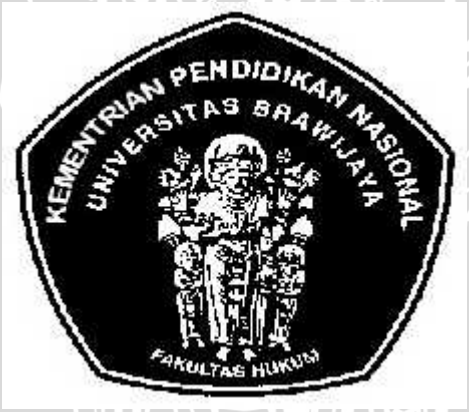
SKRIPSI

TINJAUAN MENGENAI *CYBER WARFARE* BERDASARKAN HUKUM HUMANITER INTERNASIONAL (STUDI KASUS PERANG ANTARA RUSIA DENGAN GEORGIA PADA 7 AGUSTUS 2008)

SKRIPSI

Untuk Memenuhi sebagian Syarat- syarat
Untuk Memperoleh Gelar Kesarjanaan
Dalam Ilmu Hukum

Oleh:
IVAN HILMI ALVIANTO
NIM. 0910110180



KEMENTRIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS BRAWIJAYA
FAKULTAS HUKUM
MALANG
2013

LEMBAR PERSETUJUAN

Judul Skripsi	**: TINJAUAN CYBER WARFARE BERDASARKAN HUKUM HUMANITER INTER NASIONAL (STUDI KASUS PERANG ANTARA RUSIA DENGAN GEORGIA PADA 7 AGUSTUS 2008**
Identitas Penulis	**:**
a. Nama	**: Ivan Hilmi Alvianto**
b. NIM	**: 0910110180**
Konsentrasi	**: Hukum Internasional**
Jangka Waktu Penelitian	**: 6 bulan**

Disetujui pada tanggal:

Pembimbing Utama	Pembimbing Pendamping
Setyo Widagdo, SH. MHum	Ikaningtyas,SH. LLM
NIP. 19590320 198601 1 003	NIP.19810531 2000501 2 002

Mengetahui,

Ketua Bagian

Hukum Internasional

Nurdin, SH. MHum

NIP. 19561207 198601 1 001

LEMBAR PENGESAHAN

TINJAUAN MENGENAI *CYBER WARFARE*

BERDASARKAN HUKUM HUMANITER INTERNASIONAL

(STUDI KASUS PERANG ANTARA RUSIA DENGAN GEORGIA PADA 7 AGUSTUS 2008)

Oleh :

IVAN HILMI ALVIANTO

0910110180

Skripsi ini telah disahkan oleh Majelis Penguji pada tanggal : ……..

Ketua Majelis Penguji	Anggota
Nurdin, SH., MH.	Setyo Widagdo, SH., MH.
NIP. 19561207 198601 1 001	NIP. 19590320 198601 1 003
Anggota	Anggota
Sucipto, SH., MH.	Dr. Dhiana Puspitawati, SH., LLM.
NIP. 19501211 198010 1 001	NIP. 19740603 201012 2 001
Anggota	Ketua Bagian Hukum Internasional
Ikaningtyas, SH., LLM.	Nurdin, SH., MH.
NIP. 19810531 200501 2 002	NIP. 19561207 198601 1 001

Mengetahui

Dekan Fakultas Hukum

Dr. Sihabudin, SH., MH.

NIP. 19591216 198503 1001

KATA PENGANTAR

Segala puji penulis panjatkan hanya kehadirat Tuhan Yang Maha Kuasa yang telah memberikan rahmat dan karunia yang tiad henti hingga penulis dapat sampai pada tahap ini, khususnya dengan selesainya skripsi ini.

Terima ksih penulis sampaikan kepada :

1. Bapak Setyo Widagdo, SH. MHum selaku Dosen Pembimbing Utama, atas bimbingannya.
2. Ibu Ikaningtyas, SH. L.L.M selaku Dosen Pembimbing Pendamping, atas bimbingan dan kesabarannya
3. Saudara Rizwan dan teman-teman yang lainnya, atas semua saran dan bantuannya
4. Kepada komputer saya

Penulis yakin skripsi ini masih sangat jauh dari kata sempurna, sehingga masukan dan kritik akan selalu penulis harapkan untuk memperbaiki skripsi ini.

Akhir kata penulis mohon maaf yang sebesar-besarnya jika dalam proses pembuatan skripsi ini melakukan kesalahan baik yang disengaja maupun tidak disengaja.

Semoga Tuhan Yang Maha Esa mengampuni kesalahan kita dan berkenan menunjukkan jalan yang benar.

Malang, July 2013

Penulis

DAFTAR ISI

ABSTRAKSI

IVAN HILMI ALVIANTO, Hukum Internasional, Fakultas Hukum Universitas Brawijaya, Juli 2013, *Tinjauan Mengenai Cyber Warfare Berdasarkan Hukum Humaniter Internasional (Studi Kasus Perang Antara Rusia dengan Georgia Pada 7 Agustus 2008)*, Setyo Widagdo, SH. MHum.; Ikaningtyas, SH.LLM.

Skripsi ini membahas tentang tinjauan mengenai cyber warfare berdasarkan hukum humaniter internasional. Hal ini dilatar belakangi oleh adanya *cyber warfare* atau peperangan cyber yang dilakukan oleh Negara maju terhadap Negara lain, dimana hal tersebut dilakukan untuk menghancurkan infrastruktur yang terkomputerisasi. Pada tanggal 7 Agustus 2008 terjadi *cyber warfare* yang dilakukan oleh Rusia dengan Georgia dalam hal ini, *cyber warfare* yang terjadi telah membuat website-website penting dan infrastruktur internet milik Georgia tidak dapat berfungsi. Permasalahan yang di angkat adalah bagaimana pengaturan *cyber warfare* berdasarkan prespektif dari hukum humaniter internasional dan bagaimana penerapan aturan-aturan dalam hukum humaniter internasional di terapkan dalam kasus *cyber warfare* yang terjadi di Georgia dalam perang antara Rusia dengan Georgia. Penelitian ini menggunakan jenis penelitian Yuridis Normatif, dengan pendekatan *case approach, conceptual approach* dan *statuta approach.*

Dari hasil analisis yang dilakukan maka dapat diketahui bahwa, hukum humaniter internasional dapat diterapkan dalam *cyber warfare,* dengan melihat pada dampak atau akibat yang ditimbulkan, dan unsur-unsur yang sama dengan perang konvensional pada umumnya. Mengenai penerapan hukum humaniter di dalam kasus cyber warfare antara Rusia dengan Georgia diketahui bahwa, StopGeorgia.ru dapat di kualifikasikan sebagai kombatan karena, mereka telah terorganisir di bawah kepemimpinan dari Maksim Zharov. Namun, serangan cyber yang dilakukan oleh Rusia tidak sesuai dengan prinsip-prinsip pembedaan maupun proporsionalitas karena, melakukan serangan terhadap website umum atau publik.

Kesimpulan dari skripsi ini adalah prinsip-prinsip yang terdapat di dalam prinsip hukum humaniter internasional yang terdapat di dalam sumber hukumnya dapat diterapkan dalam *cyber warfare*. Saran dari penulis adalah perlunya untuk melakukan kerjasama antara para ahli teknologi dan informasi serta para ahli hukum internasional khususnya hukum humaniter dalam mengkaji *cyber warfare,* serta melakukan sosialisasi dan peningkatan status *Tallinn Manual* sebagai sumber hukum internasional dalam hal *cyber warfare.*

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi yang cukup pesat belakangan ini memunculkan istilah yang disebut *cyberspace* atau di dalam bahasa Indonesia disebut sebagai dunia maya yaitu, sebuah domain operasional yang menggunakan elektro dan elektromagnetik, untuk membuat, menyimpan, memodifikasi, serta saling menukar informasi.[1] *Cyberspace* kemudian melahirkan infrastruktur-infrastruktur dalam suatu Negara yang terkomputerisasi dan saling terhubung satu sama lain, hal inilah yang kemudian memunculkan pihak-pihak yang mempunyai tujuan negatif (*hacker* dan *cracker)* yaitu untuk mengacaukan sistem dari infrastruktur yang terkomputerisasi,[2] namun pihak-pihak tersebut bukan lagi sebagai individu melainkan negara yang kemudian disebut sebagai *cyberattack*.

Cyberattack di latar belakangi oleh hal-hal bersifat politik, dan ada suatu unsur perintah yang resmi dari pemerintah suatu negara dengan kata lain melegalkan dan mendukung serta memfasilitasi. *Cyberattack* yang baru-baru ini terjadi, antara USA v Iran dimana adanya keinginan pihak USA untuk menghentikan atau menggagalkan

[1] Kuehl, Dan, ***From Cyberspace to Cyberpower: Defining the Problem***, Information Operations at the National Defense University, USA, www.carlisle.army.mil/DIME/documents/ (20 Februari 2013)

[2] Merupakan kata serapan dari kata computerize, yang artinya *provide a computer to do the work of something*, menggunakan atau penyediaan komputer untuk melakukan suatu pekerjaan

proyek nuklir Iran, dengan mengirimkan *virus* yang diberi nama *Stuxnet*.[3] Timbul masalah lain ketika *cyberattack* mulai di nilai dapat memberikan keuntungan-keuntungan militer, dan di koordinasikan dengan konflik bersenjata atau peperangan sebagaimana telah diatur dalam hukum humaniter internasional, yang kemudian merubah *cyberattack* menjadi *cyber warfare*.[4] Inilah permasalahan yang akan diangkat oleh penulis.

Ketika pada bulan Agustus 2008, terjadi perang antara Rusia dengan Georgia. perang yang merupakan representasi konflik yang panjang antara kedua negara ini yang melibatkan sektor politik, kultur, dan ekonomi. Di mulai dengan perdebatan argumentasi selama beberapa minggu mengenai masa depan wilayah Osettia Utara yang mengalami jalan buntu.[5] Ossetia Utara merdeka secara *de facto* dari Georgia sekitar tahun 1991, saat terjadinya konflik dengan Georgia.[6] Namun, ketika itu masyarakat internasional masih mengakui Ossetia Utara sebagai bagian yang tak terpisahkan dari Georgia.[7]

Adanya pembentukan pasukan perdamaian di tahun 1992 yang melibatkan angkatan bersenjata dari Rusia, Georgia, dan Ossetia Utara yang di nilai gagal, membuat ketegangan antara Rusia dengan Georgia semakin memuncak. Pada 7 Agustus 2008, Georgia yang di dukung dan di provokasi oleh pihak separatis yang Pro Georgia, melancarkan serangan militer yang di tujukan pada pasukan separatis yang dalam hal ini Kontra Georgia dan Pro terhadap Rusia, yang kemudian direspon oleh pihak Rusia

[3] Sanger , David. E., 2012, ***Obama Order Sped Up Wave of Cyberattacks Against Iran***, The New York Times: Middle East, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against iran.html?_r=2& (18 Desember 2012)

[4] The Economist, 2008, ***Marching off to cyberwar***, The internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with “cyberwar”, http://www.economist.com/node/12673385 (29 September 2012)

[5] Hollis, David, ***Cyber War Case Study: Georgia 2008***, Small Wars Journal, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 (29 September 2012)

[6] Tikk, Eneken, 2008, ***Cyber Attacks Against Georgia: Legal Lessons Identified***, Cooperative Cyber Defense Center of Exellence, hal.4

[7] Tikk, Eneken, *Loc.Cit*, hal. 4

dengan melakukan operasi militer di wilayah teritorial Georgia. Sebelum hari dimana operasi militer atau perang konvensional tersebut dimulai, *cyberattack* telah dilakukan terhadap website-website milik Georgia.[8] Tercatat 54 website yang berhubungan dengan komunikasi, keuangan, dan pemerintahan diserang oleh pihak Rusia.[9]

Penyerangan dengan metode *Distributed Denial of Service (DDoS)*[10] yang diarahkan pada website dengan alamat *www.president.gov.ge*, yaitu website dari Presiden Georgia Mikheil Saakasvili, kemudian *www.nbg.gov.ge,* yaitu website dari bank nasional Georgia, dan yang terakhir adalah *www.mfa.gov.ge*, yaitu website dari menteri luar negeri Georgia.[11] Website yang berkaitan dengan sektor privat dan publik juga ikut diserang, *www.forum.ge* (merupakan forum terbesar di Georgia), *www.civil.ge* (halaman berita Georgia dalam bahasa Inggris), *www.presa.ge* (website dari Asosiasi Press Georgia), dan *www.hacking.ge* (website dari perkumpulan hacker Georgia).[12]

Data statistik penyerangan yang dirilis oleh *Arbor Network*, menunjukan bahwa intensitas dari serangan tersebut sangat tinggi dengan *traffic data* atau jalur data yang rata-rata mencapai 211,66 Mbps (*megabyte per second*), dan pada titik maksimum mencapai 814,33 Mbps (*megabyte per second*). Durasi dari serangan tersebut rata-rata adalah sekitar 2 jam 15 menit, dan yang terlama adalah 6 jam.[13] Beberapa blog, forum, dan website Rusia, telah menyebarkan sebuah *Microsoft Windows batch script* yaitu

---

[8] Tikk, Eneken, *Loc.Cit*, hal. 4

[9] Hollis, David, *Op.cit*

[10] DDoS merupakan perkembangan dari DoS yaitu, adalah aktifitas yang bertujuan untuk menghambat kerja sebuah layanan (*service*) atau mematikannya, sehingga user yang berhak atau yang berkepentingan tidak dapat menggunakan layanan tersebut, lebih lengkapnya akan dijelaskan dalam kajian pustaka

[11] Tikk, Eneken, *Op.cit* hal 7.

[12] *Ibid*, hal 8.

[13] Nazario, J., 2008, ***Georgia DDoS Attacks - A Quick Summary of Observations***, Arbor Network, asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/, yang dikutip oleh Tikk, Eneken, 2008, *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defense Center of Exellence, hal. 9

sebuah file yang berekstensi .BAT yang berisi perintah-perintah untuk mengerjakan tugas tertentu, yang di desain untuk menyerang website-website milik Georgia, adapun file tersebut diberi nama *"war.bat"*. [14] Selain itu serangan juga diarahkan pada e-mail milik politisi Georgia dengan metode *spamming.*

Berdasarkan penelitian dari *Swedish National Defence University*,[15] dan di dukung oleh *Shadowserver* menyatakan bahwa, *stopgeorgia.ru* yang juga diketahui sebagai *stopgeorgia.info* menyediakan alat-alat atau *software DDoS* untuk di unduh yang kemudian dapat digunakan untuk melakukan penyerangan, yang di indikasi target dari serangan tersebut adalah website-website atas nama Georgia *(.ge). The Project Grey Goose,*[16] menyatakan bahwa sulit untuk menemukan bukti yang cukup untuk menentukan asal penggalangan atau *guiding* dari serangan *cyber* tersebut karena, adanya organisasi-organisasi pemerintahan Rusia yang sengaja menghindari dan menutupinya.

Dalam kasus sebelumnya yang juga melibatkan pihak Rusia, yaitu kasus *cyber attack* yang di tujukan kepada Estonia, di picu karena adanya pemindahan monumen patung perak simbol penghargaan atau untuk mengenang mereka yang gugur dalam perang antara Uni Soviet melawan pasukan NAZI Jerman. Namun dalam kasus ini masih ada kepedulian atau toleransi dari pihak Rusia untuk mengusutnya, karena memang pihak

---

[14] Tikk, Eneken, *Loc.Cit*, hal. 9

[15] Berdasarkan E-mail yang diterima dari *Swedish Defence University with preliminary conclusions on 'Cyberattack against Georgia'*. Yang di publikasikan oleh Tikk, Eneken, 2008, ***Cyber Attacks Against Georgia: Legal Lessons Identified***, Cooperative Cyber Defense Center of Exellence, hal 10

[16] *Project Grey Goose* adalah sukarelawan yang terdiri dari para ahli Informasi dan Teknologi, yang di pimpin oleh Jeff Carr dari *IntelFusion* yang bekerjasama dengan Palantir Technologies, yang bertujuan untuk mengetahui aktivitas *cyber* antara Rusia dengan Georgia, *www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I- Report,* (20 Februari 2013)

Rusia menyatakan tidak mengkoordinasikan atau melakukan hal-hal yang bersifat mendukung serangan tersebut.[17]

Melihat akibat efek dari *cyber warfare* yang terjadi di Georgia, berdasarkan data dari CERT-EE, dua penyedia utama layanan internet di Georgia yaitu, *United Telecom of Georgia* dengan router jenis Cisco 7206 yang tidak dapat menyediakan pelayanan selama beberapa hari, kemudian *Caucasus Network Tbilisi*[18] yang telah di banjiri *(flooded*[19]*)* secara besar-besaran dengan berbagai *queries*.[20] Hal tersebut seolah-olah telah membuat infrastruktur *Caucasus Network* telah masuk dalam zona perang dan telah menjadi sasaran atau target, yang mengakibatkan *physical disconnections*.[21] Lebih dari itu tidak dapat di aksesnya atau tidak tersedianya website-website yang penting bagi pemerintah Georgia, karena akibat dari serangan *DoS* dan *DDoS*, telah melumpuhkan komunikasi serta informasi baik yang bersifat internasional dan nasional.

Berdasarkan hukum humaniter internasional, serangan atau *attack* akan selalu menimbulkan sebuah akibat baik secara fisik *(physically)* maupun mental *(mentally)*, namun serangan tersebut juga terkait dengan domain-domain atau wilayah-wilayah yang telah di akui dalam hukum humaniter internasional, seperti darat *(land)*, laut *(sea)*, dan udara *(air)*. Secara keseluruhan *cyber warfare* terjadi dalam suatu ruang yang disebut sebagai *cyberspace* atau dunia maya, mengacu pada kasus diatas, ketika negara dalam

---

[17] BBC News, 25 Januari 2008, ***Estonia fines man for 'cyber war'*** , http://news.bbc.co. uk/2/hi /technology/7208511.stm (22 Februari 2013)

[18] *Caucasus Network Tbilisi* adalah perusahaan penyedia layanan internet di Georgia sama halnya dengan *United Telecom of Georgia*, jika di Indonesia sama dengan Telkom Speedy

[19] *Flooded* adalah salah satu teknik routing sederhana dalam jaringan komputer yang cara kerjanya adalah dengan mengirimkan paket-paket data melalui link-link yang telah ditargetkan, flooded merupakan bagian dari metode *Distributed Denial of Services* (DDoS)

[20] Berasal dari kata *query*, di dalam dunia komputer dan jaringan query merupakan pertanyaan atau permintaan terhadap informasi tertentu dari sebuah basis data yang ditulis dalam format tertentu, query identik dengan manipulasi database yang kemudian di standarkan menjadi *Structured Query Language* (SQL)

[21] Danchev, Dancho, 2008, *"**Coordinated Russia vs Georgia**"*, http://www.zdnet.com/blog /security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (22 Februari 2013)

keadaan konflik *(state of war)* maka, informasi dan komunikasi merupakan hal yang utama bagi seluruh masyarakat negara tersebut, ketika informasi dan komunikasi lumpuh, akan timbul kekacauan dan timbul keadaan yang dapat membuat orang kehilangan semuanya bahkan nyawa.

Kemudian *cyber warfare* akan di hadapkan pada *indiscrimate attack* karena serangannya yang tidak dapat membedakan, dan yang lebih penting lagi adalah *distinction principles* atau prinsip pembedaan yang harus diterapkan terkait dengan sebuah serangan baik yang terkait dengan targetnya dan pelakunya. Secara keseluruhan *cyber warfare* menimbulkan domain perang atau domain konflik yang baru, serta sarana dan metode berperang yang baru. Akan tetapi, hal-hal tersebut diatas menimbulkan pertanyaan bagaimana konsepsi *cyber warfare* jika di dasarkan pada perspektif hukum humaniter internasional, dan yang terakhir bagaimana penerapan prinsip dan aturan yang ada di dalam hukum humaniter internasional di terapkan dalam kasus tersebut.

Berdasarkan uraian diatas maka penulis merasa perlu untuk dilakukannya penulisan mengenai ***Tinjauan Mengenai Cyber Warfare Berdasarkan Hukum Humaniter Internasional (Studi Kasus Perang Antara Rusia dengan Georgia pada 7 Agustus 2008).***

B. RUMUSAN MASALAH.

1. Bagaimana pengaturan *cyber warfare* berdasarkan prespektif dari hukum humaniter internasional?

2. Bagaimana penerapan aturan-aturan dalam hukum humaniter internasional di terapkan dalam kasus *cyber warfare* yang terjadi di Georgia dalam perang antara Rusia dengan Georgia ?

C. TUJUAN PENULISAN.

1. Untuk mengetahui dan menganalisis konsepsi *cyber warfare* berdasarkan prespektif dari hukum humaniter internasional.
2. Untuk mengetahui dan menganalisis penerapan aturan-aturan dalam hukum humaniter internasional diterapkan dalam kasus *cyber warfare* yang terjadi di Georgia dalam perang antara Rusia dengan Georgia.

D. MANFAAT PENULISAN.

Adapun manfaat dari penelitian ini adalah:

1) Manfaat Teoritis.

Sebagai pengembangan ilmu untuk memberikan pemahaman secara teoritis mengenai *Cyber Warfare* yang ditinjau berdasarkan hukum humaniter internasional.

2) Manfaat Praktis.

a) Bagi masyarakat internasional, agar dapat menindak lanjuti dan menerapkan hukum internasional sebagai mana mestinya terhadap sarana dan metode konflik bersenjata yang baru dalam hukum humaniter internasional.

b) Bagi akademisi, untuk dijadikan referensi dalam mempelajari serta memahami hukum humaniter internasional khususnya mengenai *cyber warfare* ini

c) Bagi pemerintah Indonesia, untuk dapat turut serta melakukan pengkajian terhadap sarana dan metode berperang yang baru seperti *cyber warfare*.

d) Bagi peneliti, untuk dapat dijadikan Referensi dalam mengkaji masalah yang sama dimasa yang akan datang.

e) Sebagai tambahan wawasan dan ilmu pengetahuan bagi penulis khususnya dalam hukum humaniter internasional dan *cyber warfare.*

BAB II

KAJIAN PUSTAKA

A. *Cyberspace*

Istilah *cyberspace* menurut terjemahan dari *freedictionary* adalah suatu jaringan yang bersifat global yang berbentuk infrastruktur teknologi informasi dan saling terhubung antara satu dengan yang lain dan menjadi tempat dimana komununikasi secara *online* terjadi. *Cyberspace* sebenarnya merupakan istilah yang tercipta dari sebuah novel yang berjudul *Cyberpunk* yang merupakan karya dari novelist William Gibson.

International Telecomunication Union (ITU) dari *United Nation* menyatakan bahwa *cyberspace* 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.[22] Berdasarkan pernyataan dari ITU, US *Military Document* mendefinisikan *cyberspace* 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.[23]

Menurut Rebecca Bryant, terdapat 4 (empat) konsep yang ada di dalam *cyberspace,* yaitu;[24]

---

[22] Even, Shmuel, and Siman-Tov, David, 2012, ***Cyber Warfare: Concepts and Strategic Trends***, Institute For National Security Studies, hal. 10

[23] *Ibid*, hal. 11

[24] Bryant, Rebecca, 2001, ***What Kind of Space is Cyberspace?***, Minerva-An Internet Journal of Philosophy, hal. 141

1. *Place* (tempat)
2. *Distance* (jarak)
3. *Size* (ukuran)
4. *Route* (arah atau navigasi)

Konsep yang pertama yaitu *place*, mengandung pertanyaan "*where-type*" atau "dimana" dalam bahasa Indonesia, kata tersebut akan merujuk kepada suatu tempat yang ingin kita ketahui yang mungkin berhubungan dengan hal-hal yang kita cari, yang kedua adalah *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 di tuju. Yang ketiga adalah *size* atau ukuran, pertanyaan yang timbul adalah "*how big-type*" atau "seberapa besar", pertanyaan tersebut menerangkan ukuran benda-benda, yang keempat adalah "*route*" berhubungan dengan "*navigation-type*", menerangkan navigasi atau penunjuk jalan maupun arah ke tempat yang dituju.

Terdapat 4 (empat) lapisan atau layer di dalam *cyberspace*, lapisan yang pertama adalah *physical layer*, lapisan ini merupakan pondasi dari *cyberspace* yaitu tempat dimana perangkat-perangkat fisik dibangun atau di susun, seperti PC dan servernya, supercomputer dengan jaringan listriknya, sensor dengan transdusernya, serta internet dengan berbagai macam jaringan dan saluran-saluran telekomunikasinya.[25] Yang kedua adalah *logical layer* yaitu, lapisan atau layer yang berisi perintah-perintah, layanan, dan tempat dimana suatu keputusan dibuat,[26] kemudian yang 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

[25] Clark, David, 2010, ***Characterizing cyberspace: past, present and future***, MIT CSAIL, hal 2
[26] Clark, David, *Loc.Cit*, hal 2

world wide web, dan lain-lain.[27] Yang keempat adalah top *layer people*, yaitu dimana orang-orang sebagai pengguna *cyberspace* berada. Merekalah yang menentukan dan membentuk karakter *cyberspace* dengan berbagai cara, tidak akan ada halaman website jika tidak ada yang membuatnya yaitu manusia, tidak ada *tweet* yang dilakukan orang-orang dalam jejaring sosial *Twitter*, maka twitter mungkin juga tidak akan ada.[28]Jadi, *cyberspace* 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.

B. *Cyber Warfare*

a. Definisi

Cyber Warfare merujuk atau mengacu pada peperangan yang dilakukan melalui Dunia Maya (*Cyber*) dan dikordinasikan dengan perang konvensional, sementara perang yang umumnya dipahami adalah perang yang mengacu pada suatu konflik bersenjata.[29] *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 biasa menggunakan alat-alat yang berhubungan dengan komputer baik yang merupakan *software* atau yang berupa *hardware*, alat-alat tersebut biasa di sebut sebagai senjata *cyber* (*Cyber Weapon*).[30] Di dalam *cyber warfare* sendiri, terdapat

---

[27] *Ibid*, hal 3
[28] *Ibid*, hal 4
[29] Nils Melzer, 2011, ***Cyber Warfare and International Law***, UNIDIR. RESOURCES. IDEAS FOR PEACE AND SECURITY, unidir.org/pdf/activites/pdf2-act649.pdf *(20 Oktober 2012)*
[30] SECPOINT, *What is Cyberwarfare?*, http://www.secpoint.com/what-is-cyberwarfare.html (20 Oktober 2012)

metode *(methods)* serangan atau menyerang (*Methods of Attack*) dan metode bertahan (*Methods of Defense*).

b. *Methods of attack* di dalam *cyber warfare*

Terdapat banyak cara untuk melakukan penyerangan terhadap sistem komputer namun di sini hanya akan di paparkan beberapa cara atau media umum yang digunakan dalam *cyber warfare* yaitu[31]:

a) *Malware (Malicious Software)*

Pada dasarnya *malware* adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma[32] yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji *malware* sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.[33] Namun, pengertian tersebut berkembang menjadi software yang digunakan untuk mengganggu pengoperasian komputer, mengumpulkan informasi-informasi yang bersifat rahasia dan sensitif, atau masuk dan mengambil alih sistem komputer pribadi.

Terdapat beberapa jenis *malware* yang umum dikenal dan sering menyerang sistem komputer seperti *Virus, Worm, Trojan Horse, Backdoors, Keystroke Logger, rootkit* atau *Spyware*. Adapun definisinya adalah sebagai berikut:

---

[31] Chad Nelson, ***Cyber Warfare: The Newest Battlefield***, Washington University in St. Louis, http:// www.cse.wustl.edu/~jain/cse571-11/ftp /cyberwar.pdf (20 Oktober 2012)

[32] Menurut Sutrisno dan kawan-kawan dari Teknik Informatika UB, dalam presentasi mengenai Dasar-Dasar Pemrograman dan Pengantar Algoritma (*online*), Algoritma diambil dari ilmuwan yang berasal dari Persia yaitu Al Khawarizmi, menurutnya algoritma adalah sekumpulan instruksi atau langkah-langkah yang jelas, dalam pemrogaman komputer, algoritma berarti satu set instruksi atau langkah-langkah yang dijalankan dengan komputer untuk menyelesaikan suatu masalah, iaknuranda.lecture.ub.ac.id/files/2011/10/DPK-PengantarAlgoritma-IA-UB.ppt, (19 Februari 2013)

[33] Prof. Richardus Eko Indrajit, **Analisa Malware**, http://www.idsirtii.or.id/content/files/IDSIRTII-Artikel-MalwareAnalysis.pdf *(20 Oktober 2012)*

1) Worm

Worm adalah sebuah program komputer yang di desain untuk menyalinan dirinya sendiri secara berulang-ulang, pada drive lokal, jaringan, email, atau internet. Program ini menggunakan jaringan komputer untuk mengirimkan salinan dirinya ke komputer lainnya dan dapat menginfeksi tanpa sepengetahuan pengguna. Tujuan utama *Worm* adalah untuk mereproduksi.[34]

Worm tidak menginfeksi file atau memodifikasi file melainkan menimbulkan kerugian pada jaringan karena *worm* akan mengkonsumsi bandwith jaringan, sehingga mengakibatkan speed internet lambat. *Worm* menginfeksi host korban dan memasukkan kode program sebagai bagian dari program *worm* ke dalamnya. Kode tersebut dapat berupa kode mesin atau *routine* untuk menjalankan program lain yang sudah ada pada host korban. Dalam proses penyebarannya, *worm* harus mencari korban baru dan menginfeksi korban dengan salinan dirinya. Proses pendistribusian tersebut dapat berlangsung sebagai proses distribusi satuan (dari satu host[35] ke host yang lain), atau sebagai proses distribusi masal (dari satu host ke banyak host).

Proses distribusi masal dipertimbangkan sebagai metode penyebaran tercepat dengan asumsi batasan yang digunakan adalah satuan waktu. Terdapat beberapa mekanisme penyebaran yang digunakan worm untuk menemukan calon korban, yaitu dengan melakukan scanning, mencari korban berdasarkan daftar

[34] Kumar, H.Shravan, ***Seminar Report on Study of Viruses and Worms***, KReSIT, I.I.T Bombay, hal. 1

[35] Host adalah sistem komputer yang diakses oleh pengguna yang bekerja pada lokasi yang jauh. Biasanya, istilah ini digunakan jika ada dua sistem komputer yang terhubung dengan modem dan saluran telepon. Sistem mengandung data yang disebut host, sedang sitem yang digunakan untuk mengases dari jarak jauh disebut remote terminal. Istilah host juga digunakan untuk menyebut komputer yang terhubung dengan jaringan TCP/IP, termasuk Internet.

target yang sudah disiapkan terlebih dulu oleh pembuat worm, atau berdasarkan daftar yang ditemukan pada sistem korban, maupun di metaserver, serta melakukan pengawasan secara pasif.

Metode scanning melibatkan proses probing terhadap sejumlah alamat di internet dan kemudian mengidentifikasi host yang mudah di serang (*vulnerable)*.[36] Dua format sederhana dari metode scanning adalah mencoba mengidentifikasi sebuah blok alamat dari awal sampai akhir (*sequential*) dan acak (*random*). Penyebaran worm dengan metode scanning, baik *sequential* maupun *random*, secara komparatif dapat dikatakan lambat, namun jika dikombinasikan dengan aktivasi secara otomatis, *worm* dapat menyebar lebih cepat lagi.

Worm yang menggunakan metode scanning biasanya mengeksploitasi celah keamanan *(security holes)* yang sudah teridentifikasi sebelumnya sehingga secara relatif hanya akan menginfeksi sejumlah host saja. Metode *scanning*[37] lainnya yang dinilai cukup efektif adalah dengan menggunakan *bandwidth limited routine*[38] seperti yang digunakan oleh *CodeRed*,[39] yaitu dengan membatasi target dengan latensi koneksi dari sistem yang sudah terinfeksi dengan calon korban yang baru, mendefinisikan target yang hanya terdapat pada alamat lokal, seperti dalam sebuah LAN maupun WAN, dan permutasi pada proses pencarian.

---

[36] Kumar, H.Shravan, *Op.Cit*, hal 3

[37] Di dalam bahasa inggris dimaknai sebagai, "*look at all parts of (something) carefully in order to detect some feature*, dalam bahasa indonesia di artikan pemindai"

[38] *bandwidth limited routine* yaitu keterbatasan kecepatan dalam akses dan melambatnya jalur data

[39] Menurut CERT Advisory CE-2001-19, *CodeRed is self-replicating malicious code that exploits a known vulnerability in Microsoft IIS servers* yang dapat diartikan bahwa yang dimaksud *CodeRed* bekerja dengan melakukan replikasi diri. CERT/CC, 2001, *CERT® Advisory CA-2001-19 "**Code Red**" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL*, http://www.cert.org/advisories/CA-2001-19.html (19 Februari 2013)

Terdapat 4 (empat) macam media penyebaran *Worm* antara lain, *Worm E-mail* yaitu jenis *worm* yang menyebar melalui e-mail, *Worm* ini bisa berupa suatu attachment atau e-mail yang berisi link dari website yang terinfeksi *Worm Instant Messanging. Worm* ini mempunyai metode penyebaran tunggal. Mereka menyebar menggunakan aplikasi *chatting* (*instant messaging*), seperti ICQ dan MSN dengan mengirimkan link yang mengarah pada website yang terinfeksi ke setiap orang yang berada dalam daftar. Perbedaan antara *worm* ini dengan *worm e-mail* terletak pada perantara yang digunakan.

Worm internet merupakan worm yang dibuat atau diciptakan untuk melakukan pengcopyan diri pada jaringan server, mengeksploitasi kelemahan sistem operasi untuk mengambil alih komputer dan/atau jaringan, mengambil alih jaringan publik, menumpang/menggunakan *malware* lain yang bertindak sebagai pembawa worm ini.

2) *Trojan Horse.*

Virus Trojan (*Trojan Horse*) adalah suatu *software* yang dirancang sedemikian rupa sehingga terlihat seperti sebuah file yang memang berguna bagi suatu komputer, akan tetapi memiliki fungsi dan tujuan yang berbahaya bagi komputer dan pengguna. Trojan merupakan *tool* yang dapat digunakan untuk memonitoring sistem komputer lain. Pengertian umumnya, dapat di katakan sebagai kamera yang tersembunyi yang di tempatkan di komputer target.[40]

Virus trojan masuk melalui dua bagian, yaitu bagian *client* dan *server*. Ketika korban (tanpa diketahui) menjalankan komputer, kemudian penyerang

[40] Anonymous, 1999, ***Advisory CA-1999-02 Trojan Horses***, CERT: Software Engineering Institute Carnegie Mellon University, http://www.cert.org/advisories/CA-1999-02.html, (24 Maret 2013)

akan menggunakan *client* untuk koneksi dengan server dan mulai menggunakan virus trojan tersebut.[41] Trojan dapat menyebar melalui file *attachment* (file yang dilampirkan) yang ada pada e-mail, selain itu protokol TCP/IP adalah jenis protokol yang umum digunakan untuk komunikasi, dan virus trojan dapat bekerja dengan baik dengan jenis protokol ini, beberapa trojan juga dapat menggunakan protokol UDP dengan baik.[42]

Sebagian pemakai internet beranggapan bahwa trojan hanya bersifat merusak saja. Anggapan tersebut tidak benar, karena trojan dapat digunakan alat untuk mata-mata dan melakukan penyadapan pada beberapa komputer korban. Data yang disadap berupa data pribadi maupun informasi yang sensitif (misalnya spionase dalam industri).

3) Backdoors

Backdoor adalah salah satu jenis trojan yang sering digunakan untuk mengontrol suatu komputer dari jarak jauh melalui jaringan baik lokal maupun internet. Ciri khas *backdoor* adalah berjalan secara tersembunyi, tidak menampilkan hal-hal yang mencurigakan, serta membuka port agar komputer dapat diakses secara remote.[43] *Backdoor* dapat juga disebut sebagai *Remote Access Trojan* atau *Remote Administration Tool* (RAT). Contoh *trojan backdor* (RAT) adalah *Posion Ivy, Bifrost, Optix Pro, DarkComet-Rat, XpertRAT, Back Orifice* dan *Sub Seven* (Sub7).

---

[41] *Ibid*
[42] *Ibid*
[43] Wysopal, Chris, ***Static Detection of Application Backdoors***, Veracode.Inc., Burlington, MA USA, hal 4

Ada dua bagian *backdoor*, yaitu *client* dan *server*. *Client* adalah program yang diinstal di komputer target sedangkan server merupakan program yang digunakan *attacker* dalam mengoperasikan komputer target. Ada dua metode komunikasi antara *client* dan *server* yaitu *direct connection* dan *reverse connection*.[44] Pada *direct connection*, *server* berusaha melakukan koneksi ke IP (*internet protocol*) target agar dapat berkomunikasi dengan *client.* Tapi hal ini lebih mudah diblok oleh program *firewall*.

Pada *reverse connection* tidak membutuhkan IP target karena serverlah yang berusaha melakukan koneksi ke IP *client* (*attacker*). Ketika *attacker* menjalankan *client* dengan koneksi Internet lain, IP pun akan berubah, lalu bagaimana membuat IP client yang bersifat taktis? Untuk mengatasi hal ini, *attacker* dapat memakai *dynamic DNS* yang banyak disediakan secara gratis oleh website-website tertentu. *trojan backdoor* merupakan jenis *malware* yang sangat berbahaya. Pasalnya, selain pencurian data, komputer korban dapat dijadikan *zombie* untuk menyerang server.

4) Spyware.

Spyware adalah salah satu bentuk *malware* yang menginfeksi komputer, masuk ke komputer melalui file program yang di unduh dari internet, sebab rata-rata *spyware* "menempel" (*embeded*) pada sebuah program. Pada umumnya program yang *embeded* dengan *spyware* adalah sebuah piranti lunak palsu *(fake software)* yang ditawarkan secara gratis di internet.[45] Tampilan *interface* nya sangat meyakinkan dan didesain profesional, disertai penjelasan yang sangat

[44] *Ibid*
[45] Nelson, Chad, *Op.Cit*

teknis. Yang jelas apapun yang dikatakannya, software ini adalah *fake* atau *rough* alias software penipu atau palsu, dan juga merupakan (mengandung) suatu *malware* dari *jenis Spyware*, yang akan menginfeksi dan memata-matai komputer dan aktivitas penggunanya.

b) DoS (Denial of Service)

Denial of Service adalah aktifitas yang bertujuan untuk menghambat kerja sebuah layanan (*service*) atau mematikannya, sehingga user yang berhak atau yang berkepentingan tidak dapat menggunakan layanan tersebut, serangan *DoS* mentargetkan bandwidth dan koneksi sebuah jaringan untuk dapat mencapai misinya.[46] Pada serangan terhadap *bandwidth*, sang penyerang melakukan pembanjiran lalu-lintas data dalam suatu jaringan, dengan menggunakan perangkat yang sudah tersedia pada jaringan itu sendiri, sehingga membuat user yang sudah terkoneksi didalam nya mengalami hilang koneksi.

Di sisi lain, jenis serangan terhadap aktifitas koneksi, adalah dengan sedemikian rupa banyaknya, meminta koneksi langsung terhadap server ataupun router yang bersangkutan, sehingga membuat operasi sistem menjadi tidak memiliki "spot koneksi" lagi untuk user lain, dan membuat user-user tersebut tidak dapat terkoneksi ke server itu.

Perkembangan dari serangan *DoS* adalah *DDoS (Distributed Denial of Service)*. Serangan *DDoS* adalah jenis serangan dengan cara memenuhi trafik server situs tersebut hingga situs menjadi lambat dan susah diakses, Efek dari serangan *DDoS* sangat menganggu pengguna internet yang ingin mengunjungi situs yang telah diserang menggunakan *DDoS*. Situs yang terserang *DDoS* sulit

[46] *Ibid*

untuk diakses bahkan mungkin tidak bisa untuk diakses. Kesulitan pengaksesan sebuah situs diinternet bisa saja merugikan bagi sebagian orang yang bisnisnya sangat tergantung kepada layanan internet.[47]

c) *BotNet*

Terdapat banyak istilah-istilah yang memaparkan apa itu *bot* atau *botnet*. Menurut John Tay dan Jeffrey Tosco pada presentasinya di *APNIC Training,*[48] menyatakan bahwa *bot* merupakan software yang bekerja secara otomatis (seperti robot) dalam menyebarkan dirinya ke sebuah host secara diam-diam dan menunggu perintah dari *botmaster*. *botnets* sudah menjadi suatu bagian penting dari keamanan jaringan internet, karena sifatnya yang tersembunyi pada jaringan server internet.

Sering kali, suatu *botnet* akan masuk di dalam bermacam koneksi-koneksi, seperti telepon, ADSL dan kabel telegram, dan bermacam jaringan, termasuk bidang pendidikan, perseroan/perusahaan, pemerintah dan bahkan jaringan militer. Kadang-kadang menyembunyikan satu instalasi server IRC di satu bidang pendidikan atau lokasi perseroan/perusahaan, di mana koneksi-koneksi yang kecepatan tinggi dapat mendukung sejumlah besar bots yang lain.

c. Methods of defense* di dalam *cyber warfare

Terdapat beberapa metode dalam bertahan antara lain yaitu;

a) Active Defense

Active defense adalah serangkaian tindakan yang bertujuan untuk melakukan tindakan preventif dan dapat juga melakukan pembalasan atau *retaliation*, salah satu

[47] Nelson, Chad, *Op.Cit*
[48] Nelson, Chad, *Op.Cit*

bentuk pertahanan yang sering digunakan adalah *Honeypot*. *Honeypot* membuat jaringan palsu yang dilekatkan atau dipasangkan pada jaringan yang telah diproteksi, akan tetapi dengan membiarkan beberapa lubang atau celah keamanan tetap terbuka dan tetap aman.[49] Berdasarkan metode *honeypot* seorang administrator dapat menemukan atau melacak siapa yang telah menyerang system keamanan komputernya.

b) *Passive Defense.*

Merupakan metode pertahanan yang bertujuan agar komputer terhindar dari serangan, dengan memberdayakan *Firewall*, *Antivirus*, dan *Access Control*. *Firewall* dapat melakukan monitoring terhadap mereka yang memang melakukan tindakan yang membahayakan system komputer melalui koneksi yang masuk, *Firewall* juga dapat melakukan penolakan. Antivirus dapat melakukan pemindaian terhadap file-file yang ada di dalam komputer maupun yang akan masuk untuk memastikan file-file tersebut tidak membahayakan system komputer.[50] *Access Control* adalah metode pemberian izin (*permission*) yang berbeda kepeda setiap pengguna dan komputer. Hal ini adalah untuk mencegah komputer diganggu (*compromised*) yang kebanyakan bermula dari satu komputer kemudian menyebar kepada komputer lain.[51]

C. Hukum Humaniter Internasional

a. Pengertian

Hukum humaniter Internasional merupakan bagian dari hukum internasional publik yang meliputi peraturan mengenai perlindungan terhadap mereka yang tidak terlibat dalam konflik bersenjata atau peperangan, serta mereka yang tidak lagi terlibat

---

[49] Eric, Peter, ***A Practical Guide to Honeypot***, Washington University in St. Louis, http://www.cse. wustl.edu /~jain/cse571-09/ftp/honey/index.html#sec1.2 (24 Maret 2013)

[50] Nelson, Chad, *Op.Cit*

[51] Ibid

dalam tindakan permusuhan, dan membatasi sarana dan metode berperang yang diterapkan. Menurut ICRC hukum humaniter internasional mengacu pada perjanjian-perjanjian internasional atau kebiasaan-kebiasaan internasional yang secara khusus bertujuan untuk mengatasi masalah yang berkaitan dengan kemanusiaan yang terjadi di dalam sebuah konflik bersenjata, baik yang bersifat internasional atau non-internasional.[52]

Dalam kepustakaan hukum internasional istilah hukum humaniter merupakan istilah yang dianggap relatif baru. Istilah ini baru lahir sekitar tahun 1970-an, ditandai dengan diadakannya *Conference of Government Expert on the Reaffirmation and Development in Armed Conflict pada tahun 1971*. Selanjutnya, pada tahun 1974, 1975, 1976, dan 1977 diadakan *Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflict.*[53] Terdapat beberapa ruang lingkup ada tiga kelompok yang umumnya dikenal, yaitu aliran luas, aliran tengah, dan aliran sempit.[54]

Jean Pictet yang menganut aliran luas menyatakan bahwa, hukum humaniter mencakup baik Hukum Jenewa, Hukum Den Haag, dan Hak Asasi Manusia, Haryomataram dan J.G Starke menganut aliran tengah yang menyatakan bahwa, hukum humaniter terdiri atas Hukum Jenewa dan Hukum Den Haag, dan yang terakhir yaitu

---

[52] Anonymous, 2002, ***International Humanitarian Law: Answer to Your Question***, International Committee of the Red Cross, http://cdn.peaceopstraining.org/ course_promos/ international_humanitarian_law/international_humanitarian_law_english.pdf, hal 4 (19 Februari 2013)

[53] Arlina Permanasari dkk, **Pengantar Hukum Humaniter**, ICRC Jakarta, Miamata Print, Jakarta, 1999, hal. 8

[54] *Ibid*, hal. 10

Geza Herzegh yang menganut aliran sempit menyatakan bahwa, hukum humaniter hanya menyangkut Hukum Jenewa saja.[55]

b. Jenis Konflik Bersenjata

1. Konflik Bersenjata Internasional

Di dalam common article 2 dari Konvensi Jenewa 1949 di jelaskan bahwa;

> *In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.*

Menurut artikel tersebut yang dimaksud High Contracting Parties adalah Negara. Sebuah konflik bersenjata internasional terjadi ketika adanya suatu negara yang menyerang negara lain, yang di mungkinkan melibatkan lebih dari dua negara, terlepas dari alasan timbulnya konflik atau intensitas dari konfrontasi tersebut.[56] *International armed conflict* atau konflik bersenjata internasional ini kerap kali di persamakan dengan *internationalised armed conflict* yakni ketika suatu negara melakukan intervensi dengan angkatan bersenjatanya dalam suatu konflik non-internasional yang terjadi di negara lain, dengan maksud untuk membela pihak pemerintah atau pihak pemberontak dari negara tersebut.[57]

---

[55] *Ibid*, hal. 10

[56] Anonymous, 2008, ***How is the Term "Armed Conflict" Defined in International Humanitarian Law?***, International Committee of the Red Cross (ICRC) Opinion Paper, www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (25 Februari 2013)

[57] Anonymous, 2012, ***Rule of Law in Armed Conflict Object: Qualification of Armed Conflict***, Geneva Academy of International Humanitarian Law and Human Rights, http://www.geneva-academy.ch/RULAC/qualification_of_armed_conflict.php (25 Februari 2013)

Kasus Tadic, dimana terdapat campur tangan negara secara tidak langsung tanpa penggunaan angkatan bersenjata dalam konflik internasional, dimana putusan dari ICTY (*International Criminal Tribunal of Yugoslavia)* menyatakan bahwa, adanya *overall controll* atau kontrol secara keseluruhan terhadap kelompok pemberontak akan cukup untuk menginternasionalisasi konflik.[58]

2. Konflik Bersenjata Non-Internasional

Konflik non-internasional atau biasa disebut *non-international armed conflict* adalah konfrontasi angkatan bersenjata yang terjadi di dalam wilayah atau teritorial suatu negara dan tidak melibatkan negara lain atau tidak ada intervensi negara lain, dan juga tidak termasuk meluasnya konflik ke dalam dua atau lebih negara.[59]

Adapun konvensi yang mengatur *non-internasional armed conflict* ini yakni, *Common Article 3 of the 1949 Geneva Conventions for the Protection of War Victims; the 1977 Protocol Additional (II) to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflict* atau pengaturan mengenai perlindungan terhadap korban dari konflik non-internasional yaitu, *the 1980 Convention on Certain Conventional Weapons, as amended, Protocols the 1998 Statute of the International Criminal Court; the 1997 Ottawa Convention banning anti-personne, the 1993 Chemical*

[58] Anonymous, 2012, *Op.Cit*

[59] Prof. Schimitt, N. Michael, Prof. Garraway, Charles H.B, Prof. Dinstein, Yoram, 2006, *The **Manual on the Law of Non International Armed Conflict With Commentary***, International Institute of Humanitarian Law, www.iihl.org/iihl/Documents/The%2520 Manual% 2520on%2520the%2520 Law%2520of%2520NIAC.pdf (25 Februari 2013)

Weapons Convention, the 1954 Hague Convention for the Protection of Cultural Property, dan *1999 Second Protocol.*[60]

c. Sarana dan Metode Berperang

Kombatan mempunyai hak untuk memilih sarana dan metode berperangnya sendiri yang diatur dan dibatasi oleh hukum humaniter internasional, adapun pengaturan dan pembatasan tersebut dapat ditemukan dalam *Additional Protocol I in 1977* mengenai the *Protection of Victims of Interntional Armed Conflict.* Selain itu terdapat juga peraturan tentang pelarangan penggunaan senjata seperti senjata biologi, senjata yang mempunyai efek membakar, senjata yang membutakan, dan ranjau.[61]

Dalam Deklarasi St. Petersburg yang kemudian di adopsi oleh International Military Commission, menjelaskan mengenai larangan penggunaan peluru-peluru yang mempunyai efek ledak terutama terhadap tubuh manusia. Di dalam *Article 36 Additional Protocol I of 1977* menyatakan bahwa;

> *In the study, development, acquisition or adoption of new weapon, means or methods of warfare, a High Contarcting Party is under an obligation to determine whether its employment would in some or all circumstances, be prohibited by this Protocols or by any other rule of International law applicable to the High Contracting Party.*

Artikel tersebut bertujuan untuk mencegah penggunaan senjata-senjata baru, sarana dan metode berperang baru yang mempunyai efek-efek yang secara umum dilarang di dalam hukum internasional. *Article 36* diatas juga di lengkapi dengan adanya *Article 82 Additional Protocol I,* di mana artikel tersebut banyak dibutuhkan oleh para penasihat

---

[60] Prof. Schimitt, N. Michael, Prof. Garraway, Charles H.B, Prof. Dinstein, Yoram, *Loc.Cit*

[61] Anonymous, 2006, ***A Guide to The Legal Review of New Weapon***, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol 1 of 1977, International Committee of The Red Cross, www.icrc.org/eng/assets/files/other/irrc_ 864_icrc_ geneva.pdf, hal 932

hukum atau ahli hukum untuk melakukan pembelaan terhadap *military commanders* atau komandan militer.[62]

d. Perkembangan Sarana dan Metode Dalam Konflik Bersenjata

1. Terrorisme

War on terror adalah doktirn yang berkembang setelah adanya serangan 11 September yang di duga telah dilakukan oleh kelompok atau jaringan Al-Qaedah,[63] kemudian dengan alasan tersebut Amerika melakukan operasi militer ke timur tengah khususnya di Afghanistan dan Irak. Secara politik *War on Terror* yang telah di lakukan Amerika Serikat memang dibenarkan akan tetapi berdasarkan hukum internasional khususnya hukum humaniter internasional masih diragukan.

International Committee of The Red Cross menyatakan bahwa, *War on Terror* atau perang terhadap terrorisme ini bukan lagi sebuah perang melainkan bisa disebut sebagai *War on Drugs.*[64] Banyak ahli hukum dan bidang lainnya merasa kesulitan dalam mendefinisikan istilah terrorisme, dalam *the Shorter Oxford English Dictionary* terrorisme didefinisikan sebagai, *A system of terror, Government by intimidation; the system of the terror, A policy intended to strike with terror those against whom it is adopted, the fact of terrorizing or condition*.[65]

Kemudian *the Webster's New Twentieth Century Dictionary* mendefinisikan

---

[62] Anonymous, 2006, *Op.cit*, hal 933

[63] Chelimo, Getrude.C, 2011, ***Defining Armed Conflict in International Humanitarian Law***, Student Pulse:Online Academic StudentJournal, http://www.studentpulse.com/ articles/508/2/ defining-armed-conflict-in-international-humanitarian-law (26 Februari 2013)

[64] Milanovic, Marko, 2007, ***Lesson For Human Rights and Humanitarian Law In The War on Terror: Comparing Hamdan and The Israeli Targeted Killing Case***, International Committee of The Red Cross, hal. 375

[65] Williamson, Myra, 2009, ***Terrorism, War, and International Law: The Legality of the Use of Force Against Afghanistan in 2001***, The University of Waikato, New Zealand, hal 39

terrorisme sebagai, *terrorizing; use of terror and violence to intimidate, subjugate, etc, especially as a political weapon or policy, intimidation an subjugation so produced*.[66]

The Shorter Oxford menjelaskan bahwa terrorisme digunakan sebagai bentuk intimidasi dari pemerintah, kemudian *The Webster's* mengkaitkan terrorisme sebagai tujuan politik (*political objectives*), sejarah terrorisme bermula dengan adanya grup dari Gerakan *Sicarii*[67]pada tahun 66-73 setelah masehi, dimana *Sicarii* menggunakan taktik dengan menyerang musuh-musuhnya pada siang hari terutama ketika hari libur ketika Jerusalem banyak di sesaki orang.[68]Anggota dari *The Sicarii* terdiri dari para extremist, nationalist, anti-Roman, dan korban-korbannya adalah anggota dari perdamaian Yahudi, dan simpatisan Roman, mereka memandang perbuatan mereka adalah hal yang syahid, dan mereka percaya bahwa setelah Jerusalem runtuh maka rezime yang murka tersebut tidak akan berkuasa lagi, dan Tuhan akan menunjukkan diri-Nya kepada para makhluk-Nya.[69]

Gerakan *Sicarii* tersebut atas, ternyata belum bisa memenuhi sebagai tindakan terrorisme pertama menurut beberapa ahli karena, tindakan tersebut ada karena tujuannya yang cenderung meluas dan asalnya juga dari satu wilayah yang sama. Sekitar abad ke sebelas munculah gerakan religius yang populer yaitu *The Assassins*[70], mereka terdiri dari sekte *Shi'ite* yang berasal dari Persia yang

---

[66] Williamson, Myra, *Loc.Cit*, hal 39
[67] Merupakan bahasa latin berasal dari kata *Sicarius* yang berarti pisau, dan erat kaitannya dengan pembunuh bayaran
[68] Williamson, Myra, *Op.cit*, hal 41
[69] Williamson, Myra, *Loc.cit*, hal 41
[70] Merupakan istilah dari bahasa Arab *hashashin*

kemudian menyebar ke Syria.[71] Mereka menentang adanya pembentukan Muslim *Sunni*, pemimpin mereka yang pertama adalah *Hassan Bin Sabbah*, mereka membunuh para politikus, para pemimpin keagamaan, gubernur, dan kalifa, serta target yang utama adalah para kaum *Sunni*.[72]

The Assassins menyerang mereka yang terkuat selain itu tidak termasuk dalam target, tujuan mereka terwujud dengan melenyapkan satu persatu individu yang memiliki hubungan atau terkait dengan tujuan mereka. Banyak ahli yang mengklaim bahwa *The Assassin* merupakan bentuk dari tindakan terrorisme pertama.

Jika melihat pengertian yang diberikan oleh *the Webster's New Twentieth Century Dictionary* maka hal itu akan lebih condong pada *Reign of Terror* yang terjadi pada masa revolusi Perancis sekitar tahun 1700 an, di mana pada waktu itu revolusi Perancis mendapatkan ancaman dari para emigran kelas atas.[73] Kemudian para biarawan dan pendeta yang di pimpin oleh Jacobin, menyatakan terror sebagai solusinya. Terror tersebut di desain untuk mengkonsolidasikan kekuatan dari pemerintahan yang baru dengan mengintimidasi penentang revolusioner, mereka yang berbuat makar, dan semua orang-orang yang dianggap membangkang.[74]

---

[71] Williamson, Myra, *Loc.cit*, hal 41
[72] Williamson, Myra, *Loc.cit*, hal 41
[73] Williamson, Myra, 2009, ***Terrorism, War, and International Law: The Legality of the Use of Force Against Afghanistan in 2001***, The University of Waikato, New Zealand, hal 43

[74] Williamson, Myra, *Loc.cit* hal 43

2. Senjata Pemusnah Massal

Istilah menegnai senjata pemusnah massal atau biasa disebut sebagai *Weapon of Mass Destruction* muncul pertama kalinya pada saat Hari Raya Natal tahun 1937 yang di ucapkan oleh Uskup Agung dari Cantenbury yaitu William Cosmo Gordon Lang,[75]

> *Take, for example, the question of peace. Who can think without dismay of the fears, jealousies, and supicions which have compelled, nation, our own among them, to pile up their armaments ? Who can think at this present time without a sickening of the heart of the appalling slaughter, the suffering, the manifold misery brought by war to Spain and to China ? Who can think without horror of what another widespread war would mean, waged as it would be with all the new weapons of mass destruction ?*

dari apa yang telah di ucapkan oleh Uskup Agung tersebut masih belum jelas apa yang di maksud dengan senjata pemusnah massal atau weapon of mass destruction, sekilas Uskup Agung tersebut menggambarkannya sebagai pemboman udara (aerial bombard) atau senjata-senjata peledak yang memang pada saat itu marak digunakan dalam peperangan di Spanyol dan China.

Penjelasan dari *The UN Commission on Conventional Armaments* (CCA) yang di sesuaikan dengan pendapat dari Atomic Energy Commision yaitu;[76]

> *The Commission for Conventional Armaments resolves to advise the Security Council: 1. that it considers that all armaments and armed forces, except atomic weapons and weapons of mass destruction, fall within its jurisdiction, and that weapons of mass destruction should be*

[75] Carus, W., Seth, 2012, ***Defining Weapon of Mass Destruction***, National Defense University Press Washington, D.C, hal 7

[76] Carus, W., Seth, *Op.Cit*, hal 9

> *defined to include atomic explosive weapons, radio active material weapons, lethal chemical and biological weapons, and any weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above*

dari definisi tersebut CCA pada dasarnya menyamakan senjata pemusnah massal dengan *Chemical, Biological, Radio active, and Nuclear Weapon* (CRBN). Definisi tersebut juga termasuk pada senjata-senjata yang belum ditentukan yang mungkin akan ada di masa depan yang mempunyai efek-efek yang sama dengan CRBN.[77]

Pengaturan mengenai senjata pemusnah massal juga terdapat dalam beberapa perjanjian internasional, yaitu dalam *Outer Space Treaty* 1967, *Seabed Treaty* 1972, *Strategic Arms Reduction Treaty* 1991, dan *Moon Agreement*.[78] Di dalam *Outer Space Treaty* 1967 pada artikel IV dijelaskan bahwa; *State Parties to the Treaty undertake not to place in orbit around the earth any object carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapon in outer space in any other manner*. Menurut artikel tersebut menaruh senjata pemusnah massal di luar angkasa atau terhadap obyek yang mengitari Bumi tidak diperbolehkan. Kemudian di dalam Seabed Treaty 1972 pada artikel I *Prohibition of the Emplacement of Nuclear Weapon and Other Weapon of Mass Destruction on the Seabed and the Ocean Floor* di sebutkan;

---

[77] *Ibid*, hal 10
[78] *Ibid*, hal 11

> *The State Parties to this Treaty undertake not to emplant or emplace on the seabed and the ocean floor and in the subsoil thereof beyond the outer limit of a sea-bed zone, as defined in article II, any nuclear weapon or any other type of weapons of mass destruction as well as structures, launching installations or any other facilities specifically designed for storing, testing or using such weapons.*

artikel tersebut melarang adanya penempatan senjata nuklir atau senjata pemusnah massal lainnya di dasar laut. Artikel tersebut juga di pakai dalam Strategic Arms Reduction Treaty 1991 pada artikel V, paragraf 18.[79]

Selanjutnya dalam Moon Agreement 1979 di jelaskan di dalam artikel 3 yaitu; *State Parties shall not place in orbit araound or other trajectory to or around the Moon objects carrying nuclear weapons or any other kinds of weapons of mass destruction or place or use such weapons on or in the moon.* Artikel tersebut hampir sama dengan apa yang terdapat dalam Outer Space Treaty, namun dalam artikel tersebut lebih fokus pada *Moon* atau Bulan.

Terdapat banyak definisi dari senjata pemusnah massal ini namun lebih tepat jika mendefinisikan dahulu mengenai *mass destruction* atau pemusnah massal, dari beberapa yang ada yang memang sesuai adalah definisi yang di berikan oleh Department of Defense U.S.A yaitu, *capable of a high order of destruction, significant damage to property* atau *significant damage to infrastructure*.[80]

[79] Carus, W., Seth, *Op.Cit*, hal 18
[80] Carus, W., Seth, *Op.Cit*, hal 36

3. *Asymmetry Warfare* (Kesenjangan Dalam Peperangan)

Penggunaan teori *asymmetry warfare* ini adalah untuk menjelaskan atau menggambarkan bahwa, dalam kasus cyber warfare antara Rusia dengan Georgia, terdapat kesenjangan atau ketidakseimbangan yang di alami oleh pihak Georgia yang memiliki pertahanan cyber yang lebih lemah. *Asymmetry warfare* pertama kali diperkenalkan oleh Sun Tzu dan Liddell Hart,[81] di dalam karyanya yang berjudul *The Art of War* yang ditulis sekitar 1500 tahun yang lalu, Sun Tzu mengatakan;[82] *All warfare is based on deception. When confronted with an enemy an enemy one should offer the enemy a bit to lure him, feign disorder and strike him. When he concentrate, prepare against him, where he is strong avoid him*. Perkataan tersebut menerangkan bahwa, strategi yang baik dalam suatu peperangan adalah dengan selalu melihat suatu kesenjangan atau ketidak seimbangan lalu mengeksploitasinya.

Kemudian Liddell Hart mengajarkan, *The wisest strategy avoids the enemy's strength and probes for weakness*.[83] Pada tahun 1999 Qiao Liang dan Wang Xiangsui dari China, telah menulis sebuah buku yang berjudul *Unrestricted Warfare* yang intinya, bahwa selain adanya kekerasan dalam segi militer, juga terdapat kekerasan dari segi politik, ekonomi, dan teknologi yang terus meningkat dan bentuk-bentuk kekerasan itu tidak akan sepenuhnya patuh pada prinsip-

[81] Buffaloe, David L., 2006, ***Defining Asymmetric Warfare***, The Institute of Land Warfare, Association of The United State Army, hal. 7

[82] Buffaloe, David L, *Loc Cit*, hal. 7

[83] Buffaloe, David L, *Loc Cit*, hal. 7

prinsip dalam perang.[84] Colonel Robert Shaw dari U.S Army, mendefinisikan *asymmetic warfare* sebagai;

> *Warfare in which the two or more belligerents are mismatched in their military capabilities or accustomed methods of engagement such that the militarily disadvantaged power must press its special advantages or… its enemy particular weaknesses if they are to prevail*

dalam definisi tersebut pada intinya adalah mengenai ketidak seimbangan antara pihak yang satu dengan pihak yang lain dalam suatu peperangan atau konflik sama halnya seperti yang telah disampaikan oleh Sun tzu.

Ada beberapa faktor yang mempengaruhi *asymmetric warfare*, yang pertama adalah *Asymmetry of Cost*, dari catatan David Galula ditahun 1964, *asymmetry of cost* atau kesenjangan dalam hal biaya terjadi ketika kubu pemberontak meledakkan sebuah jembatan, kemudian kubu yang kontra terhadap pemberontak harus melindungi semua jembatan yang ada, kemudian pemberontak melempar granat ke dalam gedung bioskop maka kubu yang kontra pemberontak harus mengeluarkan banyak biaya untuk melindungi populasinya.[85] Semakin banyak yang harus dilindungi dan dipertahankan akan semakin banyak biaya yang akan di tanggung.

Yang kedua adalah *Cultural Asymmetry*, adanya kegagalan dalam memahami kultur atau budaya pihak musuh, beranggapan bahwa musuh tak ubahnya seperti anda, dan anda akan mengalami kegagalan untuk mencapai kemenangan karena tidak mampu mempelajari tentang apa yang dimaksud

[84] Buffaloe, David L, *Op.Cit*, hal 9
[85] *Ibid*, hal 14

dengan *center of gravity*, Anthony Zinni seorang anggota angkatan laut Amerika Serikat menyatakan bahwa musuh Amerika setelah adanya serangan 9/11 atau *center of gravity*-nya adalah *angry young Muslim men* atau kemarahan dari seorang Muslim muda.[86] Yang ketiga adalah *Asymmetric Threat*, adapun komponen-komponen yang terdapat dalam *asymmetric* threat ini adalah terrorisme, *insurgency* (pemberontak), *information operations*, *disruptive threats*, dan *unknown threat.*[87]

Kemudian yang terakhir adalah *Asymmetric Operations* yaitu sebuah operasi yang telah direncanakan dan dilaksanakan oleh pihak yang lebih kuat dalam sebuah *asymmetric warfare*, adapun operasi tersebut terdiri dari diplomasi, informasi, militer, dan ekonomi.[88]

4. *Non Lethal Weapon*

Non Lethal Weapon adalah jenis-jenis senjata yang secara eksplisit di desain untuk meminimalisir terjadinya akibat yang fatal, cidera permanen, dan kerugian-kerugian atau akibat-akibat yang tidak di inginkan terhadap benda maupun lingkungan.[89] Tidak seperti senjata konvensional pada umumnya, yang bersifat menghancurkan target dengan cara meledak, penetrasi atau menembus masuk, dan menjadi serpihan, non lethal weapon bersifat lebih mencegah target untuk menjalankan fungsinya.[90] *Non-lethal weapons* banyak diakui sebagai

[86]Buffaloe, David L, *Loc Cit*, hal. 14
[87]*Ibid*, hal 17
[88] *Ibid*, hal 20
[89] Koplow, David A., 2006, ***Non Lethal Weapons; The Law And policy of Revolutionary Technologies for The Military And Law Enforcement***, George Town University Law Center, hal. 7

[90] Koplow, David A., *Loc.Cit*, hal. 7

kebutuhan pokok bagi para militer khususnya dalam hal persenjataan, jenis-jenis dari *non-lethal weapon* yang umumnya digunakan sejak dari dulu adalah pentungan, water canon, dan K-9 corps atau anjing pelacak.[91]

Peralatan-peralatan tersebut terus berkembang pesat hampir diseluruh dunia, penggunaannya di nilai efektif untuk menghalau keributan, demonstrasi yang ilegal dan brutal, serta untuk gangguan-gangguan lainnya yang mungkin terjadi, dengan meminimalisir terjadinya akibat-akibat yang fatal. Seirng berkembangnya zaman, muncul jenis-jenis baru *non-lethal weapon* seperti, *slippery Foam* atau busa pelicin,[92] *electric guns* atau biasa disebut pistol kejut,[93] kemudian *pepper spray* atau semprotan merica yang dapat menyebabkan selaput mata merasa seperti terbakar, dan perih, bahkan menimbulkan kebutaan sekitar 15 menit,[94] *acoustic rays* yaitu penggunaan gelombang suara atau *infrasound* untuk melumpuhkan organ-organ yang ada di dalam tubuh target.[95]

Pada tahun 2002 memanasnya konflik antara Rusia dengan Chechens, memaksa militer Rusia untuk mengirim pasukan elite mereka untuk melumpuhkan pasukan pemberontak Chechens, dengan menggunakan *chemical narcotic* melewati lubang-lubang ventilasi di Dubrovka Theater, dimana mereka yang ada di dalamnya adalah para pemberontak dan terroris.[96] Adapun efek dari *chemical narcotic* tersebut membuat korbannya merasa pening, lesu, bahkan tidak

---

[91] *Ibid*, hal. 10
[92] *Ibid*, hal. 14
[93] *Ibid*, hal. 16
[94] *Ibid*, hal. 18
[95] *Ibid*, hal. 19
[96] Koplow, David A., *Op.Cit*, hal. 102

sadarkan diri.[97] Tujuan dari digunakannya *chemical narcotic* tersebut adalah untuk mencegah para pemberontak dan terroris meledakkan bom yang telah mereka buat.[98]

5. *Unmanned Aerial Vehicles*

Unmanned aerial vehicles biasa disebut *predator* atau *drone*, adalah salah jenis pesawat udara tanpa awak atau tanpa pilot, NATO mendefinisikan *unmanned aerial vehicles* sebagai;[99]

> *"a powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload. Ballistic or semi-ballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles".*

umanned aerial vehicles sebelumnya telah diprogram untuk melakukan suatu tugas khusus, berdasarkan definisi NATO apa yang disebut sebagai *piloted remotely* atau disertai pengendali yang dapat berasal dari pihak militer atau penduduk sipil.

Pengendali *unmanned aerial vehicles* berada jauh dari medan pertempuran, mereka menjalankan tugasnya dengan memantau melalui infrared atau sensor TV yang dipasang di *umanned aerial vehicles* tersebut secara

---

[97] *Ibid*, hal. 103
[98] Koplow, David A., *Loc.Cit*, hal. 103
[99] Ochmannova, Petra, 2011, ***Unmanned Aerial Vehicles And Law of Armed Conflict Implications***, Czech Year Book of International Law, hal. 145

online.[100] *Umanned aerial vehicles* oleh beberapa ahli juga biasa disebut sebagai *umanned combat aicraft system* (UCAS), UCAS pertama kali digunakan pada tahun 2001 saat terjadinya operasi militer Amerika di Afghanistan, UCAS tersebut dikendalikan oleh *Central Intelligence Agency* (CIA) untuk menyerang anggota Al-Qaedah yang bernama Ali Qaed Senyan al-Harithi.[101]

D. Pengertian Perang

Perang secara purba di maknai sebagai pertikaian bersenjata, Di era modern, perang lebih mengarah pada superioritas teknologi dan industri. Hal ini tercermin dari doktrin angkatan perangnya seperti "Barang siapa menguasai ketinggian maka menguasai dunia". Hal ini menunjukkan bahwa penguasaan atas ketinggian harus dicapai oleh teknologi. Namun kata perang tidak lagi berperan sebagai kata kerja, namun sudah bergeser pada kata sifat. Yang memopulerkan hal ini adalah para jurnalis, sehingga lambat laun pergeseran ini mendapatkan posisinya, namun secara umum perang berarti pertentangan.

Sejarah pengertian perang tersebut mengalami perubahan bukan hanya karena adanya pendapat-pendapat dari para jurnalis namun, juga adanya pernyataan-pernyataan yang bersifat politis yang juga dapat diartikan sebagai peperangan seperti, *The Cold War* atau perang dingin yang banyak disebut sebagai perang ideology dan teknologi. Perang ideology antara ideology sosialis dengan demokrasi, dan perang teknologi dalam hal persenjataan khususnya persenjataan nuklir. Perang tersebut di pelopori oleh dua kubu

[100] Ochmannova, Petra, *Loc.Cit*, hal. 145
[101] Shimitt, Michael N., 2012, ***Umanned Combat Aircraft System And International Humanitarian Law: Simplifying The Oft Benighted Debated***, Boston University School of Law, hal. 598

yakni Uni Soviet (sekarang Rusia) dan Amerika Serikat. Perang dingin juga mempelopori adanya pemikiran mengenai *all aspect warfare* atau perang dalam semua aspek.

E. *Attack* (Serangan)

Di dalam Artikel 49 ayat 1 Protokol Tambahan I mendefinisikan *attack* atau serangan sebagai *act of violence* atau tindakan kekerasan baik dalam keadaan bertahan maupun menyerang (*offense*). Dalam praktiknya serangan dihubungkan dengan kehancuran atau kerusakan (*destroy*), dalam hal ini belum ada definisi yang formal mengenai kehancuran maupun kerusakan di dalam hukum humaniter internasional.[102] Di dalam suatu pertempuran atau peperangan, hancurnya suatu benda pasti karena adanya suatu serangan, namun hal tersebut banyak diragukan karena, serangan tidak selalu identik dengan kehancuran, contohnya saat terjadinya konflik di Kosovo, ketika NATO menyerang stasiun pembangkit tenaga listrik milik Serbia dengan filament atau sejenis kawat bermuatan listrik yang mengakibatkan sirkuit dari pembangkit listrik tersebut menjadi tidak berfungsi karena adanya hubungan arus pendek namun hal tersebut tidak menghancurkan stasiun pembangkit tenaga listrik tersebut.[103] Kemudian hal tersebut juga terjadi ketika Amerika menginvasi Irak, serangan pasukan udara Amerika dengan menembakkan gelombang eletromagnetik (EMP) ke jaringan satelit televisi milik Irak untuk melumpuhkan semua perlengkapan dan peralatan penyiaran.[104]

Beberapa ahli sependapat bahwa serangan (*attack*) bila di hadapkan dengan hukum humaniter menjadi serangan bersenjata (armed attack), menurut Jean Pictet, serangan bersenjata terkait dengan durasi dan intesitas yang memadai. Namun, tidak

---

[102] Hayashi, Nobuo, 2010, ***Requirement of Military Necessity in International Humanitarian Law and International Criminal Law***, Boston University Internasional Law Journal, hal. 110
[103] Hayashi, Nobuo *Loc.Cit*, hal. 110
[104] *Ibid*, hal. 111

sedikit ahli yang menanggapi bahwa, durasi dan intensitas sebagai patokan terhadap suatu serangan dirasa masih belum cukup, Michael N. Schimitt mengemukakan 6 kriteria untuk dapat memenuhi sebagai suatu serangan;[105]

1. *Severity*, dilihat dari ruang lingkup dan intesitas serangan tersebut, seperti banyaknya korban jiwa yang diakibatkan, luas area yang terkena dampaknya dan banyaknya benda-benda yang rusak karena serangan tersebut
2. *Immediacy*, melihat pada durasi dari serangan tersebut, seperti berapa banyak waktu yang dibutuhkan agar efek dari serangan tersebut dapat dirasakan, dan berapa lama efek dari serangan tersebut terjadi,
3. *Directness*, melihat pada luka atau kerusakan yang di timbulkan oleh adanya serangan tersebut,
4. *Invasiveness*, melihat pada locus dari serangan tersebut, maksudnya bagaimana serangan tersebut melintasi batas-batas Negara,
5. *Measurability*, yaitu akibat dari serangan tersebut dengan melakukan penafsiran dan pengukuran,
6. *Presumptive Legitimacy*, melihat pada penilaian serta legitimasi dari serangan tersebut yang didasarkan pada praktik Negara-Negara, dan norma-norma yang ada di dalam komunitas internasional, suatu tindakan dapat memperoleh legitimasi berdasarkan hukum ketika hal tersebut diterima oleh komunitas internasional.

Selain itu serangan juga di kaitkan dengan prinsip-prinsip di dalam hukum humaniter internasional seperti *proportionality*, *military necessity*, dan *indiscriminate attack*.

[105] Carr, Jeffrey, 2010, ***Inside Cyber Warfare***, O'Reilly, hal. 60

F. Sumber Hukum Humaniter Internasional

1. Konvensi

a. Konvensi Den Haag

Konvensi Den Haag merupakan ketentuan hukum humaniter yang mengatur mengenai cara dan alat berperang. Hukum Den Haag berhubungan dengan hasil-hasil Konferensi Perdamaian I yang diadakan pada tahun 1899 dan konferensi perdamaian II yang diadakan pada tahun 1907. Konferensi Perdamaian I tahun 1899 menghasilkan tiga Konvensi dan tiga deklarasi. Konvensi-konvensi yang dihasilkan adalah:

1. Konvensi I tentang Penyelesaian Damai Persengketaan Internasional. Konvensi ini untuk mencegah adanya perang atau paling tidak menentukan secara sangat terbatas persayaratan yang harus dipenuhi untuk melakukan pernyataan perang.
2. Konvensi II tentang Hukum dan Kebiasaan Perang di Darat. Memuat ketentuan yang mengatur cara melakukan operasi militer. Prinsip-prinsip dari Konvensi ini kemudian dimasukkan dalam Hukum Jenewa, yaitu Bab III Protokol tambahan I Konvensi Jenewa 1949. Ketentuan yang paling penting dari Konvensi II ini adalah menetapkan bahwa hak setiap yang terlibat dalam pertikaian bersenjata untuk memilih sarana dan metode perang tidaklah tanpa batas.
3. Konvensi III tentang Adaptasi Asas-asas Konvensi Jenewa Tanggal 22 Agustus 1864 tentang HukumPerang Di Laut. Instrumen Konvensi III ini melindungi tentara yang luka, sakit, dan menjadi korban kapal karam serta tawanan perang. Pada perkembangan selanjutnya perlindungan ini telah diperluas dan lebih

diperinci dalam Konvensi-konvensi Jenewa sehingga Konvensi Den Haag mengenai perlindungan ini tidak berlaku lagi.

Sedangkan tiga deklarasi yang dihasilkan adalah sebagai berikut:

1. Melarang penggunaan peluru-peluru dum-dum, yaitu peluru yang bungkusnya tidak sempurna menutup bagian dalam, sehingga dapat pecah dan membesar dalam tubuh manusia. Deklarasi ini disetujui di Den Haag tanggal 29 Juli 1899 dan mengembangkan deklarasi St. Peterspurg Tahun 1868 yang melarang penggunaan proyektil dengan berat di bawah 400 gram yang mengandung bahan peledak atau bahan pembakar.
2. Pelarangan peluncuran proyektil-proyektil dan bahan peledak dari balon, selama jangka lima tahun yang berakhir pada tahun 1905. Deklarasi ini disetujui pada tahun 1899 dan direvisi pada tahun 1907. Deklarasi kemudian dihidupkan kembali dalam Protokol Tambahan I Konvensi Jenewa mengenai Perlindungan Masyarakat Sipil.
3. Pelarangan penggunaan proyektil-proyektil yang menyebabkan gas cekik dan beracun. Deklarasi ini disetujui pada tahun 1899 dan merupakan upaya pertama untuk melarang penggunaan gas sebagai metode perang yang dianggap sangat kejam dan khianat. Prinsip ini ditegaskan kembali di Jenewa dalam protokol yang melarang penggunaan gas cekik, racun, dan senjata bakterial sebagai metode perang pada tanggal 17 Juni 1925.

Kemudian yang merupakan sumber hukum dari hukum den haag adalah Konvensi Den Haag 1907, Konvensi ini adalah hasil Konferensi Perdamaian II tahun 1907 sebagai

lanjutan dari Konferensi Perdamaian I tahun 1899 di Den Haag terdiri dari konvensi-konvensi sebagai berikut:

1. Konvensi I Den Haag tentang Penyelesaian Damai Persengketaan Internasional;
2. Konvensi II Den Haag tentang Pembatasan Kekerasan Senjata dalam Menuntut Pembayaran Utang yang Berasal dari Perjanjian perdata;
3. Konvensi III Den Haag tentang cara memulai peperangan yang berjudul "*Convention Relative to the Opening of Hostilities*". Perang dalam arti hukum adalah perang yang dimulai dengan konvensi ini. Perang tidak dapat dimulai tanpa adanya pernyataan perang yang disertai alasan atau dengan suatu ultimatum, dengan pernyataan perang jika ultimatum itu tidak dipenuhi;
4. Konvensi IV Den Haag tentang Hukum dan Kebiasaan Perang di Darat Dilengkapi dengan Peraturan Den Haag yang berjudul lengkap "*Convention Respecting to Laws and Customs of War on Land*" merupakan penyempurnaan dari Konvensi Den Haag Tahun 1899. Konvensi IV Den Haag hanya terdiri dari 9 pasal, yang dilengkapi dengan lampiran yang disebut Hague Regulation;
5. Konvensi V Den Haag Mengenai Hak dan Kewajiban Negara serta Warga Negara Netral dalam Perang di Darat yang berjudul "*Neutral Power and Persons in Land*". Pengertian tersebut membedakan antara Negara Netral dengan Orang Netral. Negara Netral merupakan negara yang menyatakan akan bersikap netral dalam suatu peperangan yang sedang berlangsung,

sedangkan Orang Netral adalah warga negara dari suatu negara yang tidak terlibat dalam peperangan;

6. Konvensi VI Den Haag tentang Status Kapal Dagang Musuh pada saat Dimulai Peperangan;
7. Konvensi VII Den Haag tentang Status Kapal Dagang yang Menjadi Kapal Perang;
8. Konvensi VIII Den Haag tentang Penempatan Ranjau Otomatis di dalam Laut;
9. Konvensi IX Den Haag tentang Pemboman oleh Angkatan Laut di Waktu Perang;
10. Konvensi X Den Haag tentang Adaptasi Asas-asas Konvensi Jenewa tentang Perang di Laut;
11. Konvensi XI Den Haag tentang Pembatasan Tertentu terhadap Penggunaan Hak Penangkapan dalam Perang Angkatan Laut;
12. Konvensi XII Den Haag tentang Mahkamah Barang-barang Sitaan;
13. Konvensi XIII Den Haag yang berjudul "*Neutral Right and Duties in Maritime War*" mengatur Hak dan Kewajiban Negara Netral dalam Perang di Laut.

b. Konvensi Jenewa

Konvensi Jenewa mengatur mengenai perlindungan korban perang, terdiri dari atas beberapa perjanjian pokok. Perjajian tersebut adalah keempat konvensi jenewa 1949, yang masing-masing adalah;

1. *Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Conflict.*

2. *Geneva Convention II for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*
3. *Geneva Convention III relative to the Treatment of Prisoners of War*
4. *Geneva Convention IV relative to the Protection of Civilian Persons in Time of War.*

Pada tahun 1977 ditambahkan lagi beberapa protocol yang biasa disebut Protokol Tambahan (*Additional Protocol*), yaitu;

1. *Protocol Additional to the Geneva Convention of 12 August 1949, And relating to the Protections of Victims of International Armed Conflict (Protocol I)*
2. *Protocol Additional to the Geneva Conventions of 12 August 1949, And relating to the Protection of Victims of Non International Armed Conflict (Protocol II)*

2. Hukum Kebiasaan Humaniter Internasional

Hukum kebiasaan humaniter internasional merupakan bagian dari hukum kebiasaan internasional, hukum kebiasaan humaniter internasional telah dianggap relevan untuk diterapkan di dalam konflik bersenjata internasional. Di rumuskannya hukum kebiasaan humaniter internasional adalah sebagai langkah antisipasi terhadap Negara yang tidak atau belum meratifikasi perjanjian internasional yang dianggap penting, sehingga Negara tersebut akan tetap terikat dengan hukum kebiasaan humaniter internasional tersebut.

Penelitian mengenai hukum kebiasaan humaniter internasional di mulai pada tahun 1996, di mana penelitian tersebut diprakarsai oleh ICRC yang bekerja sama dengan

berbagai ahli yang berasal dari berbagai Negara, dan adanya ahli-ahli tersebut adalah untuk mempermudah bagaimana praktik Negara khususnya dalam bidang hukum humaniter internasional.[106] Penelitian tersebut menghasilkan 161 peraturan, peraturan tersebut didasarkan pada aturan-aturan hukum humaniter yang pada umum telah diterapkan pada konflik-konflik bersenjata.[107] Penelitian tersebut terbagi menjadi dua bagian, bagian pertama berisi aturan-aturan mengenai penerapan hukum kebiasaan dalam konflik bersenjata, dan bagian kedua berisi, semua aspek didalam hukum humaniter internasional, rangkuman yang relevan mengenai praktik Negara (undang-undang, pedoman militer, kasus hukum, dan pernyataan dari pemerintah), serta praktik organisasi internasional, konferensi, badan-badan yudisial dan quasi yudisial.[108]

3. Prinsip Hukum Umum

Prinsip-prinsip hukum umum yang diakui oleh bangsa yang beradab pertama kali diperkenalkan oleh Statuta *Permanent Court of International Justice* dengan maksud untuk menghindari masalah non liquet dalam suatu perkara yang dihadapkan pada hakim.[109] Hakim tidak dapat menolak suatu perkara yang dijatuhkan pedanya dengan alasan tidak ada dasar hukumnya, bila hakim tidak menemukan perjanjian juga hukum kebiasaan yang relevan dengan kasus yang dihadapinya, maka hakim dapat menggunakan prinsip hukum umum ini.

Prinsip hukum umum merupakan prinsip-prinsip hukum yang secara umum tidak hanya terbatas pada hukum internasional saja, tetapi prinsip dalam hukum nasional suatu

---

[106] Anonymous, 2010, ***Customary International Humanitarian Law***, International Committee of the Red Cross, http://www.icrc.org/eng/war-and-law/treaties-customary-law/customary-law/overviewcust omary -law.htm (26 Maret 2013)

[107] *Ibid*

[108] Anonymous, 2010, ***Customary International Humanitarian Law***, Loc.Cit

[109] Sefriani, 2011, **Hukum Internasional: Suatu Pengantar/Sefriani**, Jakarta: Rajawali Pers, hal. 49

negara seperti, hukum pidana dan hukum perdata. Prinsip tersebut antara lain adalah *pacta sunt servanda, good faith, res judicata, nullum delictum nulla poena legenali, nebis indem, clean government*, dan lain-lain.

4. Putusan Pengadilan

Dalam pasal 38 Statuta Mahkamah Internasional menyebutkan putusan pengadilan sebagai sumber hukum tambahan (*subsidiary*).[110] Putusan pengadilan dikatankan sebgai sumber hukum tambahan kerena sumber hukum ini tidak dapat berdiri sendiri sebagai dasar putusan yang diambil oleh hakim, dan putusan pengadilan hanya dapat digunakan untuk memperkuat sumber hukum diatasnya. Putusan pengadilan tidak menciptakan hukum, putusan pengadilan hanya mengikat para pihak saja dan hanya untuk kasus tertentu saja.[111] Hal tersebut dibuktikan dengan adanya pasal 59 Statuta Mahkamah Internasional yang menganut asas *non precedence*.

Putusan pengadilan pada akhirnya juga dapat menimbulkan hukum kebiasaan internasional, ketika putusan pengadilan yang sama untuk kasus-kasus serupa diterapkan berulang. Kemudian hukum kebiasaan internasional tersebut dapat digunakan oleh hakim sebagai dasar putusannya. Adapun kasus yang putusannya telah menjadi hukum kebiasaan internasional adalah, putusan mengenai genosida di tahun 1951, putusan tersebut di jadikan patokan terhadap kasus *Barcelona Traction*, dan kasus lain yang serupa.[112]

---

[110] *Ibid*, hal. 50
[111] Sefriani, *Op.Cit*, hal. 50
[112] Chetail, Vincent, 2003, ***The Contribution of International Court of Justice to International Humanitarian Law***, International Committee of The Red Cross, hal. 248

5. *Public Conscience*

Terdapat 2 (dua) perspektif mengenai *public conscience*, yang pertama, merupakan pendapat publik yang terbentuk dari perilaku-perilaku para pihak dalam sebuah konflik dan mendorong perkembangan hukum humaniter internasional, termasuk juga hukum kebiasaan.[113] Yang kedua, *public conscience* merupakan refleksi dari *opinio juris* atau opini hukum. Public conscience banyak dikaitkan dengan prinsip-prinsip kemanusiaan seperti yang terkandung dalam Klausula Martens, pada tahun 1899 ketika diselenggarakannya *Hague Peace Conferences*, perwakilan dari pihak Rusia mengusulkan sebuah klausula yang harus dimasukkan di dalam pembukaan atau *preamble* dari *Hague Convention II*, adapun bunyi dari klausula tersebut adalah;[114]

> *Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilised nations, from the laws of humanity, and the requirements of the public conscience.*

Inti dari klausula tersebut adalah, bahwa apabila hukum humaniter belum mengatur suatu ketentuan hukum mengenai masalah-masalah tertentu, maka ketentuan yang dipergunakan harus mengacu kepada prinsip-prinsip hukum internasional yang terjadi dari kebiasaan yang terbentuk diantara negara-negara yang beradab, dari hukum kemanusiaan, serta dari pendapat publik (*public conscience*).[115]

---

[113] Meron, Theodor, 2000, ***The Martens Clause, Principles of Humanity, and Dictates of Public Conscience***, The American Journal of International Law, hal. 83

[114] Crawford, Emily, 2011, ***The Modern Relevance of The Martens Clause***, The University of Sydney, Sydney Law School, hal. 3

[115] Arlina Permanasari dkk, *Op.Cit*, hal. 50

Versi pertama dari klausula martens yang terdapat dalam pembukaan Konvensi Den Haag II 1899 mengacu pada *laws of humanity* sedangkan versi berikutnya yaitu yang tertulis di dalam Protokol Tambahan I, mengacu kepada ungkapan *principles of humanity* yang ditafsirkan sebagai pelarangan atas penggunaan sarana dan metode berperang yang tidak penting bagi tercapainya suatu keuntungan militer yang nyata.[116]

G. Prinsip-Prinsip Dalam Hukum Humaniter Internasional

1. Prinsip Pembedaan (*Distinction Principle)*

Prinsip pembedaan lahir dari hukum kebiasaan internasional khususnya humaniter, prinsip ini menuntut para pihak dalam suatu peperangan untuk selalu membedakan antara penduduk sipil (*civilian*) dan kombatan (*combatant*) serta obyek sipil (*civilian object*) dan obyek militer (*military object*), untuk menghindarkan populasi penduduk sipil dari tindakan permusuhan dan efeknya.[117] Pada dasarnya prinsip pembedaan mengatur siapa dan apa saja yang dapat diserang (*attacked*), dan serangan tersebut sesuai dengan nilai kekerasan (*act of violence*) atau penderitaan yang akan timbul.[118]

Di dalam artikel 52 (2) Protokol I mendefinisikan obyek militer berdasarkan hukum kebiasaan internasional, terdapat 2 (dua) kriteria dalam menentukan obyek militer yang pertama, obyek tersebut memberikan kontribusi secara efektif terhadap aksi-aksi militer yang ditujukan pada pihak musuh, yang kedua adalah jika dihancurkan, dikuasai, atau dinetralisir akan memberikan keuntungan militer bagi pihak tersebut.[119] Dalam perang modern timbul apa yang disebut *dual use object*, yaitu suatu obyek yang memiliki

---

[116] Arlina Permanasari dkk, *Op.Cit*, hal. 51
[117] Sassoli, Marco, 2003, ***Legitimate Targets of Attack Under International Humanitarian Law***, Program on Humanitarian Policy and Conflict Research at Harvard University, hal. 1
[118] Sassoli, Marco, *Loc.Cit*, hal. 1
[119] *Ibid*, hal. 3

2 (dua) fungsi, fungsi yang merupakan kategori sipil, dan fungsi yang dapat mendukung tujuan-tujuan militer.[120]

Penerapan *dual use object* yaitu ketika sebuah negara memiliki *power generating stations* atau sumber tenaga listrik, yang secara umum diperuntukkan bagi penduduk sipil, namun secara bersamaan juga menyalurkan tenaga listrik kepada pabrik-pabrik pembuatan senjata untuk memenuhi tujuan militer. Ketika operasi udara NATO di Kosovo, radio dan stasiun TV di Belgrade juga diserang oleh pasukan NATO karena dinilai mendukung menyediakan jaringan komunikasi bagi militer.[121] Prinsip pembedaan telah mendukung deskripsi para pihak dalam suatu peperangan selain kombatan dan penduduk sipil, terdapat mereka yang disebut *unlawful combatant, levee en masse,* tentara bayaran dan lain-lain.

a. Kombatan dan Penduduk Sipil

Kombatan adalah mereka yang memiliki kewenangan untuk terlibat dalam tindakan permusuhan dalam suatu konflik, berdasarkan hukum internasional khususnya hukum humaniter. Hal tersebut di sebutkan dalam Artikel 43 ayat 2 Protokol Tambahan I tahun 1977, bahwa; *Member of the armed forces of a Party to a conflict (other than medical personel and chaplains …) are combatants, that is to say, they have the right to participate directly in hostilities.* Kombatan dapat diserang setiap saat sampai mereka menyerah atau menjadi hors *de combat*, didalam *Common Article 2* disebutkan bahwa, kombatan tidak selamanya menjadi kombatan, mereka dapat mundur dari tindakan permusuhan dengan melalui

[120] *Ibid*, hal. 7
[121] Sassoli, Marco, *Op.Cit*, hal. 4

pensiun atau purna tugas, mobilisasi atau pemindahan, dan menjadi *hors de combatant.*[122]

Kombatan yang jatuh ke tangan musuh harus memperoleh haknya tawanan perang sebagai tawanan perang berdasarkan hukum humaniter internasional, kombatan mempunyai kewajiban untuk setiap saat membedakan dirinya dengan penduduk sipil, seperti yang tertulis dalam Artikel 44 ayat 3 Protokol Tambahan I tahun 1977, yaitu; *In order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population when they are engaged in an attack or in military operation preparatory to an attack.* Dengan adanya artikel tersebut adalah untuk melindungi penduduk sipil dari adanya serangan musuh atau dari tindakkan permusuhan.

Penduduk sipil adalah mereka yang tidak terlibat dalam tindakkan permusuhan dan berhak mendapatkan perlindungan pada saat terjadinya konflik bersenjata. Di dalam praktiknya terkadang sulit untuk membedakan antara penduduk sipil dengan tentara atau kombatan, seperti dalam kasus perang antara Ammerika dengan Vietnam dengan tentara Vietnam yang biasa disebut Vietcong, disiang hari mereka menjadi petani atau pedagang akan tetapi di malam hari mereka menjadi tentara.

b. Milisi dan Korps Sukarelawan

Milisi dan korps sukarelawan atau mereka yang biasa disebut *member of other militias and member of other volunteer,* adalah mereka yang tergolong sebagai partisan dan gerilyawan, mereka dapat turut serta dalam tindakan

[122] Solis, Gary D., 2010, ***The Law of Armed Conflict***, Cambridge University Press, hal 188

permusuhan dan bila tertangkap oleh musuh baik dengan menjadi hors de combat atau menyerah, mereka dapat memperoleh hak-haknya sebagai tawanan perang apabila dianggap telah memenuhi persyaratan yang terdapat di dalam Bab I *Hague Regulation,* yaitu;

> *The laws, rights, and duties of war apply not only to armies, but also to militia and volunteer corps fulfilling the following conditions:*
>
> 1. *To be commanded by a person responsible for his subordinates;*
> 2. *To have a fixed distinctive emblem recognizable at a distance;*
> 3. *To carry arms openly; and*
> 4. *To conduct their operations in accordance with the laws and customs of war.*
>
> *In countries where militia or volunteer corps constitute the army, or form part of it, they are included under the denomination "army."*

berdasarkan artikel tersebut maka, milisi dan korps sukarelawan ketika telah memenuhi persyaratan tersebut diatas, mereka dianggap sebagai tentara atau kombatan yang resmi atau sah.

c. *Levee en Masse*

Di dalam pasal 2 dari Hague Regulations menyatakan bahwa;

> *The inhabitants of territory which has not been occupied, who on the approach of the enemy, spontaneously take arms to resist the invading troops without having had time to organize themselves in accordance with Article 1, shall be regarded as the belligerents if they carry arms openly and if they respect the laws and customs of war*

pasal diatas menjelaskan mengenai siapa yang dianggap sebagai *levee en masse*, *levee en masse* juga bersifat temporal, artinya jika penduduk yang bersangkutan akan melanjutkan perlawanannya maka mereka harus mengorganisir dirinya.[123]

Istilah dari *levee en masse* muncul di tahun 1789 pada saat terjadinya Revolusi Prancis, kemudian mulai mencuat kembali di tahun 1941 dua minggu setelah peristiwa Pearl Harbour, ketika Jepang akan menguasai pulau Wake, lebih dari seratus orang penduduk Amerika yang bekerja sebagai pekerja bangunan di pulau tersebut tewas, lebih dari enam puluh orang yang tewas di sebabkan karena mereka mengadakan perlawanan terhadap tentara Jepang, mereka menggunakan senjata berat untuk mempertahankan pulau tersebut.[124]

d. *Unlawful Combatant*

ICRC Legal Advisory mendiskripsikan apa yang disebut sebagai *unlawfull combatant* sebagai,[125] *All persons taking a direct part in hostilities without being entitled to do so and who thereof cannot be classified as prisoners of war on falling into the power of the enemy (one might add to that definition that the persons taking a direct part must be civilians)* menurut deskripsi tersebut, mereka yang disebut sebagai *unlawful combatant* adalah orang-orang yang terlibat dalam tindak permusuhan akan tetapi tidak dapat memperoleh haknya sebagai tawanan perang.

Istilah unlawful combatant pertama kali muncul di tahun 1951 dalam artikel yang ditulis oleh Richard Baxter, dalam artikel tersebut *unlawful*

[123] Arlina Permanasari dkk, *Op.Cit*, hal. 78
[124] Solis, Gary D, *Op.Cit*, hal 200
[125] Solis, Gary D., *Op.Cit*, hal. 207

combatant disebut sebagai *unprevileged belligerents*.[126] Unlawful combatant dapat terdiri dari sebuah grup yang terorganisir. Ketika terjadinya perang antara Amerika dengan Vietnam, grup tentara penduduk Vietnam atau yang dikenal sebagai Vietcong, mereka melakukan pertempuran atau terlibat dalam tindak permusuhan pada malam hari akan tetapi di siang hari mereka hidup sebagi petani atau pedagang.

2. *Military necessity*

Military necessity merupakan gagasan dari Francis Lieber yang tercantum didalam artikel 14 Lieber Code, yang menyebutkan bahwa, military necessity , *as understood by modern civilized nations, consist in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usage of war*, yang intinya adalah tindak kekerasan yang berlebihan dan penggunaan kekuatan harus sesuai dengan keperluan.[127] *Military necessity* juga tercantum di dalam Konvensi Den Haag 1907 di artikel 23(g). Sebelumnya, *military necessity* dianggap sebagai cabang dari *doktrin kriegraison geht vor krieg manier (necessity in war overrules the manner of warfare)*.[128]

Para ahli hukum internasional bahwa, military necessity dal paktiknya harus disertai dengan prinsip-prinsip kemanusiaan atau *humanity*, untuk mewujudkan suatu keseimbangan. Belakangan ini *military necessity* disebut sebagai suatu pengecualian, berdasarkan jurnal yang di tulis oleh Nobuo Hayashi bahwa, syarat-syarat untuk bisa dikatakan sebagai *military necessity* adalah:

---

[126] *Ibid*, hal. 208
[127] Solis, Gary D., *Op.Cit*, hal. 258
[128] Schmitt, Michael.N., 2010, ***Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance***, Virginia Journal of International Law Vol. 50:4, hal. 797

1. *That the measure was taken primarily for some specific military puspose;*
2. *That the measure was required for the attainment of military purpose;*
3. *That the military purpose for which the measure was taken was in conformity with internasional humanitarian law, and;*
4. *That the measure itself was otherwise in conformity with international humanitarian law*

Nobuo Hayashi berpendapat bahwa, poin ke tiga dan ke empat dari spesifikasi tersebut mengarah pada suatu kewajiban yang spesifik, yang menyatakan suatu klausa yang bersifat pengecualian.[129]

3. Penderitaan Yang Tidak Perlu (*Unnecessary Suffering*)

Unneccesary suffering tercantum di dalam *Additional Protocol I Article 35*, yang menyatakan bahwa; *It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering*. Menurut artikel tersebut, penggunaan senjata, proyektil, dan metode berperang yang menyebabkan cidera yang berlebihan dan penderitaan yang tidak perlu sepenuhnya dilarang. Contoh dari *superfluous injury* yaitu, tentang senjata *combat shotgun*, Amerika menyatakan bahwa;[130]

> *The combat shotgun raises two issues with regard to legality. First, does a weapon capable of inflicting multiple wounds upon a single enemy combatant cause superfluous injury,… second, does the No.∞ buckshot projectile… expand or flatten easily, in violation of the Hague Declaration Concerning Expanding Bullets of 29 July 1899? … In determining whether a weapon causes superfuous injury, a balancing test is applied between the force dictated by military necessity to achieve a legitimate objective vis-à-vis injury that may be considered*

[129] Hayashi, Nobuo, 2010, ***Requirements of Military Necessity in Internasional Humanitarian Law and Internasioanal Criminal Law***, Boston University International Law Journal, hal. 62
[130] Solis, Gary D., *Op.Cit*, hal. 271

> *superfluous to achievement of the … objective (in other words, whether the suffering caused is out of proportion to the military advantage to be gained) … The degree of superfluous injury must be clearly disproportionate to the intended objectives for the development of the weapon (that is, the suffering must outweigh substantially the military necessity for the weapon).*

dalam pernyataan tersebut, *combat shotgun* menimbulkan cidera yang berlebihan karena menimbulkan luka yang berlipat-lipat terhadap satu orang musuh, serta peluru yang berjenis *buckshot* yang dapat meluas dan merata, dimana hal tersebut bertentangan dengan *Hague Declaration Concerning Expanding Bullets of 29 July 1899.*

International committee of the red cross atau ICRC juga melarang penggunaan ranjau anti personil karena, tidak bisa membedakan antara kombatan dengan penduduk sipil, berdasarkan *The Red Cross Wound Classification*, terdapat tiga tingkat untuk menentukan luka, yang pertama adalah luka yang disebabkan oleh energi yang ringan atau rendah (*low energy),* yang kedua adalah luka yang disebabkan oleh energi yang tinggi atau *high energy*, yang terakhir adalah luka-luka yang berat melebihi tingkat ke dua atau biasa disebut *very large wounds.*[131] Efek dari persenjataan yang menimbulkan luka juga dapat diukur berdasarkan beberapa faktor:[132]

1. *the mortality caused by a weapon system in the field (in military terms, those killed in action*
2. *proportion of casualties that die after reaching a medical facility (died of wounds)*
3. *the hospital mortality*
4. *the number of days the survivors have to stay in hospital*
5. *the number of operation they require*

---

[131] Coupland, Robin M., 1996, ***The Effect of Weapon: Defining Superflous Injury and Unnecessary Suffering***, A1 Medicine & Global Survival Vol.3, hal. 2

[132] *Ibid*, hal. 3

6. *the number of units of blood they need during treatment*
7. *the residual disability among the survivors*

4. Prinsip Proporsionalitas *(Proportionality)*

Di dalam *Additional Protocol* I Tahun 1977 di artikel 51 ayat 5 (b) mendiskripsikan *proportionality* sebagai, *an attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated*. Pasal tersebut menuntut adanya antisipasi dari komandan militer dalam kaitannya dengan serangan-serangan yang berlebihan yang dapat menimbulkan hilangnya nyawa penduduk sipil serta hancurnya obyek sipil. Dasar dari *proportionality* adalah serangan yang mengenai penduduk sipil.

Prinsip *proportionality* berkaitan dengan *indiscrimate attack* atau serangan yang tidak dapat membedakan, *indiscrimate attack* tercantum di dalam artikel 51 ayat 4 Protokol Tambahan I, yaitu;

Indiscrimate attack are prohibited, Indiscrimate attack are;

a) which are not directed at a specific military objective
b) which employ a method or means of combat which cannot be directed at a specific military objective; or
c) which employ a method of means of combat the effects of which cannot be limited as required by this protocol

and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Dalam Subparagraf (a), menjelaskan bahwa penyerangan harus diarahkan pada *military object* (obyek militer), senjata dalam penyerangan tersebut tidak diperbolehkan mengenai obyek sipil atau keduanya secara bersamaan yaitu obyek sipil dan obyek militer. Contoh kasus adalah pada saat Perang Teluk, Irak menyerang Israel dengan menembakkan

missile ke pemukiman padat penduduk, namun area tersebut juga merupakan basis militer dari Israel.[133] Contoh kasus lainnya, yaitu pada saat Amerika Serikat menginvasi Irak, saat Amerika Serikat menyerang menggunakan serangan udara di mana pesawat tempur yang digunakan memakai sofware yang di beri nama *bug splat* yang mengakibatkan banyaknya korban sipil berjatuhan karena adanya *collateral damage.*[134]

H. *Tallinn Manual On International Law Applicable to Cyber Warfare*

Tallinn Manual merupakan sebuah pedoman atau petunjuk mengenai perang cyber atau *cyber warfare*, dimana pedoman tersebut di dasarkan atas hukum internasional khususnya mengenai hukum humaniter internasional. Tallinn Manual tersebut mulai di susun di tahun 2009 yang di pelopori oleh NATO *Cooperative Cyber Defence Centre of Exelence,* sebuah organisasi militer internasional yang berbasis di Tallinn dan Estonia, dan telah diakreditasi oleh NATO sebagai *Centre of Exelence*. Selain itu, penyusunan Tallinn Manual juga di dasari oleh banyaknya serangan cyber atau *cyber attack* yang dilakukan oleh sebuah Negara terhadap Negara lain yang telah terjadi sejak tahun 1990 atau ketika mulai diperkenalkannya istilah *Cyber Operations* sampai di tahun 2007, Estonia terkena dampak dari adanya *cyber attack* yang dilakukan oleh Rusia.

Ruang lingkup dari Tallinn Manual sendiri meliputi, *jus ad bellum* atau hukum internasional yang mengatur mengenai *use of force* atau tindakan-tindakan penggunaan kekuatan bersenjata yang dalam hal ini adalah aktivitas-aktivitas cyber yang ditujukan untuk menyerang Negara lain. Kemudian, ketika hal tersebut telah menjadi konflik bersenjata atau *cyber warfare* maka *jus in bello* akan diterapkan. Cyber Espionage atau spionase cyber bukan termasuk hal yang diatur di dalam Tallinn Manual. Tallinn Manual

[133] Solis, Gary D., *Op.Cit*, hal. 275
[134] *Ibid*, hal. 277

diterapkan berdasarkan cyber to cyber operation, hal yang seperti penyerangan terhadap cyber infrastruktur dengan menggunakan senjata lethal atau senjata konvensional tidak dapat dikategorikan sebagai *cyber warfare* atau *cyber attack.*

Aturan dalam Tallinn Manual di bagi dalam 7 bagian, yaitu;

I. States And Cyberspace
II. The Use of Force
III. The Law of Armed Conflict Generally
IV. Conduct of Hostilities
V. Certain Persons, Object, and Activities
VI. Occupation
VII. Neutrallity

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan metode *yuridis normatif* yaitu mengkaji dan menganalisis mengenai konsepsi *cyber warfare* berdasarkan peraturan-peraturan dalam hukum internasional. Penelitian yuridis normatif *(normative legal)*, disini dimaksudkan bahwa, permasalahan hukum yang menjadi objek kajian dianalisis berdasarkan pada sumber-sumber berupa peraturan-peraturan yang berlaku, teori-teori hukum dan doktrin-doktrin para sarjana hukum terkemuka.

B. Pendekatan Penelitian

Pendekatan penelitian yang digunakan dalam karya ilmiah ini yaitu pendekatan *statute approach*,[135] yaitu pendekatan yang digunakan dalam penelitian hukum yang dilakukan dengan menelaah peraturan-peraturan yang berhubungan dengan isu hukum di bidang hukum humaniter internasional. Kemudian pendekatan selanjutnya yaitu model pendekatan konsep *(conceptual approach)*,[136] yakni pendekatan yang di dasarkan atas konsep atau gagasan yang berhubungan dengan *cyber warfare*. Terakhir adalah pendekatan kasus atau *case approach* yaitu dengan melakukan telaah terhadap kasus *cyber warfare* antara Rusia dengan Georgia.

---

[135] Peter Mahmud Marzuki, **Penelitian Hukum, Kencana**, Jakarta, 2005, hal. 93

[136] Johny Ibrahim, **Teori dan Metode Penelitian Hukum Normatif**, Bayumedia, Malang, 2006, hlm 313-315

C. Bahan Hukum

a. Bahan Hukum Primer

Bahan hukum primer merupakan data yang diperoleh dari bahan-bahan hukum yang mempunyai kekuatan hukum tetap dan mengikat137 serta berhubungan langsung dengan masalah yang diteliti. Bahan-bahan primer dalam penelitian ini terdiri dari:

a) Konvensi Den Haag:
   1) Konvensi Den Haag 1899, Konvensi I,II, dan III
   2) Konvensi Den Haag 1907, Konvensi I-XIII
b) Konvensi Jenewa 1949:
   1) Konvensi Jenewa I, mengenai Perbaikan Keadaan Anggota Angkatan Bersenjata yang Terluka dan Sakit di Darat.
   2) Konvensi Jenewa II, mengenai Perbaikan Keadaan Anggota Angkatan Bersenjata yang Terluka, Sakit, dan Karam di Laut.
   3) Konvensi Jenewa III, mengenai Perlakuan Tawanan Perang.
   4) Konvensi Jenewa IV, mengenai Perlindungan Orang Sipil di Masa Perang
c) Konvensi Jenewa 1977:
   1) Protokol Tambahan I, mengenai Perlindungan Korban dalam Konflik Bersenjata Internasional.
   2) Protokol Tambahan II, mengenai Perlindungan Korban dalam Konflik Bersenjata Non-Internasional

137 Amirudin, Zainal Asikin, 2003, **Pengantar Metode Penelitian Hukum**, PT RajaGrafindo Persada: Jakarta, hlm 47

d) *Draft Talinn Manual on the International* Law *Applicable to* Cyber Warfare

b. Bahan Hukum Sekunder

Bahan hukum sekunder adalah bahan-bahan hukum yang memberikan penjelasan mengenai bahan hukum primer. Bahan hukum sekunder dalam penelitian ini yaitu:

a) Pendapat para pakar Hukum Internasional mengenai *Cyber Warfare*.
b) Buku-buku Hukum Humaniter.
c) Jurnal Hukum Humaniter Internasional.
d) Artikel Hukum Humaniter Internasional.

c. Bahan Hukum Tersier

Bahan hukum tersier adalah bahan hukum yang dapat menunjang bahan hukum primer dan bahan hukum sekunder. Bahan hukum tersier dalam penelitian ini adalah:

a) Round Table on Cyberwar and the Rule of Law
b) Website Ilmiah Hukum
c) Kamus Hukum

D. Teknik Pengumpulan Bahan Hukum

Bahan hukum primer yang digunakan oleh penulis di kumpulkan melalui studi pustaka dan mengumpulkan berbagai informasi yang terkait serta beberapa informasi penunjang yang dapat membantu menemukan baik data terbaru mengenai *Cyber Warfare*. Penulis juga mendapat bahan dari mengutip langsung baik dari kamus dan buku- buku lain yang membantu penulisan ini.

E. Metode Analisis Bahan Hukum

Metode analisis bahan hukum dalam penulisan ini menggunakan *Diskriptif analytis*. Sumber bahan hukum yang diperoleh kemudian dianalisis dengan cara; *pertama* mendiskripsikan ataupun memberikan suatu gambaran berdasarkan objek kajian yang di analisis. Disini diartikan bahwa bahan hukum yang diperoleh berkenaan dengan objek kajian yaitu mengenai *cyber warfare* Berdasarkan Hukum Humaniter. *Kedua* melakukan interpretasi mengenai *cyber warfare.*

Ketiga membandingkan hasil dari hasil interpretasi tersebut dengan fakta-fakta yang berkaitan dan yang terjadi di lapangan agar terlihat permasalahan-permasalahan yang timbul di lapangan untuk kemudian dilakukan analisis terhadap beberapa hal yang diperbandingakan tersebut agar diperoleh suatu hasil analisis berupa kelebihan ataupun kelemahan yang terdapat di dalamnya. *Keempat* memberikan suatu simpulan serta rekomendasi terhadap bahan hukum yang telah dianalisis tersebut ataupun berdasarkan dari hasil pembahasan yang telah dilakukan.

F. Definisi Konseptual

1) *Cyber Warfare*, adalah penggunaan teknologi *Cyber* untuk melakukan penyerangan ke wilayah lawan dengan melakukan perusakan pada Infrastruktur yang terkomputerisasi, dengan di koordinasikan dengan perang konvensional pada umumnya.
2) Hukum Humaniter Internasional, adalah keseluruhan asas, kaidah dan ketentuan internasional baik tertulis maupun tidak tertulis yang mencakup hukum perang

dan hak asasi manusia, bertujuan untuk menjamin penghormatan terhadap harkat dan martabat seseorang.

3) *Cyberspace*, adalah ruang 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.
4) *Cyberattack,* adalah tindak penyerangan yang dilakukan oleh salah satu pihak terhadap pihak lain melalui *cyberspace* yang tujuannya adalah untuk mengacaukan sistem jaringan komputer serta motivasinya adalah hal-hal yang bersifat politik.
5) Perang, adalah konflik bersenjata yang terjadi baik yang bersifat internasional maupun non-internasional.
6) Serangan, di dalam hukum humaniter internasional di terangkan sebagai *act of violence* atau tindak kekerasan, tindak kekerasan tersebut dapat menimbulkan penderitaan secara fisik maupun mental.

BAB IV

TINJAUAN MENGENAI CYBER WARFARE BERDASARKAN HUKUM HUMANITER INTERNASIONAL (STUDI KASUS PERANG ANTARA RUSIA DENGAN GEORGIA PADA 7 AGUSTUS 2008)

A. Konsepsi cyber warfare berdasarkan prespektif dari hukum humaniter internasional

a. Cyberspace sebagai domain peperangan

Penerapan hukum humaniter internasional dalam suatu konflik bersenjata terikat pada suatu ketentuan dimana perang tersebut terjadi. Di laut, peraturan mengenai peperangan ada dalam konvensi-konvensi yang dihasilkan oleh Konferensi Perdamaian II di Den Haag seperti, konvensi VI tentang Status Kapal Dagang Musuh pada saat Permulaan Peperangan, konvensi IX tentang Pemboman oleh Angkatan Laut di Waktu Perang, dan konvensi XIII tentang Hak dan Kewajiban Negara Netral dalam Perang di Laut, kemudian terdapat San Remo Manual yang juga memuat petunjuk perang dilaut. Kemudian di darat, hampir semua peraturan mengenai konflik bersenjata mengatur perang di darat seperti konvensi jenewa dan konvensi den haag, serta di udara juga terdapat aturan mengenai larangan menembak pesawat sipil yang terdapat di dalam San Remo Manual.

Menurut *Joint Publication*, cyberspace adalah *domain global* (global domain) yang merupakan lingkungan informasi yang terdiri dari jaringan infrastruktur teknologi

informasi yang saling terkait, termasuk internet, jaringan telekomunikasi, sistem komputer, serta processors and controllers.[138] Kemudian, juga dinyatakan bahwa,[139]

> *Cyberspace is a man-made domain, and is therefore unlike the natural domains of air, land, maritime, and space. It requires continued attention from humans to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable freedom of action for activities in the other domains can create effects in and through cyberspace*

Pernyataan tersebut menyatakan bahwa, *cyberspace* adalah sebuah domain buatan manusia, *cyberspace* membutuhkan perhatian manusia agar tetap ada, kemudian *cyberspace* secara fisik berada atau terletak di semua domain, kegiatan yang dilakukan di dalam *cyberspace* dapat mempengaruhi kegiatan yang dilakukan di domain lainnya, dan sebaliknya kegiatan yang dilakukan di domain lainnya juga dapat mempengaruhi kegiatan yang dilakukan di dalam *cyberspace*

Dalam Artikel 2 (4) Piagam PBB;[140]*All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.* Di dalam artikel tersebut disebutkan mengenai *territorial integrity*, maka penggunaan angkatan bersenjata di laut, darat, dan udara di dasarkan pada adanya teritorial yang di miliki suatu negara, dan teritorial berhubungan dengan kedaulatan (*sovereignty*). Demikian halnya dengan *cyberspace*, untuk dapat dikatakan

---

[138] Anonymouse, 2010, ***Cyber Operations***, Air Force Doctrine Document 3-12, hal. 1
[139] *Ibid*, hal. 2
[140] Hovel, Devika, 2004, ***Chinks in the Armour: International Law, Terrorism, and The Use of Force***, UNSW Journal, hal. 399

sebagai domain di dalam peperangan maka, terlebih dahulu harus ditentukan kedaulatan (*sovereignty*) suatu Negara di dalam *cyberspace*.

Bodley mendefinisikan kedaulatan (*sovereignty*) sebagai berikut;[141]

> *States whose subjects or citizens are in the habit of obedience to them, and which are not in themselves subject to any other (or paramount) State in any respect… In the intercourse of nations, certain States have a position of entire independence of others … This power of independent action in external and internal relations constitutes complete sovereignty.*

Definisi tersebut menjelaskan bahwa, kedaulatan suatu Negara terdiri dari kedaulatan eksternal dan internal, dimana kedaulatan eksternal adalah semua hal yang berkaitan dengan luar negeri serta kekuatan pertahanan untuk melindungi teritorial Negara dari serangan Negara lain.[142] Sedangkan kedaulatan yang internal adalah kewenangan yang dimiliki oleh suatu Negara untuk menjalankan fungsinya dalam lingkup nasional.[143]

Dari definisi mengenai kedaulatan diatas maka, penentuan kedaulatan di dalam *cyberspace* di dasarkan pada adanya kewenangan dari suatau Negara untuk mengatur aktivitas *cyber* di dalam Negara tersebut (*internal sovereignty*) dan bagaimana penggunaan aktivitas *cyber* dan infrastruktur *cyber* dalam hal pertahanan dan keamanan di dalam Negara tersebut (*external sovereignty*). Dalam *Tallinn Manual The International Law Applicable to Cyber Warfare Rule 1. Sovereignty* menyatakan bahwa;[144]*A State may exercise control over cyber infrastructure and activities within its sovereign territory.* Peraturan tersebut menjelaskan bahwa, suatu Negara dapat

---

[141] MP Ferreira-Snyman, 2006, ***The Evolution of State Sovereignty: A Historical Overview***, University of Leyden Netherland, hal. 4
[142] MP Ferreira-Snyman, *Loc.Cit*, hal. 4
[143] MP Ferreira-Snyman, *Loc.Cit*, hal. 4
[144] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 1.

menjalankan kontrol terhadap infrastruktur *cyber* dan aktivitas *cyber* di dalam wilayah kedaulatannya.

Berdasarkan kedua penjelasan diatas yang di dasarkan dari definisi yang diberikan oleh Bodley mengenai kedaulatan dan peraturan mengenai kedaulatan yang tercantum dalam *Tallinn Manual The International Law Applicable to Cyber Warfare* maka, ketika suatu Negara memiliki kapabilitas dalam hal infrastruktur *cyber* dan aktivitas *cyber*, Negara tersebut dapat dikatakan telah memiliki kedaulatan di dalam *cyberspace*, dan syarat umum yang terdapat dalam hukum internasional mengenai *cyberspace* untuk dapat dikatakan sebagai domain terpenuhi.

b. **Serangan (*Attack*) Dalam Cyber Warfare**

Serangan yang dilancarkan oleh pihak-pihak yang terlibat dalam suatu peperangan atau konflik bersenjata, merupakan suatu bentuk tindak kekerasan atau *act of violence*, umumnya serangan tersebut dilakukan dengan senjata konvensional. Di dalam *cyber warfare* yang dimaksud serangan adalah serangan *cyber* atau *cyber attack*, untuk mengkategorikan *cyber attack* sebagai serangan bersenjata atau *armed attack* di perlukan tinjauan dan kriteria tertentu.

Serangan cyber atau *cyber attack* yang menggunakan senjata *cyber* atau *cyber weapon* yang merupakan bagian dari *methods of attack* pada umumnya disebut sebagai virus, trojan, worm, botnets yang memiliki efek-efek melumpuhkan yang umumnya bersifat non-lethal membuatnya sulit di identifikasi. Kriteria mengenai serangan bersenjata tidak di tulis secara jelas di dalam peraturan-peraturan mengenai konflik bersenjata.

Peraturan mengenai konflik bersenjata tradisional menekankan bahwa, kematian atau cedera/luka-luka fisik yang terjadi pada seseorang dan kehancuran benda-benda merupakan kriteria dari *use of force* dan *armed attack.* Seorang ahli hukum internasional Michael Schmitt mengajukan enam kriteria yang sekaligus menjadi pedoman bahwa, *cyber attack* merupakan serangan bersenjata atau *armed attack*, yaitu;

1. ***Severity*** *looks at the scope and intensity of an attack. Analysis under this criterion examines the number of people killed, size of the area attacked, and amount of property damage done.* Melihat akibat yang ditimbulkan dari adanya serangan *cyber* yaitu, penggunaan virus, botnet, *DDoS* untuk melumpuhkan sistem komputer termasuk infrastruktur yang terkomputerisasi atau yang tergolong sebagai *critical infrastructure* seperti bendungan, pembangkit listrik, infrastruktur medis, telekomunikasi, ekonomi, bahkan mengacaukan *air traffic control (area attacked)* dimana hal-hal tersebut secara tidak langsung akan menimbulkan kematian (*people killed*) karena, tidak adanya listrik, air yang sulit didapat, tidak ada pertolongan medis, dan tidak adanya komunikasi. Meskipun di dalam hukum humaniter internasional di jelaskan bahwa yang dapat menjadi target adalah hal-hal yang berkaitan dengan militer namun, kembali kepada sifat dari pada *cyber attack* yang pada umumnya tidak bisa membedakan atau *indiscriminate*. Menurut Scimitt dan berbagai analisis mengenai efek-efek dari *cyber attack* tersebut, hampir sama dengan apa yang mungkin bisa disebabkan oleh nuklir atau bom Hiroshima dan patutlah bila *cyber attack* dikatakan memenuhi kriteria ini. Selain itu

penyerangan yang ditujukan kepada website pemerintahan, dapat menyebabkan terganggunya kinerja pemerintah.

2. ***Immediacy*** *looks at the duration of a cyber attack, as well as other timing factor. Analysis under this criterion examines the amount of time the cyber attack lasted and duration of time that the effect were felt.* Dalam cyber attack, serangan menggunakan virus, worms, dan trojan menimbulkan dampak yang panjang, tergantung dari penanganan yang dapat dilakukan. Virus, worms, dan trojan akan menginfeksi file yang berada dalam sistem komputer selama sistem komputer tersebut menyala atau bekerja (*the amount of time the cyber attack lasted*), efeknya mulai dirasakan ketika file-file atau program-program yang penting bagi sistem komputer tersebut terinfeksi dan mengacaukan kinerja komputer tersebut. Menurut Schmitt, adanya jumlah waktu dari *cyber attack* untuk bertahan dan durasi yang dibutuhkan agar efek tersebut dapat dirasakan maka, *cyber attack* memenuhi kriteria ini. Selain itu waktu eksekusi yang cepat turut mendukung.
3. ***Directness*** *looks at the harm caused. If the attack was the proximate cause of the harm, it strengthens the argument that the cyber attack was an armed attack. If the harm was caused in full or in part by other parallel attacks, the weaker the argument that the cyber attack was an armed attack.* Efek yang ditimbulkan dari adanya *cyber attack* dapat merugikan atau melukai secara mental atau *mentally harm*, dimana luka mental mengawali timbulnya *incidental loss of life* atau korban jiwa. Contohnya, *shutting down a power grid* atau mematikan pembangkit listrik, membuat semua aspek kehilangan

kinerjanya, tidak adanya proses medis, tidak berfungsinya pabrik, menimbulkan penderitaan mental.

4. ***Invasiveness*** *looks at the locus of the attack. An invasiveness attack is one that physically crosses state border, or electronically crosses borders and causes harm within the victims state.* Menurut Schmitt, *the more invasiveness the cyber attack, the more looks like an armed attack.*
5. ***Measurability*** *tries to quantify the damage done by the cyber attack. Quantifable harm is generally treated more seriously in the international community. The more a state can quantify the harm done to it.* Terpenuhinya kriteria ini dibuktikan dengan adanya *harm* atau luka-luka.
6. ***Presumptive legitimacy*** *focuses on state practice and the accepted norms of the behavior of international community. Actions may gain legitimacy under the law when international community accepts certain behavior as legitimate.*Menurut Schmitt, kurangnya diterimanya *cyber attack* berdasarkan praktik Negara-negara (*states practice*), memperkuat bukti bahwa, *cyber attack* adalah *illegal use of force or an armed attack.*

Di dalam *Additional Protocol I Article 49*, mendefinisikan *attacks* sebagai, *acts of violence against the adversary, whether in offence or in defence*.[145] Dalam Artikel tersebut *violence* harus dianggap sebagai pengertian dari *violent consequences* dari pada *violent acts.*[146] Dalam kasus Nicaruagua v. U.S berdasarkan keputusan dari *International Court of Justice* bahwa, kriteria dari *use of force* dapat didasarkan pada skala (*scale*) dan

[145] Protocol Additional to The Geneva Convention of 12 August 1949, Article 49 (1)
[146] Richardson, John, 2011**, *Stuxnet As Cyberwarfare: Distinction and Proportionality On The Cyber Battlefield***, National Academic of Science, hal. 14

efek (*effect*). Beberapa sarjana menyetujui tiga model pendekatan yang diberikan oleh Jean Pictet yang disebut sebagai *Use of Force Continuum*, yakni;[147]

1. *Instrument based approach*, *cyber attack* yang ditujukan untuk mematikan sumber pembangkit listrik yang terkomputerisasi atau mematikan *air traffic control system* seperti halnya menjatuhkan bom di sumber pembangkit listrik yang dikenal dalam perang konvensional. Namun pendekatan ini tidak dapat diterapkan pada serangan yang hanya mengakibatkan hancurnya data-data seperti yang diakibatkan oleh virus.
2. *Strict liability approach*, seraangan terhadap kritikal infrastruktur merupakan serangan bersenjata (*armed attack*) apabila serangan tersebut menimbulkan efek yang berat, pendekatan ini tidak dapat diterapkan apabila efek dari serangan tersebut kecil atau tidak memiliki pengaruh yang besar terhadap Negara yang diserang.
3. *Effects based approach*, biasa disebut juga dengan *consequence based approach*, pendekatan ini menjelaskan bahwa, yang menjadi dasar adalah bukan dari apakah kerusakan yang dihasilkan oleh suatu serangan dapat diterima berdasarkan pengertian kerusakan secara tradisional, melainkan semua efek yang ditimbulkan oleh serangan tersebut terhadap suatu Negara. Berdasarkan pendekatan ini maka, *cyber attack* bisa dikatan sebagai *armed attack* karena, efek dari *cyber attack* yang menimbulkan kekacauan atau gangguan yang mempengaruhi penduduk yang berada di Negara tersebut

[147] *Ibid*, hal. 16

c. Penerapan Prinsip Pembedaan *(Distinction Principle)* dalam *Cyber warfare*

Adapun Artikel yang mengawali prinsip pembedaan adalah *Article 48 Additional Protocol I* yang menjelaskan bahwa;[148]

> *In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.*

Artikel tersebut menjelaskan mengenai kewajiban para pihak untuk membedakan antara, penduduk sipil dan kombatan, serta obyek sipil dengan obyek militer. Artikel tersebut berlanjut pada kualifikasi untuk dapat dikatakan sebagai kombatan atau penduduk sipil, seperti dalam perang konvensional kualifikasi ini juga di perlukan di dalam *cyber warfare,* kualifikasi tersebut adalah;

a) Kualifikasi kombatan

Sebagaimana dijelaskan dalam *Article 43 (2) Additional Protocol I*, bahwa;[149] *Member of armed forces of a party to a conflict (other than medical personnel, and chaplains covered by Article 33 of the Third Convention) are combatant, that is to say, they have the right to participate directly in hostilities*. Dalam artikel tersebut dijelaskan bahwa, *member of armed forces* adalah kombatan, namun untuk dapat dikatakan kombatan ada syarat lain yang harus dipenuhi yang terdapat didalam *Article 4A (2) Geneva Convention III*, yaitu;[150]

a. Being commanded by a person responsible for his subordinates

b. Wearing a distinctive emblem or attire that is recognizeable at a distance

---

[148] Protocol Additional to The Geneva Convention of 12 August 1949, *Article 48*
[149] Protocol Additional to The Geneva Convention of 12 August 1949, Article 43 (2)
[150] Convention III relative to the Treatment of Prisoners of War. Geneva, 12 August 1949, Article 4A (2)

c. *Carrying arms openly*

d. *Conducting operation in accordance with the law of armed conflict*

Dalam perang konvensional yang umumnya terjadi, seseorang yang memegang komando belum tentu dia akan berada di medan pertempuran, akan tetapi semua pasukan atau bawahannya cukup diberikan arahan melalui perantara delegasi komando (dari komando tertinggi kepada komando yang berada dibawahnya). Dalam konteks *cyber warfare,* pemegang komando atau pemimpin pasukan harus memiliki kemampuan atau pengetahuan mengenai *cyberspace,* sekaligus mengetahui hukum perang yang berlaku.

Dalam *Tallinn Manual The International Law Applicable to Cyber Warfare Rule 26. Commentary 9, Members of the Armed Forces* dijelaskan bahwa;[151]

> *The condition of being commanded by a person responsible for subordinates is best understood as an aspect of the requirement that the group in question be 'organized'. The criterion of organization was previously discussed in the context of non-international armed conflict (Rule 23). There, the unique nature of virtual organisations was highlighted. The same considerations apply in the present context. While not normally an issue in respect of regularly constituted State armed forces, or even well-established organized armed groups, a claim of combatant status could be significantly weakened if the persons asserting that status are part of a loosely organised group or association. This could result, for example, from organising solely over the internet. In a similar vein, members of such a group may have difficulty establishing that they are acting under a responsible commander. Even more problematic is the requirement that the group be subject to an internal*

[151] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 26, Commentary 9

> *disciplinary system capable of enforcing compliance with the law of armed conflict. Cumulatively, these requirements make it highly unlikely that a purely virtual organisation would qualify as an organised armed group for the purposes of determining combatant status*.

Menurut *Rule 26. Commentary 9* tersebut, *being commanded by a person responsible for subordinates* harus di pahami sebagai suatu syarat bahwa, adanya seorang pemegang komando atau pemimpin membuktikan bahwa suatu grup terorganisir atau *organized*. Sulit untuk menerapkan status sebagai kombatan jika pengorganisasian hanya dilakukan melalui internet karena, anggota kelompok atau grup akan mengalami kesulitan untuk menetapkan bahwa mereka bertindak berdasarkan adanya komando yang bertanggung jawab. Selain itu, berdasarkan syarat ke empat mengenai *Conducting operation in accordance with the law of armed conflict* akan sulit di terapkan, kepada selain organisasi militer.

Mengenai syarat yang kedua yakni, *wearing a distinctive emblem*, dalam *Tallinn Manual Rule 26. Commentary 10, Member of the Armed Forces,* di jelaskan bahwa;[152]

> *Combatant status requires that the individual wear a 'fixed distinctive sign'. The requirement is generally met through the wearing of uniforms. There is no basis for deviating from this general requirement for those engaged in cyber operations. Some members of the International Group of Experts suggested that individuals engaged in cyber operations, regardless of circumstances such as distance from the area of operations or clear separation from the civilian population, must always comply with this requirement to enjoy combatant status. They emphasised that the customary international law of armed conflict in relation to combatant*

[152] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 26, Commentary 10

> *immunity and prisoner of war status offers no exceptions to this rule. Article 44(3) of Additional Protocol I does provide for an exception. However, it does not reflect customary international law.*

Menurut aturan tersebut, syarat mengenai *Wearing a distinctive emblem or attire that is recognizeable at a distance* syarat tersebut harus dipatuhi, terlepas dari jarak daerah operasi atau pemisahan yang jelas dari penduduk sipil, karena tidak ada pengecualian. Namun, di dalam *Article 44 (3) Additional Protocol I,* yaitu;[153]

> *In order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack. Recognizing, however, that there are situations in armed conflicts where, owing to the nature of the hostilities an armed combatant cannot so distinguish himself, he shall retain his status as a combatant, provided that, in such situations, he carries his arms openly:*
> *(a) During each military engagement, and*
> *(b) During such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate.*

Dalam Artikel tersebut dijelaskan mengenai pengecualian jika kombatan tidak dapat membedakan dirinya dengan penduduk sipil maka, terdapat syarat lain yang harus di penuhi yaitu *he carries his arms openly* atau kombatan tersebut harus membawa senjata secara terang-terangan. Namun dalam *Tallinn Manual Rule 26.*

[153] Protocol Additional to The Geneva Convention of 12 August 1949, Article 44 (3)

Commentary 10, Member of the Armed Forces adanya pengecualian tersebut dianggap tidak sesuai dengan hukum kebiasaan internasional.[154]

Dalam konteks *cyberspace*, kombatan dan penduduk sipil tidak dapat dilihat secara fisik atau secara nyata seperti di dalam medan pertempuran karena, adanya jarak dan tempat yang tidak tentu. Namun, ketika *cyber warfare* di koordinasikan dengan perang konvensional, maka permasalahan mengenai *Wearing a distinctive emblem or attire that is recognizeable at a distance* dapat di tangani, dengan melakukan pemahaman bahwa, pasukan yang menyerang secara konvensional, sama dengan pasukan yang menyerang secara *cyber*, terlepas dari apakah dia pasukan udara, laut, atau darat.

Selanjutnya mengenai syarat ke tiga yaitu, *carrying arms openly* dalam *Tallinn Manual Rule 26. Commentary 13, Member of the Armed Forces*, di jelaskan bahwa;[155]

> *The issue of whether computers and software constitute weapons is discussed in Rule 41 and its accompanying Commentary. However, even if they qualify as weapons, the requirement to carry arms openly has little application in the cyber context.*

Dalam aturan tersebut dijelaskan bahwa, status mengenai *cyber weapons* atau senjata cyber telah di jelaskan dalam Rule 41, yang antara lain yaitu;[156]

> *For the purposes of this Manual:*
>
> *(a) 'means of cyber warfare' are cyber weapons and their associated cyber systems; and*

[154] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 26, Commentary 10
[155] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 26. Commentary 13
[156] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 41

(b) 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted

Kemudian juga di perjelas melalui Commentary 2, bahwa;[157]

> *For the purposes of this Manual, 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 30). The term means of cyber warfare encompasses both cyber weapons and cyber weapon systems. A weapon is generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons. Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack (Rule 30).*

Dalam *Rule 41* tersebut dijelaskan bahwa, sarana-sarana berperang cyber adalah senjata cyber dan mereka di asosiasikan dengan sistem cyber, selanjutnya dalam Commentary 2 di jelaskan bahwa, senjata cyber atau *cyber weapon* merupakan sarana berperang cyber, dengan desain dan penggunaan, yang dapat menyebabkan luka, kematian, kehancuran, atau kerusakan, selain itu dijelaskan pula bahwa, sarana berperang cyber juga termasuk perangkat, peralatan, dan perlengkapan termasuk software yang di desain, dan dapat dipergunakan untuk melakukan serangan cyber. Berdasarkan hal tersebut, maka untuk dapat dikatakan memenuhi persyaratan ke tiga mengenai *carrying arms openly*, di perlukan pemahaman bahwa, membawa senjata secara terang-terangan berarti berkemampuan, memiliki sarana dan perlengkapan, dan memiliki tujuan utama yaitu melancarkan serangan cyber.

[157] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 41, Commentary 2

b) Kualifikasi Penduduk Sipil

Dalam *Article 50 (1) Additional Protocol I*, penduduk sipil atau civilian di definisikan sebagai;[158]

> *A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.*

Penduduk sipil adalah mereka yang tidak memenuhi persyaratan sebagaimana diatur di dalam *Article 4 A Geneva Convention III* dan Article *43 Additional Protocol I*, dengan kata lain penduduk sipil adalah mereka yang tidak dapat memenuhi syarat sebagai kombatan. Dalam konteks *cyberspace*, banyak Negara yang mengandalkan peran penduduk sipil dalam hal, jaringan telekomunikasi atau internet, seperti kerjasama antara pemerintah dengan perusahaan penyedia layanan internet atau yang biasa di sebut *Internet Service Provider* bahkan, dalam hal pembuatan program untuk melindungi jaringan komputer atau melakukan penyerangan.[159] Jika mereka melakukan pekerjaannya pada saat terjadinya *cyber warfare* maupun perang konvensional, mereka dapat dianggap sebagai *persons who accompany the armed forces*, seperti yang tercantum dalam *Article 4 A (4) Geneva Convention III*, yaitu;[160]

> *Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they*

[158] Protocol Additional to The Geneva Convention of 12 August 1949, Article 50 (1)
[159] Schmitt, Michael.N, 2002, ***Wired Warfare: Computer Network Attack***, IRRC, June Vol.84, No. 846
[160] Convention III relative to the treatment of Prisoner of War, Geneva, 12 Agustus 1949, Article 4 A (4)

have received authorization, from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model.

Berkaitan dengan penduduk sipil, di dalam *Tallinn Manual, Rule 29-Civilians*, di jelaskan bahwa; *Civilians are not prohibited from directly participating in cyber operation amounting to hostilities but forfeit their protection from attacks for such time as they so participate.* Aturan tersebut dapat diartikan bahwa, tidak ada larangan bagi penduduk sipil untuk berpartisipasi dalam operasi cyber atau serangan cyber, akan tetapi mereka juga akan kehilangan perlindungan terhadap serangan selama mereka berpartisispasi. Di dalam konvensi tidak ada artikel yang menjelaskan suatu pelarangan mengenai partisipasi penduduk sipil dalam konflik bersenjata, dalam konvensi hanya diterangan mengenai konsekuensi, selain itu dalam konteks cyber warfare, adanya perlawanan dari *hacker patriotic* dapat terjadi, mungkin dalam perang konvensional hal itu dapat disebut sebagai *levee en masse*. Namun, *levee en masse* hanya ditujukan kepada *inhabitant* yaitu penduduk atau masyarakat buka individu atau kelompok kecil.

c) Obyek Sipil dan Obyek Militer

Penjelasan mengenai obyek sipil dan obyek militer terdapat di dalam *Article 52 Additional Protocol I*, yaitu; [161]

(1) Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives

(2) Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those

[161] Protocol Additional to The Geneva Convention of 12 August 1949, Article 52

> *objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military of advantage.*

Jika diperhatikan Artikel diatas memberikan dua syarat terhadap apa yang bisa disebut sebagai obyek militer yaitu, memberikan kontribusi yang efektif terhadap tindakan atau aksi militer dan bila dihancurkan, di kuasai, atau di netralisasi baik secara keseluruhan maupun sebagian dapat memberikan keuntungan militer yang jelas. Jika syarat pertama yaitu, mengenai memberikan kontribusi yang efektif, diartikan sebagai sarana baik yang bersifat lethal maupun non-lethal (wujud dan efeknya) maka, software, perangkat keras, atau peralatan lain yang di gunakan dalam *cyber attack* dapat di golongkan sebagai obyek.

Syarat kedua, mengenai bila dihancurkan, di kuasai, atau di netralisasi baik secara keseluruhan maupun sebagian dapat memberikan keuntungan militer yang jelas, bila kehancuran dapat diartikan juga sebagai kehancuran yang bersifat non-lethal maka, software, perangkat keras, atau peralatan lain yang di gunakan dalam *cyber attack* dapat di golongkan sebagai obyek. Selanjutnya, jika di kuasai atau di netralisasi di artikan sebagai di kuasainya sistem komputer atau infrastruktur yang terkomputerisasi, dan di netralisir berarti menetralisir sistem komputer atau infrastruktur yang terkomputerisasi maka, software, perangkat keras, atau peralatan lain yang di gunakan dalam *cyber attack* dapat di golongkan sebagai obyek.

Mengenai obyek sipil dalam Artikel diatas telah dijelaskan bahwa, obyek sipil adalah semua obyek yang bukan merupakan obyek militer, dengan kata lain

yang di sebut sebagai obyek sipil adalah obyek yang tidak dapat memenuhi dua syarat yang telah diberikan dalam *Article 52 (2) Additional Protocol I*, berarti bahwa, software, perangkat keras atau infrastruktur yang terkomputerisasi memang sepenuhnya tidak di pergunakan untuk *cyber attack*, tidak memberikan keuntungan yang efektif terhadapa aksi-aksi militer, serta tidak memberikan keuntungan militer yang jelas bila dikuasai, di hancurkan atau di netralisir.

Kemudian Artikel tersebut di jelaskan dalam *Tallinn Manual Rule 38 Civilian Object and Military Objectives* , yaitu;[162]

> *Objects Civilian objects are all objects that are not military objectives. Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Military objectives may include computers, computer networks, and cyber infrastructure.*

Isi yang tercantum dalam *Rule 38* tersebut diatas memiliki kesamaan dengan apa yang ada di dalam *Article 52 Additional Protocol I* akan tetapi, dalam Rule 28 dikatakan bahwa, obyek militer dapat termasuk komputer, jaringan computer, dan infrastruktur cyber atau infrastruktur yang terkomputerisasi dimana hal tersebut lebih bersifat menjelaskan. Selain itu, di dalam *Commentary* yang terdapat di dalam *Rule 38* lebih spesifik menerangkan apa yang disebut sebagai obyek dalam aturan tersebut, yaitu;[163]

[162] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38
[163] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38, Commentary 4

The meaning of the term "object" is essential to understanding this and other Rules found in the Manual. An 'object' is characterized in the ICRC Additional Protocols Commentary as something "visible and tangible". This usage is not to be confused with the meaning ascribed to the term in the field of computer science, which connotes entities that can be manipulated by the commands of a programming language. For the purpose of this Manual, computers, computer networks, and other tangible components of cyber infrastructure constitute objects.

Bahwa, istilah mengenai obyek dalam Rule 36 tersebut di dasarkan pada definisi obyek yang ada di dalam *ICRC Additional Protocol Commentary*, dimana dalam Commentary tersebut di jelaskan bahwa obyek merupakan sesuatu yang *visible and tangible* atau obyek tersebut berwujud dan nyata. Berdasarkan Commentary tersebut maka, komputer, jaringan komputer, dan komponen yang lainnya yang merupakan bagian dari infrastruktur cyber harus di pahami sebagai sebuah benda yang berwujud.

Selain itu, berdasarkan *Article 52 (2) Additional Protocol I* juga tercantum bahwa, untuk dapat di katakan sebagai obyek militer harus dapat memenuhi empat kriteria yaitu, *nature, location, purpose, or use*. *Nature* atau sifat meliputi karakter yang melekat pada suatu obyek, dalam konteks militer bisanya mengacu pada benda-benda yang pada dasarnya merupakan benda militer dan dirancang untuk memberikan kontribusi terhadap aksi-aksi militer.[164] Komputer militer dan infrastruktur militer yang terkomputerisasi merupakan contoh paradigmatis benda yang memenuhi kriteria pertama yaitu *nature* atau sifat.[165] Contohnya, infrastruktur militer atau sarana militer yang terkomputerisasi dimana pun benda

[164] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38, Commentary 6
[165] *Ibid*

tersebut ditempatkan, baik permanen maupun tidak, benda tersebut merupakan obyek militer.[166]

Selanjutnya obyek militer di kualifikasikan menurut kriteria yang kedua yaitu, *location* atau lokasi, *location* biasanya merujuk kepada wilayah geografis militer, tetapi location dijelaskan bukan mengenai penggunaan atau peruntukan dari lokasi tersebut untuk kepentingan militer tetapi karena lokasi tersebut memberikan kontribusi yang efektif bagi pihak militer.[167] Contohnya seperti, sebuah operasi cyber yang ditujukan kepada system *supervisory control data acquisition* (SCADA) suatu bendungan, dengan tujuan untuk melepaskan air yang berada di dalam bendungan tersebut untuk menyerang operasi militer musuh yang berlokasi di tempat yang sama dengan bendungan tersebut berada.[168]

Kualifikasi ketiga yaitu, *use* atau kegunaan dijelaskan bahwa, ketika sebuah obyek sipil atau fasilitas-fasilitas tertentu yang digunakan untuk tujuan-tujuan militer, dapat menjadi obyek militer berdasarkan kriteria *use* ini.[169] Seperti penggunaan jaringan computer penduduk sipil untuk tujuan militer.[170] Yang keempat adalah *purpose* atau tujuan, mengacu pada penggunaan suatu obyek di kemudian hari yaitu, obyek yang kemungkinan akan digunakan untuk tujuan-tujuan militer di kemudian hari.[171] Seperti, pembelian perangkat-perangkat komputer oleh pihak militer dan pihak militer tersebut memiliki kemampuan dalam hal teknologi dan informasi, benda-benda tersebut akan memperoleh

[166] *Ibid*
[167] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38, Commentary 7
[168] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38, Commentary 7
[169] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38, Commentary 8
[170] *Ibid*
[171] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 38, Commentary 11

statusnya sebagai obyek militer segera setelah tujuannya jelas, penyerang atau pasukan yang akan menyerang tidak perlu menunggu pihak tersebut menggunakannya untuk tujuan militer karena tujuannya sudah jelas.[172]

d) *Dual use Object*

Dalam konteks *cyberspace*, *dual use object* atau obyek dengan fungsi ganda tidak bisa di hindari keberadaannya contohnya seperti, bandara, rel kereta api, sistem komunikasi, sistem sumber daya listrik, dan pabrik-pabrik yang digunakan untuk memproduksi barang-barang sipil serta barang-barang yang digunakan oleh pihak militer selain itu, satelit juga merupakan *dual use object* contohnya INTELSAT, EUROSAT, dan ARABSAT.[173] Saat terjadinya konflik di Serbia, pasukan udara NATO melakukan pemboman terhadap stasiun televisi milik Serbia yang menurut pihak NATO, stasiun televisi tersebut selain digunakan untuk keperluan sipil juga digunakan untuk keperluan komunikasi militer. Contoh yang terbaru adalah mengenai proyek nuklir Iran yang berada di Natanz (*Natanz facility*), yang menurut pemerintah Iran proyek nuklir tersebut dipergunakan untuk keperluan sumber daya energi dengan adanya hasil dari gas uranium hexafluoride yang dapat di jadikan bahan bakar atom namun, banyak pihak yang mengkalim bahwa kapasitas proyek nuklir tersebut dapat memicu perang nuklir.[174]

Dual use object di dalam Tallinn Manual disebut sebagai *objects used for civilian and military purpose* yang diatur di dalam *Rule 29*, yang menjelaskan bahwa; *An object used for both civilian and military purposes including*

[172] *Ibid*
[173] Schmitt, Michael.N, 2002, *Op.Cit*, hal 384
[174] Richardson, John, 2011, *Op.Cit*, hal. 28

computers, computer network, and cyber infrastruktur is a military objective. Dalam *Commentary* dari *Rule 29* tersebut di jelaskan bahwa, dual use object dapat di terapkan dalam kasus ketika pihak sipil dan pihak militer saling berbagi komputer, jaringan komputer, dan infrastruktur cyber.[175] Dan yang populer adalah penggunaan media sosial atau jejaringan sosial untuk tujuan militer, seperti penggunaan Facebook untuk operasi organisasi perlawanan bersenjata serta penggunaan Twitter untuk melakukan pengiriman informasi militer yang berharga.[176] Akan tetapi ada tiga hal yang harus diperhatikan bahwa didalam Rule 29 tersebut juga di dasarkan pada proporsionalitas dan *precaution attack* atau antisipasi serangan, yang kedua keabsahan operasi cyber yang ditujukan terhadap jejaring sosial bergantung kepada apakah operasi tersebut dapat meningkat menjadi sebuah serangan, yang ketiga, penggunaan Facebook dan Twitter untuk keperluan militer bukan berarti dapat meningkatkan statusnya menjadi target serangan, akan tetapi hanya komponen-komponennya yang digunakan untuk tujuan militer yang dapat di serang.[177]

d. ***Indiscriminate attack***

Dalam *distinction principle* di jelaskan bahwa, serangan harus langsung mengarah pada obyek militer, selain itu juga dilarang adanya *indiscriminate attack* atau serangan yang tidak dapat membedakan. Hal tersebut di jelaskan dalam *Article 51 (4) Additional Protocol I,* yaitu;[178]

Indiscriminate attacks are prohibited. Indiscriminate attacks are:

[175] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 29, Commentary 1
[176] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 29, Commentary 4
[177] *Ibid*
[178] Protocol Additional to The Geneva Convention of 12 August 1949, Article 51 (4)

(a) Those which are not directed at a specific military objective;

(b) Those which employ a method or means of combat which cannot be directed at a specific military objective; or

(c) Those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Dalam Artikel tersebut memuat istilah *method or means of combat* dimana dalam *Commentary Additional Protocol I* dijelaskan bahwa, *means of combat as a weapon* ini berarti bahwa, sarana bertempur yang digunakan merupakan senjata sedangkan, *methods of combat* adalah cara-cara dalam menggunakan senjata tersebut.[179] Dalam cyber warfare, dalam suatu serangan cyber yang di dalamnya terdapat virus atau worm yang di buat dari kode-kode computer yang dapat berubah menjadi tidak terkontrol karena, virus dan worm sendiri tak lebih dari sekedar buatan manusia yang rentan terhadap *human error* dan dapat menimbulkan kerugian terhadap warga sipil. Kelsey memberikan suatu contoh, pada saat terjadinya konflik di Kosovo pasukan udara NATO merancang sebuah serangan cyber terhadap system jaringan komputer pangkalan militer udara milik Serbia dengan tujuan untuk menyisipkan pesan atau perintah yang salah dan target yang salah.[180]

Kemudian NATO mengirimkan serangan tersebut melalui jaringan internet yang terdapat di Serbia, akibat dari serangan tersebut adalah terbatasnya kemampuan pasukan Serbia untuk mengarahkan serangannya kepada pesawat tempur NATO, akan tetapi di sisi lain hal tersebut juga akan mengakibatkan kerugian dan kehancuran di pihak sipil karena, serangan cyber tersebut dapat menimbulkan pesawat sipil atau pesawat swasta

[179] Schmitt, Michael.N, 2002, *Op.Cit*, hal. 389

[180] Kodar, Erki, 2012, ***Applying the Law of Armed Conflict to Cyber Attack : From the Martens Clause to Additional Protocol I***, ENDC Proceedings, Volume 15, pp. 107-132, hal. 122

menjadi target serangan karena kesalahan dalam penargetan.[181] Selain itu, missile dan rocket yang di luncurkan dengan tidak sesuai dengan targetnya dapat menghancurkan pemukiman penduduk serta fasilitas atau infrastruktur sipil.

Mengenai *indiscriminate attack* di dalam *Tallinn Manual Rule 49. Indiscriminate Attack, di jelaskan bahwa*;[182] *Cyber attacks that are not directed at a lawful target, and consequently are of a nature to strike lawful targets and civilians or civilian objects without distinction, are prohibited*. Menurut *Commentary 3* nya di jelaskan bahwa, *cyber weapon* yang memiliki kemampuan untuk dapat langsung diarahkan kepada target yang tertulis di dalam *Tallinn Manual Rule 43. Indiscriminate means or methods*[183] akan tetapi, yang menggunakan atau yang meluncurkannya gagal untuk mengarahkannya, adalah termasuk dalam kategori aturan tersebut. Contoh yang di berikan dalam *Commentary* tersebut adalah *cyber attack* dengan menggunakan *malicious script* dimana *malicious script* tersebut di lekatkan dalam sebuah gambar digital atau *digital image* kemudian, gambar tersebut di terbitkan atau di publikasikan dalam sebuah website umum.[184] Setelah itu, komputer yang mengunduh gambar tersebut akan terkena dampak dari *malicious script* tersebut.[185] Hal tersebut merupakan bentuk dari *indiscriminate attack*, karena siapa pun yang melakukan pengunduan dan kemudian membuka gambar

---

[181] Kodar, Erki, *Loc.Cit*, hal. 122

[182] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule, 49

[183] *It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be:*
a) directed at a specific military objective
b) limited in their effects as required by the law of armed conflict
and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction.

[184] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 49, Commentary 3

[185] *Ibid*

tersebut dapat terinfeksi oleh malware tersebut. *Malicious code* yang seharusnya dapat di gunakan secara *discriminate* akan tetapi digunakan secara *indiscriminate.*[186]

Dari contoh yang diberikan di dalam *Commentary* yang berada di dalam Rule 43 tersebut menjelaskan bahwa, *indiscriminate* bukan di timbulkan oleh sifat *cyber weapon* itu sendiri melainkan adanya kesengajaan atau kegagalan yang dilakukan oleh penggunanya untuk membuat *cyber weapon* menjadi *indiscriminate*. Hal tersebut berbeda dengan apa yang terdapat di dalam Rule 43 mengenai *Indiscriminate means or methods* bahwa, dalam hal ini yang *indiscriminate* adalah sifat dari *cyber weapon* itu sendiri.

e. **Prinsip Proporsionalitas**

Adapun prinsip proporsionalitas menyatakan bahwa kerusakan yang akan diderita oleh penduduk sipil atau objek-objek sipil harus proporsional sifatnya dan tidak berlebihan dalam kaitan dengan diperolehnya keuntungan militer yang nyata dan langsung yang dapat diperkirakan akibat dilakukannya serangan terhadap sasaran militer. Seperti yang dijelaskan dalam *Article 51(5) b Additional Protocol I,* yaitu;[187] *An attack when maybe expected to cause incidental loss of civilian life, injury to civilian, damage to civilian object, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.* Contoh yang familiar yang berkaitan dengan proporsionalitas adalah serangan bom atom sekutu di Hiroshima dimana, hilangnya nyawa penduduk sipil dengan keuntungan militer yang diperoleh tidak sebanding. Dalam konteks *cyber warfare*, serangan cyber yang ditujukan pada jaringan telepon di suatu Negara dengan tujuan untuk melumpuhkan jaringan telekomunikasi

[186] *Ibid*
[187] Protocol Additional to The Geneva Convention of 12 August 1949, Article 51(5) b

militer akan tetapi, pada akhirnya berimbas kepada jaringan telekomunikasi penduduk sipil yang berada di Negara tersebut.

Prinsip proporsionalitas yang berada di dalam konteks cyber warfare sebagai mana dijelaskan di dalam *Tallinn Manual Rule. 51 Proportionality*, yaitu;[188] *A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilian, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited*. Aturan tersebut menyatakan bahwa, adanya luka, kehancuran, dan hilangnya nyawa penduduk yang timbul secara incidental adalah dilarang, hal tersebut merupakan *collateral damage*. *Collateral damage* terdiri dari efek yang bersifat langsung (*direct effect*) dan yang tidak langsung (*indirect effect*), *direct effect* bersifat segera, tidak berubah dengan adanya tekanan baik secara kejadian maupun mekanisme.[189] Sedangkan, mengenai *indirect effect* terdapat penundaan atau perubahan, menurut Commentary, *collateral damage* harus dapat diperkirakan sebelumnya oleh pihak yang terkait, dengan melihat *planning*, *approving*, dan *executing* dalam melakukan serangan cyber.[190] Contohnya seperti, serangan cyber terhadap *Global Positioning Satellite*, akan berdampak pada sistem sarana transportasi atau layanan transportasi yang mengandalkan *Global Positioning Satellite* tersebut yang dapat menimbulkan kecelakaan.[191]

Selain *planning*, *approving*, dan *executing*, tiga hal pokok mengenai mekanisme yang harus diperhatikan mengenai prinsip proporsionalitas yang ada di dalam *cyber warfare*, yaitu;

---

[188] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 51
[189] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 51, Commentary 6
[190] *Ibid*
[191] *Ibid*

a) *Vulnerabilities* (kerentanan), merupakan bagian dari sistem komputer yang dapat digunakan oleh penyerang untuk melakukan *compromise* terhadap satu atau lebih atribut, dengan kata lain hal tersebut merupakan titik lemah dalam suatu komputer atau jaringan komputer.[192] Kelemahan tersebut dapat secara tidak sengaja muncul dari adanya pengenalan desain-desain sistem komputer atau adanya kesalahan yang terjadi dalam implementasinya, selain itu, kelemahan juga dapat muncul karena adanya kesengajaan.[193] Pada umumnya kerentanan di publikasikan setelah adanya *patch*[194] yang telah disebarluaskan dan diinstal. Selain itu, penyerang juga dapat menggunakan cacatnya sebuah program atau sistem operasi sebagai sebuah rahasia yang berharga atau yang biasa disebut sebagai *zero day exploit. Vulnerabilities* dapat timbul melalui berbagai komponen yang terdapat di dalam komputer atau jaringan komputer, yaitu;[195]

1. *Software*, aplikasi atau sistem perangkat lunak yang secara sengaja atau tidak sengaja telah memperkenalkan atau menunjukkan kelemahan atau kerentanannya, dimana kelemahan atau kerentanan tersebut dapat mengagalkan fungsinya sebagai mana tujuan dari dibuatnya software tersebut.
2. *Hardware* (perangkat keras), *microprocessors*, *microcontroller*, *motherboard* atau *circuit board*, *power supplies*, *printer* atau

[192] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., 2009, ***Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities***, National Research Council of The National Academy, Washington D.C, hal.83

[193] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., *Loc. Cit*, hal. 83

[194] *Patch* merupakan bagian kecil dari software yang digunakan untuk memperbaiki kesalahan atau celah yang terdapat di dalam suatu program software ataupun sistem operasi komputer

[195] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., *Op.Cit*, hal. 85

scanner, *storages device* seperti *flashdisk*, dan *modem*. Perusakkan terhadap perangkat tersebut dapat menimbulkan perubahan terhadap fungsinya.

3. *Seams between hardware and software,* contohnya seperti adanya read-only memory dalam sebuah komputer yang mungkin dapat bersifat *reprogrammable,* yang dapat secara diam-diam mengalami pemrograman ulang.
4. *Communications channels,* saluran komunikasi yang terhubung dengan dunia luar dapat dimanfaatkan oleh penyerang dengan berbagai cara seperti, berpura-pura menjadi authorized user atau user yang berwenang dan secara mudah dapat mengetahui informasi yang berada di dalam komputer atau jaringan komputer.
5. *Configuration,* sebagian besar sistem komputer menyedikan beragam konfigurasi yang dapat digunakan oleh pengguna, berdasarkan keamanan dan kenyamanan yang sesuai menurut pengguna. Namun, banyaknya pengguna yang lebih memilih kenyamanan dari keamanan terkadang membuat komputer tersebut tidak aman atau rentan.
6. *Users and operators,* user yang berwenang atau operator dari sebuah sistem atau jaringan terkadang dapat ditipu atau diperas untuk melakukan sesuatu.
7. *Services provider,* banyak instalasi komputer yang mengandalkan pihak luar dalam menyediakan layanan internet atau pemeliharaan

server. Seorang penyerang dapat membujuk atau meyakinkan sebuah *service provider* untuk melakukan suatu tindakan khusus atas nama perusahaannya, untuk menginstal suatu software yang dapat dimanfaatkan oleh penyerang.

b) *Access*, untuk mengambil keuntungan dari kerentanan yang ada di dalam suatu komputer atau jaringan komputer diperlukan akses, dalam hal ini keuntungan terkait dengan *cyber attack.* Suatu target yang memiliki persiapan relatif sedikit aksesnya dapat lebih mudah, sebaliknya target yang memiliki persiapan lebih lengkap akan sulit untuk memperoleh aksesnya, contohnya, *on-board avionics* dari sebuah pesawat tempur yang tidak terhubung ke internet, dengan kata lain untuk melakukan serangan cyber terhadap avionic tersebut membutuhkan beberapa akses terdekat yang dapat memperkenalkan atau menunjukkan suatu kerentanan yang dapat dimanfaatkan. Selain itu, jalur akses yang diperoleh juga dapat bersifat sementara, contohnya missile antiradiasi yang sering menimbulkan emisi pada sistem radar milik musuh bahkan dapat mematikannya, missile tersebut diarahkan sesuai dengan posisi terakhir dari radar tersebut. Terdapat dua cara untuk memperoleh jalur akses khusunya yang berkaitan dengan serangan cyber yaitu;

1. *Remote-access cyber attack,* yaitu metode serangan yang di lancarkan dari jarak tertentu, serangan di luncurkan melalui jaringan internet yang di manfaatkan sebagai jalur akses.
2. *Close access cyber attack,* yaitu serangan dengan memanfaatkan instalasi lokal seperti *hardware* dan *software* secara fungsional,

metode serangan ini dalam memperoleh jalur aksesnya harus berhubungan atau memanfaatkan pihak ketiga (seperti, pembuat software, dan produsen hardware)

c) *Payload*, adalah istilah yang digunakan terhadap tindakan-tindakan yang dilakukan setelah kerentanan atau *vulnerabilities* dapat dieksploitasi seperti, pemrograman virus yang telah dimasukkan ke dalam komputer untuk melakukan berbagai hal sperti, merubah file dan merusak file.

Dengan melihat *vulnerabilities, access, dan payload* ketika hal tersebut dengan mudah dapat diraih oleh salah satu pihak maka, setidaknya tindakan-tindakan yang di nilai dapat memberikan dampak yang berlebihan seharusnya di hindari. Namun, kembali pada *Article 51(5) b Additional Protocol I* bahwa, kata *excessive* atau berlebihan tidak secara eksplisit di jelaskan di dalam hukum internasional, di dalam *Air and Missile Warfare Manual* di jelaskan bahwa, *excessive* bukan mengenai penghitungan dan pembandingan korban sipil dengan pihak kombatan musuh.[196]

Selain memperkirakan atau memprediksi mekanismenya (*vulnerabilities, access, dan payload)*, efek dan kerusakan yang di timbulkan juga harus dapat diprediksi. Memprediksi efek dari senjata yang dipakai dengan target sasaran yang akan diserang merupakan hal yang dapat di terapkan untuk menegakkan prinsip proporsionalitas, dalam konteks persenjataan khususnya senjata jarak jauh yang bersifat meledakkan, senjata yang berjenis fusing, dan senjata yang memiliki kemungkinan meleset atau keluar dari jangkauan target sasaran dengan rata-rata 50 persen, harus di sesuaikan dengan target

[196] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 51, Commentary 7

sasaran baik berdasarkan karakteristiknya (ketebalan atau kekerasannya, ukuran, dan bentuk) maupun berdasarkan lingkungan sekitar (medan dan cuaca).[197]

Dalam konteks *cyber warfare*, penyerang sering tidak memiliki informasi serta detail dari target sasaran. Selain itu, adanya efek yang bersifat *cascading* atau mengalir lebih jauh dari yang diharapkan. Contohnya seperti, ketika sistem komputer saling terhubung, misalnya, kerusakan pada suatu komputer milik *NATO Defense College* di Italia dapat merambat sampai *U.S Air Force Rome Labolatory* di New York.[198] Adanya ketentuan prediksi dari serangan cyber yang akan di luncurkan dan adanya efek-efek *collateral*, *wide spread*, dan *cascading* maka, harus di bahas pula mengenai antisipasi atau *precaution* dan *neutrallity* untuk melengkapi prinsip proporsionalitas.

a. Precaution

Dalam hukum humaniter internasional, para pihak yang terlibat konflik bersenjata memiliki kewajiban untuk melakukan antisipasi dan perlindungan terhadap pihak-pihak yang tidak terlibat dalam tindak permusuhan, baik berdasarkan serangan maupun efek yang ditimbulkan, adapun hal tersebut disebut sebagai *precaution* seperti yang tercantum di dalam *Article 57 (1) Additional Protocol I*, yakni;[199]*In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.* Ketika pihak militer atau pimpinan militer memutuskan untuk mendirikan sebuah tempat untuk memasok pasukan atau *military supply depot* di pelabuhan sipil maka, sesuai dengan *Article 52 Additional Protocol I* pelabuhan tersebut dapat menjadi sasaran militer, jika

[197] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., *Op.Cit*, hal. 121
[198] *Ibid*, hal.122
[199] Protocol Additional to The Geneva Convention of 12 August 1949, Article 58 (a)

musuh memutuskan untuk menyerang maka, prinsip proporsionalitas harus ditegakkan karena, adanya potensi hilangnya nyawa penduduk sipil dan luka-luka.

Penerapan antisipasi terhadap serangan tersebut sebagaimana yang tercantum di dalam *Article 58 (a) Additional Protocol I*, bahwa; *Without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives.* Menurut Artikel tersebut pihak militer berkewajiban untuk berusaha memindahkan warga sipil dan membatalkan semua pelayaran sipil di pelabuhan tersebut untuk meminimalisir dampak dari serangan musuh. Jika letak pelabuhan tersebut berada di tengah-tengah daerah yang padat penduduk, maka pihak militer harus dapat menempatkan posisinya dengan layak yang jauh dari penduduk sesuai dengan *Article 58 (b) Additional Protocol I* ;[200] *Avoid locating military objectives within or near densely populated areas.*

Jika penjelasan tersebut di aplikasikan di dalam konteks *cyber warfare* akan sulit untuk di wujudkan karena, adanya sistem komputer atau jaringan komputer yang saling terkait antara pemerintah dan sipil. Bila dilakukan pemisahan berdasarkan *Article 58 (b) Additional Protocol I* maka, pemerintah dan pihak militer harus dapat membuat dan menetapkan jalur komunikasinya sendiri, kemudian pemerintah maupun pihak militer harus membuat *software* dan *hardware* sendiri.[201]

[200] Protocol Additional to The Geneva Convention of 12 August 1949, Article 58 (b)
[201] Jensen, Eric. T, 2010, ***Cyber Warfare Against the Precaution of the Effects of Attacks***, Texas Law

Selanjutnya mengenai *precaution* di jelaskan pula mengenai tindakan lain (selain pemisahan) yang di anggap perlu oleh pemerintah maupun militer untuk melakukan antisipasi, berdasarkan *Article 58 (c) Additional Protocol I*; *Take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.* Menurut Artikel tersebut berdasarkan contoh yang telah di berikan, ketika terdapat obyek sipil atau pihak sipil yang berada di pelabuhan tersebut telah berada di bawah kontrol dari pihak militer maka, pihak militer wajib untuk mengambil tidakkan antisipasi yang perlu untuk melindungi obyek sipil tersebut dari operasi militer.

Dalam konteks *cyber warfare*, adanya jaringan komputer dan sistem komputer yang saling terhubung antara militer dengan sipil, jika di dasarkan pada *Article 58 (c)* maka pihak militer memiliki kewajiban untuk melakukan perlindungan terhadap komputer sipil, karena secara tidak langsung pihak militer melakukan kontrol terhadap jaringan dalam melakukan pertahanan maupun penyerangan dalam *cyber warfare.*

Selain di dalam *Additional Protocol I, precaution* di jelaskan pula di dalam *Tallinn Manual International Law Applicable to Cyber Warfare,* yang pertama yaitu mengenai *costant care* yang diatur di dalam Rule 52, yang menjelaskan bahwa;[202] *During hostilities involving cyber operation, constant care shall be taken to spare the civilian population, individual civilian, and*

Review Vol:88, hal. 1553

[202] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 52

civilian objects. Di dalam *Commentary* dari Rule tersebut dijelaskan bahwa, *constant care* merupakan kewajiban dalam hal kepedulian yang melibatkan semua pihak dalam suatu operasi militer, kepedulian tersebut di maksudkan untuk peka terhadap penduduk sipil dan obyek sipil untuk menghindari adanya efek yang tidak perlu.[203]

Selanjutnya dalam *Tallinn Manual International Law Applicable to Cyber Warfare* berkaitan dengan *precaution*, menghendaki adanya verifikasi terhadap target sasaran dalam *cyber warfare*, seperti yang tercantum di dalam *Rule 53 Verification of Targets;*[204] *Those who plan or decide upon a cyber attack shall do everything feasible to verify that the objectives to be attacked are neither civilian nor civilian objects and are not subject to special protection.* Dalam Rule tersebut mengutamakan fokus terhadap perencanaan dan pengambilan keputusan, dengan memandang bahwa, pihak yang melancarkan *cyber attack* terkadang juga dapat menjadi pihak yang mensahkan atau menyetujui adanya serangan terhadap suatu obyek, karena penyerang terkadang juga mempunyai kapabilitas untuk mengetahui sifat atau jenis dari target dan sekaligus juga dapat membatalkan serangan tersebut.[205] Contohnya, seorang yang memegang komando yang memiliki kemampuan dalam hal *cyber attack* serta memiliki informasi mengenai target. Selain itu, individu yang melancarkan *cyber attack* terkadang juga tidak mengetahui informasi mengenai target tersebut karena ia hanya menjalankan perintah, dalam hal ini seharusnya dilakukan pembatasan yang layak.

[203] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 52, Commentary 4
[204] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 53
[205] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 53, Commentary 3

Kemudian mengenai efek dari adanya serangan cyber dalam cyber warfare yang harus dapat di antisipasi sesuai dengan Rule 59 mengenai *Precautions Against The Effects of Cyber Attacks,* yaitu;[206]

> *The Parties to an armed conflict shall, to the maximum extent feasible, take necessary precautions to protect the civilian population, individual civilian, and civilian objects under their control against the dangers resulting from cyber attack.*

Dapat dikatakan bahwa, Rule tersebut merupakan kelanjutan dari *Article 58 (c) Additional Protocol I* atau pengembangannya dalam konteks *cyber warfare* namun, dalam Rule tersebut diatas menghendaki adanya passive *precaution* atau antisipasi yang bersifat pasif seperti, pemisahan infrastruktur cyber milik militer dengan sipil, pemisahan suatu sistem komputer dari infrastruktur penting warga sipil khususnya yang bergantung pada internet, melakukan back up terhadap data-data sipil yang penting, dan penggunaan anti-virus.[207]

Adanya kewajiban bagi para pihak untuk melakukan antisipasi secara pasif merupakan perwujudan dari adanya *the maximum extent feasible* dalam *Rule 59,* dimana *maximum extent* merupakan syarat penting yang diperlukan dalam melakukan tindakan namun, tidak dapat diartikan sebagai adanya kewajiban untuk melakukan sesuatu yang secara teori dapat dilakukan tapi secara praktik tidak dapat diterapkan.[208] Sedangkan mengenai *feasible* atau kelayakan, adanya pemisahan obyek militer dengan sipil juga dapat di katakan

[206] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 59
[207] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 59, Commentary 3
[208] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 59, Commentary 6

tidak layak atau tidak sesuai misalnya seperti, pembangkit tenaga listrik atau *air traffic control* yang di sediakan baik untuk militer maupun sipil.[209]

b. Neutrality

Prinsip netralitas mengenai Negara yang menyatakan atau memposisikan dirinya sebagai Negara yang netral dalam sebuah konflik bersenjata.[210] Posisi dari Negara netral adalah *inviolable* atau tidak dapat diganggu gugat sebagaimana tercantum di dalam *Article 1 Hague Convention V*, yaitu; *The territory of neutral Powers is inviolable*.[211] Prinsip neutrality juga mengatur mengenai pengecualian dalam hal telekomunikasi seperti yang tercantum di dalam *Article 8 Hague Convention V,* yaitu;[212] *A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.* Mengenai Artikel tersebut diatas *United Nation* menyatakan bahwa, satellite dan juga *ground based facility* juga termasuk dalam Artikel tersebut.[213] Namun, di dalam *Hague Convention V* tidak menyatakan pembatasan mengenai sistem digital yang dapat menghasilkan informasi, seperti citra satellite, satellite cuaca, dan satellite sistem navigasi.[214]

---

[209] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 59, Commentary 7

[210] Kelsey, Jeffrey.T.G, 2008, ***Hacking Into International Humanitarian Law: The Principles of Distinction And Neutrality In The Age of Cyber Warfare***, Michigan Law Review Vol. 106, Hal. 1441

[211] Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907. Article 1

[212] Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907. Article 8

[213] Kelsey, Jeffrey.T.G, 2008, *Op.Cit*, hal.1442

[214] Kelsey, Jeffrey.T.G, 2008, *Loc.Cit*, hal.1442

Dalam *cyber warfare*, adanya serangan cyber yang memanfaatkan jaringan internet internasional yang kemudian berimbas kepada Negara netral dapat dikatakan bertentangan dengan prinsip netralitas. Berdasarkan *Article 2 Hague Convention V*, bahwa; *Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.* Berkaitan dengan status dari *cyber weapon*, adanya penggunaan virus, malware, maupun DDoS yang di salurkan melewati Negara netral dapat di katakan melanggar prinsip ini.

Prinsip netralitas di dalam *Tallinn Manual* menjelaskan bahwa, *neutral state* atau Negara netral adalah Negara yang tidak ikut serta dalam konflik bersenjata, di mana di dalam Negara netral tersebut, terdapat *neutral cyber infrastruktur* atau infrastruktur yang terkomputerisasi yang bersifat netral baik yang bersifat publik maupun privat.[215] Selain itu, para ahli juga menyadari bahwa, prinsip netralitas berkaitan dengan masuk atau keluar dari territorial Negara netral, faktanya bahwa di dalam konteks *cyberspace* yang meliputi seluruh dunia telah menimbulkan berbagai pendapat seperti, sebuah email yang dikirim dari Negara yang terlibat konflik dapat secara otomatis di salurkan melalui *netral cyber infrastructure* sebelum mencapai lokasi yang dituju.[216]

Dalam *Tallinn Manual Rule 91 Protection of Neutral Cyber Infrastructure,* tercantum bahwa; *The exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited.* Istilah

[215] Tallinn Manual On The International Law Applicable to Cyber Warfare, Chapter VII: Neutrality: 2
[216] Tallinn Manual On The International Law Applicable to Cyber Warfare, Chapter VII: Neutrality: 4

exercise of belligerent rights merupakan sinonim dari *hostile act* dalam *Hague Convention V* dan *act of hostility* di dalam *Hague Convention XIII* , menurut para ahli *exercise of belligerent rights* dapat di pahami sebagai tindakan yang dilakukan oleh pihak-pihak yang terlibat konflik dimana tindakan tersebut berhubungan dengan konflik yang terjadi termasuk operasi cyber.[217]

Dalam konteks *cyber warfare*, suatu serangan cyber yang di tujukan kepada server yang berada di dalam territori *belligerent* dapat secara signifikan berdampak pada territory Negara netral. Namun para ahli menyatakan bahwa, jika efek dari serangan cyber tersebut terhadap Negara netral tidak dapat di duga maka serangan tersebut tidak dapat dikategorikan melanggar prisip netralitas berdasarkan Tallinn Manual ini.[218] Menurut *Commentary*-nya di jelaskan bahwa, dalam menerapkan Rule 91 tersebut harus memperhatikan keseimbangan antara *belligerent rights* dan *rights of neutrality state.*

f. ***Unnecessary Suffering***

Unnecessary suffering atau penderitaan yang tidak perlu, merupakan prinsip yang harus diterapkan dalam *cyber warfare*, sebagai bagian dari *military necessity* dan *humanity* terutama berkaitan dengan pemilihan sarana dan metode berperang atau persenjataan. Seperti yang tercantum di dalam *Article 35 (2) Additional Protocol I, yaitu*;[219] *It is prohibited to employ weapon, projectiles, and material and methods of warfare of nature to cause superfluous injury or unnecessary suffering*. Berdasarkan Artikel tersebut, akan sulit untuk menerapkan *unnecessary suffering* dalam konteks *cyber*

[217] Tallinn Manual On The International Law Applicable to Cyber Warfare, Chapter VII: Neutrality: 6
[218] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 91, Commentary 4
[219] Protocol Additional to The Geneva Convention of 12 August 1949, Article 35 (2)

warfare dalam hal *cyber weapon*, jika prinsip tersebut hanya di pandang dari segi perang konvensional dan perang konvensional. Penerapan *unnecessary suffering* di dalam perang konvensional di dasarkan adanya efek yang langsung, berkaitan dengan hal tersebut maka prinsip *unnecessary suffering* dapat di terapkan dalam serangan cyber yang memiliki efek yang langsung.

Akan tetapi adanya efek yang timbul secara tidak langsung dari adanya serangan cyber yang juga menimbulkan *unnecessary suffering*, seperti penggunaan malware yang di rancang untuk melakukan hal-hal yang secara potensial dapat melanggar prinsip *unnecessary suffering* ini. Contohnya seperti, serangan cyber yang berimbas kepada peralatan, perlengkapan, data, dan infrastruktur medis yang seharusnya digunakan untuk melakukan pengobatan dan perawatan pasien baik kombatan maupun sipil.[220] Selain itu, serangan cyber yang dapat dilakukan secara terpisah yang tidak menimbulkan kecurigaan akan tetapi efek yang timbul begitu besar juga bertentangan dengan prinsip ini.

Selanjutnya *unnecessary suffering* yang tercantum di dalam Tallinn Manual di dalam Rule 42 mengenai *superfluous injury or unnecessary suffering* menyatakan bahwa,[221] *It is prohibited to employ means or methods of cyber warfare that are of a nature to cause superfluous injury or unnecessary suffering.* Sekilas sama dengan yang tercantum di dalam *Additional Protocol I* namun, yang ada di dalam *Tallinn Manual* tersebut lebih *bersifat weapon as means or methods of cyber warfare* atau senjata sebagai sarana dan metode berperang dalam cyber. Hanya penggunaan *means or methods of cyber warfare* dalam tingkat yang normal saja yang dapat di golongkan di dalam Rule

[220] Arimatsu, Louise, 2012, ***A treaty for Governing Cyber Weapons: Potential benefits and pratical limitation, International Law Programme***, Chartam House, UK, hal 104

[221] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 42

ini.[222] Tidak di jelaskan apa yang dapat dijadikan dasar mengenai tingkat yang normal atau keadaan yang normal, bila di kaitkan dengan senjata konvensional seperti penggunaan peluru dum-dum, bisa dikatakan bahwa, keadaan normal berarti adanya penderitaan yang cukup untuk di katakan berlebihan atau tidak langsung menimbulkan hilangnya nyawa dari penggunaan senjata tersebut.

Berdasarkan pembahasan di atas dapat dikatakan bahwa, aturan maupun prinsip yang terdapat di dalam hukum humaniter internasional dapat diterapkan dalam *cyber warfare*. Hal tersebut di dasarkan pada, dalam hukum internasional khususnya hukum humaniter, domain atau wilayah bukan di dasarkan secara physical maupun non-physical akan tetapi berdasarkan kedaulatan dan territorial, adanya kedaulatan di dalam *cyberspace* serta infrastruktur cyber di dalam territorial suatu Negara yang di tandai dengan adanya *IP address* serta, pengelolaan dan pengaturan suatu Negara terhadap lingkup *cyberspace*, mendukung cyberspace sebagai domain konflik bersenjata.

Selain itu mengenai adanya *cyber weapon* yang dapat mengakibatkan kerugian-kerugian seperti hilangnya nyawa penduduk atau mereka yang tidak terlibat di dalam pertempuran karena, digunakan untuk menyerang infrastruktur penting yang terkomputerisasi atau biasa disebut *critical infrastructure* seperti rumah sakit, bendungan, atau instalasi nuklir. Hal tersebut sama halnya dengan serangan bom terhadap bendungan maupun rumah sakit.

[222] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 42, Commentary 5

B. Penerapan hukum humaniter internasional terhadap kasus *cyber warfare* yang terjadi di Georgia

a. Kronologis kasus *cyber warfare* antara Rusia dengan Georgia

Di awali dengan adanya serangan pasukan Georgia ke wilayah Ossetia Utara pada 7 Agustus 2008 kemudian pada 8 Agustus 2008, Rusia memutuskan untuk menginvasi wilayah Georgia. Sebelum hari dimana Rusia melakukan invasi terhadap Georgia, pihak Rusia telah meluncurkan serangan cyber yang ditujukan ke berbagai website milik Georgia terutama website-website pemerintahan. Dalam cyber warfare yang di lancarkan oleh Rusia, terdapat dua aktor atau kelompok yang melakukan serangan terhadap infrastruktur cyber milik Georgia yaitu, StopGeorgia.ru dan *Russian Bussiness Network* (RBN). StopGeorgia.ru merupakan sebuah forum internet dengan alamat website www.StopGeorgia.ru, mula-mula hanya terdiri dari 30 member atau anggota kemudian menjadi 200 member pada 15 September 2008.[223] Mereka terdiri dari hacker-hacker yang berpengalaman selain itu, mereka juga mempublikasikan 37 target di Negara Georgia yang terkomputerisasi yang di nilai berharga, dan setiap target tersebut telah di evaluasi dan di tentukan apakah target tersebut dapat diakses melalui Rusia atau *IP address* Lithuania. Forum StopGeorgia.ru menyediakan alat-alat atau software untuk melakukan DDoS yang dapat di download oleh para member.[224]

Dalam forum StopGeorgia.ru terdapat pembagian tugas yang di kelola oleh para pemimpin forum atau administrator, seperti penyedia alat-alat atau software, sebagai pemberi petunjuk mengenai kerentanan (*vulnerabilities*) suatu aplikasi stau software, dan yang memberikan daftar sasaran yang umum yang memiliki level rendah untuk para

[223] Carr, Jeffrey, 2010, ***Inside Cyber Warfare***, O'Reilly, hal. 15
[224] Carr, Jeffrey, *Loc.Cit*, hal. 15

anggota yang belum memiliki keahlian yang cukup atau *newcomers*.[225] Menurut berbagai praktik, mereka yang mendapat bagian sebagai penunjuk atau sebagai pemberi penjelasan mengenai kerentanan yang dianggap mempunyai kemampuan yang tinggi.

Kemudian Pravada.ru mempublikasikan sebuah artikel yang ditulis oleh Maksim Zharov dari *the Foundation For Effective Politics* yang di beri judul *"Russia versus Georgia: War on the Net – Day one"*. [226] Kemudian Zharov juga menuliskan kalimat yang berisi ajakan yang berbunyi "*who want to fight the enemies of Russia"*.[227] *The Foundation For Effective Politics* merupakan organisasi pemerintah yang di bentuk oleh Gleb Palovsky yaitu, orang pertama yang mengadopsi mengenai kegunaan internet di Rusia untuk tujuan propaganda.[228]

Adanya penggalangan milisi cyber oleh pemerintahan Rusia khususnya oleh seorang Maksim Zharov tidak sampai disitu, Zharov juga membuat komentar mengenai penggunaan gerakan pemuda Rusia untuk melaksanakan perang dari internet yang kemudian komentar tersebut di muat di dalam forum StopGeorgia.ru, yang berbunyi;[229] *Let me remind you that on August 8, Leaders of several Russian youth movement have signed the statement which calls for supporters to wage information war against the President of Georgia Michael Saakashvili on all internet resource*. Selain keterangan tersebut, banyak lagi yang dapat di jadikan bukti bahwa pernyataan dan ajakan yang dilakukan oleh Zharov dapat di jadikan suatu pedoman mengenai adanya pengorganisiran gerakan cyber untuk melakukan serangan cyber.

---

[225] Carr, Jeffrey, *Op.Cit*, hal.16
[226] *Ibid*, hal. 17
[227] Carr, Jeffrey, *Loc.Cit*, hal. 17
[228] Carr, Jeffrey, *Loc.Cit*, hal. 17
[229] *Ibid*, hal. 18

Selain StopGeorgia.ru ada kelompok terorganisir lainnya yang disebut sebagai *Russian Business Network* atau RBN, menurut *Georgian National Security Chief*, Eka Tkeshelashvili menyatakan bahwa;[230]

> *At the top of the hierarchy are the Soldiers the professional planners, computer scientist, engineers, and other implementers, including the military itself. Next, are what some call the mercenaries, these are criminal organizations paid to carry out certain elements of the attacks. In this case, they are strong signs implicating an outfit known as the Russian Business Network (RBN). And, finally, there are the volunteers, there are individuals with PC who are recruited to carry out attacks they are provided with access to all necessary software tools, as well as to detailed instructions for carrying out the attacks.*

Berdasarkan keterangan tersebut disebutkan bahwa, RBN adalah *mercenaries* atau organisasi yang bergerak karena di bayar untuk melakukan sesuatu. Di dalam berbagai sumber tidak di jelaskan secara rinci mengenai keterlibatan dari RBN dalam serangan cyber terhadap Georgia namun, di jelaskan mereka telah melakukan *cyber blockade* dengan mengarahkan semua lalu lintas internet Georgia menuju Rusia.

Serangan cyber yang pertama dilancarkan, ditujukan untuk melumpuhkan website Presiden Georgia (www.president.gov.ge) dengan menggunakan *distributed denial of service* (DDoS), sedikitnya satu perintah atau instruksi berbasis web and kontrol server atau (C&C) di arahkan ke website tersebut.[231] Berdasarkan data yang diperoleh, berbagai variasi serangan seperti, penggunaan botnet terhadap TCP, ICMP, dan HTTP dilakukan untuk menjatuhkan atau melumpuhkan website tersebut. *Shadowserver Foundation* sebagai grup yang melakukan penelitian terhadap serangan tersebut

---

[230] Watts, Sean, 2010, ***Combatant Status and Computer Network Attack***, Virginia Journal of interntional Law Vol 50:2, hal. 41

[231] Tikk, Eneken, *Op.Cit*, hal. 36

menyatakan bahwa, botnet yang digunakan dalam serangan terhadap website kepresidenan Georgia tersebut adalah MachBot dimana Bot tersebut sering digunakan oleh pihak-pihak Rusia.[232]

Kemudian setelah berhasil melumpuhkan website kepresidenan Georgia, serangan DDoS di arahkan kepada beberapa website pemerintahan milik Georgia lainnya seperti website Kementrian luar negeri Georgia, yang kemudian terpaksa harus memindahkannya ke dalam bentuk akun Blogspot.[233] Dalam sebuah statement yang dikeluarkan melalui website pengganti yang di buat dalam blog-hosting service milik Google pada tanggal 11 Agustus 2008, Menteri Luar Negeri Georgia menyatakan bahwa, *cyber warfare* yang dilancarkan oleh Rusia telah secara serius mengganggu website-website milik Georgia, termasuk Kementerian Luar Negeri.[234]

Pada tanggal 9 Agustus 2008, TBC yang merupakan bank komersial terbesar di Georgia di beritakan juga telah di serang.[235] Berdasarkan pengamatan dan penelitian yang dilakukan oleh Dancho Danchev[236] dari ZDnet menyatakan bahwa, terdapat pola atau bentuk dari serangan tersebut yaitu, yang pertama adanya pembagian target serangan untuk menghindari adanya serangan yang terpusat di mana pembagian tersebut di lakukan dengan mempublikasikan daftar target di website forum milik pihak Rusia yaitu, StopGeorgia.ru.[237] Kemudian tersedianya peralatan DDoS atau software untuk di download serta, instruksi atau tutorial seperti bagaimana melakukan ping flood terhadap

---

[232] Tikk, Eneken, *Loc.Cit*, hal. 36
[233] *Ibid*, hal. 37
[234] Tikk, Eneken, *Loc.Cit*, hal. 37
[235] *Ibid*, hal. 38
[236] Dancho Danchev adalah seorang konsultan keamanan independen dan analis gangguan cyber, dengan pengalaman yang luas di bidang intelligence gathering, malware, dan E-crime, serta sebagai security blogger sejak tahun 2007.
[237] Tikk, Eneken, *Loc.Cit*, hal. 38

website pemerintah Georgia dan juga melakukan DDoS terhadap website tersebut.[238] Selanjutnya yang ketiga, adanya publikasi mengenai website Georgia yang memiliki kerentanan terhadap serangan defacement, yang keempat yaitu, adanya penyalahgunaan alamat e-mail milik politisi Georgia untuk melakukan spamming dan di jadikan target serangan, dan yang terakhir adalah penyerangan terhadap forum komunikasi komunitas Informasi dan Teknologi.[239]

Kemudian pada tanggal 10 Agustus 2008, *Shadowserver* melaporkan adanya serangan baru, namun target dari serangan ini tidak hanya website pemerintahan tetapi juga website-website publik atau umum seperti, apsny.ge, news.ge, tbilisiweb.info, newsgeorgia.ru, os-inform.com, kasparov.ru, hacking.ge, mk.ru, newstula.info, dan skandaly.ru.[240] Tanggal 11 Agustus 2008, Civil.ge menjadi target serangan cyber berikutnya dengan metode serangan DDoS. Pada tanggal 13 Agustus 2008, *Shadowserver* melaporkan adanya serangan dengan skala yang besar berdasarkan lalu lintas ICMP yang besar, serangan tersebut secara langsung mengarah kepada website pemerintahan Georgia dan serangan tersebut berasal dari berbagai komputer milik pihak Rusia dan berasal dari beberapa *Internet Service Provider* yang berbeda di Rusia.[241]

Blog-blog, forum, dan website-website Rusia juga melakukan penyebaran *Microsoft Windows* batch script yang telah di desain untuk menyerang website Georgia.[242] Serangan cyber yang dilakukan oleh Rusia berhenti setelah para penyerang tersebut berhasil dihentikan pada tanggal 28 Agustus 2008.[243]

---

[238] Tikk, Eneken, *Loc.Cit*, hal. 38
[239] *Ibid*, hal. 39
[240] Tikk, Eneken, *Loc.Cit*, hal. 39
[241] *Ibid*, hal. 40
[242] Tikk, Eneken, *Loc.Cit*, hal. 40
[243] *Ibid*, hal. 41

b. Analisis terhadap *cyber warfare* yang dilakukan oleh Rusia terhadap Georgia berdasarkan Hukum Humaniter Internasional

1. Serangan cyber yang terjadi sebagai suatu peperangan atau konflik

Serangan cyber yang dilancarkan oleh Rusia terhadap Georgia, merupakan *cyber warfare* karena, serangan cyber yang dilakukan telah di kondisikan atau di barengi dengan adanya invasi yang dilakukan oleh Rusia ke wilayah Georgia, berdasarkan Article 2 (4) UN Charter bahwa, Rusia telah melakukan *use of force*. Dalam hal ini tidak memerlukan adanya keabsahan mengenai tindakan permusuhan *(mutual hostilities)* atau serangan cyber yang dapat membentuk suatu konflik atau *act of war (cyber act of war)*

2. Kombatan (*distinction principle*)

Dalam hukum humaniter internasional konflik bersenjata selalu melahirkan dua kubu yakni, kombatan dan non-kombatan (termasuk sipil), dalam hal ini berkaitan dengan *distinction principle* atau prisip pembedaan. Di jelaskan di dalam *Article 4 A Geneva Convention* III bahwa, mereka yang merupakan kombatan atau mereka yang dapat berpartisipasi dalam konflik bersenjata adalah mereka yang dipimpin orang seorang komando, menggunakan emblem atau lambang yang membedakan, membawa senjata secara terang-terangan dan mematuhi hukum perang. Dalam hal forum StopGeorgia.ru, penerapan syarat pertama mengenai adanya pemimpin atau pemegang komando dapat dilihat dari pernyataan-pernyataan yang di berikan oleh Maksim Zharov, dimana dia yang melakukan penggalangan atau melakukan support terhadap serangan serangan cyber.

Tidak ada klasifikasi yang pasti mengenai *commanders* dalam suatu konflik bersenjata namun, bila dilihat dari kapasitas seorang Maksim Zharov dan mengenai kedudukannya di dalam pemerintahan Rusia dapat dikatakan bahwa dia adalah seorang *commander*. Sedangkan administrator atau pengelola forum tersebut dapat dikatakan sebagai penerima mandate, terlepas dari *commander* sebagai pemegang pangkat tertinggi di dalam suatu organisasi militer, banyak keputusan-keputusan militer di buat berdasarkan keputusan dari pimpinan lembaga yang lebih tinggi seperti menteri pertahanan bahkan Presiden, seperti dalam kasus *cyber attack* antara U.S.A dengan Iran di mana, President Barrack Obama yang memberikan perintah secara langsung.

Menurut *Tallinn Manual Rule 26. Commentary 9* di jelaskan bahwa, adanya commander adalah untuk membuktikan bahwa kelompok tersebut terorganisir namun, akan sulit bagi individu-individu untuk menyatakan dirinya telah terorganisir jika pengorganisasiannya melalui media internet. Akan tetapi dalam hal StopGeorgia.ru mereka secara tidak langsung terorganisir karena, adanya dorongan dari pernyataan Maksim Zharov dan kapasitasnya sebagai bagian dari pemerintahan Rusia. Selain itu, para anggota forum sebelumnya telah mengetahui tentang, mereka-mereka yang dianggap sebagai leader atau administrator dalam forum tersebut karena, apa yang mereka lakukan merupakan apa yang telah di paparkan oleh administrator.

Berdasarkan *Joint Publication* dari *Departemen of Defense* Amerika Serikat menjelaskan bahwa, adanya commander berarti terdapat *command and control*. Dimana terdapat pengaturan mengenai personil, peralatan, perlengkapan,

komunikasi, fasilitas, dan prosedure yang berdasarkan perencanaan, pengarahan, pengkoordinasian, dan kontrol dan operasi dalam mencapai tujuan misi.[244] Menurut keterangan tersebut, dapat di katakan bahwa, StopGeorgia.ru merupakan kolompok yang terorganisir berdasarkan syarat mengenai commander karena, terdapat personil (anggota forum), peralatan dan perlengkapan (software untuk melakukan DDoS), serta adanya perencanaan (pemaparan mengenai 37 target dan metode yang digunakan, yang tercantum di forum tersebut).

Mengenai syarat kedua yakni, pemakaian tanda atau emblem dalam konteks cyber warfare, ini merupakan syarat yang bersifat alternatif sesuai dengan *Article 44 (3) Additional Protocol I,*yang menyebutkan bahwa, jika kombatan tidak dapat melakukan pembedaan termasuk dengan menggunakan tanda atau emblem maka dapat dilakukan dengan membawa senjata secara terang-terangan. Sebagaimana diketahui bahwa, hal tersebut merupakan syarat ketiga. Berdasarkan syarat ketiga ini, sesuai dengan yang dibahas di dalam permasalahan pertama mengenai kualifikasi kombatan, dalam kasus ini adanya software DDoS yang termasuk *cyber weapon (means and methods)* yang di publikasikan di dalam forum, dan adanya software berarti terdapat juga penggunaan hardware, kemudian adanya kejelasan tujuan bahwa forum tersebut memang ditujukan untuk melakukan *cyber attack*. Berdasarkan hal tersebut maka, mereka yang terlibat dalam forum tersebut dianggap telah memenuhi syarat ketiga.

Selanjutnya mengenai Russian Business Network atau RBN, di mana telah disebutkan oleh *Georgian National Security Chief* bahwa mereka adalah *mercenaries* atau tentara bayaran. Di dalam *Article 47 (2) Additional Protocol I* di

[244] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., *Op.Cit*, hal. 129

jelaskan bahwa, *mercenaries* adalah mereka yang direkrut baik dari dalam negeri maupun luar negeri untuk berperang, dan mereka bergerak berdasarkan imbalan yang mereka terima. Ketidak jelasan terhadap sumber-sumber yang telah di baca oleh penulis membuat kedudukan RBN sebagai mercenaries tidak jelas. Namun, dapat dinilai bahwa mereka memperoleh imbalan berupa jaminan dari pemerintah Rusia agar organisasi mereka tetap terlindungi, sebagai organisasi kriminal.

Sesuai dengan apa yang telah di jelaskan di atas maka StopGeorgia.ru dapat dikatakan sebagai kombatan, dan mengenai syarat yang keempat mengenai apakah mereka mematuhi hukum perang yang berlaku, merupakan hal yang bersifat praktik dan belum dapat ditentukan apakah kelompok militer bersenjata telah melanggar hukum humaniter sebelum ada bukti yang terang, selain itu bila di tentukan mereka telah melanggar hukum perang yang berlaku, mereka akan berkedudukan tetap sebagai kelompok militer, dan sejauh ini dapat dikatakan bahwa syarat keempat merupakan syarat yang tidak begitu efektif.

3. Target serangan cyber berkaitan dengan *civilian object* maupun *military objectives*

Berbagai sumber memberikan keterangan yang berbeda mengenai serangan cyber yang dilakukan terhadap website kepresidenan Georgia yakni www.President.gov.ge namun, sebagian besar sumber menyatakan bahwa serangan tersebut dilakukan dengan menggunakan DDoS dan kemudian melakukan defacement. Jika dilakukan analisis berdasarkan obyek sipil atau obyek militer berdasarkan *Article 52(2) Additional Protocol I* maka, website kepresidenan belum tentu dapat di jadikan sasaran militer yang sah. Namun,

sebelum melakukan analisis lebih lanjut harus dilakukan penjelasan terlebih dahulu terhadap struktur dari website. Di dalam sebuah website terdapat unsur-unsur yang harus dipenuhi agar web tersebut dapat bekerja, unsur-unsur tersebut terdiri atas domain name, web hosting, desain web site, bahasa program, program transfer data atau *File Transfer Period*.

Domain name atau Domain Name System (DNS) memiliki fungsi untuk menterjemahkan IP address yaitu, nomer yang terdapat dalam setiap komputer ketika komputer tersebut sedang terhubung ke internet, nomer tersebut di terjemahkan dalam bentuk alphabet. Misalnya seperti, IP address 192.180.1.163 di terjemahkan menjadi www. ebookdownloadfree.com. Sedangkan web hosting merupakan ruang yang terdapat pada storage atau hardisk sebagai tempat penyimpanan data-data atau database yang nantinya data-data tersebut akan ditampilkan di dalam website.

Mengenai analisis lebih lanjut terhadap website presiden Georgia berdasarkan *Article 52(2) Additional Protocol I* bahwa, yang merupakan obyek militer adalah obyek yang sifat, lokasi, tujuan, dan penggunaannya dapat memberikan kontribusi yang efektif bagi aksi-aksi militer maka, berdasarkan sifat dan tujuannya website tersebut memuat mengenai informasi-informasi mengenai kegiatan kepresidenan atau pemerintahan. Dengan kata lain website tersebut belum tentu memuat informasi-informasi yang berkaitan dengan militer. Mengenai lokasinya jelas bahwa, di dalam website tersebut berdasarkan DNSnya di buat atas nama kepresidenan Georgia bukan atas nama lembaga militer.

Selanjutnya berdasarkan penggunaannya website tersebut seketika dapat menjadi sasaran militer apabila, memuat informasi-informasi yang berkaitan dengan militer meskipun di sisi lain juga memuat informasi mengenai kepresidenan atau umum. Berdasarkan teori mengenai *dual use object* yang terdapat di dalam *Rule 39 Tallinn manual* yang dijelaskan bahwa, obyek yang digunakan untuk kepentingan sipil maupun militer termasuk komputer, jaringan komputer, dan infrastruktur cyber adalah obyek militer. Jadi, sekecil apapun perbandingannya antara informasi militer yang dimuat dengan informasi umum, website tersebut adalah sasaran militer.

Namun, jika dikaitkan dengan keuntungan militer yang dapat di dapat dan di dasarkan pada strategi operasi yang popular digunakan, seperti *compellence operation* yaitu, operasi militer yang ditujukan untuk menyerang secara langsung pemimpin dari sebuah Negara dalam hal ini adalah presiden Georgia dengan menghancurkan kediamannya atau yang hal lainnya yang berupa psikologis, ideologis, atau simbolis yang penting,[245] dimana hal tersebut di nilai lebih efektif dan dapat memberikan keuntungan militer yang lebih. Selanjutnya, yang membuat website presiden tersebut sah untuk diserang adalah adanya perang konvensional yang terjadi sehingga dapat di katakan bahwa, presiden merupakan komando tertinggi.

Selain adanya serangan cyber terhadap website pemerintahan seperti website kepresidenan, serangan cyber juga ditujukan kepada website perbankkan nasional Georgia yaitu, www.nbg.gov.ge. Dalam kapasitasnya sebagai bank

[245] Anonymous, 2005, ***Report Expert Meeting: Targeting Military Objectives***, the University Centre for International Humanitarian Law Geneva, hal. 9

nasional, serangan yang dilakukan tersebut dapat dikatakan sah apabila dikaitkan dengan teori *war sustaining capability* yang tercantum di dalam *Commanders Handbook on the Law of Naval Operation* mengenai *proper economic target* atau target-target yang bersifat ekonomi yang dapat membuat perang yang dilakukan dapat terus berlanjut atau dengan kata lain terus berlanjutnya pembiayaan perang.[246]

Kemudian berkaitan dengan serangan yang ditujukan kepada website pemberitaan seperti www.civil.ge, www.presa.ge, www.apsny.ge, www.rustavi2.com, www.news.ge, dan interpress.ge, berdasarkan *Article 52(2) Additional Protocol I* hal tersebut dapat di kategorikan sebagai serangan yang tidak sah atau melanggar bila, di terangkan bahwa website-website pemberitaan tersebut merupakan bagian dari kegiatan jounalistik, dan hal tersebut seharusnya dilindungi berdasarkan *Article 79 Additional Protocol I,* yang menjelaskan bahwa; *Journalist engaged in dangerous professional missions in areas of armed conflict shall be considered as civilians within the meaning of Article 50, paragraph I.* Namun, di dalam praktiknya penyerangan terhadap kantor-kantor atau pusat pemberitaan banyak dilakukan di dalam suatu peperangan, misalnya seperti serangan NATO terhadap Radio Televisija Srbije (RTS).

Serangan tersebut dilakukan untuk menghentikan propaganda atau menghentikan dukungan-dukungan yang timbul dari penduduk dan pihak luar yang Pro, dengan adanya penyiaran pemberitaan-pemberitaan yang berkaitan dengan perang tersebut. Karena, hal tersebut dapat membuat perang menjadi semakin panjang dengan adanya dukungan dari pihak-pihak selain pihak militer

[246] *Ibid*, hal. 3

Negara. Di sisi lain, bila serangan tersebut dianggap bagian dari *military advantage* atau pun dianggap sebagai obyek yang memberikan *effective military contribution* dan kemudian melegalkannya maka hal tersebut akan merubah hukum humaniter internasional yang berlaku karena, target tersebut bukan merupakan obyek militer secara tradisional.

Selanjutnya, apabila dilakukan analisis berdasarkan *Rule 39 Talinn Manual* berdasarkan apa yang di sebut sebagai *dual use object* bahwa, jika website-website tersebut memuat pemberitaan atau menyiarkan pemberitaan yang di tujukan untuk militer maupun sipil, website tersebut dapat dianggap sebagai target militer dan sah untuk dilakukan penyerangan. Selain itu efek yang akan ditimbulkan juga dapat mempengaruhi keabsahan target sasaran khususnya dalam *cyber warfare*, seperti serangan cyber terhadap reactor nuklir yang dapat menimbulkan kebocoran atau malfungsi. Sama halnya dengan serangan yang dilakukan terhadap website tersebut.

Efek yang ditimbulkan dari adanya serangan terhadap website-website pemberitaan tersebut adalah keterbatasan informasi yang dapat diakses oleh penduduk Georgia, serta terputusnya informasi-informasi baik dari luar maupun luar negeri. Dimana hal tersebut dapat menimbulkan kekacauan atau kesalahan komunikasi dan yang terpenting adalah hal tersebut terjadi pada saat peperangan sedang berlangsung. Berdasarkan hukum humaniter hal tersebut dapat di kategorikan sebagai *collateral damage* yang tercantum di dalam *Article 51 (5) (b) Additional Protocol I* karena, adanya kerugian yang bersifat insidental yang di alami oleh penduduk sipil.

Dalam hal ini kerugian tersebut lebih bersifat mental berdasarkan kekacauan yang terjadi, namun dapat di interpretasikan bahwa, hilangnya komunikasi atau tidak adanya komunikasi antara pemerintah dengan penduduk dalam suatu peperangan tidak hanya akan menimbulkan penderitaan mental namun juga penderitaan secara fisik seperti, tidak adanya informasi-informasi mengenai wilayah-wilayah yang akan di serang atau kemungkinan akan di serang oleh musuh dapat membuat penduduk yang tidak mengetahuinya dapat terkena serangan tersebut. Selain itu, adanya efek yang timbul dari serangan cyber yang di arahkan kepada bank nasional Georgia turut mendukung penderitaan mental, karena kerugian materi yang di alami.

Menurut *Cooperative Cyber Defence Center of Exelence,* serangan DDoS yang dilakukan oleh pihak Rusia juga mengakibatkan dua perusahaan penyedia layanan internet yakni, *Caucasus Network Tbilisi* dan *United Telecom of Georgia* tidak dapat berfungsi atau tidak ada layanan. Terganggunya atau tidak berfungsinya penyedia layanan internet atau *Internet Service Provider* berarti semua komputer atau jaringan komputer yang mengandalkan koneksi internet juga terputus. Bahkan, kemungkinan juga terkena serangan botnet yang menjadikan infrastruktur penting seperti rumah sakit tidak dapat berfungsi dengan normal. Hal tersebut juga dapat bertentangan dengan prinsip *unnecessary suffering,* apabila infrastruktur medis tersebut digunakan untuk perawatan para prajurit perang karena, akan menambah penderitaan yang seharusnya tidak diperlukan.

Berdasarkan penelitian tersebut diatas, StopGeorgia.ru dapat dikatakan memenuhi syarat sebagai kombatan untuk dapat ikut serta dalam peperangan berdasarkan prinsip pembedaan *(distinction principle)*. Namun, serangan cyber yang dilakukan oleh Rusia dalam *cyber warfare* tersebut telah melanggar prinsip-prinsip pembedaan khususnya mengenai obyek sipil (bank, pemberitaan, forum umum, televisi) berdasarkan *Article 52 Additional Protocol I.* Selain itu, dampak yang diakibatkan dengan melakukan serangan terhadap *Internet Service Provider Caucasus Network Tbilisi* dan *United Telecom of Georgia* dapat melumpuhkan semua aktivitas pengguna internet dimana hal tersebut, tidak sesuai dengan prinsip proporsionalitas maupun *unnecessary suffering*.

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan pembahasan diatas dapat ditarik beberapa kesimpulan bahwa;

1. Konflik yang terjadi di dalam domain *cyberspace* atau disebut sebagai *cyber warfare*, memiliki unsur-unsur yang sama dengan konflik bersenjata konvensional, yaitu;
    1) Para pihak (*distinction principle*)
    2) Serangan yang terjadi (*act of violence*)
    3) Akibat yang ditimbulkan (*Proportionality*)

    Para pihak yang secara umum di kenal dalam suatu konflik bersenjata yaitu, kombatan maupun sipil yang berada dalam *cyber warfare* juga dapat dibedakan berdasarkan *distinction principle* yang ada pada hukum humaniter internasional di mana pengguna komputer yang melancarkan serangan cyber atau secara terorganisir melancarkan serangan cyber dapat disebut sebagai kombatan, sedangkan pengguna komputer yang tidak turut serta dalam serangan cyber dapat disebut sebagai penduduk sipil. Akibat yang terjadi dari serangan cyber juga tidak jauh berbeda dengan apa yang dapat di sebabkan oleh bom atau semacamnya seperti, mematikan sistem komputer stasiun pembangkit tenaga listrik yang dapat menyebabkan terhentinya semua pasokan listrik suatu Negara yang juga dapat menimbulkan hilangnya nyawa

meskipun tidak secara langsung. Selain itu, adanya serangan cyber yang tidak dapat membedakan atau serangan yang bertentangan dengan prinsip proporsionalitas seperti, penyertaan atau mengupload virus atau malware dalam situs atau website yang bersifat publik, dimana malware tersebut dapat menginfeksi siapa saja yang membuka website tersebut. Selanjutnya, apa yang telah tersusun dalam *Tallinn Manual* antara lain seperti,

1) *Participation in armed conflict* yang mengatur mengenai pihak-pihak dalam *cyber warfare* yaitu*;*
    1. *Member of armed forces,* yang ada dalam Rule 26
    2. *Mercenaries,* yang ada di dalam Rule 28
    3. *Civilian,* yang ada di dalam Rule 29
2) *Means and Methods of cyber warfare* atau *cyber weapon* yang mengatur mengenai sarana dan metode dalam *cyber warfare*, yaitu;
    1. *Definition of means and methods of cyber warfare,* yang ada dalam Rule 41
    2. *Superfluous injury or Unnescessary suffering,* yang ada dalam Rule 42
    3. *Indiscriminate means and methods,* yang ada dalam Rule 43
3) *Attack against object* yang mengatur mengenai;
    1. *Prohibition on attacking civilian object*, yang diatur dalam Rule 37
    2. *Civilian Object and military objectives*, yang diatur dalam Rule 38

3. *Object used for civilian and military purpose*, yang diatur dalam Rule 39

Merupakan wujud atau gambaran bahwa, hukum humaniter internasional dapat di terapkan dalam *cyber warfare*.

4. Dalam analisis mengenai kasus *cyber warfare* antara Rusia dengan Georgia, dapat dinyatakan bahwa hukum humaniter internasional yang diterapkan dalam *cyber warfare* pada rumusan masalah pertama dapat diterapkan dalam kasus tersebut. Kombatan yang menjadi pihak dalam peperangan tersebut adalah anggota forum StopGeorgia.ru yang telah mendapatkan dukungan dari seorang Maksim Zharov, yang dalam hal ini merupakan komander, karena unsur-unsurnya seperti, sebagai pihak pemerintah dan pernyataan-pernyataan yang di keluarkannya secara tidak langsung mengorganisir para pemuda Rusia untuk melakukan serangan cyber. Kemudian berdasarkan target serangan cyber yang dilakukan mereka dapat di katakan talah melanggar prinsip pembedaan mengenai penyerangan terhadap obyek-obyek selain obyek militer.

B. Saran

1. Hukum Humaniter Internasional melalui konvensi-konvensinya belum dapat dikatakan sempurna untuk diterapkan dalam kasus *cyber warfare*. Perlu adanya kerjasama dengan para ahli yang memiliki kemampuan dalam bidang teknologi dan informasi serta para ahli dalam bidang hukum humaniter untuk melakukan analisis atau pencarian fakta.

2. *Tallinn Manual* sebagai petunjuk penerapan hukum internasional dalam *cyber warfare* sebaiknya, harus segera di tingkatkan statusnya sejajar dengan konvensi melalui kesepakatan Negara-negara atau komunitas Internasional, untuk dapat di jadikan sebagai dasar hukum yang sah selain sebagai petunjuk.

DAFTAR PUSTAKA

Amirudin, Zainal Asikin, **Pengantar Metode Penelitian Hukum**, PT RajaGrafindo Persada, Jakarta, 2003

Arlina Permanasari dkk, **Pengantar Hukum Humaniter**, ICRC Jakarta, Miamata Print, Jakarta, 1999

Buffaloe, David L, ***Defining Asymmetric Warfare***, The Institute of Land Warfare, Association of The United State Army., 2006

Carr, Jeffrey, ***Inside Cyber Warfare***, O'Reilly, 2010

Carus, W., Seth, ***Defining Weapon of Mass Destruction***, National Defense University Press Washington, D.C, 2012

Even, Shmuel, and Siman-Tov, David, 2012, ***Cyber Warfare: Concepts and Strategic Trends***, Institute For National Security Studies

Johny Ibrahim, **Teori dan Metode Penelitian Hukum Normatif**, Bayumedia, Malang, 2006

Koplow, David A, ***Non Lethal Weapons; The Law And policy of Revolutionary Technologies for The Military And Law Enforcement***, George Town University Law Center., 2006

Peter Mahmud Marzuki, **Penelitian Hukum,** Kencana, Jakarta, 2005

Sefriani, **Hukum Internasional: Suatu Pengantar/Sefriani**, Rajawali Pers, Jakarta, 2011

Solis, Gary D, ***The Law of Armed Conflict***, Cambridge University Press., 2010

Williamson, Myra, ***Terrorism, War, and International Law: The Legality of the Use of Force Against Afghanistan in 2001***, The University of Waikato, New Zealand, 2009

JURNAL

Anonymous, ***A Guide to The Legal Review of New Weapon***, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol 1 of 1977,

International Committee of The Red Cross, www.icrc.org/eng/assets/files/other/irrc_ 864_icrc_ geneva.pdf, 2006

Anonymous, ***Cyber Operations***, Air Force Doctrine Document 3-12, 2010

Anonymous, ***How is the Term "Armed Conflict" Defined in International Humanitarian Law?***, International Committee of the Red Cross (ICRC) Opinion Paper, www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf, 2008

Anonymous, ***International Humanitarian Law: Answer to Your Question***, International Committee of the Red Cross, http://cdn.peaceopstraining.org/ course_promos/ international_ humanitarian_law/ international_ humanitarian_law_english.pdf, 2002

Anonymous, 2005, ***Report Expert Meeting: Targeting Military Objectives***, the University Centre for International Humanitarian Law Geneva

Arimatsu, Louise, ***A treaty for Governing Cyber Weapons: Potential benefits and pratical limitation, International Law Programme***, Chartam House, UK, 2012

Bryant, Rebecca, ***What Kind of Space is Cyberspace?***, Minerva-An Internet Journal of Philosophy, 2001

Chelimo, Getrude.C, ***Defining Armed Conflict in International Humanitarian Law***, Student Pulse:Online Academic StudentJournal, http://www.studentpulse.com/ articles/508/2/ defining-armed-conflict-in-international-humanitarian-law, 2011

Chetail, Vincent, 2003, ***The Contribution of International Court of Justice to International Humanitarian Law***, International Committee of The Red Cross

Clark, David, ***Characterizing cyberspace: past, present and future***, MIT CSAIL, 2010

Coupland, Robin M., , ***The Effect of Weapon: Defining Superflous Injury and Unnecessary Suffering***, A1 Medicine & Global Survival Vol.3, 1996

Crawford, Emily, ***The Modern Relevance of The Martens Clause***, The University of Sydney, Sydney Law School, 2011

Hayashi, Nobuo, ***Requirement of Military Necessity in International Humanitarian Law and International Criminal Law***, Boston University Internasional Law Journal, 2010

Hovel, Devika, ***Chinks in the Armour: International Law, Terrorism, and The Use of Force***, UNSW Journal, 2004

Jensen, Eric. T, ***Cyber Warfare Against the Precaution of the Effects of Attacks***, Texas

Law Review Vol:88, 2010

Kelsey, Jeffrey.T.G, ***Hacking Into International Humanitarian Law: The Principles of Distinction And Neutrality In The Age of Cyber Warfare***, Michigan Law Review Vol. 106, 2008

Kodar, Erki, ***Applying the Law of Armed Conflict to Cyber Attack : From the Martens Clause to Additional Protocol I***, ENDC Proceedings, Volume 15, pp. 107-132, 2012

Kumar, H.Shravan, ***Seminar Report on Study of Viruses and Worms***, KReSIT, I.I.T Bombay

Meron, Theodor, ***The Martens Clause, Principles of Humanity, and Dictates of Public Conscience***, The American Journal of International Law, 2000

Milanovic, Marko, ***Lesson For Human Rights and Humanitarian Law In The War on Terror: Comparing Hamdan and The Israeli Targeted Killing Case***, International Committee of The Red Cross, 2007

MP Ferreira-Snyman, ***The Evolution of State Sovereignty: A Historical Overview***, University of Leyden Netherland, 2006

Ochmannova, Petra, ***Unmanned Aerial Vehicles And Law of Armed Conflict Implications***, Czech Year Book of International Law, 2011

Owens, William A., Dam, Kenneth. W., Lin, Herbert S., , ***Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities***, National Research Council of The National Academy, Washington D.C, 2009

Prof. Schimitt, N. Michael, Prof. Garraway, Charles H.B, Prof. Dinstein, Yoram, *The* ***Manual on the Law of Non International Armed Conflict With Commentary***, International Institute of Humanitarian Law, www.iihl.org/iihl/Documents/The%2520 Manual% 2520on%2520the%2520 Law%2520of%2520NIAC.pdf

Richardson, John***, Stuxnet As Cyberwarfare: Distinction and Proportionality On The Cyber Battlefield***, National Academic of Science, 2011

Sassoli, Marco, ***Legitimate Targets of Attack Under International Humanitarian Law***, Program on Humanitarian Policy and Conflict Research at Harvard University, 2003

Schmitt, Michael.N, ***Wired Warfare: Computer Network Attack***, IRRC, June Vol.84, No. 846, 2002

----------, ***Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance***, Virginia Journal of International Law Vol. 50:4, 2010

----------, ***Umanned Combat Aircraft System And International Humanitarian Law: Simplifying The Oft Benighted Debated***, Boston University School of Law, 2012

Tikk, Eneken, ***Cyber Attacks Against Georgia: Legal Lessons Identified***, Cooperative Cyber Defense Center of Exellence, 2008

Watts, Sean, ***Combatant Status and Computer Network Attack***, Virginia Journal of interntional Law Vol 50:2, 2010

Wysopal, Chris, ***Static Detection of Application Backdoors***, Veracode.Inc., Burlington, MA USA

UNDANG-UNDANG

Convention III relative to the Treatment of Prisoners of War. Geneva, 12 August 1949

Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907

Protocol Additional to The Geneva Convention of 12 August 1949

Tallinn Manual On The International Law Applicable to Cyber Warfare, Cambridge University Press

INTERNET

Anonymous, 1999, ***Advisory CA-1999-02 Trojan Horses***, CERT: Software Engineering Institute Carnegie Mellon University, http://www.cert.org/advisories/CA-1999-02.html, (24 Maret 2013)

Anonymous, 2010, ***Customary International Humanitarian Law***, International Committee of the Red Cross, http://www.icrc.org/eng/war-and-law/treaties-customary-law/customary-law/overviewcust omary -law.htm (26 Maret 2013)

BBC News, 25 Januari 2008, ***Estonia fines man for 'cyber war'*** , http:// news. bbc.co. uk/2/hi /technology/ 7208511.stm (22 Februari 2013)

CERT/CC, 2001, *CERT® Advisory CA-2001-19 "**Code Red**" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL,* http://www. cert.org/ advisories/CA-2001-19.html (19 Februari 2013)

Chad Nelson, ***Cyber Warfare: The Newest Battlefield***, Washington University in St. Louis, http:// www.cse.wustl.edu/~jain/cse571-11/ftp /cyberwar.pdf (20 Oktober 2012)

Danchev, Dancho, 2008, *"**Coordinated Russia vs Georgia**"*, http://www.zdnet.com/blog /security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (22 Februari 2013)

Eric, Peter, ***A Practical Guide to Honeypot***, Washington University in St. Louis, http://www.cse. wustl.edu /~jain/cse571-09/ftp/honey/index.html#sec1.2(24 Maret 2013)

Hollis, David, ***Cyber War Case Study: Georgia 2008***, Small Wars Journal, http://smallwarsjournal.com/ jrnl/art/ cyberwar-case-study-georgia-2008 (29 September 2012)

iaknuranda.lecture.ub.ac.id/files/2011/10/DPK-PengantarAlgoritma-IA-UB.ppt (19 Februari 2013)

Kuehl, Dan, ***From Cyberspace to Cyberpower: Defining the Problem***, Information Operations at the National Defense University, USA, www.carlisle.army.mil/DIME/documents/ (20 Februari 2013)

Nils Melzer, 2011, ***Cyber Warfare and International Law***, UNIDIR. RESOURCES. IDEAS FOR PEACE AND SECURITY, *unidir.org/pdf/activites/pdf2-act649.pdf (20 Oktober 2012)*

Sanger , David. E., 2012, ***Obama Order Sped Up Wave of Cyberattacks Against Iran***, The New York Times: Middle East, http://www.nytimes .com /2012 /06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against iran.html?_r=2& (18 Desember 2012)

SECPOINT, ***What is Cyberwarfare?***, http://www.secpoint.com/what-is-cyberwarfare.html (20 Oktober 2012)

Prof. Richardus Eko Indrajit, **Analisa Malware**, http:// www.idsirtii.or.id/ content/files/IDSIRTII-Artikel-MalwareAnalysis.pdf *(20 Oktober 2012)*

The Economist, 2008, ***Marching off to cyberwar***, The internet: Attacks launched over the internet on Estonia and Georgia highlight the difficulty of defining and dealing with "cyberwar", http:// www.economist.com /node/ 12673385 (29 September 2012)