JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v5i5

Paradoks Hukum Humaniter di Era Perang Siber dan Drone: Antara Kepatuhan Normatif dan Realitas Operasional

Takdir Mattanete[1], Joko Wahyudi[2], Tarsisius Susilo[3], Dinand Tumpak Sirait[4], Wahyu RS[5].
[1]Sesko TNI, Bandung, Indonesia, takdirmattanete777@gmail.com
[2]Sesko TNI, Bandung, Indonesia, jackw45@gmail.com
[3]Sesko TNI, Bandung, Indonesia, muchus70@gmail.com.
[4]Sesko TNI, Bandung, Indonesia, departemen.faljuang@gmail.com
[5]Sesko TNI, Bandung, Indonesia, departemen.faljuang@gmail.com

Corresponding Author: takdirmattanete777@gmail.com

Abstract: *development of military technologies such as drones and cyber operations has created a new landscape in modern warfare. This article analyzes the paradox that arises between normative compliance with international humanitarian law—in particular the principles of distinction, proportionality, and precaution—and the operational realities of the digital and unmanned battlefield. The study uses a qualitative approach based on document review and case studies of drone attacks in Yemen and cyber attacks on health facilities in Ukraine. The analysis shows a serious gap between applicable legal doctrine and practice on the ground, especially in terms of accountability, attribution, and civilian protection. The article recommends strengthening international legal instruments through the revision of Additional Protocol I to the Geneva Conventions and the adoption of new norms for technology-based conflicts.*

Keyword: *humanitarian law, drones, cyber attacks, modern conflicts, civil protection principles*

Abstrak: Perkembangan teknologi militer seperti drone dan operasi siber telah menciptakan lanskap baru dalam peperangan modern. Artikel ini menganalisis paradoks yang muncul antara kepatuhan normatif terhadap hukum humaniter internasional khususnya prinsip *distinction, proportionality*, dan *precaution* dengan realitas operasional di medan perang digital dan nirawak. Studi ini menggunakan pendekatan kualitatif berbasis kajian dokumen dan studi kasus serangan *drone* di Yaman serta serangan siber terhadap fasilitas kesehatan di Ukraina. Hasil analisis menunjukkan adanya ketimpangan serius antara doktrin hukum yang berlaku dan praktik di lapangan, terutama dalam hal akuntabilitas, atribusi, dan perlindungan sipil. Artikel ini merekomendasikan penguatan instrumen hukum internasional melalui revisi Protokol Tambahan I Konvensi Jenewa dan adopsi norma baru untuk konflik berbasis teknologi.

Kata Kunci: hukum humaniter, drone, serangan siber, konflik modern, prinsip perlindungan sipil.

PENDAHULUAN

Sejak ditetapkannya Konvensi Jenewa dan Protokol Tambahan I, hukum humaniter telah menjadi fondasi utama dalam membatasi dampak destruktif konflik bersenjata terhadap penduduk sipil. Namun, kemajuan teknologi militer seperti penggunaan drone bersenjata dan peperangan siber telah menantang validitas dan efektivitas prinsip-prinsip tersebut. Konflik modern memperlihatkan kompleksitas baru di mana pelaku perang dapat menyerang dari jarak jauh, secara otomatis, dan tanpa kehadiran manusia secara fisik di medan tempur. Fenomena ini menimbulkan dilema: bagaimana hukum yang disusun pada era analog mampu mengatur tindakan dalam domain digital dan nirawak?. Dalam konteks ini, muncul paradoks hukum humaniter yaitu benturan antara norma hukum yang mengatur perlindungan warga sipil dan kenyataan operasional yang cenderung mengaburkan garis antara target militer dan objek sipil. Konflik Yaman dan invasi Rusia ke Ukraina menunjukkan eskalasi penggunaan teknologi militer yang tidak sepenuhnya sejalan dengan prinsip *distinction, proportionality,* dan *precaution* yang mendasari hukum humaniter. Oleh karena itu, perlu dilakukan pengkajian ulang terhadap daya jangkau hukum humaniter di era konflik modern.

METODE

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode kualitatif dengan memusatkan perhatiannya pada prinsip-prinsip umum yang mendasar perwujudan satuan-satuan gejala dalam kehidupan sosial manusia. Menurut Sugiyono (2020) “penelitian kualitatif merupakan metode penelitian yang berlandaskan pada filsafat positivisme, digunakan untuk meneliti pada kondisi obyek yang alamiah dimana peneliti adalah sebagai instrumen kunci, dan hasil penelitian kualitatif lebih menekankan makna dari pada generalisasi”. Menurut John W. Creswell (2010) “penelitian kualitatif adalah metode untuk dapat mengeksplorasi serta memahami makna masalah sosial atau kemanusiaan. Dalam proses penelitian kualitatif cenderung melibatkan upaya-upaya penting, seperti mengumpulkan data yang spesifik dari partisipan, mengajukan pertanyaan dan prosedur, menganalisis data secara induktif mulai tema khusus ke umum dan menafsirkan makna data”. Desain penelitian yang digunakan dalam menyelesaikan penelitian ini menggunakan desain deskriptif, Menurut Sudjana (2010) mendefinisikan penelitian deskriptif adalah “Penelitian yang berusaha mendeskripsikan suatu gejala, peristiwa, kejadian yang terjadi pada saat sekarang”. Ciri-ciri dari metode deskriptif seperti yang dikemukakan oleh Nasution (2003) yaitu : (1) Memusatkan diri pada pemecahan-pemecahan masalah yang ada pada masa sekarang atau masalah-masalah yang aktual. (2) Data yang dikumpulkan mula-mula disusun, dijelaskan dan kemudian dianalisa, oleh karena itu metode ini sering disebut metode analisa.

HASIL DAN PEMBAHASAN

Kemajuan teknologi militer dalam bentuk perang siber dan penggunaan drone bersenjata telah menciptakan tantangan serius terhadap penerapan prinsip-prinsip *International Humanitarian Law* atau Hukum Humaniter Internasional. Di satu sisi, hukum humaniter tetap menjadi rujukan normatif universal yang menetapkan prinsip-prinsip utama seperti *distinction, proportionality*, dan *necessity*. Namun, dalam praktiknya, penerapan prinsip-prinsip tersebut sering kali menghadapi paradoks akibat sifat teknologi militer modern yang asimetris, tersembunyi, dan berkecepatan tinggi. Penggunaan drone yang dikendalikan jarak jauh sering kali menggiring pada keputusan “klinikal” yang memisahkan pelaku dari medan pertempuran, menurunkan beban psikologis namun meningkatkan risiko *collateral damage* akibat kesalahan intelijen atau algoritma otomatisasi yang keliru (Shmitt, 2013). Dalam konteks perang siber, serangan terhadap infrastruktur sipil seperti jaringan listrik, rumah sakit, atau sistem air bersih, meskipun tidak menimbulkan kerusakan fisik secara langsung, tetap berpotensi melanggar hukum humaniter karena dampaknya terhadap kehidupan warga sipil (Melzer, 2010).

Ketidakjelasan aktor dalam ruang siber dan kesulitan atribusi memperparah kesenjangan antara norma dan realitas. Banyak negara memanfaatkan ruang abu-abu hukum untuk melaksanakan operasi siber ofensif tanpa deklarasi perang resmi, menjadikan prinsip attribution dalam hukum konflik bersenjata sulit ditegakkan. Dalam banyak kasus, negara atau aktor non-negara yang melakukan serangan siber berskala besar berhasil menghindari akuntabilitas karena kurangnya bukti keterlibatan langsung yang dapat diterima dalam fora internasional (Tikk & Vihul, 2010). Sementara itu, hukum humaniter konvensional masih bergulat dengan adaptasi terhadap medan pertempuran baru ini. Ketidaksiapan ini menyebabkan enforcement gap yang cukup lebar antara kerangka hukum yang ada dan dinamika konflik kontemporer. Maka dari itu, perlu pembaruan hukum internasional yang tidak hanya bersifat responsif terhadap teknologi, tetapi juga menjamin bahwa kepatuhan terhadap hukum humaniter tidak hanya menjadi norma formalistik, tetapi juga nyata di medan perang modern yang tak kasat mata.

Ketidakseimbangan Normatif dan Teknologis Drone dan sistem senjata otonom memang menjanjikan efektivitas militer tinggi. Namun, menurut laporan Human Rights Watch (2020), dari 91 serangan drone AS di Yaman antara 2012–2018, sekitar 30–40% korban adalah non-kombatan. Ini menunjukkan potensi pelanggaran terhadap prinsip proportionality sebagaimana dimuat dalam Pasal 51(5)(b) Protokol Tambahan I Konvensi Jenewa, yang menyatakan bahwa suatu serangan dilarang jika "diharapkan menimbulkan kerugian terhadap warga sipil yang berlebihan dibandingkan dengan keuntungan militer yang konkret dan langsung yang diantisipasi." Kritik juga datang dari *UN Special Rapporteur on extrajudicial, summary or arbitrary executions* yang menekankan bahwa penggunaan drone di luar zona perang formal dapat melanggar hukum humaniter dan hukum hak asasi manusia internasional. Hal ini semakin memperjelas kesenjangan antara doktrin hukum dan realitas operasional di medan non-konvensional.

Ambiguitas Target dalam Serangan Siber Kasus serangan WhisperGate terhadap infrastruktur kesehatan di Ukraina (2022) menyebabkan lumpuhnya sistem rekam medis digital dan sistem logistik rumah sakit nasional. WHO mencatat bahwa lebih dari 300 serangan siber menarget sektor kesehatan Ukraina dalam 6 bulan pertama invasi Rusia (WHO, 2023). Namun, Pasal 49(1) Protokol Tambahan I, yang mendefinisikan "serangan" sebagai "tindakan kekerasan terhadap musuh", masih diperdebatkan dalam konteks siber. Tallinn Manual 2.0 (Rules 92–94) menekankan bahwa serangan siber dapat dianggap serangan dalam hukum humaniter hanya jika menimbulkan efek serupa seperti serangan kinetik, yakni kerusakan fisik, cedera atau kematian. Ini berarti serangan seperti ransomware, yang merusak sistem informasi namun tanpa kerusakan fisik, tidak serta-merta memenuhi definisi serangan. Dengan demikian, serangan siber terhadap objek sipil penting masih berada di area abu-abu hukum (*legal grey zone*), padahal dampaknya terhadap layanan kemanusiaan bisa sangat besar. Kekosongan normatif ini menuntut redefinisi terhadap objek perlindungan hukum humaniter di era digital.

Masalah Atribusi dan Akuntabilitas Dalam konteks hukum internasional, prinsip *command responsibility* sebagaimana diatur dalam Pasal 28 Statuta Roma menyatakan bahwa atasan militer dapat dimintai pertanggungjawaban atas kejahatan yang dilakukan oleh pasukannya jika mereka mengetahui atau seharusnya mengetahui, dan gagal mencegah atau menghukum pelaku. Namun, dalam konteks serangan drone yang dilakukan dari jarak jauh (misalnya dari pangkalan di Nevada terhadap target di Yaman), rantai komando menjadi lebih kompleks dan sulit dilacak. Tambahan lagi, sebagian besar serangan dilakukan berdasarkan data intelijen yang tidak dapat diverifikasi secara independen oleh pengamat hukum.

Untuk serangan siber, persoalan atribusi lebih parah. Karena sifatnya yang anonim, aktor negara dapat menyembunyikan keterlibatannya melalui proksi digital atau *false flag*. ICRC (2021) mencatat bahwa tanpa standar atribusi internasional, pelaku serangan siber terhadap objek sipil hampir selalu lolos dari pertanggungjawaban hukum. Ini berlawanan

dengan prinsip tanggung jawab negara atas tindakan yang melanggar hukum internasional sebagaimana dimuat dalam *Draft Articles on State Responsibility* oleh ILC (2001), terutama Pasal 2 dan 8. Pada pasal 2 dinyatakan bahwa "*There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State*." Sedangkan pasal 8 menyatakan "*The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct*."

Tantangan Etika Operasional dan Moral Injury Laporan Brookings Institution (2021) menyebutkan bahwa operator drone militer AS mengalami tingkat stres pascatrauma (PTSD) yang setara dengan tentara di medan tempur konvensional. Ini disebabkan oleh distorsi kognitif antara tindakan jarak jauh dan dampak mematikan yang ditimbulkan. Dalam hukum humaniter, aspek psikologis ini belum banyak diperhitungkan, namun secara etis penting untuk memperdebatkan bagaimana teknologi seharusnya tidak mendistorsi tanggung jawab moral. Di sisi lain, pelatihan militer modern cenderung menekankan pada efisiensi operasional, bukan pada pendidikan hukum humaniter secara substansial. Padahal, Pasal 83 Konvensi Jenewa I mengamanatkan bahwa "Pihak-pihak yang terlibat dalam konflik wajib menyebarluaskan teks Konvensi dan Protokol Tambahan kepada angkatan bersenjata mereka." Dengan demikian, tidak cukup hanya memperbaiki perangkat hukum, tetapi juga penting untuk membangun budaya kepatuhan terhadap etika dan norma hukum dalam pengoperasian teknologi militer.

Berdasarkan hasil analisis dan tantangan yang diidentifikasi dalam studi ini, berikut beberapa rekomendasi yang dapat dijadikan rujukan normatif dan praktis:

1) Amendemen Protokol Tambahan I Konvensi Jenewa Komunitas internasional perlu merumuskan tambahan pasal atau protokol baru yang secara eksplisit mencakup serangan berbasis siber dan penggunaan sistem senjata nirawak. Definisi "serangan" dalam Pasal 49 harus diperluas untuk mencakup tindakan yang berdampak sistemik terhadap infrastruktur sipil tanpa harus menghasilkan kerusakan fisik langsung. Perubahan ini harus dibahas melalui forum internasional seperti Konferensi Internasional Palang Merah dan Bulan Sabit Merah atau sidang Majelis Umum PBB.
2) Penguatan Mekanisme Atribusi dan Akuntabilitas Internasional Diperlukan lembaga yang memiliki otoritas investigatif dan forensik digital global, semisal pembentukan International Digital *Conflict Observatory* di bawah naungan Dewan HAM PBB atau ICRC. Lembaga ini akan bertugas melakukan investigasi serangan siber dan drone terhadap objek sipil, mengeluarkan laporan terbuka (open-access), serta mendukung proses hukum di Mahkamah Pidana Internasional (ICC) atau pengadilan ad hoc.
3) Integrasi Etika Teknologi dalam Pendidikan Militer Kurikulum pendidikan militer di negara-negara peserta Konvensi Jenewa harus disesuaikan untuk mencakup pembelajaran etika algoritma, tanggung jawab moral dalam pengoperasian teknologi, dan keterampilan verifikasi target berbasis data intelijen. Ini sejalan dengan mandat Pasal 83 Konvensi Jenewa I tentang kewajiban penyebarluasan hukum humaniter.
4) Standardisasi Global terhadap Sistem Otonom Mematikan (LAWS) Negara-negara harus menyepakati standar minimum terhadap *Lethal Autonomous Weapon Systems (LAWS),* termasuk pembatasan penggunaan, mode kontrol manusia (meaningful human control), dan audit pascakejadian terhadap setiap penggunaan senjata berbasis AI. Proses ini dapat dimediasi melalui forum Konvensi Senjata Konvensional (CCW) PBB.
5) Peningkatan Kapasitas Negara Berkembang Negara-negara di Global South memerlukan dukungan dalam membangun sistem pertahanan siber dan struktur hukum nasional yang kompatibel dengan kerangka hukum humaniter modern. Bantuan teknis dan pendanaan

dari lembaga multilateral seperti UNDP, EU Cyber Direct, dan ASEAN *Cybersecurity Cooperation Framework* perlu diperluas dan disinergikan.

Rekomendasi-rekomendasi ini ditujukan tidak hanya untuk memperkuat dimensi perlindungan sipil, tetapi juga untuk menjamin legitimasi dan relevansi hukum humaniter internasional dalam menghadapi disrupsi akibat perkembangan teknologi militer.

KESIMPULAN

Paradoks hukum humaniter di era teknologi militer khususnya penggunaan drone dan operasi siber menunjukkan adanya jurang yang signifikan antara kepatuhan normatif dan realitas operasional di medan konflik kontemporer. Prinsip-prinsip dasar hukum humaniter seperti distinction, proportionality, dan precaution mengalami tantangan serius dalam penerapannya akibat sifat asimetris dan tidak kasat mata dari teknologi militer baru. Serangan jarak jauh tanpa kehadiran fisik, serta kompleksitas dalam atribusi dan verifikasi target, mengaburkan batas antara legalitas dan pelanggaran.

Kelemahan struktural dalam perangkat hukum yang ada, terutama tidak memadainya definisi "serangan" dalam Pasal 49 Protokol Tambahan I dan kesulitan penerapan Pasal 28 Statuta Roma terhadap sistem senjata nirawak, memperlihatkan urgensi untuk memperbarui fondasi normatif hukum humaniter internasional. Serangan siber yang tidak merusak secara fisik namun melumpuhkan sistem layanan sipil esensial seperti rumah sakit, seharusnya diposisikan secara hukum setara dengan serangan konvensional. Tanpa pembaruan ini, pelindungan terhadap warga sipil dalam konflik modern hanya akan menjadi retorika kosong.

Di sisi lain, aspek etika yang berkaitan dengan penggunaan teknologi tempur belum cukup mendapat tempat dalam kebijakan militer dan kerangka hukum. Fenomena moral injury pada operator drone serta rendahnya internalisasi nilai hukum dalam pelatihan militer menunjukkan bahwa regulasi hukum harus dibarengi dengan pendidikan moral dan profesionalisme yang kuat. Dengan demikian, diperlukan pendekatan ganda: pertama, pembaruan instrumen hukum internasional yang mencakup domain siber dan otonomi senjata; kedua, penguatan kapasitas institusional negara-negara berkembang agar dapat mengadopsi dan menerapkan prinsip-prinsip hukum humaniter secara kontekstual. Hanya dengan perpaduan antara reformasi normatif, kolaborasi global, dan etika profesional, hukum humaniter akan tetap relevan dan operasional dalam menghadapi tantangan peperangan abad ke-21.

REFERENSI

Geneva Conventions Additional Protocol I. (1977).

Human Rights Watch. (2020). Death by Drone: Civilian Harm in Yemen.

ICRC. (2021). Cyber Warfare and International Humanitarian Law. Geneva.

International Law Commission (ILC). (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts.

Melzer, N. (2011). *Cyberwarfare and International Law.* United Nations Institute for Disarmament Research.

Melzer, N. (2010). *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*. ICRC.

Schmitt, M. N. & Vihul, L. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Schmitt, M. N. (2013). *Drone Operations and International Law*. Harvard National Security Journal, Vol. 4,

Sugiyono (2020) *Metode Penelitian Kualitatif.* (Bandung: Alfabeta)

Statute of the International Criminal Court (Rome Statute), 1998.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations.* Cooperative Cyber Defence Centre of Excellence (CCDCOE), NATO

WHO. (2023). Impact of Cyberattacks on Healthcare in Conflict Zones.