referensi awal untuk mengetahui sejarah perang siber yang disajikan dengan gaya a la novel sains fiksi.