BAB II

DEFINISI DAN PERKEMBANGAN SERTA KEAMANAN DAN ANCAMAN CYBER

Pada bab ini, penulis akan memaparkan definisi dan perkembangan cyber dari awal mula tercipta hingga masa kini. Selain itu, keamanan dan ancaman cyber juga akan dijabarkan sejelas mungkin.

Terdapat beberapa sistem yang dirancang untuk menangkal serangan komputer ataupun cyber. Juga berbagai macam jenis malware atau software yang terus dikembangkan guna membobol sistem keamanan akan coba dipaparkan.

A. Definisi dan Perkembangan Cyber

Cyber merupakan kata yang berasal dari bahasa Yunani, yaitu kybernetes yang berarti Gubernur dan di era sekarang digunakan untuk mendeskripsikan benda, orang ataupun ide sebagai bagian dari internet di era informatika.[45]

Cyber merupakan domain yang memiliki karakteristik ditinjau dari penggunaan spektrum elektromagnetik dan elektronik untuk mengubah, menyimpan dan mengganti data melalui sistem jaringan dan infrastruktur fisik yang telah terhubung.[46]

Dunia cyber merupakan metafora yang diciptakan oleh William Gibson dalam novelnya dan digunakan untuk mendeskripsikan wilayah non-

[45] Darwin, "cyber space", dalam http://askville.amazon.com/word-cyber-older-modern meaning/AnswerViewer.do?requestId=4086267, Diakses pada tanggal 21 November 2014.
[46] Margaret Rouse, "cyberspace", dalam http://searchsoa.techtarget.com/definition/cyberspace, Diakses pada 7 Januari 2015.

fisik yang diciptakan oleh sistem komputer melalui sistem online yang memungkinkan orang untuk berkomunikasi dengan orang lain, melakukan penelitian atau berbelanja.[47] Dunia cyber sama seperti dunia nyata, sama-sama memiliki objects, seperti surat, pesan dan grafik dan memiliki metode pengiriman objek tersebut dengan cara yang sama sekali berbeda, cukup dengan menekan tombol di keyboard.

Semenjak pertengahan tahun 1950an, pemerintahan maupun perusahaan melahirkan departemen Electronic Data Processing (EDP) untuk mempercepat dan membuat tugas secara otomatis.[48] Kejadian tersebut menjadi langkah awal lahirnya komputer, meski masih memiliki banyak kekurangan, terutama dibidang pemograman yang masih sederhana dan kerusakan elektro mekanik. Pertumbuhan komputer pada tahun 1970an terjadi secara signifikan. Dimana harga software dan hardware menjadi lebih murah, serta teknologi komputer yang semakin baik. Lubang yang sangat jelas adalah karena orang memiliki akses masuk ke komputer dan input data yang dapat memicu terjadinya pencurian data dan penipuan.[49]

Perkembangan komputer memicu pengembangan operating sistem seperti MULTICS yang memungkin adanya banyak pengguna dan proses pada komputer, yang menjadi pondasi awal terciptanya password untuk

---

[47] Vangie Beal, "cyberspace", dalam http://www.webopedia.com/TERM/C/cyberspace.html, diakses pada 7 Januari 2015.
[48] Peter Sommer dan Ian Brown, "Reducing Systemic Cybersecurity Risk", Makalah disajikan dalam *OECD study into Future Global Shocks*, OECD (United Kingdom: Oxford University, January 2011), Hal. 9.
[49] Ibid, hal. 15.

sebuah akun individu.[50] Password sendiri menjadi jaminan akan keselamatan data bagi penggunanya.

Di era akhir 1970an hingga awal 1980an, komputer marak digunakan untuk membuat laporan dan menganalisis kebutuhan pelanggan, perputaran uang dan proses produksi serta kemunculan jaringan data yang dioperasikan melalui komputer raksasa dan perusahaan telekomunikasi.[51] Para pelanggan mulai melakukan bisnis berbasis jaringan yang memungkinkan terjadinya pertukaran data dan pesan. Diadaptasi pertama kali oleh perusahaan penyedia layanan keuangan dan kemudian sukses besar melalui Society for Worldwide Interbank Financial Telecommunication (SWIFT) ditahun pertama beroperasi pada 1977.

Di akhir tahun 1980an, personal computer mulai marak dimiliki orang-orang, dan memiliki sambungan untuk modem sehingga dapat melakukan komunikasi eksternal.[52] Karena semakin banyak orang-orang yang memiliki komputer, kasus eksploitasi jaringan internet oleh perorangan mulai muncul hanya dengan bermotifkan untuk kesenangan. Metodenya adalah dengan penyebaran malware melalui disket.[53]

Pengembangan internet sangat lamban awalnya, bermula dari akhir 1960an hingga akhir 1980an, yang merupakan jaringan penelitian penghubung universitas dengan pemerintah.[54] Pengembangan World Wide Web pada awal 1990 menambah pengguna non-akademisi, dan pada 1995

[50] Ibid.
[51] Ibid.
[52] Ibid, hal. 16.
[53] Ibid..
[54] Ibid, hal. 17.

internet mulai dikomersilkan hingga pada tahun berikutnya sekitar 15 juta komputer terhubung dengan internet.[55] Perkembangan internet yang cepat dan luas membuat resiko tindakan kriminal pun semakin meningkat.

Dan di era globalisasi, penggunaan internet menjadi semakin marak. Hampir semua kalangan dari berbagai rentang usia memanfaatkan internet. Yang sedang menjadi tren adalah penyimpanan file disebuah cloud.

Istilah cloud computing pertama kali terdengar ketika IBM dan Google membuat proyek bersama pada kuartal keempat tahun 2007.[56] The National Institute of Standards and Technology (NIST) mendefinisikan cloud computing sebagai model yang menyediakan akses jaringan ke konfigurasi komputer, seperti penyimpanan, jaringan, server dan pelayanan yang dapat diunggah dan dirilis secara cepat melalui pengelolaan dan interaksi dengan penyedia layanan seminimal mungkin.[57]

Terdapat empat jenis cloud, yaitu publik, pribadi, campuran dan komunitas. Publik, pengelolaan cloud seperti data applikasi, penyimpanan dan computing dilakukan oleh organisasi yang bukan merupakan pengguna. Dapat diakses melalui internet, gratis dan data pengguna dapat tersebar kebeberapa wilayah didunia. Contohnya instagram, facebook, dll. Selanjutnya, cloud tipe pribadi. Tipe ini sangat bertolak belakang dengan tipe publik, dimana pelanggan tidak dikenakan biaya dan kerahasiaan data

---

[55] Ibid.

[56] Abilio Cardoso dan Paulo Simoes, "Cloud Computing and Security", dalam Eric Filiol and Robert Erra (Ed.), Proceedings of the 11th European Conference on Information Warfare and Security, (United Kingdom: Academic Publishing International Limited., 2012), Hal. 33.

[57] Ibid.

pelanggan merupakan suatu jaminan. Contonya adalah icloud dan Google drive. Cloud versi campuran menggabungkan antara cloud publik dan pribadi. Yang mana kerahasiaan data terjaga namun ditarik biaya. Sedang cloud komunitas membuat komunitas yang menjadi pelanggan memiliki kuasa penuh untuk mengelola cloud dan membuat kerahasiaan data komunitas tetap terjaga. Contonya adalah negara yang membuat cloud untuk menyimpan data-data rahasia.

Secara keseluruhan, pengelolaan sistem cloud dilakukan oleh penyedia layanan, misal google, yang membuat ketidaknyamanan karena membuat pelanggan merasa khawatir akan kerahasiaan data.[58]

Information Technology Infrastructure Library (ITIL), diterbitkan oleh Central Communications and Telecommunications Agency (CCTA) dan the Office of Government Commerce (OGC), meneydiakan tata cara serta kerangka bisnis yang meliputi identifikasi, perencanaan, pengiriman dan mendukung pelayanan IT. [59] Dan cloud computing masih belum sepenuhnya tercover oleh ITIL.

Secara garis besar, permasalah cloud computing adalah keamanan, integritas dan privasi.[60] Merupakan sesuatu yang sangat vital untuk tetap menjaga kerahasiaan informasi dan penyediaan layanan IT.

B. Keamanan Cyber

Keamanan cyber, seperti didefinisikan oleh ITU merupakan sekumpulan alat, kebijakan, konsep keamanan, pendekatan manajemen

[58] Ibid, hal. 9.
[59] Ibid, .hal. 12.
[60] Ibid, hal. 9.

beresiko, tindakan, asuransi dan teknologi yang digunakan untuk melindungi lingkungan cyber, asset berharga yang dimiliki oleh pengguna maupun organisasi.[61]

Keamanan cyber kini telah menjadi isu yang sangat penting. Sejalan dengan perkembangan teknologi dan internet, semua elemen, baik negara, organisasi, individu dapat memiliki senjata untuk membobol keamanan suatu instansi pemerintah. Konsekuensi yang didapat adalah, sekarang banyak permasalahan politik maupun militer bersumber dari penyerangan cyber, dan juga pertempuran didunia cyber pun tidak dapat diprediksi kapan datangnya.

Karena resiko yang sangat besar, diciptakanlah program yang dapat mendeteksi dan mencegah virus, malware atau trojan supaya informasi penting tetap aman. Acces control and identity management, Authentication, Malware scanners, Firewalls, Intrusion Detection Systems (IDS), Cryptography, Load Balancing, Penetration Testing.

Acces control and identity management adalah sistem yang menggabung password/username.[62] Permasalahan utama yang dihadapi sistem ini adalah bagaimana mengamankan password, bagaimana mengatur individu yang tidak lagi memiliki izin untuk masuk ke sistem. Semakin banyak pengguna, membuat permintaan sistem akan password yang berbeda meningkat untuk pelayanan yang berbeda

---

[61] Tim Maurer, "Cyber norm emergence at the United Nations–An Analysis of the UN's Activities Regarding Cyber-securitys". Makalah disajikan dalam *Explorations in Cyber International Relations Discussion Paper Series,* (Cambridge: Harvard Kennedy School, 2011), Hal. 8.

[62] Peter Sommer dan Ian Brown, Op. Cit., hal. 36.

Authentication merupakan program yang menggunakan metode PKI (Public Key Infrastruktur). Didasarkan pada kebutuhan untuk mengechek keaslian identitas pengguna dalam sistem komputer, ada semacam persyaratan bagi individu untuk menghubungkan dengan beberapa "identitas digitalnya" untuk kemudian dapat melakukan metode sharing.[63] Contoh lainnya adalah dokumen yang harus melalui tahap authentication, untuk mengetahui bahwa dokumen tersebut berasal dari sumber yang terpercaya dan tidak diubah-ubah.

Malware scanners merupakan software yang rutin melakukan check pada file dan pesan yang terkandung "malicious code" yang dapat berjalan pada hardware melalui trafik komunikasi yang rutenya telah dipetakan.[64] Software ini memiliki database yang besar mengenai virus, Trojan dan malware dan rutin melakukan update setiap harinya dan lemah terhadap malware Zero-day exploit yang susah untuk dideteksi sehingga mudah tersebar.

Firewalls merupakan program yang membatasi pengguna mengakses internet melalui komputer.[65] Program ini akan melakukan monitor atas trafik data yang masuk dan keluar dari komputer dan mengingatkan pengguna akan penggunaan internet yang tidak aman. Firewall biasanya rutin melakukan update setiap hari, dan jika komputer yang tidak dipasang firewall akan menjadi sangat rentan mengalami penyerangan dari virus, Trojan dan terutama malware.

---

[63] Ibid, hal. 37.
[64] Ibid.
[65] Ibid.

Intrusion Detection Systems (IDS) merupakan program yang memonitor aktivitas secara perlahan yang berujung pada gangguan tidak diinginkan ketimbang mengklain telah adanya penyusup, seperti virus atau malware sebagai penyebab gangguan.[66] Masalah utama dalam program ini adalah menetapkan peringatan atas batas yang tidak boleh dilewati pengguna dalam aktivitas berinternet. Peringatan yang sifatnya terlalu sensitif dapat membuat program melaporkan kejadian false positif atau false negatif, berujung pada laporan IDS yang aman tapi sebenarnya tidak.

Cryptography digunakan pada dua arah utama keamanan, dengan menyediakan enkripsi data yang tersimpan dan transit.[67] Masalah pada sistem program ini adalah kunci manajemen, bagaimana memberikan kebebasan pada pengguna untuk melakukan dekripsi informasi. Serta semakin banyak yang menyimpan informasi yang telah terenkripsi semakin banyak masalah yang ditimbulkan. Kunci Cryptography merupakan solusi yang membuat mungkinnya dilakukan pengembangan sistem untuk proses autentikasi dan identifikasi dokumen, mesin dan individu.

Load Balancing berfungsi untuk mendistribusikan beban kerja diantara beberapa komputer secara dinamis.[68] Di tingkat penggunaan normal, kerjanya adalah untuk mengoptimisasi kemampuan komputer. Load balancing juga dapat digunakan untuk keamanan, terutama untuk melindungi website dan sejenisnya yang sedang diserang DDoS. Juga Program ini dapat

[66] Ibid, hal. 38.
[67] Ibid.
[68] Ibid.

digunakan dibidang telekomunikasi untuk mengatasi kerusakan kabel dan pusat perpindahan.

Penetration Testing bekerja dalam aturan yang ketat, memastikan bahwa sistem aman dan tidak terjadi sesuatu yang tidak diinginkan.[69] Hal ini didasarkan pada sistem informasi modern yang begitu kompleks dan rapuh dikarenakan perubahan yang sangat cepat. Sistem ini banyak digunakan oleh pemerintah disektor komersial.

C. Ancaman Cyber

Di era teknologi dan informatika seperti sekarang ini, infrastruktur penting pemerintah tersambung dengan komputer dan internet, sehingga membuat negara sangat rawan akan serangan cyber. Alasannya karena kemudahan mengelola infrastruktur jika terhubung dengan komputer dan internet. Meski negara telah menggelontorkan dana yang sangat besar untuk membeli software pengamanan dari pengembang, sepertinya hasilnya akan tetap nihil karena pengembangan virus yang digunakan untuk aksi serangan cyber selangkah lebih maju.

Terdapat beberapa ancaman pada komputer. Anatara lain adalah malware, senjata ampuh untuk melakukan penyerangan cyber. Generasi pertama malware adalah logic bomb yang muncul ke permukaan pada era 1960an yang dapat membuat komputer mati dengan sendirinya ataupun memicu hal-hal yang dapat berujung pada kasus penipuan.[70] Kasus yang

[69] Ibid, hal. 39.
[70] Ibid, hal. 24.

pernah terjadi adalah ledakan pipa trans-siberia pada 1982 dan percobaan penghapusan data di roket di General Dynamics pada 1992.

.Trojan Horse dapat membuat lubang pada akses internet yang nantinya memungkinkan untuk dilakukannya penghapusan dan pencurian data, memonitor pengguna komputer bahkan mengendalikan komputer korban untuk melakukan aksi kejahatan yang sulit dilacak.[71] Virus, merupakan program yang dapat menggandakan diri yang biasanya mengandung Trojan Horse atau Logic Bomb, biasa digunakan untuk merusak sistem komputer, membobol e-mail, membuat celah dan menghilangkan data-data.[72]

Keylogger juga ancaman yang terbilang serius yang dapat merekam dan memonitor ketikan pada komputer, utamanya untuk mencuri password.[73] Root-kit awalnya merupakan program yang mengendalikan komputer secara total dan kini merupakan malware yang tersembunyi disistem operasi dan sangat susah untuk dideteksi serta berisi virus.[74]

Serangan DDoS (Denial of Service attack) membanjiri sistem yang terhubung dengan internet dan jaringan dengan trafik jaringan berjumlah besar kemudian mengambil alih komputer target untuk melakukan aksi penyerangan.[75] Pengambil alihan komputer dilakukan melalui e-mail atau malware berbasis website. Komputer yang berhasil direbut dapat dikendalikan dari mana saja.

---

[71] Ibid, hal. 24.
[72] Ibid, hal. 25.
[73] Ibid.
[74] Ibid.
[75] Ibid.

Zero-day exploits/attack memanfaatkan celah yang dilakukan secara bertahap pada percobaan atau lembaran penelitian dan menyebar secara perlahan melalui jaringan internet dan komputer.[76] Program yang melacak virus, seperti firewall masih mungkin untuk melacak dan memblok aktivitas penyebaran virus ini.

Malware yang secara sengaja ditanam oleh pengembang software keamanan juga penanaman chip yang dapat menyebabkan kerusakan perlu diwaspadai. Cara kerjanya dengan memanfaatkan celah yang ada disistem operasi yang terpasang di berbagai sektor. Sistem berbasis Windows yang terpasang di ATM bank dan sistem tiket pada transportasi, Linux yang digunakan pada pemutar musik dan internet router dan kasus meledaknya pipa trans-siberia yang diduga karena AS telah menanamkan chip yang salah pada perlengkapan yang dibeli Russia.[77]

Metode lain yang digunakan oleh para hacker adalah botnet. Penyedia sistem keamanan cyber biasanya tidak menyadari bahwa sistem yang mereka kembangkan telah terinfeksi malware bertipe bot yang menyebabkan pengguna komputer yang terhubung dengan internet terjebak dalam botnet.[78]

Bots tersebar diseluruh dunia, sebagian besar server kendali dan perintah berasal dari AS dan China dan menyerang infrastruktur yang

---

[76] Ibid.
[77] Ibid.
[78] Ibid.

memiliki bandwith, terhindar dari pembatasan jaringan dan menyamarkan lokasi pelaku[79].

Para hacker dapat menggunakan berbagai cara untuk menjalankan misinya, salah satunya dengan botnets untuk melakukan aksi penyerangan ke pasar global dengan cukup mengeluarkan biaya yang sangat murah. Botnet selain dapat dibeli secara murah seharga $0.04 juga dapat "disewakan".[80] Cara kerja botnet adalah dengan bersembunyi didalam milyaran komputer, dan kemudian komputer yang menjadi korban dapat digunakan untuk melakukan penyerangan.

Selama ini, keamanan cyber selalu lekat dengan perangkat komputer. Belakangan, keamanan cyber dibidang transportasi dan peralatan rumah tangga menjadi perbicangan hangat. Yang menjadikan bidang otomotif elektrik rawan terhadap serangan cyber karena kendaraan memiliki MCU (Micro Controller Unit) dan beberapa perangkat software. Juga kendaraan elektrik terpasang sistem operasi yang memiliki banyak celah, seperti Windows, Linux, GENIVI, AUTOSAR, dll.

Kendaraan elektrik menggunakan perangkat wireless yang digunakan untuk berkomunikasi, seperti melakukan panggilan darurat, melakukan panggilan layanan, dll. Selain memanfaatkan wireless, mobil elektrik juga terhubung dengan gadget, seperti smartphone, music player, sistem GPS portable. Melalui video atau musik yang terdownload, virus merasuk

---

[79] Ibid, Hal. 26.

[80] Peter Dombrowski dan Chris C. Demchak, "Cyber War, Cybered Conflict, And The Maritime Domain", Journal of Naval War College Review, Spring 2014, Vol. 67, No. 2, Hal. 83.

perangkat seperti smartphones dan pemutar musik portable yang terhubung kekendaraan, barulah kemudian masuk ke mobil elektrik.

Kesulitan yang dialami dalam menanggulangi permasalahan keamanan cyber dalam kendaraan adalah minimnya koneksi, rendahnya performa perangkat komputer, sulitnya dalam melakukan monitoring kendaraan dan resiko keselamatan bagi pengendara atau penumpang.[81] Bagian mobil yang harus mendapatkan perlindungan adalah setir dan rem, karena berkaitan dengan keselamatan pengendara.

Penyebab utama munculnya berbagai ancaman dalam dunia cyber, yaitu berkaitan dengan kelemahan dalam konsep internet, ketergatungan untuk memindahkan barang atau informasi penting ke internet dan kelemahan yang terdapat pada hardware dan juga software.[82]

Menurut profesor Harvard, Joseph Nye, ada empat ancaman utama terhadap keamanan cyber, yaitu cyber espionage, perang cyber, kriminal cyber dan terorisme cyber.[83]

1. Kriminal Cyber

Praktek kriminal cyber menggunakan media komputer untuk mencuri data untuk kemudian di perjual belikan, biasanya motif yang melandasi tindakan memata-matai adalah semata-mata faktor ekonomi.[84] Biasanya,

---

[81] Hiro Onishi, "Paradigm Change of Vehicle Cyber Security", dalam 2 C. Czosseck, R. Ottis, K. Ziolkowski (Ed.), *4th International Conference on Cyber Conflict*, (Talinn: Nato, 2012), hal. 383.
[82] Tim Maurer, Op. Cit., hal. 27.
[83] Ibid, hal. 34.
[84] Kenneth Geers, *Strategic Cyber Security*. (Estonia: Nato Cooperative Cyber Defence Centre Of Excellence, 2011).

korban kejahatan ini merupakan individu atau organisasi. Kerugian yang diderita korban kriminalitas cyber tidak dapat dihitung secara pasti, tetapi kerugian yang diderita sangatlah besar. Perusahaan yang menjadi korban kriminal cyber, cenderung enggan untuk melaporkan besaran kerugian yang didapatnya, berdasar pada alasan bahwa hal tersebut dapat membuat publik atau investor berkurang kepercayaannya.

Kerugian dalam hal berkurangnya pelanggan dan biaya oportunis suatu instansi yang menjadi korban juga sulit untuk diperkirakan. Namun Mc Afee mengestimasikan kerugian yang diderita oleh ekonomi global karena tindak krimial cyber sepanjang tahun 2008 berupa kekayaan intelektual sebesar $1 milyar.[85] Akan tetapi kerugian yang terlampau banyak tersebut dipandang sebagian orang sebagai hal yang wajar, karena dalam berbisnis kerugian dapat dialami sewaktu-waktu dan jumlahnya yang tidak dapat diperkirakan. Tren kriminal cyber belakangan ini cenderung meningkat tajam. Di dasarkan pada perkembangan teknologi yang kian pesat.

Modus kriminal cyber biasanya menggunakan metode pembuatan akun palsu di jaringan internet untuk meraih informasi-informasi sensitif.[86] Cara tersebut hingga kini terbilang efektif dan masih sering digunakan.

Serangan cyber yang dilakukan Jonathan James alias "cOmrade" pada tahun 2000 membuat AS merugi $10.000 karena informasi berharga yang ada

---

[85] Robert E. Kahn, dkk, "America's Cyber Future: Security And Prosperity In The Information Age", dalam Kristin M Lord And Travis Sharp (Ed.), (United States:Center For American New Security,2011), hal. 17.

[86] Ibid.

disistem komputer NASA dan DoD berhasil dicuri.[87] Tidak hanya itu, sistem yang dijebolnya memerlukan waktu yang terbilang lama untuk memulihkan diri paska diserang. Meski begitu, tidak ada korban jiwa dalam peristiwa tersebut.

2. Spionase Cyber

Awal mula terjadinya penggunaan internet dan komputer untuk mendapatkan data-data militer terjadi pada tahun 1980-an di Uni Soviet yang dilakukan oleh MTR, Military Technology Revilutionary.[88] Penyerangan berbasis cyber biasanya digunakan untuk memata-matai negara lain, untuk mengacak-acak pelayanan publik hingga penghancuran infrastruktur penting suatu negara.

Seperti halnya krimimal cyber, mata-mata cyber atau cyber espionage juga terjadi diseluruh belahan dunia. Salah satu contoh betapa mengerikannya aktifitas cyber espionage, adalah ketika peneliti asal Kanada memecahkan cara kerja Ghostnet. Ghostnet menginfeksi sekitar 1295 komputer yang mentargetkan foreign affairs ministries, kedutaan dan organisasi multilateral yang terletak di Iran, India, Korea Selatan, Jerman dan banyak lagi.[89]

Melalui Ghostnet, hacker dapat mengaktifkan kamera yang terdapat pada komputer dan sistem suara pada komputer berbasis sistem operasi

---

[87] Jenna Miller, "Jonathan James (a.k.a c0mrade), dalam https://prezi.com/fnkysftgwq1y/jonathan-james-aka-comrade, di akses pada tanggal 9 Januari 2015.

[88] Kenneth Geers, Op. Cit., hal. 9.

[89] Ron Deibert Dan Rafal Rohozinski, "Shadows In The Cloud: Investigating Cyber Espionage 2.0". Ottawa: The Secdev Group, hal. 2.

Windows yang telah terinfeksi, yang dapat dimanfaatkan untuk melakukan aktifitas mata-mata kepada pengguana komputer.

Aksi yang pernah dilakukan Kevin Poulsen menunjukkan bahwa spionase cyber merupakan tindakan yang sangat berbahaya. Ketika ia berhasil menembus sistem jaringan angkatan udara AS, Air Force dan mencuri data-data penting. Meski tidak diketahui, secara pasti untuk apa data yang dicurinya.[90]

3. Terorisme Cyber

Terorisme cyber merupakan perpaduan antara terorisme dan cyber. Terorisme cyber merupakan aksi penyerangan yang melanggar hukum cyber dan mengancam komputer, jaringan pertahanan dan informasi, baik perseorangan atau organisasi pemerintah. Supaya dapat disebut sebagai terorisme cyber, sebuah serangan harus mengakibatkan kekerasan kepada orang atau properti atau membuat rasa takut maupun timbulnya kekhawatiran. Serangan yang mengakibatkan kematian atau setidaknya cedera serius pada jasmani, pesawat yang hancur, ledakan, air yang terkontaminasi atau kerugian besar pada sektor ekonomi merupakan contoh yang shahih.[91]

Penggunaan internet untuk perekrutan anggota oleh organisasi teroris dan juga perluasan informasi mengenai taktik serta perencanaan operasional

---

[90] Jacob Silverman, " The Last Hacker : He Called Himself Dark Dante. His Compulsion Led Him to Secret Files and, Eventually, the Bar of Justice ", dalam http://articles.latimes.com/1993-09-12/magazine/tm-34163_1_kevin-poulsen, diakses pada tanggal 12 Januari 2015.

[91] Sarah Gordon dan Richard Ford, "Cyberterrorism?", Journal of overview of conceptual debate on terrorism more broadly, Vol. 21, No. 7, hal. 4.

juga dapat dikategorikan dalam terorisme cyber.[92] Jadi definisi terorisme cyber tidak hanya berkutat pada penyerangan terhadap informasi semata.

The United States Department of Defense (DOD) mendefinisikan terorisme cyber sebagai penggunaan kekerasan atau kekuatan kepada individual atau properti untuk mendapatkan sesuatau atau mengintimidasi, terutama sektor pemerintahan dan masyarakat demi untuk kepentingan politik, agama ataupun secara ideologi.[93]

Salah satu contoh dari terorisme cyber adalah fasilitas yang terdapat di Iran dihajar oleh Stuxnet melalui malware yang ditanamkan didalam komputer meski Stuxnet sendiri tidak terhubung secara langsung dengan internet. Kasus yang sama juga kerap terjadi pada jaringan pertahanan AS, komputer terinfeksi virus ketika ditancapkan flash disk yang ditemukan dijalan. Aksi tersebut diduga didalangi oleh organisasi intelijen asing.[94]

4. Perang Cyber

Perang cyber dapat terjadi kebanyakan karena dilandasi oleh kepentigan ekonomi ataupun politik, dan menggunakan operasi militer didunia cyber. Perang cyber dapat terjadi antara pihak pemerintah suatu negara ataupun komunitas biasa. Perang cyber biasa terjadi karena konflik didunia maya atau kelanjutan dari perang didunia nyata yang melibatkan angkatan militer didarat, laut ataupun udara. Namun, kenyataannya adalah perang cyber masih belum benar-benar terjadi. Hanya aksi saling serang

---

[92] Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations". (Brookings: 21st Century Defense Initiative., 2012), hal. 8.
[93] Sarah Gordon dan Richard Ford, Op. Cit., hal. 5.
[94] Kenneth Lieberthal dan Peter W. Singer, Op. Cit., hal. 16.

bermotifkan balas dendam atau tidak terima yang melatar belakangi aksi gempur antara AS dengan China.

Efek yang ditimbulkan oleh perang cyber lebih kearah kinetic, dan sampai saat ini belum dapat menimbulkan pertumpahan darah atau kehancuran yang masif berhubungan dengan perang sesungguhnya. Penyerangan didunia cyber masih belum memakan korban jiwa, hanya saja serangan cyber dapat menyebabkan perusakan pada program atau mengubah program yang dapat menyebabkan orang kehilangan nyawa.

Kerusakan atau kerugian yang terjadi akibat dari aksi serangan cyber dipandang tidak seberapa bila dibandingkan dengna perang cyber. Sama seperti perang didunia nyata yang mengakibtkan banyak kerusakan. Juga perang cyber sama seperti perang didunia nyata yang kondisi kedua pihak yang berperang sama-sama tidak mau mengalah sehingga berpotensi untuk menyebabkan kerugian yang jumlahnya sangat banyak.[95]

Komputer telah lama hadir dalam masyarakat. Dari hanya sekedar untuk keperluan bisnis hingga kini untuk berselancar didunia maya. Pun perkembangan internet yang mulai dikomersilkan pada pertengahan tahun 1990an, yang hanya memiliki puluhan juta pengguna hingga kini milyaran jumlahnya.

Sistem keamanan cyber juga mengalami perkembangan pesat. Bermula hanya sebagai "perisai" bagi komputer menghadang malware atau virus yang masuk melalui disket hingga kini berfungsi sebagai pelindung

[95] Robert E. Kahn, dkk, Op. Cit., hal. 38.

disistem jaringan milik perusahaan atau pemerintah. Serta ancaman cyber yang terdiri dari serangan cyber, spionase cyber, terorisme cyber dan perang cyber, seperti yang telah diungkapkan oleh Joseph Nye.[96] Ancaman cyber tersebut sangat berbahaya karena mengincar infrastruktur penting negara untuk kemudian mencuri data ataupun merusak sistem yang akan membuat negara rugi jutaan dollar. Juga perusahaan merupakan sasaran empuk dari para hacker. Negara pun tidak menganggap remeh ancaman cyber, sehingga dibuatlah organisasi yang langsung mengurusi permasalahan cyber baik dalam maupun luar negeri, karena tidak mau mengalamai kerugian yang diakibatkan oleh serangan cyber.

[96] Tim Maurer, Op. Cit., hal. 8-9.