PERBEDAAN BENTUK KEJAHATAN YANG DIKATEGORIKAN SEBAGAI CYBER CRIME DAN CYBER WARFARE

Indah Sari
indah.alrif@gmail.com
Universitas Dirgantara Marsekal Suryadarma

Abstract

The reason behind this writing is based by the development of technology which plays significant role in daily life. Computer device and internet have become important thing for country's life, enable them to conquer, control, and observe every human movement in other world. Computer device and internet have created a new world called cyberspace. Along with the progress of cyberspace, it also develops many lawbreaking actions that based with computer device and internet, some of them are cyber crime and cyber warfare. From this background, the writer elevates two problem from this case. First, what form of crime that can be categorized as cyber crime and cyber warfare? Second, how to protect ourselves from the threat of cyber crime and cyber warfare? The kind of typing that the writer uses in this research is descriptive research (describing an object and taking simple conclusion from it) with secondary data and use statute approach, case approach, and conceptual approach. This kind of technique is collected by library research and the data will be analyzed qualitatively. As for the study result, it consists of: the writer found many different form between cyber crime and cyber warfare. Example of cyber crime are Unauthorized Access to Computer System and Service, Illegal Contents, Data Forgery, Cyber Espionage, Cyber Sabotage and Extortion, Offence Against Intellectual Property, and Infringements of Privacy, while the example of cyber warfare are spionase cyber, vandalism, sabotage, and power grid hacking. In this report, the writer also explain some tips to defend yourself from the threat of cyber crime and cyber warfare.

Keywords: *internet, cyber space, cyber crime, cyber warfare, crime, law*

PENDAHULUAN

Seiring dengan semakin populer Inter-Net sebagai "*the network of the net-works*", masyarakat penggunanya (*inter global community*) seakan-akan mendapati suatu dunia baru yang dinamakan dengan *cyberspace* sebagaimana di populerkan oleh William Gibson dalam novel sci-finya *"Neuromancer"* yang merupakan kayalan tentang adanya alam alam lain pada saat teknologi telekomunikasi dan informatika bertemu (FH UI *Online*,tt.)

Howard Rheingold menyatakan, *cyber space* adalah sebuah "ruang imajiner" atau "maya" yang bersifat artifisial, dimana setiap orang melakukan apa saja yang bisa dilakukan dalam kehidupan sosial sehari hari dengan cara yang baru (Yasraf Amir Piliang, tt.)

Berkaitan dengan *cyber space* ini Agus Raharjo mengatakan, *cyber space* sesungguhnya merupakan sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Dunia ini menawarkan realitas baru dalam kehidupan manusia yang disebut dengan virtual (maya) (Agus Raharjo, 2002:91)

Realitas atau alam baru yang terbentuk oleh medium internet ini pada perkembangannya menciptakan masyarakat baru sebagai warganya yang dalam istilah pengguna dan pemerhati internet lazim disebut dengan *nitizen.* Pada gilirannya, realitas baru yang terbentuk oleh medium internet ini membawa

perubahan paradigma dalam kehidupan umat manusia. Kehidupan manusia tidak lagi hanya merupakan aktivitas yang bersifat fisik dalam dunia nyata (real) belaka akan tetapi menjangkau juga aktivitas non fisik yang dilakukan secara *virtual.*

Dengan internet, netizen dapat menjelajahi *cyber space* tanpa dapat dihalangi oleh sekat-sekat teritorial negara. Aktivitas apapun yang dilakukan di *cyber space* seakan terlepas dari yurisdiksi nasional suatu negara. Berkaitan dengan ini, Onno W. Purbo menyatakan dalam tulisannya, internet terlihat oleh sebagian besar orang, pengguna, pengamat sosial sebagai dunia tanpa batas, dunia tanpa aturan, dunia kebebasan.

Internet telah membuat manusia-manusia (sebagai pengguna) mampu menjelajah ruang maya ke mana-mana, berkomunikasi dengan beragam informasi global, memasuki jagad perbedaan dan lintas etnis, agama, politik, budaya, dan lain sebagainya. Manusia diajak bercengkrama, berdialog, dan mengasah ketajaman nalar dan psikologisnya dengan alam yang hanya tampak di layar, namun sebenarnya mendeskripsikan realitas kehidupan manusia.

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 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 (Awaludin, 2018). Dengan adanya *cyber space* ini, berkembang juga kejahatan kejahatan dengan menggunakan internet berbasis kecanggihan teknologi komputer diantaranya adalah *cyber crime* dan *cyber warfare.*

Dalam beberapa kepustakaan, *cyber crime* atau kejahatan siber sering diidentikkan sebagai *computer crime.* Menurut the U.S. Department of Justice, *computer crime* adalah "*….any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution"*. Sementara dalam "*background paper*" Kongres PBB X/2000 untuk *"Workshop on crimes related to the computer network"* (doc.A/CONF 187/10, 3-2-2000) memberi batasan *cybercrime* dalam arti sempit (*in the narrow sense)* dan arti luas (*in the broader sense*) c*ybercrime in a narrow sense (computer crime): any legal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them.* Sementara dalam arti luas disebutkan *"…computer related crime is any illegal behavior committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network"*. *Cyber crime* dapat dilakukan lintas batas negara atau dilakukan di dalam satu negara saja. Hal ini yang kemudian membuat hukum siber sebagai dasar hukum *cyber crime* tidak hanya menjadi bagian dari hukum nasional, tetapi juga menjadi bagian hukum internasional.

Motif pelaku kejahatan di dunia maya (*cyber crime)* pada umumnya dapat dikelompokan menjadi dua kategori:

1. Motif intelektual yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukan bahwa dirinya telah mampu untuk merekayasa dan mengimplemetasikan bidang teknologi informasi. Kejahatan dengan motif ini pada umumnya dilakukan oleh seseorang secara individu .
2. Motif ekonomi, politik dan kriminal yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain. Karena memiliki tujuan yang dapat berdampak besar, kejahatan dengan motif ini pada umumnya dilakukan oleh sebuah korporasi.

Sedangkan c*yber warfare* sendiri berkembang dari c*yber 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) *Cyber Crime* 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. *Cyber Crime* merupakan kejahatan transnasional yang membahayakan karena akan mengarah kepada *Cyber Warfare*.

Adapun karakteristik dari *cyber warfare* adalah:

a. subjek : negara atau *hacker-group* (*non-state actor*);
b. objek yang diserang : *cyber system* dan *cyber-infrastructure*
c. metode : *cyber attack* tertentu
d. sarana : *cyber weapon;*
e. motif : mendapat akses terhadap *cyber-infrastructure* negara lawan

Bertolak dari uraian diatas, maka menarik bagi penulis untuk meneliti lebih lanjut batas batas perbedaan antara *cyber crime* dan *cyber warfare* sehingga dapat dirumuskan beberapa permasalahan pokok yang diteliti dan diungkapkan dalam penulisan ini sebagai berikut:

1. Bagaimanakah bentuk-bentuk kejahatan yang dikategorikan sebagai *cyber crime* dan *cyber warfare*?
2. Bagaimana perlindungan-perlindungan yang dilakukan dalam menghadapi ancaman *cyber crime* dan *cyber warfare*?

Adapun tujuan dari penulisan ini adalah: *pertama,* untuk mengkaji dan menganalisis lebih dalam lagi mengenai batasan perbedaan antara *cyber crime* dengan *cyber warfare, kedua,* untuk mengetahui dan menjelaskan sejauh mana bentuk-bentuk perlindungan yang dilakukan dalam menghadapi serangan *cyber crime* dan *cyber warfare* termasuk di dalamnya perlindungan hukum.

Adapun kegunaan dari penulisan ini adalah:

a. Dapat memberikan wawasan dan pengetahuan bagi dosen, mahasiswa, civitas akademika, praktisi hukum, praktisi sistem informasi mengenai batasan perbedaan antara *cyber crime* dan *cyber warfare* kemudian

mencari bagaimana solusi-solusi melakukan perlindungan dari ancaman *cyber crime* dan *cyber warfare* termasuk di dalamya perlindungan hukum.

b. Tulisan ini dapat mendorong penelitian lebih lanjut untuk dapat mengembangkan kajian dan pengetahuan tentang kriteria batasan perbedaan antara *cyber crime* dengan *cyber warfare* serta usaha-usaha apa yang dilakukan dalam memberikan perlindungan dari kejahatan *cyber crime* dan *cyber warfare.*

Dalam penulisan ini penulis memparkan sistematika penulisan sebagai berikut: *pertama,* Pendahuluan yang berisikan latar belakang penulisan, rumusan masalah, tujuan penulisan, kegunaan penulisan serta sistematika penulisan, *kedua,* dimana penulis memaparkan kajian-kajian literatur yang berkaitan dengan *cyber crime* dan *cyber warfare* dan bentuk- bentuk perlindungan apa yang dilakukan dalam menghadapi ancaman *cyber crime* dan *cyber warfare*. *Ketiga,* Metode Penelitian yang berisikan jenis penelitian, pendekatan penelitian, jenis data, teknik pengumpulan data, serta metode analisis data. *Keempat,* Hasil Penelitian dan Pembahasan. Adapun di dalam hasil penelitian dan pembahasan akan di paparkan; bentuk-bentuk *cyber crime,* bentuk-bentuk *cyber warfare*, contoh-contoh kasus dari *cyber crime,* contoh-contoh kasus dari *cyber warfare,* usaha-usaha yang dilakukan dalam memberikan perlindungan dari ancaman *cyber crime* dan *cyber warfare. Kelima*, Simpulan yang akan menjawab dua rumusan permasalahan yang diangkat dalam penulisan ini.

Berdasarkan uraian di atas akhirnya penulis tertarik untuk mengkaji dan mendalami mengenai "**PERBEDAAN BENTUK KEJAHATAN YANG DIKATEGORIKAN SEBAGAI CYBER CRIME DAN CYBER WARFARE**

Pada akhirnya kita akan dapat membedakan kriteria bentuk antara *cyber crime* dan *cyber warfare* serta bagaimana perlindungan-perlindungan yang akan dilakukan ketika menghadapi ancaman *cyber crime* dan *cyber warfare.*

KAJIAN LITERATUR

Internet

Dalam sebuah situs di internet, yaitu *www.MyPersonalLibraryOnline.com* "internet" (*inter-network*) didefinisikan sebagai jaringan komputer yang menghubungkan situs akademik, pemerintahan, komersil, organisasi, maupun perorangan. Dalam definisi ini tampak bahwa internet mencakup juga terhadap jaringan yang biasa disebut dengan LAN (*local area network)* dan WAN (*wide area network*).

Sementara *The US Supreme Court* mendefinisikan internet sebagai internasional *network of interconnected computers,* (Reno V ACLU, 1997 dalam Ari Juliano Gema, 2000) artinya jaringan internasional dari komputer-komputer yang saling berhubungan. Dari definisi ini terlihat dimensi internasionalnya, artinya bahwa jaringan antar komputer tersebut melewati batas batas teritorial suatu Negara.

Agus Raharjo mendefinisikan internet sebagai jaringan komputer antar negara atau antar benua yang berbasis protokol t*ransmission control protocol/ internet protocol* (TCP/IP) (Agus Raharjo, 2002: 59)

Informasi Elektronik dan Transaksi Elektronik

Dalam ketentuan umum pasal 1 Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elek-

tronik bahwa disebutkan pengertian Informasi Elektronik, Transaksi Elektronik dan Dokumen Elektronik:

a. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
b. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Cyber Space

Induk dari *cyber crime* yaitu *cyber space*. *Cyber space* di pandang sebagai sebuah dunia komunikasi yang berbasis komputer. Dalam hal ini *cyber space* dianggap sebagai sebuah realitas baru dalam kehidupan manusia yang dalam sehari-hari dikenal dengan internet. Realitas baru ini dalam kenyataannya terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis protokol *transmission control protocol/internet protocol*. Hal ini berarti, dalam sistem kerjanya dapatlah dikatakan bahwa *cyber space*/internet telah mengubah jarak dan waktu menjadi tidak terbatas.

Kejahatan

Secara empiris definisi kejahatan dapat dilihat dari dua persfektif, *pertama* adalah kejahatan dalam persfektif yuridis, kejahatan di rumuskan sebagai perbuatan yang oleh negara diberi pidana. Pemberian pidana ini dimaksudkan untuk mengembalikan keseimbangan yang terganggu akibat perbuatan itu (B. Simanjuntak, 1981:70). Perbuatan atau kejahatan yang demikian itu dalam ilmu hukum pidana biasa disebut dengan tindak pidana (*straftbaarfeit*). *Kedua*, kejahatan dalam arti (persfektif) sosiologis (kriminologis) merupakan suatu perbuatan yang dari sisi sosiologis merupakan kejahatan sedangkan dari yuridis (hukum posistif) bukan merupakan suatu kejahatan (B.Simanjuntak, 1982:70). Artinya perbuatan tersebut oleh negara tidak dijatuhi pidana. Perbuatan ini dalam ilmu hukum pidana disebut dengan *strafwaardig*, artinya perbuatan tersebut patut atau pantas dipidana. Ini dikarenakan penjatuhan pidana merupakan upaya untuk mengembalikan keseimbangan yang terganggu akibat perbuatan (kejahatan) tersebut.

Batasan kejahatan menurut Bonger adalah perbuatan yang sangat anti sosial yang memperoleh tantangan dengan sadar dari negara berupa pemberian penderitaan (hukuman atau penderitaan). selanjutnya Bonger mengatakan "Kejahatan merupakan sebagian dari perbuatan immoral. Oleh sebab itu maka perbuatan immoral adalah perbuatan anti sosial. Namun demikian haruslah dilihat juga bentuk tingkah lakunya dan masyarakat, sebab perbuatan seseorang tidaklah sama dan suatu perbuatan immoral belum tentu

dapat dihukum" (B. Simandjuntak & I.L. Pasaribu, 1984: 45).

Van Bammelen merumuskan, kejahatan adalah tiap kelakuan yang bersifat tidak susila dan merugikan, dan menimbulkan begitu banyak ketidak tenangan dalam suatu masyarakat tertentu, sehingga masyarakat itu berhak untuk mencelanya dan menyatakan penolakannya atas kelakuan itu dalam bentuk nestapa dengan sengaja diberikan karena kelakuan tersebut (B. Simandjuntak, 1981: 72).

Cyber Crime

Cyber Crime adalah tindak pidana kriminal yang dilakukan pada teknologi internet (*Cyber Space*), baik yang menyerang fasilitas umum maupun kepemilikan pribadi. Secara teknik dapat dibedakan menjadi *offline crime*, *semi online crime*, dan *cyber crime*. Contoh dari *offline crime* adalah dengan cara yang sederhana misal mencuri dompet seseorang untuk kemudian diambil kartu kreditnya, atau bekerjasama dengan kasir untuk mencatat nomor kartu kredit seseorang kemudian menduplikatnya. Contoh teknik *semi online crime* adalah memasang *skimming* di mesin ATM untuk mencuri informasi kartu debit korban. Sedangkan untuk *cyber crime* orang pelaku dan korban tidak perlu bertatap muka, dan bersentuhan, yaitu dengan menggunakan teknologi yang canggih, seperti penggunaan situs palsu klik BCA, dll. Masing-masing teknik memiliki karakter tersendiri, namun perbedaan utama diantara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

Cyber crime dapat 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 Offlenderes* di Havana, Cuba pada Tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal:

1. *Cyber crime* dalam arti sempit disebut *computer crime*, yaitu perilaku illegal/melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses dari komputer.
2. *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu perilaku illegal/melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pengertian di atas, *cyber crime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Cyber Warfare

Perkembangan teknologi informasi dan komunikasi memberi banyak kemudahan dalam menjalankan aktivitas pemerintahan, namun melahirkan ancaman baru yang berdampak bagi kestabilan kedaulatan suatu negara juga, yaitu *cyber warfare*. *Cyber warfare* merupakan perkembangan dari *cyber attack* dan *cyber crime*. *Cyber warfare* dapat diartikan sebagai perang di dalam *cyber space*, namun di dalam *cyber warfare* terdapat penyerangan yang berbeda dengan penyerangan dalam perang konvensional atau perang fisik lainnya. Media utama yang digunakan di dalam *cyber warfare* adalah komputer dan internet. Objek yang diserang dalam *cyber warfare* bukan merupakan wilayah fisik, wilayah territorial ataupun wilayah geografis, namun objek dalam *cyber space* yang dikuasai oleh suatu negara.

Belum ada perjanjian internasional yang menjelaskan secara eksplisit mengenai definisi *cyber warfare*. Hingga saat ini, definisi *cyber warfare* yang digunakan adalah definisi-definisi yang dikemukakan oleh para ahli dan beberapa organ PBB seperti UNTERM dan UNICJRI. Menurut Richard Clarke *cyber warfare* adalah "*actions by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption*". UNTERM mendefinisikan *cyber warfare* sebagai "*the offensive and defensive use of information and informations system to deny, exploit, corrupt or destroy an adversary's computer based network while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries*".

Menurut UNTERM, *cyber warfare* merupakan tindakan militer yang memanfaatkan teknologi untuk merusak/ menghancurkan informasi milik target untuk memperoleh keuntungan militer dan bisnis. Sementara UNICJRI mendefinisikan *cyber warfare* sebagai "*any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some sort of damage*". Definisi yang diberikan oleh UNICJRI memiliki persamaan dengan definisi yang diberikan oleh Richard Clarke, yaitu merupakan tindakan dari aktor negara untuk mempenetrasi jaringan komputer negara lain dengan tujuan menyebabkan beberapa kerusakan.

METODE PENELITIAN

Jenis penelitian (tipologi penelitian) atau metode penelitian yang dipergunakan dalam penelitian ini adalah dilihat dari segi sifatnya, penelitian ini adalah penelitian deskriptif, artinya penelitian yang menggambarkan objek tertentu dan menjelaskan hal-hal yang terkait dengan atau melukiskan secara sistematis fakta-fakta atau karakteristik populasi tertentu dalam bidang tertentu secara faktual dan cermat. Penelitian ini bersifat deskriptif karena penelitian ini semata-mata menggambarkan suatu objek untuk mengambil kesimpulan-kesimpulan yang berlaku secara umum.

Pendekatan penelitian (*approach)* yang digunakan dalam penelitian ini yaitu pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach),* pendekatan perbandingan (*comparative approach*)

Adapun jenis data yang digunakan dalam penelitian ini adalah data sekunder yang diperoleh dari bahan hukum primer dan sekunder. Sedangkan teknik pengumpulan data dilakukan secara studi kepustakaan (*library research*). Studi kepustakaan dilakukan untuk mencari dan memperoleh data sekunder adalah berupa studi dokumen. Alat pengumpulan data berupa studi dokumen tersebut dilakukan agar dapat mengetahui sebanyak mungkin pendapat atau konsep para ahli yang telah melakukan penelitian dan penulisan tentang *cyber crime*, *cyber warfare* serta bentuk-bentuk perlindungan yang dilakukan dalam menghadapi ancaman serangan *cyber crime* dan *cyber warfare*. Kemudian metode analisis data yang dipergunakan adalah metode analisis *kualitatif.* Penelitian kualitatif adalah penelitian yang bersifat menyeluruh dan merupakan satu kesatuan bulat (*holistic*), yaitu meneliti data yang diperoleh secara mendalam dari berbagai segi

PEMBAHASAN

Adapun hasil pembahasan yang penulis paparkan dalam penelitian ini adalah yang berkaitan dengan bentuk bentuk *cyber crime,* bentuk bentuk *cyber warfare,* contoh-contoh kasus *cyber*

crime dan *cyber warfare* serta bentuk-bentuk perlindungan yang dilakukan dalam menghadapi ancaman *cyber crime* dan *cyber warfare.*

Bentuk-Bentuk Cyber Crime

Ari Juliano Gema menyatakan bahwa dalam beberapa literatur dan praktik kejahatan yang berhubungan dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi (*cyber crime*) dikelompokkan dalam beberapa bentuk yaitu:

1. *Unauthorized Access to Computer System and Service*. Kejahatan ini dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik jaringan komputer yang dimasukinya. Motifnya bisa bermacam-macam, antara lain adalah sabotase, pencurian data dsb. Sebagai contoh adalah website milik Pemerintah RI dirusak oleh hacker (Kompas, 11/08/1999).
2. *Illegal Contents*. Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh yang termasuk kejahatan jenis ini adalah pornografi, pemuatan berita bohong, agitasi termasuk juga delik politik dapat dimasukkan dalam kategori ini bila menggunakan media ruang siber.
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. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau datanya tersimpan dalam suatu sistem yang *computerized*.
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 ke Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program tertentu sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Kejahatan ini juga kadang disebut dengan *cyber terrorism*.
6. *Offence Against Intellectual Property*. Kejahatan ini ditujukan terhadap HAKI yang dimiliki pihak lain di internet. Sebagai contoh, meniru tampilan web suatu situs tertentu, penyiaran rahasia dagang yang merupakan rahasia dagang orang lain.
7. *Infringements of Privacy*. Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan secara *computerized*. Yang apabila diketahui orang lain maka dapat merugikan korban secara materiil atau immaterial, seperti nomor PIN ATM, nomor kartu kredit dan sebagainya. (Ari Juliano Gema, 2000)

Di samping itu berdasarkan beberapa literatur serta praktiknya, *cyber crime* memiliki karakteristik yang khas

dibandingkan dengan kejahatan konvensional, yaitu:

- Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang/wilayah siber (*cyber space*), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
- Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
- Perbuatan tersebut mengakibatkan kerugian material maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
- Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
- Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara (Ari Juliano Gema, 2000)

Bentuk-Bentuk Cyber Warfare

Dalam c*yber warfare*, terdapat metode penyerangan yang tentunya berbeda dengan perang klasik, perang konvensional atau perang fisik lainnya. Domain dari c*yber 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*:

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

Igor Bernik (2014) Di dalam bukunya yang berjudul Cybercrime and Cyber Warfare memaparkan beberapa jenis dan teknik dari cyber warfare: *"Using the techniques of cyberwarfare at the state level is usually aimed at obtaining information on the economic, political, cultural and military situations in another country - the target - or for specific offensive and defensive operations in cyberspace. In the first case, countries most often achieve the objectives through espionage, and in the second case, these are carried out through actions in cyberspace that are similar to military activities. However, cyberwarfare does not fall only within the competence of states, but is also used by corporations or those organizations, which need information for which they do not have authorized access for their survival, development and competition. New guidelines and needs for information, as well as knowledge related to it, will be increasingly dictated by aggressive competition and organizations lagging behind.*

As an offensive activity, cyberwarfare consists of the following six components:

1. *Psychological operations, which impact the mental state of an opponent (propaganda or dissemination of information to influence the decision making of people, whereby the Internet is a great tool for achieving this).*
2. *Electronic warfare, which includes disabling of access to information needed by the opponent (usually carried out by terrorists, hacktivists and countries).*
3. *Military deception, which is similar to the one in traditional forms of warfare, whereby the opponent is misled regarding actual military capability.*
4. *Physical cyberwarfare, which includes physical attacks on information systems.*
5. *Protection measures to protect information system; the aim is to have a system that cannot be disabled by the opponent.*
6. *Information attack, which covers the abuse, use or destruction of information.*

An offensive information operation involves the collection of confidential information, unauthorized access to information systems, creating security loopholes in it, the modification or destruction of data and disabling or destroying an information system, whereas this kind of information "fighting" has the following two fundamental forms:

1. *Disinformation or deceiving the opponent and attack on the computer network;*
2. *Distruption or destruction of the opponent's information.*

Contoh-Contoh Kasus Cyber Crime

Ada beberapa contoh fakta kasus *cyber crime* yang terjadi di Indonesia, diantaranya adalah:

1. Pencemaran nama baik

   Dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) No. 11 Tahun 2008 tidak disebutkan tentang pencemaran nama baik, tapi dengan merujuk pasal 310 ayat (1) KUHP pencemaran nama baik dapat diartikan sebagai perbuatan menyerang kehormatan atau nama baik seseorang dengan menuduhkan

sesuatu hal yang dimaksudnya terang supaya hal itu diketahui umum, tentu dalam hal ini menggunakan media elektronik.

2. Ujaran kebencian
   Adalah tindakan komunikasi yang dilakukan suatu individu atau kelompok dalam bentuk provokasi, hasutan, ataupun hinaan kepada individu maupun kelompok yang lain dalam hal berbagai aspek seperti ras, warna kulit, etnis, gender, dll.
3. Pencurian *Account User Internet*
   Merupakan salah satu dari kategori *Identity Theft and Fraud* (pencurian identitas dan penipuan), hal ini dapat terjadi karena pemilik *user* kurang sigap terhadap keamanan di dunia maya, dengan membuat user dan password yang identik atau gampang ditebak memudahkan para pelaku kejahatan dunia maya ini melakukan aksinya.
4. *Deface* (Membajak situs web)
   Metode kejahatan *deface* adalah mengubah tampilan sesuai keinginan pelaku kejahatan. Bisa menampilkan tulisan-tulisan provokatif atau gambar-gambar lucu. Merupakan salah satu jenis kejahatan dunia maya yang paling favorit karena hasil kejahatan dapat dilihat secara langsung oleh masyarakat.
5. *Probing* dan *Port Scanning*
   Salah satu langkah yang dilakukan *cracker* sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan "*port scanning*" atau "*probing*" untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil *scanning* dapat menunjukkan bahwa server target menjalankan program web server *Apache*, mail server *Sendmail*, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall* atau tidak) dan seterusnya.
6. *Virus* dan *Trojan*
   Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. *Trojan* adalah sebuah bentuk perangkat lunak yang mencurigakan (*malicious software*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari *Trojan* adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam sistem log, data dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).
7. *Denial of Service* (DoS) *Attack*
   Adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.
8. *Carding*
   Adalah aktivitas pembelian barang di Internet menggunakan kartu kredit bajakan. Kartu kredit tersebut diperoleh dengan cara meminta dari carder lain (dengan catatan harus tergabung dalam komunitas carder pada server IRC tertentu), ataupun dengan menggunakan kemampuan *social engineering* yang dimiliki oleh carder. Kejahatan *carding* juga seringkali dilakukan dengan sistem *Phishing* yaitu dengan penyadapan melalui situs *website* aspal (asli tapi

palsu) agar personal data nasabah dapat di curi. Kasus yang pernah terjadi adalah pengubahan nama situs www.klikbca.com menjadi www.kilkbca.com.

9. Perjudian online
   Pelaku menggunakan media internet untuk melakukan tindak pidana perjudian.
10. *Cybersquatting*
    Adalah mendaftar, menjual atau menggunakan nama *domain* dengan maksud mengambil keuntungan dari merek dagang atau nama orang lain. Umumnya mengacu pada praktik membeli nama domain menggunakan nama-nama bisnis yang sudah ada atau nama orang-orang terkenal dengan maksud untuk menjual nama mereka untuk mengambil keuntungan. Contoh *domain domain* perusahaan milik Carlos Slim diserobot orang dengan cara menjual iklan google milik perusahaan Carlos Slim kepada perusahaan pesaing. Penyelesaiannya menggunakan prosedur *Anti cybersquatting Consumer Protection Act* (ACPA) yaitu mengembalikan domain kepada pemiliknya melalui dan memberi hak merek.

Contoh-Contoh Kasus Cyber Warfare

1. Kerusuhan anti Cina Bulan Mei 1998
   Dalam bukunya tentang *Cyber Warfare*, Jeffrey Carr (Carr, 2012) memberikan beberapa contoh kejadian terkait dengan perang dunia maya. Untuk kasus yang terkait dengan Indonesia diberikan contoh tentang kejadian kerusuhan anti-Cina yang terjadi di bulan Mei 1998. Pada saat itu berbagai hackers dari berbagai organisasi – seperti misalnya China Hacker Emergency Center – menyerang berbagai situs yang terkait dengan pemerintah Indonesia sebagai protes. Serangan yang dilakukan pada saat itu tidak hanya ditujukan kepada situs pemerintahan Indonesia saja tetapi terhadap situs-situs lain pelaku bisnis Indonesia. Perlu diingat bahwa pada tahun 1998 itu wawasan pemerintah Indonesia terhadap internet belum besar. Belum banyak instansi pemerintah yang memiliki situs web. Akhirnya serangan di arahkan ke mana saja selama terkait dengan Indonesia.
2. Kasus Timor-Timur
   Pada kasus yang lain, yaitu kasus Timor Timur, sempat terjadi serang menyerang antara hackers Indonesia dan Portugal. Untuk kasus yang ini, serangan dilakukan untuk melumpuhkan komputer yang ditargetkan. Jika penyerang dapat masuk, maka dia akan berusaha menghapus semua berkas atau memformat disk. Perhatikan bahwa itikad dari penyerang berbeda dari contoh sebelumnya.
3. Virus Stuxnet yang menyerang infrastruktur negara Iran.
   Kejadian yang dianggap sebagai bukti telah terjadinya perang teknologi informasi – meskipun tidak terang-terangan – adalah ditemukannya virus *Stuxnet* di sekitar bulan Juni 2012. Virus yang menyerang sistem operasi Microsoft Windows ini dipercaya dibuat untuk menyerang infrastruktur dari negara Iran dengan menyerang perangkat (*hardware* dan *software*) yang dibuat oleh Siemens. Perangkat Siemens tersebut banyak digunakan sebagai basis dari SCADA (*supervisory control and data acquisition*) yang digunakan di berbagai tempat industri dan pertahanan Iran. Sampai saat ini masih diduga siapa pembuat virus Stuxnet tersebut.
4. Kasus Penyadapan yang terjadi di Yunani
   Kasus penyadapan lain juga terjadi di Yunani, dikenal dengan nama “the Athens Affair” Kasus ini bermula

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

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

Bentuk-Bentuk Usaha Yang Dilakukan Dalam Memberikan Perlindungan Terhadap Ancaman Cyber Crime

1. Buat kata sandi yang kuat
   Kata sandi adalah salah satu perlindungan paling dasar yang dapat diterapkan untuk mencegah ancaman dunia maya. Dengan menggunakan kata sandi yang kuat, dapat mengurangi upaya peretas untuk mencuri kata sandi dan membobol sistem keamanan Salah satu metode kriminal yang harus kamu waspadai adalah brute force. Peretas akan mencoba mengambil alih akun melalui coba-coba untuk memecahkan kata sandi, login, atau kunci enkripsi. Metode ini relatif sederhana dibandingkan dengan metode lainnya. Namun hingga saat ini, serangan *brute force* masih sering digunakan dan kasusnya semakin meningkat, terutama karena transaksi sudah mulai berpindah ke dunia digital.
2. Lakukan maintenance situs web secara berkala
   Manajemen situs web adalah pekerjaan yang perlu dilakukan secara teratur. Misalnya, kita harus memperbarui dan memelihara situs web secara teratur untuk menghindari lubang keamanan yang tidak diketahui. Sebaiknya lakukan pemeliharaan situs secara rutin, misalnya menetapkan prioritas pemeliharaan yang bisa dilakukan harian, mingguan, bulanan atau tahunan. Dengan cara ini, website akan memiliki sistem dan komponen yang selalu up to date.
3. Menggunakan SSL/TLS dan *firewall*
   SSL atau *Secure Socket Layer* merupakan salah satu sertifikat keamanan yang harus dimiliki sebuah website. Penggunaan utamanya adalah untuk meningkatkan keamanan transmisi data yang terjadi di situs web. Situs aman akan memiliki gembok di sebelah bilah alamat dengan URL HTTPS. Proses pertukaran data online seperti mengakses website, transaksi online, mengirim dan menerima email, mentransfer data dilakukan dengan menggunakan metode enkripsi *end-to-end*. Dengan cara ini, hanya pengirim dan penerima permintaan yang dapat membaca informasi tersebut. Selain SSL, aplikasi *firewall* sering kali menyediakan fungsionalitas untuk memblokir serangan peretas dan berpotensi menyaring spammer dan bot berbahaya untuk situs web. *Firewall* dapat memblokir beberapa

situs web yang dapat menyerang situs web lain.

4. Jangan pakai email domain gratis
   Cara selanjutnya untuk melindungi situs webdari serangan siber adalah dengan menghindari penggunaan email domain gratis. Sebab, salah satu cara untuk login ke situs tersebut adalah melalui email. Banyak peretas meretas email untuk membobol situs web. Jika berhasil, data penting seperti akses ke aplikasi login, situs web atau item terkait sistem keamanan dapat diperoleh dengan mudah. Domain email gratis seringkali menjadi incaran para hacker karena memiliki sistem keamanan yang terbatas.
5. Memilih jenis *hosting* yang tepat
   Langkah pertama yang perlu dipastikan sebelum membuat website adalah memilih jenis hosting dan penyedia layanan *hosting* yang berkualitas. Setiap jenis *hosting* memiliki standar dan fitur keamanan yang berbeda. Misalnya, untuk memilih jenis hosting yang tepat, dan harus berhati-hati dengan volume dan ketersediaan lalu lintas. Oleh karena itu, pemilihan jenis *hosting* yang tepat sesuai dengan kebutuhan *website* sangat penting untuk memastikan kapasitas dan sistem keamanan yang memadai.
6. Gunakan layanan *hosting* standar ISO 27001
   Selain jenis *hosting*, memilih layanan hosting yang berkualitas dan aman juga penting untuk menghindari risiko ancaman *cyber*. Solusinya, menggunakan layanan penyimpanan yang disertifikasi oleh Exabytes ISO 27001 *International Security Standard*. Exabytes menyediakan *cloud hosting* yang mengutamakan keamanan data dengan perlindungan DDoS terbaik di kelasnya dari Cloudflare dan lainnya.
7. Perlindungan dan Penegakan Hukum yang tegas
   Alat-alat negara bertanggungjawab untuk menggunakan hukum sebagai senjata guna melawan berbagai bentuk kejahatan yang akan, sedang atau telah mengancam bangsa Indonesia. Alat negara (penegak hukum) dituntut bekerja keras seiring dengan perkembangan dunia kejahatan, khususnya perkembangan *cyber crime* yang semakin mengkwatirkan. Alat negara ini menjadi subjek utama yang berperang melawan *cyber crime*. Misalnya Resolusi PBB No.55 Tahun 1963 tentang upaya untuk memerangi kejahatan penyalah gunaan TI (Teknologi Informasi) pada tanggal 4 Desember 2001, memberikan indikasi bahwasannya ada masalah internasional yang sangat serius, gawat dan harus segera ditangani. Penyalahgunaan TI telah menjadi salah satu agenda dari kejahatan tingkat global. Kejahatan di tingkat global ini menjadi ujian berat bagi masing-masing negara untuk memeranginya. Alat yang digunakan oleh negara untuk memerangi *cyber crime* adalah hukum. Hukum difungsikan, salah satunya untuk mencegah terjadinya dan menyebarkan *cyber crime*, serta menindak jika *cyber crime* terbukti telah meyerang atau merugikan masyarakat dan negara. Disamping itu juga Kitab Undang-Undang Hukum Pidana (KUHP) masih menjadi sebagai dasar hukum untuk menjaring *cyber crime*, khususnya jenis *cyber crime* yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Beberapa dasar hukum dalam KUHP yang digunakan oleh aparat penegak hukum yaitu sebagai berikut: pasal 167 KUHP, pasal 406 ayat (1) KUHP, pasal 282 KUHP, pasal 378 KUHP, pasal 112 KUHP,

pasal 362 KUHP, pasal 372 KUHP. Selain itu ada juga ketentuan pidana yang digunakan dalam menjaring *cyber crime* diantaranya terumus di dalam pasal 72 dan pasal 73 Undang-Undang Hak Cipta Nomor 12 Tahun 2002. Dalam ketentuan ini, penegak hukum menggunakannya sebagai dasar hukum untuk menjerat pelaku yang diduga melakukan *cyber crime*. Kemudian terdapat juga peraturan yang lain untuk menjerat pelaku kejahatan dalam *cyber crime* yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

8. Memberikan kesadaran hukum kepada masyarakat tentang bahaya *cyber crime.*

   Kurangnya kesadaran hukum masyarakat berimplikasi dan pemahaman serta ketidaktaatan mereka terhadap hukum. Didik M. Arief Mansur dan Elisatris Gultom merumuskan beberapa alasan maka sampai saat ini kesadaran hukum masyarakat Indonesia masih sangat kurang, yakni sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cyber crime*. *Lack information* ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan piñataan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas yang di duga berkaitan dengan *cyber crime*, maka dengan demikian perlu ditumbuhkan dan diberikan kesadaran hukum terhadap masyarakat akan bahaya dan ancaman dari *cyber crime*

Bentuk-bentuk usaha yang dilakukan dalam memberikan perlindungan dari ancaman cyber warfare

1. Perlindungan Infrastruktur Utama

   Untuk melakukan perlindungan perlu diketahui dahulu aset apa yang ingin dilindungi. Setelah itu baru dapat kita buatkan rencana dan strategi perlindungannya. Bagi perusahaan, sebelum melakukan perlindungan dilakukan pendataan aset. Hal yang sama juga dapat dilakukan pada level negara. Untuk ini biasanya perlindungan pada level negara dikenal istilah "*national critical infrastructure protection*". Langkah awal adalah dilakukan pemetaan apa yang masuk ke dalam kategori "*critical infrastructure*". Beberapa negara telah melakukan proses ini. Nampaknya perlu dilakukan sebuah pemetaan untuk skala Indonesia. Secara umum yang dapat dikategorikan sebagai infrastruktur dari sistem berbasis teknologi informasi adalah:

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

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

2. Kesiapan Sumber Daya Manusia

   Salah satu aspek utama dalam perang dunia maya adalah aspek manusia. Ada beberapa isu terkait dengan aspek manusia ini. Apakah pelaku dalam perang dunia maya hanya terbatas kepada tentara saja? Pada kenyataannya, rakyat ikut berperang.

Tentu saja rakyat ini harus dilatih dulu agar dapat ikut berperang dan bertahan. Hal yang sudah pasti harus dilakukan adalah menyiapkan dan melatih tentara yang secara resmi memahami berbagai aspek perang dunia maya. Mereka harus memiliki kemampuan (*skill*) teknis. Bidang ini merupakan bidang yang baru, untuk itu biasanya dikembangkan sumber daya dari usia muda. Hal ini bukan berarti bahwa tentara yang sudah berusia lanjut tidak perlu dilatih. Justru penguasaan teknologi informasi tidak dibatasi dengan kemampuan fisik yang biasanya terkendala dengan usia. Artinya siapapun dengan usia berapapun dapat dilatih. Hanya kemauan yang membatasi. Salah satu tantangan yang harus dihadapi adalah kecepatan perkembangan teknologi di bidang ini. Untuk itu penguasaan kemampuan harus terus dilatih dengan teknologi terbaru. *Training* dan *re-training* merupakan salah satu kunci yang penting. Secara keilmuan, *information and communication technology security* dapat dianggap masih baru meskipun pemanfaatannya sudah dilakukan sejak dari jaman dahulu. Pendidikan secara formal di bidang ini juga masih terbatas. Belum banyak perguruan tinggi yang menyediakan kuliah security.

3. Penguasaan Teknologi
   Teknologi selalu memiliki peran dalam perang. Kemampuan pihak Sekutu dalam memecahkan sistem sandi (kriptografi) dari Jerman (yang menggunakan *Enigma*) dianggap sebagai sebuah hal yang membantu mempercepat selesainya perang dunia kedua. Bahkan teknologi-teknologi banyak yang berkembang dari dunia pertahanan (*defense*). Terlebih lagi dengan perang di dunia maya, peran teknologi adalah mutlak. Penguasaan teknologi adalah mutlak. Beberapa bidang yang harus dikuasai terkait dengan perang dunia maya antara lain: jaringan, sistem operasi, pemprograman, kriptografi, protokol, malware, *security tools*, dan *security* secara umum.
4. Menerapkan Hukum Humaniter Internasional bagi *Cyber Warfare*
   Hukum Humaniter Internasional bersumber dari Konvensi Den Haag 1907 dan Konvemsi Jenewa 1949 yang pada prinsipnya menyatakan bahwa perang harus lebih memperhatikan prinsip-prinsip kemanusiaan. Hukum Humaniter Internasional/ HHI adalah seperangakat aturan yang karena alasan kemanusiaan di buat untuk membatasi akibat-akibat dari pertikaian senjata. Hukum ini melindungi mereka yang tidak atau tidak lagi terlibat dalam pertikaian, dan membatasi cara-cara dan metode berperang. Hukum Humaniter Internasional/HHI adalah istilah lain dalam hukum perang (*laws of war*) dan hukum konflik. Adapun tujuan yang hendak dicapai dalam Hukum Humaniter Internasional adalah:
   1. Memberikan perlindungan terhadap kombatan maupun penduduk sipil dari penderitaan yang tidak perlu *(unnecessary suffering*)
   2. Menjamin Hak Asasi Manusia yang sangat fundamental bagi mereka yang jatuh di tangan musuh harus dilindungi dan dirawat serta berhak diperlakukan sebagai tawanan perang.
   3. Mencegah dilakukannya perang secara kejam tanpa mengenal batas. Disini yang terpenting adalah asas kemanusiaan.

   Dengan melihat ketentuan Hukum Humaniter Internasional, *cyber warfare* masuk ke ranah antar negara dan ini perlu aturan main agar perang

cyber ini tidak mengancam nilai-nilai kemanusiaan, maka Hukum Humaniter dapat diterapkan dalam ranngka perlindungan dari ancaman *cyber warfare.*

Terdapat beberapa alasan mengapa Hukum Humaniter Internasional bisa diterapkan pada *cyber warfare*: *pertama,* hukum humaniter internasional dapat diterapkan dalam *cyber warfare* dengan melihat dampak atau akibat yang ditimbulkan dan mengandung unsur-unsur yang sama dengan perang konvensional pada umumnya, *kedua*, prinsip-prinsip yang terdapat dalam prinsip hukum humaniter internasional dapat diterapkan dalam *cyber warfare, ketiga*, dalam hukum humaniter internasional terdapat tiga pihak yang terkait dalam peperangan yaitu: kombatan, non-kombatan dan sipil. Pelaku dalam *cyber warfare* orang yang turut dalam konflik secara langsung termasuk di dalamnya kategori kombatan,

SIMPULAN

Adapun kesimpulan dari penulisan ini adalah menjawab dua rumusan masalah diatas yaitu: *Pertama* mengenai bentuk bentuk kejahatan yang dapat dikategorikan *cyber crime* dan *cyber warfare*. Adapun bentuk-bentuk kejahatan yang dapat dikategorikan sebagai *cyber crime* adalah *Unauthorized Access to Computer System and Service, Illegal Contents, Data Forgery, Cyber Espionage, Cyber Sabotage and Extortion, Offence Against Intellectual Property, Infringements of Privacy*. Sedangkan kejahatan yang dapat dikategorikan sebagai *cyber warfare* adalah*: pertama*, pengumpulan informasi. Dimana spionase *cyber* merupakan bentuk aksi pengumpulan informasi bersifat rahasia dan sensitif dari individu, pesaing, rival, kelompok lain pemerintah dan musuh baik dibidang militer, politik, maupun ekonomi. Metode yang digunakan dengan cara eksploitasi secara ilegal melalui internet, *kedua*, vandalism yaitu serangan yang dilakukan sering dimaksudkan untuk merusak halaman web (*Deface*), atau menggunakan serangan *denial-of-service* yaitu merusak sumberdaya dari komputer lain. *Ketiga*, sabotase merupakan kegiatan militer yang menggunakan komputer dan satelit untuk mengetahui koordinat lokasi dari peralatan musuh yang memiliki resiko tinggi jika mengalami gangguan. *Keempat*, 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.

Kedua, adapun bentuk-bentuk usaha yang dilakukan dalam memberikan perlindungan dari ancaman *cyber crime* adalah sebagai berikut: membuat kata sandi adalah salah satu perlindungan paling dasar yang dapat diterapkan untuk mencegah ancaman dunia maya, lakukan maintenance situs web secara berkala, menggunakan SSL/TLS dan *firewall*, jangan pakai email domain gratis, memilih jenis *hosting* yang tepat, gunakan layanan *hosting* standar ISO 27001 perlindungan dan penegakan hukum yang tegas terutama dalam penerapan Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE) dan meningkatkan kesadaran hukum masyarakat akan bahaya ancaman *cyber crime.* Sedangkan bentuk-bentuk yang di lakukan dalam memberikan perlindungan dari ancaman *cyber warfare* adalah: pada level negara dikenal istilah "*national critical infrastructure protection*". Langkah awal adalah dilakukan pemetaan apa yang masuk ke dalam kategori

"*critical infrastructure*". Beberapa negara telah melakukan proses ini. Secara umum yang dapat dikategorikan sebagai infrastruktur dari sistem berbasis teknologi informasi adalah: sumber daya energi/ listrik; infrastruktur telekomunikasi (telepon); dan infrastruktur internet, negara juga harus mempersiapkan sumber daya manusianya dalam penguasaan teknologi informasi dalam menghadapi ancaman *cyber warfare* dengan memberikan *training* dan *re-training information and communication technology security* karena belum banyak Perguruan Tinggi memberikan pendidikan dalam melakukan perlindungan terhadap ancaman *cyber warfare*. Dalam perang di dunia maya, peran teknologi adalah mutlak. Penguasaan teknologi adalah mutlak. Beberapa bidang teknologi yang harus dikuasai terkait dengan perang dunia maya antara lain: jaringan, sistem operasi, pemprograman, kriptografi, protokol, *malware*, *security tools*, dan *security* secara umum, terakhir usaha yang harus dilakukan dalam memberikan perlindungan dari ancaman *cyber warfare* adalah menerapkan Hukum Humaniter Internasional bagi *cyber warfarey* yang di dasarkan pada Konvensi Jenewa 1949 dan Konvensi Den Haag 1907.

DAFTAR PUSTAKA

Buku

Bermik, Igor, 2014, *Cybercrime and Cyberwarfare,* ISTE Ltd 27-37 St George's Road, London, UK.

Carr, Jeffrey, 2012, *Inside Cyber Warfare,* Second, Edition, O'Reilly Media Inc. 1005 Gravenstein Highway North, Sebastopol, CA 95472.

Ibrahim, Jhonny, 2007, *Teori dan Metodologi Penelitian Hukum Normatif,* Cetakan ketiga, Bayu Media Publishing Malang-Jawa Timur

Mamudji, Sri, et al, 2005, *Metode Penelitian dan Penulisan Hukum*, Cet 1, Badan Penerbit FH UI, Depok

Maskun, 2022, *Kejahatan Siber (Cyber Crime) Suatu Pengantar,* Cetakan Ketiga, Kencana, Jakarta.

Marzuki, Peter Muhammad Marzuki, 2013, *Penelitian Hukum*, ed Revisi, Cet 8, Kencana Prenada Media Grup, Jakarta.

Wahid, Abdul; Labib, Mohammad, 2010, *Kejahatan Mayantara (Cyber Crime)*, Cetakan Kedua, Refika Aditama, Bandung.

Yurizal, 2018, *Penegakan Hukum Tindak Pidana Cyber Crime*, Cetakan 1, Media Nusa Creative, Malang.

Peraturan Perundang-Undangan

Resolusi PBB No.55 Tahun 1963 tentang Upaya Untuk Memerangi Kejahatan Penyalahgunaan TI (Teknologi Informasi) pada tanggal 4 Desember 2001

Konvensi Jenewa 1949

Konvensi Den Haag 1907

Kitab Undang Undang Hukun Pidana (KUHP)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE)

Undang-Undang nomor 12 Tahun 2002 Tentag Hak Cipta

Artikel Jurnal

Awaludin, M. (2018). Penerapan Algoritma Rc4 Pada Operasi Xor Untuk Keamanan Pesan Pada Smartphone Berbasis Web. *Jurnal Sistem Informasi Universitas Suryadarma*, *4*(1), 16–22. https://doi.org/10.35968/jsi.v4i1.71

Gani, A.G. 2018, Cybercrime (Kejahatan Berbasis Komputer), *Jurnal Sistem Informasi Universitas Suryadarma*, Vol 5, No 1, DOI: https://doi.org/10.35968/jsi.v5i1.18

Nugraha, Riko, 2012, Persfektif Hukum Indonesia (Cyberlaw) Penangan Kasus Cyber di Indonesia, *Jurnal Ilmiah Hukum Dirgantara*, Volume 11 Nomor 2, hal 44-58

Sari, Indah, 2021, Tinjauan Yuridis Hubungan Kejahatan Perang Dan Hukum Humaniter Internasional, *Jurnal Ilmiah Hukum Dirgantara*, Volume 11 Nomor 2, hal 23-43.

Subagyo, Agus, 2015, Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy in Facing of Cyber Warfare Threat, *Jurnal Pertahanan*, Volume 5 Nomor 1, hal 89-102.

Sumber Rujukan dari Website

Ahmad Farid, 2022, 14 Kasus Cyber Crime di Indonesia Yang Menggemparkan Warganet, https://www.exabytes.co.id/blog/kasus-cyber-crime-di-indonesia/. Diakses tanggal 5 Desember 2022

Alvianto, IvanHilmi and Ikaningtyas, and Setyo Widagdo, 2013, Tinjauan Mengenai Cyber Warfare Berdasarkan Hukum Humaniter Internasional (Studi Kasus Perang Antara Rusia dengan Georgia Pada 7 Agustus 2008, http://repository.ub.ac.id/id/eprint/111579/. Diakses tanggal 7 Desember 2022.

Budi Raharjo, 2012 Perang Dunia Maya: Cyberwar.2022, https://budi.rahardjo.id/files/perang-dunia-maya.pdf. Diakses tanggal 5 Desember 2022.

Kartini, Eliva Angel Tampubolon, 2019, Perbedaan Cyber Attack, Cybercrime dan Cyberwarfare.https://www.researchgate.net/publication/342671435_Perbedaan_Cyber_Attack_Cybercrime_dan_Cyber_Warfare. Diakses tanggal 10 Desember 2022