Jurnal Kawruh Abiyasa
Jurnal Ilmiah Berkala Multidisiplin
Cendekia Abiyasa Nusantara
Graha Bukopin Building 12th floor
Jln. Panglima Sudirman, Surabaya
Telp. : (031) 28997953
Email : editor@jurnalkawruh.id

MENINJAU PERANG SIBER: DAPATKAH KONVENSI-KONVENSI HUKUM HUMANITER INTERNASIONAL MENINJAU FENOMENA INI?

MOCH. MARSA TAUFIQURROHMAN[1], MUHAMMAD TORIQ FAHRI[2], ROBI KURNIA WIJAYA[3], I GEDE PUTU WIRANATA[4]
[1]Program Studi Ilmu Hukum Fakultas Hukum Universitas Jember
[2,3]Kejaksaan Negeri Banyuwangi
[4]Kepolisian Resor Kota Banyuwangi
Email: mochmarsa_t@yahoo.co.id

ABSTRACT
Cyberwarfare is a form of warfare that cannot be explicitly addressed by existing international law. While most experts agree that legal restrictions should 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. This article argues that this issue remains unresolved academically. Some passages in the Geneva Conventions and the Hague Convention may indeed be relevant to cyber warfare, but specifically the relevance does not respond to this phenomenon. Many cyberattacks inevitably inflict losses on parties, making these violations more likely to occur in cyber conflicts than in conventional wars. With this in mind, this article also argues that IHL should evolve to encourage the creation of a legal umbrella against cyberwarfare in some situations and provide better guidance.

Keywords: Cyber Warfare, Cyber Attack, Cyber Sovereignty, International Humanitarian Law, National Security

ABSTRAK
Perang siber adalah bentuk peperangan yang secara eksplisit tidak dapat ditangani oleh hukum internasional yang ada. Sementara sebagian besar pakar setuju bahwa pembatasan hukum harus berlaku terhadap fenomena ini. Meski demikian, komunitas internasional belum mampu mencapai konsensus tentang bagaimana hukum humaniter internasional (HHI) dapat disesuaikan. Artikel ini berpendapat bahwa masalah ini masih belum terselesaikan secara akademis. Beberapa bagian di dalam Konvensi Jenewa dan Konvensi Den Haag memang dapat relevan dengan perang siber, tetapi secara spesifik relevansi tersebut terbilang tidak dapat merespon fenomena ini. Banyak serangan siber yang tidak terhindarkan menimbulkan kerugian bagi para pihak, membuat pelanggaran-pelanggaran ini lebih mungkin terjadi dalam konflik dunia maya daripada dalam perang konvensional. Dengan mempertimbangkan hal tersebut, artikel ini juga berpendapat bahwa HHI harus berevolusi untuk mendorong terciptanya payung hukum terhadap perang siber dalam beberapa situasi dan memberikan panduan yang lebih baik.

Kata kunci: Perang Siber, Serangan Siber, Kedaulatan Siber, Hukum Humaniter Internasional, Keamanan Negara

PENDAHULUAN

Dalam dekade-dekade setelah penciptaan Internet, dunia maya telah menjadi wilayah konflik karena Negara-negara meningkatkan kemampuan dunia maya mereka dengan menciptakan persenjataan canggih persenjataan dunia maya; menambahkan personel khusus dan struktur kekuatan, dan terlibat dalam dan sumber daya penelitian dan pengembangan mutakhir kemampuan ofensif dan defensif. Diperkirakan sekitar 140 negara telah mengembangkan, atau sedang menyempurnakan, kapasitas untuk mengobarkan konflik bersenjata dunia maya.

Faktanya, pada 2016 di KTT Warsawa, NATO mengumumkan bahwa dunia maya sekarang dianggap sebagai domain operasi di mana ia harus mempertahankan diri seefektif di udara, di darat, dan di laut. Deklarasi ini secara luas diyakini sebagai pengakuan bahwa ancaman dunia maya menjadi lebih umum, kompleks, dan berpotensi merusak. Inti dari tren ini adalah pengembangan dan penggunaan senjata siber. Sampai saat ini, relatif sedikit contoh senjata siber yang diakui secara publik. Senjata siber yang paling terkenal dan kontroversial adalah yang disebut *worm Stuxnet*.

Dilihat dari latar belakang dan konteksnya, pada tahun 2006, Presiden Amerika Serikat George W. Bush ingin menggagalkan atau memperlambat program nuklir Iran. Namun, Presiden Bush tidak ingin melancarkan serangan udara terhadap fasilitas pengayaan nuklir Iran. Dia sedang mencari pilihan antara tidak melakukan apa-apa dan serangan kinetik. Bush akhirnya menyelesaikan operasi siber pada sistem kontrol komputer di fasilitas pengayaan nuklir Iran di Natanz, Iran.

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.[1] Pada prinsipnya perang siber ditujukan untuk memperoleh keuntungan dengan menghancurkan, merusak, melumpuhkan maupun merebut sistem musuh.[2]

---

[1] Istilah "perang siber" yang digunakan di sini adalah dalam arti non-normatif dan murni deskriptif. Mencakup tindakan pada penggunaan *jus ad bellum* dan orang-orang yang termasuk di dalam konflik bersenjata di bawah *jus in bello*. Artikel ini juga akan menyentuh hukum kedaulatan karena hal tersebut relevan dengan situasi perang siber.

[2] Lesley Swanson, "The era of siber warfare: Applying international humanitarian law to the 2008 Russian-Georgian siber conflict" (2010) 32 Loy Intl Comp Rev 303 hlm. 11.

Pada pertengahan 1990-an, pakar keamanan internasional mulai mempertimbangkan kemungkinan perang siber,[3] baik sebagai elemen konflik bersenjata konvensional maupun sebagai proposisi yang berdiri sendiri. Namun ternyata pertimbangan tersebut mulai teralihkan setelah terjadinya serangan 9/11.[4] Kemudian ide ini kembali mencuat pada 2007 ketika Negara Anggota NATO, Estonia, mendapat serangan siber besar-besaran.[5]

Kekosongan dalam literatur hukum internasional yang membahas perang siber adalah sangat memprihatinkan. Mengingat baru-baru ini, model serangan siber semakin menunjukkan kesiapannya untuk terlibat dalam konflik bersenjata.[6] Hal ini juga diperkuat dengan munculnya kelompok siber lain yang siap untuk melakukan operasi siber berbahaya terhadap pihak-pihak yang terlibat konflik bersenjata.[7] Apakah negara-negara di dunia telah mempersiapkan hal ini atau tidak, mau tidak mau senjata siber telah menjadi hal yang pokok di dalam perang modern.[8]

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.[9] 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 siber sebagai cara untuk melemahkan sistem infrastruktur penting dan aset lawan.[10] Serangan dilakukan dengan menyerang target yang merupakan objek yang vital bagi keamanan nasional, keamanan ekonomi, serta kesehatan dan keselamatan masyarakat.[11] Fakta-fakta ini memperlihatkan bahwa terdapat ketidakpastian tentang parameter hukum yang tepat

[3] Jeffrey TG Kelsey, "Hacking into international humanitarian law: The principles of distinction and neutrality in the age of siber warfare" (2008) Mich Law Rev 1427 hlm. 12.

[4] Russell Buchan, "Cyber Warfare and the Status of Anonymous under International Humanitarian Law" (2016) 15:4 Chinese Journal of International Law 741–772 hlm. 21.

[5] *Ibid* hlm. 22.

[6] Michael N Schmitt, "The law of cyber warfare: quo vadis" (2014) 25 Stan L & Pol'y Rev 269 hlm. 1.

[7] Swanson, "The era of cyber warfare", *supra* note 2 hlm. 7.

[8] Kosmas Pipyros et al, "Cyberoperations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare" (2016) 24:1 Information & Computer Security 38–52 hlm. 12.

[9] J Markoff, "Internet attacks seen as more potent and complex" (2008) International Herald Tribune hlm. 20–24.

[10] *Ibid*.

[11] *Ibid*.

terkait perang siber.[12] Sehingga hal ini membuat negara-negara di dunia membutuhkan regulasi sebagai payung hukum yang dapat mengontrol fenomena ini.[13]

Artikel ini mecoba menawarkan pemikiran tentang bagaimana hukum perang siber dapat mulai diformulasikan. Artikel ini dimulai dengan membandingkan konflik di dunia maya dan konflik di dunia fisik dengan menggunakan senjata konvensional. Bagian kedua membahas tentang konsepsi kedaulatan siber. Artikel ini diakhiri dengan pembahasan bagaimana respon Hukum Humaniter Internasional (HHI) terhadap fenomena perang siber.

METODE

Jenis penelitian ini adalah penelitian yuridis normatif yaitu suatu proses untuk menemukan aturan hukum, asas-asas hukum dan doktrin-doktrin hukum dalam rangka menjawab permasalahan hukum yang dihadapi. Pendekatan penelitian yang digunakan adalah pendekatan undang-undang, pendekatan komparatif, dan pendekatan konseptual.

Sumber bahan hukum yang digunakan adalah bahan hukum primer (peraturan perundang-undangan, tulisan atau catatan resmi, atau juga risalah, yang terdapat dalam pembuatan peraturan dan perundang-undangan termasuk konvensi-konvensi internasional, sekunder (buku hukum, jurnal hukum, majalah hukum, artikel hukum, dan diperoleh dari internet dalam bentuk bacaan hukum dan kasus hukum) dan tersier (bahan hukum yang dapat memberikan petunjuk atau penjelasan untuk memperkuat bahan hukum primer dan sekunder, seperti yang berasal dari ensiklopedia dan kamus hukum). Teknik analisis dalam penelitian ini dilakukan dengan studi pustaka dan studi dokumenter.

HASIL DAN PEMBAHASAN

1. Konsepsi Kedaulatan Siber

Keberhasilan teknologi digital dalam mengembangkan aktivitas sosial, ekonomi, dan budaya telah membuat batas-batas konvensional kedaulatan negara menjadi tidak lagi dapat dikendalikan. Hal ini ditegaskan dengan hilangnya batas status

[12] Michael N Schmitt & Sean Watts, "The decline of international humanitarian Law Opinio Juris and the law of cyber warfare" (2015) 50 Tex Int'l LJ 189 hlm. 11.

[13] Bandingkan dengan Eric Schmidt & Jared Cohen, *The new digital age: Reshaping the future of people, nations and business* (Hachette UK, 2013) hlm. 47.

kependudukan warga negara menjadi sebuah komunitas masyarakat digital yang disebut dengan *digital society*.[14] Sehingga fenomena ini membuat negara-negara di dunia membutuhkan regulasi yang dapat mengontrol perkembangan dunia digital.[15] Hal ini mengindikasikan bahwa perkembangan teknologi digital merupakan sebuah eksperimen yang melibatkan entitas anarki, sehingga dalam mengatasinya harus melibatkan kekuatan penuh yang dimiliki otoritas negara. [16]

Pada kebutuhan awal, regulasi ini ditujukan untuk mengendalikan perang siber di dalam dunia bisnis agar tidak menyisakan terlalu banyak korban konsumen.[17] Namun, masifnya penetrasi teknlogi digital yang seiring dengan perubahan perilaku sosial manusia membuat negara-negara di dunia juga berusaha membangun ketahanan siber di bidang sosial-politik. Hal ini ditegaskan dengan fenomena bocornya data intelejen Amerika Serikat dan kasus Edward Snowden yang membuat Jerman tersadar untuk membangun regulasi ketahanan siber.[18] Melihat kasus Edward Snowden dan bocornya data intelejen Amerika Serikat membuat kepala bidang informasi, Komisi Informasi Jerman berkonsentrasi untuk membangun aturan khusus sebagai bentuk infrastruktur yang vital bagi masyarakat Jerman. Tidak berselang lama, konsep kedaulatan siber *(Cyber Sovereignity)* juga mulai diperkenalkan di dalam kesepakatan *non-aggression elements* Rusia – Tiongkok.[19] Meski batas-batas kedaulatan digital telah disepakati, namun di tahun 2016 Kaspersky Lab, perusahaan kamanan siber Rusia mengindikasikan bahwa sepanjang tahun tersebut Tiongkok justru meningkatkan serangan siber kepada Rusia.

Di Eropa, Prancis merupakan salah satu negara yang terus berkonsentrasi untuk menyusun konsep *Cyber Sovereignity* pada tingkat kerjasama antar negara.[20] Konsepsi *Cyber Sovereignty* Prancis didefinisikan sebagai kekuasaan atas masa kini yang

---

[14] Dirk Helbing, *Thinking ahead-essays on big data, digital revolution, and participatory market society* (Springer, 2015) hlm. 114.

[15] Bandingkan dengan Eric Schmidt & Jared Cohen, *The new digital age: Reshaping the future of people, nations and business* (Hachette UK, 2013) hlm. 47.

[16] Yunia Utami Indah Haloho, Xavier Nugraha, Atiqoh Farhan Maulani, "Analisis Penerapan No First Use Policy Dalam Penggunaan Senjata Nuklir: Sebuah Tinjauan Yuridis" (2020) 12:2 Jurnal Ilmiah Living Law 107-121 hlm.111.

[17] Charles Arthur, *Digital wars: Apple, Google, Microsoft and the battle for the Internet* (Kogan Page Publishers, 2014) hlm. 14.

[18] Klaus Vitt, "Die Digitalisierung der Verwaltung braucht effiziente föderale Kooperation" (2019) 12:1 der moderne staat–dms: Zeitschrift für Public Policy, Recht und Management hlm. 49.

[19] Fabio Rugge, *Confronting an" Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace* (Ledizioni, 2018) hlm. 89.

[20] Pierre Bellanger, "On Cyber Sovereignty" (2012) 3 Le Débat 149 hlm. 17.

merupakan merupakan tujuan sebuah bangsa, dipandu dan dimanifestasikan oleh penggunaan teknologi dan jaringan komputer. Hal ini ditegaskan oleh keseriusan Prancis dalam membangun batas minimum keamanan siber, melalui penguatan penyedia layanan keamanan siber dalam bisnis dan sosial, serta penguatan kerjasama politik berbasis *CSIRTs (Computer Security Incident Response Teams)*.[21] Pembahasan serius terhadap kedaulatan digital oleh Prancis, hal ini dilatarbelakangi oleh makin tingginya ketergantungan masyarakat terhadap GAFA (Google, Apple, Facebook and Amazon). Sehingga fenomena ini menuntut perlunya perangkat peraturan yang tidak bertentangan dan sesuai dengan *free movement and freedom*. Sehingga teknologi digital telah menandaskan bahwa kedaulatan siber yang dibentuk dalam ketahanan siber telah menjadi *unbundling and partial relocation* dari otoritas negara.

Hampir tidak dapat dipungkiri, dari berbagai negara yang telah menetapkan kedaulatan siber selaras dengan alasan keamanan data nasional setelah terjadinya kasus-kasus pembobolan penting yang berkaitan dengan rahasia negara.[22] Meski beberapa juga mendasarkan terhadap alasan ekonomis dari timbulnya fenomena perang ekonomi digital yang menghasilkan ketergantungan negara terhadap penguasa ekonomi dunia.[23] Sehingga muncul istilah balkanisasi internet di Rusia, China, dan Brasil yang mengatur ketat arus internet.[24] Hal ini menegaskan bahwa perkembangan teknologi digital telah benar-benar berhasil menetralisir kedaulatan sebuah negara. Saskia Sassen menambahkan bahwa internet dan kedaulatan merupakan dua hal yang sama-sama dinamis dan cenderung sering berubah.[25]

2. Serangan Siber yang Dinilai Lebih Efektif

Internet telah muncul sebagai alat yang kuat bagi fungsi-fungsi pemerintah, informasi, serta perdagangan dan jejaring sosial.[26] Bahkan internet telah menjadi cara untuk menyebarkan pesan-pesan ideologis dan politis.[27] Dengan meningkatnya

[21] *Ibid* hlm. 18–19.

[22] David P Fidler, *The Snowden Reader* (Indiana University Press, 2015) hlm. 179.

[23] Nick Marx, "Storage wars: Clouds, cyberlockers, and media piracy in the digital economy" (2013) 3:1 Journal of e-media studies hlm. 13.

[24] Sérgio Alves Jr, "The Internet balkanization discourse backfires" (2014) Available hlm. SSRN 2498753 hlm. 15.

[25] Saskia Sassen, "Interactions of the Technical and the Social: Digital Formations of the Powerful and the Powerless" (2012) 15:4 Information, Communication & Society 455–478 hlm. 21.

[26] Kim A Taipale, *Seeking Symmetry on the Information Front: Confronting Global Jihad on the Internet* (2007) hlm. 3.

[27] *Ibid*.

pemanfaatan internet untuk lebih dari sekadar fungsi ekonomi dan sosial, masyarakat internasional harus sadar bahwa internet juga dapat berfungsi sebagai alat melakukan operasi yang mengarah pada kehancuran, bahkan kematian. Contoh-contoh serangan siber terhadap negara-negara dalam sejarah menunjukkan implikasi yang besar ketika menggunakan internet sebagai senjata dalam perang.[28] Hal ini dibuktikan oleh fakta yang menunjukkan bahwa sistem perang informasi saat ini sedang dikembangkan dan digunakan oleh setidaknya 120 negara, termasuk Peru, Iran, Uni Emirat Arab, Kroasia, Vietnam, dan Rusia.[29]

Serangan siber 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 dipastikan meluncurkan serangan berbasis komputer atau serangan siber terlebih dahulu kepada lawan.[30] Serangan-serangan tersebut ditujukan kepada sistem-sistem yang mendukung distribusi energi dan telekomunikasi. Fakta ini ditegaskan oleh sebab seluruh aspek mulai dari transportasi, kesehatan, hingga operasi militer kini terhubung pada komputer.[31]

Beberapa kasus telah terbukti, seperti peretasan terhadap pemerintah Lithuania pada Juni 2008, serangan pada situs web pemerintah Estonia pada 2007.[32] Selain menjatuhkan banyak situs web pemerintah dan komersial yang kritis di Estonia, serangan ini juga menyebabkan nomor telepon darurat yang digunakan untuk memanggil ambulan dan dinas pemadam kebakaran tidak tersedia selama lebih dari satu jam. Akibatnya, keresahan sosial meluas dan menyebabkan 150 orang terluka dan satu orang Rusia tewas. Selain itu, pelanggaran email di Pentagon pada Juni 2007, dan peretasan situs web perusahaan telepon milik pemerintah Pakistan pada Januari 2003. Serta sekitar Agustus 2008, serangan *denial of service* (DDoS) terhadap situs web resmi

[28] Natasha Solce, "The battlefield of siberspace: The inevitable new military branch-the siber force" (2008) 18 Alb LJ Sci Tech 293 hlm. 300–301.

[29] Pipyros et al, "Cyberoperations and International Humanitarian Law", *supra* note 8 hlm. 14.

[30] Cara ini dikenal dengan model spionase siber atau juga disebut dengan eksploitasi siber. Michael N Schmitt, "The law of siber warfare: quo vadis" (2014) 25 Stan Pol Rev 269 hlm. 17.

[31] Libor Klimek, "combating attacks against Information Systems: eu Legislation and Its development" (2012) 6 Masaryk UJL & Tech 87 hlm. 1–3.

[32] *Ibid* hlm. 11.

Georgia, termasuk situs kantor Presiden, Kementerian Luar Negeri, dan Kementerian Pertahanan, yang menyebabkan masalah komunikasi di seluruh Georgia.[33]

Kasus di atas menunjukkan bahwa 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, maupun semantik.[34] Senjata siber menargetkan sistem operasi komputer, termasuk kode berbahaya, seperti virus, *worm*, *Trojan 44 Horses*, *DDoS*, dan *spyware*.[35]

Dengan kata lain, serangan siber dapat terdiri dari proses mengubah informasi yang masuk ke sistem komputer untuk menghasilkan kesalahan tanpa sepengetahuan pengguna/pemilik.[36] Perangkat yang terinfeksi ini kemudian terus-menerus menaati perintah dari penyerang. Efek besar dan data-data rahasia yang didapatkan dari proses serangan ini menjadikan serangan siber dinilai lebih efektif dan berbahaya daripada serangan konvensional. Inilah yang kemudian sangat membahayakan, mengingat tidak ada payung hukum yang pasti untuk dapat memberikan perlindungan.

3. Kebutuhan Regulasi Siber di Setiap Negara

Cybersecurity— sekarang setelah kerentanan siber menimbulkan risiko serius bagi kemakmuran, demokrasi dan harmoni sosial— telah menjadi fenomena politik, sosial, ekonomi dan teknologi yang kompleks dan mencakup semua.[37] Sejak pergantian abad, sifat dan ruang lingkup internet dan penggunanya telah berubah secara mendasar. Pada tahun 1995, diperkirakan 16 juta orang di seluruh dunia memiliki akses ke internet, dan semua pengguna mengaksesnya melalui *fixed-line connections*. Dua puluh tahun kemudian, lebih dari setengah populasi dunia sudah terhubung satu sama lain (*online*) dan—di antara mereka—lebih dari setengahnya mengakses internet melalui perangkat seluler. Lebih dari 20 miliar perangkat diproyeksikan akan terhubung *ke Internet of Things* (*IoT*) dalam kurun waktu lima tahun ke depan saja. Dunia maya telah menjadi bagian integral dari arus barang dan jasa, hal ini dapat dilihat dari dukungan untuk

[33] Pipyros et al, "Cyberoperations and International Humanitarian Law", *supra* note 8 hlm. 12.

[34] Bryan Harris, Eli Konikoff & Phillip Petersen, "Breaking the DDoS attack chain" (2013) Institute for Software Research hlm. 175.

[35] Susan W Brenner & Marc D Goodman, "In defense of siberterrorism: An argument for anticipating siber-attacks" (2002) U Ill JL Tech Pol 1 hlm. 29.

[36] *Ibid* hlm. 31.

[37] Istilah *cyber* digunakan dalam arti luas: "dari, berkaitan dengan, atau melibatkan komputer atau jaringan komputer (seperti Internet)" (www.merriam-webster. com / kamus / cyber).

infrastruktur kritis seperti listrik, air, perbankan, komunikasi dan transportasi dan untuk kontrol sistem industri, keamanan dan militer. Teknologi telah mengumpulkan banyak perhatian—khususnya, tindakan individu atau kerentanan sistem tertentu di negara-negara tertentu— bersama dengan cara konten diatur di internet

Berangkat dari hal tersebut, beberapa negara di Asia yang tengah berada di puncak transformasi digital mendorong kemajuan infrastruktur dan teknologi baru untuk meningkatkan kemampuan ekonomi mereka. Bersamaan dengan perkembangan positif ini, terdapat kebutuhan untuk melindungi output dan aset yang dihasilkan oleh digitalisasi dari ancaman yang terus berkembang.[38] Merespon hal ini, Indonesia—negara dengan pertumbuhan pengguna internet terbesar keempat di dunia—menghadapi peluang besar sekaligus ancaman signifikan dengan perkembangan teknologi digital dan internet.[39]

Bukan tanpa sebab, ruang digital Indonesia sangat berbeda dengan negara adikuasa digital dunia. Indonesia adalah pengekspor informasi netto yang membawa data jutaan penduduk yang juga menjadi salah satu negara dengan pengguna internet dengan jumlah tertinggi di dunia, dengan lebih dari 80 juta pengguna aktif mengakses layanan *online* di beberapa perangkat. Dengan sedikit atau tanpa kendali atas perangkat keras yang digunakan oleh "netizen" Indonesia, serta informasi yang dibawa melalui mereka, arsitektur keamanan nasional Indonesia rentan terhadap berbagai jenis intrusi digital, mulai dari spionase, *cybercrime*, *cyber-attacks* dan bahkan perang siber.[40]

Faktanya, tanpa sistem keamanan siber yang solid, 150 juta pengguna internet di Indonesia berisiko terjebak dalam episode tragis *Black Mirror*—Pada 2018, Indonesia mengalami lebih dari 200 juta serangan *cybercrime*[41].— Untuk menghadapi serangan-serangan ini, pemerintah telah mengeluarkan peraturan dan membentuk sejumlah lembaga di Kementerian Pertahanan Republik Indonesia, namun praktisnya langkah-

[38] Reveron, D. S. (2012). *An Introduction to National Security and Cyberspace. D. S. Reveron (eds.). Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington D. C.: Georgetown University Press.

[39] *Ibid.*

[40] Ciolan, I. M. (2014*). Defining Cybersecurity as The Security Issue of The Twenty First Century: A Constructivist Approach*. The Public Administration and Social Policies Review VI 1(12) hal. 120-136.

[41] Dilansir dari laman https://www.cnnindonesia.com/nasional/20180717140856-12-314780/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia pada tanggal 24 November 2019.

langkah itu tidak cukup. Indonesia perlu mempersenjatai diri dengan hukum yang lebih kuat dan membangun sistem dan industri keamanan digitalnya. [42]

Di sisi lain, Singapura menjalankan pendekatan yang berbeda dalam merespon persoalan *cybersecurity*. Praktisnya, Singapura sampai saat ini sudah melakukan berbagai macam upaya terkait dengan keamanan siber.[43] Upaya tersebut dimulai pada tahun 2005 melalui peluncuran perencanaan berupa *Cyber Security Masterplan*. Lalu dilanjutkan dengan peluncuran perencanaan lainnya yang berupa *Infocom Security Masterplan* pada tahun 2007. Pada tahun 2013, Singapura meluncurkan perencanaan lainnya yang berupa *National Cyber Security Masterplan* serta bersamaan juga dengan dibentuknya *National Cyber Security Research and Development Program*. Di tahun yang sama juga, Singapura merintis pembentukan *National Cyber Security Center*. Perkembangan selanjutnya terjadi di tahun 2015, Singapura membentuk *Cyber Security Agency* sebagai badan dalam Pemerintah Singapura yang didedikasikan untuk berurusan dengan isu keamanan siber. Kemudian, Singapura pada bidang keamanan siber menyelenggarakan kegiatan yang bernama *Singapore International Cyber Week*. Sehingga bukan tanpa sebab Singapura diganjar sebagai salah satu negara di Asia Tenggara yang berdasarkan pada *Global Security Index* yang dirilis oleh *International Telecommunications Union* di tahun 2017 dikategorikan sebagai negara dengan posisi pertama pada keamanan siber dibandingkan dengan negara lainnya yang ada di dunia. Kondisi yang demikian pada hal keamanan siber tersebut juga membuat Singapura menjadi negara yang terdepan juga di kawasan sekitarnya.

Sebagai pemuncak saat ini dalam peringkat *Global Cybersecurity Index*, Singapura mendapatkan gelar tersebut tak lepas karena fokus mereka dalam pendanaan perbaikan dan pembenahan undang-undang terkait *cybersecurity*. Dengan *masterplan* yang dibuat sejak tahun 2005, Singapura telah menyempurnakan dan memperluas undang-undang tentang keamanan siber, dan memerangi kejahatan dunia maya, dalam dua tahun terakhir ini. Lebih lanjut lagi, Pada April 2015, *Cyber Security Agency*[44] (Selanjutnya disebut *CSA*) dibentuk untuk mengembangkan strategi nasional dalam upaya mengatasi

[42] Eka Widi Astuti, Xavier Nugraha, "ISIS Ex-WNI or Indonesian Ex-ISIS? An Overview in the Perspective of National Law and International Law" (2021) 4:3 Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences 4187-4197 hlm. 4189.

[43] ASEAN. (2016). Cyber Security and Cybercrime in ASEAN. International Symposium on "*ASEAN Cyber Security and Cyber Crime Center: Possibility and Way Forward*".

[44] *Cyber Security Agency of Singapore* (CSA) Dibentuk pada bulan April 2015 di bawah naungan Perdana Menteri adalah badan nasional yang mengawasi strategi *cybersecurity*, operasi, pendidikan, penjangkauan, dan pengembangan ekosistem.

ancaman dunia maya. Strateginya ditujukan untuk mengoordinasikan upaya sektor publik dan swasta untuk melindungi sistem nasional di 10 sektor penting termasuk kekuasaan, transportasi, telekomunikasi dan perbankan meningkat ancaman dunia maya.[45]

Di belahan dunia yang lain, Amerika Serikat semakin memantapkan status mereka sebagai salah satu negara adikuasa digital melalui strategi kolaborasi antara sektor pemerintah dan sektor privat (*sector-based approach*).[46] Faktanya, Dari sekian banyak ancaman siber—baik ancaman terhadap sektor pemerintahan ataupun swasta—Amerika Serikat berhasil mengamankan data-data digital dari berbagai infrastruktur vital.[47] Hal ini dapat dibuktikan dengan tidak adanya kepanikan besar (*big chaos*) seperti yang seharusnya terjadi jika suatu infrastruktur vital terancam dan tidak adanya kelumpuhan sistem pemerintahan yang menghambat jalannya pemerintahan. Bahkan sebaliknya, Amerika Serikat yang melakukan serangan counter. Amerika menerapkan *IT underground* sebagai alat dari *cybersecurity strategy* untuk melakukan spionase siber melalui agensi intelijensinya yaitu *the big five* di bawah *United States Cyber Command*[48] (USCYBERCOM). Lima badan intelijen ini terdiri dari *National Security Agency* (NSA), *Defense Intelligence Agency* (DIA), *National Geospatial-Intelligence Agency* (NGA) dan *The National Reconnaissance Office* (NRO) dan lembaga independen *Central Intelligence Agency* (CIA).[49]

Kelima badan intelijen tersebut merupakan level operasional dari upaya implementasi strategi, dimana peran strategis diperankan *oleh Department of Defense* (DoD).[50] Kebijakan-kebijakan dalam level strategis memunculkan pemikiran-pemikiran bersifat strategis berupa doktrin-doktrin yang kemudian direspon dalam level operasional berupa tindakan-tindakan yang bersifat taktik, teknik, dan operasional guna mengontrol perkembangan siber di Amerika Serikat. Kolaborasi dan integrasi kedua level tersebut merupakan modal utama dalam menghadapi ancaman siber serta

---

[45] Carr A. & Wallis, J. (2016). *An Introduction to Asia-Pacific Security. J. Wallis & A. Carr (eds) Asia-Pacific Security: An Introduction.* Washington, DC: Georgetown University Press.

[46] Walter Bohmayr, Stefan Deutscher, & David Mkrtchian, *Towar A Model For Public-Private Collaboration in Cybersecurity*, The Boston Consulting Group, Inc., 2018

[47] Jupling, "*The Protection of Critical Infrastructures*," special report, Oct 2007, hlm. 20

[48] Badan ini bertugas untuk memfasilitasi integrasi operasi *cyberspace* untuk dinas militer dan mengsinkronisasi misi *cyber* dan usaha peperangan, serta menyediakan dukungan untuk otoritas sipil dan partner internasional.

[49] Buzan, Barry. 1998. *Security: A Framework for Analysis. Boulder*: Lynne Reinner Publishers.

[50] GAO. 2011. *Defense Departement Cyber Effort: DOD Faces Challenges In Its Cyber Activity*. Washington: US Government Accountability Office

mengamankan infrastruktur vital pemerintahan itu sendiri. Dapat dikatakan kolaborasi ini memiliki peran ganda, berperan sebagai penjaga keamanan siber Amerika Serikat, juga berperan dapat sebagai penyerang dalam *cyber warfare*.[51]

Negara yang tidak memiliki regulasi keamanan dan ketahanan siber seperti Indonesia, agaknya akan sulit untuk membentuk tembok pertahanan siber. Jangankan untuk menahan gempuran perang siber, dalam konteks menghadapi konflik siber di lingkup internal negara, maka akan sulit menghadapinya. Sementara di Indonesia, pada tahun 2018, pengguna layanan internet telah mencapai 171,17 juta dengan penetrasi 64,8% dari seluruh kalangan dan usia. [52] Pada laporan lainnya, Indonesia menduduki peringkat ketiga sebagai negara dengan jumlah pengguna internet terbesar di dunia.[53] Bahkan, Indonesia merupakan peringkat pertama dalam hal pertumbuhan pengguna internet,[54] dan peringkat keempat dalam kepemilikan telepon genggam di dunia.[55] Ditambah kasus *e-KTP* tahun 2018, sebagaimana data digital penduduk Indonesia disinyalir berada di perusahaan asing dan tersebar di luar negeri.[56] Meski Kementerian Dalam Negeri (Kemendagri) memberikan garansi keamanan, namun hal ini tidak menjadi jaminan.[57] Hal ini disebabkan oleh belum adanya perangkat hukum keamanan data digital yang terintegrasi dan tidak adanya kerjasama internasional terkait keamanan data digital yang ditransmisikan dan diakses di luar yurisdiksi hukum Indonesia. Sehingga hal ini menegaskan diperlukannya regulasi keamanan dan ketahanan siber di Indonesia.

Keamanan dan ketahanan siber bagi sebuah negara dapat didefinisikan sebagai kemampuan untuk menguasai dan mengendalikan akses dan transaksi atas data digital secara penuh.[58] Selain itu, berkaca dari kasus peretasan data pribadi konsumen dalam

---

[51] *Ibid.*

[52] Pusat Kajian Komunikasi Universitas Indonesia, "Asosiasi Penyelenggara Jasa Internet Indonesia, 2018" (2018) Profil Pengguna Internet Indonesia 2018.

[53] Indonesia: share of internet users by age group 2019", online: *Statista* <https://www.statista.com/statistics/997264/share-of-internet-users-by-age-group-indonesia/>.

[54] "Global Digital Report 2019", online: *We Are Social* <https://wearesocial.com/global-digital-report-2019>.

[55] "The World Factbook — Central Intelligence Agency", online: <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html>.

[56] "Mendagri Sebut Data e-KTP 110 Juta Warga Indonesia Ada di Perusahaan Asing", online: <https://news.detik.com/berita/d-3353022/mendagri-sebut-data-e-ktp-110-juta-warga-indonesia-ada-di-perusahaan-asing>.

[57] Gito Yudha Pratomo, "Kemendagri Bantah Server e-KTP di Luar Negeri", online: *teknologi* <https://www.cnnindonesia.com/teknologi/20141117172756-206-12059/kemendagri-bantah-server-e-ktp-di-luar-negeri>.

[58] Reinhard Posch, "Digital sovereignty and IT-security for a prosperous society" in *Informatics in the Future* (Springer, Cham, 2017) 77 hlm. 24.

penggunaan teknologi finansial, Equifax – sebuah perusahaan tekfin internasional,[59] sehingga hal tersebut mengisyaratkan harus adanya adanya perlindungan hak privasi warga negaranya di tengah sistem demokratis.

Berbagai macam kasus yang telah disebutkan setidaknya sudah menjadi desakan untuk segera dapat memiliki aturan ketahanan siber yang mumpuni menjaga kedaulatan digital Indonesia. Pengaturan kedaulatan digital juga harus menjadi bagian dari kerja sama internasional, sehingga tidak hanya dapat memproteksi dunia digital Indonesia, namun juga dapat memberi manfaat besar bagi perkembangan bangsa. Sebagaimana negara-negara yang telah berhasil memfokuskan diri dalam membangun pengaturan ketahanan siber, juga menarik negara lain untuk ikut serta membangun kerjasama keamanan siber.[60]

Meski problematika infrastruktur digital yang dapat mendukung ketahanan siber belum memadai, serta besarnya investasi terhadap hal ini semakin dilematis, Indonesia sudah sepatutnya memiliki payung hukum ketahanan siber. Sehingga ada empat fokus yang harus diperhatikan dalam menyusun regulasi ketahanan siber, yakni yang pertama, terkait keamanan data digital yang dapat menjamin tidak ada pihak yang dapat memanfaatkan data tanpa hak atau diberi hak bagi negara. Kedua, terkait kemanfaatan digital yang meliputi pengembangan infrastruktur digital dan pengaturan persaingan usaha berbasis digital. Ketiga, kerjasama siber dalam rangka penegakan kedaulatan digital mengingat sifat nirbatas dunia digital. Dan keempat, terkait penegakan hukum berupa ketegasan sanksi terhadap pelanggaran kedaulatan digital agar perlindungan kedaulatan digital benar-benar dapat berdampak.

---

[59] Equifax merupakan perusahaan pelaporan kredit terbesar yang ada di Amerika Serikat. Equifax menawarkan jasa pemantauan kartu kredit dan perlindungan pencurian data agar tidak jatuh ke tangan orang yang tidak bertanggung jawab. Namun ternyata, perusahaan ini justru berhasil diretas oleh *hacker* yang sampai saat ini belum diketahui identitasnya. Akibatnya, 143 juta data nasabah dari Equifax berhasil dicuri oleh para peretas.Seena Gressin, "The equifax data breach: What to do" (2017) 1 US Federal Trade Commission, as viewed Oct hlm. 4.

[60] Sebagaimana yang dilakukan negara-negara seperti Prancis, Jerman dengan Uni Eropa. Begitupula dengan Rusia, China, Amerika, Singapura dan lainnya. Di NATO, masing-masing negara anggota memiliki organisasi keamanan cyber dan membangun kerjasama antar negara dengan nama *NATO Cooperative Cyber Defense Centre of Excellence* (NATO CCD COE). Murat Dogrul, Adil Aslan & Eyyup Celik, *Developing an international cooperation on cyber defense and deterrence against cyber terrorism* (IEEE, 2011) hlm. 7–9.

4. Bagaimana Hukum Humaniter Internasional Merespons?

Pertanyaan batas-batas pengaturan dalam keadaan apa serangan siber dapat dianggap sebagai konflik bersenjata, maka HHI harus masuk pada ruang ini. Pertanyaan ini menjadi penting, sebab jawabannya memberikan panduan kepada negara-negara tentang bagaimana mereka dapat merespon jika mendapat serangan siber, khususnya berkaitan dengan norma-norma hukum internasional.[61]

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. Juga mengatur tentang *jus ad bellum*, atau *"law to war,*[62] sebagai legalitas untuk menggunakan angkatan bersenjata dalam perang.

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.[63] 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, Konvensi Jenewa dan Protokol Tambahan seharusnya dapat melihat "konflik bersenjata" dengan cara yang cukup luas.[64] Sehingga prinsip-prinsip dasar HHI memperjelas bahwa HHI didirikan berdasarkan gagasan bahwa korban konflik bersenjata berhak atas perlindungan.[65]

Langkah pertama yang jelas adalah mendefinisikan apa itu senjata siber. Dari perspektif HHI, jika kemampuan dunia maya berarti "senjata, sarana, atau metode peperangan", hal itu tidak hanya memicu peninjauan senjata berdasarkan Pasal 3648, tetapi juga di bawah semua larangan dan pembatasan HHI terkait. Saat ini, tidak ada konsensus internasional tentang definisi senjata siber.

---

[61] Kelsey, "Hacking into international humanitarian law", *supra* note 3 hlm. 11.

[62] Hilaire McCoubrey, *International humanitarian law: modern developments in the limitation of warfare* (Routledge, 2019) hlm. 1.

[63] Swanson, "The era of cyber warfare", *supra* note 2 hlm. 14.

[64] Jung-Ho Eom et al, *Cyber military strategy for cyberspace superiority in cyber warfare* (IEEE, 2012) hlm. 29.

[65] Hilaire McCoubrey, *International humanitarian law: the regulation of armed conflicts* (Dartmouth Pub Co, 1990) hlm. 1.

Di bawah ini adalah tiga kemungkinan formulasi definisi. Pertama, *Commentary to Rule 103 of the Tallinn Manual 2.0* mendefinisikan senjata siber sebagai "alat perang dunia maya yang digunakan, dirancang, atau dimaksudkan untuk digunakan untuk menyebabkan cedera, atau kematian, orang atau kerusakan, atau penghancuran, objek, yaitu, yang mengakibatkan konsekuensi yang diperlukan untuk kualifikasi operasi siber sebagai serangan." Dan, lebih khusus lagi, sarana siber akan mencakup perangkat, materi, instrumen, mekanisme, peralatan, atau perangkat lunak dunia maya yang digunakan, dirancang , atau dimaksudkan untuk digunakan untuk melakukan serangan siber.

Selanjutnya, mengartikulasikan definisi dengan cara yang sedikit berbeda, penulis yang dihormati Thomas Rid dan Peter McBurney mengkonseptualisasikan senjata siber sebagai kode komputer yang "digunakan, atau dirancang untuk digunakan, dengan tujuan mengancam atau menyebabkan kerusakan fisik, fungsional, atau mental. untuk struktur, sistem, atau makhluk hidup." Terakhir, dalam peraturannya tentang Tinjauan Hukum Senjata dan Kemampuan Siber, Angkatan Udara Amerika Serikat mendefinisikan senjata sebagai "perangkat yang dirancang untuk membunuh, melukai, melumpuhkan, atau melumpuhkan sementara orang, atau menghancurkan, merusak, atau melumpuhkan properti atau materi untuk sementara."

Untuk penghargaannya, para pendukung peraturan Angkatan Udara AS mengakui dan menyoroti bahwa sebagian besar kemampuan dunia maya bukanlah perangkat. Sebaliknya, mereka adalah paket atau teknik perangkat lunak. Dengan demikian, peraturan Angkatan Udara mendefinisikan konsep kemampuan siber dan menyatakan "kemampuan siber Angkatan Udara yang memerlukan tinjauan hukum sebelum pekerjaan apa pun adalah muatan perangkat atau perangkat lunak apa pun yang dimaksudkan untuk mengganggu, menyangkal, menurunkan, meniadakan, merusak atau menghancurkan komputer musuh. sistem, data, aktivitas, atau kemampuan."

Sebagai catatan, Angkatan Udara A.S. adalah yang pertama dari dinas militer A.S. yang mengeluarkan peraturan yang secara khusus menangani masalah cara meninjau kemampuan dunia maya. Benang merah yang mengalir melalui semua definisi adalah bahwa senjata dunia maya adalah instrumen bahaya. Dari diskusi di atas, secara logis memberikan identifikasi bahwa serangan siber dapat dikategorikan konflik bersenjata, meskipun penggunaan komputer sebagai senjata bukanlah metode perang

konvensional. Sementara serangan siber menggunakan teknologi modern yang tidak pernah diprediksi maupun diperhitungkan selama penyusunan Konvensi Jenewa dan Protokol Tambahan I.[66] Namun disisi lain, HHI tidak adaptif dengan perubahan teknologi. Sehingga HHI harus berubah dan dikembangan untuk dapat menjelaskan bagaimana perlindungan kemanusiaan baru.[67]

Protokol Tambahan I 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. [68] 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.

Mirip dengan senjata nuklir, senjata siber dapat dikategorikan sebagai *sui generis*.[69] Sehingga harus diatur oleh seperangkat hukum yang unik dan dengan karakteristik tertentu juga. Namun demikian, senjata siber, seperti halnya senjata nuklir, yang juga 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.

Akhirnya, tinjauan tentang senjata siber mungkin bermasalah. Mengingat sifat kewajiban HHI yang berpusat pada Negara, sama sekali tidak mengherankan bahwa penerapan sementara Pasal 36 cukup luas. Pada akhirnya, merupakan kebijaksanaan masing-masing Negara untuk menentukan waktu yang paling tepat untuk peninjauan senjata guna memastikan kepatuhan terhadap HHI. Jika penilaian Negara terhadap senjata baru yang sedang dikembangkan mengarah pada kesimpulan bahwa penggunaannya di masa depan akan melanggar HHI, keputusan untuk menghentikan pengembangan senjata harus diambil. Dari sudut pandang ICRC, harus ada penilaian legalitas senjata baru di "studi, pengembangan, akuisisi atau adopsi". Tolok ukur ini akan mencakup tahapan tradisional dari proses pengadaan senjata, yaitu, “tahap awal dari

---

[66] Knut Dörmann, “Applicability of the Additional Protocols to computer network attacks” (2004) Int’l Committee of the Red Cross (November 19, 2004)//http://www icrc org/eng/assets/files/other/applicabilityofihltocna pdf hlm. 29.

[67] *Information warfare and international law*, by Lawrence T Greenberg, Seymour E Goodman & Kevin J Soo Hoo, Google Scholar (NATIONAL DEFENSE UNIV WASHINGTON DC, 1998) hlm. 28–29.

[68] *Ibid* hlm. 30.

[69] McCoubrey, *supra* note 63 hlm. 244.

fase penelitian (yaitu, konsepsi, studi), fase pengembangan (yaitu, pengembangan dan pengujian prototipe), dan fase akuisisi (termasuk pengadaan "off-the-shelf").

Sekali lagi, dengan menetapkan bahwa pengembangan sebagian besar senjata siber diselimuti kerahasiaan yang ekstrem, diasumsikan bahwa proses pengembangan senjata siber pada dasarnya lebih dinamis dan berulang dibandingkan dengan senjata lain yang harus ditinjau. Alasan untuk kesimpulan ini adalah bahwa senjata siber, khususnya yang sangat canggih, sedang dirancang untuk melakukan tindakan yang sangat kompleks dalam kaitannya dengan target tertentu.

Efek penggunaan senjata siber yang dapat diantisipasi secara wajar dapat berubah meskipun tujuan penggunaannya atau konsep operasinya mungkin tetap konstan. Arti penting dari kondisi ini adalah bahwa penilaian hukum yang diperbarui harus dilakukan ketika perubahan telah dilakukan pada senjata siber yang secara substansial mengubah kinerja operasional senjata siber atau efek yang dimaksudkan. Oleh karena itu, penasihat hukum yang ditugaskan untuk memberikan nasihat tersebut harus peka terhadap dinamika ini dan menanggapinya dengan tepat. Seperti isu-isu lain dalam HHI, penasihat hukum sangat penting untuk proses dan menambah nilai yang sangat besar.

Tidak diragukan lagi, ada berbagai masalah hukum, kebijakan, dan praktis yang signifikan dan kompleks terkait dengan tinjauan senjata siber di bawah HHI. Diskusidi atas hanyalah contoh dari masalah-masalah itu dan harus dilihat sebagai panggilan yang jelas untuk penelitian dan studi yang lebih besar di bidang yang sangat penting ini. Sifat embrionik penelitian ini diilustrasikan oleh fakta bahwa tidak ada konsensus bahkan pada definisi yang tepat dari senjata siber, apalagi semua implikasi yang mengalir dari penerapan prinsip dan konsep tinjauan senjata HHI tradisional ke teknologi yang muncul ini. Ambiguitas ini, bagaimanapun, tidak berarti bahwa HHI tidak berlaku secara penuh. Itu tidak. The Tallinn Manual Experts memberikan kontribusi penting untuk membuat sketsa pandangan yang masuk akal tentang *lex lata* dengan komentar yang mendalam sehubungan dengan tinjauan senjata siber. Sekarang terserah kepada Negara-negara untuk membangun upaya ini karena hukum internasional mencerminkan konsensus di antara Negara-negara mengenai norma-norma yang mengatur interaksi mereka.

Meskipun diakui spekulatif tentang bagaimana konten, interpretasi, dan penerapan HHI terkait tinjauan hukum senjata siber dapat matang dan berkembang dalam beberapa dekade mendatang, penulis ini percaya bahwa evolusi normatif aspek

HHI ini akan cukup menantang. . Alasan utama untuk kesimpulan ini adalah lingkungan keamanan di sekitar senjata siber. Yaitu, tidak mungkin untuk melebih-lebihkan keunikan lingkungan di mana senjata siber disusun, dikembangkan, dan pada akhirnya digunakan. Gudang senjata dunia maya diselimuti misteri, kerahasiaan, dan penyangkalan. Negara tidak secara terbuka mengakui pengembangan, kemampuan, atau penggunaannya. Selain itu, di dunia maya, seseorang dapat bersembunyi di balik alias, menggunakan server proxy, dan secara diam-diam memperbudak komputer lain sehingga membuat atribusi menjadi sangat sulit.

Selain itu, beberapa Negara percaya bahwa mempertahankan ambiguitas hukum di dunia maya mendorong fleksibilitas operasional dan strategis. Dan, secara relatif, senjata siber dapat dikembangkan dengan infrastruktur teknologi yang sederhana. Pertimbangan-pertimbangan ini, serta pertimbangan-pertimbangan lainnya, membuat sangat tidak mungkin bahwa Negara-negara akan menyetujui peraturan khusus apapun mengenai senjata siber. Kemungkinan besar Negara-negara akan menyetujui norma-norma hukum tertentu yang terkait dengan peningkatan perlindungan dari serangan siber terhadap infrastruktur penting tertentu daripada peraturan tentang senjata siber. Tentu saja, lingkungan keamanan bukan satu-satunya kendala. Ada orang lain. Misalnya, tidak ada definisi otoritatif tentang apa yang bahkan merupakan senjata siber dan sifat proses peninjauan senjata yang berpusat pada negara membuat regulasi internasional menjadi sangat bermasalah.

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.[70] Sehingga pada kesimpulannya, HHI harus berbenah untuk dapat masuk ke dalam pengaturan yang dapat memayungi fenomena perang siber ini.

Mengingat semua hal di atas, penulis percaya bahwa arsitektur normatif dari proses peninjauan senjata HHI akan berada di ujung tanduk dari setiap perubahan, artinya HHI harus terus menyempurnakan dan menyesuaikan dirinya dengan perkembangan zaman.

[70] Swanson, "The era of cyber warfare", *supra* note 2 hlm. 15.

KESIMPULAN

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. Sehingga prinsip-prinsip HHI 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 masing-masing negara 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 siber akan tetap ada.

UCAPAN TERIMA KASIH

Puji syukur kepada kehadirat Allah SWT atas segala rahmat dan hidayahnya, serta sholawat dan salam kepada Nabi Muhammad SAW. Penulis mengucapkan terimakasih yang sebesar-besarnya kepada editorial dan seluruh pengelola Jurnal Kawruh Abiyasa yang telah berkenan memproses artikel ini. Penulis juga mengucapkan terimakasih kepada rekan-rekan yang telah mendukung penulisan artikel ini, sehingga artikel ini dapat terselesaikan dengan baik.

DAFTAR PUSTAKA

Buku

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

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

Helbing, Dirk, *Thinking ahead-essays on big data, digital revolution, and participatory market society* (Springer, 2015).

McCoubrey, Hilaire, *International humanitarian law: modern developments in the limitation of warfare* (Routledge, 2019).

———, *International humanitarian law: the regulation of armed conflicts* (Dartmouth Pub Co, 1990).

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

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

Jurnal:

Alves Jr, Sérgio, "The Internet balkanization discourse backfires" (2014) Available at SSRN 2498753.

Bellanger, Pierre, "On Digital Sovereignty" (2012) 3 Le Débat 149–159.

Brenner, Susan W & Marc D Goodman, "In defense of cyberterrorism: An argument for anticipating cyber-attacks" (2002) U Ill JL Tech & Pol'y 1.

Buchan, Russell, "Cyber Warfare and the Status of Anonymous under International Humanitarian Law" (2016) 15:4 Chinese Journal of International Law 741–772.

Dörmann, Knut, "Applicability of the Additional Protocols to computer network attacks" (2004) Int'l Committee of the Red Cross (November 19, 2004)//http://www icrc org/eng/assets/files/other/applicabilityofihltocna pdf.

Gressin, Seena, "The equifax data breach: What to do" (2017) 1 US Federal Trade Commission, as viewed Oct.

Harris, Bryan, Eli Konikoff & Phillip Petersen, "Breaking the DDoS attack chain" (2013) Institute for Software Research.

Indonesia, Pusat Kajian Komunikasi Universitas, "Asosiasi Penyelenggara Jasa Internet Indonesia, 2015" (2014) Profil Pengguna Internet Indonesia 2014.

Kelsey, Jeffrey TG, "Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare" (2008) Michigan Law Review 1427–1451.

Klimek, Libor, "combating attacks against Information Systems: eu Legislation and Its development" (2012) 6 Masaryk UJL & Tech 87.

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

Marx, Nick, "Storage wars: Clouds, cyberlockers, and media piracy in the digital economy" (2013) 3:1 Journal of e-media studies.

Pipyros, Kosmas et al, "Cyberoperations and International Humanitarian Law: A review of obstacles in applying International Law rules in Cyber Warfare" (2016) 24:1 Information & Computer Security 38–52.

Posch, Reinhard, "Digital sovereignty and IT-security for a prosperous society" in *Informatics in the Future* (Springer, Cham, 2017) 77.

Sassen, Saskia, "Interactions of the Technical and the Social: Digital Formations of the Powerful and the Powerless" (2012) 15:4 Information, Communication & Society 455–478.
Schmitt, Michael N, "The law of cyber warfare: quo vadis" (2014) 25 Stan L & Pol'y Rev 269.
Schmitt, Michael N & Sean Watts, "The decline of international humanitarian Law Opinio Juris and the law of cyber warfare" (2015) 50 Tex Int'l LJ 189.
Solce, Natasha, "The battlefield of cyberspace: The inevitable new military branch-the cyber force" (2008) 18 Alb LJ Sci & Tech 293.
Swanson, Lesley, "The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict" (2010) 32 Loy LA Int'l & Comp L Rev 303.
Vitt, Klaus, "Die Digitalisierung der Verwaltung braucht effiziente föderale Kooperation" (2019) 12:1 der moderne staat–dms: Zeitschrift für Public Policy, Recht und Management.

Internet:

Pratomo, Gito Yudha, "Kemendagri Bantah Server e-KTP di Luar Negeri", online: *teknologi* <https://www.cnnindonesia.com/teknologi/20141117172756-206-12059/kemendagri-bantah-server-e-ktp-di-luar-negeri>.

"Global Digital Report 2019", online: *We Are Social* <https://wearesocial.com/global-digital-report-2019>.
"Indonesia: share of internet users by age group 2019", online: *Statista* <https://www.statista.com/statistics/997264/share-of-internet-users-by-age-group-indonesia/>.
"Mendagri Sebut Data e-KTP 110 Juta Warga Indonesia Ada di Perusahaan Asing", online: <https://news.detik.com/berita/d-3353022/mendagri-sebut-data-e-ktp-110-juta-warga-indonesia-ada-di-perusahaan-asing>.
"The World Factbook — Central Intelligence Agency", online: <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2119rank.html>.