Tinjauan Mengenai *Cyber Warfare* Berdasarkan Hukum Humaniter Internasional

(Studi Kasus Perang Antara Rusia Dengan Georgia Pada 7 Agustus 2008)

Artikel Ilmiah

Untuk Memenuhi sebagian Syarat- syarat

Untuk Memperoleh Gelar Kesarjanaan

Dalam Ilmu Hukum

Oleh:

IVAN HILMI ALVIANTO

0910110180

KEMENTRIAN PENDIDIKAN DAN KEBUDAYAAN

UNIVERSITAS BRAWIJAYA

FAKULTAS HUKUM

MALANG

2013

Tinjauan Mengenai Cyber Warfare Berdasarkan

Hukum Humaniter Internasional

(Studi Kasus Perang Antara Rusia Dengan Georgia Pada 7 Agustus 2008)

Ivan Hilmi Alvianto

Fakultas Hukum Universitas Brawijaya

Abstract

Ivan Hilmi Alvianto, International Law, Faculty of Law Brawijaya University, July 2013, review of cyber warfare under internasional humanitarian law (case study on warfare between Russia with Georgia on 7th August 2008). Setyo Widagdo, SH. MHum.; Ikaningtyas, SH.LLM.

This thesis discussed about review of cyber warfare under internasional humanitarian law. The background of this research is the cyber warfare conducted by developed country against the other country, in which it is done to destroy the infrastructure of computerized. On 7th August 2008, occurred cyber warfare conducted by Russia against Georgia, in this case, cyber warfare that occurred has made important websites and Georgia's Internet infrastructure may not work. The issues raised is how to arrangement cyber warfare under international humanitarian law prespective, and how to application of the rules of international humanitarian law applied in the case of cyber warfare that occurred in Georgia in the war between Russia and Georgia. This research is a juridical normative, with case approach, conceptual approach and statuta approach are involved.

The result of the issue is international humanitarian law may be applied on cyber warfare, by looking at the impact or consequences, and the elements are the same as a conventional war in generally. Regarding the application of humanitarian law in the case of cyber warfare between Russia and Georgia is known that The StopGeorgia.ru can be qualified as combatant because, they has been organized by Maksim Zharov. However, cyber attacks are carried out by

Russia is not in accordance with the principles of distinction and proportionality because, carried out attacks against public websites.

Conclusion of this thesis is the principle-principle who contained in inside principle of international humanitarian law who contained in inside the source its legal can be be applied within cyber warfare. Suggestion of the authors is the need for cooperation among experts and information technology as well as legal experts in international humanitarian law in particular examine cyber warfare, as well as to disseminate and increase the status of the Tallinn Manual as a source of international law in terms of cyber warfare.

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.*

PENDAHULUAN

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 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

---

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

[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)

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 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

---

[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

[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

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 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

---

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

[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

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 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

---

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)

[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)

(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 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.

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 ?

METODE 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. Pendekatan penelitian yang digunakan dalam karya ilmiah ini yaitu pendekatan *statute approach,* 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),* 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.

PEMBAHASAN

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. 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.[22]

[22] Anonymous, 2010, ***Cyber Operations***, Air Force Doctrine Document 3-12, hal. 1

Dalam Artikel 2 (4) Piagam PBB;[23]*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 sebagai domain di dalam peperangan maka, terlebih dahulu harus ditentukan kedaulatan (*sovereignty*) suatu Negara di dalam *cyberspace*.

Menurut Bodley, kedaulatan 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.[24] Sedangkan kedaulatan yang internal adalah kewenangan yang dimiliki oleh suatu Negara untuk menjalankan fungsinya dalam lingkup nasional.[25] Dalam *Tallinn Manual The International Law Applicable to Cyber Warfare Rule 1. Sovereignty* menyatakan bahwa;[26]*A State may exercise control over cyber infrastructure and activities within its sovereign territory.* Peraturan tersebut menjelaskan bahwa, suatu Negara dapat menjalankan kontrol terhadap infrastruktur *cyber* dan aktivitas *cyber* di dalam wilayah kedaulatannya.

Dari definisi yang di berikan oleh Bodley dan aturan yang tercantum dalam *Tallinn Manual* dapat disimpulkan bahwa, 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.

---

[23] Hovel, Devika, 2004, ***Chinks in the Armour: International Law, Terrorism, and The Use of Force***, UNSW Journal, hal. 399
[24] MP Ferreira-Snyman, *Loc.Cit*, hal. 4
[25] MP Ferreira-Snyman, *Loc.Cit*, hal. 4
[26] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 1.

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

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. 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, *severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy.* Adanya akibat atau dampak yang di timbulkan oleh cyber attack yang memenuhi kriteria tersebut maka, *cyber attack* sama dengan serangan konvensional.

Di dalam *Additional Protocol I Article 49,* mendefinisikan *attacks* sebagai, *acts of violence against the adversary, whether in offence or in defence*.[27] Dalam Artikel tersebut *violence* harus dianggap sebagai pengertian dari *violent consequences* dari pada *violent acts.*[28] 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 efek (*effect*). Beberapa sarjana menyetujui tiga model pendekatan yang diberikan oleh Jean Pictet yang disebut sebagai *Use of Force Continuum,* yakni;[29]

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.

[27] Protocol Additional to The Geneva Convention of 12 August 1949, Article 49 (1)
[28] Richardson, John, 2011***, Stuxnet As Cyberwarfare: Distinction and Proportionality On The Cyber Battlefield***, National Academic of Science, hal. 14
[29] *Ibid*, hal. 16

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

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

Di dalam *Article 48 Additional Protocol I* di sebutkan bahwa, adanya kewajiban para pihak untuk membedakan antara, penduduk sipil dan kombatan, serta obyek sipil dengan obyek militer. Berdasarkan Artikel tersebut maka, diperlukan kualifikasi mengenai kombatan maupun penduduk sipil dalam *cyber warfare*, yakni;

a) Kualifikasi kombatan

Sebagaimana dijelaskan dalam *Article 4A (2) Geneva Convention III*, terdapat beberapa syarat yang harus di penuhi untuk dapat dikatakan sebagai kombatan, yaitu;[30]

a. *Being commanded by a person responsible for his subordinates*

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

[30] 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 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;[31] *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.*

Selanjutnya mengenai *wearing a distinctive emblem,* dalam *Tallinn Manual Rule 26. Commentary 10, Member of the Armed Forces,* di jelaskan bahwa;[32] 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. 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* dan *Tallinn Manual Rule 41*, dapat di simpulkan bahwa, mengenai *carrying arms openly*, di perlukan pemahaman bahwa, membawa senjata

[31] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 26, Commentary 9
[32] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 26, Commentary 10

secara terang-terangan berarti berkemampuan, memiliki sarana dan perlengkapan, dan memiliki tujuan utama yaitu melancarkan serangan cyber.

b) Kualifikasi Penduduk Sipil

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.[33] 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*.

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.

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

c) Obyek Sipil dan Obyek Militer

Penjelasan mengenai obyek sipil dan obyek militer terdapat di dalam *Article 52 Additional Protocol I*, yaitu; [34]

> *(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 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.*

Berdasarkan Artikel tersebut, terdapat 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

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

atau infrastruktur yang terkomputerisasi maka, software, perangkat keras, atau peralatan lain yang di gunakan dalam *cyber attack* dapat di golongkan sebagai obyek.

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.[35]

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 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.[36] 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.[37]

d. ***Indiscriminate attack***

Dalam *distinction principle* di jelaskan bahwa, serangan harus langsung mengarah pada obyek militer, selain itu juga dilarang adanya *indiscriminate*

[35] Schmitt, Michael.N, 2002, *Op.Cit,* hal 384
[36] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 29, Commentary 1
[37] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 29, Commentary 4

attack atau serangan yang tidak dapat membedakan. Hal tersebut di jelaskan dalam *Article 51 (4) Additional Protocol I*, yaitu;[38]

> *Indiscriminate attacks are prohibited. Indiscriminate attacks are:*
>
> *(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.[39] 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.[40] 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

[38] Protocol Additional to The Geneva Convention of 12 August 1949, Article 51 (4)
[39] Schmitt, Michael.N, 2002, *Op.Cit*, hal. 389
[40] 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

pesawat swasta menjadi target serangan karena kesalahan dalam penargetan.[41] 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*;[42] *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*[43] 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.[44] Setelah itu, komputer yang mengunduh gambar tersebut akan terkena dampak dari *malicious script* tersebut.[45] Hal tersebut merupakan bentuk dari *indiscriminate attack*, karena siapa pun yang melakukan pengunduan dan kemudian membuka gambar tersebut dapat terinfeksi oleh malware tersebut. *Malicious code* yang seharusnya dapat di gunakan secara *discriminate* akan tetapi digunakan secara *indiscriminate.*[46]

---

[41] Kodar, Erki, *Loc.Cit*, hal. 122
[42] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule, 49
[43] *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.
[44] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 49, Commentary 3
[45] *Ibid*
[46] *Ibid*

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;[47] *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 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;[48] *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.[49] Sedangkan, mengenai *indirect effect* terdapat penundaan atau perubahan, menurut Commentary, *collateral damage* harus dapat diperkirakan sebelumnya oleh pihak yang terkait, dengan melihat

[47] Protocol Additional to The Geneva Convention of 12 August 1949, Article 51(5) b
[48] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 51
[49] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 51, Commentary 6

planning, *approving*, dan *executing* dalam melakukan serangan cyber.[50] 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.[51]

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

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.[52] 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.[53] Pada umumnya kerentanan di publikasikan setelah adanya *patch*[54] 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;[55]
    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

[50] *Ibid*
[51] *Ibid*
[52] 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
[53] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., *Loc. Cit*, hal. 83
[54] *Patch* merupakan bagian kecil dari software yang digunakan untuk memperbaiki kesalahan atau celah yang terdapat di dalam suatu program software ataupun sistem operasi komputer
[55] Owens, William A., Dam, Kenneth. W., Lin, Herbert S., *Op.Cit*, hal. 85

fungsinya sebagai mana tujuan dari dibuatnya software tersebut.

2. *Hardware* (perangkat keras), *microprocessors, microcontroller*, *motherboard* atau *circuit board*, *power supplies*, *printer* atau *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 pemeliharan 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.[56] Selain itu, prinsip mengenai precaution dan neutrality yang termasuk di dalam prinsip proporsionalitas harus di perhatikan pula

f. Unnescessary 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*;[57] *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 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

[56] Tallinn Manual On The International Law Applicable to Cyber Warfare, Rule 51, Commentary 7
[57] Protocol Additional to The Geneva Convention of 12 August 1949, Article 35 (2)

perawatan pasien baik kombatan maupun sipil.[58] 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,[59] *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 ini.[60] 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

---

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

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

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

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.

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

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.[61] 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

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

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 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,[62] 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 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.[63]

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

[62] Anonymous, 2005, ***Report Expert Meeting: Targeting Military Objectives***, the University Centre for International Humanitarian Law Geneva, hal. 9
[63] *Ibid*, hal. 3

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 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*.

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan pembahasan diatas dapat diatrik beberapa kesimpulan bahwa:

1. Sebagai konsumen atau penikmat jasa penerbangan, penumpang memiliki beberapa bentuk perlindungan hukum terhadap mereka antara lain perlindungan keselamtan, perkembangan tariff atau harga dari jasa angkutan udara itu, kwalitas dari pelayanan, keamanan, kenyamanan, dan perjanjian angkutan,. Dalam hal terjadi sebuah kecelakaan yang mana menyebabkan meninggal dunia, luka terhadap penumpang pesawat, penumpang tersebut berhak atas sebuah ganti rugi.. Dalam hukum nasional pengaturan terkait dengan pemberian ganti rugi terhadap korban kecelakaan pesawat yang meninggal dunia, cacat diatur dalam pasal 141 Undang-undang No 1 tahun 2009 tentang penerbangan yang diatur lebih lanjut dalam Peraturan Menteri Perhubungan No 77 tahun 2011 tentang tanggung jawab pengangkut angkutan udara, dalam pasal 3 huruf (a) sedangkan dalam konvensi Chicago 1944 tidak terdapat pengaturan terkait dengan pemberian ganti rugi terhadap korban kecelakaan angkutan udara.
2. Hambatan yang dialami dalam pemberian ganti rugi adalah, tidak ada satupun ketentuan yang memberikan kewajiban pemberian ganti rugi terhadap korban yang meningggal dunia dalam penerbangan bukan niaga. Dengan kata lain telah terjadi kekosongan hukum terkait dengan ganti rugi terhadap korban kecelakaan angkutan udara bukan niaga, baik dalam tatanan nasional maupun dalam tatanan internasional. Sebagaimana telah dijelaskan di atas bahwa penerbangan sukhoi super jet 100 digolongkan kedalam angkutan udara bukan niaga. Dimana ketentuan dalam tatanan internsional yaitu konvensi warsawa 1929 berserta amandemennya berlaku bagi angkutan udara internasional komersial. Begitu pula dengan ketentuan ganti rugi yang diatur

dalam undang-undang No 1 tahun 2009, ganti rugi tersebut hanya berlaku bagi penerbangan komersial atau angkutn udara niaga saja.

B. Saran

1. Sebaiknya dibuatlah pengaturan terkait dengan tanggung jawab pengangkut dalam angkutan udara bukan niaga. Karena dalam perkembangannya penerbangan dalam sektor bukan niaga mengalami peningkatan pada masa sekarang ini. Apabila tidak dibuat sebuah pengaturan terhadap angkutan udara bukan niaga ini maka aspek perlindungan hukum sulit untuk dijalankan
2. Pengaturan ini sebaiknya tidak saja dalam tatanan hukum nasional saja melainkan juga dalam tatanan hukum internasional. Hal ini ditjukan untuk menciptakan sebuah kepastian dan perlindungan hukum terhadap pengguna angkutan udara terlebih pengguna angkutan udara bukan niaga.
3. Pengaturan yang baru tersebut sebaiknya menggunakan prinsip *Strict liability*, bukan *Liability based on fault.* Sehingga lebih memberikan kepastian hukum bagi para korban.

DAFTAR PUSTAKA

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)

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)

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)

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

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

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

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

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)

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

Protocol Additional to The Geneva Convention of 12 August 1949,

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

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

Tallinn Manual On The International Law Applicable to Cyber Warfare

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

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

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

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

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