Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional

Miko Aditiya Suharto[1], Maria Novita Apriyani[2]

[1] *Fakultas Hukum UPN"Veteran" Jawa Timur*
E-mail: miko.aditiya.ih@upnjatim.ac.id
[2] *Fakultas Hukum UPN"Veteran" Jawa Timur*
E-mail: maria.ih@upnjatim.ac.id

ABSTRACT

The movement of human activities initially carried out conventionally turned into digital. This phenomenon also applies to the flow of information traffic. Information that was previously disseminated conventionally has become digitalized. Once the exchange of information and activities on the Internet is so widespread, it is as if the Internet is a world of its own with no boundaries. As a new dimension like land, sea, air, and space, Cyber space also has many problems related to the misuse of computer and internet technology for purposes that deviate from legal norms to the detriment of other parties. The implications of Cyber attacks have destructive properties such as changing, disrupting, closing access, reducing performance, or damaging computer files, computer networks, or the computer itself when associated with the rights of someone in the use of computer technology. This study uses normative research using a conceptual approach, a comparative approach, and a statutory approach. The results of this study are that the concepts and elements of cyber attack, cyber crime, and cyber warfare have differences. Cyberattack is a method used to carry out attacks using computer technology and the Internet. Cyber crime is a form of crime committed by utilizing computer and internet technology in carrying out crimes. Meanwhile, cyber warfare is a form of cyber operations (cyber operations) in an attack or defense, which is carried out to cause injury or death to people or damage or destruction of the target object or target operation.

Keywords: *cyber crime; cyber warfare; cyber attack.*

ABSTRAK

Pergerakan kegiatan manusia yang semulanya dilakukan secara konvensional berubah menjadi secara digital. Hal ini terjadi juga pada arus lalu lintas informasi. Informasi yang sebelumnya disebarkan secara konvensional berubah menjadi terdigitalisasi. Begitu maraknya pertukaran informasi dan kegiatan di Internet, menjadikan Internet seakan-akan sebagai dunia tersendiri yang tanpa batas. Cyber space sebagai Matra baru layaknya darat, laut, udara, dan ruang angkasa, juga memiliki banyak permasalahan terkait penyalahgunaan teknologi komputer dan internet untuk tujuan yang menyimpang dari norma-norma hukum untuk merugikan pihak lain. Implikasi dari *Cyberattacks* yang memiliki sifat merusak seperti merubah, mengganggu, menutup akses, mengurangi kinerja, atau merusak file komputer, jaringan komputer, atau komputer itu sendiri bila dikaitkan dengan hak dari seseorang dalam pemakaian teknologi komputer. Penelitian ini menggunakan penelitian normative dengan menggunakan pendekatan konseptual, pendekatan komparatif, dan pendekatan perundang-undangan. Hasil dari penelitian ini adalah konsep dan unsur-unsur dari *cyberattack, cyber crime, dan cyber warfare* memiliki perbedaan. *Cyberattack* merupakan metode yang digunakan dalam melakukan serangan dengan menggunakan teknologi komputer dan internet. *Cyber crime* merupakan bentuk tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer dan internet dalam melaksanakan tindak kejahatannya. Sedangkan, *Cyber warfare* merupakan bentuk operasi siber *(cyber operations)* secara menyerang atau bertahan, yang dilakukan dengan tujuan untuk membuat cedera atau kematian orang atau kerusakan atau kehancuran objek sasaran atau target operasi.

Kata Kunci: kejahatan siber; perang siber; serangan siber.

PENDAHULUAN

Konvergensi antara aspek kehidupan manusia dengan perkembangan Internet membuat pergeseran aktifitas dari manusia. Pergerakan kegiatan manusia yang semulanya dilakukan secara konvensional berubah menjadi secara digital. Hal ini terjadi juga pada arus lalulintas informasi. Informasi yang sebelumnya disebarkan secara konvensional berubah menjadi terdigitalisasi.

Informasi yang terdigitalisasi ini beredar pada *Cyberspace*. *Cyberspace* menurut *International Telecomunication Union* (ITU) dari *United Nation* menyatakan bahwa *cyber space* adalah medan *(terrain)* baik yang secara fisik maupun non-fisik yang tercipta dari adanya saling terhubungnya antara komputer, sistem komputer, *network* dan program komputer, data komputer, data konten, lalu lintas data, dan *users* atau pengguna.[1] Berdasarkan pernyataan dari *ITU*, US *Military Document* mendefinisikan *cyber space* sebagai domain global dari berbagai informasi yang terdiri dari jaringan atau *network* yang saling terhubung dengan infrastruktur teknologi informasi, jaringan internet, jaringan telekomunikasi, sistem komputer, serta prosesor.[2]

Cyber space atau dalam bahasa Indonesia disebut sebagai dunia maya yaitu, sebuah domain operasional yang menggunakan elektro dan elektro magnetik, untuk membuat, menyimpan, merubah, serta saling menukar informasi.[3] Begitu maraknya pertukaran informasi dan kegiatan di Internet, menjadikan Internet seakan-akan sebagai dunia tersendiri yang tanpa batas. Internet dapat digunakan siapa saja entah individu, badan usaha, bahkan Negara sekalipun. Dalam hal kenegaraan Internet berfungsi sebagai salah satu sarana untuk melakukan hubungan dengan Negara satu dengan Negara lainnya salah satu contohnya adalah Internet digunakan sebagai sarana untuk melakukan hubungan diplomatik secara jarak jauh. Tidak hanya digunakan untuk sarana melakukan hubungan diplomatik saja, Baru-baru ini dapat dijumpai teknologi Internet digunakan oleh Negara-negara yang bersengketa sebagai jalan lain untuk melancarkan serangan terhadap Negara lawannya secara tidak langsung. *Rebecca Bryant* menyatakan, terdapat 4 (empat) konsep yang ada di dalam *cyber space,*[4] yaitu, *place, distance, size, route.* Place mengandung pertanyaan *"where-type*" atau "di mana" dalam bahasa Indonesia, kata tersebut akan merujuk kepada suatu tempat yang ingin kita ketahui yang mungkin berhubungan dengan hal-hal yang kita cari. Distance pertanyaan yang timbul disini adalah *"how far-type"* atau "seberapa jauh", pertanyaan tersebut menerangkan seberapa jauh jarak dari satu tempat ke tempat lain atau dari tempat anda berdiri menuju ketempat yang akan dituju. Size pertanyaan yang timbul adalah *"how big-type"* atau "seberapa besar", pertanyaan tersebut menerangkan ukuran benda-benda. Route pertanyaan yang timbul berhubungan dengan *"navigation-type",* menerangkan navigasi atau penunjuk jalan maupun arah ke tempat yang dituju.

[1] Shmuel Even dan Daṿid Siman Ṭov, *Cyber Warfare: Concepts and Strategic Trends* (JSTOR, 2012), hal. 10.
[2] Even dan Ṭov, hal. 11.
[3] Daniel T Kuehl, "From Cyberspace To Cyberpower : Defining The Problem," *Cyberpower and national security*, 1 (2009).
[4] Rebecca Bryant, "What kind of space is cyberspace," *Minerva-An Internet journal of philosophy*, 5.2001 (2001), 131–38.

Terdapat 4 (empat) lapisan atau layer di dalam *cyber space*, lapisan pertama adalah *physical layer*, lapisan ini merupakan hal vital yang menjadi pondasi dari *cyber space* yaitu perangkat-perangkat fisik dibangun atau di susun, seperti PC dan *server*nya, supercomputer dengan jaringan listriknya, sensor dengan transdusernya, serta internet dengan berbagai macam jaringan koneksi dan saluran-saluran telekomunikasinya.[5] Kedua adalah *logical layer* yaitu, lapisan atau layer yang berisi perintah-perintah, layanan, dan tempat dimana suatu keputusan dibuat,[6] kemudian lapisan ketiga yaitu *information layer,* tempat dimana informasi-informasi tersedia dan diakses, informasi di dalam dunia maya terdiri dari bermacam-macam bentuk seperti musik dan video, halaman-halaman di dalam world wide web, dan lain-lain.[7] Yang keempat adalah yang berada paling atas *layer people*, yaitu dimana orang-orang sebagai *user*/pengguna *cyber space* berada. Merekalah yang menentukan dan membentuk karakter *cyber space* dengan berbagai cara dengan menggunakan bahasa komputer, tidak akan ada halaman *website* jika tidak ada *user* yang membuatnya yaitu manusia. Jadi, *cyber space* dapat dikatakan sebagai ruang atau *domain* yang memiliki kriteria yang hampir sama dengan ruang atau *domain* yang sudah ada seperti laut, udara, dan daratan, ada unsur manusia, dan ada massa bentuk, ukuran, dan jarak. Dari pernyataan di atas bisa dikatakan bahwa *cyber space* adalah medan baru layaknya darat, laut, udara, dan ruang angkasa.

Cyber space sebagai Matra baru layaknya darat, laut, udara, dan ruang angkasa, juga memiliki banyak permasalahan terkait penyalahgunaan teknologi komputer dan internet untuk tujuan yang menyimpang dari norma-norma hukum untuk merugikan pihak lain. Contoh beberapa penyalahgunaan teknologi komputer dan Internet ini diantaranya, Pada Tahun 2004 menjadi momen pertama Indonesia mengadakan pemilu dengan memanfaatkan Teknologi Telematika. Tim IT Komisi Pemilihan Umum pun meluncurkan situs Komisi Pemilihan Umum yang bernilai 152 miliar rupiah yang dikatakan tidak akan dapat ditembus keamanannya. Pernyataan tersebut justru menantang hacker bernama Xnuxer atau Dani Firmansyah untuk membobol situs tersebut. Awalnya, Xnuxer mencoba meretas dengan melakukan XSS (Cross Site Scripting), yaitu menyuntikkan kode berbahaya ke website KPU tetapi tidak berhasil. Kegagalan ini tidak membuat pelaku ini menyerah. Xnuxer pun mencoba spoofing, yaitu mengalihkan IP website sehingga dia bisa merebut kendali situs. Serangan Xnuxer akhirnya berhasil dan memungkinkannya melakukan SQL Injection (manipulasi kueri SQL). Akibatnya, hacker asal Jogja ini bisa memodifikasi halaman web dan mengubah informasi pada situs KPU. Pada Tahun 2017 Tiket.com dan Maskapai Citilink pernah terkena serangan berupa illegal access pada sistem aplikasi penjualan tiketnya. Hal ini menyebabkan kedua perusahaan ini mengalami kerugian. Pelaku dari serangan ini adalah tiga orang hacker yang dipimpin oleh remaja berumur 19 tahun asal Tangerang. Para pelaku mencuri kode booking tiket penerbangan, kemudian menjual kembali melalui Facebook dengan diskon 30 sampai 40 persen. Kejadian ini membuat

[5] David Clark, "Characterizing Cyberspace: Past, Present And Future," *MIT CSAIL, Version*, 1 (2010), 2016–28.
[6] Clark.
[7] Clark.

perusahaan tiket.com dan Citilink yang menjadi korban mengalami kerugian total sebesar 6 miliyar rupiah.[8]

Selain serangan ditingkat Nasional ada juga serangan siber yang terjadi pada tingkat Internasional. pada bulan Juni 2009. Serangan yang dilancarkan Amerika serikat menggunakan malware jenis virus komputer worm yang terdeteksi dalam sistem komputer Pembangkit listrik tenaga nuklir di Natanz, Iran dengan nama *Stuxnet*. Pada bulan Agustus 2008, terjadi perang antara Rusia dengan Georgia. Perang yang merupakan konflik yang panjang antara kedua negara ini yang melibatkan sektor politik, kultur, dan ekonomi.[9] Meskipun serangan ini sama-sama menggunakan Teknologi komputer dan internet, terdapat perbedaan unsur-unsur yang membuat serangan siber ini masuk dalam kategori hukum yang berbeda, sehingga memerlukan pendekatan dan penyelesaian hukum yang berbeda juga.

Berdasarkan uraian di atas, permasalahan yang akan dikaji dalam artikel ilmiah ini adalah perbedaan dari unsur-unsur *Cyberattack, Cyber crime, dan Cyber warfare* berdasarkan Regulasi-regulasi Internasional.

METODE

Penelitian ini merupakan penelitian normatif dan bersifat doktrinal, menggunakan pendekatan konseptual, pendekatan komparatif, dan pendekatan perundang-undangan. Analisa dilakukan dengan membandingkan unsur-unsur perbuatan berdasarkan sumber-sumber hukum internasional yang berkaitan dengan Telematika, Tindak Pidana Siber, dan Hukum Humaniter Internasional terhadap metode peperangan. Kemudian Konsep-Konsep yang ditemukan nantinya akan dapat digunakan sebagai acuan dalam menentukan dan membedakan unsur-unsur dari peristiwa hukum *Cyberattack* untuk dapat dikategorikan dalam *Cyber Crime* atau *Cyber Warfare.*

PEMBAHASAN

Kebanyakan masyarakat awam tidak sepenuhnya paham, tidak tahu, atau sering kali salah dalam mengartikan istilah *Cyberattack, Cyber crime, dan Cyber warfare.* Hal ini wajar saja, karena bagi masyarakat yang jarang melakukan aktivitas dalam dibidang ini mereka tidak sepenuhnya tahu atau bahkan bagi mereka istilah tersebut sangatlah asing.

Namun masyarakat saat ini harus tahu dan memahami ketiga istilah ini karena pada zaman yang maju seperti saat ini, internet menjadi suatu kebutuhan yang tak kalah penting diberbagai bidang. Sehingga sudah seharusnya masyarakat dan pemerintah di dunia Internasional mengetahui dan memberikan solusi terkait hal tersebut untuk mengantisipasi akan bahaya yang akan muncul ketika seseorang melakukan aktivitas siber *(Cyber).*

[8] Benefita, "7+ Kasus Hacking Menggemparkan Indonesia & Penyebabnya!" <https://www.niagahoster.co.id/blog/kasus-hacking-indonesia/> [diakses 27 Desember 2021].

[9] David Hollis, "SWJ Books | Small Wars Journal," 2008 <https://smallwarsjournal.com/index.php/books> [diakses 27 Desember 2021].

Berikut adalah pembahasan poin-poin penting yang membedakan antara *cyberattack, cybercrime* dan *cyberwarfare* yang ditinjau berdasarkan regulasi-regulasi Internasional:

1) Pemahaman Tentang Konsep *Cyberattack*

Cyberattack atau serangan siber atau juga disebut dengan *Computer Network Attack (CNA)* menurut Wilson adalah[10] *malicious computer code or other deliberate act designed to alter, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.* Perusahaan *digital security Unisys* mendefinisikan, *"cyberattack sebagai A cyberattack is an attempt to disable computers, steal data, or use a breached computer system to launch additional attacks.*[11] Perusahaan Multinasional besar yang bergerak di bidang teknologi yaitu *International Business Machine (IBM)* mendefinisikan, *"cyberattack are unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems."*[12] Sedangkan *American networking system company Cisco system incorporation* mendefinisikan, *"A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network."*[13]

Dari pengertian di atas dapat dikatakan bahwa setiap kegiatan yang dilakukan dengan menggunakan peralatan, jaringan komputer, atau kode komputer yang memiliki sifat merusak dapat digunakan untuk merubah, mengganggu, menutup akses, mengurangi kinerja, atau merusak file komputer, jaringan computer, atau computer dan jaringan computer itu sendiri dilakukan secara sengaja dan melawan hukum dapat dikatakan sebagai *Cyberattacks.*

Implikasi dari *Cyberattacks* yang memiliki sifat merusak seperti merubah, mengganggu, menutup akses, mengurangi kinerja, atau merusak file komputer, jaringan komputer, atau komputer itu sendiri bila dikaitkan dengan hak dari seseorang dalam pemakaian teknologi komputer tersebut jelas merupakan suatu hal yang tidak nyaman dan merupakan sebuah ancaman. Definisi dari ancaman atau *threat* dalam operasi informasi adalah semua jenis ancaman yang mengganggu kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersedian *(availability)* informasi. *Threat* ini bisa berupa ancaman secara fisik yang disengaja dan/atau bencana alam serta ancaman yang muncul dari *cyberattack*.

[10] Clay Wilson, "CRS Report for Congress. Computer attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress," in *Congressional Research Service. The Library of Congress.–2003, October*, 2003, XVII, 35.

[11] "What Is a Cyber Attack? | Cyber Attack Definition | Unisys" <https://www.unisys.com/glossary/cyber-attack/> [diakses 27 Desember 2021].

[12] "What is a cyber attack? | IBM" <https://www.ibm.com/id-en/topics/cyber-attack> [diakses 27 Desember 2021].

[13] "What Is a Cyberattack? - Most Common Types - Cisco" <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html> [diakses 27 Desember 2021].

2) Pengertian *Cyberattack* Dalam *Cyber crimes*

The U.S. Department of Justice memberikan pengertian Computer Crime sebagai : *"… any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution".* Pengertian lainnya diberikan oleh Organization of European Community Development, yaitu: *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data". Artinya "...* Setiap perbuatan melanggar hukum yang memerlukan pengetahuan tentang komputer untuk menangani, menyelidiki, dan menuntutnya". Indra Safitri mengemukakan, kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[14]

Dari pemahaman diatas, aktivitas yang bisa dikategorikan sebagai *Cyber crime*:

1. Tindak kejahatan dimana komputer atau jaringan komputer menjadi target, yang termasuk dalam kategori ini adalah m*alicious code (malware), exploit attacks,* dan *denial of services.*
2. Tindakan kejahatan dimana komputer atau jaringan komputer menjadi alat kejahatan, yang termasuk dalam kategori ini adalah *identity theft, fraud, cyberstalking, dan phising scams*.

Pada tanggal 23 November 2001, 30 negara sepakat untuk menandatangani Budapest *Convention on Cyber crime.* Konvensi ini merupakan kerjasama multilateral yang diadakan guna menanggulangi penyebaran aktivitas kriminal melalui internet dan jaringan komputer lainnya. Melalui kerjasama ini diharapkan dapat menggugah masyarakat Internasional untuk ikut berpartisipasi dalam penanggulangan kejahatan berteknologi tinggi.

Konvensi Budapest tentang cyber crime adalah perjanjian Internasional pertama yang berupaya mencari penyelesaian masalah kejahatan komputer dan kejahatan internet melalui harmonisasi hukum nasional.

Pada *Convention on Cyber crime* (CoC) tidak mendefinisikzn mengenai *Cyberattacks* itu sendiri, yang diatur dalam CoC hanya mengatur unsur-unsur perbuatan yang berupa pelanggaran ataupun perbuatan melawan hukum oleh individu, sekelompok orang, ataupun badan hukum saja. Dalam CoC *Chapter II* menyatakan : *Measures to be taken at the national level,* Hal ini menjelaskan bahwa *CoC* hanya memberikan substansi penting dalam peraturan *Cyber crime* sedangkan untuk unsur-unsur pelaku tindak pidana, negara-negara peserta harus menyesuaikannya sendiri dengan hukum nasional mereka sendiri. Perbuatan-perbuatan yang dianggap sebagai pelanggaran berdasarkan ketentuan Konvensi Budapest ini antara lain adalah :[15]

i. Pengaksesan komputer secara tidak sah (*illegal access)*
ii. Intersepsi sistem komputer secara tidak sah *(illegal interception)*

[14] Abdul Wahid, *Kejahatan Mayantara (Cyber Crime)* (Bandung: Refika Aditama, 2005), hal. 40.
[15] H M Sanusi, *Cyber Crime* (Jakarta: Milestone Publisher, 2011).

iii. Interferensi data *(data interference)*
iv. Interferensi sistem komputer *(system interference)*
v. Penyalahgunaan perangkat komputer *(missuse of device)*
vi. Pemalsuan yang terkait dengan perangkat komputer *(computer-related forgery)*
vii. Penipuan yang terkait dengan komputer *(computer-related fraud)*
viii. Pelanggaran-pelanggaran yang terkait dengan pornografi anak (*offence related to child phornography)*
ix. Pelanggaran-pelanggaran yang terkait dengan hak cipta maupun hal-hal sejenisnya.

3) Pengertian *Cyberattack* Dalam *Cyber warfare*

Definisi dari *Cyberattack* dalam *Cyber warfare* disebutkan pada Tallinn Manual Applicable on the International law to *cyber warfare* (Tallinn Manual) Rule 30-Definition of *Cyberattacks*, yang menyatakan : A *Cyberattacks* 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. Tallinn Manual disusun oleh pakar I.T dan Hukum Eropa akibat adanya serangan cyber di Estonia pada Tahun 2008. Tallinn manual tersebut didaftarkan pada PBB dan disetujui dan diberlakukan sebagai upaya mengatasi kekosongan hukum pada isu hukum *Cyber warfare*.

Rule 30-Definition of *Cyberattacks* dari Tallinn Manual mengadopsi dari Additional Protocol I On Geneva Convention And Relating To The Protection Of Victims Of International Armed Conflicts article 49 (1). *Cyberattack* dari *Cyber warfare* merujuk atau mengacu pada peperangan yang dilakukan melalui Dunia Maya (Cyber) dan dikoordinasikan dengan perang konvensional, sementara perang yang umumnya dipahami adalah perang yang mengacu pada suatu konflik bersenjata.[16] *Cyber warfare* dapat melibatkan organisasi-organisasi, perusahaan, dan militer dalam melakukan atau mencoba melakukan perusakan atau menyerang sistem komputer negara lain atau pihak lain. Cyber warfare itu sendiri menurut Tallinn Manual Rule 41- Definition of Means and Methods of Warfare For the purpose of this Manual : *(a) 'means of cyber warfare' are cyber weapons and their associated cyber system; (b) 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conduucted.*

Dalam hukum Humaniter Internasional, terdapat 3 pihak yang terkait dalam peperangan, yaitu : Kombatan, non-kombatan, dan sipil. Pelaku dalam *Cyber warfare*, orang yang turut dalam konflik secara langsung termasuk dalam kategori kombatan. Dalam Tallinn manual peserta perang aktif (kombatan), diatur dalam Chapter IV section 1 : Participation in Armed Conflict. Istilah kombatan hanya berlaku untuk konflik kekerasan bersenjata secara Internasional. Dijelaskan dalam Tallinn Manual Rules 25 (1): *The customary international law of armed conflict does not prohibit any individual from participating in an armed conflict, whether international or non-international. It should be noted that Article 43(2) of Additional Protocol I provides that "members of*

[16] N Melzer, "Cyberwarfare And International Law. UNIDIR Resources," *UN Institute for*, 2011.

the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of Geneva Convention III) are combatants, that is to say they have the right to participate directly in hostilities". This provision, applicable in international armed conflict, confirms that combatants enjoy immunity in respect of the acts undertaken as part of the hostilities. It does not prohibit others from engaging in those hostilities.

Adopsi dari *Additional Protocol I On Geneva Convention And Relating To The Protection Of Victims Of International Armed Conflicts article 43 (2)* yang menyatakan : *Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.* Penyesuaian terhadap pelaksanaan *International law of armed conflict* tidak melarang setiap Individu untuk berpartisipasi dalam kekerasan bersenjata. Sehingga pihak sipil diperbolehkan ikut serta dalam peperangan secara langsung. Tetapi pihak sipil yang ikut serta akan mendapatkan status kombatan dan akan mendapatkan hak-hak kombatan karena akan diakui sebagai kombatan. Hak-hak kombatan yang dimaksud dalam *Tallinn manual diatur dalam Rule 25 (2)* tersebut adalah :

1. *Combatant immunity*
2. *Prisoner of war*
3. *Targetability*

Pihak sipil yang secara langsung berpartisipasi akan kehilangan status sebagai Civilian dan hak-haknya terhadap perlindungan warga sipil. Dalam *Tallinn Manual Rule 26 (4)* menjelaskan ada 2 kategori kombatan yaitu : militer dan corps sukarela dan pasukan perlawanan lainnya. Dijelaskan dalam *geneva convention article 4 (2),* militer adalah angkatan bersenjata pihak (negara) yang berperang. Sedangkan gerakan perlawanan yang dapat dikategorikan sebagai kombatan ada 4 yaitu :

(a) dipimpin oleh seorang yang bertanggung jawab atas bawahannya,
(b) mempunyai tanda pengenal tetap yang dapat dikenal dari jauh,
(c) membawa senjata secara terang-terangan, dan
(d) melakukan operasi mereka sesuai dengan hukum-hukum dan kebiasaan perang.

Jadi *Cyberattack* yang dapat dikategorikan sebagai *Cyber warfare* apabila pelakunya memenuhi kriteria di atas menurut para ahli hukum dan ahli T.I menyatakan bahwa gerakan perlawanan dapat dikatakan sebagai kombatan apabila telah memenuhi kriteria di atas mereka tergabung dalam pasukan militer sehingga dapat diartikan sebagai member dari angkatan bersenjata tersebut.

Dari pengertian-pengertian di atas, apabila pelaku tidak memenuhi syarat-syarat sebagai kombatan dan tindak kejahatan hanya dilakukan oleh individu maupun badan hukum dan tidak memiliki struktural dan koordinasi yang sangat kompleks seperti dalam halnya persyaratan sebagai kombatan atau subyek dan obyek tindakan tidak memenuhi syarat kombatan dan termasuk sipil maka pelaku tersebut dikategorikan sebagai pelaku *Cyber crime*.

Peraturan yang mengatur antara *Cyber warfare* dan *Cyber crime* itu sendiri jelas berbeda. Dalam lingkup Internasional yang digunakan dalam mengatur *Cyber warfare* adalah *Tallinn Manual on International Law applicable to cyber warfare* yang dibuat oleh pakar I.T dan Hukum Eropa akibat adanya serangan *cyber* di Estonia. *Tallinn* manual tersebut didaftarkan pada PBB dan disetujui dan diberlakukan sebagai hukum Internasional yang mengatur tentang *Cyber warfare*. Regulasi *Cyber crime* pada hukum Internasional yang dapat diberlakukan sebagai *legal framework* adalah *Budhapest Convention on Cyber crime* yang setelah disahkan banyak diikuti oleh negara-negara lain bahkan yang tidak meratifikasinya sekalipun.

SIMPULAN

Berdasarkan pembahasan di atas, dapat disimpulkan bahwa konsep dan unsur-unsur dari *cyberattack, cyber crime, dan cyber warfare* berdasarkan regulasi Internasional memiliki perbedaan. *Cyberattack* merupakan metode yang digunakan dalam melakukan serangan dengan menggunakan teknologi komputer dan internet. *Cyber crime* merupakan bentuk tindak pidana yang dilakukan dengan memanfaatkan teknologi komputer dan internet dalam melaksanakan tindak kejahatannya. Sedangkan, *Cyber warfare* merupakan bentuk operasi siber *(cyber operations)* secara menyerang atau bertahan, yang dilakukan dengan tujuan untuk membuat cedera atau kematian orang atau kerusakan atau kehancuran objek sasaran atau target operasi. *Cyberattacks* merupakan istilah terhadap metode penyerangan dengan memanfaatkan teknologi komputer internet sehingga dapat disimpulkan pada *cyber crime* dan *cyber warfare* dalam operasionalnya menggunakan *cyberattack*. Perbedaan diantara ketiga konsep ini harus dipahami karena ketiganya mengacu kepada aspek hukum yang berbeda sehingga dalam penanganan kasusnya harus menggunakan pendekatan perspektif hukum yang berbeda pula.

REFERENSI

Benefita, "7+ Kasus Hacking Menggemparkan Indonesia & Penyebabnya!" <https://www.niagahoster.co.id/blog/kasus-hacking-indonesia/> [diakses 27 Desember 2021]

Bryant, Rebecca, "What kind of space is cyberspace," *Minerva-An Internet journal of philosophy*, 5.2001 (2001), 131–38

Clark, David, "Characterizing Cyberspace: Past, Present And Future," *MIT CSAIL, Version*, 1 (2010), 2016–28

Even, Shmuel, dan Daṿid Siman Ṭov, *Cyber Warfare: Concepts and Strategic Trends* (JSTOR, 2012)

Hollis, David, "SWJ Books | Small Wars Journal," 2008 <https://smallwarsjournal.com/index.php/books> [diakses 27 Desember 2021]

Kuehl, Daniel T, "From Cyberspace To Cyberpower : Defining The Problem," *Cyberpower and national security*, 1 (2009)

Melzer, N, "Cyberwarfare And International Law. UNIDIR Resources," *UN Institute for*, 2011

Sanusi, H M, *Cyber Crime* (Jakarta: Milestone Publisher, 2011)

Wahid, Abdul, *Kejahatan Mayantara (Cyber Crime)* (Bandung: Refika Aditama, 2005)

"What Is a Cyber Attack? | Cyber Attack Definition | Unisys" <https://www.unisys.com/glossary/cyber-attack/> [diakses 27 Desember 2021]

"What is a cyber attack? | IBM" <https://www.ibm.com/id-en/topics/cyber-attack> [diakses 27 Desember 2021]

"What Is a Cyberattack? - Most Common Types - Cisco" <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html> [diakses 27 Desember 2021]

Wilson, Clay, "CRS Report for Congress. Computer attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress," in *Congressional Research Service. The Library of Congress.–2003, October*, 2003, XVII, 35