

## **PENERAPAN HUKUM HUMANITER INTERNASIONAL DALAM KONFLIK SIBER**

**Helen Intania Surayda, Ahmad Dwi Nuryanto, Dedi Suwandi, Ismoro Hartono Ilham**

Fakultas Hukum, Universitas Semarang, Semarang

*e-mail* : intaniahelen@gmail.com

### **ABSTRAK**

Perang siber adalah suatu kondisi konflik dengan menggunakan perkembangan teknologi informasi dan komunikasi dimana menjadi sebuah fenomena sosial dalam relasi internasional yang menjadi masalah serius bagi bangsa-bangsa di dunia dalam membangun stabilitas internasional. Menghadapi variasi bentuk perang siber, dibutuhkan adanya proses pembangunan nasional berbasis keamanan siber/cyber security sebagaimana telah dilakukan oleh beberapa bangsa-bangsa di dunia. Perang siber sesungguhnya merupakan bentuk dari perang dunia ketiga yang sudah terjadi. Kekosongan dalam literatur hukum internasional membuat model serangan siber semakin menunjukkan kesiapannya untuk terlibat dalam konflik bersenjata. Konflik siber, yang melibatkan serangan terhadap sistem komputer dan jaringan digital, menimbulkan pertanyaan kompleks mengenai bagaimana prinsip-prinsip hukum humaniter yang ada dapat diterapkan dalam konteks konflik ini. Menggunakan metode penelitian yuridis normatif (*legal study research*) yang bersifat kualitatif dengan pendekatan perundang-undangan, konseptual dan kasus dari bahan primer dan sekunder. Tantangan HHI dalam mengatur konflik siber mulai dari definisi, pelacakan pelaku, perlindungan masyarakat, sampai penyesuaian hukum dengan teknologi baru. Diperlukan pembaruan hukum, peningkatan kerja sama antar negara, dan penguatan cara penegakan hukum agar perlindungan kemanusiaan tetap terjaga di zaman digital. HHI dapat diterapkan pada konflik siber tetapi perlu adaptasi melalui instrumen baru atau interpretasi progresif sebagaimana Kasus Rusia-Ukraina yang menjadi bukti urgensi penyesuaian hukum.

***Kata Kunci : Dinamika, Humaniter, Era Siber.***

### **ABSTRACT**

Cyberwarfare is a conflict situation that utilizes developments in information and communication technology. It has become a social phenomenon in international relations and poses a serious problem for nations worldwide in building international stability. Facing the various forms of cyberwarfare, a national development process based on cybersecurity/cybersecurity is necessary, as has been implemented by several nations worldwide. Cyberwarfare is actually a form of World War III, which is already underway. The gap in international legal literature makes cyberattack models increasingly demonstrate their readiness to engage in

armed conflict. Cyberconflict, which involves attacks on computer systems and digital networks, raises complex questions about how existing principles of humanitarian law can be applied in this conflict context. This study utilizes a qualitative, normative juridical research method (legal studies) with a legal regulatory approach, conceptualization, and case studies from primary and secondary sources. The challenges of IHL in regulating cyberconflict range from definition, perpetrator tracking, community protection, to adapting the law to new technologies. Legal reform, increased cooperation between states, and strengthened law enforcement are needed to ensure humanitarian protection in the digital age. IHL can be applied to civil conflicts, but it requires adaptation through new instruments or progressive interpretations, as in the Russia-Ukraine case, which demonstrates the urgency of legal adjustments.

**Keywords :** *Dynamics, Humanitarian, Cyber Era.*

## PENDAHULUAN

Era digitalisasi adalah era yang di mana manusia dalam kehidupan kesehariannya dilakukan dengan banyak menggunakan teknologi digital sebagai perkembangan akan kemajuan teknologi dan komunikasi. Konflik siber dapat didefinisikan sebagai suatu bentuk konflik yang memanfaatkan perkembangan teknologi informasi dan komunikasi, yang berimplikasi sebagai sebuah fenomena sosial dalam konteks hubungan internasional, serta menjadi isu serius dalam upaya membangun stabilitas internasional bagi semua bangsa di dunia.. Konflik siber menjadi permasalahan penting untuk dibahas karena konflik siber adalah sebuah kenyataan yang telah terjadi bahkan akan menjadi tren dari konflik modern. Konflik siber memiliki berbagai bentuk dan oleh karena itu, penanganannya memerlukan proses perencanaan dan pelaksanaan pembangunan nasional yang berlandaskan pada keamanan siber (*cyber security*), sebagaimana yang telah diterapkan oleh sejumlah negara di seluruh dunia.

Perang siber memiliki banyak bentuk yang berbeda, jadi untuk menghadapinya,

diperlukan pengembangan nasional yang fokus pada keamanan siber seperti yang telah dilakukan oleh beberapa negara di seluruh dunia. Amerika Serikat telah mempersiapkan diri menghadapi ancaman perang siber sejak tahun 2009 dengan mendirikan sebuah lembaga militer siber yang disebut *United States Cyber Command (USCYBERCOM)* yang berada di bawah *United States Strategic Command (US-STRATCOM)*. Selain itu, kementerian pertahanan Amerika Serikat (U.S. DoD) juga telah menciptakan angkatan tempur internet dan dunia maya sebagai angkatan keempat, setara dengan angkatan darat, laut, dan udara.

Sebelum Australia menciptakan CSOC, Inggris sebenarnya sudah membuat pertahanan siber dengan nama yang sama yaitu "*cyber security operations center (CSOC)*." Sejak tahun 2008, aliansi NATO juga telah membangun pertahanan siber yang dikenal sebagai NATO CCD COE yang berlokasi di Estonia. Selain negara-negara Eropa Barat, Rusia dan Cina juga telah mengembangkan kemampuan siber untuk menghadapi ancaman perang siber. Cina bahkan telah membentuk kelompok siber yang disebut "*blue Army*" yang

bertugas melindungi negara dari serangan siber dan berbasis di Guangzhou, Cina Selatan.

Perang siber pertama kali terjadi pada tahun 2007 ketika Rusia menyerang Estonia. Serangan siber ini berhasil mengacaukan jaringan keuangan, situs presiden, perdana menteri, parlemen, partai politik, perusahaan, serta situs berita. Perang siber juga terjadi pada 9 Juni 2009 ketika Korea Utara menyerang Korea Selatan dengan menyebarkan virus yang menginfeksi sekitar 30.000-60.000 komputer di Korsel. Selain itu, sekitar 166.000 komputer yang terinfeksi dari 74 negara ditugaskan untuk menyerang situs web pemerintah Korsel termasuk perbankan.<sup>1</sup>

Richard A. Clarke and Robert K. Knake dalam karya mereka yang berjudul “*Cyber War The Next Threat to National Security and What to Do About It*,” berargumentasi bahwa konflik dunia ketiga sebenarnya telah terjadi dalam bentuk konflik siber. Sejarah mencatat, pada tahun 1998 konflik siber telah dialami oleh Indonesia dengan Cina dan Taiwan, kemudian di tahun 1999 berkonflik dengan Portugal. Serangan siber berupa *worm stuxnet* juga pernah dialami oleh Indonesia, dampak respon dari sikap Indonesia dalam kasus nuklir Iran dengan dugaan pelaku oleh Amerika Serikat dan Israel. Tidak hanya itu, konflik siber dengan Malaysia juga dialami oleh Indonesia terkait isu agama dengan menggunakan metode

infiltrasi yang melibatkan hacker dari Indonesia dan Malaysia, serta selanjutnya antara Indonesia dan Australia, sebagaimana dilaporkan oleh *Sydney Morning Herald* pada tanggal 31 Oktober 2013, muncul isu terkait penyadapan terhadap pemerintahan Indonesia melalui penggunaan fasilitas gedung kedutaan negara Australia.<sup>2</sup>

Status anonim sebagai "tentara" dan alat serang seringkali terlibat dalam konflik siber. Hukum humaniter internasional belum membahas status anonim sampai saat ini. Tidak peduli apakah negara-negara di seluruh dunia mempersiapkan hal ini, senjata siber telah menjadi komponen penting dalam perang kontemporer. Peperangan tidak lagi hanya terdiri dari invasi atau serangan fisik antara negara-negara yang memiliki kekuatan militer yang berbeda. Jenis konflik baru ini menggunakan teknologi untuk menghancurkan infrastruktur yang sangat penting.<sup>3</sup> Tanggal 23 November 2001, di Kota Budapest, Hongaria, *Convention on Cyber Crime* telah dibuat dan disetujui. Ini menjadi bagian dari *European Treatt Series* dengan nomor 185.<sup>4</sup>

Dengan landasan keterangan dari latar belakang yang telah dijelaskan di atas bahwa perkembangan teknologi siber telah membawa tantangan baru dalam penerapan hukum humaniter internasional yang juga dikenal sebagai hukum perang. Konflik siber, yang melibatkan serangan terhadap sistem komputer dan jaringan digital,

<sup>1</sup> Badri, M. 2012. *Perang Cyber Dalam Dinamika Komunikasi Internasional*. Komunikasi Militer. Buku Liter. Jakarta: Mata Padi Pressindo, Universitas Prof. Dr. Moestopo Jakarta dan ASPIKOM.

<sup>2</sup> Nur Khalimatus Sa'diyah dan Ria Tri Vinata. 2016. *Rekonstruksi Pembentukan National Cyber Defence Sebagai Upaya Mempertahankan Kedaulatan Negara*. Volume XXI. Perspektif.

<sup>3</sup> Aristyawati, Dhita Evany, Rohmatun Uyun, and Adelia Zahra Nugroho. 2024. "Evaluasi Respons Hukum Terhadap Perang Siber Humaniter Internasional," no. 2: 1–10.

<sup>4</sup> Syaefudin, M A F, F A Sudewo, and K Rizkianto. 2021. *HUKUM SIBER: Perbandingan Indonesia Dan Malaysia*. PT NEM : Pekalongan.

menimbulkan pertanyaan kompleks mengenai bagaimana prinsip-prinsip hukum humaniter yang ada dapat diterapkan dalam konteks ini maka dapat diidentifikasi tantangan utama yang dihadapi hukum humaniter internasional dalam konflik siber dan dapat diterapkan atau disesuaikan dengan ancaman yang ditimbulkan.

## **METODE PENELITIAN**

Metode penelitian yang digunakan dalam penulisan artikel ini adalah penelitian yuridis normatif (*legal study research*) bersifat kualitatif, penelitian yuridis normatif merupakan penelitian yang mengkaji dan menganalisis peraturan perundang-undangan yang berkaitan dengan permasalahan yang sedang diangkat. Penelitian yuridis normatif dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, asas-asas hukum serta peraturan perundang-undangan yang berhubungan dengan penelitian ini. Pandangan normatif adalah kerangka berpikir tentang hukum, keberlakuannya, penerapannya, pembentukannya dan penegaknya harus berdasar kepada segala bentuk peraturan perundang-undangan yang mengatur tentang hukum tersebut. Penelitian kualitatif adalah penelitian yang bersifat deskriptif dan cenderung analisis. Pendekatan yang digunakan dalam jenis penelitian ini antara lain, Pendekatan Perundang-Undangan, Pendekatan Konseptual, dan Pendekatan Kasus. Pendekatan perundang-undangan dilaksanakan dengan mengkaji beberapa undang-undang atau regulasi yang mempunyai keterkaitan dengan isu-isu

yang dihadapi. Pendekatan secara konsep dilaksanakan manakala peneliti menggunakan pendekatan doktrin-doktrin atau pendapat para ahli yang berkembang dalam ilmu hukum. Pendekatan Kasus, Pendekatan ini dilaksanakan dengan melakukan kajian pada kasus-kasus yang berkaitan dengan isu hukum yang dihadapi.

Menggunakan data sekunder yang terbagi menjadi bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Bahan hukum primer terdiri dari peraturan perundang-undangan. Bahan hukum sekunder berupa buku hukum, karya ilmiah dalam jurnal hukum, hasil penelitian hukum lainnya, dan pendapat ahli hukum (doktrin). Sedangkan bahan hukum tersier atau bahan non hukum meliputi kamus, ensiklopedia dan lain-lain.<sup>5</sup> Menggunakan teknik pengumpulan data studi pustaka (*library research*) yakni dengan cara melakukan pengkajian terhadap peraturan perundang-undangan, putusan-putusan pengadilan, jurnal, buku, dan hasil penelitian lainnya yang berkaitan dengan permasalahan hukum yang diteliti. Data yang terkumpul kemudian dilakukan analisis dengan metode analisis kualitatif, yakni melakukan penafsiran terhadap bahan hukum yang telah diolah untuk memberikan jawaban terhadap penelitian yang dilakukan.

## **PEMBAHASAN**

### **Tantangan Utama Yang Dihadapi Hukum Humaniter Internasional Dalam Konflik Siber**

Transformasi teknologi telah secara signifikan mengubah cara perang dilakukan. Dulu, peperangan identik dengan penggunaan senjata seperti senapan

---

<sup>5</sup> Muhaimin, 2022. *Metode Penelitian Hukum*. Mataram: Mataram University Press.

dan tank, yang melibatkan pertarungan langsung dengan musuh. Sekarang, dengan kemajuan teknologi digital, muncul dimensi baru dalam konflik yang mengarah pada penggunaan senjata yang lebih canggih dan tidak terlihat. Akibatnya, perang modern bisa mengacaukan suatu negara tanpa harus menembakkan satu peluru pun, memperkenalkan ancaman yang jauh di luar batas pertarungan tradisional.

Salah satu contoh yang jelas dari perubahan ini adalah meningkatnya serangan siber dalam beberapa tahun terakhir. Serangan ini kini digunakan sebagai cara untuk melemahkan kekuatan negara lain. Serangan siber mencakup usaha untuk mengganggu, merusak, atau mendapatkan akses ilegal ke sistem komputer, jaringan, atau data digital. Tujuan dari serangan ini bervariasi, mulai dari pencurian informasi hingga merusak infrastruktur penting atau mengganggu layanan pemerintah. Beberapa teknik yang sering digunakan termasuk *malware*, *phishing*, serangan DDoS, pemanfaatan celah keamanan (*zero-day*), dan rekayasa sosial.

Serangan siber bisa merusak data sipil seperti catatan kesehatan, menghancurkan infrastruktur penting seperti jaringan listrik dan pasokan air, serta mengganggu layanan pemerintah yang berbasis elektronik. Dalam perang modern, serangan siber sering digunakan bersamaan dengan senjata konvensional, yang memperbesar dampaknya dengan menghentikan komunikasi atau infrastruktur pendukung lainnya. Kemampuan serangan ini untuk beroperasi tanpa bisa dideteksi secara fisik menjadikannya alat strategis yang sangat efektif dalam peperangan di era digital.

Salah satu contoh yang mencolok tentang ancaman siber terlihat dalam

konflik antara Rusia dan Ukraina yang dimulai pada tahun 2022. Serangan siber dari Rusia menargetkan berbagai sektor penting di Ukraina, termasuk pemerintah, telekomunikasi, dan transportasi. Menurut laporan dari *The State Service of Special Communications and Information Protection* (SSSCIP), Ukraina telah mengalami lebih dari 796 serangan siber sejak konflik dimulai. Serangan ini tidak hanya merusak infrastruktur tetapi juga mengganggu stabilitas negara Ukraina secara keseluruhan.

Strategi ini menunjukkan bagaimana serangan siber telah menjadi senjata utama dalam konflik modern, memungkinkan negara yang menyerang untuk melakukan serangan tanpa menggunakan kekuatan militer biasa. Rusia bukanlah satu-satunya negara yang secara terbuka menggunakan serangan siber dalam strategi militernya. Semakin banyak negara yang mengembangkan kemampuan siber militer, yang menimbulkan dilema hukum dan etika di tingkat internasional.

Dalam konteks peperangan modern, Hukum Humaniter Internasional (HHI) menghadapi tantangan besar untuk menyesuaikan diri dengan teknologi yang terus berkembang. HHI bertujuan untuk meminimalkan dampak dari konflik bersenjata terhadap manusia dengan membatasi penggunaan alat dan strategi perang serta melindungi individu yang tidak terlibat langsung dalam pertikaian. Seperti halnya hukum yang mengatur senjata konvensional seperti bom dan peluru, HHI juga berlaku untuk senjata dan metode perang modern, termasuk serangan siber. Hal ini ditegaskan dalam Pendapat Penasihat Mahkamah Internasional mengenai Senjata Nuklir pada tahun 1996, yang menyatakan bahwa HHI berlaku untuk semua bentuk peperangan, baik yang

terjadi di masa lalu, saat ini, maupun di masa depan.

Dalam Protokol Tambahan I (1977) Pasal 36, negara-negara diharuskan untuk mengevaluasi legalitas senjata baru, termasuk teknologi siber, guna memastikan bahwa mereka sesuai dengan HHI. Mahkamah Internasional juga menekankan bahwa HHI relevan untuk semua jenis konflik, termasuk yang melibatkan teknologi modern. Meskipun Protokol Tambahan I dibuat sebelum era digital, prinsip-prinsipnya tetap bisa diterapkan untuk menghadapi tantangan baru. Walaupun HHI memiliki ketentuan yang dapat diterapkan pada perang modern, perdebatan terus berlangsung mengenai apakah hukum ini perlu diperbarui atau hanya ditafsirkan ulang untuk menjawab ancaman dari serangan siber. Sebagian pakar berpendapat bahwa interpretasi ulang cukup memadai, sementara yang lain merasa bahwa revisi diperlukan untuk mengakomodasi kompleksitas teknologi saat ini.

Namun, masalah utama yang dihadapi oleh HHI tidak hanya ada pada perbaruan hukum, tetapi juga pada kurangnya kesungguhan dari negara-negara untuk menerapkan aturan yang sudah ada. Tanpa komitmen yang kuat dari negara untuk mengikuti dan melaksanakan hukum ini, keberhasilan HHI dalam mengurangi penderitaan manusia dalam konflik akan menjadi sangat sulit. Bahkan hukum baru pun hanya akan menjadi sebuah simbol tanpa pengaruh nyata jika tidak dioperasikan dengan baik.

Untuk bisa menghadapi tantangan perang yang modern, diperlukan komitmen secara global untuk menegakkan hukum yang tinggi, baik dalam konflik tradisional maupun yang baru. Kerjasama internasional sangat penting agar serangan

siber, yang bisa menyebabkan kerusakan besar tanpa adanya pertempuran fisik, tetap berada dalam kerangka hukum yang jelas. Langkah-langkah pencegahan seperti peningkatan keterbukaan, pengembangan standar internasional untuk keamanan di dunia maya, dan pelatihan untuk para pelaku di lapangan dapat membantu memperkuat usaha ini. Selain itu, dibutuhkan kerja sama di berbagai sektor antara pemerintah, bisnis, dan masyarakat internasional untuk menciptakan lingkungan yang lebih aman di era digital.

Masalah utama yang dijumpai oleh hukum humaniter internasional dalam konflik siber meliputi:

1. Menemukan Pelaku: Salah satu masalah besar dalam konflik siber adalah kesulitan dalam menemukan siapa yang bertanggung jawab atas serangan. Ketidakjelasan yang dimiliki oleh serangan siber membuatnya susah untuk menentukan apakah tindakan tersebut berasal dari negara atau individu. Dalam internet, sangat sulit untuk dengan tepat mengetahui siapa pelaku serangan siber karena penggunaan teknik menyamar dan sarana yang bersifat global. Hal ini menyulitkan untuk menegakkan tanggung jawab negara atau individu atas pelanggaran HHI
2. Prinsip Proporsionalitas dan Pembeda: HHI menekankan pada prinsip proporsionalitas (larangan melakukan serangan yang berlebihan) dan pembeda (memisahkan antara pejuang dan orang yang tidak terlibat). Tindakan siber dapat memiliki pengaruh besar pada masyarakat umum dan fasilitas penting seperti listrik, air, rumah sakit, dan informasi medis, meskipun tidak ada kerusakan fisik yang terlihat. Namun, dalam konflik siber, sukar untuk memastikan bahwa serangan hanya

- ditujukan kepada target militer dan tidak melukai warga sipil atau infrastruktur sipil. Ini menguji prinsip-prinsip utama HHI yang mencakup perlindungan warga sipil, keseimbangan, dan kehati-hatian saat melakukan serangan. Serangan siber yang tidak memisahkan antara sasaran militer dan sipil bisa mengakibatkan kerugian serius bagi masyarakat, bertentangan dengan prinsip pembeda dalam HHI.
3. Pengertian "Serangan" dalam HHI: HHI mendefinisikan "serangan" sebagai tindakan kekerasan yang mengakibatkan kerusakan fisik. Namun, serangan siber seringkali tidak melibatkan kekerasan fisik secara langsung, meskipun bisa menimbulkan kerusakan besar. Ini memunculkan pertanyaan apakah serangan siber bisa dianggap sebagai "serangan" menurut HHI. HHI telah secara klasik dibuat untuk menghadapi peperangan tradisional, sehingga tidak secara langsung mengatur tentang serangan siber. Ini menyebabkan masalah dalam menentukan apakah serangan siber tertentu dapat dianggap sebagai konflik bersenjata yang membuat HHI berlaku. Banyak serangan siber memiliki tingkat keparahan dan efek yang tidak jelas apakah memenuhi syarat sebagai konflik bersenjata menurut hukum internasional. Jika tidak memenuhi syarat itu, maka HHI tidak dapat diterapkan, dan perlindungan hukum bagi para korban menjadi kurang maksimal.<sup>6</sup>
  4. Hukum dan Tanggung Jawab Negara: Konflik siber sering kali melintasi batas-batas negara, menimbulkan pertanyaan tentang hukum dan tanggung jawab negara dalam mencegah atau menanggapi serangan siber yang terjadi dari wilayahnya. Kekurangan sistem pengenalan yang efektif membuat negara atau pelaku non-negara dapat bertindak tanpa merasa takut terhadap sanksi hukum internasional.
  5. Ketidakjelasan Status Kombatan dan Partisipasi Langsung: Dalam pertempuran di dunia maya, perbedaan antara pejuang dan bukan pejuang jadi tidak jelas. Banyak individu biasa bisa terlibat langsung dalam aktivitas siber, yang menciptakan kebingungan tentang siapa yang bisa dianggap sebagai sasaran sah menurut HHI. Penerapan konsep partisipasi langsung dalam permusuhan menjadi rumit dilakukan dengan konsisten di ranah siber.
  6. Keterlambatan Adaptasi dan Ketidakpastian Hukum: HHI masih perlu diperbarui sepenuhnya agar bisa menangani kemajuan dalam teknologi siber. Banyak ketentuan yang masih umum dan tidak memberikan kepastian hukum dalam konteks peperangan siber. Perdebatan di tingkat internasional masih berlangsung tentang perlunya regulasi baru atau penyesuaian interpretasi HHI agar sesuai dengan tantangan siber yang ada saat ini.
  7. Kurangnya Komitmen dan Kerjasama Internasional: Pelaksanaan HHI dalam pertempuran siber sangat tergantung pada keinginan negara-negara untuk mematuhi dan menerapkan peraturan yang ada. Tanpa adanya komitmen dan kolaborasi internasional, efektivitas HHI

---

<sup>6</sup> Aristyawati, Dhita Evany, Rohmatun Uyun, and Adelia Zahra Nugroho. 2024. "Evaluasi Respons

Hukum Terhadap Perang Siber Humaniter Internasional," no. 2: 1–10.

dalam melindungi korban konflik siber akan sangat terbatas.

Tabel 1. Tantangan Yang Dihadapi HHI Dalam Konflik Siber

Tantangan	Penjelasan Singkat
Ketidakjelasan dalam definisi dan klasifikasi	Susah untuk mengetahui kapan serangan siber menjadi perang menurut HHI.
Menentukan pelaku & atribusi	Sulit untuk secara hukum membuktikan siapa yang melakukan serangan siber.
Perlindungan masyarakat dan infrastruktur	Serangan siber dapat sangat merugikan masyarakat dan infrastruktur penting.
Status pejuang dan partisipasi	Perbedaan antara pejuang dan warga sipil tidak jelas dalam operasi siber.

Penyesuaian dan kepastian hukum	HHI belum sepenuhnya beradaptasi dengan teknologi dan cara-cara baru dalam siber.
Komitmen dan kerja sama antar negara	Penegakan hukum lemah tanpa kerja sama dan komitmen antara negara-negara.

Hukum Humaniter Internasional menghadapi banyak kesulitan dalam mengatur konflik siber, mulai dari definisi, pelacakan pelaku, perlindungan masyarakat, sampai penyesuaian hukum dengan teknologi baru. Untuk menghadapi masalah ini, diperlukan pembaruan hukum, peningkatan kerja sama antar negara, dan penguatan cara penegakan hukum agar perlindungan kemanusiaan tetap terjaga di zaman digital.

### **Penerapan Hukum Humaniter Internasional Atau Penyesuaian Dengan Ancaman Yang Ditimbulkan Oleh Konflik Siber**

Konflik siber adalah jenis baru dari konflik militer yang memerlukan aturan untuk mencegah dampak yang berlebihan bagi masyarakat. Pada dasarnya, aturan-aturan tersebut adalah

prinsip-prinsip HHI yang bertujuan untuk melindungi semua pihak, baik yang terlibat maupun yang tidak terlibat dalam konflik bersenjata. Ada ide yang menekankan pentingnya menciptakan instrumen HHI yang secara khusus mengatur tentang perang siber. Tujuan dari pengaturan ini adalah agar negara-negara mengikuti dan mematuhi aturan HHI tersebut saat mereka ingin melakukan perang siber. Namun, usulan untuk membuat hukum internasional mengenai perang siber masih perlu dipikirkan oleh semua negara.

Pertimbangan untuk membuat model hukum tentang perang siber muncul dari kebutuhan akan keselarasan internasional sehingga dapat terbentuk sistem hukum yang mendukung negara-negara dalam membangun undang-undang yang seragam dan konsisten. Selain itu, model hukum ini membantu dalam merumuskan hukum dalam negeri yang efisien dan selaras dengan standar internasional, yang dapat mengurangi ketidakjelasan hukum dan meningkatkan efektivitas penegakan hukum. Terakhir, model hukum ini bersifat adaptif dan dapat disesuaikan dengan kondisi unik di setiap negara. Hal ini memungkinkan negara untuk mengambil elemen-elemen yang relevan sesuai dengan kebutuhan dan prioritas nasional dalam menghadapi ancaman perang siber.

Model hukum dapat dipakai untuk mengatur hukum internasional maupun hukum domestik. Model hukum

sebagai acuan bagi hukum domestik memberikan kesempatan kepada negara-negara untuk membuat kebijakan dalam negeri yang efektif dalam menangani masalah yang berkaitan dengan perang siber. Negara dapat memastikan bahwa hukum mereka sejalan dengan standar internasional. Di sisi lain, model hukum ini juga bisa mempermudah negara-negara dalam menyusun dan melaksanakan perjanjian internasional mengenai perang siber. Dengan dasar hukum yang seragam, negara-negara dapat lebih mudah mencapai kesepakatan mengenai kerangka kerja dan protokol internasional untuk menangani dan mencegah serangan siber.

Berikut adalah beberapa hal yang perlu ada dalam model hukum tersebut, yaitu :<sup>7</sup>

1. Serangan siber bisa dikategorikan sebagai bentuk serangan yang diatur oleh Pasal 49 Protokol Tambahan I Konvensi Jenewa tahun 1977, terutama jika tindakan tersebut bersifat agresif dan berdampak langsung pada masyarakat sipil atau infrastruktur yang penting. Namun, masih ada perdebatan tentang bagaimana hukum internasional diterapkan dalam tindakan siber, terutama tentang objek '*dual-use*' yang bisa digunakan baik untuk kepentingan sipil maupun militer. Oleh karena itu, perlu ada penelitian lebih dalam mengenai penerapan prinsip-prinsip hukum

<sup>7</sup> Gunawan, Stephanie Liestia. 2024. *Urgensi pembentukan instrumen Hukum Humaniter Internasional tentang Cyber Warfare*. Jurnal Ilmu

- internasional yang berkaitan, seperti prinsip kemanusiaan, keperluan militer, proporsionalitas, dan perbedaan untuk mencegah konsekuensi dari serangan siber.
2. Senjata siber dapat dianggap sebagai "senjata" menurut Pasal 36 API Konvensi Jenewa tahun 1977 dan Klausul Martens meskipun tidak selalu menghasilkan efek fisik langsung, seperti halnya senjata biasa. Senjata siber bisa digunakan untuk menyerang, merusak, atau mengganggu sistem atau jaringan komputer. Maka dari itu, senjata siber memiliki potensi untuk menyebabkan kerusakan atau bahaya. Contohnya, serangan siber dapat merusak infrastruktur penting, menimbulkan gangguan terhadap keamanan negara, atau membocorkan informasi rahasia.
  3. Objek '*dual-use*' yang dipakai untuk tujuan sipil dan militer bisa dianggap sebagai objek militer dalam situasi tertentu. Berdasarkan Pasal 52 ayat (2) Protokol Tambahan I Konvensi Jenewa tahun 1977, suatu objek dapat disebut objek militer berdasarkan empat aspek: karakteristik, lokasi, tujuan, atau pemanfaatan. Selain itu, objek tersebut harus berperan aktif dalam kegiatan militer dan penghancurannya, penangkapannya, atau penetralan harus memberikan keuntungan militer yang nyata. Dalam konteks siber, objek seperti jaringan komputer sipil bisa menjadi target militer yang sah jika digunakan

untuk mendukung aksi militer. Misalnya, jika jaringan komputer sipil dimanfaatkan untuk melancarkan serangan siber atau jika digunakan oleh tentara lawan untuk komunikasi militer, maka jaringan tersebut bisa dianggap sebagai sasaran militer yang sah. Hal ini juga berlaku untuk negara seperti Amerika Serikat, di mana banyak komunikasi militer dilakukan melalui jaringan sipil.

HHI hanya diterapkan ketika serangan siber berlangsung dalam situasi perang (baik internasional maupun non-internasional). Protokol Tambahan I dari Konvensi Jenewa tahun 1977 mengakui kemajuan cara berperang, termasuk teknologi siber, selama memenuhi kriteria "serangan" yang menyebabkan efek fisik atau gangguan yang berarti.

HHI bisa diterapkan dan disesuaikan dengan bahaya yang ditimbulkan oleh konflik siber melalui berbagai cara dan prinsip dasar yang sesuai, meskipun HHI dibuat sebelum teknologi komunikasi dan informasi modern ada.

Penerapan HHI dalam Konflik Siber :

- a. Prinsip-prinsip dasar HHI masih berlaku: Prinsip pemisahan, proporsionalitas, dan kehati-hatian yang melindungi masyarakat sipil dan infrastruktur tetap menjadi dasar dalam operasi siber saat perang. Misalnya, serangan siber yang dapat merusak infrastruktur penting seperti listrik, sumber air, atau rumah sakit harus dihindari jika itu bisa menimbulkan bahaya yang tidak sebanding bagi warga sipil.

- b. Menentukan serangan siber sebagai konflik bersenjata: Dampak dari serangan siber, apakah itu menyebabkan kerusakan fisik, luka, atau kematian, menentukan apakah serangan tersebut dapat dianggap sebagai konflik bersenjata yang diatur oleh HHI. Jika serangan siber memberikan dampak serius, maka aturan HHI harus berlaku.
- c. Pengakuan bahwa tidak ada kekosongan hukum: Operasi siber tidak berada di luar hukum internasional. Semua negara harus menyadari bahwa operasi siber dalam konflik bersenjata harus mematuhi aturan-aturan HHI, meskipun masih perlu ada diskusi lebih lanjut tentang interpretasi spesifiknya di ruang siber.

#### Penyesuaian dan Tantangan HHI dalam Penerapan Konflik Siber :

- a. Pengembangan interpretasi dan norma: Karena HHI ditulis sebelum era digital, ada kebutuhan untuk mengembangkan penjelasan hukum yang jelas tentang operasi siber, termasuk siapa yang bisa dianggap sebagai pejuang dan bagaimana menilai proporsionalitas dalam konteks serangan siber.
- b. Manual Tallinn sebagai pedoman: Manual Tallinn adalah salah satu cara untuk menyesuaikan HHI dalam konteks operasi siber dengan memberikan aturan dan prinsip yang sesuai, meskipun belum menjadi hukum internasional yang mengikat.
- c. Kerjasama antar bidang: Untuk mengevaluasi dan mengawasi perang siber secara efektif, perlu kerjasama antara para ahli teknologi

informasi dan ahli hukum internasional untuk memastikan penerapan prinsip HHI yang tepat di tengah teknologi yang terus berkembang.

- d. Pembuatan kebijakan nasional dan internasional: Negara-negara harus membuat kebijakan pertahanan siber yang jelas dan mengintegrasikan aspek hukum humaniter, termasuk menentukan kapan serangan siber dapat dianggap sebagai "penggunaan kekuatan" atau "serangan bersenjata" serta siapa yang bisa dianggap sebagai pejuang.

Penerapan hukum humaniter internasional dalam konflik bersenjata berlaku berdasarkan ketentuan dari tempat terjadinya perang. Menurut Joint Publication, cyberspace adalah ruang global yang merupakan lingkungan informasi dengan jaringan infrastruktur teknologi informasi yang saling terhubung, termasuk internet, jaringan komunikasi, sistem komputer, serta pengontrol dan proses. Dalam Artikel 2 (4) Piagam PBB disebutkan bahwa "*Semua anggota harus menghindari dalam hubungan internasional mereka terhadap ancaman atau penggunaan kekuatan yang dapat mengganggu integritas teritorial atau kemandirian politik negara manapun, atau dengan cara lain yang tidak sesuai dengan Tujuan Perserikatan Bangsa-Bangsa.*" Dengan menyebutkan integritas teritorial, berarti penggunaan angkatan bersenjata di laut, darat, dan udara harus berdasarkan teritorial yang dimiliki suatu negara, yang berkaitan dengan kedaulatan. Demikian juga dalam cyberspace, untuk diakui

sebagai domain dalam peperangan, harus ditetapkan terlebih dahulu kedaulatan suatu negara di dalam cyberspace.

Menurut Bodley, kedaulatan terdiri dari dua jenis, yaitu kedaulatan eksternal dan internal. Kedaulatan eksternal berkaitan dengan hal-hal luar negeri dan kekuatan pertahanan untuk melindungi wilayah negara dari serangan negara lain. Sedangkan kedaulatan internal meliputi kewenangan suatu negara untuk melaksanakan fungsi-fungsinya nasional. Dalam Tallinn Manual *The International Law Applicable to Cyber Warfare Rule 1*, disebutkan bahwa "Sebuah Negara dapat mengendalikan infrastruktur dan kegiatan siber di wilayah kedaulatannya." Aturan tersebut menunjukkan bahwa negara memiliki hak untuk mengatur infrastruktur siber dan aktivitas siber dalam batas wilayah yang diakui kedaulatannya. Dari pemahaman Bodley dan aturan di Tallinn Manual, bisa disimpulkan bahwa jika suatu negara memiliki kemampuan dalam hal infrastruktur siber dan aktivitas siber, maka negara tersebut memiliki kedaulatan di cyberspace, sehingga memenuhi syarat umum dalam hukum internasional terkait cyberspace sebagai domain yang diakui.

Dalam konteks konflik siber, serangan yang ditujukan pada jaringan telepon di suatu negara dengan maksud untuk merusak jaringan komunikasi militer bisa berdampak juga pada jaringan telekomunikasi yang digunakan oleh warga sipil di negara tersebut. Namun, efek yang ditimbulkan secara tidak langsung dari serangan siber bisa menyebabkan

penderitaan yang tidak perlu, misalnya dengan penggunaan malware yang dirancang untuk melakukan hal-hal yang bisa melanggar prinsip menghindari penderitaan yang tidak perlu. Contohnya, serangan siber dapat mempengaruhi peralatan, perlengkapan, data, dan infrastruktur medis yang seharusnya digunakan untuk mengobati dan merawat pasien, baik yang bersenjata maupun sipil. Selain itu, serangan siber bisa dilakukan tanpa menimbulkan kecurigaan, meskipun dampaknya sangat besar, ini juga bertentangan dengan prinsip tersebut.

Aturan dan prinsip dalam hukum humaniter internasional dapat diterapkan dalam perang siber. Hal ini didasarkan pada wilayah yang tidak sekadar fisik atau non-fisik, tetapi berlandaskan kedaulatan dan teritorial. Kedaulatan dalam *cyberspace* serta infrastruktur siber yang ada dalam teritorial suatu negara dapat dikenali melalui alamat IP, serta pengelolaan dan pengaturan suatu negara terhadap ruang sibernya, semua mendukung cyberspace sebagai domain dalam konflik bersenjata.

## **PENUTUP**

Hukum Humaniter Internasional menghadapi banyak tantangan dalam mengatur konflik siber, mulai dari definisi, pelacakan pelaku, perlindungan masyarakat, sampai penyesuaian hukum dengan teknologi baru. Untuk menghadapi masalah ini, diperlukan pembaruan hukum, peningkatan kerja sama antar negara, dan penguatan cara penegakan hukum agar perlindungan kemanusiaan tetap terjaga di zaman digital.

HHI bisa diterapkan dan disesuaikan dengan bahaya yang ditimbulkan oleh konflik siber melalui berbagai cara dan prinsip dasar yang sesuai, meskipun HHI dibuat sebelum teknologi komunikasi dan informasi modern ada. Penerapan HHI dalam Konflik Siber : prinsip-prinsip dasar HHI masih berlaku, menentukan serangan siber sebagai konflik bersenjata, dan pengakuan bahwa tidak ada kekosongan hukum. Penyesuaian dan Tantangan HHI dalam Penerapan Konflik Siber : pengembangan interpretasi dan norma, Manual Tallinn sebagai pedoman, kerjasama antar bidang, dan pembuatan kebijakan pertahanan siber nasional dan internasional.

Dari penelitian ini di rekomendasikan pengembangan : (1) Pembentukan instrumen khusus, (2) Interpretasi dinamis penerapan prinsip HHI, (3) Kolaborasi multidisiplin dari ahli hukum, teknologi, dan militer untuk menyusun parameter dampak siber.

HHI dapat diterapkan pada konflik siber yang memenuhi kriteria konflik bersenjata dan menimbulkan dampak fisik, tetapi perlu adaptasi melalui instrumen baru atau interpretasi progresif sebagaimana kasus Rusia-Ukraina yang menjadi bukti urgensi penyesuaian hukum ini.

#### **DAFTAR PUSTAKA**

Aristyawati, Dhita Evany, Rohmatun Uyun, and Adelia Zahra Nugroho. 2024. "Evaluasi Respons Hukum Terhadap Perang Siber Humaniter Internasional," no. 2: 1–10.

Badri, M. 2012. *Perang Cyber Dalam Dinamika Komunikasi Internasional.* "Komunikasi Militer. Buku Liter. Jakarta: Mata Padi Pressindo, Universitas Prof. Dr. Moestopo Jakarta

dan ASPIKOM.

Gunawan, Stephanie Liestia. 2024. *Urgensi pembentukan instrumen Hukum Humaniter Internasional tentang Cyber Warfare.* Jurnal Ilmu Hukum Veritas et Justitia : Universitas Katholik Parahyangan.

Muhaimin, 2022. *Metode Penelitian Hukum.* Mataram: Mataram University Press.

Nur Khalimatus Sa'diyah dan Ria Tri Vinata. 2016. *Rekonstruksi Pembentukan National Cyber Defence Sebagai Upaya Mempertahankan Kedaulatan Negara.* Volume XXI. Perspektif.

yaefudin, M A F, F A Sudewo, and K Rizkianto. 2021. *HUKUM SIBER: Perbandingan Indonesia Dan Malaysia.* PT NEM : Pekalongan.