eJournal Ilmu Hubungan Internasional, 2018, 6 (1) 109-122
ISSN 2477-2623 (online), ISSN 2477-2615 (print), ejournal.hi.fisip-unmul.ac.id

ANALISIS PELANGGARAN *CYBERATTACK* RUSIA KE WILAYAH CRIMEA BERDASARKAN HUKUM HUMANITER INTERNASIONAL

Pebri Christian [1]
Nim. 1302045185

Abstract

Cyberattack is a means of a new method of war which in international humanitarian law has not been officially regulated. The use of cyberattack has been used in the conflict of the Crimea Peninsula. The purpose of this research was to analyze the violation of Russian cyberattack to the territory of crimea under international humanitarian law. This research used qualitative research methods. In this research the authors used the concept of International Humanitarian Law and Epistimic Community (Tallinn Manual) concepts that are used to perform the analysis in this research. Data analysis technique used is qualitative content analysis. The result of this research is show that cyberattack conducted by Russia against Ukraine in Crimean conflict is a form of normative violation in International Humanitarian Law when viewed from the principle of distinction, dual use object, proportionality, indiscriminate attack and unnecessary suffering, but until now International Humanitarian Law has not Officially set the cyberattack problem.

Key word: *Cyberattack, International Humanitarian Law, Violation of Russia*

Pendahuluan

Pertumbuhan yang cepat dibidang komputer dan komunikasi membuat suatu ruang baru yang dinamakan *cyberspace* atau dunia maya (Tabansky 2011). *Cyberspace* merupakan sebuah domain baru yang terdiri dari elektro dan elektromagnetik yang digunakan untuk menyimpan, merubah dan memodifikasi informasi. Namun dalam penggunaannya *cyberspace* memiliki kerentanan sehingga dapat menyebabkan terjadinya *cyberattack. Cyberattack* merupakan suatu serangan yang menggunakan jaringan komputer dan *cyberspace* yang ditujukan terhadap individu dan kelompok bahkan negara juga bisa menjadi target serangan. Semenjak akhir tahun 1990an *cyberattack* menjadi perhatian seluruh negara menyusul banyaknya kejadian *cyberattack* yang ditujukan kepada negara, seperti pada kasus Estonia, Georgia, Iran dan *cyberattack* terbaru terjadi pada konflik antara Rusia dan Ukraina di Semenanjung Crimea.

[1]Mahasiswa Program S1 Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Mulawarman. Email: pechriss.pc@gmail.com

Semenanjung Crimea merupakan wilayah yang masuk dalam negara Ukraina dan revolusi Ukraina terjadi pada Februari 2014, ketika Presiden Ukraina Viktor Yanukovych yang pro terhadap Rusia menolak untuk menandatangani Perjanjian Asosiasi Politik dengan Uni Eropa. Penolakan ini berujung pada penggulingan Presiden Yanukovych secara paksa dan setelah itu digantikan oleh pemerintahan sementara (www.koran.tempo.co, diakses 15 Oktober 2015). Perbedaan orientasi politik dulu dan sekarang membuat terjadinya demonstrasi besar-besaran diwilayah Semenanjung Crimea yang mayoritasnya merupakan etnis Rusia. Mereka menuntut agar wilayah Crimea lepas dan kembali ke Rusia. Hal ini mendapat perlawanan dari aparat kemanan dan polisi serta masyarakat pro Uni Eropa. Konflik internal yang terjadi di Crimea dianggap akan membahayakan etnis Rusia yang tinggal diwilayah tersebut maka pemerintahan Rusia menempati dan menganeksasi Semenanjung Crimea serta campur tangan di Ukraina Timur. Sebelum campur tangan resmi pemerintahan Rusia, *cyberattack* telah dilakukan oleh *Fancy Bear* (*cyber espionage group Rusia*) dan militer Rusia pada bulan November 2013, dilanjutkan pada bulan Februari dan Maret serta yang terakhir pada bulan Mei 2014.

Selama ini jika terjadi konflik bersenjata antar negara maka Hukum Humaniter Internasional (HHI) menjadi acuannya namun dalam *cyberattack,* HHI belum mengaturnya sehingga NATO *Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE) sebuah organisasi internasional yang berada di Tallin, Estonia mengundang *International Group of Experts* untuk merumuskan peraturan mengenai *Cyberwar*. Hasil rumusan ini adalah *Tallinn Manual* yang bersifat tidak mengikat. Menurut *Tallin Manual* serangan dunia maya/*Cyber-Attack* yang telah dilakukan Rusia ke Crimea merupakan bentuk *"use of force".* Menurut *The Tallin Manual on international law Applicable to CyberWarfare Rule 11 "Use of Force is Acts that kill or injure persons or destroy or damage objects are unambiguosly uses of force".* Setelah adanya penggunaan *use of ofrce* yang memiliki skala dan dampak maka bisa dikatakan sebagai konflik bersenjata konvensional. (Tallin Manual rule 11).

Tulisan ini akan menjelaskan bagaimana pelanggaran *cyberattack* yang dilakukan oleh Rusia terhadap Ukraina berdasarkan Hukum Humaniter Internasional.

Kerangka Dasar Teori dan Konsep

Konsep Hukum Humaniter Internasional

Hukum Humaniter Internasional, sebagai salah satu bagian hukum internasional, merupakan salah satu alat dan cara yang dapat digunakan oleh setiap negara, termasuk oleh negara damai atau netral untuk ikut serta mengurangi penderitaan yang dialami oleh masyarakat akibat perang yang terjadi di berbagai negara. Dalam hal ini Hukum Humaniter Internasional merupakan suatu instrumen kebijakan dalam sekaligus pedoman teknis yang dapat digunakan oleh semua aktor internasional untuk mengatasi isu internasioanl berkaitan dengan kerugian korban perang.

Dalam hukum humaniter dikenal dua bentuk perang atau sengketa bersenjata, yaitu sengketa bersenjata yang bersifat internasional dan yang bersifat non-internasional. Pada perkembangannya, pengertian sengketa bersenjata internasional diperluas dalam Protokol I tahun 1977 yang juga memasukkan perlawanan terhadap dominasi

kolonial, perjuangan melawan pendudukan asing dan perlawanan terhadap rezim rasialis sebagai bentuk dari sengketa bersenjata intemasional. Hukum humaniter juga mengatur sengketa bersenjata yang bersifat non-internasional, yaitu sengketa bersenjata yang terjadi di dalam negara. Dalam situasi-situasi tertentu, sengketa bersenjata yang tadinya bersifat internal (non-internasional) berubah menjadi sengketa bersenjata yang bersifat Internasional. Hal yang terakhir ini disebut dengan Internasionalisasi internal konflik (Ambarwaty 2012).

Prof. Mochtar Kusumaatmadja membagi hukum perang sebagai berikut:

1. *Jus ad bellum* yaitu hukum tentang perang, mengatur tentang dalam hal bagaimana negara dibenarkan menggunakan kekerasan bersenjata.
2. *Jus in belo*, yaitu hukum yang berlaku dalam perang, yang dibagi lagi menjadi 2 (dua) yaitu:
   a. Hukum yang mengatur cara dilakukannya perang *(conduct of war).* Bagian ini
      biasanya disebut *The Hague Law.*
   b. Hukum yang mengatur perlindungan orang-orang yang menjadi korban perang. Ini lazimnya disebut *The Geneva Law.*

Prinsip-prinsip Hukum Humaniter Internasional : (Fadillah 2007)
Prinsip yang merupakan tiang utama Hukum Humaniter adalah prinsip pembedaan (*distinction principle*). Prinsip pembedaan adalah prinsip yang membedakan antara kelompok yang dapat ikut serta secara langsung dalam pertempuran (kombatan) disatu pihak dan kelompok yang tidak ikut serta dan harus dilindungi dalam pertempuran (penduduk sipil). Disamping prinsip pembedaan, Hukum Humaniter juga mengenal prinsip-prinsip lainnya, yaitu:

1. Prinsip kepentingan militer (*military necessity*)
   Berdasarkan prinsip ini maka pihak yang bersengketa dibenarkan menggunakan kekerasan untuk menundukkan lawan demi tercapainya tujuan dan keberhasilan perang. Dalam praktiknya, untuk menerapkan asas kepentingan militer dalam rangka penggunaan kekerasan terhadap pihak lawan, maka prinsip-prinsip berikut harus diperhatikan ketika sebuah serangan dilakukan.
2. Prinsip proporsionalitas (*proportionality principle)*
   Prinsip yang diterapkan untuk membatasi kerusakan yang disebabkan oleh operasi militer dengan mensyaratkan bahwa akibat dari sarana dan metode berperang yang digunakan harus proporsional dengan keuntungan militer yang diharapkan.
3. Prinsip pembatasan berdasarkan orang (*Limitation Ratione Personal*)
   Penduduk sipil dan orang sipil perorangan memperoleh perlindungan umum terhadap bahaya yang timbul dari operasi militer. Atas dasar ini maka pihak-pihak yang berperang harus membedakan antara kombatan dan penduduk sipil dimana penduduk sipil tidak boleh dijadikan sasaran serangan, tindakan ancaman atau serangan untuk menteror penduduk sipil dilarang, pihak-pihak yang bersengketa harus melakukan kehati-hatian yang mungkin untuk menyelamatkan penduduk sipil atau sekurang-kurangnya menimbulkan luka

atau kerugian tak sengaja sekecil mungkin, serangan dan tangkisan hanya boleh dilakukan oleh angkatan bersenjata.

4. Prinsip pembatasan berdasarkan tempat (*Limitation ratione locz*).
   Prinsip ini menyatakan bahwa serangan harus benar-benar dibatasi pada objek militer atau yang memberikan sumbangan bagi keuntungan militer secara efektif. Berdasarkan prinsip ini maka tempat-tempat yang tidak dipertahankan, tempat yang diperuntukkan bagi ilmu pengetahuan atau amal, monumen bersejarah, bangunan-bangunan seni yang merupakan warisan budaya dan spiritual; bangunan dan instalasi yang berbahaya terhadap penduduk sipil tidak boleh diserang, objek sipil tidak boleh dijaclikan sasaran tindakan balasan. Juga dilarang untuk merusak atau memindahkan objek yang sangat diperlukan bagi kelangsungan hidup penduduk; dan dilarang melakukan penjarahan.
5. Prinsip pembedaan berdasarkan keadaan (*Limitation ratione conditionis*).
   Asas ini melarang penggunaan alat dan cara berperang yang menyebabkan Iuka berlebihan atau penderitaan yang tidak perlu. Berdasarkan asas ini, serangan tidak boleh membabi buta, secara khianat, diduga menimbulkan kerugian terhadap orang sipil dan merugikan objek sipil, atau yang menimbulkan kelaparan bagi orang atau penduduk sipil. Atas dasar ini juga, maka lingkungan alam harus dilindungi.
6. Perikemanusiaan (*humanity*).
   Berdasarkan prinsip ini maka pihak yang bersengketa harus memperhatikan perikemanusiaan, di mana mereka dilarang untuk menggunakan kekerasan yang dapat menimbulkan luka yang berlebihan atau penderitaan yang tidak perlu. Oleh karena itu prinsip ini sering juga disebut dengan *"unnecessary suffering principle"*.
7. Prinsip Kesatriaan (*chivalry*).
   Prinsip ini mengandung arti bahwa di dalam perang kejujuran harus diutamakan. Penggunaan alat-alat yang tidak terhormat perbuatan curang dan cara-cara yang bersifat khianat dilarang.

Dalam penerapannya, prinsip-prinsip tersebut dilaksanakan secara seimbang, sebagaimana dikatakan oleh Kunz bahwa : "Hukum Perang, yang diakui dan diterapkan di dalam praktik, harus mengambil posisi yang benar antara prinsip-prinsip kemanusiaan dan ksatria di satu pihak, dan kepentingan militer di lain pihak.

Epistimic Community

Epistimic Community merupakan jaringan profesional dengan keahlian yang diakui dalam kebijakan pada permasalahan tertentu. Para profesional memiliki latar belakang yang berbeda dan terletak di negara yang berbeda, tetapi mereka berbagi sebuah norma yang memotivasi tindakan bersama mereka, dalam mengevaluasi pengetahuan dan kebijakan umum (www.britanica.org, diakses 15 November 2015). Salah satu *product epistimic community* adalah *tallin manual. Tallin manual* adalah Pedoman tentang Hukum Internasional yang berlaku untuk *CyberWarfare*. Ditulis oleh *International Group of Experts*, merupakan hasil dari upaya tiga tahun untuk mengkaji bagaimana norma-norma hukum internasional berlaku untuk bentuk

peperangan yang relatif baru. Konsep *Epistimic Community* pertama kali diperkenalkan oleh John Ruggie dan kemudian disempurnakan oleh Peter M. Haas. Para sarjana ini menfokuskan pada peran yang dimainkan oleh jaringan pelaku dan konsensus yang mereka pegang tentang penyebab dan efek pada kebijakan negara dan kerjasama antar negara. Salah satu *product epistimic community* adalah *tallin manual. Tallinn manual* memberi perhatian khusus pada *jus ad bellum*, hukum internasional yang memaksa negara sebagai instrumen kebijakan nasional mereka, dan *jus in bello*, hukum internasional yang mengatur perilaku konflik bersenjata (juga diberi label hukum perang, hukum konflik bersenjata, atau hukum humaniter internasional). *Tallinn Manual* bukan dokumen resmi, melainkan ekspresi dari pendapat ilmiah dari sekelompok ahli independen yang bertindak semata-mata dalam kapasitas pribadi mereka. Hal ini tidak dimaksudkan untuk mewakili pandangan atau posisi resmi NATO atau negara yang tersedia dalam pengamat proyek (www.ccdcoe.org, diakses pada 23 November 2016).

Metode Penelitian

Jenis penelitian yang digunakan adalah penelitian deskriftif analisis. Dimana penulis menggambarkan pelanggaran *cyberattack* yang dilakukan oleh Rusia terhadap Ukraina dalam perspektif hukum humaniter internasional. Jenis data yang digunakan dalam penelitian ini adalah data sekunder, yaitu data yang diperoleh dari penelaahan studi kepustakaan dan hasil browsing data melalui jaringan internet. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah telaah pustaka. Teknik analisis yang digunakan teknik analisis data kualitatif *content analysis* yaitu penulis menganalisis data sekunder yang kemudian menggunakan teori dan konsep untuk menjelaskan suatu fenomena atau kejadian yang sedang diteliti oleh penulis yaitu analisis pelanggaran *cyberattack* Rusia ke wilayah Ukraina berdasarkan hukum humaniter internasional.

Hasil Penelitian

Revolusi Ukraina

Revolusi Ukraina merupakan rangkaian peristiwa dari berbagai demonstrasi damai hingga menjadi revolusi besar di Ukraina. Pada masa pemerintahan Vladimir Putin tahun 2012, pemerintahan Ukraina yang dipimpin oleh Presiden Yanukovych lebih pro terhadap Rusia sehingga pada November 2013, Presiden Yanukovych menolak penandatanganan perjanjian politik dengan UE *(Uni Eropa Association Agreement)* yang telah dipersiapkan dari tahun 2008 dan lebih memilih untuk melakukan kerjasama dengan Rusia. (www.euromaidanpress.com diakses pada 12 Januari 2017) Saat suasana masih memanas antara pendemo dan pemerintah, Presiden Yanukoych pada tanggal 17 Desember 2013 melakukan penandatanganan "Ukraina-Rusia *Action Plan*" dimana Rusia berjanji untuk membeli utang Ukraina sebesar $ 15 miliyar dan memotong harga impor gas alam sebesar sepertiga. Hal ini semakin memperparah suasana gerakan *Euromaidan.* Melihat situasi semakin memanas maka partai oposisi mengambil langkah untuk bergabung dengan pendemo sehingga membentuk "*Maidan People Union*".

Pada 16 Januari 2014, pemerintah mengeluarkan draft "Anti Protes" yang selanjutnya disahkan menjadi undang-undang oleh Presiden Yanukovych, hal ini membuat gerakan *Euromaidan* bukan lagi sebagai aksi protes damai. Bentrokan kekerasan

secara besar-besaran terjadi antara pendemo dengan pasukan khusus huru-hara Berkut serta pasukan khusus Kementrian Dalam Negri dijalan Hrushevskoho. Presiden Yanukovych merasa bahwa krisis politik di Ukraina semakin besar maka ia mencabut undang-undang tersebut dan memberhentikan Perdana Mentri Azarov. Dinas Keamanan Ukraina (SBU) mengumumkan sebuah operasi anti teroris yang memberikan hak kepada kepolisian untuk menggunakan peluru tajam kepada pendemo. Presiden Yanukovych mengatakan bahwa tentara akan digunakan jika krisis ini masih berlangsung dan mengancam eksitensi negara. (Elias Kuhn, hal 2)

Aksi massa pertama terjadi di Semenanjung Crimea pada 21 Februari 2014, mereka menolak ancaman pemisahan Semenanjung Crimea dari wilayah Ukraina. Saat melakukan aksi, mereka diserang oleh kelompok pro Kremlin. Kelompok pro Kremlin mengadakan rapat umum di Sevastopol dan memutuskan bahwa Walikota Olekssi Chalyi dipilih sebagai Walikota Rakyat. Gedung-gedung vital Ukraina seperti gedung parlemen Crimea dan gedung kementrian direbut secara paksa oleh pasukan tak dikenal. Media Rusia menyatakan bahwa aksi ini dilakukan oleh pasukan pertahanan Crimea yang bertujuan untuk mengambil alih kontrol dari pemerintahan resmi Ukraina. Pada 28 Februari 2014, pasukan tak dikenal memblokir semua unit militer Ukraina yang berada di Semenanjung Crimea. Situasi yang tidak menentu di Semenajung Crimea membuat pemerintahan baru mengadakan rapat dengan Presiden Putin pada tanggal 1 Maret 2014. Isi dari rapat ini merupakan permintaan penggunaan angkatan bersenjata di Crimea oleh Putin kepada Dewan Rusia. Salah satu alasanya adalah pertimbangan ancaman terhadap kehidupan etnis Rusia disana.

Parlemen Crimea pada 6 Maret 2014 mengeluarkan resolusi untuk tidak menunggu referendum sampai akhir Mei namun melakukan referendum bergabung dengan Rusia dalam waktu 10 hari yang akan datang. Sebuah kampaye propaganda besar-besaran telah dimulai pada saat yang sama di Sevastopol dengan agenda untuk mendesak rakyat Crimea untuk memilih opsi yang pertama. Semua penerbangan dari Simferopol ke Ukraina dibatalkan pada 11 Maret 2014. Keputusan ini dibuat oleh pasukan pertahanan Crimea yang sebelumnya telah mengambil alih bandara tersebut sejak akhir Februari. Penerbangan dibatalkan untuk menghindari provokasi selama referendum. Menurut data resmi 83,1% rakyat Crimea telah melakukan pemilihan pada saat referendum yang pada akhirnya 96,77% pemilih memilih untuk bergabung dengan Rusia. Menurut pemimpin etnis Tartar hanya sedikit dari mereka yang bisa melakukan pemilihan pada referendum tersebut. Perjanjian itu ditandatangani oleh Presiden Rusia dan tiga perwakilan dari Crimea. Pada 21 Maret 2014, dua peristiwa menandai akhir dari proses pelaksanaan hukum penggabungan Crimea. Pertama, kesepakatan penggabungan Republik Crimea dengan Rusia yang telah disahkan oleh Dewan Rusia dan kemudian ditandatangani oleh Presiden Rusia. Selama kurun waktu keterlibatan Rusia secara resmi pada bulan Februari 2014 dan tidak resminya pada bulan November 2013. Hacker pro Rusia dan pasukan Rusia telah melakukan beberapa *cyberattack* terhadap Ukraina.

Cyberattack Rusia

Cyberattack dikategorikan sebagai strategi dan operasi militer (serangan konvensional/kinetik) jika dilihat dari manipulasi *software*, data, pengetahuan, membuat ketidakpastian dalam pola berpikir para komandan atau pemimpin politik

yang berlawanan dan memanipulasi opini publik untuk merusak legitimasi dan ototritas lawan baik didalam dan luar negri adalah tujuan militer yang layak. Untuk menilai efek non-kinetik kita harus melihat dampak dari tiga poin *cyberattack*: menciptakan kebingungan, membentuk opini, dan menyebabkan kerusakan data dan sistem. Dengan menggunakan poin-poin diatas kita bisa melihat apa yang terjadi pada konflik di Semenanjung Crimea.

Konflik antara Rusia dan Ukraina digambarkan sebagai perang *hybrid* yaitu campuran strategi konvensional dan operasi *cyber*. Aktor-aktor yang bertanggung jawab dalam konflik ini adalah *Fancy Bear* dan militer Rusia sendiri. Beberapa perusahaan *security* internasional yang bergerak dibidang keamanan *cyber* seperti *Crowdstrike, ThreatConnect* dan *Fireeye's* mengatakan bahwa grup hacker tersebut dibiayai oleh pemerintah Rusia, bekerjasama dengan *Russian Military Intelligence Agency* (GRU) karena selalu terlibat dalam hampir semua kepentingan Rusia. Dalam konflik Crimea terjadi beberapa kali *cyberattack* yang dilakukan Rusia dari bulan November 2013 sampai Mei 2014. (www.crowdstrike.com, diakses pada 24 Juli 2017)

Serangan pertama terjadi pada 28-30 November 2013, *Fancy Bear* melakukan *deface* dan *Distributed Denial of Service* (DDOS) yang ditujukan kepada TV Ukraina, Surat kabar, situs gerakan *Euromaidan*, papan studio. (Kenneth Geers, hal 76) Serangan kedua terjadi pada bulan Februari 2014 yang ditujukan kepada cabang kantor telekomunikasi Ukraina yaitu Urktelecom. Setelah menguasainya militer Rusia memutus semua jaringan telepon, internet dan radio serta menanamkan *software* untuk menyadap informasi penting dari pemerintahan Ukraina. Serangan ketiga terjadi pada 1 Maret 2014, dimana website utama pemerintahan Ukraina seperti www.kmu.go.ua dan *National Security and Defence Council of Ukraine* mati total karena serangan DDOS secara besar-besaran. Saat konflik melebar ke daerah Donbass, serangan tertuju kepada jaringan perbankan dan beberapa perusahaan besar seperti perusahaan kereta api dan *Kievstar mobile operator*. Serangan terakhir terjadi pada bulan Mei 2014, dimana akan terjadi pemilihan presiden Ukraina. 3 hari sebelum hari pemilihan pada tanggal 22 Mei 2014, komisi pemilihan umum (*Central Election commision/CEC*) mengalami serangan DDOS sehingga tidak berfungsi namun saat hal ini sudah diperbaiki oleh dinas keamanan Ukraina ternyata Rusia sudah menanamkan *software* untuk mensabotase hasil pemilu yang akan memenangkan kandidat pro Rusia dan kandidat nasionalis/pro barat akan kalah. Pada akhirnya hal ini bisa dideteksi dan dihapus oleh dinas keamanan Ukraina.

Kedudukan Tallinn Manual dan Hukum Humaniter Internasional

Pada tahun 2009 NATO CCD COE (NATO *Cooperative Cyber Defence of Centre Excellence*) yang bermarkas di Tallinn, Estonia mengundang *International Grup of Experts* untuk merumuskan sebuah hukum yang mengatur masalah *cyberwar*. Pemilihan grup ini dilakukan secara hati-hati yang terdiri dari *legal practioners, academics*, dan *technical experts* dimana mereka berfokus pada *Jus ad belum* dan *Jus in bello* dalam HHI yang pada akhirnya dipimpin oleh Prof. Michael Schmitt dari *United State Naval War Collage* sebagai direktur. Selain para ahli terdapat tiga organisasi dunia yang terlibat yaitu NATO *Allied Command Transformation, U.S Cyber Command* dan *International Committee of the Red Cross.* Hasil dari rumusan *International Groups of Experts* ini adalah *Tallinn Manual* yang merupakan dokumen

hukum tak resmi namun bisa menghubungkan antara HHI dan *cyberwar*. (Tallinn manual, hal 23)

Cyberattack Dalam Hukum Humaniter Internasional

1. Cyberspcae sebagai domain perang baru dan cyberattack sebagai perang internasional dan non-internasional

   Penerapan HH dalam suatu perang harus melihat dimana perang tersebut terjadi. Selama ini HHI mengenal tiga domain yaitu perang didarat yang diatur didalam Konvensi ke IV Den Haag. Perang dilaut diatur dalam Konvensi IX mengenai pengeboman oleh angkatan laut dan yang terakhir perang yang terjadi diudara. Dalam Pasal 2 ayat 4 Piagam PBB: melarang negara untuk menggunakan kekerasan terhadap integritas teritorial dan politik negara lain. Dalam pasal tersebut dijelaskan mengenai integritas sosial yang berkaitan dengan kedaulatan sebuah negara, demikian halnya dengan *cyber* jika ingin dikatakan sebagai domain baru maka harus memiliki kedaulatan suatu negara dalam *cyber*. Menurut Bodin, kedaulatan terdiri dari kedaulatan internal dan eksternal. Kedaulatan internal yaitu negara berhak mengatur segala kepentingan rakyatnya tanpa campur tangan negara lain sedangkan eksternal mengadakan hubungan dengan negara lain dan juga melindungi teritorialnya. (www.politicalsciencesnotes.com, diakses pada 12 Februari 2017) Dalam *Tallinn Manual Rule 1* dijelaskan bahwa kedaulatan menyataklan suatu negara dapat melakukan kontrol atas infrastruktur *cyber* dengan segala jenis kegiatan didalamnya. Selain infrastruktur *cyber* sebuah negara juga berhak atas aktivitas *cyber* diwilayah mereka. Berdasarkan penjelasan Bodin dan *Tallinn Manual Rule 1* maka bissa disumpulkan suatu negara yang sudah memiliki kemampuan dalam infrastruktur dan aktivitas *cyber* memiliki kedaulatan atas *cyberspace*. Syarat umum dalam Hukum Internasional sudah terpenuhi mengenai *cyberspace* sebagai domain baru.

   Dalam HHI dikenal dua macam konflik bersenjata yaitu konflik bersenjata internasional dan non-internasional. Kriteria konflik ini di atur dalam Pasal 2 Konvensi Jenewa 1949. Para ahli berpendapat jika sengketa bersenjata internasional memerlukan dua negara atau lebih termasuk kombatan, MNC dan NGO. Jika negara A melakukan *cyberattack* terhadap negara B dan menimbulkan kerusakan serta korban jiwa maka bisa dikatakan sebagai sengketa bersenjata internasional. Sengketa bersenjata non-internasional diatur dalam Pasal 3 Konvensi Jenewa 1949. Konflik ini melibatkan pemerintahan suatu negara dengan kelompok bersenjata non-pemerintah. *Cyberattack* biasanya dilakukan dengan menyerang sistema komputer milik pemerintah dan lain-lainnya. Sengketa jenis ini memerlukan struktur kepemimpinan dan bergerak secara sistematis dalam melakukan *cyberattack.*

2. Definisi Konflik Bersenjata Dalam Cyberattack

   Dalam Pasal 1 Protokol Tambahan 1949, mendefenisikan *attacks* sebagai tindakan kekerasan terhadap lawan. Berlaku didarat, laut dan udara yang mempengaruhi objek sipil. Definisi dari *cyberattack* adalah serangan yang dilakukan terhadap sistem komputer atau infrastruktur *cyber* lainnya sehingga menimbulkan kerusakan atau kerugian. Para ahli hukum internasional

merumuskan beberapa model analisis untuk menggambarkan serangan *cyberattack.*

a. *Instrument-based approach,* yang melihat kerusakan oleh jenis serangan baru yang sebelumnya hanya bisa dicapai dengan serangan kinetik.
b. *Effects-based approach* atau terkadang disebut sebagai *consequence-based approach,* yang menjadi dasar adalah bukan dari apakah kerusakan serangan yang dihasilkan oleh suatu serangan dapat diterima berdasarkan pengertian kerusakan tradisional, melainkan semua efek yang ditimbulkan oleh serangan tersebut bagi suatu negara.
c. S*trict liability approach,* dimana *cyberattack* terhadap infrastruktur vital secara otomatis dikategorikan sebagai serangan bersenjata karena konsekuansi parah yang ditimbulkan. (Richardson, hal 16)

Dari ketiga model analisis ini, *effects-based approach* merupakan model analisis terbaik dalam menggambarkan *cyberattack.* Berdasarkan analisis dan pendekatan ini maka *cyberattack* bisa dikatakan sebagai *armed attack* (serangan bersenjata) karena efek yang ditimbulkan atau gangguan yang mempengaruhi penduduk suatu negara.

3. Prinsip-prinsip Hukum Humaniter Internasional

a. Prinsip Pembedaan dalam *cyberattack*

Prinsip pembedaan (*distinction princple*) merupakan suatu prinsip yang membedakan penduduk dari suatu negara yang sedang berperang. Dalam Pasal 1 Protokol Tambahan I dinyatakan bahwa untuk menghormati dan melindungi warga sipil maka pihak yang berkonflik harus membedakan antara penduduk sipil, objek sipil, kombatan, militer dan objek militer.

1) Kombatan: kombatan adalah mereka yang berhak berpartisipasi dalam konflik bersenjata. Kombatan diatur dalam Pasal 4A ayat 2 Konvensi Jenewa III. Dalam konteks *cyberattack* pemegang komando harus memiliki kemampuan dalam menggunakan teknelogi *cyber* dan memahami hukum yang ada. Dalam *Tallinn Manual Rule 26* adanya pemimpin dan kelompok terorganisir, memakai lambang dan membawa senjata yang kasat mata. Memang dalam dunia *cyber* akan sangat sulit untuk dilihat apakan mereka akan melakukan *cyberattack* tetapi jika dipahami bahwa serangan mereka sama saja seperti serangan konvensional.
2) Warga sipil: semua orang yang tidak termasuk dalam kriteria Pasal 4A ayat 1,2,3 dan 6 Konvensi Jenewa III dan Pasal 43 Protokol. Dalam *cyberattack* mereka tidak boleh diserang sama saja seperti perang konvensional namun dalam *Tallinn Manual rule 29-Civilian* dikatakan bahwa mereka akan kehilangan perlindungan jika terlibat dalam suatu konflik bersenjata.
3) Objek sipil dan objek militer : objek sipil adalah objek yang digunakan oleh sipil sedangkan objek militer digunakan oleh pihak militer, diatur dalam Pasal 52 ayat 1 Protokol Tambahan I. Dalam konteks *cyberattack* tidak diperbolehkan untuk menyerang objek yang digunakan oleh pihak sipil.
4) *Dual use object*: *dual use object* merupakan penggunaan infrastruktur ganda oleh [pihak militer dan sipil. dalam *Tallinn Manual Rule 39* dijelaskan bahwa penggunaan ganda sipil dan militer tidak dapat

dihindarkan seperti jaringan komputer dan infrastruktur *cyber* lainnya. Objek ini boleh diserang tetapi harus memiliki keuntungan militer.

b. Indiscriminate Attack

Indiscriminate attack merupakan sebuah serangan secara membabibuta dan diatur dalam Pasal 51 ayat 4 Protokol Tambahan I. Dalam *Tallinn Manual Rule 49*: *indiscriminate attack*, dijelaskan bahwa serangan *cyber* tidak diarahkan ke penduduk atau objek sipil. Dalam *Tallinn Manual Rule 43* dijelaskan kembali jika pihak penyerang gagal untuk mengkontrol dampak serangan seperti penggunaan *malicious script* maka hal ini akan memicu terjadinya *indiscriminate attack.*

c. Prinsip Proporsionalitas

Prinsip proporsionalitas menyatakan bahwa kerusakan yang diderita oleh penduduk maupun objek sipil harus proporsional sifatnya. Diatur dalam Pasal 51 ayat 5b dan Pasal 57 ayat 2 Protokol Tambahan Konvensi Jenewa 1949. Prinsip proporsionalitas yang berkaitan dengan *cyberattack* diatur dalam *Tallinn Manual Rule 51-Proportionality:* sebuah *cyberattack* yang diharapkan menyebabkan kerugian terhadap kehidupan sipil, korban sipil, dan kerusakan objek sipil atau kombinasi keduanya yang berlebihan dalam kaitannya dengan keuntungan militer langsung dapat diatisipasi. Aturan tersebut menyatakan bahwa, adanya luka, kehancuran, dan hilangnya nyawa penduduk yang timbul secara insedental 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. Sedangkan, mengenai *indirect effect* terdapat penundaan atau perubahan, menurut *Commentary*, *collateral damage* harus dapat diperkirakan sebelumnya oleh pihak yang terkait, dengan melihat *planning*, *approving,* dan *executing* dalam melakukan serangan *cyber.*

d. Unescessary Suffering

Unescessary Suffering merupakan prinsip yang menjelaskan bahwa dalam konflik bersenjata tidak diperlukan penderitaan yang berlebihan akibat penggunaan senjata. Diatur dalam Pasal 35 ayat 2 Protokol Tambahan I. Penderitaan yang tidak diperlukan juga harus diterapkan dalam konteks *cyberattack* karena sama saja efeknya seperti serangan konvensional. Contohnya *cyberattack* terhadap peralatan medis maka pengobatan tidak bisa dilakukan terhadap kombatan dan warga sipil sehingga mendapat efek yang sangat besar. Selanjutnya *unnecessary suffering* yang tercantum didalam *Tallin Manual Rule 42* mengenai *superfluous injury or unnecessary suffering* menyatakan bahwa dilarang untuk menggunakan senjata, proyektil, materi dan metode peperangan yang dapat menyebabkan luka berlebihan atau penderitaan yang tidak perlu. Peraturan ini hampir serupa dengan Protokol Tambahan I namun yang ada didalam *Tallin Manual* lebih menfokuskan kepada *weapons as means or methods of cyber warfare.*

Pelanggaran Rusia Dalam Cyberattack Ke Crimea

1. Prinsip pembedaan

   Prinsip pembedaan diatur dalam Pasal 48 Protokol Tambahan I yang isinya menjelaskan dalam konflik bersenjata harus ada pembedaan antara penduduk sipil, objek sipil, militer dan objek militer. Dalam *Tallinn Manual Rule 30, Rule 31: Distinction, Rule 32: prohibition on Attacking Civilians, Rule 37: Prohibition on Attacking Civilian objects and Rule 38: Civilian Objects and Military Objectives.* Semua peraturan ini mengacu pada Pasal 48 Protokol Tambahan I sehingga sama seperti perang konvensional, bahwa tidak diperbolehkan menyerang penduduk sipil dan objek sipil. *Cyberattack* yang dilakukan oleh *Fancy Bear* pada 28-30 November 2013 yang ditujukan kepada saluran TV, surat kabar, situs resmi gerakan *Euromaidan* dengan cara melakukan *deface* sehingga terjadi pergantian gambar dan serangan DDOS yang membuatnya tidak dapat diakses. Beberapa bulan kemudian saat Ukraina menyelenggarakan pemilihan umum preside, *Fancy Bear* sekali lagi melakukan serangan untuk menyabotase pemilihan tersebut dengan cara melakukan serangan DDOS sehingga website tersebut mati dan tidak bisa melakukan penghitungan suara kemudia mereka menanamkan *software x* untuk mengkatrol hasil pemilu yang akan memenangkan kandidat pro Rusia. namun usaha ini tidak berhasil karena digagalkan oleh dinas kemanan Ukraina.

   Jika dilihat dari semua *cyberattack* yang dilancarkan oleh *Fancy Bear* maka semuanya diarahkan ke penduduk sipil dan objek sipil bahkan serangan yang terjadi pada bulan Mei 2014 berusaha untuk menyabotas hasil pemilu. Hal ini sudah sangat tidak berhubungan dengan objek militer yang sah hukumnya untuk diserang. Maka dengan itu prinsip pembedaan telah dilanggar.

2. Dual Use Object

   Dual use object merupakan penggunaan ganda infrastruktur oleh pihak sipil dan militer yang tidak dapat dihindari dalam kehidupan sehari-hari. Contohnya penggunaan sistem komputer, satelit dan instalasi listrik dan air. Dalam *Tallinn Manual Rule 39: Objects Used for Civilian and Military Purposes.* Dijelaskan bahwa dalam zaman sekarang ini yang semuanya terkoneksi dengan teknologi *cyber* maka sangat sering ditemukan penggunaan ganda infrastruktur *cyber*. Jika mengacu pada prinsip proporsionalitas yang dijelaskan dalam pasal 51 dan 57 Protokol Tambahan Konvensi Jenewa 1949 maka objek tersebut diperbolehkan untuk diserang namun harus dilihat apakah keuntungan militer yang didapat besar. Pada 28 Februari 2014, tentara Rusia (*Spetnaz Special Force* dan *Russian Military Intelligence*) masuk kewilayah Crimea dan langsung menuju kantor cabang telekomunikasi Urktelecom. Mereka menguasai tempat tersebut dan melakukan pemotongan kabel optik, jaringan internet, telepon, dan radio. Crimea mengalami kelumpuhan total dalam hal komunikasi.

Selanjutnya pada 11 Maret 2014 serangan langsung ditujukan kepada simbol pemerintahan Ukraina yang berupa website utama pemerintahan, www.kmu.go.ua dan beberapa website lainya seperti *National Security and Defense Council of Ukraine* mati total dan tidak dapat diakses. Jika dilihat dari *Domain Name System* (DNS), website-website tersebut dibuat atas nama pemerintah bukan militer. Selanjutnya apabila tetap diputuskan menjadi objek militer maka harus memuat informasi militer, strategi maupun informasi penting lainnya sehingga jika dibandingkan dengan strategi konvensional yang terkenal seperti *compellence operation* yang menyerang gedung pemerintahan secara langsung akan memberikan keuntungan militer yang sama. Namun kenyataannya dengan matinya website-website tersebut penduduk tidak bisa mengetahui perkembangan konflik yang sedang berlangsung dan website tersebut tidak menampilkan mengenai militer sedikitpun. Jika dilihat dari penggunaan ganda maka *cyberattack* yang dilakukan Rusia dengan cara mengisolasi Crimea dengan memutus jaringan komunikasi dan *cyberattack* terhadap website pemerintahan tidak memberikan keuntungan militer yang besar sehingga hanya merugikan penduduk sipil saja. Hal ini tentu saja melanggar prinsip *dual use object.*

3. Indiscriminate Attack

   Indiscriminate attack merupakan serangan yang membabibuta dan diatur dalam Pasal 51 ayat 4 Protokol Tambahan I yaitu targer serangan harus fokus dan dampaknya tidak meluas. Dalam *Tallinn Manual Rule 49: Indiscriminate Attack* dijelaskan bahwa penggunaan seperti *malicious script* atau *worm* efeknya akan bisa meluas karen dari sifat alat tersebut yang tidak bisa dikontrol. Penanaman *malicious software* dikantor Urketelecom yang bertujuan untuk menyadap data-data penting dari lingkungan pemerintahan dan militer Ukraina pada akhirnya tidak sesuai dengan tujuan awal karena dampaknya yang meluas hingga penduduk sipil. peralatan elektronik penduduk sipil seperti laptop dan hp tidak bisa digunakan akibat *software* ini. Data-data penting seperti akun bank atau data pribadi tersebar kemana-mana sehingga menimbulkan kerugian yang sangat besar. Dengan tidak bisa dikontrolnya dampak dari serangan Rusia ini maka prinsip *indiscriminate attack* telah dilanggar.

4. Prinsip proporsionalitas

   Prinsip proporsionalitas menjelaskan bahwa penderitaan yang dirasakan oleh penduduk sipil dan objek sipil harus proporsional sifatnya. Tercantum dalam Pasal 51 ayat 5b dan Pasal 57 ayat 2 Protokol Konvensi Jenewa 1949. Dalam *Tallinn Manual Rule 51* menjelaskan *cyberattack* yang bisa menyebabkan kerusakan insidental dari hilangnya nyawa penduduk sipil, kerusakan objek sipil atau kombinasi keduanya dilarang. *Collateral damage* atau kerusakan tambahan juga tidak diperbolehkan dari serangan yang ditujukan terhadap objek militer. Pada konflik Crimea dengan menyerang kantor Urktelecom sehingga menyebabkan hilangnya komunikasi menimbulkan *collateral damage* yang dirasakan oleh penduduk sipil disana. Penduduk sipil tentu saja sangat membutuhkan jaringan komunikasi untuk saling berhubungan satu sama lainnya, mengetahui perkembangan konflik dan daerah mana saja yang harus dijauhi. Dengan tidak adanya jaringan komunikasi maka penduduk rentan menjadi korban. Rusaknya jaringan perbankan dan lumpuhnya perusahaan besar akan

menambah penderitaan penduduk. *Cyberattack* yang ditujukan kepada Crimea tidak bersifat proporsional serta menimbulkan *collateral damage* sehingga hal ini melanggar prinsip proporsionalitas.

5. Unescessary Suffering
   Unescessary Suffering merupakan prinsip yang menjelaskan bahwa dalam suatu konflik bersenjata jika terjadi serangan maka serangan tersebut tidak perlu menghasilkan penderitaan yang tidak diperlukan. Prinsip ini tercantum dalam Pasal 35 ayat 2 Protokol Tambahan I. Dalam *Tallinn Manual Rule 42* dijelaskan bahwa metode *cyberattack* tidak diperbolehkan untuk menimbulkan penderitaan yang tidak diperlukan. Pada konflik Crimea, *cyberattack* yang dilakukan Rusia dengam cara menutup jaringan internet, telepon, radio dan infrastruktur *cyber* lainnya akan menyebabkan infrastruktur lain yang bergantung terhadap hal diatas akan tidak berfungsi juga. Contohnya pabrik-pabrik obat-obatan dan kimia yang menggunkan peralatan canggih tidak bisa bekerja karena memerlukan sistem komputer. Transportasi publik yang menggunakan infrastruktur *cyber* seperti bus yang ruang lingkupnya sampai dengan 96 km^2 tidak dapat beroperasi. Hal-hal ini tentu saja memberikan penderitaan yang tidak diperlukan sehingga telah melanggar prinsip *unescessary suffering.*

Kesimpulan

Dari analisis yang telah dilakukan maka *cyberattack* oleh Rusia terhadap Ukraina di Semenanjung Crimea dilihat dari Hukum Humaniter Internasional secara normatif dikatakan sebagai pelanggaran karena melihat dari:

1. Prinsip pembedaan yang mengharuskan dalam konflik bersenjata terdapat pembedaan penduduk sipil, objek sipil dan militer. Dalam *cyberattack* di Crimea tidak terjadi pembedaan bahkan target serangan kebanyakan merupakan objek sipil bukan militer.
2. *Dual use object,* dimana penggunaan ganda oleh pihak militer dan sipil pada akhirnya bisa diserang namun harus melihat besarnya kepentingan militer yang didapat. Serangan pada bulan November 2013 dan Maret 2014 sama sekali tidak memiliki kepentingan militer dan hanya menyerang penduduk sipil serta objek sipil yang pada akhirnya merugikan penduduk saja.
3. *Indiscriminate attack* melarang adanya serangan membabibuta tetapi yang terjadi pasca penanaman *malicious software* untuk mneyadap informasi penting dari pemerintahan, efeknya meluas dan akhirnya merugikan penduduk sipil yang tidak ada hubungannya dengan pemerintah.
4. Prinsip Proporsionalitas mngeharuskan serangan bersifat proporsional dan tidak berlebihan namun kenyataannya pada konflik Crimea, *cyberattack* oleh Rusia menyebabkan kerusakan yang tidak proporsional ditambah lagi dengan adanya *collateral damage* (kerusakan tambahan)
5. *Unnescessary Suffering* menjelaskan dalam konflik bersenjata tidak perlu penderitaan berlebihan namun nyatanya dengan rusaknya infrastruktur *cyber* yang berkaitan dengan infrastruktur lainnya membuat penderitaan tidak diperlukan timbul karena penduduk tidak bisa melakukan aktivitas mereka.

Dengan adanya pelanggaran *cyberattack* secara normatif terhadap Hukum Humaniter Internasional sayangnya hingga saat ini HHI belum mengatur secara tegas mengenai persoalan *cyberattack.*

Daftar Pustaka

Buku

Agus, Fadillah. *Pengantar Hukum Internasional dan Hukum Humaniter Internasional*, Jakarta : Cetakan Pertama 2007, hal 50

Ambarwati, Denny Ramadhany, Rina Rusman. *Hukum Humaniter Internasional dalam Studi Hubungan Internasional*, (Jakarta : Rajawali Pers 2010) Hal 27

Kenneth Geers, *Cyber War In Perspective : Russian Aggression Against Ukraine*, Nato: 2015, Hal 77

Richardson J, *Stuxnet As Cyberwarfare: Distinction and Proportionality On The Cyber Battlefield*, National Academic of Science: 2011, hal 16

Schmitt, Michael. *Tallinn Manual On The International Law Applicable To Cyber warfare.* New York : Cambridge University Press. 2013.

Jurnal

Cordula Droege, "International Review of the Red Cross: *Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*", vol 94 no 886, Summer 2012

Elias Kuhn, "Inquiries Journal: *The Euromaidan Revolution in Ukraine: Stages of the Maidan Movement and Why They Constitute a Revolution*",vol 7, no 02, 2015. Hal 2

Tabansky, Lior, 2011. *Basic Concepts In Cyber Warfare*, vol 3, no 1, Hal 75

Internet

CrowdStrike Company, https://www.crowdstrike.com/executive-team/

Sovereignty: Introduction Classification and Theories, dalam http://www.politicalsciencenotes.com/sovereignty/sovereignty-introduction-classification-and-theories/777

Epistimic Community, dalam https://www.britannica.com/topic/epistemic-community

Presiden Dilengserkan, Ukraina Bentuk Pemerintahan Sementara, dalam http://koran.tempo.co/konten/2014/02/24/335645/Presiden-Dilengserkan-Ukraina-Bentuk-Pemerintahan-Sementara

Tallin Manual, dalam https://ccdcoe.org/research.html