

# ANALISIS YURIDIS PENYELESAIAN SENGKETA *CYBERATTACK* PADA KONFLIK RUSIA DAN UKRAINA DALAM HUKUM HUMANITER INTERNASIONAL

**Achmad Sya'roni**

(S1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya)  
[achmadsyaroni@mhs.unesa.ac.id](mailto:achmadsyaroni@mhs.unesa.ac.id)

**Arinto Nugroho**

(S1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya)  
[arintonugroho@unesa.ac.id](mailto:arintonugroho@unesa.ac.id)

**Elisabeth Septin Puspoayu**

(S1 Ilmu Hukum, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya)  
[elisabethseptinpuspoayu@unesa.ac.id](mailto:elisabethseptinpuspoayu@unesa.ac.id)

## Abstrak

Peristiwa *cyberattack* yang dilakukan oleh kelompok peretas yang berasal dari Rusia di wilayah Ukraina merupakan salah satu bentuk serangan yang memiliki keterkaitan dengan konflik bersenjata internasional antara Rusia dan Ukraina. Dalam beberapa rangkaian peristiwa *cyberattack* terlihat bahwa *cyberattack* menyebabkan kerugian materiil terhadap penduduk sipil yang tidak ikut dalam konflik bersenjata dan melanggar hukum humaniter internasional sebagaimana dalam Pasal 4 ayat (1) Protokol Tambahan II Konvensi Jenewa tentang perlindungan bagi penduduk sipil. Tujuan penelitian ini ialah menganalisis penerapan hukum humaniter internasional dan bentuk penyelesaian sengketa *cyberattack* pada konflik Rusia dan Ukraina menurut hukum internasional. Penelitian ini merupakan penelitian hukum normatif dengan menggunakan pendekatan perundang-undangan dan konseptual. Bahan hukum yang digunakan yaitu bahan hukum primer dan sekunder. Teknik analisis menggunakan metode preskriptif memberikan argumentasi berupa kesimpulan dan saran. Hasil penelitian dan pembahasan menjelaskan bahwa bentuk pengaturan *cyberattack* dalam hukum internasional menggunakan konvensi internasional yaitu protokol tambahan II konvensi jenewa, yurisprudensi yaitu putusan ICJ dalam kasus *Martin Clause*, hukum kebiasaan internasional yaitu Resolusi Majelis Umum PBB Nomor 53/70 dan doktrin yang terkait adalah *International Humanitarian Law and the Challenges of contemporary armed conflicts* yang dikeluarkan oleh ICRC. Bentuk penyelesaian sengketa yang dilakukan adalah penyelesaian melalui organisasi internasional yakni PBB dan melalui pengadilan internasional yakni *International Criminal Court (ICC)*. ICC memiliki kelebihan dibandingkan pilihan penyelesaian sengketa lain karena ICC memiliki statuta yang independen dan sifat pengadilan yang permanen. ICC juga memiliki putusan yang sifatnya mengikat serta sanksi kurungan dan denda.

**Kata Kunci:** *cyberattack*, hukum humaniter internasional, konflik Rusia dan Ukraina.

## Abstract

Cyberattack incident carried out by a group of hackers who came from Russia in the territory of Ukraine is one form of attack that have relevance to the international armed conflict between Russia and Ukraina. In a series of cyberattack incident, it appears that cyberattack causes material losses to civilians who do not participate in armed conflict. International humanitarian law regulates the protection of civilians or civilians who obtain Article 4 paragraph (1) Additional Protocol II of the Geneva Convention. There is a legal vacuum in terms of cyberattack conducted by actors in a state against another state. The purpose of this research are (1) to analyze the forms of cyberattack regulation in international law and (2) to analyze the forms of dispute resolution in the cyberattack conflicts between Russia and Ukraine according to international law. This research is a normative legal research by using statute and conceptual approaches. The Legal material in this research are primary and secondary legal materials. The uses prescriptive method to analyze the case. The results of the research explain that The form of cyberattack regulation in international law is in the form of international conventions related to cyberattack such as additional protocol II Geneva conventions, jurisprudence related to ICJ decisions in the case of martin clause, related international custom law is UN General Assembly Resolution 53/70 and related doctrines is the International Humanitarian Law Challenging of contemporary armed conflicts issued by the ICRC. The form of dispute resolution that can be applied is settlement through international organizations namely the United Nations and through an international tribunal namely the International Criminal Court (ICC). The ICC has advantages over other dispute resolutions option because the ICC has an independent statute and a permanent court. The ICC also have binding decisions like a body sanctions and fines. In the future it is

necessary to establish international legal instruments that specifically regulate the types of cyberattack crimes and the remove of veto rights in the UN Charter.

**Key Words:** Cyberattack, Internasional Humanitarian Law, Russian and Ukraina Conflict.

## PENDAHULUAN

Perkembangan hubungan internasional pada saat ini tidak hanya membawa kerjasama dan hidup damai berdampingan namun juga berpotensi menimbulkan sengketa antar negara. Sengketa antar negara atau biasa disebut sengketa internasional dapat disebabkan oleh beberapa alasan yakni alasan politik, strategi militer, budaya, ekonomi, sumber daya alam serta ideologi yang dianut dari negara tersebut (Adolf : 2004). Penggunaan istilah perang dalam hukum internasional telah digantikan dengan istilah pertikaian bersenjata atau konflik bersenjata seperti yang tercantum dalam beberapa instrumen hukum internasional. Dalam hukum humaniter internasional, dikenal dua macam bentuk konflik bersenjata yakni konflik bersenjata internasional (*international armed conflict*) dan konflik bersenjata non internasional (*non international armed conflict*) (Adwani : 2012).

Konflik bersenjata internasional salah satunya dapat dilihat dalam konflik antara Rusia dan Ukraina. Konflik antara Rusia dengan Ukraina disebabkan oleh tindakan Rusia yang melakukan intervensi militer ke dalam wilayah Crimea pada masa konflik dalam negeri di Ukraina berlangsung. Selama masa konflik dalam negeri dan intervensi militer Rusia terhadap beberapa wilayah di Ukraina terjadi beberapa kali *cyberattack* yang dilakukan oleh kelompok peretas yang berasal dari Rusia. Serangan tersebut dimulai pada November 2013 yakni ketika kelompok peretas Rusia melakukan perusakan dan serangan *Distributed Denial of Service* (DDOS) terhadap beberapa website seperti stasiun televisi Ukraina, perusahaan surat kabar dan website pemerintahan (Geers : 2016). Selanjutnya pada Februari 2014, perusahaan komunikasi Ukraina yaitu Ukrtelecom melaporkan adanya *Denial of Service* (DOS) dan *Distributed Denial of Service* (DDOS) yang mengganggu arus informasi dan meretas telepon selular pejabat pemerintahan Ukraina. Pada Maret 2014, pemerintahan Ukraina melaporkan serangan yang menyebabkan website penting pemerintahan Ukraina mati selama beberapa hari. Serangan tersebut berlanjut pada Mei 2014 yaitu ketika komisi pemilihan umum Ukraina atau *Central Election commission* (CEC) mengalami serangan *Distributed Denial of Service* (DDOS) yang menyebabkan putusnya jaringan internet dan mematikan sistem tampilan perhitungan suara.

Pada Desember 2015, terjadi *cyberattack* terhadap sistem jaringan perusahaan listrik daerah di Ukraina. Enam perusahaan distribusi listrik daerah mengalami pemadaman listrik namun hanya tiga perusahaan yakni Kyivoblenergo, Prykarpattyaoblenergo dan Chernivtsioblenergo yang melaporkan pemadaman listrik hingga menyebabkan 225.000 penduduk kehilangan daya listrik (E-ISAC : 2016). Laporan dari setiap perusahaan juga menunjukkan bahwa adanya serangan yang disebabkan oleh *malware* BlackEnergy meskipun belum diketahui peranan *malware* Blackenergy dari serangan tersebut (Gordon : 2015). BlackEnergy merupakan virus yang pertama kali dikembangkan di Rusia dan merupakan *malware* yang sama yang digunakan dalam serangan spionase kelompok peretas dari Rusia dan muncul dugaan adanya campur tangan pemerintah Rusia dalam serangan tersebut (Hackingnews : 2016).

Munculnya *cyberattack* sebagai bentuk serangan terhadap negara merupakan dimensi baru dalam perkembangan hukum humaniter internasional. *Cyberattack* dapat didefinisikan sebagai upaya untuk masuk, merusak dan menghancurkan jaringan sistem komputer. Pada umumnya, bentuk *malware* dalam *cyberattack* seperti *virus*, *worm* atau *trojan* dapat digunakan untuk menyusup masuk pada server sebuah web atau masuk pada jaringan sistem komputer suatu infrastruktur. *Cyberattack* juga digunakan beberapa negara untuk melakukan serangan dan mengganggu keamanan dan stabilitas nasional dari negara sasaran. Obyek serangan *cyberattack* yang menyerang infrastruktur dari sektor penting sebuah negara dapat menimbulkan kekacauan di negara tersebut.

Salah satu teori model pendekatan yang dikemukakan oleh Jean Pictet, yakni *effects based approach* atau *consequence based approach* menjelaskan penderitaan dalam pengertian secara tradisional tidak hanya dilihat dari kerusakan yang timbul tapi juga dilihat dari efek yang ditimbulkan dari serangan tersebut. Berdasarkan hal tersebut maka kekacauan yang disebabkan oleh *cyberattack* dapat menimbulkan penderitaan terhadap penduduk sipil negara tersebut. Hukum humaniter mengatur tentang perlindungan bagi penduduk sipil atau civilians yang dapat dalam Pasal 4 ayat (1) Protokol Tambahan II Konvensi Jenewa yakni sebagai berikut :

*"All persons who do not take a direct part or who have ceased to take part in hostilities, whether or not their liberty has been restricted, are entitled to*

*respect for their person, honour and convictions and religious practices. They shall in all circumstances be treated humanely, without any adverse distinction. It is prohibited to order that there shall be no survivors."*

Perlindungan terhadap penduduk sipil dalam konflik bersenjata berkaitan dengan prinsip pembedaan dalam hukum humaniter internasional. Prinsip pembedaan diatur dalam Pasal 48 Protokol Tambahan I tahun 1977 yang menjelaskan bahwa :

*"In order to ensure respect and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times differentiate between civilians and combatants and between civilian objects and military targets and hence shall directing their operations to military objectives only."*

Melihat akibat dari penggunaan *cyberattack* dalam konflik bersenjata yang sangat besar maka diperlukan pengaturan khusus tentang *cyberattack* dalam hukum humaniter internasional. Selama ini hukum humaniter internasional belum mengatur secara spesifik tentang *cyberattack* sehingga muncul dokumen tidak mengikat yakni *Tallin Manual Law Applicable to Cyber Warfare 1*. Perumusan dokumen Tallin Manual diprakarsai oleh *North Atlantic Trade Organization Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE) yang mengundang *International Group of Experts* untuk merumuskan peraturan mengenai *cyberwar*. Persoalannya yakni status dokumen Tallinn Manual bukan dokumen resmi, melainkan ekspresi pendapat ilmiah dari sekelompok ahli independen seperti dijelaskan dalam bagian *Introduction* dalam Tallin Manual yaitu :

*"Like its predecessors, the Manual on the international Law Applicable to Cyber Warfare, or Tallin Manual, result from an expert driven process designed to produce a non binding document applying existing law to cyber warfare"*

Pengaturan mengenai *cyberattack* diperlukan sebagai kejelasan dan batasan terhadap tindakan yang menyebabkan kerugian baik secara fisik maupun materiil terhadap negara maupun subyek hukum internasional lainnya.

Tujuan penelitian yaitu menganalisis dan merumuskan penerapan hukum humaniter internasional dan bentuk penyelesaian sengketa *cyberattack* pada konflik Rusia dan Ukraina menurut hukum internasional. Kajian teoritik yang digunakan yaitu mengenai hukum internasional, konflik bersenjata, hukum humaniter internasional, penyelesaian sengketa internasional dan *cyberattack*.

Penelitian ini menggunakan teori penggunaan senjata terbaru dan teori penyelesaian sengketa konflik bersenjata internasional. Dalam Balck's law Dictionary

dinyatakan bahwa perang adalah permusuhan (pertikaian) dengan menggunakan angkatan bersenjata yang terjadi di antara bangsa-bangsa, negara-negara, atau penguasa-penguasa, atau warga-warga dalam satu bangsa atau satu negara. Dalam teori penggunaan senjata terbaru dijelaskan mengenai larangan terhadap penggunaan senjata atau metode terbaru tertentu yang menyebabkan penderitaan melampaui batas keadaan/situasi yang dihadapi. Penggunaan senjata harus memenuhi dua aspek hukum sebelum dapat secara sah digunakan di medan perang, yakni senjata harus mencegah penderitaan yang tidak perlu, dan mampu membedakan target secara efektif.

*Jus ad bellum* menegaskan bahwa hak untuk menggunakan kekerasan adalah terbatas, tidak semua negara mempunyai hak untuk menggunakan kekerasan dan tidak pada setiap kesempatan kekerasan tersebut bisa digunakan karena jika demikian maka anarki akan muncul dalam kehidupan masyarakat internasional karena tidak akan ada perdamaian dan ketertiban yang dapat dipertahankan. Setelah hubungan permusuhan dimulai, atau keadaan perang telah diumumkan melalui suatu deklarasi perang, maka kemudian muncul kebutuhan untuk mengatur hubungan permusuhan yang timbul sebagai akibat dari penggunaan kekuatan bersenjata. Hal ini diperlukan untuk memberikan aturan mengenai cara dan metode peperangan agar terhindar dari kehancuran yang berlebihan serta dalam rangka meminimalisir penderitaan korban.

Teori mengenai sengketa internasional mencakup sengketa antar negara dan negara, negara dan individu, negara dan perusahaan asing serta sengketa antar negara dan kesatuan kenegaraan yang bukan negara. Sengketa-sengketa internasional secara teoritis pada pokoknya selalu dapat diselesaikan oleh pengadilan internasional, sesulit apapun sengketa sekalipun tidak ada pengaturannya suatu pengadilan internasional tampaknya bisa memutuskan dengan prinsip kepatutan dan kelayakan (*ex aequo et bono*).

Penjelasan *cyberattack* menurut kamus ilmiah Oxford Dictionary, *cyberattack* dijelaskan sebagai "*an attempt by hackers to damage or destroy a computer network or system*" dapat diterjemahkan yakni "suatu percobaan dari peretas komputer untuk merusak atau menghancurkan sebuah jaringan atau sistem komputer". Dalam *cyberattack* terdapat beberapa pelaku yang telah diketahui melakukan *cyberattack* berdasarkan identifikasi yang dilakukan baik oleh korban *cyberattack* maupun perusahaan keamanan *cyber* swasta. Tindakan siber yang seperti *scamming*, peretasan, dan serangan penolakan layanan, merupakan kegiatan yang dianggap illegal oleh undang-undang nasional di berbagai negara dan juga perjanjian internasional. Selain tindakan tersebut, tindak kejahatan di dunia maya lainnya diantaranya pencurian

identitas, pelecehan, pemerasan, pornografi anak, dan perdagangan manusia.

## **METODE**

Metode yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif yakni penelitian hukum yang dilakukan dengan cara meneliti bahan kepustakaan sebagai bahan dasar untuk diteliti dan dengan cara mengadakan penelusuran peraturan perundang-undangan dan literatur yang berkaitan terhadap permasalahan yang diteliti. (Soekanto dan Mamudji : 2001). Pendekatan-pendekatan yang digunakan di dalam penelitian ini adalah pendekatan undang-undang (*statue approach*), dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan di gunakan untuk menelaah dan menganalisis semua peraturan perundang-undangan yang erhubungan dengan masalah yang diteliti. Pendekatan konsep brawal dari pandangan-pandangan dan doktrin yang berkembang dalam ilmu hukum. Penelitian ini menggunakan bahan hukum primer dan sekunder. Bahan hukum primer yakni terdiri atas instrumen-instrumen internasional yang masih berlaku, diakui dan ditaati oleh masyarakat internasional (Fajar dan Achmad : 2010). Bahan hukum sekunder yang digunakan adalah bahan hukum yang terdiri atas buku-buku teks hukum yang berkaitan dengan hukum internasional, hukum humaniter internasional, konflik bersenjata internasional, hukum penyelesaian sengketa dan mengenai *cyberattack*, jurnal-jurnal hukum terkait, pendapat para sarjana, kasus-kasus hukum, dan hasil-hasil penelitian yang berkaitan dengan topik penelitian.

Pengumpulan bahan hukum yang digunakan dalam penelitian ini adalah studi kepustakaan yaitu dengan cara membaca dan melakukan penelusuran untuk mencari bahan-bahan hukum yang relevan terhadap problematika hukum yang dihadapi. menggunakan langkah-langkah antara lain mengumpulkan bahan hukum primer, sekunder berdasarkan topik yang dibahas, yaitu dengan cara mengidentifikasi peraturan-peraturan, konvensi-konvensi, yang ada relevansinya dengan topik penelitian, dari buku-buku hukum yang mendukung konsep yang sesuai topik penelitian. Teknik pengolahan bahan hukum yaitu diolah secara sistematis, yakni dengan cara melakukan seleksi bahan hukum yang ada, melakukan klasifikasi bahan hukum sesuai dengan problematika, dan menyusun secara sistematis.

Teknik pengolahan bahan hukum yaitu diolah secara sistematis, yakni dengan cara mereduksi bahan kepustakaan dengan tujuan memilih informasi dan bahan hukum yang telah didapatkan dalam segala segi apapun yang sesuai dan tidak sesuai dengan masalah penelitian yang akan diteliti (Soekanto, 2009). Tahap yang akan

dilakukan oleh peneliti selanjutnya adalah penyajian dilakukan setelah pemilihan atau penyaringan informasi telah selesai dikerjakan dan sudah terbentuk dalam hasil baik berbentuk tabel maupun uraian penjelasan. Tahap terakhir yang akan peneliti lakukan adalah melakukan analisis terhadap informasi dan bahan hukum yang pada akhirnya akan dapat ditarik kesimpulan hasil penelitian dan peneliti pada akhir dari laporan penelitian akan memberikan saran mengenai permasalahan yang telah diteliti oleh peneliti.

Teknik analisis bahan hukum yang dilakukan penulis yaitu dengan cara mengidentifikasi fakta hukum dan mengeliminasi hal-hal yang tidak relevan, melakukan telaah atas problematika hukum yang diajukan berdasarkan bahan-bahan hukum yang telah dikumpulkan, menarik kesimpulan dalam bentuk argumentasi untuk menjawab probelmatika hukum Metode yang digunakan adalah metode prespriksi yang bertujuan untuk memberikan gambaran atau merumuskan masalah sesuai dengan keadaan/fakta yang ada (Ibrahim, 2009).

## **HASIL DAN PEMBAHASAN**

### **Pengaturan *Cyberattack* menurut Hukum Humaniter Internasional**

Konflik antara Rusia dan Ukraina dalam prespektif hukum humaniter internasional merupakan salah satu konflik bersenjata internasional yang didasari atas faktor ekonomi, politik dan ideologi. Pelanggaran hukum humaniter internasional yang terjadi melalui serangan bersenjata terlihat pada saat krisis dalam negeri di Ukraina terjadi yakni khususnya pada saat pasukan militer Rusia memasuki wilayah Crimea yang masih merupakan wilayah kedaulatan Ukraina. Alasan utama kependudukan militer Rusia menurut Vladimir Putin adalah sebagai wujud perlindungan dari kerusakan yang tidak terkendali terhadap warga dan etnis Rusia sebagai etnis mayoritas di Crimea (Kompas : 2015).

Dimensi konflik tersebut tidak hanya dilakukan melalui serangan bersenjata namun juga dilakukan dengan serangan *cyberattack* terhadap jaringan komputer di Ukraina. Pada saat kependudukan wilayah Crimea oleh militer Rusia dilaporkan bahwa terjadi beberapa kali kerusakan akibat *cyberattack* terhadap website surat kabar di Ukraina khususnya surat kabar pergerakan Euromadian. Selanjutnya kelompok peretas yang terindikasi berpihak kepada Rusia yakni "*CyberBerkut*" melakukan upaya *cyberattack* terhadap server dari Komisi Pemilihan Umum Ukraina dengan menanamkan *malware* (EFF : 2016). Upaya tersebut berhasil mengubah grafik perhitungan perolehan suara sementara yang berusaha memenangkan calon presiden pro terhadap Rusia meskipun pada akhirnya *Ukrainian Cyber*

*Emergency* berhasil merespon secara cepat dengan menghilangkan virus yang dikendalikan dengan jarak jauh.

Upaya serangan *cyberattack* paling terlihat dan terbesar dampaknya adalah serangan *cyberattack* terhadap perusahaan jaringan distribusi listrik regional yang menimbulkan 225.000 konsumen kehilangan daya listrik dalam waktu 6 jam (IETF : 2016). Serangan tersebut dilakukan dengan metode *spearphising* yakni dengan mengirimkan lampiran Microsoft Office yang berisi *malware* melalui email dan ketika pegawai perusahaan membuka lampiran tersebut maka secara otomatis *malware* BlackEnergy telah aktif dan dapat mengendalikan penuh komputer tersebut. Menurut analisis dari perusahaan keamanan siber di Amerika Serikat menjelaskan bahwa pelaku telah menyusup masuk dan bertahan selama 6 bulan didalam sistem jaringan komputer perusahaan sebelum penyerangan dilakukan. Dalam waktu tersebut, pelaku melakukan pengintaian dan mengumpulkan informasi yang diperlukan untuk melakukan serangan.

Kerugian yang diderita oleh penduduk sipil dalam konflik tersebut baik akibat dari serangan secara kinetik maupun serangan *cyberattack* sejatinya tidak dapat dibenarkan menurut hukum humaniter internasional. Hukum humaniter sebagai seperangkat pembatasan yang diatur oleh hukum internasional, didalamnya diatur bahwa penggunaan kekerasan dapat digunakan untuk menundukan pihak musuh dengan prinsip-prinsip yang mengatur perlakuan terhadap individu dalam konflik bersenjata. Sebagai upaya untuk memanusiasikan perang tersebut, dalam hukum humaniter internasional terdapat 2 (dua) prinsip fundamental yakni *jus ad bellum* dan *jus in bello*.

*Cyberattack* merupakan dimensi baru dalam konflik bersenjata internasional maupun konflik bersenjata non internasional. Definisi *cyberattack* sendiri memiliki perbedaan dengan konflik bersenjata secara kinetik. Menurut Pasal 49 Protokol Tambahan I makna dari “*attack*” atau serangan diartikan sebagai “*acts of violence against the adversary, whether in offence or in defence*”. Sampai saat ini penerapan hukum humaniter internasional terhadap *cyberattack* masih menjadi perdebatan dari beberapa negara.

Seperti yang diketahui, hukum humaniter internasional (IHL) adalah aturan-aturan yang harus diikuti militer ketika berpartisipasi dalam perang. Sebagai hukum perang ini menggambarkan tindakan apa yang penduduk sipil. Hukum Humaniter Internasional telah melarang penggunaan banyak senjata, yang mencakup peluru bekas, senjata kimia dan biologi, senjata laser yang menyilaukan dan ranjau anti-personil. Hal ini secara

umum dapat terlihat dalam Pasal 36 Protokol Tambahan I Konvensi Jenewa tahun 1977 yakni :

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

Berdasarkan penjelasan pasal tersebut jika dikaitkan dengan *cyberattack* maka dapat dipahami bahwa penggunaan *cybeattack* sebagai senjata terbaru harus tunduk dalam ketentuan hukum internasional yang berlaku khususnya dalam Protokol Tambahan tersebut. Pasal selanjutnya dalam Protokol Tambahan I tersebut juga menambahkan ketentuan umum terhadap beberapa senjata yang dilarang, seperti dalam Pasal 51 ayat (4) Protokol Tambahan I yang menjelaskan sebagai berikut :

*“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;”*

Dalam pendapat yang disampaikan oleh Jeffrey Thumher menjelaskan bahwa penggunaan senjata harus memenuhi dua aspek hukum sebelum dapat secara sah digunakan di medan perang, yakni senjata harus mencegah penderitaan yang tidak perlu, dan mampu membedakan target secara efektif. Hal tersebut didasarkan pada Pasal 35 Protokol Tambahan Konvensi Jenewa 1977 yang menjelaskan bahwa :

- 1) In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.*
- 2) It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.*
- 3) It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.”*

Penerapan hukum konflik bersejната atau hukum humaniter internasional dalam kasus atau dimensi diluar ketentuan dalam hukum humaniter internasional sejatinya telah disebutkan dalam Putusan ICJ pada kasus *Martin Clause* yang menyatakan “ketiadaan aturan khusus tidak menghalangi penerapan aturan hukum internasional umum tertentu yang didasarkan pada prinsip kemanusiaan”. Lebih lengkap dalam Protokol Tambahan I Konvensi Jenewa dijelaskan bahwa :

*“In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the*

*principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.”*

Pendapat lain mengenai pengaturan terhadap metode dan sarana yang baru dalam hukum humaniter internasional juga ditemukan dalam *Advisory Opinion International Court of Justice (ICJ)* dalam kasus legalitas penggunaan senjata nuklir yang menyatakan bahwa :

*“these provisions do not refer to specific weapons. They apply to any use of force, regardless the weapons employed. The charter neither expressly prohibits, nor permits, the use of any weapons, including nuclear weapons”*

Berdasarkan penjelasan diatas dapat ditarik kesimpulan bahwa hukum humaniter internasional memberikan perluasan pemberlakuan hukum untuk demi menjaga stabilitas keamanan internasional serta tujuan kemanusiaan yang lebih luas. Pendapat lain juga dikeluarkan oleh ICRC melalui *International Humanitarian Law and the Challenges of contemporary armed conflicts* yang sangat tegas memberikan penjelasan bahwa :

*“in the ICRC’s view, means and methods of warfare which resort to cyber technology are subject to IHL (international humanitarian law) just as any new weapon or delivery system has been so far when used in an armed conflict by or on behalf of a party to such conflict, If a cyber operations is used against an enemy in an armed conflict in order to cause damage, for example by manipulation of an air traffic control system that results in the crash of a civilian aircraft, it can hardly be disputed that such an attack is in fact a method of warfare and is subject to prohibitions under IHL”*

PBB juga menilai bahwa *cyberattack* merupakan sebuah dampak dari perkembangan teknologi informasi dan komunikasi sehingga perlu untuk memberikan perhatian penting dalam menjaga penyalahgunaan teknologi tersebut. Melalui Resolusi Majelis Umum PBB Nomor 53/70 menegaskan bahwa

*“Advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality”*

Dapat dipahami dari beberapa sumber-sumber hukum internasional diatas dijelaskan bahwa dalam ranah konflik bersenjata internasional, dijelaskan bahwa operasi siber yang dilakukan secara langsung oleh dua atau lebih negara dapat diberlakukan suatu hukum konflik bersenjata.

### **Penyelesaian Sengketa *Cyberattack* dalam Konflik Rusia dan Ukraina**

Peristiwa *cyberattack* yang terjadi di Ukraina merupakan salah satu bentuk serangan yang memiliki keterkaitan terhadap konflik teritorial didalam Ukraina pasca terjadinya kudeta terhadap Presiden Ukraina saat itu yakni Victor Yanukovich. Konflik tersebut juga memunculkan gerakan separatisme yang bertujuan untuk memisahkan diri dari Ukraina dan bergabung dengan Rusia dengan alasan menolak pemerintahan hasil kudeta di Kiev. Gerakan separatisme yang dilakukan juga telah memberikan dorongan kepada beberapa kelompok peretas jaringan komputer atau yang biasa disebut kelompok *hacker* yang pro Rusia untuk melakukan *cyberattack* terhadap jaringan komputer di Ukraina.

Kelompok *hacker* yang menyerang masuk negara yang sedang berkonflik sulit dikualifikasikan sebagai kombatan dalam kualifikasi sebagai kombatan menurut hukum humaniter internasional. Kelompok *hacker* tersebut dijelaskan tidak memiliki keterkaitan dengan negara tempat kelompok tersebut berada sehingga kelompok tersebut dapat disebut sebagai *non-state actor* menurut kualifikasi hukum internasional. Konsep *non-state actors* dijelaskan yakni kesatuan orang yang berada dalam wilayah negara namun bukan perwakilan dari negara tersebut dan memiliki kepentingan dalam hukum internasional. Ketidakjelasan kualifikasi *non-state actor* sebagai kombatan atau penduduk sipil disebabkan dua faktor utama yakni faktor wilayah tempat *non-state actor* tersebut berada dan faktor tidak terpenuhinya syarat-syarat sebagai kombatan.

Pada perkembangannya, untuk menentukan kualifikasi status seseorang dalam konflik tidak hanya dilihat dari pemenuhan kriteria yang telah diatur namun dapat juga dilihat dari keterlibatannya dalam konflik bersenjata. Hal tersebut berdasarkan pandangan bahwa penduduk sipil yang bukan merupakan anggota angkatan bersenjata dapat terlibat aktif dalam konflik bersenjata dan berpotensi menimbulkan kerugian bagi pihak yang berkonflik. Dari pandangan tersebut dengan mengikuti perkembangan konflik bersenjata maka hukum humaniter internasional mengembangkan konsep *“direct participation hostilities”* atau partisipasi langsung dalam pertempuran.

Konsep dari *direct participation hostilities (DPH)* sejatinya dapat ditemukan dalam Protokol Tambahan I Konvensi Jenewa 1977 yakni pada Pasal 51 (3) yang menjelaskan bahwa *“civilian shall enjoy protection afforded by this section, unless and for such time as they take a direct part in hostilities”*, Hubungan antara pelaku *cyberattack* dan *direct participation hostilities (DPH)* dapat ditemukan secara khusus dalam *The HPCR Manual An International Law Applicable To Air And Missile Warfare* yang menjelaskan status dari *direct participation hostilities (DPH)* juga adalah orang yang terikat terhadap

perang secara elektronik (*cyber warfare*) baik melalui jaringan komputer maupun pengendalian jarak jauh pesawat tanpa awak yang menargetkan objek militer kombatan maupun penduduk sipil yang berpartisipasi secara langsung.

Berdasarkan pengertian diatas dapat diketahui bahwa pelaku yang mengoperasikan atau yang melakukan *cyberattack* dapat dianggap sebagai *direct participation hostilities* (DPH) atau pihak yang terlibat dalam pertempuran. Ditemukannya pelanggaran hukum humaniter internasional dalam peristiwa *cyberattack* pada konflik Rusia dan Ukraina hingga saat ini belum ditindak lanjuti dengan upaya penyelesaian sengketa kasus tersebut. Secara teoritis, pelaku *cyberattack* maupun hukum yang dapat diterapkan telah dapat ditemukan dan diidentifikasi dengan mengkaitkan terhadap konsep maupun ketentuan dalam hukum internasional. Beberapa pilihan metode penyelesaian sengketa telah tersedia dalam konteks hukum internasional namun dalam dimensi *cyberattack* perlu untuk mengidentifikasi lebih lanjut mengenai jenis penyelesaian sengketa yang tepat. Beberapa jenis penyelesaian sengketa yang dapat dijadikan sebagai pilihan adalah melalui organisasi internasional dan pengadilan internasional.

Melalui organisasi internasional, upaya pertama yang dapat ditempuh adalah melalui PBB sebagai organisasi internasional yang bersifat universal. Yurisdiksi universal PBB dapat dilihat dalam Pasal 1 Ayat (1) Piagam PBB menyatakan:

“Memelihara perdamaian dan keamanan internasional sesuai dengan prinsip-prinsip keadilan hukum internasional mengatur atau menyelesaikan sengketa-sengketa internasional yang dapat mengganggu perdamaian dan keamanan dengan cara-cara damai.”

Sebagai organisasi universal yang diberikan tugas untuk menjaga perdamaian dan keamanan internasional maka dibentuk pula Dewan Keamanan PBB. Selanjutnya dalam Pasal 33 Ayat (1) Piagam PBB diatur terkait upaya-upaya Dewan Keamanan dalam menyarankan para pihak untuk menggunakan cara-cara yang antara lain: a. Dewan Keamanan menyarankan penyelesaian secara damai; b. Dewan Keamanan menyarankan penyelesaian melalui mediasi; c. Pengusulan penyelesaian melalui jasa-jasa baik; d. Dewan Keamanan mengusulkan pencarian fakta atau penyelidikan; e. Dewan keamanan menyarankan penyelesaian sengketa melalui Mahkamah Internasional; f. Dewan Keamanan membentuk Pasukan Perdamaian PBB; g. Dewan Keamanan mengusulkan upaya atau prosedur damai; h. Dewan keamanan menjatuhkan sanksi.

PBB sendiri telah memberikan perhatian khusus dalam menangani sengketa *cyberattack* yang ditegaskan

dalam Resolusi Majelis Umum PBB Nomor 55/63 bahwa “*ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*” yang dapat diterjemahkan yakni Dari penegasan tersebut terlihat bahwa PBB memiliki semangat untuk melakukan penegakan hukum terhadap pelaku *cyberattack*. Wujud penegakan hukum yang dilakukan PBB adalah dengan menjadi koordinasi dan memberikan arahan langkah terhadap komunitas internasional.

Dihubungkan dengan kasus sengketa *cyberattack* pada konflik Rusia dan Ukraina terlihat peran dari PBB sebagai organisasi internasional akan sangat berpengaruh. Salah satu prinsip dalam Pasal 2 ayat (3) Piagam PBB menekankan bahwa:

“*All members shall settle their international disputes by peaceful means in such manner that international peace and security, and justice, are not endangered*”.

Jenis penyelesaian sengketa yang dilakukan oleh PBB adalah melalui Dewan Keamanan PBB dengan cara melakukan penyelidikan dan membentuk tim pencari fakta untuk melakukan penyelidikan. Cara tersebut dilakukan mengingat objek sengketa adalah konflik *cyberattack* yang memberikan kerugian terhadap penduduk sipil. Berbeda halnya jika objek sengketanya adalah sengketa tentang batas wilayah maka hanya dilakukan upaya negosiasi dan mediasi bagi para pihak.

Ukraina sebagai negara yang menjadi korban *cyberattack* dapat mengajukan proposal atau draft resolusi kepada Dewan Keamanan PBB sesuai dengan prosedur pengajuan perkara di Dewan Keamanan PBB dilihat dari *United Nation Security Council Provisional Rules of Procedure*. Proposal dan draft resolusi tersebut setelah mendapat persetujuan dari Sekretariat Dewan Keamanan dapat dibawa ke agenda sidang Dewan Keamanan PBB. Hasil dari sidang tersebut melahirkan resolusi Dewan Keamanan PBB yang sifatnya mengikat berdasarkan pasal 25 PBB yang menyatakan “*The Members of the United Nations agree to accept carry out the decisions of the Security Council in accordance with present Charter*”. Pelanggaran atas resolusi Dewan Keamanan tersebut dapat menimbulkan sanksi terhadap para pihak yang bersengketa. Sesuai dengan Pasal 41 Piagam PBB menjelaskan bahwa :

“*The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other*

*means of communication, and the severance of diplomatic relations”*

Kelemahan dari jenis prosedur penyelesaian sengketa melalui Dewan Keamanan PBB adalah mengenai hak veto yang dimiliki oleh anggota tetap Dewan Keamanan PBB. Kesulitan dalam membawa kasus *cyberattack* yang terjadi antara Rusia dan Ukraina juga akan muncul karena salah satu pelaku yang dihubungkan dalam tindakan *cyberattack* adalah Rusia yang merupakan anggota tetap dewan keamanan. Tercatat dalam sejarah sidang Dewan Keamanan PBB, Rusia telah 12 kali menggunakan hak veto terhadap pengambilan suara dalam sidang resolusi Dewan Keamanan PBB. Dalam ketentuannya, jika salah satu anggota tetap Dewan Keamanan PBB mengeluarkan veto maka membuat suatu resolusi tersebut tidak dapat diberlakukan dan tidak mempunyai kekuatan mengikat secara hukum.

Solusi mengatasi kebuntuan akibat tidak dapat dicapai tercapai kata sepakat dalam Dewan Keamanan PBB perihal keamanan dan perdamaian melalui Majelis Umum yang mempunyai wewenang untuk segera membahas masalah tersebut agar dapat memberikan rekomendasi kepada para anggota berdasarkan Resolusi Majelis Umum PBB nomor 377 (A) “*Uniting for Peace Resolution*” tanggal 13 November 1950. Hal ini didasarkan dikarenakan Majelis Umum memiliki tanggungjawab pula terkait dengan masalah ancaman atau pelanggaran perdamaian dunia yang disebut *residual responsibility*.

Penyelesaian penggunaan *cyberattack* juga dapat di ajukan ke *International Criminal Court* (ICC) yang merupakan badan peradilan berdasarkan statuta roma yang permanen, berdasarkan perjanjian, dan bertujuan untuk mengakhiri impunitas pelaku kejahatan yang sangat serius yang menjadi perhatian komunitas internasional. Pengadilan ICC pada Pasal 4 statuta ICC dijelaskan bahwa ICC memiliki *legal personality* dan *legal capacity* untuk menegakkan dan menjalankan tugas dan tujuannya di teritori negara peratifikasi, atau dengan persetujuan khusus dilakukan di teritorial negara lain juga dapat mengambil alih kewenangan pengadilan nasional. Statuta ICC memberikan yurisdiksi untuk ICC terbatas untuk kejahatan yang sangat serius yang menjadi perhatian seluruh komunitas internasional, seperti genosida, kejahatan kemanusiaan, kejahatan perang dan agresi, dan orang yang melakukan kejahatan didalam yurisdiksi pengadilan harus secara individu bertanggungjawab dan mampu untuk dihukum berdasarkan statuta ini. Dihubungkan dengan kasus *cyberattak* yang terjadi pada konflik Rusia dan Ukraina, kemungkinan persoalan yang dapat dibawa ke yurisdiksi ICC adalah pelanggaran kejahatan pelanggaran agresi dan perang (*war crime*). Resolusi Majelis Umum PBB

nomor 3314 tahun 1974 memberikan definisi agresi adalah :

*“the definition uses the movement of armies, the blockade by navies and the sending of armed groups as examples of aggressive acts. Allowing an attack by a state to originate from its sovereign territory is also considered an act of aggression”*

Dikaitkan dengan dimensi *cyberattack* maka dapat dilihat bahwa *cyberattack* telah masuk dalam kualifikasi the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, atau perencanaan, persiapan, inisiasi atau eksekusi, oleh seseorang dalam posisi yang efektif untuk melakukan kontrol atau mengarahkan tindakan politik atau militer suatu Negara. Fakta yang terlihat dijelaskan bahwa *cyberattack* yang dilakukan merupakan suatu keseluruhan proses dari perencanaan, persiapan, inisiasi dan eksekusi untuk melakukan kontrol terhadap suatu negara. Makna kejahatan agresi dalam pasal tersebut menjadikan agresi tidak hanya suatu pengiriman atau pengarahan suatu angkatan bersenjata ke dalam wilayah musuh namun juga usaha untuk mengambil alih kontrol terhadap suatu negara melalui media jarak jauh.

Kasus *cyberattack* juga dapat dituduh sebagai kejahatan perang(*war crimes*) yang merupakan salah satu yurisdiksi dari ICC. Dijelaskan dalam Statuta Roma mengenai definisi Kejahatan Perang adalah “*Grave breaches of the Geneva Conventions of 12 August 1949,*” dan “*Violations of the laws or customs of war*”. Pengadilan Militer Internasional di Nuremberg mendefinisikan kejahatan perang sebagai “pelanggaran terhadap hukum atau kebiasaan hukum”, termasuk pembunuhan, perlakuan buruk, atau deportasi penduduk sipil dalam wilayah yang telah diduduki, pembunuhan atau perlakuan buruk terhadap tahanan perang, pembunuhan sandera, perampasan barang-barang publik atau harta milik pribadi; perusakan tanpa alasan atas kota-kota; dan penghancuran tanpa kepentingan militer.

Berdasarkan ketentuan dari kejahatan perang tersebut maka sejatinya *cyberattack* dapat dibawa dalam proses persidangan di ICC karena telah memenuhi unsur dari kejahatan perang tersebut. Unsur konstektual yakni konflik bersenjata selain konflik bersenjata secara kinteik dalam konflik Rusia dan Ukraina terlihat dalam pembahasan sebelumnya bahwa *cyberattack* dapat dikatakan sebagai konflik bersenjata berdasarkan efek dan skala yang ditimbulkan. Salah satu kendala dalam penyelesaian sengketa melalui ICC adalah dalam Statuta memberikan kewenangan pada Dewan Keamanan untuk meminta ICC menunda pelaksanaan yurisdiksinya. Hal ini dapat disimpulkan dari apa yang ditetapkan oleh Pasal 16 Statuta Roma :

“...No investigation or prosecution may be commenced or proceeded with under this Statute for a period of 12 months after the Security Council, in a resolution adopted under Chapter VII of the Charter of the United Nations, has requested the Court to that effect; that request may be renewed by the Council under the same conditions.”

Pada perkembangannya, tanggal 16 November 2016 Rusia juga telah menyatakan menarik diri dari Mahkamah Pidana Internasional. Rusia secara tegas mengatakan alasan penarikan diri dari ICC karena mahkamah tersebut tidak memenuhi harapan yang dicanangkannya, diragukan independensinya serta ketidakefektifan dengan biaya yang telah dianggarkan. Perlu untuk diketahui bahwa keanggotaan ICC adalah berdasar dengan ratifikasi Statuta Roma oleh suatu negara yang bersifat sukarela.

Pernyataan keluarnya Rusia dari ICC tidak serta menjadikan ICC kehilangan yurisdiksinya jika pada suatu waktu Rusia telah melakukan kejahatan perang, kejahatan kemanusiaan, kejahatan agresi dan genosida. Berdasarkan Statuta Roma 1998 ICC memiliki yurisdiksi terhadap warga negara yang berasal dari non state parties dalam kondisi-kondisi sebagai berikut : a. dalam kasus yang diserahkan oleh Dewan Keamanan PBB kepada ICC; b. dalam kasus warga negara dari non state parties melakukan kejahatan di wilayah atau teritorial negara anggota Statuta Roma atau Negara yang sudah menerima yurisdiksi ICC berkaitan dengan kejahatan tersebut; c. dalam kasus negara non state parties sudah menyetujui untuk melaksanakan yurisdiksi berkaitan dengan kejahatan-kejahatan tertentu.

Poin mengenai kasus yang diserahkan oleh PBB tersebut dapat dilihat dalam Pasal 13 huruf b Statuta Roma yang menjelaskan bahwa mahkamah dapat melaksanakan yurisdiksinya berkenaan dengan kejahatan yang “suatu situasi dimana satu atau lebih kejahatan yang tampak telah dilakukan tersebut diteruskan kepada penuntut umum oleh Dewan Keamanan yang bertindak berdasarkan Bab VII Piagam PBB”. Selanjutnya dalam poin mengenai kasus warga negara dari non state parties melakukan kejahatan di wilayah atau teritorial negara anggota Statuta Roma atau negara yang sudah menerima yurisdiksi ICC dapat dilihat dalam Pasal 12 ayat (2) huruf b Statuta Roma yang menjelaskan bahwa ICC dapat melaksanakan yurisdiksinya terhadap negara peserta yang wilayahnya menjadi tempat dilakukannya kejahatan internasional. Pasal 12 ayat (3) juga menjelaskan bahwa “negara bukan anggota ICC dapat menyerahkan kasusnya dan menerima pelaksanaan yurisdiksi mahkamah dengan deklarasi yang disampaikan kepada panitera”.

## PENUTUP

### Simpulan

Hukum internasional dapat diterapkan dalam kasus *cyberattack* karena menurut yurisprudensi ICJ dalam kasus *Martin Clause* menjelaskan bahwa ketiadaan aturan khusus dalam *cyberattack* tidak menghalangi penerapan aturan hukum internasional umum tertentu yang didasarkan pada prinsip kemanusiaan. Bentuk pengaturan umum dalam hukum internasional yang dapat diterapkan dalam kasus *cyberattack* pada konflik Rusia dan Ukraina adalah berbentuk konvensi Internasional yakni Protokol Tambahan II Konvensi Jenewa. Adapun hukum kebiasaan internasional yang dapat diterapkan adalah Resolusi Majelis Umum PBB Nomor 53/70 yang menegaskan hukum internasional dan bagian dari Piagam PBB tersebut berlaku untuk memelihara perdamaian dan stabilitas dalam dimensi siber. Selanjutnya doktrin yang dapat diterapkan adalah *International Humanitarian Law and the Challenges of contemporary armed conflicts* yang dikeluarkan oleh ICRC.

Penyelesaian sengketa *cyberattack* pada konflik Rusia dan Ukraina dapat dilakukan dengan dua jenis penyelesaian yakni melalui organisasi internasional dan melalui pengadilan internasional. Bentuk penyelesaian sengketa melalui organisasi internasional yakni PBB. Dalam hal ini Ukraina sebagai pihak yang menjadi korban serangan dapat mengajukan peristiwa yang terjadi ke dalam sidang Dewan Keamanan PBB sebagai badan yang bertugas secara khusus dalam menjaga perdamaian dan keamanan internasional. Kelebihan dari jenis penyelesaian sengketa melalui PBB adalah sifatnya sebagai organisasi universal yang diberikan tugas untuk menjaga perdamaian dan keamanan internasional dan Pelanggaran atas resolusi Dewan Keamanan PBB dapat menimbulkan sanksi terhadap para pihak yang bersengketa. Sementara kelemahan dari jenis pilihan penyelesaian sengketa ini adalah Hak veto yang dimiliki oleh anggota tetap Dewan Keamanan PBB dapat menghambat proses penyelesaian sengketa. Bentuk penyelesaian sengketa melalui pengadilan internasional adalah melalui *International Criminal Court (ICC)* atau Mahkamah Pidana Internasional yang memiliki yurisdiksi menangani perkara *cyberattack* berdasarkan yurisdiksi temporal, yurisdiksi teritorial, yurisdiksi personal dan yurisdiksi kriminal. ICC memiliki kelebihan jenis penyelesaian sengketa melalui ICC adalah adanya statuta yang berdiri sendiri (independen), sifat pengadilan yang permanen dan memiliki putusan yang bersifat mengikat berupa sanksi kurungan badan dan denda. Sementara kelemahan dari jenis pilihan penyelesaian sengketa ini adalah ICC hanya memiliki yurisdiksi terhadap warga negara yang berasal dari state parties.

### Saran

Pihak-pihak yang bersengketa khususnya Rusia dan Ukraina agar melakukan kerjasama bilateral seperti penyelidikan bersama dan penyerahan pelaku *cyberattack* dalam konflik *cyberattack*. Adapun secara khusus, Ukraina agar meratifikasi Statuta Roma guna memberikan kewenangan terhadap ICC melakukan yurisdiksinya dalam konflik *cyberattack* antara Rusia dan Ukraina.

PBB dan masyarakat Internasional secara luas mengenai diperlukannya pembentukan instrumen hukum internasional yang secara khusus mengatur mengenai jenis kejahatan *cyberattack* yang turut menjadi salah satu sarana dan metode dalam berperang pada zaman modern ini. Instrumen hukum internasional yang mengatur secara khusus mengenai *cyberattack* dapat berupa konvensi internasional maupun resolusi organisasi internasional seperti PBB sebagai bentuk perlindungan terhadap penduduk sipil yang tidak terlibat langsung dalam konflik bersenjata. Perubahan terhadap Piagam PBB juga diperlukan dalam hal penghapusan terkait hak veto agar tugas dan fungsi PBB dapat dilaksanakan secara optimal tanpa terganjal intervensi kepentingan negara anggota tetap Dewan Keamanan PBB dalam suatu permasalahan.

#### DAFTAR PUSTAKA

- Adolf, Huala. 2004. *Hukum Penyelesaian Sengketa Internasional*. Bandung: Sinar Grafika.
- Auliani, Anissa, 2015, *Putin Pengerahan Tentara ke Ukraina adalah Pilihan Paling Akhir* <http://internasional.kompas.com/read/2014/03/05/0331146/Putin.Pengerahan.Tentara.ke.Ukraina.adalah.Pilihan.Paling.Akhir> diakses pada 15 Agustus 2018
- Denning. 2015. *BlackEnergy Dangerous Virus*. <http://www.hackingnews.com/cyber-crime/blackenergy-dangerous-virus> diakses pada 04 Januari 2018
- Dinstein, Yoram. 2004. *The Conduct of Hostilities under the Law of Armed Conflict*. Cambridge: Cambridge University Press.
- Stone, Jhon, 2016, *Cyber Berkut Of Cyberwarfare*, <https://www.eff.org/about> diakses 13 September 2018
- Fajar, Mukti dan Yulianto Acmad. 2015. *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar
- Geers, Kenneth. 2016. *Cyber War In Prespective : Russian Aggression Against Ukraine*. Tallins: NATO CCD COE Publications.
- Gordon, Roya T. 2016. *Cyber-attack on Ukraine's Power Grid Implications on US Grid Security*. <https://maga.fiu.edu/academic-tracks/capstone-project/2016-capstone-working-papers/roya-gordon.pdf> diakses pada 05 Januari 2018
- Ibrahim, Johny. 2008. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia Publishing.
- Lee, Robert M. (E-ISAC). 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18*. [https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf) diakses pada 26 April 2018
- McCharty. 2015. *Cyber Attacks on the Ukrainian Grid: What You Should Know*. <https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf> diakses pada 19 Februari 2018
- Perserikatan Bangsa-Bangsa. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*.
- Perserikatan Bangsa-Bangsa. *The Charter of the United Nations of 1945 is the Foundational Treaty of the United Nations, An Intergovernmental Organization*.
- Perserikatan Bangsa-Bangsa. *United Nation Security Council Resolution Number 55/63, 2004*.
- Phartiana, I Wayan. 2003. *Pengantar Hukum Internasional*. Bandung: Penerbit Mandar Maju.
- Robin, Patrice. 2016. *Ukraines Power Outage was a Cyber Attack*. <https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA> diakses pada 22 Agustus 2018
- Sefriani. 2016. *Peran Hukum Internasional Kontemporer dalam Hubungan Internasional Kontemporer*. Jakarta: Raja Grafindo Persada.
- Soekanto, Soerjono & Mamudji, Sri. 2001. *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*. Jakarta: Rajawali Pers.
- Soekanto, Soerjono. 2009. *Pengantar Penelitian Hukum*. Jakarta: UI Press.
- Starke, J.G. 2010. *Pengantar Hukum Internasional*. Jakarta: PT Sinar Grafika.
- Tucker, P. 2016, *IP Version 6 Working Group*, <http://datatracker.ietf.org/wg/ipv6/charter/> diakses 13 September 2018