# BAB II

# PERKEMBANGAN SIBERNETIKA DAN PENGARUHNYA

## A. Tinjauan Umum Sibernetika

### 1. Pengertian Sibernetika

Sibernetika adalah bidang studi yang sangat luas, tetapi tujuan penting dari sibernetika adalah untuk memahami dan menentukan fungsi dan proses dari sistem yang memiliki tujuan dan yang berpartisipasi dalam lingkaran rantai sebab akibat yang bergerak dari aksi/tindakan menuju ke penginderaan lalu membandingkan dengan tujuan yang diinginkan, dan kembali lagi kepada tindakan.

Sibernetika didefinisikan oleh Norbert Wiener sebagai suatu studi terhadap kontrol dan komunikasi pada binatang dan mesin. Stafford Beer menyebutnya sebagai ilmu organisasi efektif dan Gordon Pask memperluasnya dengan mencakup aliran informasi "pada semua media" dari bintang hingga otak.

Sibernetika berfokus kepada bagaimana sesuatu itu (digital, mekanik, atau biologis) memproses informasi, bereaksi terhadap informasi, dan berubah atau dapat diubah agar dapat mencapai dua tugas pertama dengan lebih baik. Definisi yang lebih filosofis, disarankan pada tahun 1956 oleh Louis Couffignal, salah seorang pelopor sibernetika, mengkarakterisasi sibernetika sebagai seni untuk memastikan keberhasilan tindakan. Definisi terkini

disampaikan oleh Louis Kauffman, Presiden dari *American Society for Cybernetics,* Sibernetika adalah sebuah studi dari sistem dan proses yang berinteraksi dengan diri mereka sendiri dan memproduksi diri mereka dari diri mereka sendiri.

Sibernetika kontemporer mulai sebagai studi interdisiplin yang menghubungkan bidang-bidang sistem kendali, teori sirkuit, teknik mesin, logika pemodelan, biologi evolusi, neurosains, antropologi, dan psikologi. Pada tahun 1940-an, sering dikaitkan dengan Konferensi Macy. Bidang-bidang studi lain yang telah mempengaruhi atau dipengaruhi oleh sibernetika diantaranya, teori sistem (counterpart matematis untuk sibernetika), teori kendali persepsi, sosiologi, psikologi (khususnya neuropsikologi, psikologi perilaku, psikologi kognitif), filosofi, arsitektur dan teori organisasi.

## 2. Perkembangan Sibernetika

### a. *Cyberspace*[1]

Istilah ruang *cyber* (*cyberspace*) awalnya diperkenalkan oleh William Gibson dalam buku berjudul *Neuromancer* pada 1984 guna menjelaskan dunia maya bermesin tiga dimensi (*Virtual Reality/VR*), dan pada gilirannya menyentuh hasil temuan teknologi informasi (TI) yang mampu membentuk jejaring komputer sejagat, yakni internet. Internet memiliki banyak kegunaan, namun fasilitas yang sering dimanfaatkan berupa *Electronic Mail* (*e-mail*), *Mailing List (mailist* atau *e-mail groups*), *World*

[1] M Badri, "Sibernetika" Diktat Kuliah Jurusan Ilmu Komunikasi Fakultas Dakwah dan Komunikasi UIN Sultan Syarif Kasim Riau hlm. 9.

*Wide Web (WWW*), *File Transfer Protocol (FTP), InternetRelay Chat (IRC), Netsearch* atau *Search Engine*. Pada awalnya, produsen piranti lunak komputer menyediakan aplikasi terpisah untuk masing-masing fasilitas tersebut, namun pada gilirannya pengguna Internet dapat menggunakan semua fasilitas tersebut di dalam satu aplikasi *web based*.

Dari konsep Gibson di atas, menurut Severin dan Tankard (2005) ruang siber dapat didefinisikan sebagai realitas yang terhubung secara global, didukung komputer, berakses komputer, multidimensi, artifisial atau virtual. Dalam realita ini, di mana setiap komputer adalah jendela, terlihat atau terdengar objek-objek yang bukan bersifat fisik dan bukan representasi objek-objek fisik, tapi lebih merupakan gaya, karakter, dan aksi pembuatan data, pembuatan informasi murni.

Penemuan dan perkembangan TI dalam skala massal mengubah bentuk masyarakat menjadi masyarakat dunia global. Sebuah dunia yang sangat transparan terhadap perkembangan informasi, transportasi, serta teknologi yang begitu cepat dan begitu besar mempengaruhi peradaban umat manusia, sehingga dunia juga dijuluki *thebig village* (desa global), yaitu sebuah desa yang besar yang di mana masyarakatnya saling mengenal dan saling menyapa satu dengan yang lainnya seperti layaknya kehidupan yang berkembang di desa.

Konsep desa global dikenalkan oleh Marshall McLuhan pada awal tahun 1960-an dalam bukunya yang berjudul *Understanding Media: Extension of A Man*. Konsep ini berangkat dari pemikiran McLuhan

bahwa suatu saat nanti informasi akan sangat terbuka dan dapat diakses oleh semua orang. Pada masa ini, mungkin pemikiran ini tidak terlalu aneh atau luar biasa, tapi pada tahun 1960-an ketika saluran TV masih terbatas jangkauannya, internet belum ada, dan radio masih terbatas antardaerah, pemikiran McLuhan dianggap aneh dan radikal.

Desa Global menjelaskan bahwa tidak ada lagi batas waktu dan tempat yang jelas. Informasi dapat berpindah dari satu tempat ke belahan dunia lain dalam waktu yang sangat singkat, menggunakan teknologi internet. McLuhan meramalkan pada saatnya nanti, manusia akan sangat tergantung pada teknologi, terutama teknologi komunikasi dan informasi. McLuhan memperkirakan apa yang kemudian terjadi pada masa sekarang, di abad ke-20 seperti saat ini.

McLuhan memperkirakan pada masa digital dan serba komputer tersebut, persepsi masyarakat akan mengarah kepada perubahan cara serta pola komunikasi. Bagaimana pada saat itu, masyarakat tidak akan menyadari bahwa mereka sedang mengalami sebuah revolusi komunikasi, yang berefek pada komunikasi antarpribadi. Di atas level komunikasi interpersonal yakni komunikasi antara dua-tiga orang, pada masa desa global benar-benar terjadi tren komunikasi akan ke arah komunikasi massa, yakni bersifat massal dan luas.

Di mana pembicaraan akan suatu topik dapat menjadi konsumsi dan masukanbagi masyarakat luas, kecuali, tentu saja, hal-hal yang bersifat amat rahasia sepertirahasia perusahaan, rahasia negara, keamanan-

ketahanan. Semua orang berhak untukikut dalam pembicaraan umum, dan juga berhak untuk mengkonsumsinya, tanpaterkecuali.

**b. *Cybercrime***

*Cyber crime* merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang merndapat perhatian luas di dunia internasional. Volodymyr Golubev menyebutnya sebagai *the new form of anti-social behavior*. Beberapa julukan/sebutan lainnya diberikan kepada jenis kejahatan baru ini dalan berbagai tulisan, antara lain, sebagai kejahtan dunia maya (*cyber space/virtual space offense*), dimensi baru dari *hight tech crime*, dimensi baru dari *transnational crime*, dan dimensi baru dari *whitte collar crime*.

*Cybercrime* saat ini digunakan untuk menunjukkan kepada kejahatan yang berhubungan dengan *cyberspace* dan tindakan kejahatan yang menggunakan komputer. Perkembangan *cyberspace* yang pesat menyebabkan terjadinya penyalahgunaan teknologi tersebut oleh pihak-pihak yang tidak bertanggung jawab. Penyalahgunaan dari perkembangan *cyberspace* tersebut yang akhirnya disebut sebagai *cybercrime*.

Istilah *cybercrime* biasanya digunakan secara sinonim dengan kejahatan teknologi, kejahatan teknologi tinggi, *high tech crime*, kejahatan ekonomi, kejahatan Internet, kejahatan digital, atau kejahatan elektronik, dimana beberapa istilah tersebut digunakan untuk menggambarkan

kejahatan yang berhubungan dengan komputer atau perangkat IT yang lain.

Secara umum kejahatan di dunia siber (*cybercrime*) adalah upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.

Bisa dikatakn bahwa *cyber crime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Kekhawatiran demikian terungkap pula dalam makalah *cyber crime* yang disampaikan oleh ITAC (*Informastion Technology Association of Canada)* pada Internasional Information Industry Congresss (IIIC) 2000 Millenium Congress di Quebec pada tanggal 19 september 2000, yang menyatakan bahwa *cyber crime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can alectronically enabled crime*.

Sehubungan dengan kekhawatiran akan ancaman/bahaya *cyber crime* ini karena berkaitan erat dengan *economic crimes* dan *organized crime* (terutama untuk tujuan money laundering), kongres PBB mengenai *The Prevention of Crime and the Treatment of Offenders* (yang diselengarakan tiap lima tahun) telah pula membahas masalah ini. Sudah dua kali masalah

*cyber crime* ini diagendakan, yaitu pada kongres VIII/1990 di Havana dan pada kongres X/2000 di Wina.

Terdapat beberapa bentuk kejahatan yang berhubungan erat dengan *cybercrime* dan penyalahgunaan dari sistem informasi, salah satunya adalah dari *Encyclopedia of Cybercrime* yang membagi tindakan *cybercrime* menjadi[2]

1. *Negligent use of information systems while violating security policies or engaging in unsound information security practices and thereby exposing systems and data to cyber attacks* (kelalaian dalam penggunaan sistem informasi ketika melanggar kebijakan keamanan atau terlibat didalam praktek tidak sehat informasi keamanan dan dengan cara menyebarluaskan sistem dan data untuk diserang);
2. *Conventional crimes involving use of computers or other types of electronic IT devices for communications and/or record keeping in support of their illegal activities* (kejahatan konvesional yang menyertakan penggunaan komputer atau alat elektronik lain yang digunakan untuk berkomunikasi dan/atau menyimpan hasil rekaman yang digunakan untuk membantu dalam aktivitas ilegal);
3. Penipuan online seperti *phising*, *spoofing*, *spimming*, yang bertujuan untuk menipu orang secara online untuk mendapatkan

[2] Sukma Indrajati, "Tinjauan Hukum Internasional Terhadap *Cyber Espianage* Sebagai Salah Satu Bentuk *Cybercrime",* Skripsi Fakultas Hukum Universitas Hasanudin Makasar, 2014, hlm.37.

keuntungan finansial baik dalam penipuan kartu kredit atau pencurian identitas;

4. *Hacking, computer trespassing,* dan *password cracking* yang bertujuan untuk menembus *password* akun komputer dan/atau masuk secara melanggar hukum sistem informasi untuk melakukan kejahatan secara *online* dan/atau secara *offline*;
5. *Malicious writing* dan membagikan kode komputer yang terkait membuat, mengkopi, dan/atau melepaskan *malware*;
6. Pembajakan digital terhadap musik, film, dan/atau perangkat lunak;
7. *Cyber harrasment,* ancaman, membuat malu secara sengaja, atau pemaksaan, termasuk *cyber bullying*;
8. Penguntitan secara *online* (*online stalking*) dan tindakan *cyber-sex,* termasuk mengirimkan gambar atau pesan yang tidak dinginkan yang memuat unsur seksual, mempromosikan pariwisata sex, atau menggunakan internet untuk memfasilitasi penjualan manusia untuk kegiatan seksual atau tujuan lainnya;
9. Kecurangan akademik dan *scientific misconduct* yang dilakukan oleh pelajar, guru, atau professor untuk kegiatan menjiplak, kecurangan dalam tugas atau ujian, atau penipuan metode riset atau penemuan;
10. Kejahatan terorganisir yang menyertakan penggunaan internet yang berbasis etnis untuk memfasilitasi kombinasi aktivitas ilegal

dan legal seperti penyelundupan dan penjualan manusia, senjata, dan obat-obatan;

11. Tindakan memata-matai yang dilakukan oleh pemerintah atau pekerja lepas termasuk spionase perusahaan yang melibatkan penggunaan *spyware* dan *key logger software* untuk menemukan data yang dapat dicuri atau digunakan untuk melakukan kejahatan tambahan;
12. *Cyberterrorism* yang dilakukan oleh orang-orang yang mencoba untuk memajukan tujuan sosial, agama atau politik dengan cara menanamkan secara luas ketakutan atau dengan melakukan pengerusakan atau mengganggu informasi infrastruktur yang penting.

Sedangkan diliteratur lainnya mengelompokkan *cybercrime* menjadi beberapa bentuk, antara lain:[3]

1. *Unauthorized Access to Computer System and Service*

   Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

[3] *Ibid*., hlm. 40.

2. *Illegal Contents*

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat diangap melangar hukum atau mengganggu ketertiban umum.

3. *Data Forgery*

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet.

*4. Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran.

*5. Cyber Sabotage and Extortion*

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

*6. Offense Against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain dan sebagainya.

*7. Infringements of Privacy*

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan seseorang pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain akan dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

**c. *Cyber espionage* (Spionase *cyber*)[4]**

Banyak ragam kejahatan siber yang telah beredar di seluruh dunia. Salah satu bentuk kejahatan siber tersebut adalah *Cyber Espionage* atau spionase *cyber*. *Cyber Espionage* adalah kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi. Berdasarkan salah satu perusahaan yang bergerak dibidang keamanan komputer, Symantec, spionase merupakan salah satu ke khawatiran utama dari perusahaan-perusahaan.

Perusahaan mengakui, spionase industri tetap menjadi kekhawatiran utama mereka. Sebanyak 45% persen responden mengakui menemukan orang dalam yang berbahaya. Banyak serangan yang justru berasal dari

[4] *Ibid*., hlm.43.

internal perusahaan, karena masalah persaingan. Ini dianggap lebih berbahaya, karena dibandingkan serangan dari luar yang bisa diantisipasi secara global, serangan dari dalam akan sulit terlacak secara dini.

Serangan *cyber espionage* sendiri menggunakan perantara melalui virus dengan cara mengirimkan virus masuk ke komputer lawan dan kemudian virus tersebut akan memantau aktivitas yang terjadi di komputer yang dimasukinya. Seperti halnya kasus yang terjadi di Timur Tengah, terutama di Iran dimana virus komputer baru bernama *Flame* dikabarkan telah menyerang ratusan komputer. Virus baru yang sangat pintar itu diduga dibuat Israel untuk mengacaukan program nuklir Iran.

*Flame* tak hanya mampu mengambil seluruh data yang tersimpan di dalam komputer yang terinfeksi, tapi juga mampu memantau seluruh aktivitas pengguna komputer, dengan cara mengambil gambar layar yang sedang dibuka dan merekam tombol-tombol yang ditekan pada papan ketik (*keystrokes*). *Flame* juga bisa mengaktifkan sistem audio komputer, termasuk mikrofon, sehingga bisa menguping setiap pembicaraan pengguna. Keunggulan lain *Flame* adalah mengakses telepon seluler berkoneksi *bluetooth* yang berada di sekitar komputer terinfeksi48. Kemampuan dari virus tersbut digunakan untuk memata-matai bahkan dapat digunakan untuk melakukan sabotase terhadap negara yang diserangnya.

Para periset Laboratorium McAfee yang berbasis di Santa Clara, California, Amerika Serikat, menyatakan virus jenis *malware* terdeteksi

sengaja dirancang dan diunggah khusus untuk mencari informasi yang mengacu pada kata-kata tertentu. Kata-kata yang menjadi acuan bagi *malware* tersebut bekerja misalnya "pasukan AS di Korsel", latihan perang", atau bahkan "rahasia". *Malware* tersebut diperkirakan sudah tertanam sejak tahun 2009 bahkan pada tahun 2007 telah dideteksi *malware* yang lebih kurang serupa.

Selain virus *Flame*, serangan *cyber espionage* juga dilakukan dengan menggunakan virus *Stuxnet*. *Stuxnet* merupakan virus yang dipercayai dibuat oleh Amerika Serikat dan Israel untuk menyerang fasilitas nuklir Iran. Virus ini ditemukan pada bulan Juni 2010. Virus *Stuxnet* didesain bekerja dengan cara hanya memasuki *Siemens supervisory control and data acquisition (SCADA).*

Virus *Stuxnet* didesain hanya menyerang sistem tersebut dikarenakan sistem tersebut yang digunakan oleh pihak Iran untuk mengontrol dan dan memonitor proses industri fasilitas nuklir Iran. *Stuxnet* akan memasuki sistem tersebut dan melakukan aktivitas pengintaian dan menumbangkan sistem industri dan menyertakan *programmable logic controller rootkit* yang akan mengambil alih kontrol dari komputer yang diserang.

Amerika Serikat dan Israel berhasil melumpuhkan fasilitas nuklir Iran dengan menggunakan serangan dari virus *Stuxnet*. Virus tersebut berhasil menyabotase fasilitas pengolahan uranium yang berada di Natanz. Virus tersebut menyebabkan penurunan kapasitas sebesar 30 persen. Virus tersebut menyabotase mesin pemutar dengan cara pertama menaikkan

kecepatannya dan kemudian menurunkan kembali sehingga membuat mesin pemutar menjadi rusak.

**e. *Cyberware* (Perang *Cyber*)**

Untuk mendefinisikan perang *cyber* harus didahului dengan definisi dunia maya. Departemen Pertahanan AS telah menyempurnakan definisi tersebut, melalui pembaruan dari kamus militer resmi AS Joint Publication (JP) 1-02, mendefinisakn dunia maya : *global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*

Definisi pada JP 1-02 Selain mengidentifikasi sifat global dari dunia maya, juga mereferensikan lingkungan informasi, menghubungkan dunia maya dan dunia fisik, infrastruktur kritikal masyarakat, dunia informasi, dimana data dibuat dan disimpan, dan aspek kognitif di mana persepsi manusia dan keputusan dibuat. Keterkaitan ini membuat perang *cyber* menjadi bagian menarik dari perang konvensional dan menautkan dunia maya dengan keamana nasional.

Kemudian menurut *Oxford Dictionaries, cyber (adjective) relating to or characteristic of the culture of computers, information technology, and virtual reality*. Mengatakan bahwa *cyber* berasal dari kata *cybernetics*

yaitu *the science of communications and automatic control systems in both machines and living things*.

Sedangkan pemahaman *warfare* dari sumber yang sama adalah *engagement in or the activities involved in war or conflict*. Kata *warfare* itu lebih berkenaan pada metode perang, sedangkan kata *war* memiliki definisi 1) *a state of armed conflict between different countries or different groups within a country;* 2)*a state of competition or hostility between different people or groups;* 3)*a sustained campaign against an undesirable situation or activity.*[5]

Dari definisi tersebut secara pembahasan etimologi bahasa diatas dapat disimpulkan bahwa perang sibernetika atau *cyberwarfare* adalah sebuah konflik yang memanfaatkan teknologi sibernetika, namun masyarakat luas menyimpulkan bahwa perang *cyber* hanyalah perang dalam domain dunia maya. padahal penyederhanaan tersebut tidak cukup, karena dua alasan.

Pertama, definisi perang di dunia maya terlalu luas. Perang *cyber* tidak dapat di samakan dengan *information operations* (IO), namun dapat menjadi bagian dari IO. IO terdiri dari operasi psikologis, penipuan militer, operasi keamanan, peperangan elektronik, dan *computer network operations* (CNO). CNO merupakan tindakan penggunaan jaringan komputer untuk menyerang sistem informasi masyarakat atau jaringan komputer mereka. Sedangkan perang *cyber* menggunakan dunia maya untuk menyerang personil, fasilitas, atau peralatan selain informasi dan

[5] Trisuharto Clinton, "Kajian Perang Sibernetika (*Cyber-Warfare*) Sebagai Konflik Bersenjata Internasional Berdasarkan Hukum Humaniter Internasional", Skripsi Fakultas Hukum Universitas Diponegoro Semarang, 2015, hlm.62.

komputer. Kedua, mendefinisikan perang *cyber* sebagai perang di dunia maya mengabaikan kompleksitas penerapan hukum perang yang lebih fundamental ke dunia maya.

[6]Menurut Salahuddien, *cyberwarfare (cyberwar)* adalah penggunaan teknologi komputer dan internet untuk melakukan perang di dunia maya. Pelaku *cyberwar* saling bersaing untuk menguasai dan memanfaatkan sumber daya teknologi serta informasi yang ada di dalamnya untuk menyerang, menghancurkan, menyesatkan, mempengaruhi, menyandera, mengurangi, menghilangkan, mengalihkan, mengganggu, menghentikan komunikasi, arus informasi dan isinya serta berbagai tindakan lain yang mengakibatkan kerugian dan melemahkan lawan.

[7]*Cyber warfare* juga di kenal sebagai perang *cyber* yang mengacu pada pengguna fasilitas www (*world wide web*) dan jaringan komputer untuk melakukan perang di dunia maya. Perang *cyber* juga didefinisikan sebagai peperangan yang menggunakan peralatan elektronik dan komputer untuk menghancurkan atau mengganggu peralatan elektronik dan jalur komunikasi lawan/musuh. Perang *cyber* dapat berupa konflik antara negara, maupun melibatkan aktor-aktor non-negara. Sangat sulit dalam perang *cyber* untuk mengarahkan kekuatan yang tepat dan proporsional, target yang dituju bisa militer, industry, atau sipil atau bisa hanya sebuah ruang server yang membawahi berbagai klien.

---

[6]M Badri, Op.Cit., Hlm.41-44.

[7]Moehammad Yuliansyah Saputera, "Pengaruh *Cyber Security Strategy* Amerika Serikat Menghadapi Ancaman *Cyber Warfare",* Tugas Paper Hubungan Internasional Fisip Universitas Riau", hlm.6.

[8]Dalam perkembangan *Cyber Warfare*, penggunaan teknologi sistem informasi juga dimanfaatkan untuk mendukung kepentingan komunikasi antar prajurit atau jalur komando yang difasilitasi oleh sistem komando kendali militer moderen, yaitu sistem NCW (*Network centric warfare*). *Network Centric Warfare* atau NCW adalah konsep operasi militer moderen yang mengintergrasikan seluruh komponen atau elemen militer kedalam satu jaringan komputer militer NCW berbasis teknologi satelit dan jaringan internet rahasia militer yang disebut jadingan SIPRNet(*Secret internet Protocol Router Network*).

Teknologi NCW didukung infrastuktur SIPRNet sebagai komponen militer atau elemen militer dapat saling terhubung secara *online* sistem dan *real-time*, sehingga keberadaan lawan dan kawan dapat di ketahui melalui visualisasi di layar komputer atau laptop. Teknologi NCW ini telah dimiliki dan diaplikasikan oleh militer Amerika Serikat.

Penting untuk diketahui bahwa pengertian *cyber-warfare* tidak dapat disamakan dengan *cybercrime*, meskipun keduanya memiliki kesamaan memanfaatkan adanya teknologi *cyber* guna melakukan suatu penyerangan yang disebut *cyber attack. Cyber-Crime* adalah tindakan kejahatan untuk memperoleh keuntungan dari adanya teknologi *cyber* dengan melawan hukum, dapat dikatakan *cybercrime* lebih masuk pada ranah hukum pidana atau hukum pidana internasional. Sedangkan *cyber warfare* ialah suatu

[8] *Ibid.*

tindakan memicu konflik yang memanfaatkan teknologi *cyber* dimana dalam prakteknya kental akan muatan politik.

Perang *cyber* pernah dilakkan AS ketika menginvasi Irak pada tahun 1991. Dimana pada Operasi Badai Gurun tahap pertama pihak AS melakukan misi udara strategis untuk menyerang pertahanan strategis udara Irak, lapangan udara/ pesawat, sistem komando dan kontrol,fasilitas telekomunikasi, dan elemen kunci infrastruktur nasional. AS juga menggunakan komunikasi yang ekstensif dan sistem satelit untuk mendukung aktivitas Badai Gurun.

## B. Mengukur Kekuatan *Cyber* Suatu Negara[9]

Menurut Richard A. Clarke (2010) dalam mengukur kemampuan *cyberwarafare* suatu negara secara realistic dapat dilakukan dengan mempertimbangkan pengukuran dengan tiga faktor, yaitu;

1. *Offense*

   *Offense* merupakan ukuran kemampuan suatu negara dalam melakukan penyerangan guna melemahkan jaringan-jaringan sistem komputer lawan atau merusak. *Cyberdeffense* dari suatu negara lawan

2. *Defense*

   *defense* yang dimaksud adalah pengukuran dari kemampuan suatu negara guna beraksi dalam suatu serangan *cyber*, dimana aksinya tersebut dapat memberikan pertahanan dan mengurangi serangan-serangan dari *cyber* lawan.

[9] Sigit, "Mengukur Kekuatan Cyberwarfare Negara", hlm.1-3.

3. *Dependence.*

Sedangkan *dependence* adalah suatu tingkat ketergantungan terhadap jaringan dan sistem yang dapat dengan mudah diserang oleh *cyber*.

Dengan menggunakan tiga faktor *(offense, defense, dependence)* Clarke mencoba untuk memberikan ilustrasinya tentang bagaimana faktor-faktor tersebut berinteraksi. Ilustrasi dapat dilihat di tabel 1, dimana khusus untuk *dependence* semakin sedikit jaringan di negara tersebut maka akan di beri bobot nilai yang tinggi sedangkan untuk *offense* dan *defense* semakin tinggi nilainya berarti negara tersebut memiliki kemampuan dalam kedua faktor tersebut.

Tabel 2.1 Kekuatan *Cyberwarfare* 5 Negara

| Nation | Cyber Offense | Cyber Dependece | Cyber Defense | Total |
|---|---|---|---|---|
| US | 8 | 2 | 1 | 11 |
| Russia | 7 | 5 | 4 | 16 |
| China | 5 | 4 | 6 | 15 |
| Iran | 4 | 5 | 3 | 12 |
| Nort Korea | 2 | 9 | 7 | 18 |

*(Sumber Richard A. Clarke. 2010. Cyber War The Next Threat To National Security and What To Do About It. NY: Harper Collin Publisher)*

Dari tabel di atas dapat diketahui seberapa besar kekuatan negara dalam menghadapi *cyberwarfare*. Hasil pengukuran di atas menunjukkan bahwa China mempunyai nilai defense yang tinggi, karena mempunyai perencanaan dan kemampuan untuk memutuskan hubungan jaringan ke seluruh negerinya dengan

melalui *cyberspace.* Hal tersebut bertolak belakang dengan AS yang tidak mempunyai baik merencanakan maupun kemampuan untuk memutuskan koneksi jaringan karena koneksi jaringan yang ada di AS rata-rata di operasikan dan dimiliki oleh perseorangan (swasta).

Bila kita melihat Korea Utara, maka negara ini memiliki nilai yang tinggi untuk *defense* dan *dependence*, hal ini dikarenakan Korea Utara dapat memutuskan koneksinya yang terbatas ke *cyberspace* lebih mudah dan efektif dibanding dengan China dengan alasan bahwa Korea Utara mempunyai ketergantungan terhadap sistem yang kecil dan apabila ada serangan *cyber* terhadap negara tersebut tidak akan menimbulkan kerusakan yang berarti.

AS sendiri dalam tabel di atas memiliki kesenjangan nilai yang besar dalam *offense* dan *defense* sehingga dapat disimpulkan bahwa negara besar tersebut dapat melakukan serangan-serangan yang mematikan dan merusakan terhadap negara lawannya melalui *cyberattack*, namun AS juga memiliki kerentanan dan kerawanan yang sangat besar terhadap. Serangan *cyber* lawan-lawannya. Hal tersebut dikarenakan kemampuan *cyberdefense* yang dimiliki AS sangat kecil dan memiliki ketergantungan terhadap sistem jaringan yang besar. Oleh karenanya, pemerintah AS memiliki perhatian yang sangat besar terhadap keamanan cyber negaranya untuk dapat survive dari serangan-serangan cyber lawan-lawannya, baik yang dilakukan oleh perseorangan, aktor non-negara maupun adanya sabotase yang berasal dari kalangan dalam.

## C. Potensi Konflik Ruang Siber

*Cyberspaces* kini telah menjelma menjadi ranah potensial untuk di jadikan medan pertempuran dan konflik tradisional maupun khusus. Bukan hanya pihak yang mewakili nama suatu negara namun juga kelompok masyarakat lainnya yang saling berseteru. Mereka saling berhadapan melalui ajang perdebatan, adu argumentasi, penyebaran upaya dominasi informasi hingga kegiatan yang bersifat destruktif seperti *web defacing rally* sebagai cara propaganda dan intimidasi atau yang lebih berat lagi.

Perseteruan ini tidak hanya melibatkan pelaku amatir tapi juga mereka yang punya keterampilan dan kemampuan khusus bahkan banyak kelompok profesional yang menawarkan jasa layaknya tentara bayaran. Mereka mereka yang menawarkan jasa tersebut dapat dijumpai di web dalam atau biasa disebut *deepweb,* suatu space web yang bebas dan tidak terdeteksi oleh *searchengine*.

Salah satu perang *cyber* yang menarik perhatian dunia adalah serangan yang dilakukan Rusia terhadap Estonia pada 10 Mei 2007. Serangan *cyber* Rusia telah melumpuhkan jaringan keuangan, situs presiden, perdana menteri, parlemen, partai politik, perusahaan, hingga situs berita. Lembaga pemantau trafik mencatat, salah satu dari 10 jaringan internet Estonia yang diserang *hacker* Rusia, kebanjiran trafik data sebesar 90 megabit per detik selama satu jam. Perang *cyber* antara Rusia dan Estonia itu dilihat banyak pakar sebagai perang *cyber* pertama dengan efek dan kerugian terburuk. Padahal, Estonia adalah negara dengan infrastruktur internet terbaik kedua setelah Korea Selatan.

Perang *cyber* Rusia-Estonia itu dipicu sengketa dan konflik politik di dunia nyata. Estonia yang belum lama merdeka dari Uni Soviet, ingin melepaskan diri dari segala atribut Soviet. Mereka berencana memindahkan patung perunggu tentara Soviet dari pusat kota Talinn. Hal itu ditentang banyak warga Estonia keturunan Rusia. Mereka protes di jalan-jalan, lalu berujung rusuh. Pemerintah Rusia berang dan konflik itu pun tak bisa dihindari, berlanjut ke dunia maya.

Kasus yang diduga serangan *cyber* juga terjadi di pangkalan misil Alghadir di Bid Ganeh, barat Teheran, Iran pada 12 November 2011. Sebuah ledakan dahsyat yang terasa hingga 30 mil jauhnya menewaskan 17 anggota pasukan elit Iran. Iran adalah salah satu negara yang kerap menjadi sasaran serangan *cyber* Israel yang mendapat dukungan penuh Amerika Serikat, khususnya terkait upaya Iran memperkaya uranium, salah satu komponen utama nuklir.

Sebelumnya, pada tahun 2009 pernah terjadi serangan *malware* Stuxnet pada instalasi pengayaan nuklir Iran di Natanz. Stuxnet mampu merusak atau menghancurkan *sentrifuse* untuk memproduksi bahan bakar uranium. Hal itu diperkuat dengan pengakuan mantan kepala staf *Israel Defense Forces* (IDF) bahwa Stuxnet merupakan salah satu keberhasilan utama dia saat memimpin lembaga itu).

Melihat berbagai kasus di atas, sepertinya perang *cyber* sudah menjadi bagian penting dari perang modern. Akar permasalahannya, umumnya dipicu disharmonisasi komunikasi antarnegara. Dalam konteks yang lebih luas, dapat dilihat bahwa saat ini perang *cyber* sudah menjadi ancaman serius di tengah upaya membangun dan mempertahankan tatanan dunia baru pasca Perang Dunia II.

Maka ketika banyak negara terus mengembangkan teknologi elektromagnetik dan teknologi informasi dan komunikasi, maka perangkat untuk melakukan perang *cyber* semakin mutakhir. Sehingga prediksi bahwa perang dunia maya sebagai ancaman terbesar di masa depan bukan khayalan belaka. Apalagi akhir-akhir ini mulai terjadi "perang" hegemoni antara Barat (AS dan NATO) dengan Timur (China, Rusia, Korut).

## D. Ancaman Munculnya Terorisme *Cyber*[10]

Pemerintahan AS telah menyatakan keprihatinan bahwa berbagai kelompok subnasional akan mulai melakukan serangan *cyber* melawan Amerika Serikat. Potensi lawan untuk mencoba menghindari konfrontasi langsung dengan militer AS dapat dilakukan dengan menyerang Amerika melalui media dunia maya. Bahkan, ada sejumlah besar pelaku yang berpotensi melakukan serangan *cyber* terhadap Amerika Serikat. Akibatnya, AS khawatir bahwa kelompok-kelompok yang bermusuhan atau negara nakal akan memperoleh kemampuan untuk melakukan serangan cyber terhadap Pemerintah AS.

Cyber-terorisme didefinisikan sebagai, penggunaan alat-alat jaringan komputer untuk menutup infrastruktur kritis nasional seperti sumber energi, transportasi, operasi pemerintah atau untuk memaksa atau mengintimidasi pemerintah atau penduduk sipil. Kelompok yang bermusuhan bisa berpotensi membajak jaringan komputer untuk mengganggu atau mematikan fungsi penting.

---

[10] Nathalie Caplan, *"Cyber War: The Challenge To National Security",* Dalam *Global Security Studies*, Vol.IV i*ssue* I, *Winter* 2013,Hlm.101-102.

Saat ini, kelompok dunia maya dari seluruh dunia telah membentuk aliansi. Meskipun ada beberapa insiden kecil yang dilaporkan sejak tahun 1990 belum ada serangan teroris terhadap infrastruktur dari dunia maya yang dilakukan terhadap Amerika Serikat.

Meskipun tidak bertujuan untuk mematikan infrastruktur nasional yang kritis, banyak orang menganggap operasi WikiLeaks pada tahun 2010 sebagai tindakan terorisme *cyber*. Serangan, yang menerbitkan ratusan ribu dokumen pemerintah AS telah melemahkan Amerika Serikat dengan mengekspos rahasia pemerintah. Bahkan, pada bulan Desember 2010, lebih dari 800.000 dokumen AS yang dipublikasikan.

Hal yang mengkhawatarikan ialah informasi rahasia pemerintah mengenai perang di Irak dan Afghanistan ikut terpublish. Selain itu, lebih dari 250.000 jaringan rahasia diplomatik yang dicuri dari catatan Departemen Luar Negeri. Di antara informasi yang diperoleh termasuk diskusi tentang AS tidak mampu untuk menghentikan senjata Suriah untuk Hizbullah, kekecewaan di Qatar untuk menghentikan pendanaan terorisme dan pembajakan komputer pemerintah AS dengan China.

Menanggapi insiden tersebut, pemerintahan Obama membahas tentang pembajakan, dengan alasan bahwa menempatkan serangan "yang tak terhitung jumlahnya" berisiko hidup, memundurkan upaya-upaya kontraterorisme global, dan terancamnya hubungan AS dengan sekutunya. Demikian pula, Robert Gibbs, sekretaris pers presiden Obama, menyatakan: "ini dapat membahayakan diskusi pribadi dengan pemerintah asing dan pemimpin oposisi, dan jika substansi percakapan pribadi dicetak di halaman depan surat kabar di seluruh dunia, sangat

dapat berdampak tidak hanya kepentingan kebijakan luar negeri, tetapi mereka sekutu dan mitra kami di seluruh dunia.

Unsur yang paling mengkhawatirkan dari serangan WikiLeaks adalah respon pemerintah AS. Para pejabat AS telah mengetahui sebelumnya tentang serangan, namun, Amerika Serikat tidak cukup berdaya terhadap mereka. Dengan kerusakan yang telah dilakukan, perwakilan pentagon Bryan Whitman merilis sebuah pernyataan, meyakinkan masyarakat bahwa pentagon mengambil langkah-langkah tambahan untuk mencegah kompromi lebih lanjut dari data sensitif. Selain itu, disarankan bahwa Departemen Pertahanan mencegah komputer untuk dapat menyalin data ke removable media, membatasi platform untuk memindahkan data dari baris ke sistem unclassified, menciptakan sistem penanganan dua orang dan mengembangkan pemantauan perilaku yang mencurigakan yang mirip dengan sistem pencegahan penipuan kartu bantuan kredit.