BAB I

PENDAHULUAN

A. Latar Belakang

Hukum Internasional yang begitu luas mengatur aspek besar dalam kehidupan masyarakat global. Salah satu pengaturan yang dinilai dapat mewujudkan perdamaian dunia adalah Hukum Internasional yang mencakup jalannya konflik bersenjata. Hukum Internasional tidak melarang peperangan sebagai salah satu bentuk penyelesaian sengketa,[1] Piagam PBB Pasal 2 (4) hanya mengatur bahwa negara anggota diwajibkan untuk menahan diri dari penggunaan kekerasan dalam menyelesaikan sengketa. Apabila perang terjadi, Hukum Internasional mengatur jalannya perang dalam salah satu cabangnya yakni Hukum Humaniter Internasional. Cabang hukum tersebut memiliki pengaturan komperehensif, salah satunya mengatur mengenai partisipan sah dalam peperangan. Keabsahan partisipan dianggap penting dalam keberhasilan terwujudnya peperangan yang adil dan manusiawi dengan penegakan prinsip kemanusiaan.[2] Partisipan sah dalam peperangan disebut sebagai kombatan (*combatant*), mereka yang memenuhi ketentuan dalam Hukum Internasional dapat berpartisipasi langsung dalam

---

[1] Sefriani, "Peran Hukum Internasional dalam Hubungan Internasional Kontemporer", Indonesia: RajaGrafindo Persada (2017), hlm. 388

[2] William A Schabas, "Relationships between International Criminal Law and Other Branches of International Law", Netherlands: The Hague Academy of International Law (2022), hlm. 117

kekerasan dan berhak atas status-status yang mengikutinya.[3] Status kombatan yang memberikannya hak untuk berpartisipasi dalam kekerasan menjadikannya tidak dapat dihukum atas serangan sah yang dilakukannya dan berhak menikmati status perlindungan tahanan perang (*prisoners of war*).[4]

Perkembangannya, jalannya perang siber diatur dalam *Tallinn Manual on the International Law Applicable to Cyber Warfare*, walau belum diterima sebagai bagian dari Hukum Internasional tetapi memiliki dampak yang besar sebagai acuan dalam pelaksanaan peperangan siber karena mengandung prinsip umum dalam Hukum Internasional yang dikaitkan dengan peperangan siber (*cyber warfare*).[5] Perkembangannya, perang dapat memiliki unsur siber didalamnya. Dengan begitu peperangan memiliki tambahan partisipan dengan bentuk yang berbeda. Kombatan perang dengan unsur siber memungkinkannya untuk tidak perlu terjun dalam lapangan karena pengoperasian senjata dari jarak jauh. Hal ini memicu permasalahan baru, karena banyaknya kelompok tertentu yang berpartisipasi dalam peperangan. Ada sebagian merupakan warga sipil atau bahkan mengajukan diri mereka kepada negara untuk berpartisipasi dalam peperangan karena kemampuannya di bidang siber, seperti teknisi komputer yang mendampingi angkatan bersenjata tanpa menjadi bagian darinya, atau *patriotic hackers* yang bukan merupakan bagian dari angkatan bersenjata negara tetapi melaksanakan

[3] Angelo Stirone, "Hacking and International Humanitarian Law: the Anonymous Group and the Syrian Electronic Army", Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict Vol 3 No 1/2, 2020, hlm. 130
[4] Additional Protocol 1, Article 6 (2) (c)
[5] T Ramluckan, "International Humanitarian Law and its Applicability to the South African Cyber Environment", Journal of Information Warfare Vol 19 No. 3, 2020, hlm. 103

serangan bersenjata atas inisiatifnya sendiri.[6] Sehingga warga sipil yang berpartisipasi, secara tidak sah, dalam operasi siber kehilangan status perlindungan pada saat ia melakukan serangan sebagaimana konsep *direct participation in hostilities* dalam Hukum Humaniter Internasional.[7] Warga sipil yang kehilangan status perlindungan pada saat ia melakukan serangan dapat menjadi target sah dan dapat dibunuh pada ia melakukan serangan.[8] Pada saat perlindungan kembali melekat, warga sipil tersebut tidak dapat diserang dengan alasan apapun.[9] Hilangnya status perlindungan warga sipil saat penyerangan dilakukan menggunakan tekonologi modern menjadi perdebatan dalam komunitas internasional mengenai aplikasi konsep *Direct Participation in Hostilities* (DPH) kepada *cyber warfare* modern.[10] Perdebatan tersebut cenderung membahas bagaimana pihak lawan (baik negara maupun entitas lainnya) dapat membalas atau menetralkan serangan *cyber* tersebut apabila pelaku serangan merupakan warga sipil[11] dan urgensi dibentuknya perjanjian internasional yang mengatur *cyber warfare* serta bagaimana *cyber soldier* dapat beroperasi didalam atau diluar konteks militer tradisional.[12]

Kompleksnya permasalahan tersebut dikarenakan *cyber soldier* ada yang direkrut dari kelompok warga sipil sehingga tidak dapat diserang karena serangan

---

[6] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities", Journal of Conflict and Security Law Vol 17 No 2, 2012, hlm. 285
[7] Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 29
[8] Angelo Stirone, op.cit., hlm. 131
[9] Tracy H Slaghter and John D. van Doorn, "Fundamental Perspectives on International Law", England: Cambridge University Press (2023), hlm. 516
[10] David Turns, op.cit.
[11] Hermen Philip Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century", Baltic Journal of Law & Politics, Vol. 10, No. 1, 2017, hlm. 19
[12] Rex Hughes, "A Treaty for Cyberspace", International Affairs Vol 86 No 2, 2010, hlm. 526

balasan hanya dapat dilakukan terhadap kombatan.[13] Berbeda dengan kombatan, personel *cyber soldier* yang berasal dari warga sipil yang berpartisipasi dalam operasi siber (*cyber operations*) kehilangan status perlindungan warga sipil dan kembali menyandang status warga sipil pada saat tidak menyerang.[14]

Contohnya adalah saat negara Estonia yang merekrut angkatan siber saat mereka sedang melaksanakan konflik bersenjata dengan Rusia yang sering disebut dengan Perang Siber Pertama (The First Cyber War). Saat itu mereka mendapat serangan yang melumpuhkan keadaan nasional, sehingga mereka melaksanakan rekrutmen besar-besaran kepada warga sipil untuk memperkuat pertahanan nasional. Warga sipil yang telah terdaftar dalam Cyber Defense League (CDL) tetap melanjutkan hidup seperti biasa dan bahkan tetap bekerja seperti hidup normal mereka, namun digerakkan saat dibutuhkan oleh Estonia.[15] Estonia akan menggunakan mereka untuk mempertahankan infrastruktur nasional, mengindentifikasi kelemahan Estonia dan musuh, serta merespon insiden serangan secara spontan.[16] Tetapi terdapat *cyber soldier* yang dikenal sebagai *hacktivist*, yang bertindak secara sukarela membela negara mereka. Layaknya *hacktivist* Rusia yang melakukan peretasan terhadap Estonia dan Georgia pada 2007-2008 tanpa sepengetahuan maupun perintah Rusia.[17] Tetapi terdapat bentuk *cyber soldier* yang

---

[13] Tomasz Lewandowski, "Can Mouse Clicking Be Seen As Involvement in Armed Conflict? Some Notes on the Direct Participation in Hostilities in Cyberspace", Przeglad Prawniczy Uniwersytety Im. Adam Mickiewicza, No. 2, 2013, hlm. 198

[14] Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 29 (1) menjelaskan bahwa tidak ada Perjanjian Internasional maupun Hukum Kebiasaan Internasional yang melarang warga sipil berpartisipasi dalam konflik bersenjata

[15] Sharon L Cardash and Frank Cillufo, "Estonia's Cyber Defence League: A Model for the United States?" Studies in Conflict & Terrorism Vol 36, 2013, hlm. 779

[16] Birgy Lorenz and Kaido Kikkas, "Socially Engineered Commoners as Cyber Warriors – Estonian Future or Present?", 4th International Conference on Cyber Conflict, 2012, hlm. 223

[17] David Turns, op.cit., hlm. 298

diangkat oleh negara dan melalui proses rekrutmen sah dalam kerangka hukum negara tersebut. Salah satu negara tersebut ialah Swedia yang dikenal dengan merekrut warga sipil dengan kemampuan teknologi keamanan siber melalui proses seleksi dan pelatihan lanjutan agar dapat memperkuat keamanan siber nasional Swedia.[18] Sehingga tidak semua *cyber soldier* direkrut secara sementara (*occasional*) dari warga sipil.

Tetapi bagi yang direkrut dari warga sipil berlaku konsep DPH yang menyatakan warga sipil kehilangan status perlindungannya hanya pada saat menyerang tetapi kembali menyandang status perlindungan saat tidak lagi melaksanakan serangan.[19] Perbedaan tersebut tampak tidak adil karena seolah-olah warga sipil yang merupakan *cyber soldier* warga sipil mendapat perlakuan khusus, padahal mereka memiliki potensi untuk menimbulkan dampak yang lebih besar dan meluas daripada kombatan konvensional. Dampak besar yang dimaksud adalah mungkin untuk terjadi akibat pengoperasian senjata tertentu oleh *cyber soldier* seperti *autonomous weapons*, *drone*, *guided projectiles*, atau bahkan serangan non-fisik yang dioperasikan dari jarak jauh dan dapat melumpuhkan pertahanan siber negara.[20] Hukum Humaniter Internasional mengatur konsep DPH sedemikian rupa walau terdapat potensi kelemahan terhadap pengaturan tersebut.

---

[18] Patrik Lif et.al., "Validation of Cyber Test for Future Soldiers: A Test Battery for the Selection of Cyber Soldiers", Frontiers in Psychology Vol 13, 2022, hlm. 4

[19] Michał Byczyński, "The Legal Status of 'Civilian Hackers' Under International Humanitarian Law", Acta Universitatis Lodziensis, Vol. 106, 2024, hlm. 100

[20] Amichai Cohen and David Zlotogorski, "Proportionality in International Humanitarian Law: Consequences, Precautions, and Procedures", United States: Oxford University Press, 2021, hlm. 226-227

Indonesia sendiri memiliki permasalahan komperehensif dalam keamanan nasionalnya akibat serangan-serangan *cyber* yang telah terjadi beberapa tahun lalu. Ancaman tersebut mengancam Indonesia karena adanya perkembangan teknologi peperangan global yang begitu maju sehingga sulit untuk mengetahui atribusi atau afiliasi suatu serangan siber. Serangan dapat berasal dari individu seorang atau bagian dari kelompok, atau bahkan oleh negara. Hal tersebut memungkinkan karena serangan oleh negara memiliki perubahan bentuk yang tak harus berupa serangan fisik terhadap fasilitas vital negara, namun dapat berupa serangan terhadap fasilitas penunjang kehidupan manusia seperti air, listrik, dan bahkan minyak bumi.[21] Selain itu persenjataan kini menjadi semakin canggih karena teknologi seperti *machine learning* diprogramkan ke dalam *autonomous weapons* agar serangan dapat menjadi akurat tanpa campur tangan personel manusia lagi.[22] Serangan-serangan tersebut memiliki kekuatan destruktif lebih besar daripada serangan senjata konvensional karena dijalankan dari jarak jauh, sulit dihentikan (karena tidak ada operator di lapangan), serta rentan akan pelanggaran Hukum Humaniter Internasional.[23] Sehingga, bila tidak ada unifikasi atau *unisrmity* pengaturan mengenai *cyber soldier* maka upaya "memanusiakan" perang akan begitu sulit untuk dilakukan. Salah satu kekhawatiran yang ada, terulangnya konflik Estonia-Rusia yang melibatkan banyak warga sipil dalam peperangan siber nya.[24] Warga

[21] Amichai Cohen and David Zlotogorski, op.cit., hlm. 229
[22] Ibid, hlm. 229
[23] Rex Hughes, op.cit., hlm. 538
[24] Stephen Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity", Georgetown Journal of International Affairs Vol 18 No 3, 2017, hlm. 70

sipil menjadi terekspos dalam peperangan yang brutal karena begitu besarnya partisipasi warga sipil dari pihak Estonia, hanya demi kemenangan.[25]

Dengan begitu, terdapat urgensi besar bagi Indonesia untuk menyusun pengaturan nasional mengenai pembentukan *cyber soldier* yang tentunya memerlukan hukum nasional sebagai landasan. Maka dari itu, bedasarkan pemaparan yang ada, diperlukan penelitian lebih lanjut mengenai sejauh mana kemajuan pengaturan *cyber soldier* telah dalam Hukum Internasional, arah perkembangannya, dan bagaimana seharusnya Hukum Indonesia menyusun pengaturannya agar dapat mengantisipasi potensi kelemahan yang mungkin ada dalam Hukum Internasional.

B. Rumusan Masalah

1. Bagaimana kemajuan pengaturan *cyber soldier* menurut Hukum Internasional?
2. Bagaimana seharusnya penyusunan peraturan terkait *cyber soldier* di Indonesia agar sesuai dengan Hukum Internasional?

C. Tujuan Penelitian

1. Untuk memahami pengaturan *cyber soldier* dalam Hukum Internasional dan arah perkembangannya.
2. Untuk mengetahui penyusunan kerangka hukum Indonesia mengenai *cyber soldier* agar sesuai dan mengadaptasi potensi kelemahan pengaturan dalam Hukum Internasional.

[25] Ibid

D. Manfaat Penelitian

1. Mengetahui kemajuan pengaturan *cyber soldier* dalam Hukum Internasional dan arah perkembangannya.
2. Mengetahui penyusunan pengaturan Indonesia mengenai *cyber soldier* sesuai dan lebih adaptif dari Hukum Internasional.

E. Orisinalitas Penelitian

Penelitian ini merupakan pengembangan dari 10 (sepuluh) penelitian sebelumnya yang meneliti mengenai perkembangan perang siber (*cyber warfare*). Penelitian yang dilakukan oleh Oona Hathaway dengan judul "The Law of Cyber-Attack" mengkaji kekosongan dan ketidaksesuaian hukum internasional dan nasional dalam merespons serangan siber, yang semakin kompleks dan berdampak luas terhadap keamanan nasional. Para penulis mengusulkan perlunya definisi yang jelas tentang serangan siber dan pembedaan antara cyber-crime, cyber-attack, dan cyber-warfare, serta menyerukan pembentukan kerangka hukum internasional baru yang lebih komprehensif. Studi ini memberikan kontribusi penting dengan menunjukkan bahwa hukum yang ada saat ini hanya mampu mengatur sebagian kecil dari insiden serangan siber yang berkembang. Penelitian kedua, Michael Gervis membahas bagaimana hukum perang internasional saat ini belum sepenuhnya mampu menjawab tantangan hukum yang ditimbulkan oleh serangan siber, khususnya dalam konteks jus ad bellum dan jus in bello. Gervais mengulas pendekatan-pendekatan berbeda dalam menilai apakah serangan siber dapat dianggap sebagai penggunaan kekuatan atau bahkan sebagai serangan bersenjata dalam hukum internasional. Artikel ini memberikan kontribusi penting dalam mengisi

kekosongan konsep hukum terkait serangan siber, dengan menyoroti urgensi pembaruan kerangka hukum untuk menghadapi bentuk konflik modern. Penelitian ketiga disusun oleh Ni Putu Era Daniati yang bertujuan untuk mengkaji status hukum tentara bayaran dalam konflik bersenjata menurut Hukum Humaniter Internasional, serta menelaah sanksi hukum terhadap negara yang menggunakan jasa mereka. Penulis menyoroti bahwa tentara bayaran tidak diakui sebagai kombatan maupun tawanan perang berdasarkan Protokol Tambahan I Konvensi Jenewa 1977, dan dapat dikenai sanksi hukum nasional maupun internasional. Kajian ini menegaskan pentingnya ratifikasi konvensi internasional oleh negara-negara agar penggunaan tentara bayaran tidak menimbulkan celah hukum dalam konflik bersenjata. Penelitian kelima ditulis oleh Rahadian Diffaul Barraq Suwartono, yang membahas praktik penggunaan tentara anak oleh aktor selain negara dalam konflik bersenjata serta konsep pertanggungjawaban hukumnya menurut hukum humaniter internasional. Hasil penelitian menunjukkan bahwa anak-anak direkrut secara paksa maupun sukarela, lalu diperlakukan secara tidak manusiawi dan dilibatkan langsung dalam pertempuran oleh kelompok bersenjata non-negara.

Kemudian, penelitian keenam oleh Aram Nabee Mohammed Wasani menganalisis dampak perkembangan teknologi terhadap konsep Direct Participation in Hostilities (DPH) dalam Hukum Humaniter Internasional, terutama dalam konteks partisipasi warga sipil. Penulis berargumen bahwa teknologi modern, seperti serangan siber dan penggunaan drone, telah mengaburkan batas antara kombatan dan sipil serta menantang penerapan prinsip DPH yang tradisional.

Artikel ini menegaskan pentingnya redefinisi konsep DPH agar hukum humaniter tetap relevan dalam menghadapi bentuk konflik bersenjata kontemporer. Penelitian ketujuh oleh Tomasz Lewandowski membahas partisipasi langsung warga sipil dalam permusuhan bersenjata melalui dunia maya, dan bagaimana tindakan seperti serangan siber dapat memenuhi elemen Direct Participation in Hostilities (DPH) dalam hukum humaniter internasional. Penelitian ini menyoroti bahwa meskipun tindakan seperti klik mouse atau peretasan dari jarak jauh tampak sederhana, mereka dapat menyebabkan dampak serius yang menghilangkan perlindungan hukum bagi sipil menurut IHL. Penelitian kedelapan, Hermen Philip Faga membahas perbedaan konseptual antara cybercrime, cyber-attack, dan cyber warfare, serta dampaknya terhadap penerapan Hukum Humaniter Internasional (IHL) dalam konteks ancaman dunia maya oleh aktor non-negara. Penulis menyoroti bahwa kerangka hukum internasional saat ini belum memadai untuk merespons serangan siber lintas negara, terutama yang melibatkan kelompok teroris atau peretas independen. Penelitian kesembilan oleh Michał Byczyński, membahas status hukum peretas sipil yang terlibat dalam konflik siber, khususnya dalam konteks partisipasi langsung dalam permusuhan (DPH) menurut Hukum Humaniter Internasional. Penelitian ini menyoroti konsep continuous combat function (CCF), ambiguitas waktu dalam operasi siber, dan tantangan penerapan prinsip “revolving door” dalam menentukan kapan perlindungan sipil berlaku atau hilang. Penelitian kesepuluh, buku oleh Amichai Cohen dan David Zlotogorski berusaha membahas prinsip proporsionalitas dalam Hukum Humaniter Internasional (IHL), dengan menelaah aspek konseptual, operasional, hingga prosedural dalam penerapannya,

terutama dalam konflik asimetris. Para penulis menguraikan tantangan dalam menentukan "keuntungan militer konkret dan langsung" serta membandingkannya dengan potensi kerugian terhadap warga sipil, termasuk penggunaan perisai manusia, partisipasi langsung dalam permusuhan, dan serangan terhadap sasaran strategis. Buku ini memberikan kontribusi penting dengan menawarkan pendekatan multidisipliner dan analisis mendalam terhadap dilema etika dan hukum yang muncul dalam penerapan prinsip proporsionalitas di medan perang modern.

No.	Peneliti, Judul Penelitian, Jenis Penelitian/Publikasi, dan Tahun	Rumusan Masalah Penelitian	Perbedaan dengan Penelitian yang dilakukan oleh Peneliti
1.	Oona A. Hathaway, dkk, “The Law of Cyber-Attack”, California Law Review, Vol 100 No 4, 2012	Bagaimana sistem hukum yang diperlukan untuk mengatur cyber attack secara efektif?	Penelitian ini mengkaji status pelaku serangan siber dalam Hukum Internasional yang relevan seperti The Law of Cyber Attack dan Hukum Humaniter Internasional.
2.	Michael Gervais, “Cyber Attacks and the Laws of War”, Journal of Law & Cyber Warfare, Vol. 1 No. 1, 2012.	Bagaimana regulasi hukum yang dapat mengatur serangan siber, mengacu kepada Hukum Humaniter	Penelitian ini mengkaji hukum serangan siber secara komperehensif sedangkan penelitian penulis akan mengkaji

		Internasional terkait penggunaan senjata siber?	status cyber attacker dalam Hukum Internasional
3.	Ni Putu Era Daniati dkk., "Status Hukum Tentara Bayaran dalam Sengketa Bersenjata Ditinjau dari Hukum Humaniter Internasional", Jurnal Komunitas Yustisia Universitas Pendidikan Ganesha Program Studi Ilmu Hukum Vol 3 No 3, 2020	Bagaimana sanksi yang dapat diterapkan terhadap negara pengguna jasa tentara bayaran dalam sengketa bersenjata?	Jurnal ini mengkaji sanksi yang bisa diterapkan dalam pelanggaran hukum tentara bayaran yaitu Complaint, Reprisal, Pembayaran Ganti Rugi atau Kompensasi.
4.	I Gusti Ayu Sintiya Widayanti, dkk., "Penggunaan Tentara Anak dalam Konflik Bersenjata Ditinjau dari Perspektif Hukum Humaniter Internasional", e-Journal Komunitas Yustisia Universitas	Bagaimana pengaturan hukum yang mengatur mengenai penggunaan tentara anak dalam konflik bersenjata?	Jurnal ini mengkaji bahwa pengaturan hukum yang mengatur mengenai penggunaan tentara anak dalam konflik bersenjata.

	Pendidikan Ganesha Jurusan Ilmu Hukum Vol 2 No 2, 2019		
5.	Rahadian Diffaul Barraq Suwartono, "Perlindungan Tentara Anak yang Direkrut Oleh Non State Actor pada Konflik Bersenjata", Skripsi, Universitas Islam Indonesia, 2019	Bagaimana praktik penggunaan tentara anak di lapangan oleh non state actor? Apakah pengaturan hukum humaniter internasional tentang penggunaan tentara anak dapat diterapkan pada non state actor? Bagaimanakah mekanisme sanksi terhadap penggunaan tentara anak oleh non state actor?	Skripsi ini mengkaji praktik pola perekrutan tentara anak oleh non state actor dilakukan melalui mekanisme sukarela dan paksaan.
6.	Aram Nabee Mohammed Wasani et.al., "The Effect of New Technology on the Concept of "Direct Participation in Hostilities" in International	Tindakan apa yang dapat memenuhi sebagai *direct participation in hostilities*? Apakah konsep terkini mengenai *direct participation in hostilities*	Jurnal ini mengkaji direct *participation in hostilities*, khususnya partisipasi sipil dalam konflik bersenjata internasional dan non-internasional.

	Humanitarian Law", Academic Journal of Nawroz University, Vol. 1, No. 1, 2023	dapat merespon kasus-kasus terkini? Tantangan apakah yang muncul mengenai partisipasi warga sipil dalam *hostilities*?	
7.	Tomasz Lewandowski, "Can Mouse Clicking Be Seen As Involvement in Armed Conflict? Some Notes on the Direct Participation in Hostilities in Cyberspace", Przeglad Prawniczy Uniwersytety Im. Adam Mickiewicza, No. 2, 2013	Bagaimana dampak perkembangan teknologi dalam peperangan modern? Mengapa warga sipil berpartisipasi dalam kekerasan melalui jaringan siber?	Jurnal ini mengkaji dampak dari perkembangan teknologi dalam peperangan modern.
8.	Hermen Philip Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber	Bagaimana perbedaan cybercrime, cyber-attack, dan cyber warfare di masa kini?	Jurnal ini meneliti perbedaan antara konsep kejahatan siber, serangan siber, dan perang siber dalam era informasi saat ini, di mana semakin sulit membedakan antara

	Warfare in the 21st Century", Baltic Journal of Law & Politics, Vol. 10, No. 1, 2017		aktivitas pelaku kejahatan transnasional dan tindakan para kombatan yang menggunakan ruang siber.
9.	Michał Byczyński, "The Legal Status of 'Civilian Hackers' Under International Humanitarian Law", Acta Universitatis Lodziensis, Vol. 106, 2024	Bagaimana status hukum warga sipil yang terlibat aktif dalam permusuhan siber, khususnya terkait konsep partisipasi langsung dalam permusuhan (DPH) dalam konteks perang siber? Apa saja tantangan dalam membedakan antara tindakan warga sipil yang terkait dengan konflik bersenjata yang sedang berlangsung dan tindakan yang terjadi secara independen dalam perang siber?	Artikel ini mengeksplorasi konsep partisipasi langsung dalam permusuhan (DPH) dalam konteks perang siber, dengan menekankan perlunya pendekatan yang lebih cermat dan kontekstual dalam menentukan status hukum warga sipil yang terlibat dalam permusuhan siber.

10.	Amichai Cohen dan David Zlotogorski, “8 Direct Participation in Hostilities and Its Effect on Proportionality”, Proportionality in International Humanitarian Law: Consequences, Precautions, and Procedures, (Amerika Serikat: Oxford Academic) 2021	Bagaimana konsep Partisipasi Langsung dalam Permusuhan (Direct Participation in Hostilities/DPH) mempengaruhi penerapan prinsip proporsionalitas dalam Hukum Humaniter Internasional (HHI)? Apa saja tantangan dalam mendefinisikan dan mengidentifikasi warga sipil yang secara langsung berpartisipasi dalam permusuhan, terutama dalam konteks konflik bersenjata modern yang sering melibatkan percampuran antara kombatan dan warga sipil? Bagaimana penerapan prinsip pembedaan dan proporsionalitas dalam	Buku ini memberikan kajian mendalam tentang konsep Partisipasi Langsung dalam Permusuhan (Direct Participation in Hostilities/DPH) dan dampaknya terhadap prinsip proporsionalitas dalam Hukum Humaniter Internasional (HHI).

		situasi konflik asimetris dan non-internasional, serta bagaimana hukum humaniter internasional menangani perubahan dalam karakteristik peperangan modern?	

Perbedaan sepuluh penelitian diatas dengan penelitian ini adalah obyek kajian dan aspek yang diteliti. Beberapa diantaranya meneliti status dan perlindungan tentara anak maupun bayaran dalam Hukum Internasional, konsep *direct participation in hostilities*, dan prakteknya dalam medan perang modern. Namun penelitian-penelitian sebagaimana dijelaskan belum ada yang meneliti mengenai perkembangan pengaturan *cyber soldier* dalam Hukum Internasional dan bagaimana seharusnya sikap Indonesia terhadap kebaharuan serta perkembangan tersebut. Penelitian ini juga akan mengkaji permasalahan tersebut dengan mengacu pada *Tallinn Manual on the International Law Applicable to Cyber Warfare* dan urgensi adanya perubahan tertentu serta adopsi menjadi Perjanjian Internasional.

F. Landasan Teori

Penelitian ini akan bertumpu pada Hukum Internasional dan cabangnya yakni Hukum Humaniter Internasional. Instrumen hukum dalam Hukum Humaniter Internasional telah memberikan panduan dan pengaturan dasar dalam pelaksanaan perang. Instrumen tersebut seperti keempat Konvensi Jenewa beserta

protokolnya.[26] Tidak kurang juga *commentary* serta berbagai instrumen hukum komplementer yang turut memberikan sumbangan kepada teori dan prinsip yang ditegakkan dalam pelaksanaan perang.[27] Teori dan prinsip relevan dengan penelitian ini adalah:

1. **Teori Cyber Soldier**

   Tentara dalam Matra Siber berbeda dengan satuan-satuan khusus siber yang ada dalam Matra Darat. Secara esensi Matra Siber merupakan personel-personel yang murni diseleksi, di didik, diangkat, dan dilatih dalam lingkup siber oleh suatu negara untuk menetralisir serangan siber terhadap kedaulatan negara.[28] Sehingga dalam konteks siber, kombatan sah dalam peperangan adalah *cyber soldier* yang secara otoritas dapat melaksanakan perintah negara karena proses rekrutmen nasional negara secara sah.[29] Tidak seperti yang terjadi dalam salah satu peperangan siber pertama dunia, yakni Estonia-Rusia. Peperangan tersebut menjadi salah satu kejadian penting dalam perkembangan Hukum Internasional dalam lingkup *cyberwarfare*. Peperangan yang terjadi pada tahun 2007 menjadi tinjauan berbagai ahli Hukum Internasional dengan timbulnya berbagai istilah dan entitas dalam suatu peperangan siber.[30] Cyber soldier harus dipisahkan dari hacktivist, entitas sipil temporer yang hanya

---

[26] Amichai Cohen dan David Zlotogorski, Proportionality in International Humanitarian Law Consequences, Precautions, and Procedures, England: Oxford University Press, 2021, hlm. 28
[27] William Slomanson, Fundamental Perspectives on International Law, United States: Wadsworth, 2010, hlm. 526
[28] Noah Simmons, "A Brave New World Applying International Law of War to Cyber-Attacks", Journal of Law & Cyber Warfare Vol. 4 No. 1, hlm. 101-103
[29] James E McGhee, "Hack, Attack or Whack; The Politics of Imprecision in Cyber Law", Journal of Law & Cyber Warfare Vol. 4 No. 1, 2014, hlm. 15
[30] Eric Talbot Jensen, "The Tallinn Manual 2.0 Highlights and Insights", Georgetown Journal of International Law Vol 48, 2017, hlm. 756

berpartisipasi dalam perang. Hacktivist dan sejenisnya dianggap sebagai non-kombatan karena bukanlah tentara dan entitas yang dibenarkan dalam Hukum Internasional karena mereka hanyalah warga sipil yang berpartisipasi secara sementara hanya pada saat konflik berjalan.[31] Konflik Estonia-Rusia inilah yang menjadi salah satu tahapan penting dalam perkembangan Hukum Internasional karena memberikan suatu kasus nyata mengenai peperangan siber dan potensi pelanggaran terhadap Hukum Internasional yang dapat terjadi.

2. Teori *Distinction* dan *Proportionality*

Jalannya konflik bersenjata harus mematuhi apa yang dikenal sebagai *distinction*, hal tersebut mengacu pada Hukum Humaniter positif seperti keempat Konvensi Jenewa 1949, yang telah *entered into force* pada 21 Oktober 1950, dan telah diratifikasi oleh semua negara.[32] Beberapa aturan kebiasaan yang dipakai sebagai acuan, beserta Protokol tambahannya juga harus ikut dalam pertimbangan pelaksanaan perang, termasuk mengenai *distinction*.[33] Prinsip ini berangkat dari gagasan bahwa konflik bersenjata harus berlangsung dengan membedakan kombatan dan non-kombatan serta obyek militer dan non-militer.[34] Garis batas (*dichotomy*) antara kombatan dan non-kombatan ini sangatlah penting, karena mengatur siapa yang boleh dan tidak boleh berpartisipasi dalam pertempuran di medan perang. Elemen dan komponen

---

[31] Noah Simmons, op.cit., hlm. 79
[32] Martin Dixon etc., *Cases and Materials on International Law*, England: Oxford University Press, 2016, hlm. 552
[33] Ibid
[34] René Provost, "International Human Rights and Humanitarian Law", England: Cambridge University Press, 2004, hlm. 42-43

penting dalam *distinction* adalah perlindungan warga dan obyek sipil, serta proporsionalitas. Yang dimaksud dengan perlindungan warga dan obyek sipil adalah baik warga dan obyek sipil tidak boleh menjadi sasaran serangan[35] sehingga tidak dapat berpartisipasi dalam konflik bersenjata. Hal tersebut ditujukan agar mencegah kerusakan, penderitaan yang tidak perlu, dan kematian warga sipil. Sehingga serangan apapun yang tidak membedakan targetnya dilarang untuk dilakukan dan dapat termasuk dalam kejahatan perang (war crimes).[36] Mengenai proporsionalitas, prinsip ini memiliki korelasi dengan elemen *necessity* dan *humanity*. Imunitas warga sipil dari serangan tidak serta-merta menjadikan suatu serangan ilegal karena terdapat korban sipil.[37] Dengan syarat, serangan yang terjadi tidak berlebihan melebihi kebutuhan yang ada (*exceeding the necessity*).

3. Teori *Direct Participation in Hostilities*

Konsep *direct participation in hostilities*, merupakan konsep penting dalam Hukum Humaniter Internasional. Konsep *direct participation in hostilities* merujuk kepada tindakan yang dilakukan warga sipil pada suatu konflik bersenjata yang menjadikan mereka sah untuk dilukai atau bahkan dibunuh.[38] Hal tersebut diatur dalam Additional Protocol I Pasal 51 (3) yang menyatakan bahwa:

---

[35] Roland Otto, "Targeted Killings and International Law", United States: Springer Heidelberg Dordrecht, 2010, hlm. 270
[36] Martin Dixon, op.cit., hlm. 555
[37] Roland Otto, op.cit., hlm. 217
[38] Amichai Cohen dan David Zlotogorski, op.cit., hlm. 136

”*Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities*.”

Dengan kata lain, setiap warga sipil menikmati perlindungan hukum kecuali pada saat tertentu (sekejap tersebut) mereka melakukan serangan. Mereka pun dapat diserang bahkan oleh kombatan yang telah diatur dalam hukum seperti tentara, milisi, atau kombatan sah lainnya.[39] Tetapi warga sipil kehilangan status perlindungannya dan hanya dapat diserang terbatas pada saat mereka melakukan serangan, tidak lebih dan tidak kurang.[40] Sebenarnya pelaksanaan perang siber belum memiliki banyak acuan hukum karena konsepnya yang masih relatif baru. Pelaksanaan perang dengan unsur siber juga diatur *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Tetapi karena Tallinn Manual tidaklah mengikat[41] dan general comment pada Additional Protocol I tidaklah cukup untuk menawarkan penjelasan komperehensif, timbullah celah-celah hukum. Sehingga untuk mengisi celah hukum, International Committee of the Red Cross (ICRC) menerbitkan ”*Interpretive Guidance on the Notion of Direct Participation in Hostilities*” yang memberikan petunjuk pemenuhan elemen wajib dalam penentuan *direct participation in cyber hostilities* yakni (1) *threshold of harm*; (2) *direct causation*, dan (3) *belligerent nexus*.[42] Sehingga apabila memenuhi ketiga

[39] Rahadian D B Suwartono, “Perlindungan Tentara Anak yang Direkrut oleh Non-State Actor pada Konflik Bersenjata”, Skripsi: Universitas Islam Indonesia (Yogyakarta), 2019, hlm. 18-19
[40] Elizabeth Mavropoulou, ”Targeting in the Cyber Domain Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks”, Journal of Law & Cyber Warfare Vol 4 No 2, 2015, 78
[41] Tallinn Manual on the International Law Applicable to Cyber Warfare, Rule 25
[42] Elizabeth Mavropoulou, op.cit., hlm. 79-80

elemen tersebut, maka tindakan siber seorang warga sipil dapat dikategorikan sebagai *direct participation in hostilities*. Kedudukan Tallinn Manual yang hanya sebagai panduan tak mengikat sama dengan *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*. Manual tersebut memiliki cakupan regulasi yang mengatur aktivitas maritim antar negara secara damai maupun dalam keadaan perang.[43] San Remo yang bukan merupakan perjanjian (sehingga tidak mengikat), tetap menjadi rujukan dalam melakukan peperangan dalam lingkup maritim.[44]

Agama Islam sendiri mengatur personel yang dapat berpartisipasi dalam perang dalam Islam adalah yang sudah dewasa (baligh), berakal, merdeka (bukanlah budak), laki-laki (walau perempuan dapat berpartisipasi bila mendapat izin suaminya dan anak atas izin orang tuanya), bukanlah seorang difabel, dan tidak sakit. Rasulullah SAW memberikan teladan setelah beliau menaklukkan Mekah, ia tidak melakukan perusakan bangunan dan properti serta memerintahkan agar pihak yang tertangkap dan terluka berada dalam perlindungannya.[45] Status perlindungan juga diberikan oleh Agama Islam bagi non-kombatan, sehingga Muslim yang berperang atas nama Allah tidak boleh melebihi batas dengan menyakiti pihak yang mendapat perlindungan. Pihak

[43] Fabio van Loon, "Codifying Jus in Bello Spatialis—The Space Law of Tomorrow", Strategic Studies Quarterly Vol 15 No 1, 2021, hlm. 14
[44] Efthymios D. Papastavridis, "The Use of Force at Sea in the 21st Century/ Some Reflections on the Proper Legal Framework(s)", The Journal of Territorial and Maritime Studies Vol 2 No 1, 2015, hlm. 122
[45] Miebaka Nabiebu, "Comparative Study of Islamic and International Humanitarian Law", International Journal of Law and Society Vol 2 No 3, 2023, 248

yang dimaksud adalah orang tua yang lemah, wanita, budak, dan anak kecil.[46] Tetapi pihak yang telah mengambil peran atau bahkan berpartisipasi dalam peperangan maka kehilangan status perlindungannya dan dapat diserang kembali dengan alasan membela diri. Hal tersebut sesuai tuntunan Rasulullah SAW yang melarang pembunuhan seseorang di medan perang dengan tanpa alasan yang dibenarkan.[47]

G. Definisi Operasional

1. *Cyber Soldier*

Cyber soldier belum memiliki definisi yang tetap karena memiliki banyak bentuk dalam berbagai situasi. Tetapi secara umum, *cyber soldier* merujuk kepada individu sipil yang memiliki keahlian tertentu atau spesialisasi dalam keamanan siber dan dilatih untuk melindungi infrastruktur suatu negara dari ancaman digital.[48] *Cyber soldier* merupakan salah satu perkembangan bentuk personel dalam konflik bersenjata dimana perang biasanya memiliki partisipan fisik dan kasat mata, kini penyerang bahkan tidak perlu untuk meninggalkan ruangannya karena segala persenjataan dapat dikontrol dari jarak jauh. Bahkan *cyber soldier* memiliki keahlian tertentu yang tidak dimiliki milisi biasa selain pengoperasian senjata canggih seperti pengambilan, pemrosesan, analisa, dan penyerangan bedasarkan data serta informasi mengenai pertahanan suatu

[46] Dwi Astuti Palupi dan Ahmad Iffan, "Human Rights in International Humanitarian Law and the Perspective of Islamic Sharia", South East Asia Journal of Contemporary Business, Economics and Law Vol 29 No 1, 2023, 55
[47] Ataullah Khan Mahmood et.al., "Direct Participation in Hostilities: A Comparative Study of the Norms of Islamic Law and International Humanitarian Law, Al-Adwa Vol 35 No 53, 2020, hlm. 240
[48] Patrik Lif et.al., op.cit., hlm. 3

negara.[49] *Cyber soldier* memiliki peran penting dalam konteks militer dan sipil, tidak jarang personel direkrut dari keduanya untuk menangani *cyber warfare*, espionase, dan keamanan suatu negara.[50] Sehingga proses seleksi dan rekrutmen *cyber soldier* sah memiliki perbedaan dan kesulitan tertentu. Negara seperti Swedia melakukan rekrutmen dengan memiliki beberapa kriteria harus dapat dipenuhi oleh kandidat, terdapat tes beragam yang berupa pengujian 8 (delapan) dimensi perilaku dan personalitas serta 5 (lima) kemampuan kognitif.[51]

Kualifikasi yang diatur dari negara sangatlah berat dan kompleks karena kelangsungan pertahanan siber negara berada pada personel-personel tersebut. Sehingga negara berlomba-lomba dalam membangun memperkuat pertahanan dengan memperkuat pasukan siber mereka. Negara China membangun pasukan unit "Blue Army", Korea Utara dengan unit "121", dan Russia dengan perluasan divisi siber Federal Security Service (FSB) nya untuk satu tujuan utama yakni sebagai penegasan komitmen nasional mereka atas penguatan pertahanan siber negara.[52] Tetapi, terdapat beberapa kasus yang tidak biasa dimana negara tertentu seperti Estonia yang menggelar rekrutmen relawan *hacker* serta individu sipil dengan kemampuan *cyber* untuk berpartisipasi dalam konflik bersenjata yang terjadi dalam kurun waktu tertentu saja (tidak

[49] Jae Hyun Shin et.al., "The Role and Responsibility of Cyber Intelligence in Cyber Warfare", Advanced Science and Technology Letters Vol. 51, 2014, hlm. 306
[50] Ibid
[51] Patrik Lif et.al., op.cit.
[52] Iradhati Zahra dan Diajeng Wulan Christianti, "The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual 1.0, Padjadjaran Journal of International Law Vol 5 No 1, 2021, hlm. 104

diangkat menjadi personel tentara secara tetap).[53] Bentuk *cyber soldier* seperti inilah yang telah mendapat perhatian dan menjadi perdebatan dalam komunitas internasional mengenai legalitas serta status yang melekat kepadanya, sebab bentuk tersebut memiliki garis yang sangat tipis antara warga sipil dan tentara.

2. Keamanan Nasional (*National Security*)

Istilah keamanan nasional (*national security*) sering digunakan dalam berbagai konteks, sehingga tidak memiliki istilah tertentu yang digunakan secara universal. Konsep yang dapat disetujui secara umum merujuk kepada tindakan suatu negara untuk memperkuat perlindungan dan pemeliharaan kedaulatan negara, baik secara teritorial, politik, dan kestabilan ekonomi.[54] Selain itu, keamanan nasional memiliki cakupan dan dimensi yang luas yakni militer, ekonomi, lingkungan, serta aspek ekonomi, sosial, dan budaya lainnya. Kini dengan potensi dan perkembangan teknologi beberapa komponen pertahanan mendapat perhatian khusus dari komunitas global. Komponen keamanan nasional yang kini tak kalah penting untuk dilindungi adalah dalam lingkup *cybersecurity* (keamanan siber).[55] Keamanan siber sangatlah penting karena ancaman teknologi semakin nyata, hal tersebut dibuktikan dengan tindak kejahatan berbasis siber yang terjadi di seluruh dunia tidak terkecuali Indonesia. Serangan-serangan seperti 9/11 yang terjadi melalui penembusan keamanan Pentagon, serangan siber Negara Estonia pada tahun 2007, kasus

---

[53] NPR, "Volunteer Cyber Army Emerges In Estonia", https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation, diakses pada 20 September 2024

[54] Jonna Nyman, "Towards a Global Security Studies: What Can Looking at China Tell Us about the Concept of Security?", European Journal of International Relations Vol 29 No 3, 2023, hlm. 676

[55] Asmadi et.al., op.cit., hlm. 100-101

Stuxnet di Iran, serta serangan siber dalam konflik Georgia dan Russia menjadi sebuah peringatan global terhadap urgensi perluasan cakupan dalam konteks keamanan nasional.[56]

H. Metode Penelitian

1. Jenis Penelitian

Penelitian ini adalah penelitian dengan tipe normatif. Penelitian ini menggunakan hukum sebagai norma yang meliputi aturan, doktrin, dan putusan pengadilan yang relevan dengan obyek penelitian ini.

2. Fokus Penelitian

Fokus penelitian ini adalah menganalisis status hukum cyber soldier dalam perspektif Hukum Humaniter Internasional dan relevansinya terhadap pembentukan serta pengaturan Matra Siber di Indonesia. Penelitian ini juga menitikberatkan pada bagaimana norma internasional, khususnya Konvensi Jenewa 1949, Protokol Tambahan 1977, dan Tallinn Manual (1.0 dan 2.0), dapat dijadikan rujukan dalam menyusun instrumen hukum nasional yang sesuai dan implementatif dalam konteks pertahanan siber.

3. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan historis, komparatif, perundang-undangan, dan konseptual. Pendekatan historis dilakukan dalam kaitannya untuk memahami makna dari aturan hukum dari masa ke masa serta memahami perubahan dan perkembangan makna yang mendasari aturan hukum tersebut. Pendekatan perundang-undangan digunakan untuk meninjau aturan hukum apa

[56] Iradhati Zahra dan Diajeng Wulan Christianti, op.cit

saja yang digunakan dan mengatur tentang penggunaan self defense. Pendekatan ini juga digunakan untuk memahami korelasi antara das sollen dan das sein. Pendekatan konseptual dilakukan untuk memahami aturan dan kaidah yang berlaku dalam hukum humaniter. Pendekatan ini juga membantu pelaksanaan penelitian untuk memahami pelaksanaan dari norma hukum yang berlaku.

4. Sumber Data Penelitian

a. Sumber Primer

Penelitian ini menggunaka sumber primer seperti Geneva Conventions 1949, Additional Protocol 1977, Tallinn Manual on the International Law Applicable to Cyber Operations (1.0 dan 2.0), Undang-Undang (UU) Nomor 3 Tahun 2002 tentang Pertahanan Negara, Undang-Undang (UU) Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, Peraturan Pemerintah (PP) Nomor 39 Tahun 2010 tentang Administrasi Prajurit TNI, Peraturan Panglima TNI Nomor 31 Tahun 2020 tentang Perubahan atas Peraturan Panglima TNI Nomor 27 Tahun 2017 tentang Penerimaan Perwira Prajurit Sukarela TNI, dan Peraturan Panglima TNI Nomor Perpang/45/VII/2008.

b. Sumber Sekunder

Penelitian ini menggunakan sumber sekunder seperti buku kajian Hukum Internasional, Jurnal Internasional, dan Jurnal Nasional terakreditasi, serta publikasi ilmiah relevan lainnya.

c. Sumber Tersier

Penelitian ini menggunakan sumber tersier seperti Black Law's Dictionary serta buku sejenis yang relevan lainnya.

5. Analisis Data

Teknik analisa data dalam penelitian ini adalah analisis data kualitatif yang meliputi kegiatan pengklasifikasian data, penyuntingan, penyajian hasil analisa dalam bentuk narasi yang bersifat deskriptif dan analitis.