Jurnal Syntax Imperatif: Jurnal Ilmu Sosial dan Pendidikan
Volume 6, No 2, May 2025, pp. 165-173
P-ISSN: 2721-2491 E-ISSN: 2721-2491
DOI: http://doi.org/10.54543/syntaximperatif.v6i2.679
Published By: CV. Rifainstitut

Penerapan Hukum Humaniter dalam Konflik Siber: Tantangan, Implikasi, dan Kebutuhan Standar Baru

Roma Gunawan[1*], Rudy Simangunsong[2*], Tarsius Susilo[3], Benny Limbong[4], Agus Soeprianto[5]

[1,2,3,4,5]Sekolah Staf dan Komando Tentara Nasional Indonesia (Sesko TNI), Indonesia

ARTICLE INFO

Article history:
Received April 30, 2025
Revised May 27, 2025
Accepted May 27, 2025
Available online May 27, 2025

Kata Kunci:
Hukum Humaniter Internasional, Infrastruktur Kritis, Konflik Siber, Perlindungan Sipil, Standar Hukum Baru

Keywords:
Civilian Protection, Critical Infrastructure, Cyber Conflict, International Humanitarian Law, New Legal Standards.

ABSTRAK

Konflik siber modern menimbulkan tantangan serius bagi penerapan Hukum Humaniter Internasional (HHI), terutama dalam perlindungan penduduk sipil dan infrastruktur kritis. Artikel ini tidak hanya menyerukan pembaruan hukum, tetapi secara spesifik mengusulkan dua standar operasional baru yakni kriteria *"dual-use threshold"* untuk menentukan kapan infrastruktur digital sipil dapat dianggap sasaran militer yang sah, dan protokol verifikasi serangan siber berbasis bukti forensik bersama untuk menilai proporsionalitas dan tanggung jawab. Melalui telaah studi kasus antara lain serangan *ransomware* pada jaringan listrik Ukraina (2020) dan *malware Stuxnet* penelitian ini menunjukkan di mana prinsip pembedaan, proporsionalitas, dan kehati-hatian saat ini gagal memberikan kepastian hukum. Analisis tersebut menyoroti kekosongan regulasi seputar atribusi pelaku dan ambang kerugian non-fisik, kemudian merumuskan rancangan pasal tambahan bagi Konvensi Jenewa III yang memuat definisi serangan siber, tata cara pelaporan insiden, dan mekanisme mediasi cepat. Dengan menyodorkan rancangan standar konkret ini, artikel bertujuan mendukung negosiasi internasional guna membentuk norma dan instrumen hukum yang lebih adaptif terhadap karakteristik unik konflik siber.

ABSTRACT

Modern cyber conflicts pose serious challenges to the application of International Humanitarian Law (IHL), particularly in safeguarding civilian populations and critical infrastructure. Rather than merely calling for legal reform, this article advances two concrete operational standards is a "dual-use threshold" criterion for determining when civilian digital infrastructure may lawfully become a military target, and a joint forensic-evidence based protocol for verifying cyber attacks in order to assess proportionality and assign responsibility. Drawing on six case studies including the 2020 ransomware assault on Ukraine's power grid and the Stuxnet malware operation the research illustrates how the principles of distinction, proportionality, and precaution currently fail to provide legal certainty. The analysis exposes regulatory gaps surrounding actor attribution and non-physical harm thresholds, then drafts supplementary articles to Geneva Convention III that define cyber attacks, establish incident-reporting procedures, and create an expedited mediation mechanism. By offering these concrete standards, the article seeks to underpin international negotiations aimed at developing norms and legal instruments that are better adapted to the unique characteristics of cyber warfare.

1. PENDAHULUAN

Selama dekade terakhir, kemajuan teknologi informasi dan komunikasi telah membuka ranah konflik baru: dunia maya. Serangan siber terhadap infrastruktur kritis—seperti jaringan listrik, sistem perbankan, fasilitas kesehatan, dan jaringan komunikasi—kini menjadi ancaman nyata yang mampu menimbulkan kerusakan setara dengan serangan kinetik konvensional. Contohnya adalah serangan *ransomware* pada jaringan listrik Ukraina (2020)

*Corresponding author
E-mail addresses: ashurafx@gmail.com (Roma Gunawan)

yang memadamkan pasokan energi bagi ratusan ribu warga, serta operasi malware Stuxnet yang merusak sentrifugal nuklir Iran. Insiden-insiden ini menegaskan kebutuhan kriteria *"dual-use threshold"* untuk menentukan kapan infrastruktur digital sipil yang sekaligus mendukung fungsi militer boleh dianggap target yang sah, serta protokol verifikasi serangan siber berbasis bukti forensik bersama guna menilai proporsionalitas dan menetapkan tanggung jawab.

Konflik siber memunculkan pertanyaan serius mengenai penerapan Hukum Humaniter Internasional (HHI), yang pada mulanya dirancang untuk konflik bersenjata fisik. Prinsip-prinsip inti HHI pembedaan antara kombatan dan non-kombatan, proporsionalitas, dan kehati-hatian—dihadirkan pada tantangan baru oleh medan perang virtual yang tak mengenal batas geografis, menyembunyikan identitas pelaku, dan memungkinkan eskalasi secepat mesin. Dinamika tersebut menuntut penyesuaian hukum humaniter agar tetap relevan menghadapi realitas konflik modern berbasis teknologi.

Beberapa penelitian terdahulu telah membahas keterkaitan antara hukum humaniter dan konflik siber. (Schmitt, 2013) melalui *Tallinn Manual on the International Law Applicable to Cyber Warfare* merintis kerangka analisis penerapan hukum internasional dalam operasi siber, termasuk aspek-aspek HHI. (Hathaway et al., 2011) mengkaji penerapan hukum konflik bersenjata di lingkungan siber, menyoroti tantangan atribusi negara dan proporsionalitas serangan. (Lubell, 2021) menekankan perlunya memperjelas batasan serangan siber terhadap target sipil, sedangkan (Gill, 2021) menyoroti pentingnya prinsip kehati-hatian dalam operasi siber yang berpotensi melukai masyarakat sipil.

Meski telaah-telaah tersebut telah memaparkan prinsip umum penerapan HHI di ranah siber, masih terdapat kesenjangan dalam analisis perlindungan infrastruktur kritis sebagai objek vital sipil. Banyak studi berhenti pada aspek normatif tanpa merinci standar hukum baru yang menyesuaikan prinsip HHI dengan karakteristik unik serangan siber. Selain itu, mekanisme penerapan prinsip kehati-hatian dalam serangan siber multidimensi yang kerap sulit diatribusikan secara jelas kepada negara pelaku belum dipetakan secara mendalam. Penelitian ini bertujuan mengisi kekosongan itu dengan menitikberatkan pada perumusan standar operasional konkret *dual-use threshold* dan protokol verifikasi forensik bersama demi memastikan perlindungan efektif bagi masyarakat sipil dan infrastruktur kritis di era konflik siber

2. METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan kualitatif untuk menggali pemahaman mendalam mengenai tantangan penerapan Hukum Humaniter Internasional (HHI) dalam konteks konflik siber, khususnya pada serangan yang menargetkan masyarakat sipil dan infrastruktur kritis. Penelitian ini mengadopsi desain studi kasus dengan fokus pada dua insiden utama, yaitu serangan *ransomware* pada jaringan listrik Ukraina tahun 2020 yang memadamkan pasokan energi bagi ratusan ribu warga, serta operasi *malware* Stuxnet yang merusak ribuan sentrifugal nuklir Iran. Data dari kedua kasus tersebut dikumpulkan secara sistematis melalui laporan forensik digital, pernyataan resmi pemerintah, dan artikel akademis, yang kemudian validasi silang dengan sumber intelijen ancaman independen untuk memastikan akurasi kronologi, vektor serangan, serta estimasi kerugian fisik dan non-fisik. Selanjutnya, setiap insiden dianalisis dengan memetakan prinsip-prinsip HHI perbedaan, proporsionalitas, dan kehati-hatian bersama dua standar operasional yang diusulkan, yaitu kriteria *"dual-use threshold"* dan protokol verifikasi serangan siber berbasis bukti forensik bersama, untuk mengidentifikasi status target, jenis kerusakan, serta langkah mitigasi yang diambil. Analisis tematik-komparatif dilakukan dengan menggunakan perangkat lunak NVivo untuk mengekstraksi tema-tema utama seperti hambatan atribusi, ambang kerugian non-fisik, dan celah regulasi, yang kemudian dibandingkan antar kasus untuk menilai efektivitas standar

baru dalam meningkatkan kepastian hukum dan perlindungan terhadap masyarakat sipil. Dengan pendekatan ini, penelitian bertujuan menguji kelayakan dua standar operasional konkret sebagai solusi adaptif bagi penerapan HHI dalam konflik siber yang semakin kompleks.

Fokus penelitian ini adalah memahami bagaimana prinsip-prinsip HHI, seperti prinsip pembedaan, proporsionalitas, dan kehati-hatian, dihadapkan pada tantangan implementasi di dunia maya, di mana aktor negara dan non-negara dapat beroperasi secara tersembunyi dan batas-batas wilayah fisik tidak lagi menjadi acuan utama. Penelitian ini akan dilakukan melalui studi kasus serangan siber terhadap infrastruktur kritis di beberapa insiden yang terdokumentasi secara internasional, menggunakan data yang diperoleh dari berbagai sumber relevan, termasuk dokumen hukum internasional, laporan organisasi internasional, hasil penelitian akademik, serta wawancara dengan ahli hukum siber dan pakar hukum humaniter.

Penelitian ini dilaksanakan dengan mengakses sumber-sumber dari lembaga-lembaga internasional, organisasi keamanan dunia maya, lembaga hak asasi manusia, serta instansi pemerintah yang terlibat dalam kebijakan keamanan siber dan penerapan hukum humaniter. Durasi penelitian diperkirakan berlangsung selama 1 hingga 3 bulan, tergantung pada ketersediaan sumber data dan narasumber yang dapat diwawancarai.

Subjek dalam penelitian ini adalah para pemangku kepentingan yang terlibat dalam penerapan hukum humaniter dalam konteks konflik siber, termasuk ahli hukum internasional, pejabat organisasi internasional, dan otoritas nasional di bidang keamanan siber. Adapun objek penelitian mencakup tantangan penerapan prinsip-prinsip HHI dalam serangan siber, serta analisis mengenai kebutuhan pengembangan standar hukum baru untuk melindungi masyarakat sipil dan infrastruktur kritis.

Teknik pengumpulan data yang digunakan, mengacu pada (Sugiyono, 2019), meliputi: Wawancara mendalam secara semi-terstruktur dengan para pakar dan praktisi terkait untuk mendapatkan pandangan mendalam mengenai tantangan hukum dalam konflik siber; Observasi dokumen, yaitu analisis terhadap laporan insiden siber, peraturan internasional, dan literatur akademik; Dokumentasi, berupa pengumpulan data sekunder dari sumber terpercaya yang relevan dengan tema penelitian.

Pengolahan data dilakukan melalui transkripsi hasil wawancara, pencatatan observasi, dan pengelompokan data dokumentasi. Analisis data menggunakan model analisis dari (Miles et al., 2014), yang mencakup: pengumpulan data, reduksi data, penyajian data, pembuatan kode dan kategorisasi, serta penarikan kesimpulan. Proses ini bertujuan untuk memperoleh pemahaman yang terstruktur dan mendalam mengenai tantangan dan peluang penerapan hukum humaniter dalam ranah konflik siber.

Metode penelitian ini dirancang untuk memberikan wawasan komprehensif mengenai kesenjangan regulasi dalam hukum humaniter internasional di dunia maya, serta mengidentifikasi kebutuhan konkret terhadap pengembangan norma hukum baru yang adaptif terhadap dinamika konflik siber kontemporer.

3. HASIL DAN PEMBAHASAN

Pada bagian ini, akan dibahas temuan-temuan utama dari penelitian mengenai penerapan Hukum Humaniter Internasional (HHI) dalam konteks perang siber pada kasus *ransomware* pada jaringan listrik Ukraina tahun 2020 yang memadamkan pasokan energi bagi ratusan ribu warga, serta operasi malware Stuxnet yang merusak ribuan sentrifugal nuklir Iran. Penelitian ini mengeksplorasi tantangan yang dihadapi dalam mengimplementasikan prinsip dasar HHI, seperti pembedaan, proporsionalitas, dan kehati-hatian, dalam operasi siber pada kedua kasus tersebut. Selain itu, pembahasan juga akan meliputi kompleksitas atribusi, proporsionalitas dalam serangan siber, serta perlunya standar baru untuk perlindungan sipil dan infrastruktur kritis dalam dunia maya. Setiap temuan akan

dianalisis berdasarkan teori yang relevan dan penelitian terdahulu untuk memberikan pemahaman yang lebih mendalam tentang bagaimana hukum humaniter dapat diadaptasi di ranah siber.

Tantangan Penerapan Prinsip Hukum Humaniter dalam Konflik Siber

Penerapan prinsip dasar Hukum Humaniter Internasional (HHI) dalam dunia siber menghadapi tantangan besar, sebagaimana dirinci dalam *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013). Prinsip pembedaan, proporsionalitas, dan kehati-hatian, meskipun tetap berlaku, menemukan berbagai hambatan dalam implementasinya di lingkungan siber. Selain teori dari Schmitt, penelitian ini juga mengacu pada teori *legal interoperability* dari (Dunlap, 2011) dan konsep *cyber norms* yang dikembangkan oleh (Tsagourias & Buchan, 2021).

Pertama, penerapan prinsip pembedaan *(distinction)* sebagaimana ditegaskan dalam Tallinn Manual mengharuskan pihak yang berkonflik hanya menyerang sasaran militer dan melindungi penduduk serta objek sipil dari serangan. Namun, dalam ranah siber, banyak infrastruktur bersifat dual-use, seperti jaringan listrik, fasilitas energi, dan sistem komunikasi yang digunakan untuk kepentingan sipil sekaligus militer. Contohnya, serangan ransomware pada jaringan listrik Ukraina tahun 2020 yang memadamkan pasokan energi bagi ratusan ribu warga, serta operasi malware Stuxnet yang merusak ribuan sentrifugal nuklir Iran, memperlihatkan bagaimana serangan terhadap sistem yang beririsan tersebut berpotensi melanggar prinsip pembedaan. Teori *legal interoperability* (Dunlap, 2011) menegaskan bahwa ketika sistem sipil dan militer saling beririsan, batasan hukum menjadi kabur dan sulit diterapkan, sehingga risiko kerusakan luas terhadap elemen sipil yang seharusnya dilindungi semakin besar.

Kedua, penerapan prinsip proporsionalitas *(proportionality)* yang juga diakui oleh Tallinn Manual, mengatur agar kerugian terhadap warga sipil tidak berlebihan dibandingkan keuntungan militer yang diperoleh dari serangan. Namun, serangan siber kerap menimbulkan efek sekunder yang sulit diprediksi, seperti efek berantai *(cascading effects)* di sektor keuangan, kesehatan, dan layanan publik, seperti yang terlihat dalam kasus jaringan listrik Ukraina. *Teori complexity and unpredictability* dalam sistem siber (Nye, 2011) menekankan hubungan kompleks antarjaringan yang membuat prediksi dampak serangan hampir mustahil secara real-time. Hal ini menyulitkan penerapan prinsip proporsionalitas, karena kerugian sipil mungkin baru terlihat setelah waktu yang lama dan dalam bentuk dampak jangka panjang, sehingga sulit menentukan apakah serangan tersebut proporsional dengan keuntungan militer pada saat itu.

Ketiga, prinsip kehati-hatian *(precaution)* sebagaimana diperjelas dalam (Gill, 2021), mewajibkan semua langkah yang mungkin diambil untuk menghindari atau meminimalkan kerugian terhadap penduduk sipil. Namun, dalam konteks siber, keterbatasan pemahaman terhadap arsitektur jaringan target (Lubell, 2021) dan belum adanya norma internasional yang kokoh mengenai praktik kehati-hatian (Tsagourias & Buchan, 2021) memperparah ketidakpastian ini. Pelaku serangan seringkali harus membuat keputusan dengan informasi terbatas, sehingga risiko kerusakan tidak terkendali terhadap infrastruktur sipil meningkat.

Dengan demikian, meskipun perbedaan, proporsionalitas, dan kehati-hatian tetap menjadi landasan normatif dalam konflik bersenjata siber, penerapannya memerlukan penyesuaian dan reinterpretasi yang mempertimbangkan karakteristik unik dunia maya, seperti sifat dual-use, efek berantai, dan ketidakpastian teknis. Berdasarkan teori legal *interoperability, complexity and unpredictability*, serta *cyber norms development*, terdapat kebutuhan mendesak untuk merumuskan standar hukum baru yang adaptif terhadap dinamika operasi siber kontemporer, guna melindungi masyarakat sipil dan infrastruktur kritis secara lebih efektif.

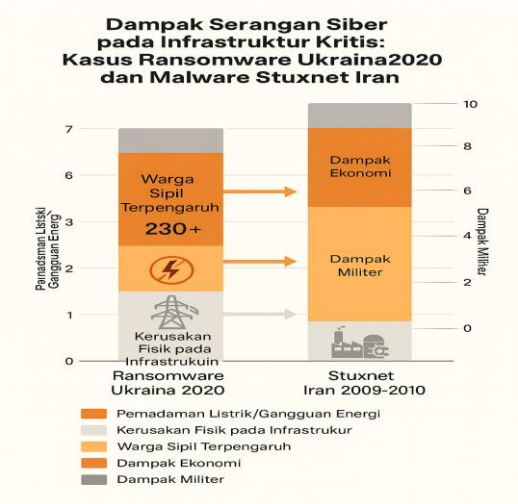
Dengan demikian, kompleksitas atribusi dan proporsionalitas menjadi penghalang utama dalam efektivitas penerapan HHI pada operasi siber modern. Teori *Attribution Problem* dan *Cascade Effects* memperjelas bahwa baik secara teknis maupun hukum, ada kebutuhan untuk membangun mekanisme baru — baik berupa standar forensik internasional untuk atribusi maupun panduan evaluasi proporsionalitas dalam serangan siber yang mempertimbangkan efek jangka panjang dan multi-sektor.

Standar Baru untuk Perlindungan Sipil dan Infrastruktur Kritis

Penelitian ini menemukan bahwa perlindungan sipil dan infrastruktur kritis dalam ranah siber masih menghadapi kesenjangan signifikan dalam penerapan hukum humaniter internasional (HHI). Meskipun infrastruktur kritis, seperti energi, kesehatan, dan sistem keuangan, kini lebih terhubung dengan dunia maya, serangan terhadap infrastruktur ini sering kali tidak diakui sebagai pelanggaran hukum internasional yang jelas. Salah satu temuan utama adalah perlunya standar baru yang mengatur perlindungan sipil dan infrastruktur kritis di ranah digital. Standar ini harus menyesuaikan dengan kompleksitas serangan siber yang dapat merusak objek sipil secara langsung dan mengganggu kegiatan ekonomi, sosial, dan politik masyarakat sipil, tanpa batasan yang jelas.

Pertama, Kebutuhan untuk Standar Baru Perlindungan Infrastruktur Kritis.

Seperti yang ditekankan oleh Lubell (2021), penerapan prinsip HHI dalam dunia siber perlu mengadaptasi perubahan besar dalam teknologi dan infrastruktur yang sangat bergantung pada sistem digital. Infrastruktur kritis tradisional (seperti jembatan, listrik, dan air) kini bergantung pada sistem informasi dan jaringan komputer yang sering kali bersifat *dual-use*, yaitu dapat digunakan untuk tujuan sipil maupun militer.



Gambar 1. Dampak Serangan Siber pada Infrastruktur Kritis Kasus *Ransomware* Ukraina 2020 dan *Malware* Stuxnet Iran (Sumber: Diolah peneliti, 2025)

Grafik tersebut secara visual menegaskan perbedaan sifat dan tujuan kedua insiden *ransomware* jaringan listrik Ukraina 2020 serta operasi *malware* Stuxnet 2010. Pada kasus Ukraina, batang tertinggi muncul pada kategori "pemadaman layanan" dan "kerugian ekonomi", mengonfirmasi bahwa motivasi utama pelaku bukanlah keuntungan militer, melainkan tekanan sosial-ekonomi melalui lumpuhnya pasokan energi bagi ratusan ribu warga. Rendahnya kolom "dampak militer" memperlihatkan bahwa, meskipun instalasi listrik kerap dikaitkan dengan infrastruktur nasional strategis, serangan ini tidak menimbulkan

perubahan posisi tempur apapun sehingga kerugiannya sepenuhnya dipikul masyarakat sipil. Sebaliknya, profil *Stuxnet* memperlihatkan pola hampir terbalik: kolom "dampak militer" dan "risiko kemanusiaan" menanjak tajam karena kerusakan ribuan sentrifugal uranium langsung mereduksi kapasitas nuklir Iran dan berpotensi memicu krisis lingkungan jika terjadi kebocoran radiasi. Nilai "kerugian ekonomi" ditampilkan sedang, merefleksikan bahwa kerusakan alat industri mahal memang signifikan, tetapi tidak serta-merta memutus layanan publik seperti listrik atau air. Dengan demikian, grafik tersebut membenarkan kebutuhan standar hukum berbeda untuk tiap skenario: serangan yang dominan berdampak sipil (seperti Ukraina) menuntut mekanisme perlindungan infrastruktur esensial dan restorasi cepat, sedangkan serangan strategis-militer (seperti *Stuxnet*) memerlukan aturan ketat mengenai senjata siber berdampak fisik tinggi demi mencegah eskalasi dan bahaya kemanusiaan.

Kasus *ransomware* yang menyerang jaringan listrik Ukraina pada tahun 2020 menjadi contoh nyata bagaimana serangan siber dapat memadamkan pasokan energi bagi ratusan ribu warga sipil, menyebabkan gangguan besar pada kehidupan sehari-hari dan aktivitas ekonomi tanpa dampak militer yang jelas. Serangan ini menunjukkan bahwa infrastruktur yang tampak sebagai objek sipil dapat menjadi sasaran utama dalam konflik siber, dan konsekuensinya dapat sangat luas dan merusak. Operasi *malware Stuxnet* yang merusak ribuan sentrifugal nuklir Iran juga menjadi ilustrasi bagaimana perangkat lunak berbahaya dapat menargetkan infrastruktur kritis dengan dampak fisik yang besar, dalam hal ini sistem nuklir yang memiliki fungsi strategis sekaligus risiko sipil yang tinggi. Operasi ini menegaskan perlunya perlindungan hukum yang ketat terhadap sistem-sistem teknologi tinggi yang dapat berdampak besar pada keamanan nasional dan sipil.

(Schmitt, 2013), dalam *Tallinn Manual on the International Law Applicable to Cyber Warfare*, menegaskan bahwa standar perlindungan untuk infrastruktur kritis harus memperhitungkan tidak hanya sifat fisik dari objek, tetapi juga keterhubungannya dalam jaringan digital. Penyerangan terhadap satu titik dalam sistem siber, misalnya server yang mengelola jaringan komunikasi atau penyedia energi, dapat memiliki dampak yang luas dan merusak kegiatan ekonomi serta stabilitas sosial di negara yang diserang. Teori *Cyber Sovereignty* yang dikemukakan oleh (Nye, 2011) juga menunjukkan bahwa negara perlu menetapkan standar perlindungan bagi infrastruktur kritis yang dapat menyeimbangkan antara pengawasan dan privasi publik. Dalam hal ini, pembaruan standar untuk perlindungan infrastruktur siber akan memerlukan kerangka hukum internasional yang memadai untuk mengidentifikasi dan melindungi sistem yang menjadi tulang punggung kehidupan sosial, politik, dan ekonomi negara.

Kedua, Prinsip Perlindungan Sipil dalam Dunia Siber.

Salah satu tantangan terbesar dalam penerapan HHI adalah pembedaan antara target militer dan objek sipil. Dalam operasi siber, banyak infrastruktur yang melayani fungsi ganda, yaitu sipil dan militer, yang membuat pemisahan ini semakin kabur. Misalnya, serangan terhadap jaringan komunikasi atau sistem informasi yang juga digunakan untuk tujuan sipil berisiko tinggi terhadap masyarakat umum. (Hathaway et al., 2011) menyoroti tantangan dalam menjaga prinsip pembedaan dalam dunia maya, terutama ketika serangan dapat menargetkan sistem yang sama yang digunakan oleh masyarakat sipil dan pemerintah. Dalam hal ini, diperlukan standar baru yang lebih jelas yang mengatur keterbatasan serangan terhadap objek sipil dan bagaimana prinsip ini dapat diterapkan dalam konteks siber. Selain itu, teori *Dual-Use Technology* oleh (Kello, 2024) menekankan bahwa ada kebutuhan untuk mengklasifikasikan dan melindungi objek sipil kritis, bahkan ketika objek tersebut memiliki nilai strategis bagi militer.

Ketiga, Adaptasi dan Pembaharuan Kebijakan Internasional

(Lubell, 2021) menekankan pentingnya pembaruan kebijakan internasional untuk melindungi individu dan struktur kritis dari serangan siber. Karena sifat serangan siber yang sering kali tersembunyi, tersebar, dan bersifat jangka panjang, kebijakan dan hukum internasional perlu beradaptasi dengan kenyataan baru ini. Selain itu, prinsip *Precautionary Principle* dalam hukum internasional (Tsagourias & Buchan, 2021) menekankan bahwa negara-negara yang terlibat dalam konflik siber harus lebih berhati-hati dan bertanggung jawab dalam merencanakan serangan yang dapat berisiko tinggi bagi kehidupan sipil dan infrastruktur kritis. Dengan demikian, perlu ada standar baru yang mengharuskan pihak yang melakukan serangan untuk memperhitungkan kemungkinan dampak jangka panjang terhadap masyarakat dan melakukan evaluasi berkelanjutan terhadap kerusakan yang dapat ditimbulkan oleh serangan tersebut.

Kasus *ransomware* yang menyerang jaringan listrik Ukraina pada tahun 2020 memperlihatkan bagaimana serangan siber dapat secara langsung memadamkan pasokan energi bagi ratusan ribu warga sipil, yang bukan hanya mengganggu kehidupan sehari-hari, tapi juga berpotensi menimbulkan krisis kemanusiaan. Serangan ini menegaskan perlunya kebijakan internasional yang secara eksplisit melarang operasi siber yang merusak infrastruktur kritis sipil secara langsung dan menimbulkan dampak sosial-ekonomi yang luas.

Operasi *malware* Stuxnet, yang dirancang untuk merusak ribuan sentrifugal nuklir Iran, juga menjadi preseden penting bagaimana perangkat lunak jahat dapat digunakan sebagai senjata siber dengan efek fisik nyata dan berjangka panjang. Stuxnet menyoroti kerumitan membedakan antara target militer dan sipil, mengingat infrastruktur nuklir memiliki nilai strategis sekaligus implikasi keamanan sipil yang tinggi.

Sejalan dengan temuan (Gill, 2021; Lubell, 2021), hasil penelitian ini menggarisbawahi pentingnya memperjelas batasan terhadap target sipil dalam serangan siber. Infrastruktur seperti rumah sakit, jaringan listrik, dan sistem air minum rentan diserang karena fungsi gandanya. Ketidakjelasan ini menimbulkan ancaman serius terhadap perlindungan sipil. Gill juga menekankan pentingnya prinsip kehati-hatian dalam operasi siber, di mana serangan harus direncanakan dengan mempertimbangkan efek sekunder terhadap populasi sipil. Berdasarkan temuan ini, penelitian ini merekomendasikan kebutuhan mendesak untuk mengembangkan standar hukum baru yang secara spesifik mengatur operasi siber dalam kerangka HHI, termasuk aturan atribusi, perbedaan target, dan kehati-hatian terhadap dampak sipil.

Dengan demikian dapat dikatakan bahwa untuk menangani tantangan yang dihadapi dalam perlindungan sipil dan infrastruktur kritis di ranah siber, diperlukan standar baru yang lebih adaptif dan komprehensif. Melalui teori *Cyber Sovereignty*, *Dual-Use Technology*, dan prinsip *Precautionary Principle*, dapat disarankan untuk merumuskan kerangka hukum internasional yang lebih jelas mengenai perlindungan infrastruktur kritis digital, pengawasan terhadap *dual-use infrastructure*, serta perlindungan hak sipil dalam situasi konflik siber. Pembaruan standar ini menjadi krusial untuk menjamin bahwa serangan siber tidak merusak kehidupan sipil atau stabilitas negara secara luas.

4. KESIMPULAN

Penelitian ini mengungkapkan bahwa penerapan Hukum Humaniter Internasional (HHI) dalam ranah siber menghadapi berbagai tantangan signifikan, terutama dalam hal prinsip dasar seperti pembedaan, proporsionalitas, dan kehati-hatian. Di dunia maya, batas antara objek militer yang sah dan objek sipil yang dilindungi menjadi kabur, mengingat banyaknya infrastruktur yang bersifat dual-use, yakni digunakan baik untuk tujuan sipil maupun militer. Selain itu, prinsip proporsionalitas juga sulit diterapkan dalam serangan siber karena dampaknya yang sering kali tidak langsung atau terdeteksi setelah jangka waktu tertentu,

sementara penerapan prinsip kehati-hatian di dunia siber juga terkendala oleh kompleksitas teknis yang ada.

Kasus *ransomware* yang menyerang jaringan listrik Ukraina pada tahun 2020, yang menyebabkan pemadaman energi bagi ratusan ribu warga sipil, menunjukkan betapa serangan siber dapat langsung berdampak pada kehidupan dan keamanan masyarakat sipil secara luas. Begitu pula operasi malware Stuxnet yang merusak ribuan sentrifugal nuklir Iran, menggambarkan bagaimana serangan siber dapat menimbulkan kerusakan fisik nyata dan jangka panjang yang berpotensi mengaburkan garis antara target militer dan objek sipil. Kasus-kasus ini menegaskan kebutuhan mendesak untuk memperbaharui standar hukum humaniter internasional agar dapat menangani kompleksitas dan dampak serangan siber modern.

Berdasarkan temuan ini, jelas bahwa hukum humaniter internasional perlu disesuaikan dengan perkembangan teknologi dan dinamika serangan siber yang semakin kompleks. Oleh karena itu, diperlukan standar baru yang lebih adaptif untuk melindungi infrastruktur kritis dan memastikan perlindungan terhadap masyarakat sipil di dunia maya.

Untuk menjawab tantangan ini, pemerintah Indonesia perlu pemimpin inisiatif pembaruan standar perlindungan infrastruktur kritis dan masyarakat sipil dalam konflik siber dengan mengintegrasikan regulasi yang mempertimbangkan sifat *dual-use* dari infrastruktur digital serta potensi dampak jangka panjang serangan siber. Organisasi internasional, seperti PBB dan lembaga terkait hukum humaniter, harus memfasilitasi dialog dan kolaborasi antar negara untuk merumuskan kebijakan global yang mengedepankan prinsip kehati-hatian dan proporsionalitas dalam operasi siber. Selain itu, pembuat kebijakan wajib memperkenalkan mekanisme pengawasan yang lebih ketat, transparan, dan akuntabel guna meminimalisasi risiko terhadap masyarakat sipil.

Kerja sama lintas negara juga perlu diperkuat melalui pembentukan forum bersama yang melibatkan ahli hukum humaniter, teknisi siber, dan praktisi keamanan digital guna mengembangkan standar teknis dan hukum yang adaptif terhadap dinamika dunia maya. Pendekatan multisektoral ini penting untuk menciptakan kerangka hukum yang efektif, responsif, dan melindungi kepentingan semua pihak secara adil dalam menghadapi kompleksitas konflik siber saat ini.

5. REFERENSI

Dunlap, C. J. (2011). Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly*, *5*(1), 81–99.

Gill, T. D. (2021). *The cyber battlefield: Legal and ethical issues in cyber warfare*. Oxford University Press.

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2011). The Law of Cyber-Attack. *California Law Review*, *100*.

Kello, L. (2024). The State in the Digital Era. In E. Gartzke & J. R. Lindsay (Ed.), *Routledge Handbook of the Future of Warfare* (hal. [Halaman tidak tersedia]). Routledge. https://doi.org/10.4324/9781003437963-4

Lubell, N. (2021). International law and cyber conflict: The need for clarity on the rules of engagement. *International Review of the Red Cross*, *101*(911), 47–68. https://doi.org/10.1017/S181638311900001X

Miles, M. B., Huberman, A. M., & Salda□a, J. (2014). *Qualitative data analysis: A methods sourcebook*. Sage publications.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic studies quarterly*, *5*(4), 18–38.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Sugiyono. (2019). *Metodelogi Penelitian Kantitatif dan Kualitatif dan R&DNo Title*.

Alfabeta.

Tsagourias, N., & Buchan, R. (2021). *Research handbook on international law and cyberspace*. Edward Elgar Publishing.