BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Sejarah perkembangan peradaban manusia telah menunjukkan bahwa karakter dari peperangan terus berevolusi seiring dengan munculnya inovasi teknologi baru yang mengubah metode beperang dalam penggunaan kekuatan bersenjata. *The International Committee of the Red Cross* (ICRC) mencatat bahwa perkembangan kemajuan teknologi telah menghasilkan metode dan sarana peperangan baru yang menuntut penyesuaian terhadap kerangka hukum internasional.[1] Pada dasarnya hukum internasional khusunya pada piagam perserikatan bangsa–bangsa pasal 2 ayat (4) telah mengatur tentang pelarangan penggunaan kekerasan dalam perang terhadap negara lain yang bertentangan dengan tujuan perserikatan bangsa bangsa yaitu sebagai berikut :

> *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*[2]
> (Semua Anggota wajib menahan diri, dalam hubungan internasionalnya, dari ancaman atau penggunaan kekuatan yang ditujukan terhadap keutuhan wilayah atau kemerdekaan politik negara mana pun, atau dengan cara apa pun yang bertentangan dengan Tujuan Perserikatan Bangsa-Bangsa.)[3]

Namun, meskipun telah diatur mengenai metode berperang memasuki abad ke–21, dunia telah mengalami perkembangan dan pergeseran teknologi yang strategis, dimana ruang siber telah menciptakan lingkungan baru yang memungkinkan terjadinya konflik secara terus menerus pada ambang batas perang

---

[1] *International Committee of the Red Cross (ICRC),* 2015, "*International Humanitarian Law and the Challenges of Contemporary Armed Conflicts", Report for the 32nd International Conference of the Red Cross and Red Crescent*, Geneva, hlm. 38.

[2] *Charter of The United Nations and Statue of The International Court of Justice, 1945, San Frasisco, article 2.*

[3] Terjemahan dari DeepL..

terbuka, namun tetap memberikan dampak yang signifikan terhadap stabilitas kedaulatan negara.[4]

Perkembangan teknologi ini ditandai dengan adanya pengakuan bahwa ancaman siber terhadap keamanan suatu negara sudah bersifat semakin kompleks, destruktif, memaksa, dan semakin sering terjadi.[5] Eksistensi ruang siber sebagai domain konflik kontemporer juga telah direspons secara akademis melalui penyusunan *Tallin Manual 2.0 on the International Law Applicble to Cyber Operations* yang merupakan aturan kajian akademik yang sistematis tentang bagaimana hukum internasional, terutama hukum penggunaan kekuatan dan hukum humaniter internasional, berlaku pada operasi siber dan konflik siber. Dokumen ini tidak mengikat secara hukum, tetapi sering menjadi referensi utama bagi penasihat hukum, militer, dan kebijakan di bidang pertahanan siber.[6]

Berdasarkan aturan 80 *Tallin Manual 2.0 on the International Law Applicble to Cyber Operations* dituliskan sebagai berikut :

> *"Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict."*[7]
>
> (Operasi siber yang dilaksanakan dalam konteks konflik bersenjata tunduk pada hukum konflik bersenjata.)[8]

Aturan ini, menegaskan bahwa setiap operasi siber yang dilakukan dalam konteks konflik bersenjata wajib tunduk pada norma-norma Hukum Humaniter Internasional (HHI), khususnya yang berkaitan dengan aturan mengenai metode dan sarana

---

[4] Christopher Whyte dan Brian Mazanec, 2018, *Understanding Cyber Warfare: Politics, Policy and Strategy*, Routledge, hlm. 11.

[5] NATO,"*Brussels Summit Communiqué*", diakses dari https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communique, dikunjungi pada tanggal 17 januari 2026 jam 20.44.

[6] Michael N. Schmitt, 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

[7] *Ibid, rule* 80.

[8] Terjemahan dari DeepL.

berperang. Hal ini memperjelas bahwa meskipun ruang siber memiliki karakteristik virtual, setiap operasi digital yang memiliki dampak destruktif maupun koersif tetap berada dalam cakupan yurisdiksi hukum internasional.

Modernisasi dari metode peperangan tidak lagi hanya berfokus pada penghancuran fisik, melainkan telah bergeser pada upaya manipulasi informasi untuk melumpuhkan sistem lawan tanpa harus melibatkan kontak fisik dan adu senjata secara langsung. ICRC mencatat bahwa operasi siber kini telah menjadi sarana dan metode peperangan yang nayata, dimana serangan melalui jaringan digital memiliki resiko yang tinggi untuk menimbulkan dampak kemanusiaan yang luas bagi penduduk sipil sebagaimana operasi militer fisik.[9] Maka, kapabilitas militer saat ini sangat bergantung pada kemampuan sebuah negara dalam menguasai teknologi informasi guna memenangkan narasi strategis dan mengelola risiko kedaulatan di ruang digital yang semakin kompleks ini.

Metode yang digunakan dalam perang sebenarnya tidaklah tidak terbatas, atau bisa diartikan metode atau cara acara yang digunakan untuk beperang itu terbatas pada aturan tertentu yang dimana aturan ini dimuat dalam Konvensi Den Haag 1907 sebagai berikut:

> *"The right of belligerents to adopt means of injuring the enemy is not unlimited."*[10]
>
> (Hak pihak-pihak yang bertikai untuk menggunakan cara-cara yang dapat melukai musuh tidaklah tak terbatas.)[11]

Meskipun terdapat aturan yang secara tegas membatasi metode berperang seiring dengan pergeseran metode peperangan ke ruang digital, muncul suatu inovasi teknologi yang secara radikal memperluas ancaman dalam peperang informasi, yaitu

---

[9] *International Committee of the Red Cross (ICRC), Op.Cit., hlm. 39-40.*
[10] *The Hague Conventions, 1907, article 22.*
[11] Terjemahan dari Google DeepL.

Deepfake. Menurut Enes Altuncu, Virginia N. L. Franqueira, dan Shujun Li, *deepfake* merupakan bentuk pemalsuan digital yang berbasis *Deep Learning* terhadap gambar, video, dan audio yang memungkinkan seseorang dibuat seolah-olah mengucapkan atau melakukan sesuatu yang tidak pernah ia ucapkan atau lakukan.[12] Secara teknis, pembuatan *deepfake* dilakukan dengan memanfaatkan algoritma kecerdasan buatan (*Artifical Intelligence*) berbasis *Generative Adversial Networks (GANs)* yang mampu menghasilkan konten visual dan audio palsu secara realistis.[13] Pentingnya teknologi ini bukan terletak pada aspek teknisnya, melainkan pada kapasitas *deepfake* yang dapat memanipulasi video atau audio orang sungguhan dan memungkinkan terciptanya peniruan realistis sehingga seolah olah seseorang telah mengatakan atau melakukan sesuatu.[14]

Deepfake tidak bekerja dengan cara menghancurkan objek materiil secara fisik, melainkan memanipulasi domain kognitif dan informasi lawan.[15] Oleh karena itu penetuan posisi *deepfake* dalam kerangka hukum internasional sangat bergantung pada pemisahan antara *means* (sarana) dan *methods* (metode) perang. Menurut Jean-Marie Henckaerts dan Louise Doswald-Beck, sarana berperang (*means of warfare*) merupakan pada aspek fisik berupa senjata dan sistem persenjataan yang berfungsi dalam operasi militer untuk menyerang dan melumpuhkan lawan. Sementara itu, metode berperang (*methods of warfare*) merupakan sistem dan taktik berperang serta tata cara penggunaan senjata tersebut untuk melemahkan atau melumpuhkan lawan.[16] Sejalan dengan itu, *International Committee of the Red Cross* (ICRC, 1987)

---

[12] Enes Altuncu, Virginia N. L. Franqueira, dan Shujun Li, 2024, "*Deepfake: Definitions, Performance Metrics and Standards, Datasets, and a Meta-Review*," *Frontiers in Big Data*, Vol. 7, 2024, hlm. 2.

[13] Ian J. Goodfellow, et Al., 2020, "*Generative Adversarial Networks"*, *Communications of the ACM*, Vol. 63, No. 11, hlm. 139.

[14] Robert Chesney & Danielle Citron, 2019, "*Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*', *California Law Review"*, Vol. 107, hlm. 1759.

[15] *Ibid.*

[16] Jean-Marie Henckaerts & Louise Doswald-Beck, 2005, "*Customary International Humanitarian Law*", Cambridge, Cambridge University Press, Vol. I, 2005, hlm 161. .

menegaskan bahwa metode berperang mencakup segala bentuk cara yang diadopsi oleh pihak bertikai dengan tujuan melemahkan atau melumpuhkan kekuatan militer lawan.[17] Spektrum taktik dan politik dalam pertempuran ini menggaungkan kembali pemikiran Carl von Clausewitz (1984) dalam karyanya *On War*, yang menyatakan bahwa perang pada hakikatnya merupakan kelanjutan dari instrumen politik melalui pemanfaatan cara-cara lain.[18]

Berdasarkan penejelasan tersebut *deepfake* tidak dapat dikategorikan sebagai sarana atau alat perang (*means of warfare*) layaknya misil atau bom siber karna *deepfake* secara konseptual dapat dianalogikan sebagai metode berperang (*methods of warfare*), yaitu sebagai suatu skema, strategi, atau tata cara bertempur melalui manipulasi psikologis dan disorientasi informasi.[19] Hal ini menjadikan *deepfake* sebagai instrumen yang potensial sebagai metode peperangan kognitif dan metode berperang psikologis yang merupakan suatu sistem militer yang tidak lagi mengandalkan destruksi fisik, melainkan berupaya memengaruhi pikiran, emosi, sikap, hingga tingkah laku dari pihak lawan, yang secara langsung menantang prinsip integritas informasi dan kejujuran dalam berkonflik melalui manipulasi persepsi secara sistematis.[20]

Adanya integrasi *deepfake* ke dalam metode peperangan menghadirkan tantangan yuridis yang kompleks terhadap implementasi Hukum Internasional. Sebagaimana diamanatkan dalam laporan ICRC, penggunaan teknologi digital sebagai sarana berperang menuntut adanya peninjauan kembali terhadap efektivitas prinsip-prinsip perlindungan penduduk sipil, khususnya yang berkaitan dengan

---

[17] *International Committee of the Red Cross (ICRC), 1987, Commentary on the Additional Protocols of 1977 to the Geneva Conventions of 12 August 177.*

[18] Clausewitz, C. von, 1984, "*On War*", Princeton University Press, hlm. 128.

[19] *Ibid.*

[20] Galih Adi Putra, Muhammad Hadianto Wirajuda, dan Helda Risman,2024, "Perang Psikologis sebagai Faktor Pendorong dalam Perkembangan Strategi Militer Selama Perang Teluk 1990-1991," *Advances in Social Sciences Research Journal* 11, no. 1, hlm. 97

aturan mengenai operasi penyesatan (*deception)*.[21] Kehadiran *deepfake* bertransformasi menjadi sarana operasi psikologis berskala luas yang mengaburkan batasan legalitas antara metode perang yang diperbolehkan (*stratagems*) dan tindakan pengkhianatan yang dilarang (*perfidy*) dalam kerangka hukum internasional.[22]

Urgensi dari permasalahan penggunaan *deepfake* sebagai metode berperang ini dapat dilihat secara nyata melalui berbagai persitiwa global yang menunjukkan bahwa *deepfake* telah diadopsi sebagai metode berperang yang baru dalam peperangan modern. Salah satu contoh terdapat dalam kasus konflik Rusia - Ukraina, penggunaan konten audio–visual hasil produksi melalui teknologi AI, dimana *deepfake* dimanfaatkan secara ofensif sebagai metode untuk melemahkan struktur komando lawan tanpa kontak fisik secara langsung. Peristiwa penting terjadi pada maret 2022, Ketika beredar video palsu presiden Volodymyr Zelensky yang bertujuan melakukan sabotase kognitif dengan menginstruksikan pasukannya untuk menyerah.[23] Selanjutnya, disusul dengan video panglima Valeri Zoluzhnyi menyerukan kepada angkatan bersenjata untuk meninggalkan zona tempur dan melakukan kudeta militer terhadap pemerintah pusat.[24]

Pada tahun 2023, spektrum serangan *deepfake* dalam konflik ini meluas dengan menyasar kedaulatan informasi di wilayah Federasi Rusia. Jaringan radio dan televisi di wilayah perbatasan strategis secara militer—seperti Belgorod, Voronezh,

---

[21] International Committee of the Red Cross (ICRC), *Op.Cit.*, hlm. 38-39.

[22] Gary P. Corn, 2026, "*Cognitive Warfare: Generative AI, False Realities, and International Humanitarian Law"*, Joint PIJIP/TLS Research Paper Series, American University Washington College of Law, hlm. 9.

[23] Bansal, R., & Petti, M, "*A deepfake video of Zelenskyy is a warning of how the technology could be used to manipulate people during the war"*. NPR. diakses dari https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia, dikunjungi pada tanggal 18 Januari 2026 jam 20.35 WIB.

[24] Meta.mk News Agency, "*Deepfake* video *manipulates that General Zaluzhny is preparing a military coup*", diakses dari https://meta.mk/en/deepfake-video-manipulates-that-general-zaluzhny-is-preparing-a-military-coup/ dikunjungi pada 18 Januari 2026 jam 21.45 WIB.

dan Rostov—menyiarkan pidato darurat palsu yang diklaim berasal dari Presiden Vladimir Putin. Siaran tersebut, yang menampilkan sosok Putin buatan AI, mengumumkan invasi darat pasukan Ukraina melintasi perbatasan, sekaligus memerintahkan pemberlakuan darurat militer nasional, mobilisasi umum, serta evakuasi segera warga sipil ke pedalaman Rusia,[25] hal ini menunjukkan bahwa *deepfake* digunakan sebagai metode peperangan informasi untuk menciptakan disintegrasi militer dari dalam.

Rangkaian peristiwa ini membuktikan bahwa *deepfake* telah bertranformasi dari sekadar konten disinformasi menjadi insturmen perang non-kinetik metode berperang yang sistematis. Analisis terhadap kasus–kasus ini menyingkap adanya kebutuhan mendesak untuk meninjau kembali batasan legalitas dalam Hukum Internasional, khususnya terkait kapan penggunaan teknologi AI ini melampaui batas muslihat perang yang diperbolehkan dan menjadi tindakan yang dilarang karena merusak asas–asas dasar dalam berkonflik secara internasional.

Eksistensi *deepfake* sebagai metode berperang menimbulkan perdebatan mendalam yaitu mengenai batasan legalitasnya karna dalam Hukum Internasional terdapat aturan yang mengatur tentang legal dan illegal nya sebuah metode berperang yaitu adanya muslihat perang (*ruse of war*) sebagai tindakan yang sah untuk menyesatkan lawan dan adanya peraturan yang melarang keras tindakan *perfidy* karena tindakan tersebut mengeksploitasi itikad baik lawan melalui pemalsuan status perlindungan guna membunuh, melukai, atau manawan lawan. Muslihat perang (*Ruses of war*) diatur dalam pasal 24 konvensi den haag 1907 dan pasal 37 (2) Protokol Tambahan I 1977 sebagai berikut :

Pasal 24 Konvesi den haag 1907:

[25] Neil MacFarquhar, "*Deepfake Video of Putin Is Broadcast on Some Russian Networks,*" *The New York Times*, diakses dari https://www.nytimes.com/2023/06/05/world/europe/putin-deep-fake-speech-hackers.html, dikunjungi pada 1 maret 2026 jam 14.16. WIB

"Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[26]
(Tipu muslihat dan penerapan langkah-langkah yang diperlukan untuk memperoleh informasi mengenai musuh dan negara tersebut dianggap diperbolehkan.)[27]

Pasal 37 ayat (2) Protokol Tambahan 1 1977

"Ruses of war are not prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation."[28]
(Tipu Muslihat tidak dilarang. Taktik semacam itu adalah tindakan yang dimaksudkan untuk menyesatkan lawan atau mendorongnya bertindak secara sembrono, namun tidak melanggar aturan hukum internasional apa pun yang berlaku dalam konflik bersenjata dan tidak bersifat licik karena tidak menimbulkan kepercayaan lawan terkait perlindungan berdasarkan hukum tersebut. Berikut ini adalah contoh-contoh taktik semacam itu: penggunaan kamuflase, umpan, operasi palsu, dan informasi yang menyesatkan.)[29]

Serta diatur juga pada *Tallin Manual 2.0* pada aturan 123 tentang *ruses of war* sebagai berikut:

"Cyber operations that qualify as ruses of war are permitted."[30]

(Operasi siber yang memenuhi kriteria sebagai tipu muslihat perang diperbolehkan.)[31]

Pada paradigma ini, *deepfake* dapat dipandang sebagai bentuk perkembangan digital dari taktik penyesatan informasi konvensional, seperti penggunaan umpan (*decoys*) atau simulasi serangan, yang diarahkan untuk menimbulkan kebingungan taktis pada pihak lawan tanpa secara langsung melanggar ketentuan hukum internasional. Permasalahan hukum muncul ketika *deepfake*

---

[26] *The Hague Conventions, 1907, Op.Cit, article 24.*
[27] Terjemahan dari DeepL.
[28] *Additional Protocol I 1977, Op.cit., article 37(2).*
[29] Terjemahan dari DeepL.
[30] Michael N. Schmitt (Ed.), 2017, *Op.cit, rule 122.*
[31] Terjemahan dari Google DeepL.

digunakan dengan cara yang memenuhi unsur pengkhianatan (*perfidy*). Berdasarkan pasal 23 konvensi den haag 1907 dan pasal 37(1) Protokol Tambahan I 1977 tentang *perfidy* yang berisi sebagai berikut:

Pasal 23 Konvesi den haag 1907 :

> *"In addition to the prohibitions provided by special Conventions, it is especially forbidden*
> *(a) To employ poison or poisoned weapons;*
> *(b) To kill or wound treacherously individuals belonging to the hostile nation or army;*
> *(c) To kill or wound an enemy who, having laid down his arms, or having no longer means of defence, has surrendered at discretion;*
> *(d) To declare that no quarter will be given;*
> *(e) To employ arms, projectiles, or material calculated to cause unnecessary suffering;*
> *(f) To make improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention;*
> *(g) To destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war;*
> *(h) To declare abolished, suspended, or inadmissible in a court of law the rights and actions of the nationals of the hostile party. A belligerent is likewise forbidden to compel the nationals of the hostile party to take part in the operations of war directed against their own country, even if they were in the belligerent's service before the commencement of the war."*[32]
> (Selain larangan-larangan yang diatur dalam Konvensi-konvensi khusus, dilarang secara khusus
> (a) Menggunakan racun atau senjata beracun;
> (b) Membunuh atau melukai secara licik individu-individu yang merupakan bagian dari negara atau angkatan bersenjata musuh;
> (c) Membunuh atau melukai musuh yang, setelah meletakkan senjatanya atau tidak lagi memiliki sarana pertahanan, telah menyerahkan diri tanpa syarat;
> (d) Menyatakan bahwa tidak akan diberikan ampun;
> (e) Menggunakan senjata, proyektil, atau bahan yang dirancang untuk menimbulkan penderitaan yang tidak perlu;
> (f) Menyalahgunakan bendera gencatan senjata, bendera nasional, atau lambang militer dan seragam musuh, serta tanda pengenal Konvensi Jenewa;
> (g) Menghancurkan atau menyita harta benda musuh, kecuali jika penghancuran atau penyitaan tersebut mutlak diperlukan oleh kebutuhan perang;
> (h) Menyatakan bahwa hak-hak dan tindakan warga negara pihak yang bermusuhan telah dicabut, ditangguhkan, atau tidak dapat diajukan ke pengadilan. Pihak yang berperang juga dilarang memaksa warga negara

[32] *The Hague Conventions, 1907, Op.Cit, article 23.*

pihak yang bermusuhan untuk ikut serta dalam operasi perang yang ditujukan terhadap negara mereka sendiri, meskipun mereka telah berada dalam dinas pihak yang berperang sebelum dimulainya perang.)[33]

Pasal 37 ayat (1) Protokol tambahn 1 1977

" It is prohibited to kill, injure or capture an adversary by resort to per- fidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy. The following acts are exam- ples of perfidy:

a) the feigning of an intent to negotiate under a flag of truce or of a surrender;
b) the feigning of an incapacitation by wounds or sickness;
c) the feigning of civilian, non-combatant status; and
d) the feigning of protected status by the use of signs, emblems or uni- forms of the United Nations or of neutral or other States not Parties to the conflict."[34]

(Dilarang membunuh, melukai, atau menangkap musuh dengan cara melakukan pengkhianatan. Tindakan yang bertujuan untuk memperoleh kepercayaan musuh sehingga ia meyakini bahwa ia berhak atas, atau wajib memberikan, perlindungan berdasarkan aturan hukum internasional yang berlaku dalam konflik bersenjata, dengan niat untuk mengkhianati kepercayaan tersebut, merupakan pengkhianatan. Tindakan-tindakan berikut ini merupakan contoh pengkhianatan:

a) berpura-pura berniat untuk bernegosiasi di bawah bendera gencatan senjata atau menyerah;
b) berpura-pura tidak mampu bertempur karena luka atau sakit;
c) berpura-pura memiliki status sipil atau non-kombatan; dan
d) berpura-pura memiliki status terlindungi dengan menggunakan tanda, lambang, atau seragam Perserikatan Bangsa-Bangsa atau negara-negara netral atau negara-negara lain yang bukan pihak dalam konflik.)[35]

Serta peraturan 122 *Tallin Manual* 2.0 tentang *perfidy* sebagai berikut:

"In the conduct of hostilities involving cyber operations, it is pro- hibited to kill or injure an adversary by resort to perfidy. Acts that invite the confidence of an adversary to believe that he or she is entitled to, or is obliged to accord, protection under the law of armed conflict, with intent to betray that confidence, constitute perfidy."[36]

(Dalam pelaksanaan pertempuran yang melibatkan operasi siber, dilarang membunuh atau melukai lawan dengan cara melakukan pengkhianatan. Tindakan yang membuat lawan percaya bahwa ia berhak atas, atau wajib

[33] Terjemahan dari DeepL.
[34] *Additional Protocol I 1977, Op.cit., article 37(1).*
[35] Terjemahan dari DeepL.
[36] Michael N. Schmitt (Ed.), 2017, *Op.cit.*, rule 122, hlm. 491.

memberikan, perlindungan berdasarkan hukum konflik bersenjata, dengan niat untuk mengkhianati kepercayaan tersebut, merupakan pengkhianatan.)[37]

Masalah fundamental dalam pengguanaan *deepfake* adalah kemampuannya untuk memalasukan identitas digital otoritas tertinggii (seperti dalam kasus Zelensky dan Zoluzhny) guna memberikan instruksi militer yang destruktif. Hal ini menciptakan wilayah abu-abu yuridis yang kritis yaitu apakah pemalsuan visual dan audio seorang panglima tertinggi dikategorikan sebagai taktik cerdik untuk mencegah persepsi lawan, atau merupakan bentuk pengkhianatan (*perfidy*) karena secara sengaja menyalahgunakan kepercayaan fundamental yang ada dalam rantai komando militer dan perlindungan terhadap identitas pejabat negara. Lebih jauh lagi, penggunaan *deepfake* dalam operasi siber intensitas rendah sering kali memanfaatkan ambiguitas doktrinal dalam prinsip non-intervensi.[38] Sebagaimana dikemukakan oleh Sean Watts, operasi siber yang dilakukan di bawah ambang batas serangan bersenjata tetap dapat dikategorikan sebagai pelanggaran hukum internasional apabila tindakan tersebut mengandung unsur pemaksaan (*coercion*) yang bertujuan untuk mendikte urusan internal atau eksternal negara target secara diktator.[39] Penggunaan *deepfake* untuk memicu kudeta atau pembangkangan militer, seperti dalam kasus Zaluzhnyi, merupakan bentuk intervensi yang melampaui batas pengaruh diplomatik yang sah dan masuk ke dalam kategori intervensi yang dilarang karena menargetkan jantung kedaulatan politik suatu negara.[40]

Ketidakjelasan kriteria dalam menentukan garis pemisah antara *ruse of war* (tipu muslihat yang legal) dan *perfidy* (pengkhianatan) yang dilarang ini bukan hanya masalah teknis, melainkan ancaman terhadap efektivitas Hukum Internasional itu

---

[37] Terjemahan dari DeepL.

[38] Sean Watts, 2014, *Low-intensity Cyber Operations and the Principle of Non-intervention*, *Tallinn Papers*, No. 5 hlm. 1.

[39] *Ibid*, hlm.10.

[40] *Ibid*, hlm.12.

sendiri. Tanpa adanya interpretasi hukum yang tegas, penggunaan *deepfake* berisiko mengubah ruang digital menjadi medan tempur tanpa aturan, di mana fabrikasi realitas menjadi alat untuk melegitimasi pelanggaran hukum perang.[41]

Selain itu, dalam situasi konflik bersenjata, kerangka hukum tetap bersandar pada aturan Hukum Humaniter Internasional yang diatur dalam Konvensi Jenewa 1949 dan Protokol Tambahan I 1977, khususnya terkait batasan muslihat perang yang dilarang untuk melakukan pengkhiatan terhadap lawan dalam pasal 37 ayat (1) Protokol Tambahan I 1977. Mengingat instrumen hukum klasik tersebut belum menjangkau dimensi teknologi kecerdasan buatan secara spesifik, *Tallin Manual 2.0 on the international law applicable to cyber operations* digunakan sebagai rujukan untuk menerjemahkan norma norma tersebut ke dalam realitas siber. *Tallin Manual 2.0* berperan krusial dalam memberikan parameter mengenai batasan kedaulatan di ruang digital, serta menyediakan alat uji melalui *rule 122* dan *rule 123* untuk menentukan apakah pemalsuan identitas digital melalui *deepfake* merupakan bentuk pekhianatan (*perfidy*) yang dilarang atau sekadar strategi penyesatan yang sah dalam peperangan.

Integrasi antara dasar hukum internasional positif dengan panduan interpretatif dari *Tallin Manual 2.0* memberikan kejelasan yuridis mengenai tanggungjawab negara atas penggunaan teknologi siber destruktif yang menciderai kedaulatan dan tatanan hukum internasional. Meskipun prinsip–prinsip hukum internasional dan *Tallin Manual 2.0* telah menyediakan kerangka awal, penggunaan *deepfake* dalam konflik bersenjata tetap menyisakan ambiguitas yang signifikan.

Masalah utama terletak pada belum adanya *consensus* internasional mengenai ambang batas (*threshold*) pemaksaan (*coercion*) dalam ruang siber.

[41] Robert Chesney & Danielle Citron, 2019, *Op.Cit*, hlm. 1778.

Sebagaimana dikemukan oleh Seab Watts, Negara-negara belum mencapai kesepakatan mengenai sejauh mana sebuah manipulasi informasi dapat dikategorikan sebagai intervensi illegal yang melanggar kedaulatan.[42] Pada kasus *deepfake*, batas antara perang informasi yang sah dan intervensi yang dilarang menjadi sangat kabur karena teknologi ini mampu memalsukan realitas dengan tingkat akurasi yang hampir sempurna.

Berdasarkan pemaparan masalah diatas, diperlukan sebuah kajian mendalam untuk merumuskan batasan yuridis yang lebih tegas terhadap penggunaan *deepfake*. Tanpa adanya kapasitas hukum, penggunaan kecerdasan buatan dalam peperangan siber tidak hanya akan mengancam kedaulatan negara target, tetapi juga berpotensi merusak stabilitas hukum internasional secara keseluruhan.[43] Hal inilah yang melatarbelakangi penulis, untuk mengurai dan menganalisis bagaimana hukum internasional seharusnya merespons tantangan *deepfake* guna memastikan bahwa perkembangan teknologi tetap berada dalam koridor hukum yang berlaku. Berdasarkan latar belakang yang telah dipaparkan di atas, penulis tertarik untuk mengangkat penelitian yang berjudul, **"ANALISIS YURIDIS PENGGUNAAN *DEEPFAKE* SEBAGAI METODE BERPERANG DALAM KONFLIK RUSIA – UKRAINA DARI PERSPEKTIF HUKUM INTERNASIONAL".**

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas, maka penulis merumuskan pertanyaan-pertanyaan penelitian sebagai berikut:

1. Bagaimana pengaturan *deepfake* sebagai metode berperang dalam hukum internasional?
2. Bagaimana penggunaan *deepfake* sebagai metode berperang dalam

[42] Sean Watts, *Op.cit*., hlm. 17.
[43] Robbert Chesney dan Danielle Citron, *Op.cit.*, hlm. 1775.

konflik Rusia-Ukraina menurut Hukum Internasional?

C. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, adapun tujuan yang ingin penulis capai adalah sebagai berikut :

1. Untuk mengetahui dan menganalisis pengaturan *deepfake* sebagai metode berperang dalam hukum internasional.
2. Untuk mengetahui dan menganalisis penggunaan deepfake sebagai metode berperang dalam konflik Rusia-Ukraina menurut Hukum Internasional.

D. Manfaat Penelitian

Melalui penelitian ini penulis berharap dapat memberikan manfaat untuk penulis sendiri maupun pembaca baik secara teoritis atau secara praktis, sebagai berikut:

1. **Manfaat Teoritis:**
   a. Memberikan klarifikasi konseptual mengenai pengaturan teknologi *deepfake* sebagai metode berperang non-kinetik dalam konflik bersenjata modern.
   b. Memperkaya diskursus akademik terkait penerapan prinsip-prinsip Hukum Humaniter Internasional terhadap perkembangan teknologi kecerdasan buatan dan perang siber.
   c. Memberikan analisis normatif mengenai batasan antara *ruses of war* yang diperbolehkan dan *perfidy* yang dilarang dalam konteks penggunaan teknologi *deepfake*.
2. **Manfaat Praktis:**
   a. Menjadi bahan rujukan bagi akademisi, mahasiswa, dan peneliti hukum

dalam memahami implikasi hukum penggunaan teknologi *deepfake* dalam konflik bersenjata.

b. Memberikan gambaran awal bagi pembuat kebijakan dan praktisi hukum internasional mengenai tantangan regulasi *deepfake* dalam konteks perang siber dan keamanan internasional.

c. Menjadi dasar pertimbangan dalam pengembangan kebijakan dan kerangka hukum di tingkat nasional maupun internasional terkait penggunaan teknologi kecerdasan buatan dalam konflik bersenjata.

E. Metode Penelitian

1. Jenis Penelitian

Jenis penelitian yang digunakan dalam tulisan ini adalah metode penelitian hukum normatif (yuridis normatif) atau sering disebut juga penelitian hukum doktrinal. Metode ini dilakukan dengan menelaah bahan-bahan pustaka, seperti peraturan perundang-undangan, putusan atau ketetapan pengadilan, kontrak/perjanjian/akad, teori hukum, serta pendapat para ahli.[44] Tahap pertama dalam penelitian hukum normatif bertujuan untuk menemukan hukum objektif (norma hukum) melalui kajian terhadap permasalahan hukum. Tahap kedua difokuskan pada pencarian hukum subjektif.

2. Pendekatan Penelitian

Penelitian hukum menggunakan berbagai pendekatan dengan tujuan memperoleh pemahaman yang komprehensif terhadap isu yang diteliti dari beragam sudut pandang. Untuk menjawab permasalahan utama dalam penelitian hukum, diperlukan penggunaan pendekatan yang tepat agar

[44] Muhaimin, 2020, *Metode Penelitian Hukum*, Mataram University Press, Nusa Tenggara Barat, hlm. 45.

analisis dapat dilakukan secara sistematis dan terarah. Pendekatan dapat dipahami sebagai cara atau metode yang digunakan untuk mencapai pemahaman terhadap permasalahan penelitian. Selain itu, pendekatan juga berfungsi sebagai sarana untuk membantu peneliti dalam memahami, membatasi, dan mengarahkan fokus permasalahan yang dikaji. Dalam penelitian hukum dikenal beberapa jenis pendekatan, yang melalui penggunaannya peneliti dapat memperoleh informasi dari berbagai aspek guna menjawab isu hukum yang diteliti.[45]

Dalam penelitian ini penulis memekai beberapa pendekatan dalam rangka mengumpulkan bahan hukum yang diperlukan, pendekatan tersebut antara lain:

a. *Statue approach*

Pendekatan ini dilakukan dengan cara menelaah seluruh peraturan perundang-undangan dan regulasi yang berkaitan dengan isu hukum yang sedang diteliti. Melalui pendekatan perundang-undangan (*statute approach*), hukum dipahami sebagai suatu sistem yang bersifat tertutup dengan karakteristik sebagai berikut:[46]

1) Komprehensif, yaitu norma-norma hukum yang ada saling berkaitan satu sama lain secara logis;
2) *All-inclusive*, yakni keseluruhan norma hukum tersebut dianggap mampu mengakomodasi berbagai permasalahan hukum yang ada sehingga tidak menimbulkan kekosongan hukum;

[45] *Ibid*, hlm.55.
[46] *Ibid*, hlm. 56.

3) Sistematis, yaitu norma-norma hukum tidak hanya saling berhubungan, tetapi juga tersusun secara teratur dan terstruktur.

b. Pendekatan Konseptual (*conspetual approach*)

Pendekatan ini bertumpu pada pandangan-pandangan serta doktrin-doktrin yang berkembang dalam ilmu hukum. Pendekatan penelitian dipilih sebagai sarana untuk menemukan jawaban atas isu-isu hukum yang dikaji dalam suatu penelitian hukum. Oleh karena itu, kesesuaian antara pendekatan yang digunakan dengan isu hukum yang diteliti menjadi pertimbangan utama dalam menentukan pilihan pendekatan tersebut.[47]

c. Pendekatan kasus (*case approach*)

Pendekatan ini dilakukan dengan cara melakukan menganalisis kasus yang berkaitan dengan isu yang dihadapi.[48]

3. Sifat Penelitian

Penelitian ini bersifat deskriptif-analitis yaitu dengan tujuan menggambarkan secara sistematis, faktual dan akurat mengenai suatu peraturan hukum, maupun hubungan antar gejala hukum yang diteliti. Metode deskriptif dipilih karena penelitian yang dilakukan adalah berkaitan dengan peristiwa-peristiwa yang sedang berlangsung.

Sifat analisis dari deskriptif dalam konteks penelitian berarti bahwa peneliti memiliki tujuan utama untuk menggambarkan, menguraikan, dan memaparkan secara sistematis karakteristik, kondisi, serta pola yang tampak pada subjek dan objek penelitian berdasarkan data yang diperoleh.

---

[47] *Ibid*., hlm. 57.
[48] *Ibid*.

Peneliti tidak berupaya untuk menguji hipotesis, menarik kesimpulan umum terhadap populasi, atau melakukan generalisasi mendalam, melainkan hanya ingin menyajikan fakta dan temuan sebagaimana adanya sesuai dengan hasil observasi, wawancara, dokumentasi, atau data sekunder.[49]

4. Jenis Data Penelitian

a. Data Sekunder

Data sekunder dalam penelitian hukum merupakan data yang diperoleh melalui penelaahan kepustakaan, yaitu dengan mengkaji berbagai literatur atau bahan pustaka yang berkaitan dengan permasalahan atau objek penelitian, yang dalam konteks penelitian hukum dikenal sebagai bahan hukum.[50] Teknik pengumpulan data sekunder dilakukan dengan cara menghimpun dan mendokumentasikan berbagai sumber kepustakaan, seperti buku, jurnal, makalah ilmiah, kamus, ensiklopedi, serta dokumen-dokumen lain yang relevan dengan permasalahan penelitian. Sumber-sumber tersebut berasal dari bahan hukum, baik bahan hukum primer, bahan hukum sekunder, maupun bahan hukum tersier.[51] Bahan Hukum yang digunakan dalam penelitian ini adalah sebagai berikut:

1) Bahan hukum primer merupakan bahan hukum yang bersifat utama dan otoritatif, yang meliputi peraturan perundang-undangan, risalah resmi, putusan pengadilan, serta berbagai dokumen resmi negara. Bahan hukum yang penulis gunakan

[49] *Ibid.*, hlm.105.
[50] Sigit Sapto Nugroho Sigit Sapto Nugroho, Anik Tri Haryani, dan Farkhani, *Loc.cit.*
[51] Muhaimin, 2020, *Op.cit*., hlm. 101.

dalam penelitian ini yakni:[52]

a) *The Hague Convention (IV) Respecting the Laws and Customs of War on Land 1907.*
b) *Charter Of The United Nations And Statute Of The International Court Of Justice 1945;*
c) *Additional Protocol I to the Geneva Conventions of 12 August 1949, adopted in 1977;*
d) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2017;*

2) Bahan hukum sekunder merupakan bahan hukum yang terdiri atas berbagai sumber pendukung, seperti buku-buku hukum, jurnal hukum yang memuat prinsip-prinsip dasar atau asas hukum, pandangan para ahli hukum (doktrin), hasil penelitian hukum, kamus hukum, serta ensiklopedia hukum. Selain itu, wawancara dengan narasumber yang memiliki keahlian di bidang hukum dapat dikategorikan sebagai bahan hukum sekunder sepanjang bertujuan untuk memperoleh pendapat hukum terhadap suatu peristiwa atau fenomena hukum. Namun demikian, narasumber tersebut harus memiliki kapasitas keilmuan yang memadai dan tidak terlibat langsung dalam peristiwa yang dikaji agar pendapat yang diberikan bersifat objektif.[53]
3) Bahan non-hukum merupakan bahan penelitian yang berasal dari sumber di luar bidang hukum, seperti buku teks non-hukum yang relevan dengan penelitian, antara lain buku politik, buku ekonomi,

[52] Sigit Sapto Nugroho, Anik Tri Haryani, dan Farkhani, 2020, *Op,.cit*., hlm.59
[53] *Ibid.*, hlm. 60.

data sensus, laporan tahunan perusahaan, kamus bahasa, serta ensiklopedia umum. Keberadaan bahan non-hukum ini penting karena berfungsi sebagai bahan pendukung yang membantu memperkaya dan memperdalam analisis terhadap bahan hukum.[54]

5. Teknik Pengumpulan Data

Teknik pengumpulan bahan hukum dalam penelitian hukum normatif pada umumnya dilakukan melalui studi pustaka dan studi dokumen, termasuk dengan menggunakan *Snowball Method* (metode bola salju) yang disesuaikan dengan kebutuhan penelitian. Pelaksanaan pengumpulan bahan hukum dapat dilakukan melalui berbagai cara, seperti penggunaan sistem kartu (*card system*), media digital seperti CD dan *flashdisk*, serta teknik pencatatan, penyalinan, perekaman, dan pendokumentasian bahan hukum lainnya.[55] Langkah-langkah yang penulis tempuh dalam mengumpulkan data hukum demi kepentingan penelitian ini adalah sebagai berikut:

a. Mengidentifikasi bahan hukum yang relevan, di mana bahan hukum yang digunakan dalam penelitian ini diperoleh dari berbagai sumber, antara lain pengaturan internasional berupa traktat atau konvensi, koleksi perpustakaan, serta tulisan-tulisan hukum maupun non-hukum yang bersumber dari media elektronik resmi, jurnal internasional, dan basis data hukum siber yang dapat diakses secara daring.

b. Menginventarisasi bahan hukum yang dibutuhkan sesuai dengan fokus penelitian, khususnya dokumen-dokumen resmi yang berasal

[54] *Ibid.*
[55] *Ibid.*, hlm. 75-76.

dari Perserikatan Bangsa-Bangsa (PBB), instrumen Hukum Humaniter Internasional seperti Konvensi Jenewa beserta Protokol Tambahannya, laporan dari *International Committee of the Red Cross* (ICRC), serta naskah interpretatif para ahli, termasuk *Tallinn Manual 2.0*, yang relevan untuk mendukung analisis mengenai kedaulatan siber dan pertanggungjawaban negara.

c. Mengutip dan memilih bahan hukum yang telah diinventarisasi yang memiliki relevansi dengan isu kualifikasi teknologi *deepfake* sebagai muslihat perang (*ruses of war*) atau pengkhianatan (*perfidy*), serta kaitannya dengan prinsip-prinsip pertanggungjawaban negara dalam ruang digital.

d. Menganalisis seluruh bahan hukum yang telah dikumpulkan guna memperoleh jawaban atas rumusan masalah terkait status hukum teknologi *deepfake* serta mekanisme pertanggungjawaban negara dalam kerangka hukum internasional.

6. Teknik Analisis Bahan Penelitian

Pada penelitian hukum yuridis-normatif, seluruh bahan hukum yang meliputi bahan hukum primer, bahan hukum sekunder, serta bahan non-hukum dikumpulkan sebagai dasar analisis. Bahan-bahan tersebut selanjutnya dianalisis untuk memperoleh konklusi atau kesimpulan yang mampu menjawab permasalahan penelitian. Analisis dilakukan dengan metode deskriptif kualitatif, yaitu dengan mengkaji bahan-bahan hukum yang telah dihimpun dan menyusunnya secara sistematis guna memberikan gambaran yang komprehensif mengenai hasil penelitian, khususnya terkait analisis yuridis penggunaan teknologi *deepfake* dalam

konflik bersenjata ditinjau dari prinsip *perfidy* dan tanggung jawab negara berdasarkan hukum internasional.

F. Sistematika Kepenulisan

Sistematika penulisan berisi bagian bab dan sub bab guna memberikan gambaran yang jelas terhadap suatu permasalahan yang akan diteliti. Sistematika penulisan penelitian ini terdiri dari 4 bab, yaitu:

BAB I: PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan

BAB II: TINJAUAN PUSTAKA

Pada bab ini dijelaskan mengenai tinjauan umum yang berkaitan dengan acuan masalah yang diteliti atau biasa disebut dengan landasan teori. Pertama, tinjauan umum tentang ruang lingkup penyelesaian sengketa internasional. kedua, tinjauan umum tentang *confidence building measures.* Ketiga, tinjauan umum tentang hukum penyelesaian sengketa internasional. keempat, tinjauan umum tentang Sengketa Kashmir antara India dan Pakistan.

BAB III: HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini memaparkan hasil penelitian dengan pembahasan ketentuan mengenai pengaturan penggunaan *deepfake* sebagai metode berperang menurut aturan Hukum Internasional serta penggunaan *deepfake* sebagai metode berperang yang digunakan oleh para pihak dalam konflik bersenjata antara Rusia dan Ukraina menurut Hukum Internasional.

BAB IV: PENUTUP

Pada bab ini terdiri dari dua bagian, yaitu kesimpulan dan saran. Kesimpulan mengemukakan secara singkat apa yang diperoleh dari penelitian serta menjawab tujuan-tujuan penelitian dan saran berisi kebijakan atau tindakan yang dianjurkan untuk diambil dalam rangka perbaikan pembangunan hukum dan ilmu pengetahuan hukum