Kosmik Hukum

Fakultas Hukum
Universitas Muhammadiyah Purwokerto
Vol. 21 No. 3 (2021)

Analisis Doktrin Perang Yang Adil *(Just War)* dalam Kasus Serangan Siber Rusia Terhadap Georgia Tahun 2008

Aryuni Yuliantiningsih✉
Fakultas Hukum, Universitas Jenderal Soedirman

E-mail: aryuni.yuliantiningsih@unsoed.ac.id

Abstract

Cyberwarfare is a warfare with information technology that has developed. It has not been regulated in humanitarian law. Cyber attacks have been **carried** *out by several countries by ignoring the Just War Theory. This article aims to analyze the implementation of the Just War theory in cyber warfare according to international humanitarian law in the case of conflict between the Russian and Georgia in 2008. The research method use the normative juridical and using secondary data sources. Qualitative data using deductive conclusion method. Based on the research results, it is known that the just war theory including jus ad bellum, jus in bello and jus post bellum is not applied in cyberwarfare. The Russian's cyber attack against Georgia violates the distiction principle , the principle of proportionality and the principles of proportionality. The losses incurred as a result of cyberattacks are not compensated by Russia.*

Keywords: *Just War, cyber attack, Russia, Humanitarian law.*

Abstrak

Cyberwarfare merupakan cara berperang dengan teknologi informasi yang telah berkembang dan belum diatur secara jelas dalam hukum humaniter. Serangan siber telah dilakukan oleh beberapa negara dengan mengabaikan Teori Perang yang Adil . Artikel ilmiah ini bertujuan untuk menganalisis penerapan teori Perang yang Adil dalam *cyberwarfare* menurut hukum humaniter internasional dalam kasus serangan siber Rusia ke Georgia tahun 2008. Metode penelitian yang digunakan adalah metode yuridis normatif dengan menggunakan sumber data sekunder. Data dianalisis secara kualitatif dengan metode pengambilan simpulan secara deduktif. Berdasarkan hasil penelitian diketahui bahwa Teori perang yang adil yang meliputi *jus ad bellum, jus in bello dan jus post bellum* tidak diterapkan dalam *cyberwarfare*. Serangan siber Rusia terhadap Georgia telah melanggar prinsip pembedaan, prinsip kemanusiaan dan prinsip proporsionalitas. Kerugian yang timbul akibat serangan siber tidak diberi ganti rugi oleh Rusia.

Kata kunci: Perang Adil, Serangan Siber, Rusia, hukum Humaniter

Kosmik Hukum Vol. 21 No. 3 (2021): 167-175
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v21i3.10613

I. Pendahuluan

Perang sudah dilakukan sejak berabad-abad yang lampau dan terus mengalami perkembangan mengenai alat dan cara berperang. Setiap zaman memiliki jenis perangnya sendiri, dengan kondisi tertentu karena karakteristik pelaku dan metode yang berbeda. Metode yang digunakan dalam perang dapat berubah seiring waktu, tetapi sifat perang itu sendiri tidak akan berubah. Militer selama ini telah merancang perang konvensional berupa strategi perang darat, laut dan udara. Seiring perkembangan teknologi, muncul dimensi keempat dalam perang bersenjata, yakni strategi perang lewat ruang *cyber*. [1]

Penggunaan teknologi informasi sebagai cara metode dalam berperang (*cyberwarfare*) adalah salah satu ancaman terhadap ketahanan pertahanan dan keamanan negara. *Cyberwar*, merupakan perang yang menggunakan jaringan komputer dan internet atau dunia maya (*cyber space)* dalam bentuk strategi pertahanan atau penyerangan sistem informasi lawan.[2]*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, namun pihak-pihak tersebut bukan lagi sebagai individu melainkan negara yang kemudian disebut sebagai serangan siber atau *cyberattack*. [3]

Ancaman serangan siber yang pernah terjadi antara lain**, pertama,** serangan Stuxnet milik Amerika Serikat yang melumpuhkan pembangkit nuklir Bushehr Iran dengan worm tahun 2010. [4] Kedua, Operasi Aurora dilakukan oleh China, menyerang perusahaan besar termasuk Google dan Adobe Systems.[5] Ketiga, kasus Estonia tahun 2007, dimana Estonia menghadapi gelombang serangan cyber yang melanda segenap infrastruktur internet negara itu, mulai dari situs-situs pemerintahan, perbankan, hingga situs-situs surat kabar lokal. Serangan ini terjadi melumpuhkan sistem pemerintahan Estonia selama 2 (dua) minggu. [6] Keempat serangan siber yang dilakukan oleh Rusia terhadap Georgia pada tahun 2008.[7] Kasus ini berawal dari konflik Rusia dan Georgia di Ossetia Selatan. Serangan siber melumpuhkan beberapa situs pemerintah Georgia dan situs-situs media lokal, setelah Georgia menyerang Ossetia Selatan. [8] Serangan siber Rusia dilakukan dalam skala besar dan telah merusak fasilitas–fasilitas umum yang mengganggu kepentingan penduduk sipil. Dengan semakin bertambahnya kasus serangan siber maka perlu untuk mengkaji kasus ini dalam perspektif teori Perang yang Adil.

Telah ada beberapa artikel ilmiah yang mengkaji mengenai cyberwar antara lain, pertama, Arlina Permanasari dalam artikel yang berjudul "**Relevansi Prinsip Pembedaan Dan *Big Data* Dalam Perang** Siber Pada Era Revolusi Industri 4.0". Artikel ini mengkaji mengenai Data. Data atau objek dalam perang siber dapat dianggap sebagai sasaran militer apabila memenuhi kriteria sifat, lokasi, penggunaan dan tujuannya. Prinsip pembedaan dapat diterapkan dalam perang siber karena tidak semua data merupakan sasaran militer.[9] Kedua,

---

1 Nur Khalimatus Sa'diyah and Ria Tri Vinata, "Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara," *Perspektif* 21, no. 3 (2016): 168-187.

2 Bagus Artiadi Soewardi, "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia", Media Informasi Potensi Pertahanan, Maret 2013

3 Idik Saeful Bahri, *Cyber Crime Dalam Sorotan Hukum Pidana*, UGM, 2020.

4 Sanger , David. E., 2012, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, The New York Times: Middle East, dikutip dari laman, http://www.nytimes. com/2012/06/01/world/middleeast/obamaordered- wave-of-cyberattacks-against iran. html?_r=2&diakses pada tanggal 15 Maret 2021

5 Bruce Middleto*n, A History of Cyber Security Attack,* Auerbach Publications, 2017, 1

6 Iradhati Zahra, Irawati Handayani, and Diajeng Wulan Christianti, "Cyber-Attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law," *Yustisia Jurnal Hukum* 10, no. 1 (2021): 48-68.

7 Tikk, Eneken, *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defense Center of Exellence, 2008, 4

8 Paulo Shakarian, "The 2008 Russian Cyber-Campaign Against," Military Review, no. May (2014).63-68

9 Arlina Permanasari, "Relevansi Prinsip Pembedaan Dan *Big Data* Dalam Perang Siber Pada Era Revolusi Industri 4.0"**,** *Jurnal Hukum Pidana dan Pembangunan Hukum*, Vol 1, No 2 (2019)

Ethan A. Wright dalam artikel yang berjudul "Of Drones and Justice: A Just War Theory Analysis of the United States' Drone Campaigns" meneliti tentang Kebijakan penggunaan Drone oleh Amerika serikat ditinjau dari sisi Etika dalam berperang.[10]

Kebaruan dari artikel ilmiah ini adalah pembahasan lebih fokus pada kajian analisis penerapan just war theory dalam kasus serangan siber yang dilakukan oleh Rusia terhadap Georgia tahun 2008. Analisis teori just war penting dilakukan untuk dapat diterapkan pada kasus perang siber yang lain. Just war teori merupakan justifikasi suatu negara untuk melakukan perang yang sah. Terdapat dua prinsip keadilan yang dikaji, pertama, apakah alasan negara melakukan perang adalah sah (*jus ad bellum*) dan kedua apakah dalam melakukan perang tindakannya bermoral atau tidak. (*jus in bello*). Perang juga harus memperhatikan etika yang dikenal dengan *just war* atau perang yang adil.) [11] Perang konvensional telah diatur secara jelas dalam Hukum Humaniter Internasional, namun mengenai serangan siber dan cyber warfare belum diatur secara khusus dalam hukum internasional. Aturan yang ada saat ini adalah berupa panduan *Talinn Manual on the applicable of Cyberwarfare* yang dikeluarkan oleh NATO pada tahun 2013.

II. Rumusan Masalah

Berdasarkan latar belakang tersebut di atas maka dapat dirumuskan permasalahan sebagai berikut : *Pertama,* bagaimanakah implementasi teori Perang yang Adil dalam hukum humaniter internasional; *Kedua,* bagaimanakah penerapan teori perang yang adil dalam cyber attack yang dilakukan oleh Rusia terhadap Georgia tahun 2008.

III. Metodologi Penelitian

Penelitian ini menggunakan metode yuridis normatif, dengan pendekatan perundang-undangan, pendekatan konseptual yang mengkaji konsep just war dan pendekatan kasus deengan melakukan studi terhadap konflik Rusia dan Georgia tahun 2008. Sumber data yang digunakan adalah sumber data sekunder yang terdiri dari bahan hukum primer dan bahan hukum sekunder. Analisis data dilakukan secara kualitatitif dengan pengambilan simpulan secara deduktif.[12]

IV. Hasil dan Pembahasan

1. Penerapan Teori Perang yang Adil dalam Hukum Humaniter Internasional

Konsep perang yang adil (*just war theory*) merupakan dasar dari suatu negara untuk melakuan perang yang sah secara hukum dan moral. Sejarah munculnya Teori Perang yang Adil dimulai dari karya beberapa filsuf penting. Agustinus (354-430) memberikan landasan bagi Teori Perang yang Adil dalam kesusastraan Barat. Thomas Aquinas (1225-1274) mengkodifikasi refleksi Agustinus ke dalam kriteria berbeda yang tetap menjadi dasar Teori Perang Adil seperti yang digunakan saat ini. [13]

Inti dari just war adalah *jus ad bellum*, *jus in bello* dan *jus post bellum*. *Jus ad bellum* mengatur tentang bagaimana negara dibenarkan menggunakan kekerasan bersenjata. *Jus ad bellum* menyangkut etika dan moral dalam perang. Mark Amstutz memisahkan konsep *jus ad bellum* menjadi enam kriteria penting yang digunakan untuk mengetahui apakah konflik itu

---

[10] Ethan A. Wright., "Of Drones and Justice: A Just War Theory Analysis of the United States' Drone Campaigns", dikutip dari laman https:/ /digitalcommons.ursinus.edu/cgi/ viewcontent.cgi? article=1003&context=ethics_ essay, diakses pada tanggal 15 Maret 2021

[11] Erich Freiberger, "Just War Theory and the Ethics of Drone Warfare", dikutip dari laman https://www.e-ir.info/2013/07/18/just-war-theory-and-the-ethics-of-drone-warfare/ diakses pada tanggal 15 Maret 2021

[12] Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta : Kencana Prenada Media), 2013, 141.

[13] Eric Patterson, "Just War Theory and Explosive Remnants of War Just War Theory and Explosive Remnants of War" Jounal of Conventional Weapon Destruction 13, no. 1 (2009): 1–3.

Kosmik Hukum Vol. 21 No. 3 (2021): 167-175
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v21i3.10613

adil, yaitu : alasan yang adil, otoritas yang kompeten, niat yang benar, tujuan terbatas, perang sebagai pilihan terakhir. [14]

Jus in bello yaitu hukum yang berlaku dalam perang. Kombatan dalam berperang harus menghormati prinsip pembedaan, proporsionalitas, nessesitas dan kemanusiaan. [15] Aturan *jus in bello* terdapat dalam Hukum Den Haag dan hukum Jenewa. Hukum Den Haag mengatur cara dilakukannya perang sedangkan hukum Jenewa mengatur perlindungan orang¬-orang yang menjadi korban perang.[16]

Jus post bello menerapkan langkah-langkah diperlukan untuk transisi dari keadaan perang ke keadaan damai setelah perang selesai. *Jus post bello* adalah bidang baru teori perang yang adil yang bertujuan mengidentifikasi prinsip-prinsip dalam periode ini. Beberapa prinsip tersebut adalah: status quo, penghukuman bagi pelaku kejahatan perang, kompensasi bagi korban, dan pembuatan perjanjian perdamaian. [17]

Dalam *Jus in bello* berlaku prinsip pembedaan, kemanusiaan dan nesesitas. Prinsip pembedaan yang berkaitan pembedaan objek-objek sipil maupun sasaran militer, telah dicantumkan dalam Konvensi-konvensi Den Haag 1899 maupun 1907, Konvensi-konvensi Jenewa 1949, dan Protokol Tambahan I tahun 1977 yang melengkapi Konvensi-konvensi Jenewa tahun 1949 . Perlindungan umum terhadap penduduk sipil diatur dalam Pasal 3 Konvensi Jenewa 1949. Pasal 48 Protokol Tambahan I tahun 1977 menegaskan bahwa: agar dapat menjamin penghormatan dan perlindungan terhadap penduduk sipil dan objek sipil, para pihak dalam sengketa setiap saat harus membedakan penduduk sipil dari kombatan dan objek sipil dari sasaran militer dan karenanya harus mengarahkan operasinya terhadap sasaran militer.

Pasal 52 ayat (1) Protokol Tambahan I menyatakan bahwa pada hakekatnya objek sipil adalah semua objek yang bukan sasaran militer. Sedangkan Pasal 52 ayat(2) menentukan bahwa sasaran militer adalah objek yang karena sifat, lokasi dan tujuan atau penggunaannya, yang apabila dikuasai, dinetralisir atau dihancurkan baik sebagian atau seluruhnya, pada suatu situasi dan waktu tertentu, akan dapat memberikan kontribusi efektif pada operasi-operasi militer dan memberikan keuntungan militer yang pasti (*definite military advantage*), sedangkan dalam ayat (3) dinyatakan bahwa apabila terdapat keragu-raguan mengenai status suatu objek, maka objek tersebut harus dianggap sebagai objek sipil, sampai terdapat keputusan bahwa ia merupakan sasaran militer.[18]

Saat ini *cyber attact* menjadi metode baru untuk menyerang pertahanan suatu negara. *Cyber attacks* (serangan siber) mengacu pada penggunaan kegiatan yang disengaja untuk mengubah, mengganggu, menipu, menurunkan, atau menghancurkan sistem komputer atau jaringan yang digunakan oleh musuh atau informasi dan / atau program penduduk di atau transit melalui jaringan systemsor. [19] Permasalahan muncul ketika *cyberattack* mulai dinilai dapat memberikan keuntungan-keuntungan militer, dan dikoordinasikan dengan konflik bersenjata seingga perlu dikaji lebih lanjut apakah serangan siber oleh Rusia telah memenuhi doktrin perang yang adil.

Untuk merespon kebutuhan aturan tentang *cyber warfare*, NATO telah mengeluarkan *Talinn Manual The International Law Applicable to Cyber Warfare Rule tahun* 2009. Talinn Manual merupakan hasil dari studi akademik yang tidak mengikat tentang bagaimana hukum

---

[14] Carson Marr, "Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus Ad Bellum and Jus in Bello," *SPICE: Student Perspectives on Institutions, Choices and Ethics* 14, no. 1 (2019): 2.

[15] Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution," *Minnesota Journal of International Law* 26, no. 2 (2017): 419–60.

[16] Arlina Permanasari, *Pengantar Hukum Humaniter*, (Jakarta :ICRC, , 1998). 15

[17] Thomas Gregory, "Ethics and War: A Critical Intervention," *Millennium: Journal of International Studies*, (2018): 1-12.

[18] Robert Kolb, "Military Objectives in International Humanitarian Law," *Leiden Journal of International Law* 28, no. 3 (2015): 691–700, .

[19] Herbert. Lin, "Cyber Conflict and International Humanitarian Law", *International Review of The Red Cross*, Volume 94, Number 886 Summer (2012): 515-531.

internasional diberlakukan dalam *cyber conflict* dan *cyber warfare*. Tallin Manual telah mengakomodasi ketentuan-ketentuan yang terdapat hukum internasional dan HHI, antara lain mengenai kedaulatan negara, prinsip tanggung jawab negara, larangan penggunaan kekerasan, bela diri , alat dan cara berperang dalam *cyber armed conflict*. [20]

2. Analisis Penerapan Perang yang Adil dalam Kasus Cyber warfare antara Iran dan Israel Tahun 2020

*The Russia-Georgia War m*erupakan salah satu contoh serangan *cyber* yang bertepatan dengan invasi suatu negara ke negara lain melalui darat, laut dan udara. Invasi Rusia ke Georgia sebagai respon serangan Georgia terhadap separatis di Ossetia Selatan. [21] Kampanye *cyber* yang terkoordinasi secara baik menyerang website bernilai strategis milik pemerintahan Georgia termasuk kedutaan AS dan Inggris melalui serangan berupa; *Distributed Denial of Service (DDoS), SQL injection,* dan *cross scripting (XSS)22.*[23]

Sebelum hari operasi militer atau perang konvensional tersebut dimulai, *cyberattack* telah *dilakukan* terhadap website-website milik Georgia. Tercatat 54 website yang berhubungan dengan komunikasi, keuangan, dan pemerintahan diserang oleh pihak Rusia.[24] Penyerangan dengan metode *DDoS* 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.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).

Akibat serangan siber yang terjadi di Georgia, dua penyedia utama layanan internet di Georgia yaitu, *United Telecom of Georgia* dengan router jenis Cisco 7206 tidak dapat menyediakan pelayanan selama beberapa hari, kemudian *Caucasus Network Tbilisi18* telah dibanjiri *(flooded*[25]*)* secara besar-besaran dengan berbagai *queries*. Hal tersebut seolah-olah telah membuat infrastruktur *Caucasus Network* telah masuk dalam zona perang dan telah menjadi sasaran atau target, yang mengakibatkan *physical disconnections*.[26] Lebih dari itu tidak dapat diaksesnya 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.

Analisis *jus ad bellum* adalah sebagai berikut, alasan Rusia menyerang Georgia pada tahun 2008 adalah untuk melakukan intervensi militer karena Georgia telah menyerang Ossetia Selatan . Intervensi Rusia telah melanggar kedaulatan negara yang bertentangan dengan Pasal 2 (4) Piagam PBB yang menyatakan bahwa setiap negara dalam hubungan internasionalnya agar menghindari penggunaan kekerasan (*use of force)* yang mengancam teritorial negara lain. Dengan memperluas cyber space sebagai dimensi teritorial selain wilayah darat, laut dan udara, maka serangan siber yang dilakukan oleh Rusia terhadap Georgia dianggap telah mengancam kedaulatan teritorial menurut hukum internasional. Tujuan dari serangan siber Rusia adalah untuk mengisolasi Georgia dari komunitas masyarakat internasional. **[27]** Perang

---

[20] Tallinn_Manual on the International Law Applicable to Cyber Warfare, tersedia di https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdfdiakses pada 23 Maret 2021

[21] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* 7, no. 1 (2011): 1–9.

[23] Jeffrey, Carr. *Inside Cyber Warfare.* USA: O'reilly Media. 2011 hlm. 3

[25] *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)

[26] Danchev, Dancho, 2008, "***Coordinated Russia vs Georgia***", tersedia di http://www.zdnet.com/blog /security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 diakses pada tanggal 11 Mei 2021

[27] Paulo Shakarian, "The 2008, The Russian Cyber- Campaign Againts Georgia", *Military Review* λ November-December (2011), 63-68

Kosmik Hukum Vol. 21 No. 3 (2021): 167-175
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v21i3.10613

antara Rusia dengan Georgia bukan merupakan last resort atau jalan terakhir yang ditempuh karena dalam konflik ini belum ditenpuh penyelesaian sengketa secara damai.

Berdasarkan *jus in bello*, perang harus menghormati prinsip pembedaan dan kemanusiaan. Serangan siber hanya boleh ditujukan kepada kombatan dan objek militer bukan pada objek sipil. Dalam kasus ini , objek yang menjadi target serangan Rusia adalah objek sipil yang tujuannya untuk melayani fasilitas umum. Tercatat 54 website yang berhubungan dengan komunikasi, keuangan, dan pemerintahan diserang oleh pihak Rusia[28]. Cyber **attack** yang dilakukan Rusia telah menimbukan kerugian baik fisik atau mental bagi penduduk sipil. Dalam hal ini Rusia telah melanggar prinsip pembedaan karena yang menjadi sasaran dalam perang termasuk penduduk sipil. Prinsip lain yang telah dilanggar adalah prinsip proporsionalitas karena untuk mencapai kemenangan, Rusia telah melanggar prinsip pembedaan yang menimbulkan kerugian terhadap penduduk sipil.

Berdasarkan Rule 38 Tallinn Manual tentang hukum internasional yang mengatur tentang perang siber, maka Tallinn Manual versi 1.0 ini telah menentukan apa yang dimaksud objek **sipil** dan sasaran militer. Dalam Rule 38 tersebut, pengertian objek sipil dan sasaran militer mengikuti definisi sebagaimana yang telah dicantumkan dalam Pasal 52 ayat (1) dan (2) Protokol Tambahan I 1977. Hanya saja, pada kalimat terakhir Rule 38, disebutkan contoh sasaran milliter yaitu dapat meliputi "*computers, computer networks and cyber infrastructures*".

Protokol I mengakui bahwa dalam setiap pertikaian bersenjata, hak dari para Pihak-pihak dalam pertikaian untuk memilih cara-cara atau alat-alat peperangan tidaklah tak terbatas,[29] sehingga penting diperhatikan ketentuan Pasal 36 Protokol Tambahan I 1977 mengenai senjata-senjata baru. Bila alat yang dipergunakan dalam *cyber warfare* termasuk kategori senjata baru, alat atau cara berperang baru, maka Pihak Peserta Agung berkewajiban menetapkan apakah di dalam keadaan tertentu atau segala keadaan penggunaannya tidak dilarang oleh Protokol ini atau oleh sesuatu peraturan lain dari hukum internasional yang berlaku terhadap Pihak Peserta tersebut.

Perlindungan umum terhadap penduduk sipil dalam konflik bersenjata diatur dalam Pasal 3 ayat 1 Konvensi Jenewa 1949, sedangkan aturan-aturan perlindungan hukum yang lain diatur dalam pasal 51 ayat 2 dan ayat 6 Protokol Tambahan 1977, Pasal 130 Konvensi Jenewa 1949, pasal 11 ayat 4 Konvensi Jenewa 1949, pasal 35 bagian I, pasal 36 Protokol I tambahan, pasal 24 Konvensi Deen Haag IV tahun 1907, dan Pasal 22 Konvensi Deen Haag IV tahun 1907. Hukum humaniter telah mengatur definisi tentang serangan (*attack*) yang terdapat dalam Pasal 49 Protokol Tambahan I 1977 Konvensi Jenewa 1949, namun tidak menyebutkan *cyber attack* secara khusus. Serangan sebagai suatu aksi kekerasan terhadap lawan, baik bersifat ofensif maupun defensif.[30]

Cyber attack dapat disamakan dengan serangan konvensional. Pasal 49 *Additional Protocol I*, mendefinisikan *attacks* sebagai, *acts of violence against the adversary, whether in offence or in defence*. Dalam Pasal tersebut *violence* harus dianggap sebagai pengertian dari *violent consequences* dari pada *violent acts.* Tahun 2012, ICRC mengeluarkan pandangan tentang cyber warfare dan ukum humaniter internasional yaitu apabila cara dan metode dari *cyber warfare* menghasilkan akibat di dunia nyata serupa dengan yang dihasilkan oleh senjata konvensional (seperti penghancuran, gangguan, kerusakan, kerugian, cedera atau kematian), maka berlaku aturan yang sama dengan penggunaan senjata konvensional.[31] Serangan siber yang dilakukan ole Rusia tidak memenuhi kriteria perang yang adil baik *jus ad bellum* maupun *jus in bello*. serta

---

[28] Madelena Anna Miniats, War of Ner ar of Nerves: Russia es: Russia's Use of Cyber W s Use of Cyber Warfare in Estonia, Georgia and Ukraine, Annandale-on-Hudson, NY May 2019.

[29] Protokol Tambahan I, 1977, Psl. 35(1).

[30] Protocol Additional to the Geneva Convention of 12 August 1949, ang relating to Protection of the Victim of International Armed Conflicts (protocol I) 8 June 1977, 1125 UNTS 3 (Additional Protocol I), pasal 49 (1); "act[] of violence against the adversary, whether in iffence or defence"

[31] IRRC 2012, Vol. 94/886 editorial.

menlanggar prinsip pembedaan dan proporsionalitas yang diatur dalam hukum h umaniter internasional.

Pada bulan Agustus 2008, Uni Eropa memprakarsai perjanjian gencatan senjata antara Rusia dan Georgia dan selanjutnya Rusia menarik pasukannya dari wilayah Georgia.[32] Hague Conventions mengatur bahwa negara akan memberi bantuan perbaikan dan restitusi bagi korban sengketa bersenjata. Dalam kasus ini Rusia tidak memberi ganti rugi dan tidak memberi bantuan untuk memperbaiki fasiliitas pasca konflik dengan Georgia.

Cyber warfare belum diatur secara khusus dalam hukum humaniter namun walaupun demikian, prinsip-prinsip hukum humaniter yang ada dan penafsiran dari aturan-aturan yang berlaku dapat diterapkan dalam cyber warfare. HHI tidak melarang kombatan atau anggota pihak yang berkonflik untuk menggunakannya, sepanjang tidak bertentangan dengan asas-asas dan prinsip-prinsip HHI. [33]

Negara harus mengakui bahwa *cyber attack* dapat dikategokan sebagai pelanggaran pasal-pasal dalam Piagam PBB berkaitan dengan penggunaan kekerasan dan tindakan agresi terhadap negara lain, yang dapat dibalas dengan menggunakan prinsip *self defence*. Untuk menyelesaikan sengketa Dewan Keamanan PBB dapat menggunakan cara damai dan kekerasan berdasarkan Bab VI dan VII Pigam PBB. [34]

V. Penutup

1. Simpulan

Teori Perang yang adil menjadi etika berperang sejak jaman dahulu yang meliputi *jus ad bellum* (alasan berperang), *jus in bello* (cara berperang) dan *jus post bellum*. (setelah konflik) . *Jus ad bellum* meliputi kriteria, alasan dilakukan perang, perang sebagai jalan terakhir. Dalam Hukum humaniter *Jus in bello* diatur dalam hukum Den Haag dan hukum Jenewa yang mengatur prinsip pembedaan, nesesitas dan kemanusiaan, sedangkan *jus post bellum* meliputi tindakan-tindakan yang dilakukan pasca terjadinya konflik seperti membuat perjanjian perdamaian, penghukuman pelaku kejahatan, dan pemberian kompensasi.

Serangan siber Rusia terhadap Georgia ditinjau *dari jus ad bellum* tidak sesuai dengan alasan perang yang sah (*just war*). Rusia menyerang Georgia untuk melakukan intervensi militer terkait kasus merdekanya Osetia Selatan. Hal ini melanggar Pasal 2 (4) Piagam PBB. Berdasarkan *jus in bello*, serangan siber Rusia secara besar-besaran secara masif yang merusak jaringan komunikasi, layanan-layanan fasilitas umum telah melanggar prinsip pembedaan karena sasarannya bukan hanya obyek militer seperti yang diatur dalam Pasal 48, Pasal 51 dan Pasal 52 Protokol Tambahan I 1977 yang menegaskan menegaskan bahwa penduduk sipil, dan obyek sipil harus dilindungi dari akibat permusuhan. Mereka tidak dapat dijadikan target dalam operasi militer, yang merupakan dasar dari prinsip pembedaan. Hukum internasional belum mengatur secara tegas mengenai *cyber warfare* namun saat ini telah terdapat Panduan yang bersifat tidak mengikat dalam *Talinn Manual The International Law Applicable to Cyber Warfare Rule* 2013.

2. Saran

Negara-negara yang melakukan serangan siber seharusnya tetap menghormati prinsip-prinsip hukum humaniter yang berlaku. Untuk menjamin kepastian hukum, Negara-negara dapat segera membuat perjanjian internasional yang secara khusus mengatur tentang *cyberwarfare* .

---

[32] Rusia Tarik Pasukannya dari Gergia tersedia di laman https://edukasi.kompas.com/read/2008/10/08/17051125/rusia.tarik.semua.pasukannya.dari.georgia

[33] Nils Melzer, , *Cyber Warfare and International Law*, UNIDIR, 2011, 4

[34] Lauri Malksoo, *The Talinn Manual as an international even*, Book Reviews Cyber Security, No 120 August 2013, , tersedia di laman http www.diplomaatia.een/enarticle

Kosmik Hukum Vol. 21 No. 3 (2021): 167-175
E-ISSN: 2655-9242 | P-ISSN: 1411-9781
DOI: 10.30595/kosmikhukum.v21i3.10613

Daftar Pustaka

Ambarwati dkk., *Hukum Humaniter Internasional Dalam Studi Hubungan Internasional*, Jakarta: Rajawali Press, Jakarta.2013.

Idik Saeful Bahri, Idik, *Cyber Crime Dalam Sorotan Hukum Pidana*, Yogyakarta: UGM, 2020.

Jeffrey, Carr. 2011. *Inside Cyber Warfare.* USA: O'reilly Media. 2011

Marzuki, Peter Mahmud, *Penelitian Hukum*, Jakarta : Kencana Prenada Media, 2013.

Middleto*n,* Bruce, *A History of Cyber Security Attack,* Auerbach Publications, 201..

Miniats, Madelena Anna, War of Ner ar of Nerves: Russia es: Russia's Use of Cyber W s Use of Cyber Warfare in Est e in Estonia, Georgia and Ukraine, Annandale-on-Hudson, New York: 2019.

Malksoo, Lauri *The Talinn Manual as an international even*, Book Reviews Cyber Security No 120 August , 2013.

Melzer, Nils, *Cyber Warfare and International Law*, UNIDIR, 2011, 4.

Permanasari, Arlina,, *Pengantar Hukum Humaniter Internasional*, Jakarta: ICRC. 1999.

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

Arlina Permanasari, Arlina, "Relevansi Prinsip Pembedaan Dan Big Data Dalam Perang Siber Pada Era Revolusi Industri 4.0"**,** *Jurnal Hukum Pidana dan Pembangunan Hukum,* Vol 1, No 2 (2019)

Carson Marr, "Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus Ad Bellum and Jus in Bello," *SPICE: Student Perspectives on Institutions, Choices and Ethics* 14, no. 1 (2019): 2.

David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* 7, no. 1 (2011): 1–9.

Eric Patterson, "Just War Theory and Explosive Remnants of War Just War Theory and Explosive Remnants of War" Jounal of Conventional Weapon Destruction 13, no. 1 (2009): 1–3.

Herbert. Lin, "Cyber Conflict and International Humanitarian Law", *International Review of The Red Cross*, Volume 94, Number 886 Summer (2012): 515-531

Iradhati Zahra, Irawati Handayani, and Diajeng Wulan Christianti, "Cyber-Attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law," *Yustisia Jurnal Hukum* 10, no. 1 (2021): 48-68

Nur Khalimatus Sa'diyah and Ria Tri Vinata, "Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara," *Perspektif* 21, no. 3 (2016): 168-187.

Paulo Shakarian, "The 2008, The Russian Cyber- Campaign Againts Georgia", *Military Review* λ November-December (2011): 63-68.

Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution," *Minnesota Journal of International Law* 26, no. 2 (2017): 419–60.

Robert Kolb, "Military Objectives in International Humanitarian Law," *Leiden Journal of International Law* 28, no. 3 (2015): 691–700, .

Thomas Gregory, "Ethics and War: A Critical Intervention," *Millennium: Journal of International Studies*, (2018): 1-12.

Bagus Artiadi Soewardi, "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang Tangguh bagi Indonesia", majalah *Media Informasi Potensi Pertahanan*, Maret 2013

Danchev, Dancho, 2008, "***Coordinated Russia vs Georgia***", dikutip dari laman, i http://www.zdnet.com/blog /security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 diakses pada tanggal 11 Mei 2021

Ethan A. Wright, Of Drones and Justice: A Just War Theory Analysis of the United States' Drone Campaigns, dikutip dari laman di https:/ /digitalcommons.ursinus.edu/cgi/ viewcontent.cgi? article=1003&context=ethics_ essay

Hollis, David, ***Cyber War Case Study: Georgia 2008***, Small Wars Journal, dikutip dari laman: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 , diakses pada tanggal 18 Maret 2021

Ethics Explainer : Just War Teory, dikutip dari laman https://ethics.org.au/ethics-explainer-just-war/, diakses pada 10 Mei 2021

Tekhnologi Perang Cyber Dalam Konflik Militer dikutip dari laman https://www.dw.com/id/teknologi-perang-cyber-dalam-konflik-militer/a-15283271, diakses pada 11 Mei 2021.

Gil Gram and Kevin Lim , Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks, dikutip dari laman di https://foreignpolicy.com diakses pada tanggal 15 Maret 2021

Erich Freiberger, "Just War Theory and the Ethics of Drone Warfare", dikutip dari laman di https://www.e-ir.info/2013/07/18/just-war-theory-and-the-ethics-of-drone-warfare/

just war theory dikutip dari laman di https:// oregonstate.edu/instruct/phl201/modules/just_war_theory/criteria_intro.html, diakses pada tanggal 11 Mei 2021