Jurist-Diction
Volume 2 No. 2, Maret 2019
Histori artikel: Submit 18 Februari 2019; Diterima 23 Februari 2019; Diterbitkan online 1 Maret 2019.

Perbedaan *Cyber Attack, Cybercrime,* dan *Cyber Warfare*

Kartini Eliva Angel Tampubolon
kartinielivaangel@gmail.com
Universitas Airlangga

Abstract
In the era of industrial revolution 4.0, many activities use internet and computers. There are many personal activities and government in real space are transformed into cyberspace. In the development of information and communication technology, many people and countries abuse it to achieve personal benefit or even to reach a certain political goals of a country. These goals are achieved by several illegal activities in cyberspace. Some illegal activities that are not found in real space are known as cybercrime, cyber attack, cyber espionage, and other terms. Then in the stages of development, illegal activities appear specifically aimed at the political goals of a country known as cyber warfare. There are several debates regarding the differences in the classification of cybercrime, cyber attacks, and cyber warfare. Cybercrime is an expansion of crime in real space, while cyber warfare is an expansion of war in real space. Then cyber attacks have their own definitions that are different from the two terms. Distinguishing these three things is important because they have different legal consequences so that they must be regulated by different laws as well.
Keywords: *Cybercrime; Cyber Attack; Cyber Warfare; Cyber Law; International Law.*

Abstrak
Di era revolusi industri 4.0, banyak aktivitas menggunakan internet dan komputer. Banyak aktivitas individu dan pemerintahan di dalam real space ditransformasikan ke dalam cyberspace. Dalam perkembangan teknologi informasi dan komunikasi tersebut, banyak orang dan negara menyalahgunakannya untuk mencapai keuntungan pribadi atau bahkan mencapai tujuan politik suatu negara. Tujuan-tujuan tersebut dicapai dengan beberapa aktivitas illegal dalam cyberspace. Beberapa aktivitas illegal yang tidak ditemukan di dalam real space tersebut dikenal dengan istilah cybercrime, cyber attack, cyber espionage, dan istilah lainnya. Kemudian dalam tahapan perkembangannya, muncul aktivitas illegal yang ditujukan khusus untuk tujuan politik suatu negara yang dikenal dengan istilah cyber warfare. Ada beberapa perdebatan mengenai perbedaan pengklasifikasian kasus mengenai cybercrime, cyber attack, dan cyber warfare. Cybercrime merupakan perkembangan dari bentuk kejahatan di real space, sementara cyber warfare merupakan perkembangan dari bentuk perang di real space. Kemudian cyber attack memiliki definisi tersendiri yang berbeda dari kedua istilah tersebut. Pembedaan ketiga hal tersebut merupakan hal yang penting karena ketiganya memiliki akibat hukum yang berbeda sehingga kemudiajn akan diatur oleh hukum yang berbeda juga.
Kata Kunci: Cybercrime; Cyber Attack; Cyber Warfare; Hukum Siber; Hukum Internasional.

Pendahuluan

Abad ke-21 dikenal sebagai era revolusi industri 4.0 dimana kehadiran komputer dan internet banyak membawa manfaat bagi manusia. Masyarakat melakukan banyak aktivitas dengan lebih mudah dan cepat dengan menggunakan komputer dan internet. Banyak aktivitas manusia sebagai individu, kegiatan

perusahaan, dan kegiatan pemerintahan yang sekarang sedang ditransformasikan dalam ruang maya atau yang disebut *cyberspace.* Istilah *cyberspace* pertama kali muncul di tahun 1984, digunakan oleh William Gibson dalam novelnya Neuromancer di tahun 1984.[1] William Gibson menggambarkan karakternya bergerak di dalam internet, menghasilkan lanskap yang stabil, ada penduduknya, mudah dinavigasikan, seukuran negara atau bahkan lebih besar.[2]

Dengan kemajuan teknologi informasi dan komunikasi, jarak dan waktu bukan lagi menjadi masalah yang besar bagi setiap orang, perusahaan termasuk pemerintah. Setiap orang dapat saling berhubungan satu sama lain tanpa harus bertemu di *real space.* Perusahaan dapat mengembangkan usahanya ke banyak negara hanya dengan melakukan pemasaran melalui internet dan komputer. Pemerintah dapat melakukan banyak aktivitas pemerintahan hanya melalui internet dan komputer. Sebagai contoh, antar negara di dunia dapat melakukan hubungan diplomat tanpa harus datang ke negara yang bersangkutan. Informasi global dan jaringan komunikasi yang sekarang menjadi bagian integral dari cara pemerintahan modern, bisnis, pendidikan, dan ekonomi beroperasi.[3]

Dalam *cyberspace,* antar pengguna dapat berkomunikasi dengan menyamarkan identitasnya (*anonymous*), tanpa dibatasi oleh batas wilayah (*borderless*), dan bahkan lintas negara (transnasional).[4] Sifat *cyberspace* tersebut yang kemudian mendorong kejahatan-kejahatan konvensional yang ada di dalam *real space* juga ikut ditransformasikan ke dalam *cyberspace* dan menimbulkan banyak pelanggaran hukum pada lapangan yang dianggap tidak ada hukum tersebut. Sebagai contoh, penipuan yang dilakukan oleh orang-orang yang melakukan aktivitas perdagangan di dalam *cyberspace.* Pencurian data yang dilakukan oleh orang-orang tertentu yang menguasai teknologi informasi dan komunikasi dengan baik, dan banyak

---

[1] Murray Andrew D, *The Regulation of Cyberspace*, *Control in the Online Environment*, (Routledge-Cavendish 2007).[5].

[2] *ibid.*

[3] Purna Cita Nugraha, 'Konsepsi Kedaulatan Negara dalam Borderless Space' (2013) 13 Jurnal Opinio Juris. [26]. eJournal: <https://pustakahpi.kemlu.go.id/dir_dok/OPINIO%20JURIS_vol_13d.pdf#page=30>.

[4] *ibid.*[25].

bentuk kejahatan konvensional lainnya yang ditransformasikan dalam *cyberspace.* Bahkan, dalam perkembangan teknologi informasi dan komunikasi, ada beberapa bentuk kejahatan dalam *cyberspace* tidak dapat ditemukan dalam *real space*. Beberapa dari bentuk kejahatan yang tidak ditemukan di dalam *real space* dikenal dengan istilah *cybercrime, cyber attack, cyber espionage5,* dan istilah lainnya. Dalam tahapan perkembangannya, muncul kasus baru dalam pemerintahan di *cyberspace,* yaitu *cyber warfare.*

Ada beberapa perdebatan mengenai perbedaan pengklasifikasian kasus mengenai *cybercrime, cyber attack,* dan *cyber warfare.* Pembedaan ketiga istilah tersebut merupakan hal yang penting. *Cybercrime* merupakan bentuk perkembangan dari kejahatan, *cyber warfare* merupakan bentuk perkembangan dari perang. Keduanya memiliki bentuk dasar dan karakteristik yang berbeda. Secara konvensional, *cyber warfare* dan *cybercrime* juga diatur oleh hukum yang berbeda. Dari bentuk konvensionalnya, pelanggaran-pelanggaran hukum tersebut sudah terlihat berbeda, dalam perkembangannya juga harus dibedakan, karena memiliki akibat hukum yang berbeda pula dalam pengaturannya. Pembedaan tersebut juga diperuntukkan sebagai bentuk dari kepastian hukum dan perlindungan hukum bagi orang-orang yang terlibat dalam pelanggaran hukum tersebut.

Cyber Attack

Penyerangan di dunia *cyberspace* sudah terjadi sejak tahun 1988 dalam peristiwa *The Morris Worm*.[6] *Worm* merupakan senjata *cyber* yang digunakan untuk memperlambat kinerja komputer yang terhubung pada jaringan sampai pada titik dimana komputer tidak dapat digunakan.[7] Pada saat itu, Robert Tapan Morris menyebarkan worm di sebagian besar komputer di Amerika Serikat.[8] Penyerangan

[5] *Cyber espionage is defined narrowly as any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party. The act must occur in territory controlled by a party to the conflict (Rule 66 Talinn Manual on The International law Applicable to Cyber Warfare).*

[6] NATO Review Magazine, *Loc. cit.*

[7] *ibid.*

[8] *ibid.*

tersebut dikenal sebagai *cyber attack.* Dalam *rule 30 Talinn Manual on The International law Applicable to Cyber Warfare* (selanjutnya disebut sebagai *Tallinn Manual*), *cyber attack* didefinisikan dengan "*cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".*

Dalam Bahasa Indonesia dapat didefenisikan sebagai serangan dalam dunia maya, baik yang ditujukan untuk menyerang ataupun bertahan yang diharapkan dapat sebagai penyebab kematian seseorang atau kerusakan suatu objek yang dituju. Dalam beberapa dekade terakhir, istilah *cyber attack* sudah menjadi sangat terkenal. *Cyber attack* mampu mematikan sentrifugal nuklir, sistem pertahanan udara, dan jaringan listrik, serangan dunia maya yang menimbulkan ancaman serius bagi keamanan nasional.[9]

Cyber attack merupakan hasil dari perkembangan teknologi informasi dan komunikasi, sehingga senjata yang digunakan dalam *cyber attack* memiliki beberapa karakteristik yang berbeda dibandingkan dengan karakteristik senjata konvensional. Tujuan sesungguhnya dari pelaku *cyber attack* bukanlah semata-mata sebatas merusak dan/atau menghancurkan suatu *cyber system* dan/atau *cyber operation.* Tujuan sesungguhnya *cyber attack* adalah lebih luas, meliputi pemusnahan integritas (*loss of integrity*), ketersediaan (*availability*), kerahasiaan (*confidentialitly*), *and* pemusnahan fisik (*physical destruction*)10 yang dampaknya telihat pada aktivitas korban di *real space.* Sebagai contoh kasus *cyber attack* adalah kasus yang menimpa eBay di awal Maret tahun 2014, dimana situs eBay tidak dapat diakses sehingga kehilangan 233 pelanggan.[11] Dari contoh kasus tersebut, tujuan

---

[9] Oona A. Hathaway, at al, '*The Law Of Cyber Attack*' (2012) *California Law Review*. [817]. eJournal: <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.co.id/&httpsredir=1&article=4844&context=fss_papers>.

[10] U.S. Army Training and Doctrine Command*, 'Cyber Operations and Cyber Terrorism Handbook'* (2005), <http://www.au.af.mil/au/awc/awcgate/army/guidterr/sup2.pdf>, pada Dean C. Alexander, '*Cyber Threats Against the North Atlantica Treaty Organization (NATO) and Selected Reponses*' (2014) Ekim. eJournal: <http://dergipark.gov.tr/download/article-file/89251>.

[11] Mochammad Yuliansyah Saputera, 'Pengaruh *Cyber Security Strategy* Amerika Serikat Menghadapi Ancaman *Cyber Warfare* (2015), 2 *JOM FISIP.*[10]. eJournal: < https://media.neliti.com/media/publications/32726-ID-pengaruh-cyber-security-strategy-amerika-serikat-menghadapi-ancaman-cyber-warfar.pdf>.

sesungguhnya atau *the real intention* dari si pelaku bukan sekedar untuk merusak sistem situs milik eBay, namun untuk membuat penurunan pendapatan eBay. *Cyber attack* yang dilakukan terhadap Perusahaan eBay adalah sebagai sarana pelaku untuk mencapai tujuannya yang sesungguhnya.

Dengan kata lain, *cyber attack* bukan tujuan pelaku yang sesungguhnya. Tujuan pelaku *cyber attack* yang sesungguhnya adalah akibat yang ditimbulkan dalam *real space* sebagai akibat rusaknya suatu sistem siber yang diserang. Dari definisi dan penjelasan mengenai *cyber attack* dapat ditentukan bahwa karakteristik *cyber attack* adalah sebagai berikut :

1. dilakukan oleh individu atau satu kelompok;
2. dilakukan secara sengaja dan melawan hukum (karena ada tertentu yang diharapkan oleh pelaku atas korban di *real space*);
3. menggunakan *cyber weapon;*[12]
4. objek yang dituju adalah sistem siber (*cyber system)*[13] dan/atau operasi siber (*cyber operation*);[14]
5. tujuan penyerangannya adalah untuk merusak dan/atau menghacurkan *cyber system* yang meliputi jaringan komputer maupun internet.

Cybercrime

Cybercrime berawal di periode 1960-an dan terus berkembang hingga saat ini.[15] *Cybercrime* terjadi pertama kali di Amerika Serikat pada tahun 1960-an.[16] Berbagai kasus *cybercrime* terjadi saat itu, mulai dari manipulasi transkrip

---

[12] *Cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack* (Penjelasan poin 2 *Rule* 41 *of Tallinn Manual on The International Law Applicable to Cyber Warfare*).

[13] *Cyber system or computer system is One or more interconnected computers with associated software and peripheral devices. It can include sensors and/or (programable logic) controllers, connected over a computer network. Computer system can be general purpose (for example, a laptop) or specialized (for example the 'blue force tracking system') (Glossary of Technical terms of Tallinn Manual on The International Law Applicable to Cyber Warfare).*

[14] *The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace (Glossary of Technical terms of Talinn Manual on The International Law Applicable to Cyber Warfare).*

[15] Maskun,[*et.,al*],*Op.Cit.*[511].

[16] Rusdi Anto, 'Kasus-Kasus Cyber Crime Sebagai Dampak Perkembangan Teknologi informasi dan komunikasi yang Meresahkan Masyarakat' (Pusat Studi Perencanaan dan Pembangunan Masyarakat 2010) <https://www.researchgate.net/publication/326225839>, accessed 26 Oktober 2018.

akademik mahasiswa di Brooklyn College New York, penggunaan komputer dalam penyelundupan narkotika, penyalahgunaan komputer oleh karyawan hingga akses tidak sah terhadap Database Security Pacific National Bank yang mengakibatkan kerugian sebesar US$10.2 juta pada tahun 1978.[17]

Dalam beberapa kepustakaan, *cybercrime* atau kejahatan siber sering diidentikkan sebagai *computer crime.*[18] Menurut the U.S. Department of Justice, *computer crime* adalah "*….any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".*[19] 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*):[20] *cybercrime 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.*[21]

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".*[22] *Cybercrime* dapat dilakukan lintas batas negara atau dilakukan di dalam satu negara saja. Hal ini yang kemudian membuat hukum siber sebagai dasar hukum *cybercrime* tidak hanya menjadi bagian dari hukum nasional, tetapi juga menjadi bagian hukum internasional.

Sebagai contoh *cybercrime* yang melibatkan beberapa negara, namun pelakunya ditemukan di satu negara adalah komplotan *hacker* bernama SBH

---

[17] *ibid.*

[18] Maskun, *Kejahatan Siber-Cyber Crime-Suatu Pengantar* (Kencana Prenada Media Group 2013).[47].

[19] *ibid.*

[20] Martin Basiang, *The Contemporary Law Dictionary (Second Edition)* (PT Gramedia Pustaka Utama 2016).[115].

[21] *background paper* Kongres PBB X/2000.

[22] *ibid.*

membobol ratusan situs dalam dan luar negeri yang ditemukan di Indonesia.[23] Para hacker menjebol sistem pengamanan dari sistem elektronik milik perusahaan dan pemerintahan negara lain. Kemudian mengancam dan/atau menakut-nakuti dengan meminta sejumlah uang agar *website* yang bersangkutan dikembalikan seperti semula.[24] Dalam contoh ini juga, peretasan dilakukan sebagai bentuk perkembangan kejahatan yang tidak ditemukan di *real space. Cybercrime* dalam contoh ini menggunakan *cyber attack*, yaitu merusak fungsi *cyber system* milik korban, sebagai metodenya untuk mewujudkan kehendaknya atas korban.

Kemudian contoh lain dari *cybercrime* adalah kasus judi *online* yang banyak terjadi di Indonesia pada tahun 2016. Para pelaku melakukan judi dengan sistem *member* dimana semua anggotanya harus mendaftar ke admin situs.[25] Kemudian setiap anggota yang telah mendaftar harus menghubungi ke hp 0811xxxxxxxx dan 024-356xxxx.[26] Mereka melakukan transaksi *online* lewat internet dan ponsel untuk mempertaruhkan pertarungan bola Liga Inggris, Liga Italia dan Liga Jerman.[27] Contoh ini berbeda dengan contoh *cybercrime* sebelumnya karena contoh ini merupakan contoh kejahatan yang dapat ditemukan juga di *real space,* namun karena perkembangan teknologi informasi dan komunikasi, ditransformasikan juga ke dalam *cyberspace* kemudian disebut *cybercrime.*

Dari penjelasan di atas, dijelaskan bahwa *cybercrime* adalah salah satu bentuk kejahatan. Beberapa dari bentuk *cybercrime* merupakan bentuk kejahatan konvensional seperti penipuan, pencurian, pornografi, pencemaran nama baik yang ditransformasikan ke dalam *cyberspace.* Namun beberapa bentuk *cybercrime,*

---

[23] Helmi Syarif, "Retas 6 Situs Pemerintahan di Jawa Timur" (Sindonews 2018), <https://metro.sindonews.com/read/1289885/170/surabaya-black-hat-pernah-retas-6-situs-pemerintahan-di-jawa-timur-1521095177&sa=D&source=hangouts&ust=1541572684313000&usg=AFQjCNFnqEY0DTOlZ-7QzEjRCVX-doegZw>, accessed 6 November 2018.

[24] *ibid.*

[25] Rusdi Anto, *Loc.cit.*

[26] *ibid.*

[27] *ibid.*

yang lain seperti *cyber espionage,*[28] *cyber sabotage and extortion,*[29] *cracking*[30] merupakan bentuk kejahatan yang tidak ditemukan di *real space*, karena hanya dapat direalisasikan dengan alat dan perangkat yang ada dalam *cyberspace.*

Dari penjelasan dan contoh kasus *cybercrime* serta dihubungkan dengan *cybercrime* sebagai bentuk kejahatan internasional yang baru, dapat dikatakan bahwa karakteristik *cybercrime* adalah sebagai berikut:

a. dilakukan oleh subjek hukum;
b. dilakukan secara melawan hukum, norma, dan nilai kepatutan;
c. dilakukan di satu atau lebih negara;
d. ditujukan kepada subjek hukum lain;
e. menggunakan tool dalam cyberspace
f. dengan atau tanpa metode tertentu;
g. dampaknya dapat terjadi di satu atau lebih negara yang berbeda dengan negara tempat pelaku melakukannya;
h. berpotensi besar untuk dilakukan secara anonymous.

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 *cybercrime. Cyber warfare* dapat diartikan sebagai perang di dalam *cyberspace,* namun di dalam *cyber warfare* terdapat penyerangan yang berbeda dengan penyerangan dalam perang konvensional atau perang fisik lainnya. Media

---

[28] *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 (Jummaidi Saputra, Anhar Nasution, 'Mengenal dan Mengantisipasi Kegiatan *Cybercrime* pada aktivitas *online* sehari-hari dalam Pendidikan, pemerintahan, dan Industri dan Aspek Hukum yang Berlaku' (Prosiding SNIKOM 2014).[4]. eJournal : < http://www.ejournal.uui.ac.id/jurnal/MENGENAL_DAN_MENGANTISIPASI_KEGIATAN_CYBERCRIME_PADA_AKTIFITAS_ONLINE_SEHARI-HARI_DALAM_PENDIDIKAN,_PEMERINTAHAN_DAN_INDUSTRI_DAN_ASPEK_HUKUM_YANG_BERLAKU-ox4-2._jurnalis_j_hius_(ks_1).pdf>).

[29] *Cyber sabotage* adalah kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program computer atau sistem jaringan computer yang terhubung dengan internet (*ibid.*)

[30] *Cracking* adalah kejahatan yang menggunakan teknologi computer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses (*ibid.*)

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 *cyberspace* yang dikuasai oleh suatu negara. [31]

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".*[32] 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".*[33]

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".*[34] Definisi yang diberikan oleh UNICJRI memiliki persamaan dengan definisi yang diberikan oleh Richard Clarke, yaitu merupakan tindakan dari actor negara untuk mempenetrasi jaringan komputer negara lain dengan tujuang menyebabkan beberapa kerusakan.

---

[31] Agus subagyo, 'Sinergi dalam Menghadapi Ancaman *Cyber Warfare'* (2015) 1 Jurnal Pertahanan.[99].<*http://jurnal.idu.ac.id/index.php/JPBH/article/view/350*>.

[32] Richard A. Clarke dan Robert K.Knake, *Loc.Cit.*

[33] United Nations Multilingual Terminology Database (UNTERM), '*Cyberwarfare*' (UNTERM 2009) <*http://unterm.un.org/DGAACS/unterm.nsf/WebView/BFDE24673F1B-1F6E85256AFD006732A3?O*>, *accessed* 26 November 2018.

[34] *The United Nations Interregional Crime and Justice Research Institute Website*, "*Cyberwarfare*", pada Trisuharto Clinton, "Kajian Perang Sibernatika (*Cyber Warfare*) Sebagai Konflik Bersenjata Internasional berdasarkan Hukum Humaniter Internasional" (Program Sarjana Fakultas Hukum Universitas Diponegoro 2015).[68].

Dari definisi-definisi di atas, secara sederhana *cyber warfare* dapat diartikan sebagai perang yang dilakukan di dalam *cyberspace.* Karakteristik utama dalam definisi *cyber warfare* yang menyatakan domain *cyber warfare* adalah *cyberspace* melahirkan karakteristik *cyber warfare* yang menggunakan *cyber weapon.* Hal ini disebutkan di dalam *Rule 41 Talinn Manual On The International Law Applicable to Cyber Warfare* (selanjutnya disebut dengan *Tallinn Manual*) yang berbunyi *"means of cyber warfare are cyber weapons and their associated cyber systems". Cyber warfare* tidak lepas dari penggunaan *cyber weapons* yang berkaitan dengan *cyber system.*

Salah satu contoh kasus *cyber warfare* yang pernah terjadi di Estonia pada tahun 2007. Sejak tahun 1990, Pemerintah Estonia telah mengubah pemerintahannya yang berbasis kertas menjadi berbasis *website* untuk mengontrol banyak bisnis.[35] Tahun 2007, Pemerintah Estonia memindahkan patung perunggu *Soldier of Tallinn* yang ada di pusat kota Tallinn, ibukota pesisir Estonia.[36] Pemerintah Estonia berpikir bahwa patung itu adalah symbol penindasan. Sementara bagi Uni Soviet, patungg tersebut adalah symbol untuk memperingati tentara Soviet yang telah membebaskan Estonia.[37]

Pemindahan patung tersebut menimbulkan kekacauan pada aktivitas pemerintahan Estonia yang banyak bergantung pada internet.[38] Pemerintah Estonia menyadari negaranya sedang dalam pengeboman digital yang menyebabkan layanan perbankan dan pemerintahan *offline* (peretasan tersebut dianggap perbuatan Rusia, namun pihak berwenang Rusia menyangkalnya).[39] Estonia kemudian meminta bantuan kepada NATO.[40] Kemudian NATO mengirimkan pasukan militer dengan kemampuan teknik yang dibutuhkan untuk membela dan memperbaiki keadaan Pemerintah Estonia seperti semula.[41]

---

[35] Jason Andress, Steve Winterfield, *Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners* (Elsevier Inc. 2014).[13].

[36] *ibid.*

[37] *ibid.*

[38] *ibid.*

[39] Steve Ranger, "*What is Cyberwar? Everything You Need to Know About The Frightening Future of Digital Conflict*" (ZDNet 2018) <*http://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/*>, *accessed* 23 Oktober 2018.

[40] *ibid.*

[41] *ibid.*

Ada beberapa contoh kasus *cyber warfare* yang lain, di antaranya adalah kasus antara Amerika Serikat dengan Iran di tahun 2008 dimana Amerika Serikat merusak sistem sentrifugal Pembangkit Listrik Tenaga Nuklir milik Iran.[42] Kemudian kasus Georgia dan Rusia di tahun 2008 dimana Rusia menyerang situs-situs milik Pemerintah Georgia sebelum Rusia dan Georgia melakukan perang konvensional.[43] Semakin banyaknya kasus *cyber warfare* didukung dengan data dari *Government Computer Security Incident Response Team* (Govt – CSIRT), yang mengatakan bahwa selama rentang waktu Januari sampai dengan September 2013, insiden keamanan informasi yang paling sering terjadi yaitu *web defacement*, disusul dengan *malware, spam, ip brute force, phising* dan lain-lain.[44]

Objek yang diserang di dalam *cyber warfare* adalah *cyber system* yang berkenaan langsung dengan aktivitas pemerintahan suatu negara di dalam *cyberspace* atau dalam istilah *cyber warfare* disebut sebagai *cyber-infrastructure.* Di dalam daftar kata *Tallinn Manual cyber-infrastructure* didefinisikan sebagai *"... a physical or virtual system and assets under the jurisdiction of a state that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment."*

Dari beberapa contoh di atas, dapat dilihat bahwa *cyber warfare* dapat mengakibatkan lumpuhnya aktivitas pemerintahan yang berbasis komputer dan internet. Dengan kata lain, domain yang digunakan dalam *cyber warfare* adalah *cyberspace.* Domain *cyber warfare* kemudian yang membuat sulit untuk menentukan pelaku *cyber warfare.* Sulit untuk benar-benar membuktikan bahwa sebuah tindakan di dalam *cyber warfare* merupakan tindakan suatu negara.

---

[42] Miko Aditya Suharto, *Perlindungan Hukum Terhadap Kombatan Dalam Cyber Warfare Berdasarkan Asas Public Conscience Dalam Hukum Humaniter Internasional (Studi Cyber Warfare Antara Rusia dan Georgia Pada Agustus Tahun 2008)* (Program Magister Ilmu Hukum Universitas Airlangga, Surabaya, 2017).[2].

[43] Eneken Tikk, *Cyber attacks Against Georgia: Legal Lessons Identified*, *Cooperative Cyber Defence Center of Excellence,* (2008) [4].

[44] KOMINFO, 'Ancaman Cyber Attack dan Urgensi Keamanan Informasi Nasional' (Siaran Pers, 2013) <https://kominfo.go.id/index.php/content/detail/3479/Siaran+Pers+-No.+83-PIH-KOMINFO-11-2013+tentang+Ancaman+Cyber+Attack+dan+Urgensi+Keamanan+Informasi+Nasional/0/siaran_pers>, *accessed* 30 Oktober 2018.

Dari definsi dan analisa beberapa kasus di atas, dapat dilihat bahwa *cyber warfare* yang dilakukan dengan metode apapun pada hakikatnya pelaku menyerang suatu objek yang dikuasai oleh suatu negara untuk melakukan aktivitas pemerintahannya di dalam *cyberspace.* Hal ini menunjukkan bahwa di dalam *cyber warfare* terdapat pelanggaran hukum, norma, serta nilai kepatutan karena *cyber warfare* merusak suatu keadaan yang stabil dalam kehidupan suatu negara. Hal ini dapat dilihat dari contoh kasus Estonia dimana ketika situs-situs pemerintahan Estonia diserang, masyarakat tidak lagi dapat mengakses layanan pemerintahan, bahkan masyarakat tidak dapat melakukan transaksi melalui bank yang terintegritas menggunakan *cyber system.*

Dalam jangka waktu panjang, *cyber warfare* akan memberikan dampak yang lebih luas dan dapat mengganggu kestabilan kedaulatan negara. Hukum kebiasaan internasional mengenal istilah *act of state doctrine* yang berarti setiap negara berdaulat wajib menghormati kemerdekaan negara berdaulat lainnya. Namun, yang terjadi di dalam *cyber warfare* adalah negara tidak menghormati kedaulatan negara lain di dalam *cyberspace* dan melakukan penyerangan terhadap *cyber-infrastructure* milik negara lain.

Dari penjelasan di atas, *cyber warfare* dapat didefinisikan sebagai tindakan serang-menyerang di dalam *cyberspace* yang dilakukan oleh subjek hukum internasional untuk mendapat akses terhadap infrastruktur lawan di dalam *cyberspace* dengan menggunakan *cyber weapon.* Dari definisi tersebut kemudian dapat dirinci karakteristik *cyber warfare* sebagai berikut:

a. subjek : negara atau *hacker-group*[45] (*non-state* actor);
b. objek yang diserang : *cyber system* dan *cyber-infrastructure;*[46]
c. metode : *cyber attack* tertentu;

[45] *Hacker group is a group who gains or attempts to gain unauthrized access to hardware an/or software.* (Kelompok peretas adalah kelompok yang memperoleh atau berupaya mendapatkan akses tanpa izin ke perangkat keras dan/atau perangkat lunak).

[46] *Cyber-infrastructure is physical or virtual system and assets under the jurisdiction of a state that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment (Glossary of Talinn Manual On The International Law Applicable to Cyber Warfare).*

d. sarana : *cyber weapon;*[47]
e. motif : mendapat akses terhadap *cyber-infrastructure* negara lawan;

Cybercrime, Cyber Attack, dan Cyber Warfare

Dari penjelasan *cybercrime, cyber attack,* dan *cyber warfare,* dapat dipetakan bahwa *cyber attack* merupakan satu metode yang dapat dilakukan untuk tujuan *cybercrime* maupun *cyber warfare. Cybercrime* dan *cyber warfare* juga tidak serta merta dapat dipisahkan karena tidak menutup kemungkinan dalam satu fenomena *cyber warfare* terdapat *cybercrime.*

Kesimpulan

Cybercrime, cyber attack, dan *cyber warfare* merupakan tiga aktivitas *illegal* dalam *cyberspace* yang memiliki akibat hukum yang berbeda. *Cyber crime* merupakan perkembangan dari bentuk kejahatan, baik kejahatan konvensiomal yang dikembangakan dari *real space* maupun bentuk kejahatan baru yang hanya dapat dilakukan di dalam *cyberspace. Cyber warfare* merupakan bentuk perkembangan dari perang konvensional dari segi metode dan cara berperang. Sementara *cyber attack* merupakan serangan yang dilakukan di *cyberspace. Cyber attack* dapat ditujukan untuk *cybercrime* maupun *cyber warfare.* Dengan kata lain *cyber attack* merupakan satu metode yang digunakan untuk tujuan *cybercrime* maupun *cyber warfare.*

Daftar Bacaan

Buku

Andrew, Murray D, *The Regulation of Cyberspace, Control in the Online Environment* (Routledge-Cavendish 2007).

Andress Jason, Steve Winterfield, *Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners* (Elsevier Inc. 2014).

[47] *Cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack (Rule 41 Talinn Manual On The International Law Applicable to Cyber Warfare).*

Clarke, Richard A. dan Robert K.Knake, *Cyber War-The Next Threat to National Security and What to Do About It,* (*An Imprint of HarperCollins Publishers* 2010).

Clinton Trisuharto, "Kajian Perang Sibernatika (*Cyber Warfare*) Sebagai Konflik Bersenjata Internasional berdasarkan Hukum Humaniter Internasional" (Program Sarjana Fakultas Hukum Universitas Diponegoro 2015).

Martin Basiang, *The Contemporary Law Dictionary (Second Edition)* (PT Gramedia Pustaka Utama 2016).

Maskun, *Kejahatan Siber-Cyber Crime-Suatu Pengantar* (Kencana Prenada Media Group 2013).

Miko Aditya Suharto, *Perlindungan Hukum Terhadap Kombatan Dalam Cyber Warfare Berdasarkan Asas Public Conscience Dalam Hukum Humaniter Internasional (Studi Cyber Warfare Antara Rusia dan Georgia Pada Agustus Tahun 2008* (Program Magister Ilmu Hukum Universitas Airlangga 2017).

Rahma Novita Pura*, Pertanggungjawaban Pelaku Kejahatan Siber Melalui Deep Web Ditinjau Dari Aspek Hukum Pidana* (Program Magister Ilmu Hukum, Fakultas Hukum, Universitas Airlangga 2017).

Tikk Eneken, *Cyber attacks Against Georgia: Legal Lessons Identified*, (*Cooperative Cyber Defence Center of Excellence* 2008).

Jurnal

Alexander, 'Cyber Threats Against the North Atlantica Treaty Organization (NATO) and Selected Reponses' (2014) Ekim, eJournal: <http://dergipark.gov.tr/download/article-file/89251>.

Hathaway, Oona A, at al, '*The Law Of Cyber Attack*' (2012) *California Law Review*, eJournal: <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.co.id/&httpsredir=1&article=4844&context=fss_papers>.

Nugraha, Purna Cita, 'Konsepsi Kedaulatan Negara dalam *Borderless Space*' (2013) 13 Jurnal Opinio Juris eJournal: <https://pustakahpi.kemlu.go.id/dir_dok/OPINIO%20JURIS_vol_13d.pdf#page=30>.

Rusdi Anto, 'Kasus-Kasus *Cyber Crime* Sebagai Dampak Perkembangan Teknologi informasi dan komunikasi yang Meresahkan Masyarakat', (2012) *Pusat Studi Perencanaan dan Pembangunan Masyarakat*, <https://www.researchgate.net/publication/326225839>.

Saputra Jummaidi, Anhar Nasution, 'Mengenal dan Mengantisipasi Kegiatan *Cybercrime* pada aktivitas *online* sehari-hari dalam Pendidikan, pemerintahan, dan Industri dan Aspek Hukum yang Berlaku', (2014) *Prosiding SNIKOM,* eJournal <http://www.ejournal.uui.ac.id/jurnal/MENGENAL_DAN_MENGANTISIPASI_KEGIATAN_CYBERCRIME_PADA_AKTIFITAS_ONLINE_SEHARI-HARI_DALAM_PENDIDIKAN,_PEMERINTAHAN_DAN_INDUSTRI_DAN_ASPEK_HUKUM_YANG_BERLAKU-ox4-2._jurnalis_j_hius_(ks_1).pdf>.

Saputera, Mochammad Yuliansyah, 'Pengaruh *Cyber Security Strategy* Amerika Serikat Menghadapi Ancaman *Cyber Warfare'* (2015) 2 JOM FISIP, eJournal: <https://media.neliti.com/media/publications/32726-ID-pengaruh-cyber-security-strategy-amerika-serikat-menghadapi-ancaman-cyber-warfar.pdf>.

Laman

Colonel James B. Dermer dan United State Air Force, '*Cyber Warfare: New Character with strategic Results*' (U.S. Army War College 2013) <http://www.dtic.mil/dtic/tr/fulltext/u2/a589312.pdf>. *accessed* 23 Oktober 2018.

Helmi Syarif, "Retas 6 Situs Pemerintahan di Jawa Timur" (Sindonews 2018) <https://metro.sindonews.com/read/1289885/170/surabaya-black-hat-pernah-retas-6-situs-pemerintahan-di-jawa-timur-1521095177&sa=D&source=hangouts&ust=1541572684313000&usg=AFQjCNFnqEY0DTOlZ-7Qz-EjRCVX-doegZw>.*accessed* 6 November 2018.

KOMINFO, 'Ancaman Cyber Attack dan Urgensi Keamanan Informasi Nasional' (*Siaran Pers* 2013), <https://kominfo.go.id/index.php/content/detail/3479/Siaran+Pers+No.+83-PIH-KOMINFO-11-2013+tentang+Ancaman+Cyber+Attack+dan+Urgensi+Keamanan+Informasi+Nasional/0/siaran_pers>. *accessed* 30 Oktober 2018.

Steve Ranger, "What is Cyberwar? Everything You Need to Know About The Frightening Future of Digital Conflict" (*ZDNet* 2018) <*http://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/*>. *accessed* 2 Oktober 2018.

United Nations Multilingual Terminology Database (UNTERM), "*Cyberwarfare*", <*http://unterm.un.org/DGAACS/unterm.nsf/WebView/BFDE24673F1B1F6E85256AFD00732A3?O*>. *accessed* 26 Oktober 2018.

Pengaturan Internasional

The Hague Convention (IV) 1907, respecting the Laws and Customs of War on

Land and Its annex : Regulations concerning the Laws and Customs of War,

Additional to the Geneva Convention of 12 August 1949, and Relating to The Protection of Victims of International Armed Conflict (Protocol I), of 8 June 1977.

Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to The Protection of Victims of International Armed Conflict (Protocol II), of 8 June 1977.

Tallinn Manual on International Law Applicable to Cyber Warfare 2013.

HOW TO CITE: Kartini Eliva Angel Tampubolo, 'Perbedaan *Cyber Attack, Cybercrime,* dan *Cyber Warfare*' (2019) Vol. 2 No. 2 Jurist-Diction.