SINERGI DALAM MENGHADAPI ANCAMAN *CYBER WARFARE*
SYNERGY IN FACING OF CYBER WARFARE THREAT

Agus Subagyo[1]

FISIP UNJANI dan Seskoad Bandung
(subagyoeti@yahoo.com.au dan subagyo@scientist.com)

Abstrak - Di era globalisasi, hakekat ancaman tidak hanya berasal dari aspek militer dan fisik semata, melainkan juga datang dari ancaman nir militer dan non fisik, salah satunya adalah ancaman dunia maya. Saat ini, dunia telah memasuki era dunia maya, yang melahirkan kejahatan dunia maya dan sangat potensial menimbulkan ancaman perang dunia maya. Indonesia memerlukan tentara dunia maya untuk menghadapi ancaman perang dunia maya. Kementerian Pertahanan RI harus menjadi ujung tombak dalam proses menyusun kebijakan pertahanan dunia maya untuk menghadapi ancaman perang dunia maya. Sinergi antar pemangku kepentingan dan pihak-pihak terkait untuk menghadapi perang dunia maya adalah kunci sukses.

Kata kunci : dunia maya, kejahatan dunia maya, tentara dunia maya, pertahanan dunia maya

Abstract – *In the globalizations era, the origin of threat not only come from military and phisically aspect, but also come from nir military and non phisic, one of them is cyber threat. Today, the world entering an era of cyber space which could result to cyber crime and potentially threat of cyber warfare. Indonesia needs cyber troops to face threat of cyber warfare. Ministry of Defence must become a leading sector in the process of making cyber defence to contain threat of cyber warfare. The synergy of stakeholders to face threat of cyber warfare is the key to succeed.*

Keywords : *cyber space, cyber crime, cyber troops, and cyber defence*

Pendahuluan

Perkembangan politik dunia selalu mengalami perubahan dari waktu ke waktu sehingga mempengaruhi seluruh tatanan kehidupan dunia. Dunia yang dinamis terus mengalami perubahan yang kadangkala diwarnai turbulensi yang mempengaruhi relasi antar negara dan konstelasi isu global sehingga mempengaruhi sendi-sendi kehidupan berbangsa dan bernegara. Setiap perkembangan global di dunia selalu akan mempengaruhi seluruh kehidupan nasional di masing-masing negara sehingga memaksa setiap negara untuk selalu mencermati dan menelaah setiap perkembangan lingkungan strategis baik di tingkat global, regional, nasional, maupun lokal.

[1] Dr. Agus Subagyo, S.IP, M.Si, adalah Dosen Jurusan Hubungan Internasional FISIP UNJANI Bandung dan Dosen Non Organik Seskoad Bandung.

Pada era Perang Dingin (1945 – 1990), aktor dan isu global sangat diwarnai oleh "suasana kebatinan" perang ideologi antara Blok Barat (Amerika Serikat dan sekutunya yang berideologikan liberalisme kapitalisme) dengan Blok Timur (Uni Soviet dengan ideologi sosialisme komunisme). Kedua blok dunia tersebut saling serang dan saling berebut pengaruh di berbagai belahan dunia sehingga membuat negara-negara di dunia terbelah antara mendukung Blok Barat atau Blok Timur. Penentuan kawan atau lawan di masa Perang Dingin ditentukan oleh aspek idologi. Ancaman berat yang dihadapi saat itu adalah ideologi.

Pada masa pasca Perang Dingin (1990–2001), konstelasi politik internasional diwarnai oleh isu global berupa hak asasi manusia, demokrasi dan lingkungan hidup. Penentuan kawan atau lawan dalam politik internasional sangat ditentukan olehapakah suatu negara menjunjung tinggi nilai-nilai HAM dan demokrasi atau tidak. Isu-isu negara berbasis HAM, negara demokratis, dan negara-negara yang anti demokrasi dan anti HAM mengemuka ke permukaan sehingga menimbulkan polemik yang mewarnai tata internasional di dunia.

Pada masa pasca tragedi WTC dan Pentagon, 11 September 2001, sampai dengan sekarang ini, dunia diwarnai oleh perang global melawan terorisme (*Global War on Terror,* GWOT) yang dicanangkan oleh Amerika Serikat dan didukung oleh negara-negara Barat lainnya. Isu terorisme mulai menyeruak ke permukaan sehingga membelah dunia menjadi dunia teroris dan dunia anti teroris. Amerika Serikat menjadikan terorisme sebagai kampanye global untuk diperangi dan penentuan kawan atau lawan sangat didominasi oleh "apakah anda mendukung teroris atau anda anti teroris". Terorisme menjadi aktor dan isu global abad ke-21 sehingga menempatkan Al Qaeda, ISIS, Boko Haram, Al Shabab, Jamaah Islamiyah, dan lain-lain sebagai aktor utama dalam hubungan internasional.

Dinamika politik dunia semakin kompleks dan beragam sehingga mempengaruhi konstelasi politik domestik masing-masing negara. Setiap negara di dunia sekarang ini meningkatkan kewaspadaan akan adanya berbagai ancaman berupa konflik antar negara dan konflik domestik intra negara yang membahayakan keamanan nasional masing-

masing negara [2]. Ditambah lagi dengan adanya globalisasi telah mendorong perkembangan teknologi sehingga berbagai ancaman konflik dan perang antar milisi dengan pemerintah maupun antara negara besar dengan negara kecil makin kompleks sarana-prasarananya. Hal initerjadi karena penggunaan teknologi informasi dan komunikasi, khususnya dunia maya, yang kemudian mengarah pada ancaman perang *cyber (Cyber Warfare).*

Globalisasi dan Transnasionalisme Dunia

Arus globalisasi yang terjadi di seluruh dunia sekarang ini telah membawa dunia pada era perkembangan teknologi informasi dan komunikasi sehingga menciptakan era yang serba digital *(digital world).*Dalam hal ini, perkembangan teknologi komputer dan internet menjadi sarana baru bagi negara-negara di dunia untuk dimanfaatkan sebagai alat untuk melakukan berbagai penetrasi, pengaruh dan infiltrasi ke berbagai negara sehingga sangat mendorong dunia pada perkembangan yang kompleks, beragam dan majemuk.[3]

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

Transnasionalisme dunia di era globalisasi disatu sisi bermanfaat bagi kemakmuran dunia dan kesejahteraan masyarakat di dunia. Namun, disisi lain, terdapat dampak negatif

[2] Dinamika politik internasional di era pasca Perang Dingin mengalami perubahan yang sangat pesat, plural dan majemuk karena melahirkan berbagai dinamika ancaman yang bersifat militer dan nirmiliter dan sumber ancaman yang bisa berasal dari dalam negeri dan luar negeri. Untuk hal ini lihat dalam Anak Agung Banyu Perwita & Yanyan Moch Yani, *Pengantar Ilmu Hubungan Internasional*, (Bandung: Rosda, 2005), hlm. 119–121.

[3] Globalisasi telah menciptakan tatanan baru dalam hubungan internasional dengan adanya berbagai isu global dan aktor global yang menciptakan ancaman global di tengah arus perkembangan digital. Khususnya perkembangan teknologi informasi dan komunikasi yang melahirkan mobilitas manusia lintas negara sehingga melunturkan batas-batas yurisdiksi antar negara. Untuk hal ini, lihat dalam James Lee Ray, *Global Politics*, (New York: Houghton Miffin, 1998), hlm. 73-75.

berupa munculnya berbagai kejahatan transnasional yang sulit untuk diberantas oleh aparatur keamanan negara. Globalisasi telah melahirkan berbagai kejahatan lintas batas negara, berupa *illegal logging, illegal fishing, illegal mining, drug trafficking, human trafficking, smuggling*, dan kejahatan narkoba. Mafia atau sindikat kejahatan transnasional ini sulit dideteksi karena modus operandinya di beberapa negara, melibatkan pelaku dari beberapa negara, dan menggunakan teknologi informasi dan komunikasi dalam melakukan modus operandinya.

Selain itu, globalisasi juga telah memberikan "kesempatan" kepada beberapa kelompok radikal atau militan untuk melakukan berbagai aksi dan gerakan yang membahayakan kedaulatan negara, seperti kejahatan separatisme, terorisme, radikalisme, militanisme, dan fundamentalisme, yang menguat di era sekarang ini. Maraknya gerakan perjuangan kemerdekaan, organisasi kejahatan, dan militansi ideologi dan agama telah melahirkan konflik baru di setiap negara sehingga memposisikan negara berhadapan langsung dengan warga negara yang tergabung dalam kelompok militan berbasis ideologi dan agama tertentu. Hal inilah yang kemudian menjadikan ancaman dunia makin kompleks dan beragam, karena mereka memiliki jaringan yang luas di setiap negara dan didukung oleh penguasaan teknologi informasi dan komunikasi yang canggih sehingga mampu menjalankan aksinya secara nyata dan luas.[4]

Teknologi, *Cyber Space,* dan Sosial Media

Di era digital sekarang ini, teknologi memainkan peran yang sangat penting. Perangkat teknologi komputer dan internet telah menjadi alat kehidupan sehari-hari sehingga menjadikan setiap negara harus mampu menguasai, mengendalikan, dan mengawasi pergerakan manusia didalam dunia maya. Teknologi komputer dan internet telah menciptakan dunia baru yang bernama dunia maya, *cyber cpace,* yang didalamnya terdapat warga negara dunia maya dengan sebutan 'netizen', dan melakukan berbagai

[4] Di era global sekarang ini, ancaman militer telah meluas menjadi ancaman nirmiliter. Ancaman keamanan tidak hanya menyerang negara semata, melainkan telah menyerang langsung manusia yang ada dalam negara tersebut. Inilah yang kemudian melahirkan konsepsi "human security" yang telah menggeser konsepsi "national security". Untuk hal ini, lihat dalam Barry Buzan, *People, State, and Fear : An Agenda for International Security Studies in the Post-Cold War Era*, (Hempstead: Harvester Wheatsheaf, 1991), hlm. 32–36.

komunikasi, interaksi dan gerakan melalui media sosial sehingga sangat penting untuk diperhatikan setiap negara.

Dunia maya telah menjadi dunia kedua manusia untuk melakukan aktivitas kehidupan sehari-hari sehingga berbagai transaksi, pelayanan maupun perizinan dilakukan melalui penggunaan teknologi informasi dan komunikasi. Dunia maya telah melahirkan berbagai hal yang serba elektronik, seperti *e-commerce, e-procurement, e-bisnis, e-trade, e-service, e-life style*, dan lain-lain. Bahkan, sekarang ini, banyak sekali berbagai aplikasi yang berbasis elektronik di berbagai komunitas bisnis, perbankan, pemerintahan, kementerian, kampus, dan lain-lain. Hal ini menunjukkan bahwa dunia maya telah menjadi 'mainan' baru dalam kehidupan politik global.

Media sosial yang lahir karena adanya dunia maya, seperti *facebook*, *twitter, path, instagram*, dan lain-lain juga telah dijadikan sebagai alat komunikasi politik, propaganda, dan berbagai aktivitas gerakan sosial politik di berbagai negara. Munculnya fenomena "Arab spring" yang terjadi di negara-negara Timur Tengah berupa gerakan rakyat menumbangkan kekuasaan otoriter dilakukan dengan alat mobilisasi media sosial, khususnya *facebook* kala itu, sehingga perlu diperhatikan bagaimana dinamika perkembangan media sosial sebagai faktor pencipta citra publik dunia.

Indonesia sebagai negara yang aktif di dunia maya juga tidak kalah dalam hal rekam jejak di dunia maya. Beberapa perusahaan Indonesia yang bergerak di dunia media sosial menerbitkan data statistik yang menarik mengenai seberapa besar partisipasi Indonesia di dunia tersebut. Salah satunya adalah 2,4% dari jumlah seluruh tweet yang ada di dunia berasal dari pemilik akun Twitter yang berdomisili di Jakarta. Perusahaan yang merilis data statistik tersebut adalah adalah Social Bakers, Media Bistro, Brand24, dan Joy Intermedia. Data yang diperoleh merupakan hasil riset yang dilakukan di Indonesia mulai dari Desember 2012 hingga Maret 2013.[5]

Simak beberapa fakta menarik yang dihimpun dari perusahaan-perusahaan tersebut, terkait dengan media sosial di Indonesia berikut ini :[6]

[5] https://www.facebook.com/Motivasi.Bisnis.Motivasi.Hidup/posts/349529861845197,diunduh pada 12 Maret 2015.

[6] *Ibid.*

1. Media Sosial #1 : Twitter. Indonesia memegang ranking ke-5 sebagai negara dengan pengguna Twitter terbanyak. Saat ini, jumlah pengguna dari Indonesia adalah 29.000.000 akun Twitter. Indonesia berada di urutan ke-5 setelah Amerika Serikat, Brazil, Jepang, dan Inggris. Sekitar 2,4% tweet dari seluruh jumlah tweet di dunia berasal dari Jakarta. Jumlah tweet dari seluruh dunia adalah 10,6 miliar. Jakarta menyumbang 2,4% dari keseluruhan jumlah tersebut atau sekitar 255 juta tweets. Dengan jumlah ini, Jakarta mengungguli Tokyo (2,3%) dan London (2%).
2. Media Sosial #2 : Facebook. Ibukota Negara Indonesia, Jakarta, mempunyai 11,65 juta pengguna Facebook. Jakarta berada di urutan kedua dalam peringkat ibukota yang memiliki jumlah pengguna Facebook terbanyak. Peringkat pertama adalah Bangkok dengan jumlah 12,7 juta dan yang ketiga adalah Sao Paulo dengan jumlah 8,7 juta pengguna.59% pengguna Facebook di Indonesia adalah laki-laki.Perbandingan pengguna Facebook: Indonesia memiliki 59% laki-laki dan 41% wanita pengguna Facebook. Hal ini cukup berbeda dengan India yang memiliki 75% laki-laki dan 25% perempuan.
3. Media Sosial #3 : YouTube. Channel yang paling banyak dilihat adalah malesbangetdotcom.
4. Media Sosial #4 : LinkedIn. Indonesia mempunyai 1,3 juta pengguna LinkedIn. Sejak diluncurkan LinkedIn berbahasa Indonesia, negara ini termasuk salah satu negara yang paling besar pertumbuhan jumlah penggunanya, selain Turki dan Kolombia. Tiga akun perusahaan Indonesia yang terpopuler adalah Medco E&P Indonesia, Telkomsel, dan Pertamina.

Pengguna internet di Indonesia saat ini mencapai 63 juta orang. Dari angka tersebut, 95 persennya menggunakan internet untuk mengakses jejaring sosial. Direktur Pelayanan Informasi Internasional Ditjen Informasi dan Komunikasi Publik (IKP), Selamatta Sembiring mengatakan, situs jejaring sosial yang paling banyak diakses adalah Facebook dan Twitter. Indonesia menempati peringkat 4 pengguna Facebook terbesar setelah USA, Brazil, dan India. Indonesia menempati peringkat 5 pengguna Twitter terbesar di dunia. Posisi Indonesia hanya kalah dari USA, Brazil, Jepang dan Inggris. Selain Twitter, jejaring sosial lain yang dikenal di Indonesia adalah Path dengan jumlah

pengguna 700.000 di Indonesia. Line sebesar 10 juta pengguna, Google+ 3,4 juta pengguna dan Linkedlin 1 juta pengguna.[7]

Sebuah lembaga agensi dari luar negeri, *We Are Social*, juga membuat sebuah laporan yang sangat menarik untuk kita lihat. Laporan ini berisi mengenai bagaimana data jumlah pengguna website, *mobilephone*, dan media sosial dari seluruh dunia. Berikut adalah perkembangan dunia digital Indonesia:72,7 juta pengguna aktif internet. 72 juta pengguna aktif media sosial, dimana 62 juta penggunanya mengakses media sosial menggunakan perangkat *mobile*. Sebanyak 308,2 juta pengguna handphone. Selain itu, laporan tersebut juga mengungkapkan bahwa facebook masih menjadi media sosial yang paling banyak digunakan di Indonesia. Kemudian WhatsApp menjadi aplikasi *chatting* yang paling digemari penduduk tanah air.[8]

Cyber Crime, Cyber Police, dan *Cyber Law*

Perkembangan dunia maya telah melahirkan kejahatan dunia maya (*cyber crime*). *Cyber crime* adalah salah satu jenis kejahatan transnasional, karena melibatkan pelaku yang berasal dari dua negara atau lebih, korbannya bisa lebih dari satu negara, modus operandinya di dunia maya dengan menggunakan perangkat komputer dan internet, serta alat buktinya berupa alat bukti elektronik, sehingga memerlukan proses penegakan hukum yang modern dan canggih. *Cyber crime* bisa menyerang berbagai situs, blog, email, media sosial, maupun berbagai perangkat lunak komputer lainnya sehingga sangat membahayakan berbagai perusahaan, perbankan, instansi pemerintahan, maupun militer dan kepolisian yang berbasis pada komputer dan internet secara *online*.

Cyber crime yang marak belakangan ini tentunya memerlukan proses penegakan hukum yang dijalankan oleh pihak kepolisian secara terintegrasi. Wacana tentang "cyber police" mengemuka ke ruang publik seiring dengan adanya kekhawatiran dari berbagai pihak yang merasa dirugikan oleh aksi para *hacker* dan *cracker* di dunia maya. Banyak kasus di sektor perusahaan yang kehilangan data rahasia perusahaan oleh para *hacker* dan *cracker*.Sementara di komunitas perbankan juga merasa terancam karena

[7] http://harianti.com/ini-data-jumlah-pengguna-media-sosial-di-indonesia/,diunduh pada 13 Maret 2015.

[8] http://droidindonesia.com/apps/lifestyle/kebiasaan-pengguna-android-dan-internet-di-indonesia/, diunduh pada 13 Maret 2015.

pengamanan jaringannya seringkali jebol oleh ulah para *hacker* dan *cracker* yang melakukan aksi kriminal di dunia maya. Bahkan, seringkali para *hacker* menyebarkan virus untuk merusak jaringan yang dimiliki oleh situs-situs pemerintahan sehingga sangat membahayakan kedaulatan negara di dunia maya.

Di Indonesia, memang sudah ada unit khusus *cyber crime* di Mabes Polri yang menangani berbagai tindak pidana dunia maya. Namun demikian, kualifikasi maupun kompetensinya perlu ditingkatkan lagi sehingga mampu memberantas berbagai tindak kejahatan dunia maya yang marak belakangan ini. Perlu kiranya ke depan, Polri membentuk detasemen khusus dunia maya dimana terdapat unit-unit khusus di setiap Polda dan Polres yang menangani tentang *cyber crime* sehingga akan lahir *cyber police* di lingkungan Polri untuk menegakan hukum terhadap setiap laporan masyarakat yang dirugikan dan menjadi korban dari aksi *cyber crime.*

Selain itu, munculnya *cyber space* dan *cyber police* juga telah mendorong setiap negara di dunia, termasuk Indonesia untuk membentuk *cyber law* sehingga dapat dijadikan sebagai panduan dan payung hukum dalam menangani berbagai *cyber crime* sehingga *cyber security* Indonesia menjadi lebih aman dan nyaman. Di Indonesia sekarang ini, baru ada UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), sehingga belum ada lagi aturan hukum atau *cyber law* lainnya sebagai dasar dalam menegakan hukum terhadap kasus-kasus dan kejahatan *cyber crime*.

Ancaman *Cyber Warfare*

Kehadiran *cyber space, cyber threat, dan cyber crime* dalam kehidupan global dewasa ini telah memunculkan *cyber defence* atau pertahanan *cyber* di berbagai negara di dunia. Bahkan sudah banyak negara-negara di dunia membentuk berbagai unit khusus seperty *cyber army, cyber naval, cyber air force, cyber military, cyber troops,*maupun *cyber force*. *Cyber force* sangat diperlukan oleh setiap negara di dunia sekarang ini, khususnya di era teknologi, era komputer, era internet dan *era cyber,* sehingga berbagai cara harus dilakukan untuk melindungi berbagai pertahanan dunia mayanya dari berbagai serangan di dunia *cyber*.

Setiap negara di dunia harus mengembangkan kekuatan dan pengamanan di dunia maya mengingat banyak sekali ancaman yang dilakukan oleh pihak-pihak tertentu di dunia maya. Banyak sekali contoh kasus bagaimana sebuah situs atau *website* di suatu negara diretas atau disadap oleh pihak-pihak yang tidak bertanggungjawab. Sebagai contoh kasus perusahaan film terkemuka dunia, yakni Sony Pictures, di Amerika Serikat, yang diretas oleh *hacker* yang disinyalir berasal dari Korea Utara. Selain itu ada pula kasus Stuxnet, kasus peretasan situs kementerian pertahanan Amerika Serikat (Pentagon), kasus wikileaks (Edward Snowden), kasus penyadapan Australia dan Selandia Baru terhadap terhadap Indonesia, khususnya Presiden Ke-6, SBY, dan berbagai kasus penyadapan lainnya yang terjadi di dunia.

Hal ini mengindikasikan bahwa setiap negara di dunia harus mampu mengembangkan kekuatan pertahanan *cyber* agar dapat menahan serangan dunia maya dari berbagai pihak yang akan melakukan peretasan, penyadapan, dan pengrusakan terhadap berbagai sistem, *software,* maupun perangkat lunak lainnya. Semua negara harus menyadari bahwa ancaman keamanan global sekarang ini tidak hanya bersifat fisik semata, melainkan ancaman yang bersifat virtual, digital, dan dunia maya, berupa aksi kejahatan yang menyerang situs, *website* maupun berbagai instalasi dunia maya lainnya. Inilah yang kemudian melahirkan ancaman baru dalam dunia internasional, berupa ancaman perang *cyber* (*cyber warfare*).

Cyber Warfare memiliki arti perang yang dilakukan di dunia maya (*cyber space*) dengan menggunakan teknologi canggih dan jaringan *nircabel/wifi*. Sudah banya tulisan yang membahas tentang *Cyber Warfare* itu sendiri tetapi dewasa ini pengetahuan tentang ada *Cyber Warfare* baru sekedar dianggap sebagai pengetahuan yang baru serta tidak ditanggapi terlalu serius oleh para pengguna jaringan internet (*user*). Dalam tulisan ini penulis akan mencoba memaparkan bahaya yang akan dihadang oleh negara berkembang termasuk dalam ini Indonesia dalam menghadapi *Cyber Warfare.*[9]

[9] Internet muncul dan berkembang pada tahun 1969 melalui Proyek APRANET (*Advanced Research Project Agency Network*)yang merupakan proyek dari Departemen Pertahanan Amerika Serikat. Dengan berjalannya waktu, dirasa perlu ada suatu jaringan yang dapat menghubungkan antar wilayah satu dengan wilayah lainnya.Berawal dari gagasan ini, Departemen Pertahanan Amerika mulai membuka jaringan internet untuk dapat dinikmati oleh publik. Dengan internet dapat diakses oleh seluruh masyarakat dunia, membuat dunia ini seperti tidak ada sekat yang membatasi wilayah satu dengan lainnya. Lihat dalam Deky Rosdiana, "Cyber Warfare menjadi Ancaman NKRI di Masa Kini dan Masa Depan", dalam

Cyber Warfare sendiri berkembang dari *Cyber Crime* yang memiliki arti bentuk-bentuk kejahatan yang ditimbulkan karena pemanfaatan teknologi internet. Dapat juga didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. *The Prevention of Crime and The Treatment of Offenders* di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal: (1) *CyberCrime* dalam arti sempit disebut *computer crime*, yaitu perilaku ilegal/ melanggar yang secara langsung menyerang sistem keamanan komputer dan data yang diproses oleh komputer; (2) *Cyber Crime* dalam arti luas disebut *computer related crime*, yaitu perilaku ilegal/ melanggar yang berkaitan dengan sistem komputer atau jaringan.[10]

Cyber Crime merupakan kejahatan transnasional yang membahayakan karena akan mengarah kepada *Cyber Warfare*. Adapun jenis-Jenis kejahatan *Cyber Crime* dapat berupa :[11]

1. *Hacking* adalah kegiatan menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar mengotak-atik komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan (*security*)-nya. "Hacker" memiliki wajah ganda; ada yang budiman ada yang pencoleng. "Hacker" budiman memberi tahu kepada programer yang komputernya diterobos, akan adanya kelemahan-kelemahan pada program yang dibuat, sehingga bisa "bocor", agar segera diperbaiki. Sedangkan, *hacker* pencoleng, menerobos program orang lain untuk merusak dan mencuri datanya.
2. *Cracking* adalah hacking untuk tujuan jahat. Sebutan untuk "cracker" adalah "hacker" bertopi hitam (*black hat hacker)*. Berbeda dengan "carder" yang hanya mengintip kartu kredit, "cracker" mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, "hacker" lebih fokus pada prosesnya. Sedangkan "cracker" lebih fokus untuk menikmati hasilnya.

---

http://hankam.kompasiana.com/2013/09/23/cyber-warfare-menjadi-ancaman-nkri-dimasa-kini-dan-masa-depan-592343.html,diunduh pada 11 Maret 2015.

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

[11] *Ibid.*

3. *Cyber Sabotage* adalah kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
4. *Cyber Attack* adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi. Tindakan ini bisa ditujukan untuk mengganggu secara fisik maupun dari alur logis sistem informasi.
5. *Carding* adalah berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, biasanya dengan mencuri data di internet. Sebutan pelakunya adalah "carder". Sebutan lain untuk kejahatan jenis ini adalah *cyberfraud* alias penipuan di dunia maya.
6. *Spyware* adalah program yang dapat merekam secara rahasia segala aktivitas *online user*, seperti merekam *cookies* atau *registry*. Data yang sudah terekam akan dikirim atau dijual kepada perusahaan atau perorangan yang akan mengirim iklan atau menyebarkan virus.

Dalam *Cyber Warfare*, terdapat metode penyerangan yang tentunya berbeda dengan perang klasik, perang konvensional atau perang fisik lainnya. Domain dari *Cyber Warfare* berada dalam dunia maya, dimana yang menyerang adalah orang yang ahli teknologi informasi yang tidak harus datang langsung ke negara yang diserang. Wilayah yang diserang juga bukan wilayah fisik, wilayah teritorial, atau wilayah geografis, melainkan wilayah dunia maya.

Medan peperangan yang umum terjadi dalam perang fisik adalah perang di darat, perang di laut, perang di udara, dan perang di ruang angkasa. Namun, untuk perang *cyber*, wilayahnya di dunia maya. Berikut ini adalah metode penyerangan dalam *cyber warfare* :[12]

1. **Pengumpulan Informasi.** Spionase *cyber* merupakan bentuk aksi pengumpulan informasi bersifat rahasia dan sensitif dari individu, pesaing, rival, kelompok

[12] "Konsep Cyber War", dalam https://fairuzelsaid.wordpress.com/2010/08/29/cyber-law-konsep-cyber-war/, diunduh pada 13 Maret 2015.

lain pemerintah dan musuh baik dibidang militer, politik, maupun ekonomi. Metode yang digunakan dengan cara eksploitasi secara ilegal melalui internet, jaringan, perangkat lunak dan atau komputer negara lain. Informasi rahasia yang tidak ditangani dengan keamanan menjadi sasaran untu dicegat dan bahkan diubah.

2. **Vandalism.** Serangan yang dilakukan sering dimaksudkan untuk merusak halaman web (*Deface*), atau menggunakan serangan *denial-of-service* yaitu merusak sumberdaya dari komputer lain. Dalam banyak kasus, hal ini dapat dengan mudah dikembalikan. *Deface* sering dalam bentuk propaganda. Selain penargetan situs dengan propaganda, pesan politik dapat didistribusikan melalui internet via email, *instant messages*, atau pesan teks.
3. **Sabotase.** Sabotase merupakan kegiatan militer yang menggunakan komputer dan satelit untuk mengetahui koordinat lokasi dari peralatan musuh yang memiliki resiko tinggi jika mengalami gangguan. Sabotase dapat berupa penyadapan Informasi dan gangguan peralatan komunikasi sehingga sumber energi, air, bahan bakar, komunikasi, dan infrastruktur transportasi semua menjadi rentan terhadap gangguan. Sabotase dapat berupa *software* berbahaya yang tersembunyi dalam *hardware* komputer.
4. **Serangan Pada Jaringan Listrik.** Bentuk serangan dapat berupa pemadaman jaringan listrik sehingga bisa mengganggu perekonomian, mengalihkan perhatian terhadap serangan militer lawan yang berlangsung secara simultan, atau mengakibatkan trauma nasional. Serangan dilakukan menggunakan program sejenis *trojan horse* untuk mengendalikan infrastruktur kelistrikan.

Mengapa perlu tentara *cyber* ? Tentara *cyber* sangat diperlukan mengingat hakekat ancaman sekarang ini yang tidak hanya ancaman yang bersifat militer semata, melainkan ancaman yang bersifat nirmiliter, berupa - salah satunya - ancaman serangan *cyber*. Ancaman serangan *cyber* ini potensial terjadi karena era sekarang adalah era digital, era informasi, era komputer, era internet, dan era media sosial, dimana semua aktivitas manusia, semua transaksi ekonomi, semua data dilakukan dan disimpan dalam bentuk elektronik melalui *website*, situs, maupun berbagai data penyimpanan elektronik

lainnya. Serangan *cyber* sangat mungkin terjadi mengingat sudah banyak berbagai kasus penyadapan, pencurian data, dan pengrusakan sistem informasi yang dilakukan oleh para *hacker* terhadap berbagai situs kementerian pertahanan di banyak negara, khususnya Amerika Serikat.

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

Bagaimana kualifikasi tentara *cyber*? Tentara Cyber harus memiliki kualifikasi yang kompeten dan mumpuni dalam mengoperasionalkan komputer, mengelola internet, menyelidiki media sosial, melakukan penyadapan, dan mengunakan berbagai perangkat lunak dan perangkat keras lainnya. Tentara *cyber* harus mampu membangun sistem, jaringan, dan melakukan operasi dunia maya, penyidikan dunia maya, dan menangkis berbagai virus dunia maya, serta melindungi berbagai data dan informasi dalam sistem elektronik di Indonesia. Bahkan, tentara *cyber* harus memiliki kualifikasi untuk melakukan serangan balik terhadap serangan *cyber* dari negara lain atau pihak lain untuk menjaga kedaulatan negara di domain dunia maya.

Bagaimana cara merekrut tentara *cyber*? Tentara *cyber* harus direkrut oleh Kementerian Pertahanan melalui berbagai cara. Cara pertama adalah melalui tata cara pendaftaran sebagaimana yang umum dilakukan oleh TNI dalam merekrut calon TNI baik dalam mekanisme tamtama (secatam), bintara (secaba) dan perwira (Akmil, AAL, AAU, dan Sepawamil). Dalam perekrutan tamtama, bintara, dan perwira ini maka harus diberi kriteria tambahan, misalnya untuk sepawamil, maka kriterianya adalah sarjana teknologi informasi, sarjana komputer, dan sarjana pemrograman, sehingga ketika menjadi anggota TNI aktif maka dapat diarahkan untuk mengisi unit khusus / detasemen khusus tentara *cyber* atau *cyber force,* karena sudah memiliki latar belakang pendidikan, keahlian, dan

kualifikasi sarjana IT. Cara kedua adalah dengan cara menginventarisasi, mendata dan merekrut para anggota TNI aktif yang memang sudah memiliki keahlian dan kemampuan di bidang IT di berbagai kesatuan masing-masing sehingga dijadikan satu untuk dilakukan pelatihan khusus sehingga dapat mengisi unit khusus tentara *cyber*/*cyber force*.

Apa saja kesiapan dalam membentuk tentara *cyber*? Pembentukan tentara *cyber* harus melalui berbagai kesiapan yang matang dan sistematis, khususnya dengan dukungan anggaran, sarana prasarana, dan piranti lunak / regulasi yang lengkap dan terperinci. Anggaran yang besar sangat diperlukan untuk membentuk tentara *cyber* karena para tentara yang direkrut harus dididik, dilatih, dan dilakukan berbagai pendampingan, mentoring maupun pembinaan yang optimal sehingga akan terwujud tampilan dan sosok tentara *cyber* yang kompeten di bidangnya. Sarana prasarana berupa perangkat lunak dan perangkat keras komputer, jaringan dan berbagai perangkat pendukung lainnya perlu disiapkan sehingga akan mendukung tugas dan fungsi dari tentara *cyber.* Piranti lunak berupa aturan perundang-undangan, juklak, juknis, jukmin, protap maupun SOP dalam pelaksanaan tugas pokok dan fungsi tentara *cyber* harus jelas, detail dan terperinci.

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

Apakah perlu badan pertahanan *cyber*? Badan Pertahanan *Cyber* Nasional sebenarnya sangat diperlukan oleh Indonesia. Badan Pertahanan *Cyber* Nasional atau apapun namanya harus segera dipikirkan untuk dibentuk agar terwujud mekanisme koordinasi, komunikasi, dan sinergi antar berbagai aktor keamanan dan pertahanan dalam melindungi kedaulatan dunia maya Indonesia dari berbagai ancaman serangan

cyber. Kementerian Pertahanan, TNI, Polri, BIN, Kemenkominfo, Lembaga Sandi Negara dan berbagai instansi terkait lainnya harus mampu bersinergi untuk menangkis, menangkal, dan mencegah serangan *cyber* dari pihak tertentu atau dari negara lain yang mencoba untuk menganggu kedaulatan dunia maya Indonesia saat ini dan di masa depan.

Dalam kaitan ini, maka perlu sebuah analisis mendalam tentang penggunaan media sosial yang luarbiasa pada masyarakat Indonesia dengan potensi perang siber. Apakah penggunaan media sosial oleh masyarakat Indonesia (termasuk 5 terbesar dunia) dapat dianggap sebagai potensi positif (kekuatan) atau potensi negatif (kerentanan/kelemahan) jika dikaitkan dengan potensi perang siber. Penggunaan media sosial yang marak belakangan ini di tengah masyarakat Indonesia sebenarnya bisa menjadi kekuatan sekaligus juga kelemahan. Menjadi kekuatan karena melalui media social, maka masyarakat Indonesia dapat mewarnai opini public dunia dan mampu menjadi "trending topics" dalam berbagai media sosial, khususnya terkait dengan berbagai persoalan lokal, nasional maupun regional serta global. Melalui media sosial, maka akan berpotensi munculnya berbagai pengetahuan tentang dunia teknologi informasi, komunikasi dan digital, sehingga akan dapat merangsang tumbuhnya budaya melek teknologi, melek media sosial, dan melek dunia digital, serta dunia maya, yang pada akhirnya akan menjadi potensi dalam perang siber.

Namun demikian, pengguna media sosial yang sangat besar di tengah masyarakat Indonesia juga bias berpotensi menjadi kelemahan. Segala aktivitas kehidupan manusia Indonesia yang serba digital, serba siber, dan serba menggunakan teknologi informasi akan mudah disadap atau diretas oleh para hacker maupun cracker dari negara asing, sehingga akan menciptakan kerawanan, khususnya informasi intelijen yang menggunakan dunia maya sebagai sarana transmisi. Teknologi penyadapan yang canggih mampu secara cepat dan tepat melakukan upaya retas terhadap berbagai pengguna media sosial sehingga justru akan sangat membahayakan dalam era perang siber. Para pengguna media sosial harus menyadari tentang hal ini dan mampu membentengi diri melalui proteksi dari upaya penyadapan atau peretasan pihak-pihak asing dalam era perang siber.

Munculnya ancaman perang siber harus mendorong kesadaran semua pihak di Indonesia untuk memberikan perhatian lebih terhadap sistem pertahanan Indonesia. Seperti diketahui bahwa sistem pertahanan Indonesia adalah sistem pertahanan semesta

(sishanta), dimana komponen utama adalah TNI, dan komponen pendukungnya adalah rakyat. Dalam konteks ini, sistem pertahanan semesta yang tertuang dalam UU No. 3 Tahun 2002 Tentang Pertahanan Negara, harus mampu dimaknai sebagai semesta yang bersifat tidak hanya fisik semata, melainkan non fisik, khususnya digital dan dunia maya. Artinya, segala upaya dilakukan termasuk memberdayakan semua potensi dunia maya yang ada dalam menghadapi perang siber.

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

Sinergitas Menghadapi *Cyber Warfare*

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

Dalam menghadapi serangan *cyber*, diperlukan analisis terhadap eskalasi ancaman dan gradasi dalam menghadapi serangan *cyber*. Berikut ini diuraikan tentang eskalasi ancaman *cyber* dan lembaga terdepan sebagai ujung tombak yang menanganinya :

Tabel 1. Eskalasi Serangan Cyber

No	Jenis Ancaman	Intansi Utama Penanganan
1	Ancaman *Cyber (Cyber Threat*)	Kemenkominfo, Kemlu, Komunitas Informasi, Instansi Terkait Lainnya
2	Kejahatan *Cyber (Cyber Crime*)	Polri & Interpol
3	Perang *Cyber (Cyber Warfare*)	Kemhan, TNI, BIN

Sinergitas antar *stakeholders* sangat penting dilakukan untuk menangani dan menghadapi ancaman *Cyber Warfare*. Kementerian Pertahanan dan TNI harus melakukan berbagai langkah dan tindakan sinergitas untuk menghadapi ancaman *Cyber Warfare*. Dalam kaitan untuk menciptakan sinergitas menghadapi *Cyber Warfare*, maka Kementerian Pertahanan harus melakukan langkah sebagai berikut :

1. Kementerian Pertahanan harus mampu melakukan koordinasi dan meningkatkan kerjasama dengan Kementerian Informasi dan Komunikasi (Kemenkominfo) untuk menangkis, menangkal, dan mencegah berbagai potensi serangan *cyber* yang menyerang berbagai situs, *website*, media sosial, maupun jaringan komunikasi di semua lembaga perbankan, perusahaan, dan pemerintahan, sehingga akan mampu melindungi kedaulatan dunia maya Indonesia.
2. Kementerian Pertahanan harus membuat jalinan komunikasi, koordinasi dan kerjasama dengan komunitas pelaku informasi dan komunikasi, seperti berbagai operator telepon, seperti Telkom, Indosat, dan Excelcomindo, untuk mengantisipasi adanya serangan *cyber* berupa penyadapan telepon yang umum dilakukan oleh para penyerang dunia maya sehingga keamanan telepon dari masyarakat Indonesia, khususnya para pimpinan lembaga negara dapat terjamin dengan baik.
3. Kementeriaan Pertahanan harus menjalin kerja sama dengan aktor-aktor keamanan, seperti Polri, BIN, Lembaga Sandi Negara, dan aktor keamanan lainnya untuk menyatukan pandangan tentang berbagai ancaman *cyber* beserta pembagian tugas dan langkah penanganan terpadu sehingga akan dapat menangkal berbagai serangan *cyber* ke dalam berbagai wilayah dunia maya

Indonesia, termasuk penanganan *Cyber Crime* yang dapat meluas ke arah *Cyber Warfare.*

4. Kementerian Pertahanan harus mampu memberdayakan komunitas *hacker,* komunitas *cracker,* komunitas blog, komunitas media sosial, dan berbagai komunitas informasi dan dunia maya lainnya untuk selalu berpartisipasi dan memberikan informasi kepada Kementerian Pertahanan tentang berbagai potensi ancaman *cyber* dan bertukar informasi tentang langkah menghadapi berbagai serangan *cyber* yang membahayakan kedaulatan dunia maya Indonesia.
5. Kementerian Pertahanan harus menjalin kerjasama dengan berbagai perguruan tinggi yang memiliki pakar, ahli dan konsultan di bidang teknologi informasi, komunikasi dan dunia maya, untuk saling berdiskusi, berkoordinasi, tukar pengalaman dan tukar pendapat tentang berbagai ilmu, pengetahuan, inovasi, dan penemuan baru dalam teknologi dunia maya sehingga akan dapat meningkatkan keterpaduan dalam menghadapi ancaman *Cyber Warfare.*
6. Kementerian Pertahanan harus menjalin kerja sama internasional melalui mekanisme kerja sama bilateral, trilateral maupun multilateral dengan negara-negara lain di dunia, mengembangkan regulasi dunia maya, menciptakan etika dalam dunia maya, serta mencegah saling serang antar negara dalam dunia maya yang tentunya akan merusak hubungan antar negara.

Kesimpulan

Dalam era globalisasi sekarang ini, ancaman keamanan terhadap kedaulatan setiap negara tidak hanya bersifat ancaman militer yang bersifat fisik semata, melainkan telah meluas ke ancaman non fisik yang bersifat nirmiliter, yakni ancaman dunia maya atau ancaman *cyber,* yang mengarah pada *Cyber Crime*, dan berpotensi menyebabkan *Cyber Warfare.* Ancaman *Cyber Warfare* bersifat halus, tidak terlihat, dan sulit dirasakan, namun dampaknya sangat mematikan karena langsung menyerang "jantung" dan "hati" pertahanan setiap negara, sehingga sangat membahayakan.

Ancaman *Cyber Warfare* menyadarkan setiap negara di dunia, termasuk Indonesia untuk membentuk tentara *cyber,* karena ancaman *Cyber Warfare* tidak bisa dihadapi

dengan jumlah persenjataan, alutsista dan jumlah tentara yang banyak dan canggih, melainkan diperlukan tentara *cyber* yang memahami teknologi informasi, komunikasi, komputer, internet, dan media sosial. Ancaman *Cyber Warfare* sudah saatnya mendorong Indonesia untuk menyusun ulang sistem pertahanan yang berbasis pada *cyber* atau *cyber defence* dan *cyber security,* yang tentunya memerlukan persiapan yang matang dan sistematis dengan dukungan dari berbagai pihak dengan ujung tombak kementerian pertahanan dan TNI.

Sinergitas dalam menghadapi ancaman *Cyber Warfare* merupakan sebuah keniscayaan dan keharusan bagi Indonesia. Kementerian pertahanan harus mampu menjadi ujung tombak dalam mempelopori sinergitas antar berbagai komponen bangsa untuk melawan ancaman *Cyber Warfare.* Mekanisme pembangunan jalinan komunikasi, koordinasi, jaringan, dan kerja sama teknis harus digalakkan oleh Kementerian Pertahanan untuk membentuk komunitas pertahanan *cyber* (*cyber defence community*) yang dapat menangkal, mendeteksi, menangkis, dan mencegah secara dini berbagai potensi serangan ancaman *Cyber Warfare.*

Daftar Pustaka

Buku

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

Barda, Nawawi Arief. 2006. *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia.* Jakarta: RajaGrafindo Persada.

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

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

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

Perwita, Anak Agung Banyu & Yanyan Moch Yani. 2005. *Pengantar Ilmu Hubungan Internasional*. Bandung: Rosda.

Ray, James Lee. 1998. *Global Politics*. New York: Houghton Miffin.

Jurnal

Gollese, Petrus Reinhart, 2006. "Perkembangan cyber crime dan upaya penanganannya Di Indonesia oleh Polri". *Buletin Hukum Perbankan*. Vol.4 No. 2.

Sinaga, Dian, 2004, "Kejahatan TerhadapBuku dan Perpustakaan". *Jurnal Visi Pustaka*. No.6. Vol.1.

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

Website

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

Said, Fairuzel, "Konsep Cyber War", dalam https://fairuzelsaid.wordpress.com/2010/08/29/cyber-law-konsep-cyber-war/, diunduh pada 13 Maret 2015.

http://droidindonesia.com/apps/lifestyle/kebiasaan-pengguna-android-dan-internet-di-indonesia/, diunduh pada 13 Maret 2015.

http://harianti.com/ini-data-jumlah-pengguna-media-sosial-di-indonesia/, diunduh pada 13 Maret 2015.

https://www.facebook.com/Motivasi.Bisnis.Motivasi.Hidup/posts/349529861845197, diunduh pada 12 Maret 2015.

http://capungtempur.blogspot.com/2012/04/pengertian-cyber-crime.html. Diunduh pada 14 Maret 2015.

http://id.wikipedia.org/wiki/Teknologi_Informasi_Komunikasi, diunduh pada 14 Maret 2015.

http://karimullah83.blogspot.com/2011/04/pengertian-hacking-carding-dan-cracking.html, diunduh pada 14 Maret 2015.

http://jupren.blogspot.com/2009/04/faktor-penyebab-cybercrime.html, diunduh pada 14 Maret 2015.

http://amicha321.files.wordpress.com/2010/06/cybercrime-kelompok-7.pdf, diunduh pada 14 Maret 2015.

Undang-Undang

UU No. 36 Tahun 1999 Tentang Telekomunikasi.

UU No. 2 Tahun 2002 Tentang Polri.

UU No. 3 Tahun 2002 Tentang Pertahanan Negara.

UU No. 34 Tahun 2004 Tentang TNI.

UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

UU No. 17 Tahun 2011 Tentang Intelijen Negara.

Lain-lain

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