Indonesian Journal of Law and Justice Volume: 2, Number 2, 2024, Page: 1-10

Evaluasi Respons Hukum Humaniter Internasional terhadap Perang Siber

Dhita Evany Aristyawati*, Rohmatun Uyun, Adelia Zahra Nugroho

Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Muhammadiyah Surakarta

DOI:
https://doi.org/10.47134/ijlj.v2i2.3394
*Correspondence: Dhita Evany Aristyawati
Email: c100220031@student.ums.ac.id

Received: 05-12-2024
Accepted: 12-12-2024
Published: 31-12-2024

Abstract: *Cyberwarfare is a form of warfare that cannot be explicitly addressed by existing international law. While most experts agree that legal restrictions must apply to this phenomenon, However, the international community has not been able to reach a consensus on how international humanitarian law (IHL) can be adapted. After outlining several cyber conflicts, this article argues that this issue is still unresolved academically. We use descriptive research methods to look for adequate and sufficient descriptions of processes, objects, activities, and people. Some parts of the Hague Convention and the Geneva Convention may indeed be relevant to cyber warfare, but their specific relevance cannot respond to this phenomenon. This is confirmed by the emergence of the virtual world, which is more recent when compared to the birth of the instrument. Many cyberattacks unavoidably result in losses for the parties, making these breaches more likely in cyber conflicts than in conventional wars. States have strong incentives to engage in cyberattacks, despite the risk of being accused of war crimes. With this in mind, this article also argues that IHL should evolve to encourage the creation of a legal umbrella against cyber warfare in some situations and provide better guidance for states in carrying out these types of attacks.*

Keywords: *Cyber Warfare; Cyberspace; International Humanitarian Law; Cyber Attacks, State Security*

Pendahuluan

Perang siber diidentifikasikan sebagai tindakan yang diambil oleh pihak-pihak yang berada di dalam konflik dengan menggunakan berbagai alat teknologi yang disertai dengan orang-orang berbasis teknik. Pada prinsipnya perang siber ditujukan untuk memperoleh keuntungan dengan menghancurkan, merusak, melumpuhkan maupun merebut sistem musuh (Swanson, 2010). Di berbagai kasus kegiatan ini seringkali digunakan untuk mendapatkan informasi yang dirahasiakan oleh pihak musuh (Schmitt, 2014). Aktor dalam perang siber dapat diklasifikasikan ke dalam negara, individu, kelompok kejahatan terorganisir termasuk kelompok teroris (Pipyros et al., 2016).

Pada pertengahan 1990-an, pakar keamanan internasional mulai mempertimbangkan kemungkinan perang siber, baik sebagai elemen konflik bersenjata konvensional maupun sebagai proposisi yang berdiri sendiri (Kelsey, 2008). Namun ternyata pertimbangan tersebut mulai teralihkan setelah serangan 9/11. Kemudian ide ini kembali mencuat pada 2007 ketika Negara Anggota NATO, Estonia, mendapat serangan siber besar-besaran. Serangan tersebut sebagai besar berasal dari mereka yang mengaku sebagai etnis Rusia

(Buchan, 2016). Tahun berikutnya, perang siber semakin masif pada konflik bersenjata internasional antara Rusia dan Georgia (Pipyros et al., 2016). Menanggapi hal ini dan Pusat Siber-NATO meluncurkan proyek penelitian besar pada akhir 2009 untuk memeriksa hukum internasional publik yang mengatur perang siber (Kelsey, 2008).

Perang siber juga seringkali membawa status anonim sebagai 'tentara' dan alat serang (Buchan, 2016). Namun sampai saat ini, belum ada diskusi akademis tentang status anonim di bawah hukum humaniter internasional. Setelah serangan teroris Paris November 2015, kelompok *Anonymous* ini menyatakan "perang terhadap ISIS" (Swanson, 2010).

Kekosongan dalam literatur hukum internasional adalah sangat memprihatinkan. Mengingat baru-baru ini, model serangan siber semakin menunjukkan kesiapannya untuk terlibat dalam konflik bersenjata. Hal ini juga diperkuat dengan munculnya kelompok daring lain yang siap untuk melakukan operasi siber berbahaya terhadap pihak-pihak yang terlibat konflik bersenjata. Apakah Negara-negara di dunia telah mempersiapkan hal ini atau tidak, namun senjata siber telah menjadi hal yang pokok di dalam perang modern. Peperangan tidak lagi hanya terdiri dari serangan fisik atau invasi di antara negara-negara dengan unit militer yang berbeda. Jenis peperangan baru ini menggunakan teknologi untuk menghancurkan infrastruktur vital (T. Bos, 2005).

Masyarakat modern semakin bergantung pada struktur informasi global dan domestik, struktur ini justru cenderung menjadi sasaran selama perang ataupun konflik lainnya. Bahkan, survei terhadap tujuh puluh operator internet terbesar di Amerika Utara, Amerika Selatan, Eropa, dan Asia menemukan bahwa serangan siber meningkat tajam dan semakin canggih. Selain itu, serangan ini digunakan tidak hanya dalam konflik politik, tetapi juga dalam skema pemerasan dan untuk tujuan kejahatan berbahaya lainnya. Sementara serangan siber telah menjadi ancaman selama bertahun-tahun, hal ini dibuktikan dengan konflik siber Rusia-Georgia tahun 2008 yang menggambarkan bagaimana negara lebih kuat terlibat dalam serangan dunia maya sebagai cara untuk melemahkan sistem infrastruktur penting dan aset lawan. Serangan dilakukan sebab target tersebut merupakan objek yang vital bagi keamanan nasional, keamanan ekonomi, serta kesehatan dan keselamatan masyarakat (J. Markoff).

Fakta-fakta tersebut memperlihatkan bahwa terdapat ketidakpastian tentang parameter hukum yang tepat terkait perang siber (Schmitt & Watts, 2015). Lebih lanjut fakta tersebut juga menegaskan adanya fakta lain, bahwa hukum humaniter internasional pada dasarnya adalah sesuatu yang dinamis. Sehingga hal ini membuat negara-negara di dunia membutuhkan regulasi sebagai payung hukum yang dapat mengontrol fenomena ini.

Artikel ini mecoba menawarkan pemikiran tentang bagaimana hukum perang siber mungkin akan matang dalam beberapa dekade mendatang. Artikel ini dimulai dengan pengenalan singkat tentang munculnya konsep kedaulatan siber. Bagian kedua membandingkan konflik di dunia maya dan konflik di dunia fisik dengan menggunakan senjata konvensional. Bagian terakhir membahas bagaimana respon Hukum Humaniter Internasional (HHI) terhadap fenomena perang siber.

Singkatnya, artikel ini membahas penggunaan serangan SIBER atau jaringan komputer dan mempertimbangkan bagaimana *jus in bello*. Artikel ini pada akhirnya

berupaya menjawab pertanyaan: "Apakah serangan dunia maya merupakan tindakan perang sedemikian rupa sehingga prinsip-prinsip hukum humaniter internasional dapat berlaku dan mengatur penggunaannya?"

Metodologi

Metode penelitian merupakan cara yang mana dilaksanakan dengan tujuan agar didapatkan data sesuai dengan tujuan yang diinginkan (Lasa, 2009). Menurut KBBI (Kamus Besar Bahasa Indonesia) kata ilmiah memiliki arti yaitu keilmuan atau juga dapat dikatakan sebagai pemenuhan syarat maupun kaidah terkait dengan ilmu pengetahuan sehingga kebenaran yang ada bisa dipertanggung jawabkan dengan penuh kebenarannya.

Dalam penelitian yang dilaksanakan ini menggunakan metode penelitian deskriptif, hal ini dikarenakan tujuan dari penelitian ini yaitu agar diperoleh jawaban yang berhubungan dengan tanggapan, pendapat, maupun presepsi orang-orang, oleh karena itu pembahasan yang dipaparkan wajib dilakukan secara kualitatif ataupun dengan menggunaikan uraian menggunakan kata.kata.Penelitian deskriptif mencoba melakukan pencarian deskripsi yang sesuai dan tepat serta cukup memuat proses, objek, aktivitas, serta manusia (Basuki, 2010).

Hasil dan Pembahasan

1. Konsepsi Kedaulatan Siber

Batas-batas tradisional kedaulatan negara kini tidak dapat dikendalikan karena efektivitas teknologi dalam memajukan aktivitas sosial, ekonomi, dan budaya. Hilangnya pembatasan status kewarganegaraan untuk menciptakan "masyarakat digital" menegaskan hal ini. Akibatnya, negara-negara di dunia membutuhkan undang-undang yang dapat membatasi kemajuan dunia digital (Helbing, 2015).

Tujuan awal aturan ini adalah untuk membatasi prang siber terkait bisnis guna membatasi jumlah korban konsumen (Arthur, 2014). Namun, adopsi teknologi digital yang meluas dan modifikasi perilaku sosial di antara orang-orang telah mendorong negara-negara di seluruh dunia untuk berupaya meningkatkan ketahanan digital sosiopolitik mereka. Masalah bocornya data intelijen AS dan memang kasus Edward Snowden, yang juga menyadarkan Jerman untuk mengembangkan aturan keamanan siber, menjadi buktinya. Gagasan kedaulatan digital (juga dikenal sebagai "Kedaulatan Digital") segera ditambahkan ke klausul non-agresi dari perjanjian Rusia-Tiongkok (Klaus Vitt, 2019).

Perancis merupakan salah satu negara di Eropa yang terus fokus pada pemajuan gagasan kedaulatan digital di tingkat kerja sama global (Bellanger, 2012). Hal ini didukung oleh komitmen Prancis untuk menetapkan standar minimum keamanan digital, yang ditunjukkan dengan upaya negara tersebut untuk mengembangkan penyedia layanan keamanan siber sosial dan komersial serta kolaborasi politik berdasarkan CSIRT (*Computer Security Incident Response Teams*). Konsekuensinya, tidak bisa dipungkiri karena teknologi digital telah menyoroti bagaimana kedaulatan digital yang diciptakan dalam

konteks ketahanan siber, telah berkembang menjadi decoupling dan penggeseran parsial otoritas negara.

Hampir tidak dapat disangkal bahwa banyak negara yang telah membangun kedaulatan dunia maya sesuai dengan alasan keamanan data nasional sebagai akibat dari kasus pencurian yang signifikan yang melibatkan rahasia Negara (Fidler, 2015). Hampir tidak dapat disangkal bahwa banyak negara yang telah membangun kedaulatan dunia maya sesuai dengan alasan keamanan data nasional sebagai akibat dari kasus pencurian yang signifikan yang melibatkan rahasia negara. Karena peraturan lalu lintas internet yang ketat di negara-negara seperti Brasil, Cina, dan Rusia, istilah "balkanisasi internet" muncul (Marx, 2013). Hal ini menunjukkan betapa efektifnya kedaulatan suatu negara telah dinetralkan oleh kemajuan teknologi digital (Alves Jr, 2014).

Dalam kasus e-KTP di Indonesia tahun 2018, diklaim data digital penduduk Indonesia diduga dialihkan antar organisasi di luar negeri (Sassen, 2012). Ini karena tidak ada kerangka hukum yang komprehensif untuk keamanan data digital, dan tidak ada kerjasama internasional untuk memastikan kontrol akses data digital yang ditransfer dan diakses di luar lingkup hukum Indonesia. Indonesia kini mengambil inisiatif dan mendesak segera dibuatnya regulasi sistem pertahanan kedaulatan siber akibat hal tersebut.

Kapasitas untuk sepenuhnya menguasai dan mengontrol akses ke sesuatu dan interaksi melalui data digital dapat digunakan untuk menggambarkan keamanan dan ketahanan dunia maya suatu Negara (Posch, 2017). Selain itu, mengingat contoh pelanggaran data konsumen menggunakan teknologi keuangan, Equifax, sebuah perusahaan fintech global, ini menunjukkan bahwa di tengah masyarakat demokratis, hak privasi individu harus dilindungi (Gressin, 2017).

Berbagai insiden yang dijelaskan di atas telah meningkatkan tekanan pada negara-negara untuk mengadopsi peraturan keamanan siber yang dapat melindungi kedaulatan siber dengan segera. Kerja sama internasional kini mencakup undang-undang kedaulatan digital, yang tidak hanya melindungi kedaulatan dunia maya tetapi juga memiliki manfaat yang signifikan bagi pembangunan suatu negara. Mereka memikat negara lain untuk bergabung dengan mereka dalam mengembangkan kerja sama keamanan siber karena mereka telah berhasil berkonsentrasi pada pengembangan perjanjian keamanan siber (Mogrul et al., 2011).

2. Serangan Siber yang Dinilai Lebih Efektif

Internet telah muncul sebagai alat yang kuat bagi fungsi-fungsi pemerintah, informasi, serta perdagangan dan jejaring sosial. Bahkan internet telah menjadi cara untuk menyebarkan pesan-pesan ideologis dan politis (Taipale, 2007). Dengan meningkatnya pemanfaatan Internet untuk lebih dari sekadar fungsi ekonomi dan sosial, masyarakat internasional harus sadar bahwa hal tersebut juga dapat berfungsi sebagai alat untuk melakukan operasi yang mengarah pada kehancuran, dan bahkan kematian. Contoh-contoh serangan dunia maya terhadap negara-negara dalam sejarah baru-baru ini menggarisbawahi implikasi potensial dalam menggunakan Internet sebagai senjata dalam perang, serta bagaimana sekarang ada pengakuan internasional yang jelas tentang dunia maya sebagai medan perang (Solce, 2008).

Hal ini dibuktikan oleh fakta bahwa sistem perang informasi saat ini sedang dikembangkan dan digunakan oleh setidaknya 120 negara, termasuk Peru, Iran, Uni Emirat Arab, Kroasia, Vietnam, dan Rusia. Untuk memahami sepenuhnya serangan siber dan implikasinya, kita harus terlebih dahulu mendefinisikan perang siber dan konsep-konsep terkaitnya (Solce, 2008).

Buku Pegangan Operasi Siber dan Terorisme Angkatan Darat AS (2006) mendefinisikan serangan dunia maya sebagai: "Kegiatan mengganggu yang direncanakan yang ancamannya berdampak terhadap komputer dan/atau jaringan, dengan maksud untuk membahayakan atau untuk memajukan sosial, ideologis, agama, politik atau tujuan yang serupa. Termasuk untuk mengintimidasi siapa pun dalam melanjutkan tujuan tersebut." Kerusakan semacam itu dapat ditimbulkan pada jaringan komputer, serta fasilitas fisik dan orang.

Serangan dunia maya yang telah terjadi dalam beberapa tahun terakhir menggambarkan bagaimana negara yang menggunakan teknologi modern, justru lebih kuat dalam melemahkan infrastruktur vital milik lawan. Sehingga hal ini membuat kekhawatiran internasional yang signifikan bahwa negara-negara yang saling berperang, hampir dapat dipastkan terlebih dahulu meluncurkan serangan berbasis komputer atau serangan siber kepada lawan. Serangan-serangan tersebut ditujukan kepada sistem-sistem yang mendukung distribusi energi, telekomunikasi, dan jasa keuangan. Hal ini ditegaskan oleh sebab seluruh aspek mulai dari transportasi, pasokan komoditas, perawatan kesehatan, keselamatan publik hingga operasi militer kini bergantung pada sistem informasi computer (Klimek, 2012). Bahkan serangan dunia maya berpotensi menyebabkan kerusakan yang jauh lebih besar daripada senjata konvensional.

Hal ini dibuktikan dengan serangan pada situs komersial dan pemerintah Lithuania pada Juni 2008, serangan pada situs web pemerintah Estonia pada 2007, pelanggaran email di Pentagon pada Juni 2007, dan meretas situs web perusahaan telepon milik pemerintah Pakistan pada Januari 2003 (Klimek, 2012). Serta sekitar Agustus 2008, serangan *denial of service* (DDoS) situs web resmi Georgia dinonaktikan sementara, termasuk situs kantor Presiden, Kementerian Luar Negeri, dan Kementerian Pertahanan, dan menyebabkan masalah komunikasi di seluruh negeri.

Bahkan telah ditemukan bahwa peretas Cina telah berhasil meretas jaringan komputer Gedung Putih serta berhasil mendapatkan komunikasi email yang dilakukan antara pejabat pemerintah. Belum lagi serangan terhadap Lituania yang merusak perusakan situs web pemerintah dan komersial yang menampilkan narasi anti-Lituania dan 41 simbol komunis (Harris, et al., 2013). Dua contoh ini menunjukkan bahwa kerusakan akibat serangan dunia maya seringkali tidak dapat diprediksi.

Senjata siber jelas tidak seperti senjata perang tradisional. Serangan siber justru lebih mematikan. Hal ini dibuktikan dengan individu atau negara yang menggunakan senjata siber dapat memilih dari berbagai opsi, termasuk sintaksis, semantik, dan campuran 43 senjata. Senjata sintaksis, menargetkan sistem operasi komputer, termasuk kode berbahaya, seperti virus, worm, Trojan 44 Horses, DDoS, dan spyware. Melalui serangan DDoS, seperti yang digunakan terhadap Georgia, penyerang siber menutup situs web dengan membombardirnya dengan lalu lintas dalam jumlah besar. Sebaliknya, senjata

semantik menargetkan "keakuratan informasi yang dapat diakses oleh peretas (Brenner & Goodman, 2002).

Dengan kata lain, serangan semantik terdiri dari proses mengubah informasi yang masuk ke sistem komputer untuk menghasilkan kesalahan tanpa sepengetahuan pengguna/pemilik (Brenner & Goodman, 2002). Sementara senjata campuran adalah model senjata yang menggabungkan senjata sintaksis dan semantik untuk menyerang informasi dan sistem operasi komputer, menghasilkan serangan yang lebih canggih. 'Contoh senjata campuran adalah "jaringan bot". Model serangan ini dilakukan dengan ditanam di komputer pihak ketiga yang tidak bersalah secara diam-diam. Bot ini kemudian dapat mengendalikan komputer lawan dari jarak jauh. Seorang peretas yang mengontrol bot dapat memata-matai, menyalin, dan mengirimkan data sensitif terhadap komputer yang ditargetkan (Cerf & Leiner, 1997).

Perangkat yang terinfeksi ini kemudian terus-menerus menaati perintah dari penyerang dan menindaklanjutinya. Efek besar dan data-data rahasia yang didapatkan dari proses serangan ini menjadikan serangan siber dinilai lebih efektif daripada serangan konvensional. Inilah yang kemudian sangat membahayakan, mengingat tidak ada payung hukum yang pasti untuk dapat memberikan perlindungan.

3. Respon Hukum Humaniter Internasional

Pengumpulan dan gangguan informasi selalu menjadi alat utama dalam model perang siber. Mengganggu jaringan komunikasi musuh bahkan lebih memiliki nilai strategis lebih besar daripada menghancurkan gudang senjata atau jalur pasokan. Memang, beberapa metode perang siber dianggap begitu buruk sehingga dapat dilarang oleh hukum perang (McCoubrey, 1990). Dengan konsekuensi ini, serangan siber dapat dikategorikan sebagai konflik bersenjata. Sehingga HHI dapat mengatur, jika kriteria tertentu telah dipenuhi.

Pertanyaan batas-batas pengaturan dalam keadaan apa serangan siber dapat dianggap sebagai konflik bersenjata, maka HHI harus masuk pada ruang ini. Ini adalah pertanyaan penting karena jawabannya memberikan panduan kepada negara-negara tentang bagaimana mereka dapat merespon jika mendapat serangan siber dengan cara yang konsisten, khususnya dengan norma-norma hukum internasional.

HHI adalah cabang hukum internasional publik yang berupaya memoderasi perilaku konflik bersenjata dan mengurangi penderitaan yang disebabkannya. Ini adalah salah satu dari dua pembagian prinsip hukum perang yang disebut dengan *jus in bello*. atau hukum saat perang. Beberapa lainnya dikenal dengan *jus ad bellum*, atau *"law to war,* yang mengatur legalitas untuk menggunakan angkatan bersenjata dalam perang (McCoubrey, 2019).

Jus di bello secara konvensional melibatkan Konvensi Jenewa dan Konvensi Den Haag. Konvensi Jenewa bertumpu pada empat Konvensi Jenewa 1949 dan dua Protokol Tambahan 1977. Perjanjian-perjanjian ini terutama berkaitan dengan perlindungan para korban konflik bersenjata, dengan Protokol Tambahan I yang berfokus pada cara dan metode perang. Sebaliknya, Konvensi Den Haag mengacu pada Konvensi Den Haag 1899 dan 1907, terutama berkaitan dengan metode, cara perang, taktik, dan perilaku peperangan secara umum.

Namun demikian, evaluasi terhadap Konvensi Jenewa dan Protokol Tambahan menyatakan bahwa "konflik bersenjata" harus dapat dilihat dengan cara yang cukup luas. Sehingga prinsip-prinsip dasar HHI memperjelas. HHI didirikan berdasarkan gagasan bahwa korban konflik bersenjata berhak atas perlindungan (Eom et al., 2012).

Dari diskusi di atas, secara logis memberikan identifikasi bahwa serangan dunia maya dapat merupakan konflik bersenjata, meskipun penggunaan komputer sebagai senjata bukanlah metode perang tradisional atau fisik. Sementara serangan dunia maya menggunakan teknologi modern yang tidak pernah diprediksi maupun selama penyusunan Konvensi Jenewa, maupun Protokol Tambahan I (Dormann, 2004). Sehingga hukum konflik bersenjata harus berubah dan dikembangan untuk dapat menjelaskan bagaimana perlindungan kemanusiaan baru. Namun faktanya, HHI mengantisipasi perubahan teknologi.

Hal ini ditegaskan dengan Klausula Martens yang ditemukan di Mukadimah Konvensi Den Haag IV tahun 1907. Di dalam klausula tersebut ditegaskan bahwa dalam kasus-kasus yang tidak secara eksplisit tercakup oleh perjanjian khusus, warga sipil tetap berada di bawah perlindungan dan otoritas prinsip-prinsip hukum internasional yang berasal dari adat yang sudah mapan, prinsip-prinsip kemanusiaan, dan dari perintah dari nurani public. Dengan kata lain, serangan pada dasarnya harus dinilai dengan seberapa besar oleh efeknya, bukan oleh bagaimana cara melakukannya (Greenberg et al., 1998).

Protokol Tambahan I ke Konvensi Jenewa sebenarnya menyediakan panduan penting dalam menilai penerapan HHI terhadap serangan dunia maya. Protokol I mengkodifikasi banyak prinsip yang ada dan memperkenalkan ketentuan perjanjian baru yang penting terkait dengan konflik bersenjata internasional. Namun memang, beberapa ketentuan Protokol Tambahan I dapat dikatakan kontroversial sehingga hanya mengikat negara pihak pada perjanjian. Dengan demikian, mereka tidak mencerminkan hukum yang secara universal dapat mengatur semua pihak.

Pasal 35 Protokol Tambahan I menyatakan: "Dalam setiap konflik bersenjata, menjadi hak para pihak atas konflik untuk dapat memilih metode atau cara peperangan dengan tidak terbatas. Namun Dilarang menggunakan senjata, proyektil dan bahan serta metode perang yang menyebabkan cedera berlebihan dan penderitaan yang tidak perlu." Prinsip ini kemudian berfungsi dapat digunakan membatasi berbagai cara perang dan senjata perang.

Mirip dengan senjata nuklir, senjata siber dapat dikategorikan sebagai *sui generis*. Sehingga harus diatur oleh seperangkat hukum yang unik dan dengan karakteristik tertentu juga. Namun demikian, senjata siber, seperti halnya senjata nuklir, adalah senjata yang menghasilkan konsekuensi yang mirip dengan senjata tradisional. Sehingga, prinsip-prinsip HHI, seperti konsep penderitaan yang tidak perlu dan proporsionalitas, masih memiliki relevansi dalam kasus serangan siber.

Namun kemudian timbul pertanyaan lain seperti: Sejauh mana prinsip-prinsip ini berlaku? Sementara beberapa ketidakpastian masih tetap ada. Beberapa menjawab bahwa "konflik bersenjata" terjadi ketika salah satu pihak mengambil tindakan yang dapat melukai, membunuh, merusak, atau menghancurkan, terlepas dari senjata yang digunakan.[1]

[1] Swanson, *supra* note 2 at 15.

Conclusion

Perang siber telah terjadi selama beberapa tahun terakhir, tetapi entitas pelaku perang semakin memanfaatkan domain ini sebagai cara untuk melakukan berbagai jenis serangan dengan bantuan komputer. Hal ini menimbulkan banyak kekhawatiran, mengingat bahwa aspek-aspek utama dari infrastruktur fisik atau kritis suatu negara sudah banyak terhubung ke ruang maya. Artikel ini telah menunjukkan bahwa hukum internasional yang berlaku saat ini dapat mengatasi sifat perang yang selalu berubah.

Ditambah dengan konsep kedaulatan siber yang telah digunakan oleh negara-negara maju, menunjukkan betapa vitalnya pertahanan siber bagi sebuah negara. Selain itu, prinsip-prinsip HHI tentang proporsionalitas dan penderitaan yang tidak perlu, semua harus juga dapat mengatasi masalah perang siber. Namun, komunitas hukum internasional harus terus bekerja untuk mengatasi ambiguitas tertentu yang ada dalam penerapan HHI. Sehingga negara-negara memiliki pemahaman yang jelas tentang bagaimana cara melaksanakan atau mempertahankan diri terhadap serangan siber. Kunci bagi negara dan organisasi internasional di tahun-tahun mendatang adalah menemukan cara yang lebih baik, lebih efisien untuk menentukan siapa yang bertanggung jawab atas serangan siber. Di sisi lain perlu membuat kebijakan nasional yang lebih transparan mengenai evolusi perang siber.

Meskipun serangan siber biasanya tidak langsung diarahkan pada manusia, mereka memiliki potensi lebih parah daripada perang konvensional. Efek dari serangan siber akan menentukan apakah itu diklasifikasikan sebagai konflik bersenjata yang diatur HHI. Oleh karena itu, negara dan organisasi internasional harus mengambil sikap proaktif dalam membangun strategi keamanan siber nasional dan mengikuti norma hukum internasional, dengan pengakuan bahwa perang dunia maya akan tetap ada.

References

Alves Jr, S. (2014). The Internet balkanization discourse backfires. *SSRN*. https://doi.org/10.2139/ssrn.2498753

Arthur, C. (2014). *Digital wars: Apple, Google, Microsoft and the battle for the Internet*. Kogan Page Publishers.

Bellanger, P. (2012). On digital sovereignty. *Le Débat, 3*, 149.

Bos, T. (2005). The impact of using virtual reality technology to train for law enforcement critical incidents. *J. Calif. Law Enforc, 39*(2), 5.

Brenner, S. W., & Goodman, M. D. (2002). In defense of cyberterrorism: An argument for anticipating cyber-attacks. *U. Ill. J.L. Tech & Pol'y*, 1.

Buchan, R. (2016). Cyber warfare and the status of Anonymous under international humanitarian law. *Chinese Journal of International Law, 15*(4), 741.

Cerf, V. G., & Leiner, B. M. (1997). Brief history of the Internet. *Internet Society*.

Dörmann, K. (2004). Applicability of the Additional Protocols to computer network attacks. *International Committee of the Red Cross*.

Dogrul, M., Aslan, A., & Celik, E. (2011). Developing an international cooperation on cyber defense and deterrence against cyber terrorism. *IEEE*.

Eom, J.-H., et al. (2012). Cyber military strategy for cyberspace superiority in cyber warfare. *IEEE*.

Fidler, D. P. (2015). *The Snowden Reader*. Indiana University Press.

Gressin, S. (2017). The Equifax data breach: What to do. *U.S. Federal Trade Commission*.

Greenberg, L. T., Goodman, S. E., & Soo Hoo, K. J. (1998). Information warfare and international law. *National Defense University Washington DC*.

Harris, B., Konikoff, E., & Petersen, P. (2013). Breaking the DDoS attack chain. *Institute for Software Research*.

Helbing, D. (2015). *Thinking ahead: Essays on big data, digital revolution, and participatory market society*. Springer.

Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review, 1427*.

Klimek, L. (2012). Combating attacks against information systems: EU legislation and its development. *Masaryk University Journal of Law and Technology, 6*, 87.

Markoff, J. (2008). Internet attacks seen as more potent and complex. *International Herald Tribune*.

Marx, N. (2013). Storage wars: Clouds, cyberlockers, and media piracy in the digital economy. *Journal of E-Media Studies, 3*(1).

McCoubrey, H. (1990). *International humanitarian law: The regulation of armed conflicts*. Dartmouth Publishing.

McCoubrey, H. (2019). *International humanitarian law: Modern developments in the limitation of warfare*. Routledge.
No, DCSINT Handbook. (2006). Critical infrastructure threats and terrorism.

Pipyros, K., et al. (2016). Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare. *Information and Computer Security, 24*(1), 38.

Posch, R. (2017). Digital sovereignty and IT-security for a prosperous society. In *Information Future* (pp. 77–90). Springer.

Rugge, F. (2018). *Confronting an "Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace*. Ledizioni.

Sassen, S. (2012). Interactions of the technical and the social: Digital formations of the powerful and the powerless. *Information, Communication & Society, 15*(4), 455.

Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. Hachette UK.

Schmitt, M. N. (2014). The law of cyber warfare: Quo vadis. *Stanford Policy Review, 25*, 269.

Schmitt, M. N., & Watts, S. (2015). The decline of international humanitarian law opinio juris and the law of cyber warfare. *Texas International Law Journal, 50*, 189.

Solce, N. (2008). The battlefield of cyberspace: The inevitable new military branch-the cyber force. *Albany Law Journal of Science & Technology, 18*, 293.

Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loyola International & Comparative Review, 32*, 303.

Taipale, K. A. (2007). Seeking symmetry on the information front: Confronting global jihad on the Internet.

Terry, J. P. (1999). Cyberspace and the use of force. *Duke Journal of Comparative & International Law, 9*(2), 491.

Vitt, K. (2019). Die Digitalisierung der Verwaltung braucht effiziente föderale Kooperation. *Der Moderne Staat–dms Zeitschrift für Public Policy, Recht und Management*, *12*(1).

"Mendagri sebut data e-KTP 110 juta warga Indonesia ada di perusahaan asing." (2016). Retrieved from https://news.detik.com/berita/d-3353022/mendagri-sebut-data-e-ktp-110-juta-warga-indonesia-ada-di-perusahaan-asing.