



**KAJIAN HUKUM HUMANITER INTERNASIONAL MENGENAI CYBER WARFARE DALAM KONFLIK BERSENJATA INTERNASIONAL ANTARA ISRAEL DAN PALESTINA ATAS GAZA**

**Yohana Tri Meiliyanti\*, Joko Setiyono, Kabul Supriyadhie**  
Program Studi S1 Ilmu Hukum, Fakultas Hukum, Universitas Diponegoro  
E-mail : [yohanatm16@gmail.com](mailto:yohanatm16@gmail.com)

**Abstrak**

Kemajuan teknologi informasi dan komunikasi mempengaruhi kehidupan berbangsa dan bernegara. Di samping memberikan dampak yang positif ternyata memberikan dampak yang negatif. Salah satu dampak negatif tersebut ialah munculnya senjata perang modern yaitu cyber warfare (perang siber) atau perang dunia maya dengan metode operasional yang berbeda dengan senjata-senjata militer pada umumnya. Penggunaan senjata ini sudah banyak diterapkan oleh negara-negara maju yang terlibat dalam konflik bersenjata seperti Israel dan Palestina atas perebutan otoritas "Tanah Suci" yang termasuk didalamnya jalur Gaza. Metode yang digunakan dalam penelitian ini adalah metode yuridis normatif yaitu penelitian dengan menggunakan data sekunder yang meliputi konvensi-konvensi, kebiasaan-kebiasaan, teori hukum, serta dokumen-dokumen dalam ruang lingkup Hukum Humaniter Internasional. Sampai saat ini belum ada ketentuan Hukum Humaniter Internasional yang merumuskan *cyber warfare* secara khusus, namun terdapat korelasi terhadap bunyi-bunyi pasal dalam konvensi-konvensi Hukum Humaniter Internasional.

Kata kunci: *Cyber Warfare*; Konflik Bersenjata Internasional; Hukum Humaniter Internasional

**Abstract**

*The progress of information and communication technology affects the life of the nation and state. Besides giving a positive impact it has a negative impact. One of the negative impacts is the emergence of modern war weapons called cyber warfare with operational methods that are different from military weapons in general. The use of this weapon has been applied by developed countries that is involved in conflicts such as Israel and Palestine over the seizure of the authority of the "Holy Land" which includes the Gaza Strip. The method used in this study is a normative juridical method, namely research using secondary data that contains conventions, habits, legal theory, and documents in space that discuss International Humanitarian Law. Until now there have been no provisions of International Humanitarian Law which specifically form cyber warfare, but there is a correlation to the sounds of articles in the conventions of International Humanitarian Law.*

*Keywords: Cyber Warfare; International Conflict; International Humanitarian Law*

**I. PENDAHULUAN**

Teknologi mengalami perkembangan yang sangat pesat. Hal ini disebabkan oleh perkembangan zaman yang semakin modern sehingga mengubah pola hidup manusia menjadi lebih dinamis. Zaman yang semakin maju mendorong manusia untuk terus berinovasi khususnya di bidang

teknologi. Teknologi telah memberikan banyak kemudahan bagi kehidupan manusia perkembangannya memberikan pengaruh yang sangat besar pada setiap bidang kehidupan manusia, baik di bidang pendidikan, transportasi, kesehatan, informasi dan komunikasi, serta bisnis.

Perkembangan teknologi mencapai puncak kemajuannya ialah dengan diciptakannya internet. Internet merupakan hasil pengembangan teknologi di bidang informasi dan komunikasi yang mana internet ini memiliki kemampuan untuk menghubungkan seluruh komputer di dunia melalui bantuan satelit khusus. Berkat internet setiap orang dapat berhubungan satu sama lain baik jarak dekat maupun jauh.

Perkembangan teknologi informasi dan komunikasi memberikan dampak positif. Dalam kaitannya dengan negara, teknologi informasi dan komunikasi telah memberikan kemudahan dalam menjalankan fungsi internal yaitu yang berkaitan dengan urusan rumah tangganya sendiri sedangkan fungsi eksternal yaitu dalam urusan menjalin hubungan dengan negara-negara lain.

Dampak negatif dari perkembangan teknologi senantiasa mengikuti hubungan antar negara atau hubungan internasional. Semakin sering berhubungan atau berkomunikasi satu sama lain maka semakin besar pula potensi timbulnya konflik atau sengketa diantara kedua belah pihak. Konflik atau sengketa antar negara dapat bermula dari berbagai sumber potensi sengketa. Sumber potensi sengketa antar negara dapat disebabkan karena beberapa alasan, diantaranya karena alasan politik, strategi militer, ekonomi maupun ideologi atau perpaduan antara kepentingan-kepentingan tersebut.<sup>1</sup>

Konflik atau sengketa internasional bisa timbul karena adanya interaksi antar dua negara atau lebih

yang kemudian terganggu akibat salah satu pihak (negara) tidak memenuhi kewajiban internasional terhadap negara lainnya dan tindakan tersebut menimbulkan kerugian (*injury*). Penyelesaian konflik atau sengketa internasional terdapat 2 (dua) cara, yaitu cara penyelesaian secara damai dan kekerasan. Penyelesaian konflik atau sengketa internasional dengan cara kekerasan merupakan cara penyelesaian lainnya disamping cara-cara damai dalam studi ilmu hukum internasional. Cara-cara kekerasan tersebut meliputi diantaranya perang (militer), retorsi (*retortion*), tindakan-tindakan pembalasan (*reprisal*) meliputi blockade, embargo, boikot serta intervensi (*intervention*).<sup>2</sup> Hukum internasional tidak melarang perang karena pada dasarnya perang merupakan suatu kenyataan yang tidak dapat dihindari. Oleh karena itu dibentuklah suatu hukum yang mengatur pelaksanaan perang yaitu Hukum Humaniter Internasional yang berlaku dalam konflik bersenjata, dengan tujuan yang paling utama adalah membatasi penggunaan senjata dalam perang yang dapat menimbulkan korban dari penderitaan yang tidak perlu (*unnecessary suffering*).

Perkembangan teknologi di era modern ini mendorong negara-negara yang terlibat dalam konflik atau sengketa bersenjata internasional untuk berinovasi menemukan senjata ataupun metode baru dalam berperang yang lebih efektif dan efisien dalam mematikan lawan atau

<sup>1</sup>Huala Adolf, *Hukum Penyelesaian Sengketa Internasional*, (Bandung: Sinar Grafika, 2004), halaman 1.

<sup>2</sup>Wisnu Dewanto, *Penyelesaian Sengketa Internasional*, diakses dari [https://www.academia.edu/32631287/PENYELESAIAN\\_SENGKETA\\_INTERNASIONAL](https://www.academia.edu/32631287/PENYELESAIAN_SENGKETA_INTERNASIONAL), pada 28 Januari 2019 pukul 17.57 WIB.

musuh. Penemuan ini terus dilakukan negara-negara guna mempersiapkan penyerangan dan pertahanan ketika konflik bersenjata meledak. Hal ini mempengaruhi penyelesaian konflik atau sengketa internasional dengan cara kekerasan menjadi bervariasi tidak lagi sebatas perang konvensional menggunakan senjata-senjata militer saja melainkan menjadi lebih beragam bentuk dan operasinya.

Dalam praktik konflik bersenjata internasional banyak negara yang dewasa ini telah melibatkan teknologi informasi dan komunikasi sebagai metode dalam penyerangan dan pertahanannya. Saat ini telah berkembang teknologi persenjataan siber yang memanfaatkan jaringan telekomunikasi internet dengan domain operasi yang dinamakan *cyber space* atau ruang maya. Operasi dengan domain *cyber space* menjadi suatu metode perang baru dimana perang tidak lagi hanya dilakukan secara konvensional dengan tembak-menembak atau menggunakan senjata militer secara langsung, namun dapat dilakukan dari jarak jauh dengan menyerang sistem jaringan informasi dan komunikasi milik komputer negara lawan atau musuh seperti *website* pemerintahan atau terhadap sistem kontrol fasilitas umum penduduk sipil seperti rumah sakit, pembangkit listrik, dan lain sebagainya melalui serangan siber (*cyber attack*) yaitu penyebaran virus. Virus komputer dapat menyebabkan lumpuhnya sistem komputer sehingga terhambat untuk melakukan fungsinya atau bahkan dapat mematikan keseluruhan sistem pada komputer, maka dengan begitu pertahanan negara lawan atau musuh akan melemah. Senjata dengan menggunakan metode operasional

seperti demikian dikenal dengan *cyber warfare*.

Penggunaan *cyber warfare* sebagai senjata dalam konflik bersenjata internasional merupakan fakta yang pernah dicatat oleh Discovery antara lain, kasus Georgia tahun 2008, berawal dari konflik Rusia dan Georgia di Ossetia Selatan, serangan siber melumpuhkan beberapa situs pemerintah Georgia dan situs-situs media local melalui penolakan layanan *Distributed Denial of Service attacks* (DDoS). Kejadian ini merupakan serangan yang mirip dengan serangan Estonia pada 2007, serangan Stuxnet melumpuhkan pembangkit nuklir Bushehr dengan *worm* tahun 2010.<sup>3</sup>

Selain Selain kasus-kasus di atas, penggunaan senjata *cyber warfare* juga terjadi dalam konflik bersenjata internasional antara Israel dan Palestina atas perebutan otoritas "Tanah Suci" yang termasuk didalamnya jalur Gaza. Tiga konflik besar antara Israel dan Palestina telah terjadi di Jalur Gaza sejak 2005 yang mana Pasukan Pertahanan Israel (IDF) melancarkan sistem operasi militer *Operation Cast Lead* (2008-2009) dan *Operation Pillar of Defense* (2012) untuk menanggapi serangan roket dari Palestina ke perbatasan Gaza-Israel selanjutnya pada tahun 2014 yang dikenal dengan operasi militer *Operation Protective Edge* terindikasi adanya serangan-serang siber (*cyber attacks*) disamping serangan militer.

---

<sup>3</sup>Erwin Kurnia, *Kebijakan Strategi Keamanan Cyber Nasional Dalam Menghadapi Perang Cyber (Cyber Warfare)*, (Jakarta: Universitas Pertahanan Indonesia, 2014), halaman 3.

Serangan-serangan maya (*cyber attacks*) terhadap Israel menyerang lebih dari 1.000 situs web Israel, penyedia Internet Israel dialihkan dan IP asing diblokir selama beberapa jam, alamat IP dan email pekerja kementerian Israel terpapar yang mana semuanya itu melalui *Distributed Denial of Service attacks* (DDoS).<sup>4</sup>

Dari uraiandi atas maka permasalahan yang dapat disusun antarlain:

1. Bagaimana Hukum Humaniter Internasional mengatur mengenai *cyber warfare* dalam konflik bersenjata internasional?
2. Bagaimana Implementasi Hukum Humaniter Internasional terhadap penggunaan *cyber warfare* dalam Konflik Bersenjata Internasional Antara Israel dan Palestina Atas Gaza?

## II. METODE

Metodependekatanyang digunakan dalam penelitian ini yuridis normatif yaitu pendekatan yang menggunakan konsep legis positivis yang menyatakan bahwa hukum adalah identik dengan norma-norma tertulis yang dibuat dan diundangkan oleh lembaga-lembaga atau pejabat yang

berwenang.<sup>5</sup> Penelitian Yuridis Normatif adalah penelitian hukum yang dilakukan dengan *library research* (penelitian kepustakaan), yaitu penelitian yang dilaksanakan dengan menggunakan bahan pustaka atau data sekunder belaka seperti undang-undang, hasil penelitian dari kalangan hukum terdahulu.<sup>6</sup>

Spesifikasi penelitian dalam penulisan hukum ini adalah dekriptif-analitis. Menurut Winarno Surachmad penelitian ini memusatkan diri pada analisis masalah-masalah yang ada pada masa sekarang dan pada masalah yang actual dan data yang dikumpulkan mula-mula disusun, dijelaskan, dan kemudian dianalisa dengan menggambarkan secara lengkap tentang ciri, keadaan, perilaku para pihak serta gejala berdasarkan fakta yang sebagaimana adanya.<sup>7</sup> Dengan penelitian yang bersifat deskriptif analitis maka penulisan hukum ini akan menggambarkan serta menentukan isi atau makna dari peraturan (perjanjian internasional) dalam konvensi-konvensi Hukum Humaniter Internasional yang berlaku dikaitkan dengan teori-teori hukum dan praktek pelaksanaan hukum positif menyangkut dengan permasalahan *cyber warfare* dalam penulisan hukum yang dikaji ini.

<sup>4</sup>Daniel Cohen dan Danielle Levin, *Cyber Infiltration During Operation Protective Edge*, diakses dari <https://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/>, pada tanggal 21 November 2018 pukul 08.45 WIB.

<sup>5</sup>Ronny Hanitio Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, (Jakarta: Ghalia Indonesia, 1988), halaman 11.

<sup>6</sup>M. Iqbal Hasan, *Pokok-Pokok Materi Metodologi Penelitian Dan Aplikasinya*, (Bogor: Ghalia Indonesia, 2002), halaman 11.

<sup>7</sup>Winarno Surachmad, *Dasar Dan Tehnik Research: Pengertian Metodologi Ilmiah*, (Bandung: CV Tarsito, 1973), halaman 39.

### III. HASILDAN PEMBAHASAN

#### A. Pengaturan *Cyber Warfare* Dalam Hukum Humaniter Internasional

Pembentukan Hukum Humaniter Internasional sebagian besar dipengaruhi oleh penggunaan senjata dalam perang yang berdampak secara khusus bagi penduduk sipil. Perubahan penggunaan senjata atau metode dalam perang mengalami evolusi dari zaman kuno sampai kepada zaman modern. Sebagai contoh, pada zaman Yunani kuno perang masih menggunakan kebiasaan tradisional yaitu dengan formasi militer Phalanx, yaitu formasi militer berbentuk kotak yang mana seluruhnya terdiri dari infanteri bersenjata berat dengan dipersenjatai tombak panjang, sarissa, atau senjata serupa lainnya seperti pedang.

Pada zaman modern kebiasaan perang tradisional yang seperti demikian sudah ditinggalkan, berubah menjadi penggunaan senjata perang yang berbasis teknologi. Kita dapat melihat praktiknya pada Perang dunia I dan Perang dunia II, dimana pada masa perang tersebut lahir senjata-senjata perang yang berbasis teknologi dan sangat mematikan, diantaranya:<sup>8</sup>

##### 1. Senapan Maxim

Senapan Maxim adalah senjata api yang telah mengalami revolusi pada abad 19. Senjata ini memiliki pendingin udara yang bisa menembakkan lebih

dari 500 putaran per menit pada jarak efektif lebih dari 2.000 yard (1.830 meter). Senjata ini digunakan dalam Perang Dunia I.

##### 2. Senjata Biologi

Dalam sejarah konflik bersenjata, penyakit sering menelan lebih banyak memakan korban daripada pertempuran. Oleh karena itu, ada ilmuwan yang terlibat dalam peperangan untuk menciptakan senjata biologis. Bibit-bibit sumber penyakit, Virus dan bakteri tak mengenal ras dan bangsa dari setiap kelompok yang berperang oleh karena itu setiap makhluk hidup dapat terkena dampaknya. Pada Perang Dunia I Jerman menggunakan dua bakteri patogen, yaitu *Burkholderia mallei* penyebab *Glanders* dan *Bacillus anthracis* penyebab *Anthrax* untuk menginfeksi ternak dan kuda tentara Sekutu. Perang Dunia II ditemukan lagi senjata-senjata yang lebih mutakhir, antara lain:<sup>9</sup>

##### 3. Roket V2 dan V1

Senjata ini merupakan cikal bakal rudal balistik antar benua yang berkembang pesat pada era perang dingin. Ditemukan oleh ahli peroketan Nazi Jerman Wernher von Braun. Roket ini telah meluluhlantakan ibu kota Inggris London, yang

<sup>8</sup>Aswab Nanda Pratama, "5 Senjata Perang yang Mematikan dalam Catatan Sejarah", diakses dari <https://internasional.kompas.com/read/2018/08/28/09144311/5-senjata-perang-yang-mematikan-dalam-catatan-sejarah>, pada 10 Januari 2019 pukul 13.46.

<sup>9</sup>Trisuharto Clinton, *Skripsi: Kajian Perang Sibermetika (Cyber-Warfare) Sebagai Konflik Bersenjata Internasional Berdasarkan Hukum Humaniter Internasional*, (Semarang: Universitas Diponegoro, 2015, halaman 97.

mana roket ini diluncurkan dari jarak jauh yaitu pantai barat Perancis.

4. Nuklir "*Little Boy*" dan "*Fat Man*"

Nuklir juga dikenal sebagai senjata perang yang mematikan karena merupakan salah satu pemusnah massal yang tercipta pada Perang Dunia II berkat proyek Manhattan yang dikembangkan Sekutu. Dampaknya, lebih dari 70.000 jiwa meninggal dunia ketika "*Little Boy*" dijatuhkan di Hiroshima Jepang pada 6 Agustus 1945 sedangkan "*Fat Man*" dijatuhkan di Kota Nagasaki pada 9 Agustus 1945. Ledakan bahan tersebut dipercaya menyebabkan ratusan ribu pekerja dilaporkan meninggal baik saat kejadian atau karena penyakit radiasi nuklir yang timbul pasca-insiden tersebut. Efek radiasi nuklir di kota itu mengakibatkan kelainan genetika pada warga sipil Jepang di Hiroshima dan Nagasaki.

Kemajuan teknologi di dunia terus mendorong perkembangan persenjataan perang berikut dengan metode atau caranya. Itulah sebabnya lahir salah satu senjata modern dalam konflik bersenjata internasional yang dikenal dengan *cyber warfare*.

**A. *Cyber Warfare* Sebagai Dalam Konflik Bersenjata Internasional**

Cara atau metode pada *cyber warfare* sedikit berbeda dengan perang konvensional. Perang konvensional menggunakan senjata-senjata perang yang riil atau nyata-nyata dapat dilihat secara kasat mata, sedangkan *cyber warfare* menggunakan komputer melalui bantuan sistem komunikasi dan jaringan pada ruang maya (*cyber space*). Metode operasional dari senjata *cyber warfare* secara umum dilakukan melalui penyebaran virus komputer berbahaya yaitu dikenal dengan "*Malware*" mencakup virus komputer dengan banyak bentuk perangkat lunak berbahaya diantaranya "*worm*" komputer, *trojan horse*, dan perangkat lunak berbahaya lainnya. Virus sering melakukan beberapa jenis aktivitas berbahaya pada komputer *host* yang terinfeksi, seperti perolehan ruang hard disk atau waktu unit pemrosesan pusat (CPU), mengakses informasi pribadi misalnya nomor kartu kredit, merusak data, menampilkan pesan politis di komputer, mengirim *spam* ke kontak email, mencatat penekanan tombol, atau bahkan yang paling parah membuat komputer tidak berguna. Disamping penyebaran virus, *cyber attacks* dapat berupa *Denial Of Service (DoS)* atau *Distributed Denial Of Service Attack (DDoS Attack)* yang mana serangannya membuat mesin atau sumber daya jaringan

tidak tersedia bagi pengguna yang dituju dengan layanan sementara atau tanpa batas, biasanya dilakukan dengan membanjiri mesin atau sumber daya yang ditargetkan dengan permintaan berlebihan sebagai upaya membebani sistem dan mencegah sebagian atau bahkan semua permintaan sah pemilik aslinya.

Negara-negara yang terlibat dalam konflik bersenjata dewasa ini telah menggunakan *cyber warfare* sebagai salah satu senjata dengan operasi ofensif dan defensif. Berikut beberapa peristiwa perang siber yang pernah terjadi, diantaranya:<sup>10</sup>

#### 1. The Morris Worm 1988

Diciptakan oleh Robert Tapan Morris, worm merupakan salah satu virus yang diibaratkan seperti cacing pada komputer. Virus ini dapat mempengaruhi infrastruktur siber dengan menyebar ke seluruh komputer sebagian besar di Amerika Serikat. Worm ini menggunakan kelemahan dalam sistem UNIX Noun 1 dan mereplikasi dirinya secara teratur sampai kepada tujuannya untuk memperlambat komputer sampai tidak dapat digunakan lagi. Penemuan virus worm menjadi tonggak awal munculnya *cyber warfare* (perang siber) yang mana worm ini menjadi salah satu senjata yang paling sering digunakan dalam perang siber di dunia

karena tingkat risiko yang dihasilkan dari serangannya terbilang cukup tinggi dibanding virus-virus lainnya.

#### 2. Estonia (Serangan terhadap Negara) 2007

Rangkaian serangan siber terhadap situs pemerintah, penegak hukum, perbankan, media, dan infrastruktur internet selama sekitar 3 (tiga) minggu. Sistem perbankan on-line milik Estonia diserang dengan metode *Distributed Denial of Service* (DDoS), sehingga berdampak terhadap perekonomian Negara tersebut. Peristiwa tersebut dipicu oleh pemindahan monument peringatan Perang Dunia I Uni Soviet dari ibukota Estonia, Talinn, sehingga mendapat reaksi keras dari publik Russia dan etnis minoritas di Estonia.

#### 3. Georgia (Botnet) 2008

Situs milik pemerintah Georgia dan Azerbaijan lumpuh diserang oleh peretas selama konflik Ossetia Selatan dengan Russia. Metode yang digunakan adalah DDoS, dimana pada peristiwa tersebut kelompok penyerang memperkenalkan "Botnet" yang dapat di unduh oleh publik yang ingin turut serta melakukan serangan siber terhadap Georgia.

### **A.1. Pengaturan Penggunaan Cyber Warfare Dalam Konvensi-Konvensi Hukum Humaniter Internasional**

Walaupun tidak ada konvensi hukum humaniter

<sup>10</sup>Adi Sulisty, *Tugas 3 (Cyber Warfare Dynamics): Sejarah dan Perkembangan Perang Siber*, (Bogor: Universitas Pertahanan Indonesia, 2014), halaman 1.

internasional tentang *cyber warfare*, tidak berarti bahwa *cyber warfare* bukan termasuk objek dari ketentuan dalam Hukum Humaniter Internasional.

1. Konvensi Den Haag

a. Larangan-Larangan Penggunaan Senjata Perang

Konvensi Den Haag Tahun 1899 dan 1907 secara garis besar mengatur mengenai alat (sarana) dan cara (metoda) yang boleh dipakai untuk berperang (*conduct of war*), yang mana konvensi ini merupakan aturan tertulis yang mengatur secara khusus mengenai penggunaan senjata di dalam perang. Pada Pasal 23 Konvensi Den Haag IV Tahun 1907 menyatakan larangan-larangan yaitu khusus untuk penggunaan senjata beracun dan senjata, proyektil, atau materi yang diperhitungkan menyebabkan penderitaan yang tidak perlu. Proyektil merupakan senjata yang ditembakkan ke udara dengan menggunakan gaya penggerak seperti misalnya senjata peluru, panah, dan tombak. Merujuk kepada pasal 22, dinyatakan bahwa hak para pihak yang berperang untuk menggunakan alat-alat untuk melukai musuh adalah terbatas pada akibat yang ditimbulkan. Berdasarkan bunyi kedua pasal tersebut dapat disimpulkan bahwa setiap senjata yang digunakan dalam berperang dilarang untuk menimbulkan penderitaan yang tidak perlu bagi tentara, milisi, kelompok sukarelawan dan penduduk sipil.

b. Pembatasan Penyerangan Di dalam Perang

Pasal 25 dan Pasal 27 Konvensi Den Haag IV Tahun 1907 Mengenai Hukum Dan Kebiasaan Perang Didarat pada Pasal mengatur bahwa penyerangan dan pemboman dengan alat apapun sejauh mungkin menghindari bangunan-bangunan ibadah, kesenian, ilmu pengetahuan dan panti sosial, monumen bersejarah, rumah sakit dan tempat orang sakit dan terluka dikumpulkan, asalkan tempat-tempat tersebut tidak digunakan untuk tujuan-tujuan militer. Pasal 25 mengisyaratkan bahwa *cyber warfare* merupakan bagian dari alat ataupun senjata yang penggunaannya dapat dibatasi oleh Konvensi Den Haag. Redaksional “Penyerangan atau pemboman dengan alat apapun...” dapat dijadikan sebagai landasan bahwa senjata, cara atau metode dalam perang tidak dibatasi termasuk *cyber warfare* yang merupakan salah satu senjata perang di era modern. Ketentuan tersebut membatasi bahwa semua penyerangan tidak boleh ditujukan terhadap kota-kota, kampung-kampung, pemukiman atau bangunan-bangunan yang mana lokasi-lokasi tersebut terdapat penduduk sipil.

2. Konvensi Jenewa 1949

Pasal 18 Konvensi Jenewa IV Tahun 1949 mendukung ketentuan Pasal 25 dan 27 Konvensi Den Haag IV Tahun 1907 yang mengatur bahwa

bangunan-bangunan umum dimana penduduk sipil berkumpul tidak boleh dijadikan sebagai sasaran serangan. Secara khusus dirumuskan “rumah sakit sipil yang diorganisir untuk memberikan perawatan kepada yang luka dan sakit, yang lemah serta wanita hamil, dalam keadaan bagaimanapun tidak boleh menjadi sasaran serangan, tetapi harus selalu dihormati dan dilindungi oleh pihak-pihak dalam pertikaian”. unyi pasal ini merupakan penerapan kewajiban negara-negara yang bertikai untuk menghormati hak untuk mempertahankan hidup dalam situasi konflik bersenjata.

Pasal 27 Konvensi Jenewa IV Tahun 1949 memberikan perlindungan bahwa: “dalam segala keadaan orang-orang yang dilindungi berhak akan penghormatan atas diri pribadi, kehormatan hak-hak kekeluargaan, keyakinan dan praktek keagamaan, serta adat-istiadat dan kebiasaan mereka. Mereka selalu harus diperlakukan dengan perikemanusiaan, dan harus dilindungi khusus terhadap segala tindakan kekerasan atau ancaman-ancaman kekerasan dan terhadap penghinaan serta tidak boleh menjadi objek tontonan umum. ”Pasal ini secara garis besar memberikan perlindungan terhadap orang-orang sipil dari akibat-akibat perang yang dapat mencederai hak asasi pribadi setiap individu di dalam situasi konflik bersenjata. Tindakan kekerasan memiliki makna yang luas yaitu

tindakan-tindakan baik yang dilakukan secara langsung maupun tidak langsung yang menyebabkan seseorang atau sekelompok orang tersiksa atau menderita baik batin, jasmani maupun rohani. Pasal 31 kemudian melengkapi bahwa: “penduduk sipil tidak boleh dilakukan paksaan fisik atau moral, terutama untuk memperoleh keterangan-keterangan dari mereka atau dari pihak ketiga.” Kata “moral” disini merujuk kepada tindakan-tindakan kekerasan non-fisik atau tidak langsung yaitu bicara soal akibat terhadap kondisi psikis penduduk sipil.

*Cyber warfare* (perang siber) atau perang dunia maya yang merupakan salah satu bentuk senjata perang modern dikategorikan sebagai tindakan kekerasan dalam konflik bersenjata yang dilakukan secara tidak langsung atau non-fisik, namun akibat yang ditimbulkan berpotensi sama dengan penggunaan senjata-senjata militer apabila serangan ditujukan secara nyata-nyata kepada objek-objek dan penduduk sipil.

3. Protokol Tambahan I Tahun 1977  
a. Cara dan Alat Peperangan

Pasal 36 Protokol Tambahan I Konvensi Jenewa 1949: “Di dalam penyelidikan, mengembangkan menghasilkan atau mendapatkan **suatu senjata baru, alat-alat baru atau cara peperangan**, suatu pihak Peserta

Agung berkewajiban menetapkan apakah di dalam keadaan tertentu atau segala keadaan penggunaannya tidak akan dilarang oleh Protokol ini atau sesuatu peraturan lain dari Hukum Internasional yang berlaku terhadap Pihak Peserta Agung tersebut”

Ketentuan Pasal 36 Protokol Tambahan I Tahun 1977 menunjukkan bahwa aturan Hukum Humaniter Internasional tidak membatasi penggunaan senjata, alat atau bahkan cara peperangan (metode) dalam konflik bersenjata internasional. *Cyber warfare* bukan sejenis senjata militer seperti pada umumnya, namun *cyber warfare* merupakan senjata baru yang mana cara pengoperasian serangannya disebut dengan *cyber attack* (serangan siber) pada domain khusus *cyber space* atau ruang maya. Serangan menurut Pasal 49 (1) Protokol Tambahan I Tahun 1977: “*Attacks means act of violence against the adversary, whether in offence or in defence*” (Serangan berarti tindakan kekerasan terhadap pihak musuh, baik dalam menyerang atau bertahan dalam mempertahankan diri). Tindakan kekerasan (*act of violence*) dalam Pasal 49 (1) tidak harus dipahami sebagai aksi yang dapat dilihat pergerakannya, artinya tidak selalu bicara soal melepaskan kekuatan kinetis seperti tembak-menembak. Syarat dari suatu tindakan dikategorikan sebagai tindakan kekerasan (*act of*

*violence*) lebih luas yaitu harus menghasilkan konsekuensi dalam arti keras, tidak terbatas pada tindakan keras secara langsung melainkan juga tidak langsung sepanjang serangan-serangan tersebut dapat mempengaruhi penduduk sipil, perorangan-perorangan sipil atau obyek-obyek sipil didarat (Pasal 49 ayat 3). Apabila konsekuensi yang dihasilkan bersifat menghancurkan, operasi-operasi seperti apapun bentuknya, telah memenuhi unsur dari ‘tindakan kekerasan (*act of violence*)’.

#### b. Perlindungan Umum Bagi Obyek-Obyek Dan Penduduk Sipil

Ketentuan mengenai perlindungan objek dan penduduk sipil dalam konflik bersenjata internasional tertuang di dalam Protokol Tambahan I tahun 1977 ketentuan pasal 51, 52, 53, 54, 55, dan 56. Pasal 51 (1) Protokol Tambahan I Konvensi Jenewa 1949 berbunyi demikian: “Penduduk sipil dan orang-orang sipil perorangan harus menikmati perlindungan umum terhadap bahaya-bahaya yang timbul dari operasi-operasi militer.”

Perlindungan umum terhadap obyek-obyek sipil dapat kita temukan di dalam pasal 52-56 Protokol Tambahan I Konvensi Jenewa. Secara umum diatur bahwa: “Obyek-obyek sipil tidak boleh dijadikan sasaran serangan atau tindakan pembalasan. Obyek-obyek sipil adalah semua obyek yang bukan sasaran militer.” Pasal 52 (3) kemudian memberikan

gambaran mengenai apa saja yang tergolong sebagai objek sipil, diantaranya: tempat pemujaan, rumah atau tempat tinggal lainnya atau rumah sekolah.

Pengoperasian serangan-serangan siber (*cyber attacks*) dalam *cyber warfare* diarahkan kepada sistem komputer yang mengontrol infrastruktur fisik dan sosial milik negara seperti tenaga pembangkit listrik, bandar udara, rumah sakit, dan lain-lain, yang mana semuanya itu merupakan kebutuhan dasar fisik pengorganisasian sistem struktur yang diperlukan untuk menjamin berlangsungnya perekonomian sektor publik dan privat sebagai layanan dan fasilitas yang disediakan oleh negara untuk penduduk sipil adalah dilarang.

## **B. Implementasi Hukum Humaniter Internasional Terhadap *Cyber Warfare* Dalam Konflik Bersenjata Israel Dan Palestina Atas Gaza**

### **B.1. Latar Belakang Konflik Bersenjata Internasional**

Konflik bersenjata Israel dan Palestina diawali dengan konflik dalam memperebutkan otoritas tanah yang dinamakan "Tanah Suci".Kedua negara mengklaim mempunyai hak atas tanah tersebut.Perebutan otoritas tanah ini dilatarbelakangi oleh unsur-unsur agama yang dianut oleh kedua belah pihak yaitu Islam dan Yahudi.Kedua agama tersebut sama-sama memiliki pemahaman bahwa tanah

palestina adalah hak masing-masing mereka.Bangsa Yahudi mengklaim bahwa tanah itu adalah hak mereka karena tanah tersebut merupakan tanah perjanjian Tuhan bagi bangsa Israel.Sedangkan bangsa Palestina mengklaim tanah itu hak mereka karena mereka sudah menetap disana selama beberapa abad dan dit tanah tersebut berdiri Masjid Al-Aqsa yang menjadi kiblat pertama umat Islam.Yang mendorong bangsa Yahudi juga bersikeras mengklaim tanah tersebut adalah tepat dibawah masjid itu terdapat Tembok Ratapan yang menjadi tempat sakral agama yahudi untuk berdoa kepada Tuhan.Oleh karena itu konflik ini erat sekali kaitannya dengan nilai historis dan nilai keagamaan yang amat tinggi bagi Agama Islam dan Yahudi.Konflik perebutan tanah suci ini dimulai pada 14 Mei 1948 "Perang Kebebasan". Kemenangan Israel atas perang tersebut menimbulkan bencana bagi bangsa Palestina karena banyak warga yang tewas akibat perang ini. Konflik perebutan otoritas tanah suci ini dimulai pada tahun 1967 dimana Israel menyerang Mesir, Yordania, dan Suriah.Israel berhasil merebut Sinai, Jalur Gaza, dataran tinggi Golan (Suriah), dan Yerusalem.

### **B.2. Penggunaan *Cyber Warfare* Oleh Palestina**

Israel mendapatkan serangan siber yang cukup dahsyat dari pihak Palestina sepanjang

menjalankan operasi militer tahun 2009, 2012, 2014 bahkan sampai sekarang. Selain serangan darat, laut, dan udara Israel juga dihadapkan dengan serangan-serangan siber yang sifatnya provokatif. Serangan-serangan siber (*cyber attacks*) tersebut telah menyerang diantaranya:

1. Tahun 2009 (*Operation Case Lead*)

Selama operasi 2009 terhadap Palestina di Gaza, Israel dipukul dengan empat gelombang serangan siber yang sangat kuat yaitu lebih dari setengah juta komputer diserang. Israel mencurigai serangan itu dibayar oleh Hamas atau Hizbullah dan dilakukan oleh organisasi yang tidak dikenal bekas Uni Soviet. Beberapa situs Web Israel dibuat offline seperti situs publik Badan Keamanan Israel (ISA, atau Shin Bet) dan *Home Front Command* yang mengatur warga bagaimana melindungi diri dari roket dan ancaman lainnya.<sup>11</sup>

2. Tahun 2012 (*Operation Pillar of Defense*)

Ketika kembali bertarung dengan Hamas pada tahun 2012, Israel menghadapi operasi siber yang begitu canggih. Diantaranya adalah:

- a. Rumah sakit Israel, Menurut Pusat Medis Sheba, Tel Hashomer, Mossad mengidentifikasi beberapa upaya untuk masuk ke situs web rumah sakit, mirip dengan serangan dunia maya sebelumnya di situs web lembaga-lembaga penting Israel, namun sejauh mana kerusakan yang disebabkan pada file pribadi pasien belum terlihat.
- b. Situs web Haaretz Hebrew <https://www.haaretz.co.il/> diturunkan dalam serangan penolakan layanan (DDoS) yang didistribusikan,<sup>12</sup>
- c. Situs-situs Tel Aviv Stock Exchange dan Situs Web El Al, situs Web untuk Bank Yerusalem diturunkan ketika situs publik IDF mengalami masalah dan partai Kadima dirusak. Ada juga gangguan online ke tiga bank: Bank Internasional Israel Pertama (FIBI) dan dua bank anak perusahaan, Massad dan Otzar Hahayal. Seorang juru bicara mengatakan situs pemasaran mereka telah diretas tetapi situs yang menyediakan layanan online untuk klien tidak terpengaruh. Pihak berwenang Israel mengatakan 15.000 akun diretas dan informasi kartu kredit sekitar 6.000 warga Israel lainnya diungkapkan

<sup>11</sup> Cohen, Matthew S, dkk, *Israel and Cyberspace: Unique Threat and Response*, (The Author, Oxford University Press, International Studies Association, 2015). Halaman 4, Diakses dari, [https://www.researchgate.net/publication/288823312\\_Israel\\_and\\_Cyberspace\\_Unique\\_Threat\\_and\\_Response](https://www.researchgate.net/publication/288823312_Israel_and_Cyberspace_Unique_Threat_and_Response).

<sup>12</sup>Oded Yaron, dkk, *Pro-Palestinian Hackers Bring Down Haaretz Hebrew Website*, diakses dari <https://www.haaretz.com/1.5174761> pada 31 Januari 2019 pukul 15.05 WIB.

secara online. Seorang peretas yang menyebut dirinya "OxOmar" menerbitkan secara online rincian kartu kredit ribuan orang Israel, setelah membobol apa yang dia katakan lebih dari 80 server Israel.<sup>13</sup>

- d. Dalam sebuah pesan Twitter Palestina Anonim mengklaim atas serangan terhadap [israelhayom.co.il](http://israelhayom.co.il) bahkan [google.co.il](http://google.co.il) down.<sup>14</sup>

3. Tahun 2014 (*Operation Protective Edge*)

serangkaian serangan siber yang diberi nama #OpIsrael membuat situs keuangan, bisnis, pendidikan, nirlaba, dan berita tidak dapat diakses. Rangkaian serangan cyber yang dinamakan #OpIsrael berlanjut ditahun selanjutnya 2014, kali ini tidak hanya mencakup DDoS sederhana, defokasi dan serangan kebocoran data, tetapi juga phishing, spoofing SMS dan pembajakan satelit (bagian dari perang psikologis Hamas).<sup>15</sup>

<sup>13</sup>Dan Even and DPA, *Hackers Paralyze Israeli Hospital Websites, as Cyber War Heats*, diakses melalui <https://www.haaretz.com/1.5174723>, pada 2 Februari 2019 pukul 13.12 WIB.

<sup>14</sup>Hugh Naylor, *Pro-Palestinian hackers apologise for cyber attack on Haaretz newspaper website*, diakses melalui <https://www.thenational.ae/world/mena/pro-palestinian-hackers-apologise-for-cyber-attack-on-haaretz-newspaper-website-1.373309>, pada 31 Januari 2019 pukul 16.38 WIB.

<sup>15</sup>Gilad Zahavi, *#OpSaveGaza Campaign – Insights from the Recent Anti-Israel Cyber Operation*, diakses dari <https://blog.sensecy.com/2014/08/11/opsave-gaza-campaign-insights-from-the-recent->

Selama kampanye 2014 melawan Hamas, situs *Home Front Command Web* sekali lagi offline untuk sementara, seperti beberapa situs web IDF publik. Tentara Elektronik Suriah dapat meretas blog IDF dan pada akun Twitter mereka memposting gambarnya sendiri. Iran, Hamas dan Hizbullah diduga melakukan serangkaian serangan besar-besaran terhadap "sistem vital nasional," termasuk air, listrik, dan situs perbankan.<sup>16</sup>

Secara umum *cyber attacks* yang dilakukan oleh pihak palestina selama masa operasi militer Israel baik tahun 2009, 2012 ataupun 2014, merupakan satu rangkaian dalam konflik bersenjata yang menggunakan serangan *Distributed Denial Of Service (DDoS)* yang menyerang lebih dari 1.000 situs web Israel

#### **B.4.Penerapan Pasal-Pasal Dalam Konvensi-Konvensi Hukum Humaniter Internasional**

Ketika bicara soal implementasi peraturan internasional pada konflik atau sengketa bersenjata internasional kita perlu memastikan bahwa masing-masing negara telah meratifikasi atau mengikatkan diri dengan perjanjian internasional dalam hukum humaniter. Ratifikasi adalah pengesahan tanda-tanda yang dilakukan oleh wakil-wakil

[anti-israel-cyber-operation/](https://blog.sensecy.com/2014/08/11/opsave-gaza-campaign-insights-from-the-recent-anti-israel-cyber-operation/) pada 31 Januari 2019 pukul 17.07 WIB.

<sup>16</sup>Cohen, Matthew S, dkk, *Op.cit.*

negara yang turut serta dalam perundingan.<sup>17</sup>

Hukum Humaniter Internasional merupakan kaidah hukum konflik bersenjata yang terdiri dari konvensi-konvensi internasional yang tertulis: Konvensi-Konvensi Jenewa 1949, Konvensi-Konvensi Den Haag 1899 dan 1907, Protokol Tambahan I dan II Tahun 1977, Protokol Tambahan III Tahun 2005 serta aturan-aturan tidak tertulis lainnya seperti norma atau hukum kebiasaan internasional dalam perang. Keempat Konvensi Jenewa 1949 telah diratifikasi oleh semua negara di dunia termasuk di dalamnya Israel dan Palestina. Swiss sebagai negara pengawas Konvensi Jenewa mengumumkan bahwa negara Palestina menandatangani Konvensi-Konvensi Jenewa 1949 pada tanggal 2 April 2014, sedangkan Israel meratifikasi pada tahun 1951.<sup>18</sup> Palestina telah meratifikasi Protokol Tambahan I dan II Tahun 1977 dan pada tahun 2014 dan 2015, namun disisi lain Israel hanya meratifikasi Protokol Tambahan III Tahun 2005. Untuk Konvensi Den Haag 1899, baik Israel dan Palestina tidak meratifikasinya, namun Konvensi Den Haag 1907 Israel dan Palestina sama-

sama telah meratifikasi konvensi ini. Berdasarkan data-data tersebut maka dapat diketahui bahwa ketentuan-ketentuan dalam Keempat Konvensi Jenewa 1949 dapat sepenuhnya diterapkan dalam konflik bersenjata internasional antara Israel dan Palestina atas Gaza karena kedua belah pihak telah meratifikasinya.

Palestina tidak menerapkan beberapa bunyi pasal dalam konvensi-konvensi Hukum Humaniter Internasional yang berkenaan dengan penggunaan senjata *cyber warfare* dalam konflik bersenjata internasional, diantaranya adalah:

- a. Pasal 51 ayat 1 Protokol Tambahan I Tahun 1977 sebagai ketentuan dasar perlindungan penduduk sipil (Prinsip Pembedaan (*Distinction Principle*) dalam konflik bersenjata internasional, bahwa penduduk sipil dan orang-orang sipil perorangan harus menikmati perlindungan umum terhadap bahaya-bahaya yang timbul dari operasi-operasi militer. Dalam konteks penggunaan senjata *cyber warfare* disini dimaknai bahwa serangan-serangan siber (*cyber attacks*) tidak boleh ditujukan kepada sistem komputer yang mengelola aktivitas-aktivitas penduduk sipil dalam aspek apapun dijauhkan dari tujuan militer (Prinsip Kepentingan Militer (*military necessity*)). Secara luas, sistem komputer yang mengontrol pemenuhan

<sup>17</sup>Syahmin A.K., *Hukum Perjanjian Internasional* (menurut Konvensi Wina tahun 1969), (Bandung: CV. Armico, 1985), halaman 104.

<sup>18</sup>ICRC Data base diakses dari [https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp\\_countrySelected=IL](https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=IL) pada 5 Februari 2019 pukul 17.51 WIB.

kelangsungan hidup manusia dilarang untuk dijadikan sasaran militer, seperti: rumah sakit, sekolah, perbankan, transportasi, hiburan (satelit tv), instalasi air, perkebunan, peternakan, pembangkit listrik dan lain sebagainya.

Faktanya Palestina telah menyerang situs web Rumah sakit Israel yaitu Pusat Medis Sheba, Tel Hashomer, Mossad, Situs-situs Tel Aviv Stock Exchange (bursa efek) dan Situs Web El Al (maskapai penerbangan) melalui *Distributed Denial Of Service (DDoS)* yang mengakibatkan web-web tersebut *down* dalam beberapa waktu sehingga menimbulkan kesulitan bagi pemegang sah website untuk menjalankan fungsi utamanya.

- b. Pasal 27 Konvensi Jenewa IV Tahun 1949 memberikan perlindungan bahwa “dalam segala keadaan orang-orang yang dilindungi berhak akan **penghormatan atas diri pribadi**, kehormatan hak-hak kekeluargaan, keyakinan dan praktek keagamaan, serta adat-istiadat dan kebiasaan mereka. Mereka selalu harus diperlakukan dengan perikemanusiaan, dan harus dilindungi khusus terhadap segala tindakan kekerasan atau ancaman-ancaman kekerasan dan terhadap penghinaan serta tidak boleh menjadi objek tontonan umum.” Untuk mendukung itu Pasal 46 Konvensi Den

Haag IV Tahun 1907 menegaskan bahwa “Kehormatan dan hak-hak keluarga dan hak hidup manusia serta **hak milik pribadi** dan juga praktik keagamaan serta kebebasan beribadah harus dihormati. Hak milik pribadi tidak boleh dirampas.”

Pada kenyataannya Palestina melakukan serangan siber (*cyber attack*) yang ditujukan kepada beberapa bank di Israel dan mengakibatkan terungkapnya informasi kartu kredit kurang lebih 6000 warga Israel. Seperti yang kita ketahui bahwa kartu kredit sifatnya sangat personal sehingga dalam keadaan konflik bersenjata sekalipun hak milik pribadi penduduk sipil harus tetap dihormati.

- c. Pasal 62 ayat 3 Protokol Tambahan I Tahun 1977 (Prinsip proporsionalitas (*Proportionality Principle*) dan Prinsip Pembatasan (*limitation Principle*) “gedung-gedung dan **materiel yang digunakan untuk tujuan-tujuan pertahanan sipil dan tempat-tempat berlindung yang disediakan bagi penduduk sipil**, obyek-obyek yang digunakan untuk tujuan-tujuan pertahanan sipil tidak boleh dihancurkan atau pihak yang memiliki obyek-obyek itu.” Sedangkan pada kenyataannya serangan siber dari Palestina ditujukan kepada situs web Shin Bet

(ISA) dan Home Front Command milik organisasi pertahanan sipil dimana situs tersebut memberikan pemberitahuan tentang bagaimana penduduk sipil Israel melindungi diri dari ancaman dan serangan-serangan roket. Dengan diserangnya kedua situs web tersebut, pemerintah Israel menjadi kesulitan dalam memberikan perlindungan kepada warga sipilnya dari serangan-serangan Palestina, sehingga secara tidak langsung Palestina telah melanggar unsur pemenuhan hak untuk hidup penduduk sipil dalam situasi konflik bersenjata.

- d. Aksi propaganda berbasis *cyber* diantaranya: pembajakan satelit tv sebagai bagian dari perang psikologis Hamas. Salah satu berita online melaporkan bahwa pemimpin Gaza Hamas mengambil alih *feed* satelit Israel yang memasok Channel 10 dan Channel 2 selama Operasi Pilar Pertahanan tahun 2012. Program-program pada Saluran 2 dan 10 terputus selama sekitar 30 detik bahkan beberapa menit untuk menyiarkan foto-foto orang yang terluka akibat serangan udara Israel di Gaza serta pesan propaganda yang menjanjikan lebih banyak serangan roket ke Israel dari sayap militer Hamas. Serangan-serangan siber (*cyber attacks*) tersebut memang dilaporkan tidak

menimbulkan dampak yang membahayakan secara fisik, namun berdasarkan ketentuan dalam Protokol Tambahan I Tahun 1977 Pasal 51 ayat 2: "...penduduk sipil maupun perorangan-perorangan sipil tidak boleh menjadi sasaran serangan, tindakan-tindakan atau ancaman-ancaman kekerasan yang tujuan utamanya adalah menyebarkan teror dikalangan penduduk sipil adalah dilarang"

### E.3. Penindakan Terhadap Pelanggaran-Pelanggaran Konvensi Jenewa 1949 Atas Penggunaan *Cyber Warfare*

Pengaturan didalam Hukum Humaniter Internasional secara khusus membatasi tindakan-tindakan kejahatan perang.Kejahatan perang dalam arti sempit ialah sebatas pada pelanggaran terhadap hukum dan kebiasaan perang yaitu Hukum Humaniter Internasional.Adapun tindakan-tindakan yang termasuk sebagai tindakan yang didefinisikan sebagai kejahatan perang adalah sebagai berikut Pasal 50 Konvensi Jenewa I dan Pasal 147 Kovensi Jenewa IV Tahun 1949:

- a. Penjarahan barang-barang milik publik atau milik pribadi;
- b. Pembunuhan sengaja terhadap orang yang dilindungi;
- c. Penganiayaan atau perlakuan tidak manusiawi (termasuk percobaan biologis);
- d. Dengan sengaja menyebabkan penderitaan yang hebat atau luka yang serius terhadap tubuh dan kesehatan;

e. Menggunakan senjata atau cara perang yang dilarang;

Tindakan kekerasan dengan penggunaan senjata *cyber warfare* melalui operasi serangan siber (*cyber attack*) sebagai senjata dalam konflik bersenjata internasional oleh Palestina kepada Israel, sampai sejauh ini tidak menimbulkan korban luka yang serius ataupun korban jiwa, namun akibatnya sampai kepada penduduk sipil. Meskipun tidak terjadi pelanggaran hak asasi manusia yang serius, tetapi prinsip utama di dalam Hukum Humaniter Internasional yaitu prinsip pembedaan (*distinction principle*) harus tetap dihormati oleh negara-negara pihak dalam konflik bersenjata. Penegasan lebih lanjut tentang kewajiban negara pihak mengenai penindakan dirumuskan dalam pasal 49 ayat (1) Konvensi I, Pasal 50 ayat (1) Konvensi II, Pasal 129 ayat (1) Konvensi III, dan Pasal 146 ayat (1) Konvensi IV, yang menyatakan bahwa “Para Pihak Peserta Agung berjanji untuk menetapkan undang-undang yang diperlukan yang memberikan sanksi pidana efektif terhadap orang-orang yang melakukan atau memerintahkan untuk melakukan salah satu diantara pelanggaran berat atas Konvensi ini seperti ditentukan dalam pasal berikut.” Berdasarkan ketentuan-ketentuan tersebut, negara yang telah meratifikasi konvensi mempunyai kewajiban untuk selanjutnya membuat mekanisme nasional yang akan memberikan sanksi pidana terhadap setiap

orang yang melakukan atau yang bertanggung jawab sepenuhnya dibalik setiap penyerangan dengan kata lain orang yang memerintahkan untuk melakukan pelanggaran berat atas ketentuan-ketentuan dalam konvensi ini. Kewajiban negara pihak dalam Konvensi Jenewa 1949 mencakup: (1) menerbitkan peraturan yang berhubungan dengan pelanggaran hukum humaniter, (2) mencari orang yang dituduh melakukan pelanggaran, (3) mengadili pelaku pelanggaran. Berdasarkan ketentuan tersebut, dapat disimpulkan bahwa setiap pelanggaran dalam konflik bersenjata, mekanisme pengadilannya dikembalikan kepada hukum nasional Negara Pihak tempat dimana terjadinya pelanggaran. Apabila penggunaan senjata *cyber warfare* mengakibatkan penderitaan yang tidak perlu yaitu melanggar hak asasi manusia maka tindakan tersebut termasuk kejahatan perang.

Dalam hal negara pihak tidak mau atau tidak memiliki mekanisme untuk mengadili dalam hukum nasionalnya, atau ternyata pengadilan nasional tidak berlaku secara adil, maka bisa ditempuh jalur pengadilan internasional dengan mengajukan individu yang melakukan pelanggaran hukum humaniter tersebut kepada Mahkamah Pidana Internasional (*Internasional Criminal Court atau ICC*). Pasal 8 Statuta Mahkamah Pidana Internasional menyebutkan bahwa kejahatan

perang adalah tindakan pelanggaran-pelanggaran berat terhadap Konvensi Jenewa 1949. Mengenai penerapan Hukum Humaniter Internasional terhadap aksi *cyber warfare* yang dilakukan oleh Palestina, dengan ini Israel dapat mengajukan perkara ini kepada Jaksa Penuntut atau Dewan Keamanan PBB hendak mengajukan perkara ini ke Mahkamah, atau atas inisiatif Jaksa Penuntut sendiri membuat penuntutan kepada Palestina di Mahkamah, dan individu yang melakukan atau memerintahkan untuk dilakukannya kejahatan tersebut dapat diadili pada Mahkamah Pidana Internasional.<sup>19</sup>

#### IV. KESIMPULAN

1. Hukum Humaniter Internasional sampai saat ini belum merumuskan secara eksplisit mengenai *cyber warfare* (perang siber) atau perang dunia maya di dalam setiap konvensi-konvensinya, tidak berarti bahwa *cyber warfare* bukan merupakan objek Hukum Humaniter Internasional. *Cyber warfare* merupakan suatu bentuk senjata perang modern yang mana metode operasionalnya cenderung baru dan berbeda dengan senjata-senjata perang pada umumnya (konvensional) yaitu *cyber attacks* (serangan-serangan siber) melalui program
2. Israel dan Palestina telah meratifikasi Konvensi Jenewa 1949 dan Konvensi Den Haag Tahun 1907, dengan demikian apabila terjadi pelanggaran-pelanggaran dalam perang maka ketentuan-ketentuan di dalamnya dapat diterapkan. Setiap pelanggaran dalam konflik bersenjata mekanisme pengadilannya dikembalikan kepada hukum nasional Negara Pihak tempat dimana terjadinya pelanggaran (Pasal 49 Konvensi Jenewa 1949). Dalam hal negara pihak tidak mau atau tidak memiliki mekanisme untuk mengadili dalam hukum nasionalnya, atau ternyata pengadilan nasional tidak berlaku secara adil, maka bisa ditempuh jalur pengadilan internasional dengan

<sup>19</sup>Evi Deliana HZ, *Penegakan Hukum Humaniter Internasional Dalam Hal Terjadinya Kejahatan Perang Berdasarkan Konvensi Jenewa 1949*, (Pekanbaru: Fakultas Hukum Universitas Riau, 2011), halaman 15.



mengajukan individu yang melakukan pelanggaran hukum humaniter tersebut kepada Mahkamah Pidana Internasional (*Internasional Criminal Court* atau ICC) dengan catatan bahwa pelanggaran tersebut merupakan kejahatan perang yang diatur dalam Pasal 50 Konvensi Jenewa I ataupun Pasal 147 Konvensi Jenewa IV Tahun 1949 mengenai pelanggaran-pelanggaran berat.

## V. DAFTAR PUSTAKA

### Buku Literatur

- Adolf, Huala. 2004. Hukum Penyelesaian Sengketa Internasional. Bandung: Sinar Grafika.
- A.K. Syahmin. 1985. Hukum Perjanjian Internasional (menurut Konvensi Wina tahun 1969). Bandung: CV. Armico.
- Clinton, Trisuharto. 2015. Skripsi: Kajian Perang Sibernetika (Cyber-Warfare) Sebagai Konflik Bersenjata Internasional Berdasarkan Hukum Humaniter Internasional, Semarang: Universitas Diponegoro.
- Hasan, M. Iqbal. 2002. Pokok-Pokok Materi Metodologi Penelitian Dan Aplikasinya. Bogor: Ghalia Indonesia.
- Soemitro, Ronny Hanitijo. 1982. Metodologi Penelitian Hukum. Jakarta: Ghalia Indonesia.

Surachmad, Winarno. 1973. Dasar Dan Teknik Research: Pengertian Metodologi Ilmiah. Bandung: CV Tarsito.

### Jurnal

Cohen, dkk. 2015. Israel and Cyberspace: Unique Threat and Response. The Author Oxford University Press, International Studies Association.

Deliana HZ, Evi. 2011. Penegakan Hukum Humaniter Internasional Dalam Hal Terjadinya Kejahatan Perang Berdasarkan Konvensi Jenewa 1949. Pekanbaru: Fakultas Hukum Universitas Riau.

Kurnia, Erwin. 2014. Kebijakan Strategi Keamanan Cyber Nasional Dalam Menghadapi Perang Cyber (Cyber Warfare). Jakarta: Universitas Pertahanan Indonesia

Sulistyo, Adi. 2014. Tugas 3 (Cyber Warfare Dynamics): Sejarah dan Perkembangan Perang Siber. Bogor: Universitas Pertahanan Indonesia.

### Website

Daniel Cohen dan Danielle Levin, 12 Agustus 2014. Cyber Infiltration During Operation Protective Edge, diakses dari <https://www.forbes.com/sites/realspin/2014/08/12/cyber-infiltration-during-operation-protective-edge/>, pada 21 November 2018.



- Even, Dan dan DPA.25 Januari 2012.Hackers Paralyze Israeli Hospital Websites, as Cyber War Heats, dikases dari <https://www.haaretz.com/1.5174723>.pada 2 Februari 2019.
- Gilad\_Zahavi, 11 Agustus 2014.#OpSaveGaza Campaign – Insights from the Recent Anti-Israel Cyber Operation, diakses dari <https://blog.sensecy.com/2014/08/11/opsavegaza-campaign-insights-from-the-recent-anti-israel-cyber-operation/> pada 31 Januari 2019.
- Naylor, Hugh, 27 Januari 2012. Pro-Palestinian hackers apologise for cyber attack on Haaretz newspaper website, diakses dari <https://www.thenational.ae/world/mena/pro-palestinian-hackers-apologise-for-cyber-attack-on-haaretz-newspaper-website-1.373309>, pada 31 Januari 2019.
- Pratama, Aswab Nanda. 28 Agustus 2018.5 Senjata Perang Yang Mematikan Dalam Catatan Sejarah, diakses dari <https://internasional.kompas.com/read/2018/08/28/09144311/5-senjata-perang-yang-mematikan-dalam-catatan-sejarah> pada 10 Januari 2019.
- Putrayasa, I.N.A. 6 Mei 2014.Tidak Efektifnya Peranan PBB dalam Perdamaian Israel-Palestina, diakses melalui <https://www.kompasiana.com/inyoman.ap/54f76942a3331184358b47e0/tidak-efektifnya-peranan-pbb-dalam-perdamaian-israel-palestina> pada 28 Januari 2019.
- Annisa Auliani, Palupi. 30 Juli 2013.Pertemuan Washington, Jalan Panjang Perdamaian Palestina-Israel, diakses dari <https://internasional.kompas.com/read/2013/07/30/0602307/Pertemuan.Washington.Jalan.Panjang.Perdamaian.Palestina-Israel> pada 28 Januari 2019.
- Yaron, Oded, dkk. 25 Januari 2012.Pro-Palestinian Hackers Bring Down Haaretz Hebrew Website, diakses dari <https://www.haaretz.com/1.5174761>, pada 31 Januari 2019